Security of advanced quantum key distribution protocols in realistic conditions

Guillermo José Currás Lorenzo

Faculty of Engineering

University of Leeds

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

May 2021

The candidate confirms that the work submitted is his own, except where work which has formed part of jointly authored publications has been included. The contribution of the candidate and the other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others.

The work in Chapter 2 is a manuscript currently under peer review:

Currás-Lorenzo, G., Navarrete, Á., Pereira, M., & Tamaki, K. (2021). Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory. Physical Review A **104**, 012406. DOI: 10.1103/PhysRevA.104.012406.

K.T. and the candidate independently conceived the original idea behind the work. As the lead author, the candidate devised the security proof and performed the simulations for the prepare-and-measure protocol, together with M.P., and devised and the security proof and performed the simulations for the measurement-device-independent protocol, together with A.N. The candidate wrote more than half of the manuscript, while A.N. and M.P. wrote the rest. K.T. checked the validity of the results, and provided feedback on the content of the manuscript and its writing.

The work in Chapter 3 of this thesis has appeared in publication as follows:

Currás Lorenzo, G., & Razavi, M. (2020). Finite-key analysis for memory-assisted decoy-state quantum key distribution. New Journal of Physics **22**, 103005. DOI: 10.1088/1367-2630/abb16b.

As the lead author, the candidate performed most analytical calculations and all numerical simulations, as well as wrote the majority of the manuscript. M.R. conceived the original idea behind the work, checked the validity of the results, provided feedback on the security proof and improved the writing of the paper.

The work in Chapter 4 and Appendix A of this thesis has appeared in publication as follows:

Currás-Lorenzo, G., Navarrete, Á., Azuma, K., Kato, G., Curty, M., & Razavi, M. (2021). Tight finite-key security for twin-field quantum key distribution. npj Quantum Information **7**, 22. DOI: 10.1038/s41534-020-00345-3.

As the lead author, the candidate conceived the original idea behind the work, proposed more than half of the steps in the security proof, computed the numerical results, and wrote the majority of the manuscript. All authors contributed to constructing the security proof, checking the validity of the results and providing feedback on the content and writing of the article.

The work in Chapter 5 of this thesis has appeared in publication as follows:

Currás-Lorenzo, G., Wooltorton, L., & Razavi, M. (2021). Twin-field quantum key distribution with fully discrete phase randomization. Physical Review Applied **15**, 014016. DOI: 10.1103/PhysRevApplied.15.014016.

As the lead author, the candidate conceived the idea behind the work, devised the security proof, and wrote the majority of the manuscript. L.W. performed some of the numerical simulations, and provided some feedback, both in the ideas of the paper and its writing. M.R. checked the validity of the results, provided feedback on the security proof and improved the writing of the manuscript.

Acknowledgements

I would like to start by sincerely thanking my supervisor, Mohsen Razavi, for all his support, on both a professional and personal level, for all that I have learned from him, for his patience, for believing in me, and for giving me the freedom to pursue the projects that I was most interested in. Also, I would like to thank him for his hard work in coordinating the European Innovative Training Network QCALL.

Thanks also to everyone in Mohsen's group in Leeds: Daniel Alsina, Sima Bahrani, Osama Elmabrok, Masoud Ghalaii, Yumang Jing, Shradhanjali Sahu and Lewis Wooltorton. Special thanks to my friend Daniel for the many good moments, discussions, and squash games we had together.

I would also like to thank Marcos Curty for teaching me about quantum cryptography, and pushing me to pursue a PhD in the field. Without him, I definitely would not be writing this thesis. Thank you also for receiving me during my long secondment in the University of Vigo, in which I learned a lot about the security of QKD.

Thanks also to the members of Marcos' group, Álvaro Navarrete, Margarida Pereira, Róbert Trényi, Weilong Wang and Víctor Zapatero, who made me feel like the sixth member of the group. Special thanks to my friend Álvaro for our discussions and collaborations.

I am very grateful for having been a part of QCALL, which has allowed me to meet exceptional people and visit beautiful places. I would like to thank all of its members. A special thank you goes to all my fellow Early Stage Researchers.

I would also like to thank all the other people whom I have had the pleasure to collaborate with, and learn from, in the past four years. Special thanks

to Koji Azuma, Go Kato, and Kiyoshi Tamaki. Thanks also to Bill Munro, and everyone in his group, for receiving me during my secondment in NTT.

I would like to thank my parents, Ana and Pepo, for their relentless support and unconditional love. Another thank you goes to all my friends, and to Pilar, for all her support in my decision to start my PhD and during my first year.

Finally, I would like to thank my partner, Margarida. On a professional level, thank you for all our discussions, and for your feedback in writing this thesis. On a personal level, a heartfelt thank you for always standing by my side, loving me, and helping me grow as a person.

The work in this thesis was funded by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement number 675662 (QCALL).

Abstract

Quantum key distribution (QKD) allows two users to generate a random secret key, which they can use to securely exchange a message. Unlike many other cryptographic schemes, QKD offers information-theoretical security based on the laws of physics. In recent years, major theoretical and experimental advancements have been made. Among these are two novel protocols, memory-assisted (MA) QKD and twin-field (TF) QKD, which can both improve the secret-key rate scaling with channel length, potentially allowing QKD to be performed at longer distances. The main motivation of this thesis is to incorporate more realistic assumptions into the security proofs and performance analyses of these new protocols.

One common assumption made in QKD security proofs is that the protocol is run for an infinitely long time, which allows the users to obtain a perfect statistical characterisation of the quantum channel. In this thesis, we drop this assumption for a TF-QKD variant that is well suited for experimental implementation, proving its security in the finite-key regime. We also analyse the finite-key performance of MA-QKD, concluding that it is particularly resistant to its statistical fluctuation effects. Moreover, we develop an alternative finite-key security analysis approach based on random sampling theory, and apply it to the loss-tolerant protocol, which can ensure security in the presence of flawed sources. Compared to previous finite-key security proofs of the protocol, our analysis offers better performance.

Another common assumption is that the users can emit laser pulses with a continuous random phase. In practice, this is difficult to achieve, and the phase is often randomised discretely. In this thesis, we prove the security of a TF-QKD variant that relies on discrete phase randomisation, and show that, using certain post-selection techniques, it can provide higher secret-key rates than an equivalent continuously-randomised protocol.

Abbreviations

BS	Beam splitter
BSM	Bell-state measurement
CA	Cold atom
EPP	Entangled photon pair
IID	Independent and identically distributed
QKD	Quantum key distribution
QM	Quantum memory
QND	Quantum-non-demolition
LT	Loss-tolerant
MA	Memory-assisted
MDI	Measurement-device-independent
PBS	Polarising beam splitter
PDF	Probability density function
P&M	Prepare-and-measure
POVM	Positive operator-valued measurement
PRCS	Phase-randomised coherent state
RHS	Right-hand side
SDP	Semidefinite programming
SNSPD	Superconducting nanowire single-photon detector
SPD	Single-photon detector
SPFs	State preparation flaws
SV	Silicon vacancy
TF	Twin-field
USD	Unambiguous state discrimination
WV	Warm vapour
WCP	Weak coherent pulse

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Over the past half century, our increasingly globalised society has come to depend on the secure exchange of information between physically distant locations. To achieve this, we rely mostly on certain cryptographic algorithms that can guarantee secrecy even if the physical communication channels that carry the messages are compromised. The security of an important class of these algorithms is based on certain mathematical problems that are thought, but not proven, to be very hard for conventional computers to solve. For this reason, they are vulnerable to improvements in computational hardware and software. Rapid advancements could put a halt to our ability to securely exchange messages, potentially causing severe societal disruptions. Slow advancements could give us time to update our cryptographic infrastructure, but they would still compromise the secrecy of the information being exchanged today, an important problem for sensitive applications that need long-term security, such as DNA data or medical records.

The appearance of a new computation paradigm, quantum computing, poses a particularly severe threat, since quantum computers have already been shown to provide exponential speed-ups in solving the very mathematical problems that our current cryptographic systems are based on. Interestingly, the emerging field of quantum communications could also provide a solution to the problem. Namely, its most mature application, quantum key distribution (QKD), can provide information-theoretic communication security based on the laws of physics, rather than on computational assumptions. Thus, it is not vulnerable to future hardware or software advancements, ensuring long-term communication security. In the last decades, intense research ef-

forts have resulted in tremendous progress, on both the theoretical and experimental fronts of QKD. However, it still needs to solve important practical problems before it can be deployed as an alternative, or a complement, to our current cryptographic infrastructure.

In this thesis, we focus on two of the most important of these problems: (1) ensuring that practical QKD implementations are secure, despite inevitable imperfections; and (2) preventing QKD communication rates to drop sharply as the channel distance increases. In particular, in the recent years, novel protocols have been proposed to improve the key rate scaling with the channel length, potentially allowing QKD to be performed over longer distances. Understandably, the first security and performance analyses of these new protocols have assumed idealised experimental conditions. The main motivation of this thesis is addressing the security and performance of these protocols under more realistic assumptions.

In this introductory chapter, we lay down the relevant background to the work presented in this thesis, and, in that context, we summarise our novel contributions. In Section 1.1, we situate QKD in the wider field of cryptography, the problem it can solve, and give an intuition of why it can do so. Then, we continue by reviewing the fundamental ideas behind QKD and its security. After that, in Section 1.2, we provide an overview of the challenges currently preventing QKD from becoming a global technology, with a focus on how the work presented in this thesis has contributed towards overcoming these challenges.

1.1 Background

The aim of cryptography is to provide secure communications in the presence of an adversary. In this thesis, we focus on the problem of ensuring communication confidentiality over an untrusted channel, one of the most fundamental goals of cryptography. We assume that a sender, Alice, wants to send a secret message to a receiver, Bob, through an untrusted channel that may be accessed, or even fully controlled, by an eavesdropper, Eve.

Cryptography has a long history, but modern academic research on the field started in the 70s, when public-key cryptography, and, in particular, the widely used RSA [1] algorithm, was developed. In these schemes, Bob has two keys associated to him: a

public key, which he publicly announces, used to encrypt messages destined to him; and a private key that only Bob himself knows, which he uses to decrypt these messages. That is, if Alice wants to send a message to Bob, she encrypts it with Bob's public key, and then sends the ciphertext to Bob, who decrypts it using his private key.

These schemes are widely used because of their convenience, as the same public-private key pair can be reused to encrypt and decrypt many messages. However, their security is based on certain problems that are thought (but not proven) to be very hard for current computers to solve. For example, the security of RSA is based on the assumed difficulty of finding the prime factors of very large composite numbers. For this reason, public-key cryptography is vulnerable to breakthrough developments in hardware and software. One of these would be the advent of quantum computers, since Shor [2] devised a quantum algorithm that can perform prime factorisation in polynomial time, much faster than the sub-exponential time needed by known classical algorithms [3]. Thus, if a large-scale quantum computer is ever developed, an eavesdropper could use it to decrypt secret communications based on public-key cryptography, including those made many years before, if she had the foresight to make a copy of the ciphertext. Today, after decades of intense theoretical and experimental research, small-scale quantum computers can already provide computational advantages in some very specific tasks [4]. Given that multinationals around the world have already invested billions of dollars in the race to build the first truly practical quantum computer, the possibility that they may succeed in the next decades cannot be ignored.

Clearly, it is essential to update our cryptographic infrastructure before such a major disruption occurs. One possible approach is to develop and deploy the so-called *post-quantum* cryptographic algorithms: alternative public-key schemes that are not vulnerable to currently known quantum attacks. They have the advantage of being relatively easy to implement, since they would be compatible with the current cryptographic infrastructure. However, their main drawback is that they have only been shown to be secure against known quantum attacks, while the full potential of quantum algorithms is far from being known today.

Ideally, we would like to employ cryptographic methods that are secure independently of the computational power available to Eve; this is known as *information-theoretic* security. In fact, such an encryption technique has been known for more than one hundred years: the one-time pad [5], see Fig. 1.1. To use this technique, Alice

and Bob need to share a completely random string that is unknown to everyone else, including the eavesdropper. We call such a string a *secure key*. Using her copy of the key, Alice can encrypt a message and send the ciphertext to Bob, who decrypts it using his copy. It can be shown that, if Eve has no information at all about the key, she cannot learn any information about the original message, even if she intercepts the ciphertext. Importantly, the message to be encrypted needs to be of the same length as the key, and each key bit can only be used to encode a single message bit. This is the reason why, despite its incredibly strong security guarantees, the one-time pad has received much less use than public-key cryptosystems: the former only allows Alice and Bob to secretly communicate if they have some pre-shared secure key to spend. If they do not, then Shannon [6] showed that it is impossible to generate a secure key using an untrusted (classical) channel. This is known as the *key distribution problem*. Intuitively, the idea is that any information exchanged by the users through the channel can be intercepted and copied by Eve, and any processing of this information to generate the key can be replicated by Eve.

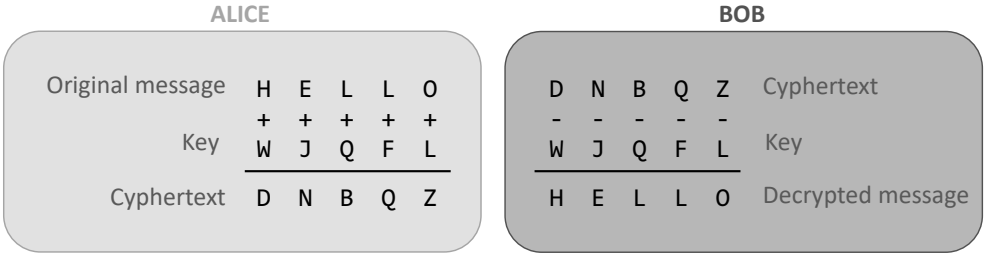


Figure 1.1: Intuitive representation of the one-time pad algorithm[2]. Each letter is encoded as an integer between 0 and 25, according to its position in the English alphabet. The key is a random five letter string, shared by Alice and Bob. Alice encrypts the original message with her copy of the key and publicly announces the ciphertext, after which Bob decrypts the ciphertext using his copy of the key. The encryption and decryption operations are addition and subtraction modulo 26, respectively. For Eve, who has access to the ciphertext but no information about the key, all five-letter strings are equally likely to be the key. Thus, from her point of view, all five-letter strings are also equally likely to be the original message. In other words, the ciphertext alone provides no information at all about the message.

[2]In a practical computer implementation, the message and the key are bit strings, and the encryption and decryption operations are both addition modulo 2.

This impossibility result does not apply if Alice and Bob have access to an untrusted *quantum* channel. The fundamental difference is that it is impossible to copy unknown quantum states [7], which prevents Eve from obtaining exactly the same information as the legitimate users. In fact, any measurement that attempts to distinguish non-orthogonal quantum states necessarily disturbs them. Thus, the error rate of a quantum communication attempt can be used to detect the possible presence of an eavesdropper, or even to bound the amount of information that she may have gained, which opens up an avenue to use quantum mechanics to solve the key distribution problem: *quantum key distribution* (QKD).

The first and best known QKD protocol is BB84, proposed by Bennett and Brassard [8] and based on earlier ideas by Wiesner [9]. It relies on Alice preparing two-dimensional quantum states (*qubits*) that belong to two conjugate bases, commonly referred to as Z and X. In each round, Alice chooses a random basis and a random bit, encodes the bit in that basis, and sends the quantum state to Bob, who measures the incoming states in a random basis. The idea is that Eve cannot know Alice's basis choice, and therefore, any attempt by Eve to learn information about the Z-encoded states will necessarily introduce errors in the X-encoded states, and vice versa. Of course, Bob does not know Alice's encoding basis either, but their advantage over Eve is that, once the quantum communication is complete, they can announce their basis choices and discard all data in which their choices did not match. After that, Alice and Bob compare some of their results and estimate the error rate of the quantum communication, which provides them a bound on the amount of information that Eve could have learned. Using this knowledge, they are able to distil a secure key by applying classical post-processing algorithms to their measurement results.

In the rest of this introduction, we review the basics of QKD. In Section 1.1.1, we give an overview of the structure common to most quantum protocols, finishing with a particular example, the BB84 protocol. In Section 1.1.2, we give a rigorous definition of what it means for a key to be secure, and in Section 1.1.3, we see how one can prove that the output of a QKD protocol is indeed a secure key.

1.1.1 Structure of a QKD protocol

Usually, a QKD protocol is divided in two phases: a quantum phase and a classical phase. In the quantum phase, Alice and Bob encode and/or measure quantum states,

obtaining some *raw* classical data. In the classical phase, Alice and Bob process this classical data, turning it into a secure key.

Quantum phase According to their quantum phase, QKD protocols can be divided in three types, as depicted in Fig. 1.2. In all of these, Alice and Bob assume that anything that is outside of their labs is controlled by Eve; this includes the quantum channel and, if it exists, the middle node Charlie. Usually, in prepare-and-measure and measurement-device-independent protocols, the sending users choose a random bit and a random encoding basis, and then encode the bit in that basis; and in prepare-and-measure and entanglement-based protocols, the measuring users choose a random basis, and measure the incoming states in that basis.

Figure 1.2: Classes of QKD protocols according to their quantum phase. The tail (head) of each arrow indicates the party that emits (measures) the quantum states.

Classical phase Typically, the first step is a *detection announcement*: whoever performed the measurements announces which rounds were successfully detected. Then, Alice and Bob announce some choices that they made in the detected rounds, usually the basis that they used, and according to these choices, they divide their raw classical data in three groups: (1) key data, (2) test data, and (3) discarded data. This step is called *sifting* and the key data is typically referred to as the *sifted key*. After that, Alice and Bob perform *parameter estimation*: they announce their test data, and use its statistics (typically its error rate) to estimate the amount of sifted-key information that may have leaked to Eve. Then, Alice and Bob use classical *error correction* protocols to guarantee that their keys are identical with a very high probability. Finally, Alice and Bob perform *privacy amplification*, turning their error-corrected key pair into a shorter secure key pair, from which Eve's information has been effectively removed.

1.1.1.1 Example of a QKD protocol: BB84

The above discussion is very general, since it attempts to cover most QKD protocols. It is useful to look at a particular example: the BB84 protocol. Here, we consider its efficient version [10], in which the users' basis selection probabilities are biased, in order to maximise the sifting efficiency.

Quantum phase In each round $u \in \{1, ..., N_{\text{tot}}\}$, Alice selects an encoding basis $T \in \{Z, X\}$ with probability p_{T_A}, where typically $p_{Z_A} \gg p_{X_A}$, selects a random bit $b \in \{0, 1\}$, and then emits the quantum state $|b_T\rangle$ through the quantum channel. The emitted states are such that $|0_Z\rangle$ and $|1_Z\rangle$ are orthogonal, and $|b_X\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle + (-1)^b |1_Z\rangle)$, i.e. Z and X are two mutually unbiased bases in a qubit space. For example, Alice may emit polarisation-encoded single photons, in which case $|0_Z\rangle$ and $|1_Z\rangle$ correspond to horizontally and vertically polarised single photons, while $|0_X\rangle$ and $|1_X\rangle$ are 45° and 135° polarised single photons, respectively.

On his side, Bob selects a random measurement basis $T \in \{Z, X\}$ with probability p_{T_B}, and attempts to measure the incoming photons in that basis, obtaining either a bit value or an unsuccessful result. As we will see in Section 1.1.3, modern security frameworks of QKD only need a perfect characterisation for the devices of one of the users, allowing for some imperfections in the other's. Typically, Bob is chosen for the latter, since measurement devices are more difficult to characterise than sources. Thus, Bob does not necessarily need to perform perfect Z and X basis measurements on qubit states, but his choice of basis needs to be completely random, and the overall detection efficiency (i.e. the probability of obtaining a bit value) needs to be the same for both measurement bases, regardless of the state that arrives to his lab.

Classical phase

Sifting and parameter estimation After Bob has finished all measurements, he announces which rounds have been successfully detected, and then both users announce their basis choices in those rounds. Then, Alice and Bob define their sifted keys as the bit values associated to the detected rounds in which they both used the Z basis, and define the test rounds as the set of detected rounds in which they both used the X basis. After that, they announce the bit values associated to the test rounds, learning

their error rate e_X. Alice and Bob then use this information to estimate the phase-error rate e_{ph} of their sifted keys, which quantifies the amount of information that could have been leaked to Eve. In the limit of $N_{\text{tot}} \to \infty$, $e_{\text{ph}} = e_X$; for practical finite values of N_{tot}, Alice and Bob need to apply a random sampling analysis to obtain an upper-bound e_{ph}^{U} on e_{ph} using the observed value of e_X. We elaborate on this step in Section 1.1.3.

Error correction and error verification Next, Alice and Bob use classical error correction codes to correct errors in their sifted keys. Typically, Alice sends some information about her key, the syndrome, to Bob, who uses it to correct all errors in his key with very high probability. The cost of error correction is commonly expressed as $\lambda_{\text{EC}} = fNh(e_Z)$, where N is the sifted key length, e_Z is its bit-error rate, $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon binary entropy function, and $f > 1$ is the error correction inefficiency, since the actual cost is typically larger than the theoretical Shannon limit of $Nh(e_Z)$. After error correction, Alice and Bob typically perform error verification: they compute a tag of their respective keys, using a hash function, and Alice sends her tag to Bob, who checks if the two tags are identical. If so, their keys are also identical with a very high probability; if not, they abort the protocol. Note that both the syndrome and the tag contain information about Alice's key. To prevent Eve from learning this information, Alice typically encrypts them using some pre-shared secure key; the bits spent on this step need to be taken into account when computing the *net* secret-key length of the protocol. Some security proofs allow Alice to publicly announce her syndrome and tag, and then remove the extra information that Eve has gained in the privacy amplification step. Both methods result in the same net secret key length, but only the latter can be used if Alice and Bob do not share any secret key to begin with. For simplicity, throughout this introduction we assume that Alice encrypts the syndrome and tag.

Privacy amplification Finally, Alice and Bob transform their N-bit error-corrected key into a secure key of length approximately $K \approx N - h(e_{\text{ph}}^{\text{U}})$ bits. For this, Alice selects a random N-to-K two-universal hash function and announces it, and then both Alice and Bob apply this hash function to their respective corrected keys, obtaining

their secure key pair. In Section 1.1.2, we explain exactly what we mean by secure key, and in Section 1.1.3, we review how one can ensure that the key is indeed secure.

Note on authentication Some communications in the classical phase need to be authenticated; otherwise, Eve could easily perform a man-in-the-middle attack, disguising as Alice to Bob, and as Bob to Alice. If one wants the whole QKD protocol to be information-theoretically secure, the authentication method also needs to be. Fortunately, symmetric-key authentication algorithms are information-theoretically secure, and require only $O(\log m)$ secure key bits, where m is the length of the message [11]. However, this implies that Alice and Bob would need to share a short secure key to be able to perform QKD and obtain a longer secure key. For this reason, it would be perhaps more accurate to call the full scheme quantum key *expansion*, rather than *distribution* [12].

If Alice and Bob do not share any previous secure key, they can rely on computationally-secure public-key authentication schemes for their first round of QKD, and then use a small portion of the resulting secret key to authenticate future rounds. At first glance, this may seem strange; after all, Alice and Bob could have relied on public-key encryption, rather than QKD, for their secret communications. There is an important difference, however: if Eve is not able to break the authentication scheme during the first QKD round, all the generated keys (and any messages encrypted with them) will remain secure forever [13]. Conversely, messages encrypted using public-key schemes will always be vulnerable to future technological advances, potentially allowing Eve to retroactively break their encryption.

1.1.2 Definition of security

Ideally, the output of a QKD protocol would be a fully secure key pair: two identical keys $k_A = k_B = k$ that are completely random, and which Eve knows nothing about. Formally, an ideal key pair of length K is represented by the *classical-classical-quantum* state

$$\sigma_{ABE}^{\text{ideal},K} = 2^{-K} \sum_{k\in\{0,1\}^K} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \sigma_E, \tag{1.1}$$

where k runs over all possible binary strings of length K, and σ_E is the final state of the eavesdropper, which is completely decoupled from the subsystems A and B, i.e. Eve

has no information on k. Unfortunately, in a realistic QKD protocol, it is impossible to guarantee that Alice and Bob's key pair is ideally secure; there is always a possibility that Alice and Bob end up with different keys $k_A \neq k_B$, or that Eve gains some side information on the key. In general, we can write the output of the real protocol as

$$\sigma_{ABE}^{K} = \sum_{k_A,k_B \in \{0,1\}^K} \Pr(k_A, k_B|K)\, |k_A\rangle\langle k_A|_A \otimes |k_B\rangle\langle k_B|_B \otimes \sigma_E^{k_A,k_B}. \tag{1.2}$$

where $\Pr(k_A, k_B|K)$ is the probability that Alice and Bob obtain final keys $k_A, k_B \in \{0,1\}^K$, respectively, conditioned on them actually obtaining a key pair of length K, i.e. not aborting the protocol; and $\rho_E^{k_A,k_B}$ is the final state of Eve conditioned on Alice and Bob obtaining k_A, k_B[3]. To evaluate the security of a QKD protocol, we need to define a security parameter ϵ_{sec} using some sort of distance measure between the real key σ_{ABE}^{K} and an ideal secure key $\sigma_{ABE}^{\text{ideal},K}$. Moreover, since we want to use the key in combination with other protocols (such as the one-time pad), it is important that this definition of security is *composable* [14]. That is, if we have a set of cryptographic protocols, each of which have a security parameter ϵ_{sec}^i, we would like to claim that the whole system has a security parameter $\sum_i \epsilon_{\text{sec}}^i$. In QKD, a composable security definition is given by the trace distance [15, 16]

$$\frac{1}{2}(1 - p_{\text{abort}}) \left\| \sigma_{ABE}^{K} - \sigma_{ABE}^{\text{ideal},K} \right\| \leq \epsilon_{\text{sec}}. \tag{1.3}$$

If the key generated in a QKD protocol satisfies Eq. (1.3), the protocol is said to be ϵ_{sec}-secure. The trace distance is related to the distinguishing problem: if Eq. (1.3) holds, then it is impossible for anyone, including Eve, to distinguish the real key pair from an ideal key pair with probability more than ϵ_{sec}. This implies that, if Alice uses her half of the real key pair to encrypt a message, Eve cannot distinguish the ciphertext from a fully random string with probability more than ϵ_{sec}; if she could, then she could

[3] Note that this definition assumes that Eve has already fixed her attack, but Alice and Bob have not yet run the protocol; $\Pr(k_A, k_B|K)$ is the probability that Alice and Bob will obtain final keys k_A, k_B once they run the protocol, conditioned on it not aborting. It is not possible to define the security of the final key conditioned on the actual outcomes obtained in the protocol. For example, there is always the possibility that Alice and Bob have been extremely unlucky, and Eve has managed to (randomly) guess all of their basis choices correctly, allowing her to learn the key while introducing no disturbance. Such an outcome is extremely unlikely, however, and is covered by the *a priori* security definition in Eqs. (1.2) and (1.3).

also tell that Alice has encrypted the message using the real key rather than an ideal key, contradicting Eq. (1.3).

The definition of security can be divided into correctness and secrecy:

Correctness This criterion is met when Alice and Bob's final keys are identical. A protocol is ϵ_{c}-correct if $\Pr[k_A \neq k_B] \leq \epsilon_{\mathrm{c}}$.

Secrecy This criterion is met when Eve has no information about Alice's key. A protocol is ϵ_{s}-secret if

$$\frac{1}{2}(1-p_{\mathrm{abort}})\left\|\sigma_{AE}^{K}-\sigma_{AE}^{\mathrm{ideal},K}\right\| \leq \epsilon_{\mathrm{s}}, \tag{1.4}$$

where

$$\begin{aligned}\sigma_{AE}^{K} &:= \mathrm{Tr}_B(\sigma_{ABE}^{K}) = \sum_{k_A\in\{0,1\}^K} \Pr(k_A)\,|k_A\rangle\langle k_A|_A \otimes \sigma_E^{k_A},\\ \sigma_{AE}^{\mathrm{ideal,K}} &:= \mathrm{Tr}_B(\sigma_{ABE}^{\mathrm{ideal},K}) = 2^{-N}\sum_{k\in\{0,1\}^K} |k\rangle\langle k|_A \otimes \sigma_E.\end{aligned} \tag{1.5}$$

If a protocol is ϵ_{c}-correct and ϵ_{s}-secret, then it is ϵ_{sec}-secure, with $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{c}} + \epsilon_{\mathrm{s}}$. This decomposition is useful because the correctness criterion can be trivially ensured by the use of error verification based on hashing; if the length of the error verification tag is $\lceil \log_2(1/\epsilon_{\mathrm{c}}) \rceil$, then the final key is ϵ_{c}-correct [11, 17]. Thus, the objective of the security proofs of QKD is reduced to showing that Alice's key is ϵ_{s}-secret.

The definition of ϵ_{sec} and ϵ_{s} in Eqs. (1.3) and (1.4) assumes that the length of the final keys k_A, k_B is fixed and equal to K for all possible runs of the protocol, provided that it does not abort. For protocols or security proofs in which this is not the case, one may use the alternative definitions [18]

$$\frac{1}{2}\sum_{K}\Pr(K)\left\|\sigma_{ABE}^{K}-\sigma_{ABE}^{\mathrm{ideal},K}\right\| \leq \epsilon_{\mathrm{sec}}, \tag{1.6}$$

$$\frac{1}{2}\sum_{K}\Pr(K)\left\|\sigma_{AE}^{K}-\sigma_{AE}^{\mathrm{ideal},K}\right\| \leq \epsilon_{\mathrm{s}}, \tag{1.7}$$

where $\Pr(K)$ is the probability that the length of the final key is K. In the definition above, $K = 0$ accounts for the events in which the protocol aborts, in which case the zero-length output "key" is considered to be trivially secure.

1.1.2.1 Attack levels

It is often difficult to prove the security of a QKD protocol against any eavesdropping attack. For this reason, security proofs have traditionally divided Eve's possible attacks into three classes of increased sophistication. In all of them, Eve is assumed to prepare N_{tot} quantum ancillas, one corresponding to each pulse emitted by Alice, and they differ in what Eve is allowed to do afterwards.

Individual attack Eve performs an independent and identical quantum operation between each of Alice's pulses and her corresponding ancilla. After the classical phase of the protocol, she measures each ancilla separately.

Collective attack Similar to the previous, but after the classical phase of the protocol, she performs an arbitrary joint measurement on all of her ancillas.

Coherent attack Eve performs an arbitrary joint quantum operation between *all* the pulses emitted by Alice and *all* of her ancillas. After the classical phase of the protocol, she performs an arbitrary joint measurement on all of her ancillas.

The latter class is also sometimes referred to as *general*, since any attack allowed by the laws of quantum mechanics can be expressed as a coherent attack.

A QKD protocol is only information-theoretically secure when it is proven to be secure against coherent attacks. However, it is a known result that, in the asymptotic regime in which $N_{\text{tot}} \to \infty$, proving security against collective attacks is equivalent to proving security against general attacks, as long as the classical post-processing satisfies some reasonable assumptions [19, 20]. Thus, asymptotic security proofs often consider collective attacks, and regard Eve's action as independent and identically distributed (IID) between different rounds of the protocol, which often simplifies the proof. Conversely, security proofs in the finite-key regime often prove security directly against general attacks[4].

[4] In the finite-key regime, one can also first prove security against collective attacks, and then apply the aforementioned results to extend the security against coherent attacks. However, doing so results in a degradation of the security parameter ϵ_{sec}, and proving security directly against coherent attacks is, in most cases, much tighter.

1.1.3 Security of QKD

The first proofs of the information-theoretic security of the BB84 protocol against coherent attacks appeared around fifteen years after its introduction [21, 22]. Since then, the ideas in these early proofs have been refined, and nowadays, mainly two frameworks are used to prove the information-theoretic security of a QKD protocol:

- *Phase-error correction* approach: Based on showing the equivalence between the actual protocol and a fictitious scenario in which Alice and Bob perform phase-error correction based on quantum error correction codes. This method is essentially a refinement of the early security proofs mentioned above. See Ref. [23] and Ref. [18].

- *Leftover hashing lemma* approach: It is based on finding a lower bound of the smooth min-entropy of the sifted key, after which the security of the final key is guaranteed by applying the leftover hashing lemma. It was introduced by Renner [24], see also Ref. [25].

Even though these two approaches are based on different mathematical tools, their conclusions are very similar. In fact, Tsurumaru [26] has recently shown that both approaches are essentially equivalent. In what follows, we treat them as a single security framework, and summarise its conclusions.

1.1.3.1 Security framework

Let us assume that Alice and Bob share some unknown quantum state ρ_{ABE}, where A (B) represents Alice's (Bob's) system, and E represents anything else in the universe that may be entangled with these systems, which we assume to be held by the eavesdropper, Eve. Let us further assume that, to generate her raw key $\mathbf{Z}$ of length N, Alice performs a positive operator-valued measurement (POVM) $\mathbb{Z}$ on A. For simplicity, we assume here that the system A is composed of N qubit subsystems, and Alice's measurement can be decomposed as $\mathbb{Z} = \mathbb{Z}^{(1)} \otimes \mathbb{Z}^{(2)} \otimes \ldots \otimes \mathbb{Z}^{(N)}$, where $\mathbb{Z}^{(k)}$ is a Z-basis measurement on the k-th qubit. Essentially, the objective of the security proof is to estimate how much information Eve could have on $\mathbf{Z}$. After doing so, this information can be removed from the key in the privacy amplification step. To generate his sifted key $\mathbf{Z}'$, Bob also performs a measurement on B; however, since Bob will later correct

his key to match Alice's, the details of his measurement are not important for the task of proving the secrecy of Alice's key $\mathbf{Z}$.

To estimate Eve's information on $\mathbf{Z}$, we consider an alternative fictitious scenario in which, instead of $\mathbb{Z}$, Alice performs an alternative measurement $\mathbb{X}$ on system A, obtaining a string $\mathbf{X}$. Alice's alternative measurement $\mathbb{X}$ must be mutually unbiased[5] with $\mathbb{Z}$; for simplicity, we will assume that it can be decomposed as $\mathbb{X} = \mathbb{X}^{(1)} \otimes \mathbb{X}^{(2)} \otimes \ldots \otimes \mathbb{X}^{(N)}$, where $\mathbb{X}^{(k)}$ is an X-basis measurement on the k-th qubit. In this alternative fictitious scenario, usually called the *virtual protocol*, Bob will attempt to predict Alice's string $\mathbf{X}$ by performing some measurement on his system B; we denote by $\mathbf{X}'$ the result of this measurement. The fundamental question to ask is: if Alice and Bob had run the virtual protocol, what would be the error rate between $\mathbf{X}$ and $\mathbf{X}'$? This quantity is known as the phase-error rate, e_{ph}. Let us suppose that we could guarantee that, if Alice and Bob had run the virtual protocol, they would have obtained an error rate of $e_{\mathrm{ph}} = 0$. Then, it would be impossible for Eve to have any information at all on Alice's actual key $\mathbf{Z}$. Moreover, in general, if Alice and Bob could guarantee that there is some upper-bound $e_{\mathrm{ph}}^{\mathrm{U}} \leq 1/2$ such that $e_{\mathrm{ph}} \leq e_{\mathrm{ph}}^{\mathrm{U}}$ with certainty, then Eve's information on $\mathbf{Z}$ is guaranteed to be at most $Nh(e_{\mathrm{ph}}^{\mathrm{U}})$ bits.

In practice, due to the probabilistic nature of quantum mechanics, Alice and Bob can never be certain that, if they had run the virtual protocol, they would have obtained an error rate $e_{\mathrm{ph}} \leq e_{\mathrm{ph}}^{\mathrm{U}}$ for any $e_{\mathrm{ph}}^{\mathrm{U}} < 1/2$. At most, they will be able to make a statistical claim on e_{ph}, i.e. find an $e_{\mathrm{ph}}^{\mathrm{U}} < 1/2$ such that $\Pr\left[e_{\mathrm{ph}} > e_{\mathrm{ph}}^{\mathrm{U}}\right] \leq \varepsilon$ for some small failure probability ε. If they are able to do so, then, provided that they sacrifice $Nh(e_{\mathrm{ph}}^{\mathrm{U}}) + \log_2 \epsilon_{\mathrm{PA}}^{-1}$ bits in the privacy amplification step, Alice's final key is guaranteed to be ϵ_{s}-secret, as defined in Eq. (1.7), with [18]

$$\epsilon_{\mathrm{s}} = \sqrt{2}\sqrt{\varepsilon + \epsilon_{\mathrm{PA}}}. \tag{1.8}$$

It is useful to see ε as the probability that Alice and Bob's estimation of the phase-error rate is wrong, and ϵ_{PA} as the probability that the privacy amplification step won't produce a fully secret key, even if the estimation of the phase-error rate is correct. Taking into account the secret-key bits spent in the error correction and verification

[5] The *leftover hashing lemma* framework can prove security even if Alice's measurement bases are not mutually unbiased, but the performance degrades significantly.

steps, the net secret key length of the protocol is

$$K_{\text{net}} = N\big[1 - h(e_{\text{ph}}^{\text{U}})\big] - \lambda_{\text{EC}} - \log_2 \epsilon_{\text{c}}^{-1} - \log_2 \epsilon_{\text{PA}}^{-1}, \tag{1.9}$$

and the key is guaranteed to be ϵ_{sec}-secure, where $\epsilon_{\text{sec}} = \epsilon_{\text{s}} + \epsilon_{\text{c}}$.

Asymptotic regime The previous equations imply that there is a trade-off between the ϵ_{s} and ϵ_{c} parameters and the secret-key length: the more bits one is willing to sacrifice in the privacy amplification and error verification steps, the more secure the final key is. This trade-off is especially important for low values of N, but as N grows, its effect becomes progressively less pronounced. In fact, in the limit of $N \to \infty$, one can choose any desired value of ϵ_{s} and ϵ_{c} with no penalty. To see why, note that, if we divide the net secret-key length in Eq. (1.9) by the total amount of rounds N_{tot}, we obtain the net secret-key rate

$$R_{\text{net}} = Q_{\text{s}}\big[1 - h(e_{\text{ph}}^{\text{U}})\big] - \frac{\lambda_{\text{EC}}}{N_{\text{tot}}} - \frac{\log_2 \epsilon_{\text{c}}^{-1}}{N_{\text{tot}}} - \frac{\log_2 \epsilon_{\text{PA}}^{-1}}{N_{\text{tot}}}, \tag{1.10}$$

where $Q_{\text{s}} = N/N_{\text{tot}}$ is the per-round probability to obtain a sifted-key bit. In the limit of $N_{\text{tot}} \to \infty$[6], for any (non-zero) value of ϵ_{c} and ϵ_{PA}, the last two terms in Eq. (1.10) vanish; thus, we can take $\epsilon_{\text{c}} \to 0$ and $\epsilon_{\text{PA}} \to 0$ with no effect in the key rate. Moreover, if $N_{\text{tot}} \to \infty$, all statistical fluctuations in the estimation of the phase-error rate vanish, and we can take $\varepsilon \to 0$ with no penalty in the estimation. Since ϵ_{s} is a function of ε and ϵ_{PA}, see Eq. (1.8), we can take $\epsilon_{\text{s}} \to 0$ and $\epsilon_{\text{c}} \to 0$ with no key-rate penalty.

Many security proofs of QKD assume the asymptotic regime in which $N_{\text{tot}} \to \infty$; in these, the ϵ_{s} and ϵ_{c} parameters do not play an important role. Conversely, they are relevant in the so-called finite-key security proofs, which take into account the statistical fluctuations that arise in a real implementation of the protocol. In Section 1.2.1.4, we elaborate on this distinction.

1.1.3.2 Example: BB84 protocol

At first glance, the security framework above seems to be applicable only to entanglement-based protocols, in which Alice and Bob make measurements on the incoming states, which they regard as having been prepared by Eve. However, for

[6] Note that, since the length of the sifted key N is an increasing function of the total number of rounds N_{tot}, the conditions $N \to \infty$ and $N_{\text{tot}} \to \infty$ are equivalent.

prepare-and-measure protocols, one can always find an equivalent entanglement-based scenario in which, instead of preparing quantum states, Alice entangles the photonic mode with a fictitious ancilla system, and then performs a measurement on the ancilla. For example, in the BB84 protocol, when Alice chooses the Z basis, she randomly selects and emits one of $|0_Z\rangle_B$ or $|1_Z\rangle_B$, where B is the photonic system sent to Bob. Instead, she could have generated the entangled state

$$|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle_A |0_Z\rangle_B + |1_Z\rangle_A |1_Z\rangle_B), \tag{1.11}$$

and performed a Z-basis measurement on the qubit ancilla A. Similarly, when she chooses the X basis, she randomly selects and emits one of $|0_X\rangle_B$ or $|1_X\rangle_B$; instead, she could have generated the state

$$|\Psi_X\rangle = \frac{1}{\sqrt{2}}(|0_X\rangle_A |0_X\rangle_B + |1_X\rangle_A |1_X\rangle_B), \tag{1.12}$$

and performed an X-basis measurement on A. Note that $|\Psi_Z\rangle = |\Psi_X\rangle =: |\Psi\rangle$, implying that Alice could generate the state $|\Psi\rangle$ in all rounds, and then randomly decide a basis to measure system A. Moreover, since only Alice has access to system A, it does not actually matter *when* she performs her measurement: we can imagine that Alice waits until Bob has received all signals to randomly choose a basis and carry out the measurement.

The security framework in Section 1.1.3.1 assumes that Alice's (Bob's) sifted key is the result of a Z-basis measurement on the system A (B) of some state ρ_{ABE}. Since in the BB84 protocol Alice and Bob define their sifted keys as the outcomes of the detected Z-basis rounds, we need to define the state ρ_{ABE} for the systems A and B corresponding to these rounds only. For this, in the fictitious entanglement-based scenario, Bob must first learn whether or not each signal will produce a click in his detectors, and only afterwards perform his actual measurement on these detected signals. More specifically, we assume that Bob first performs a quantum-non-demolition (QND) measurement on all incoming pulses and stores the surviving signals in a quantum memory. Then, for each of the stored signals, Alice and Bob each choose a random measurement basis; the state ρ_{ABE} is defined as the systems A and B corresponding to the detected rounds in which they both selected the Z basis, and E represents Eve's side information on these states. Afterwards, Alice and Bob measure their respective systems A and B in their chosen basis.

To prove the security, we consider the error rate that Alice and Bob would have obtained if they had run the virtual protocol, i.e. if they had measured systems A and B of ρ_{ABE} in the X basis, rather than in the Z basis. Note that, in the virtual protocol, Alice generates $|\Psi\rangle$ in all rounds, Bob performs a QND measurement, learning which rounds are detected, and then, for each detected round:

1. With probability $p_{Z_A}p_{Z_B}$, the round is considered a key round; Alice and Bob measure their systems A and B in the X basis, obtaining strings $\mathbf{X}$ and $\mathbf{X}'$, which have an error rate e_{ph}.

2. With probability $p_{X_A}p_{X_B}$, the round is considered a test round; Alice and Bob measure their systems A and B in the X basis and announce their bit outcomes, learning their error rate e_X.

3. With probability $p_{Z_A}p_{X_B} + p_{X_A}p_{Z_B}$, the round is discarded.

That is, in the virtual protocol, Alice and Bob perform exactly the same measurement in the key rounds and in the test rounds. Thus, in the limit of $N \to \infty$, the error rates of both sets of rounds must be identical, i.e. $e_{\text{ph}} = e_X$. For finite values of N, the two error rates may not be exactly identical, due to statistical fluctuations. However, the task of finding an upper bound e_{ph}^{U} on e_{ph} from the observed value of e_X is a simple random sampling problem, which can be tightly solved using existing statistical results [11, 18, 25].

Role of Alice and Bob in the proof The security framework in Section 1.1.3.1 introduces a fundamental distinction between Alice's and Bob's roles in the protocol. Namely, its objective is to estimate the information that Eve has on Alice's Z-basis key $\mathbf{Z}$, and it achieves this by considering how well Bob could predict Alice's key $\mathbf{X}$ if she had used the X basis instead. This asymmetry results in different assumptions about the users: the security framework assumes that Alice's measurements are performed on qubits, and that her (X-basis) measurement of ρ_{ABE} in the virtual protocol is mutually unbiased with her (Z-basis) measurement in the actual protocol, while it makes no such assumptions on Bob's measurement. This has important consequences when using the framework to prove the security of a prepare-and-measure protocol such as BB84, in which Alice's "measurement" is performed on a *fictitious* ancilla qubit. The requirement

that she uses two mutually unbiased bases to perform her *fictitious* measurement means that, in the actual protocol, Alice must encode her signals in two mutually unbiased bases[7]. On the other hand, Bob does not need to use two mutually unbiased qubit bases to perform his actual measurement; his devices can be imperfect, to some extent. However, the proof in Section 1.1.3.2 does require two important assumptions on Bob's measurement setup:

1. Bob's choice of basis is fully random; Eve cannot tamper with the probability that in a given round Bob will choose one basis or another.

2. Bob's overall detection efficiency (the probability that a given pulse is detected) is independent of his choice of basis; this must hold for any signal that Eve may send to Bob.

Note that we could also have applied the security framework to prove the secrecy of Bob's key, rather than Alice's. If we did so, the assumptions on the two users would flip: Bob must now perform a perfect qubit measurement in two mutually unbiased bases, while Alice does not need to employ two mutually unbiased bases in her *fictitious* measurement. In the actual protocol, this would allow for some flaws in her state preparation. Namely, Alice's source could be uncharacterised, as long as it is basis independent [23, 27], i.e. $\rho_Z = \rho_X$, where ρ_Z (ρ_X) is the average state emitted when Alice chooses the Z (X) basis. Nevertheless, as we will see in Section 1.2.1.3, Bob's measurement device is considered to be more difficult to secure and characterise than Alice's source; thus, in security proofs, one usually chooses to prove the secrecy of Alice's key. In fact, the above two requirements on Bob's measurement setup are already very difficult to meet in practical implementations of QKD.

1.2 Challenges and contribution

Here, we introduce two of the main hurdles that QKD needs to clear before it can be widely deployed as an alternative to the current public-key cryptographic infrastructure: (1) how to ensure that practical implementations are information-theoretically secure, despite their inevitable imperfections; and (2) how to obtain higher secret-key rates over

[7] The condition on the encoding bases is actually slightly *weaker* than being mutually unbiased; see discussion around Eq. (1.25) in Section 1.2.2.2.

longer distances. In doing so, we review recent theoretic and experimental advances to tackle these problems, including the contributions made in the works presented in this thesis.

1.2.1 Challenge I: Practical security

Security proofs of QKD are essentially mathematical theorems that start from the postulates of quantum mechanics and assumptions about the devices used by Alice and Bob, and their conclusion is the information-theoretic security of the protocol, as defined in Section 1.1.2. However, security proofs only apply to real-life scenarios if the latter perfectly meet all the assumptions made in the former. Some common assumptions made in QKD security proofs include:

- Alice and Bob's labs are perfectly shielded from the outside; Eve can only interact with the signals that travel through the quantum channel;
- Alice's source emits perfectly-encoded single photons;
- Bob's choice of basis is fully random, and the overall detection efficiency is the same for both bases; and
- Alice and Bob run the protocol for an infinite number of rounds, allowing them to perform a perfect statistical characterisation of their quantum channel.

These assumptions are often not met in real-life implementations of QKD. In the following, we review the main imperfections, and the theoretical developments that have been proposed to deal with them.

1.2.1.1 Single-photon sources, weak-coherent pulses, and the decoy-state method

While many different systems have been proposed to implement quantum computers, such as ions, atoms, light, or spins, the inevitable part of any QKD protocol is light, since Alice and Bob are separated by a macroscopic distance [28]. The BB84 protocol assumes that Alice emits qubit states, so it must be implemented using qubit states of light, for example, the polarisation state of a single photon, or the relative phase between the single-photon states of two spatial or temporal modes of light. However, it

is experimentally challenging to produce a high-quality and high-performance heralded single-photon source. Thus, in practice, attenuated laser sources are used in most QKD experiments. The output of these sources can be regarded as a coherent state $|\alpha\rangle$, where α is a complex number and $\mu = |\alpha|^2$ is the intensity of the pulse. This coherent state is a superposition of photon-number states,

$$|\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,, \tag{1.13}$$

and the phase of the complex number α determines the relative phases between different photon-number components. If one is able to randomise the phase of α, then the output state becomes

$$\rho_\mu = \frac{1}{2\pi} \int_0^{2\pi} \left|\sqrt{\mu}e^{i\theta}\right\rangle\!\left\langle\sqrt{\mu}e^{i\theta}\right| \mathrm{d}\theta = \sum_{n=0}^{\infty} P_{n|\mu} \, |n\rangle\langle n| \,, \tag{1.14}$$

where $P_{n|\mu} = e^{-\mu}\mu^n/n!$ follows a Poisson distribution of mean μ. That is, a *phase-randomised* coherent state (PRCS) is a classical mixture, rather than a superposition, of photon-number states.

Most QKD experiments rely on PRCS sources, rather than single-photon sources, although these introduce security loopholes that need to be dealt with. For example, in the BB84 protocol with a PRCS source, a powerful Eve could perfectly learn Alice's key bit in all multi-photon ($n \geq 2$) emissions, using the *photon-number-splitting attack* [29, 30]: (1) Eve performs a non-demolition measurement, learning the photon number of each signal; (2) she splits multi-photon signals, storing one photon in a quantum memory; and (3) she waits until the basis announcement step to measure it in the correct basis, thus learning the encoded bit without introducing any errors. In principle, Eve could also block single-photon signals, and ensure that all multi-photon signals produce a click in Bob's detectors, thus learning a significant fraction of the key.

Fortunately, Ref. [31] showed that, to prove the security of the protocol, it is sufficient to obtain a lower bound on the fraction of bits in the sifted key that originated from single-photon emissions, as well as an upper bound on the phase-error rate of these bits. That is, it is not necessary to know which specific bits originated from single photon emissions; by estimating these parameters, one can bound Eve's total sifted-key information, and then remove this information in the privacy amplification step. The authors of Ref. [31] themselves proposed a method to obtain these bounds:

take the pessimistic assumption that all errors are caused by single-photon emissions, and that all multi-photon signals emitted by Alice have been detected by Bob. Unfortunately, this assumption results in a poor performance in the presence of high loss: if the rate of multi-photon emissions exceeds the rate of detections, *all* detections could be caused by multi-photon signals, and no secret-key rate can be extracted at all. Thus, in the presence of high losses, Alice must use a very weak laser intensity to ensure that the rate of multi-photon emissions is very low. However, this also reduces the rate of single-photon emissions, resulting in a key-rate drop. It can be shown that, for a channel with transmissivity η, the optimal laser intensity is $\mu_{\text{opt}} \approx \eta$, and the resulting protocol has $O(\eta^2)$ scaling [30], rather than $O(\eta)$ as in the single-photon case.

Shortly after, a much more precise way to estimate the relevant parameters was proposed: the decoy-state method [32–34]. Its key idea is to employ different laser intensities to statistically characterise the effect of the channel on different photon number states. Let Q_μ^T be the detection rate (gain) of the PRCS ρ_μ when Alice and Bob both choose basis $T \in \{Z, X\}$ and let Y_n^T be the detection probability (yield) of the photon-number state $|n\rangle$ when Alice and Bob both choose basis T. In the asymptotic regime, observed gains and yield probabilities converge to the same value, and from Eq. (1.14), it must be that

$$Q_\mu^T = \sum_{n=0}^{\infty} P_{n|\mu} Y_n^T, \tag{1.15}$$

for any intensity μ. Similarly, if we denote by E_μ^X the error rate observed when Alice chooses intensity μ and both users choose the X basis, and by e_n^X the error probability when Alice emits $|n\rangle$ and both users choose the X basis, it must be that

$$Q_\mu^X E_\mu^X = \sum_{n=0}^{\infty} P_{n|\mu} e_n^X Y_n^X. \tag{1.16}$$

Therefore, by using different intensities μ, and observing their gains and error rates, one obtains restrictions on the possible values of Y_n^Z and e_n^X. In fact, if one were to use infinitely-many values of μ, one could precisely estimate Y_n^Z and e_n^X for all n. However, to obtain a good lower bound on Y_1^Z and a good upper bound on e_1^X, it is enough to use three different intensities [34, 35]. The net key rate obtainable is

$$R_{\text{net}} \geq Q_1[1 - h(e_1^X)] - f Q_\mu h(E_\mu), \tag{1.17}$$

where $Q_1 = Y_1 \mu e^{-\mu}$ is the gain due to single-photon signals. Decoy-state BB84 has $O(\eta)$ scaling, and offers a performance comparable to the single-photon version of the protocol.

Continuous vs discrete phase randomisation The results above assume that Alice can generate pulses with a uniformly random phase in the continuous range $[0, 2\pi)$, see Eq. (1.14). However, this is difficult to achieve experimentally. A naive attempt to produce continuous-phase-randomised pulses would be turning the laser on and off for each emission. However, experiments have shown that this approach results in residue correlations between consecutive pulses [36], especially in high-speed systems [37, 38], which breaks the *uniform* randomness assumption. Moreover, continuous phase randomisation has a fundamental problem: it is extremely challenging to verify that a continuous phase is indeed fully random.

An alternative approach is to randomise the phase actively, using a random number generator to choose a phase, and a phase modulator to modulate it into the pulse. However, using this method, the set of possible random phases is necessarily *discrete*, and while discrete randomness is much easier to certify, it breaks the *continuous* assumption of the decoy-state method. Thus, the standard decoy-state security proofs cannot be applied to a discretely-randomised QKD implementation. This problem was considered by Cao *et al.* [39], who proved the security of a discrete-phase-randomised decoy-state BB84 protocol using computational methods. Their numerical results showed that, while discretely-randomised decoy-state BB84 offers strictly worse secret-key rates than the equivalent continuously-randomised protocol, the performance of the former is close to the latter with as few as ten random phases. Recently, in Ref. [40], we have used similar ideas to prove the security of a discrete-phase-randomised twin-field QKD protocol. We expand on this work in Section 1.2.2.2.

1.2.1.2 Countermeasures against source flaws

Security proofs often assume that Alice's source can produce perfectly encoded single-photon states, or if they consider decoy-state sources, that Alice's single-photon components are perfectly encoded. For example, in the ideal BB84 protocol, it is assumed that Alice prepares the perfect qubit states $|0_Z\rangle$, $|1_Z\rangle$, $|0_X\rangle$ and $|1_X\rangle$, which belong to two mutually unbiased encoding bases. As we have seen in Section 1.1.3.2, when we

have such a source, we can estimate the phase-error rate in one basis directly using the observed bit-error rate in the other basis. More precisely, in the asymptotic regime, the phase-error rate in one basis is *exactly* equal to the bit-error rate in the other basis, while in the finite-key regime, the two quantities can be easily related using a trivial random sampling analysis. As we have seen in Section 1.1.3.2, if one can guarantee that Bob's measurement is ideal, the condition to apply this trivial phase-error rate estimation is relaxed to ensuring that Alice's source is basis independent, i.e. $\rho_Z = \rho_X$. However, due to flaws in the encoded states, even the basis independence condition may not be met in practical implementations, allowing Eve to gain information on which basis Alice has chosen in a specific round. In fact, by performing an unambiguous state discrimination (USD) attack, Eve can in principle unambiguously determine Alice's basis choice, although she will sometimes obtain an indeterminate result, which she can try to mask as channel loss. However, if the source is such that $\rho_Z \approx \rho_X$, this USD attack would result in very high losses that may not be compatible with the actual measurement results obtained in the protocol, suggesting that security may still be possible. In fact, Lo and Preskill [41] proposed an analysis that can prove security even if the source is basis dependent. The performance of their protocol depends on a parameter that quantifies the basis dependency: if the source is close to basis independent, the performance is good, but the secret-key rate deteriorates very quickly as the basis dependency increases. Their framework was later extended to prove security in the presence of information leakage from the phase modulator [42] and the decoy-state intensity modulator [43, 44].

State preparation flaws and the loss-tolerant protocol Because the analysis of Lo and Preskill [41] is general, it results in very pessimistic key rates for a certain type of source imperfection, the so-called *state preparation flaws* (SPFs). These arise from the finite precision of modulation devices, and are very common in experimental implementations. For example, Alice's source may produce states of the form

$$|\psi_i\rangle = \cos(\theta_i/2)\,|0_Z\rangle + \sin(\theta_i/2)\,|1_Z\rangle\,, \tag{1.18}$$

where $|0_Z\rangle$ and $|1_Z\rangle$ form an orthonormal qubit basis, and $i \in \{0_Z, 1_Z, 0_X, 1_X\}$ represents Alice's choice of state. With ideal encoding, Alice's states would be such that

$\theta_{0_Z} = 0$, $\theta_{1_Z} = \pi$, $\theta_{0_X} = \pi/2$, and $\theta_{1_X} = 3\pi/2$; however, due to SPFs, the real angles may differ from these ideal values. The crucial difference between the states in Eq. (1.18) and those produced by an arbitrary basis-dependent flaw is that, in the latter, the encoding flaws may be in an arbitrary dimension, while in the former, all the encoded states are in the same qubit space, spanned by the basis vectors $\{|0_Z\rangle, |1_Z\rangle\}$. Because of this, Eve will not be able to exploit channel loss to perform an undetected USD attack. The idea is the following: let us assume that $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$ are any states in the same qubit space. These states form a plane in the Bloch sphere, and any other state $|\psi_4\rangle$ that is also in this plane may be expressed as,

$$|\psi_4\rangle\langle\psi_4| = c_{1|4}\,|\psi_1\rangle\langle\psi_1| + c_{2|4}\,|\psi_2\rangle\langle\psi_2| + c_{3|4}\,|\psi_3\rangle\langle\psi_3|\,, \tag{1.19}$$

where $c_{1|4}$, $c_{2|4}$ and $c_{3|4}$ are real coefficients. Let us assume that Alice and Bob run a protocol in which Alice emits $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$, and let Y_i be the yield of the state $|\psi_i\rangle$, i.e. the probability that Bob obtains a successful detection given that Alice emits $|\psi_i\rangle$. Then, from Eq. (1.19), it follows that

$$Y_4 = c_{1|4}Y_1 + c_{2|4}Y_2 + c_{3|4}Y_3. \tag{1.20}$$

That is, Alice and Bob can estimate the yield of the state $|\psi_4\rangle$ without actually emitting this state.

Based on this idea, Tamaki *et al.* [45] proposed the loss-tolerant protocol, which can provide an almost identical performance to a perfect BB84 protocol in the presence of large SPFs. In this protocol, Alice emits three different states, and the only assumption is that they are characterised and in the same qubit space. For simplicity, let us assume that the three states are in the form of Eq. (1.18), i.e. in the XZ plane of the Bloch sphere, and denote them as $|\psi_{0_Z}\rangle$, $|\psi_{1_Z}\rangle$ and $|\psi_{0_X}\rangle$. Let us also assume that Alice and Bob generate their sifted keys from the detected events in which Alice selects $|\psi_{0_Z}\rangle$ or $|\psi_{1_Z}\rangle$ and Bob chooses the Z basis. As in Section 1.1.3.2, to prove the security, we consider the phase-error rate e_{ph} that Alice and Bob would have obtained in the virtual protocol, a fictitious scenario in which, in the key rounds, Alice prepares the entangled state

$$|\Psi_Z\rangle = \frac{1}{\sqrt{2}}(|0_Z\rangle_A\,|\psi_{0_Z}\rangle_B + |1_Z\rangle_A\,|\psi_{1_Z}\rangle_B), \tag{1.21}$$

and Alice and Bob respectively measure systems A and B in the X basis. This is equivalent to Alice preparing the state $|\psi_{\text{vir}j}\rangle \propto {}_A\langle j_X|\Psi_Z\rangle$ with probability $p_{\text{vir}j} =$

$\|_A\langle j_X|\Psi_Z\rangle\|^2$, where $j \in \{0,1\}$. The phase-error rate formula can then be expressed as $e_{\text{ph}} = (p_{\text{vir}0}Y^{1_X}_{\text{vir}0} + p_{\text{vir}1}Y^{0_X}_{\text{vir}1})/Y_Z$, where $Y^{k_X}_{\text{vir}j}$ is the probability that Bob's X-basis measurement results in an outcome k when Alice emits $|\psi_{\text{vir}j}\rangle$, and Y_Z is the rate at which Bob obtains a successful detection when Alice chooses the Z basis. To know e_{ph}, we need to estimate $Y^{1_X}_{\text{vir}0}$ and $Y^{0_X}_{\text{vir}1}$, since Y_Z is directly observable. For this, since the *virtual* states are in the same Bloch sphere plane as the real states, one can use the idea in Eqs. (1.19) and (1.20) to find the following expressions,

$$Y^{1_X}_{\text{vir}0} = c_{0_Z|\text{vir}0}Y^{1_X}_{0_Z} + c_{1_Z|\text{vir}0}Y^{1_X}_{1_Z} + c_{0_X|\text{vir}0}Y^{1_X}_{0_X} \tag{1.22}$$

$$Y^{0_X}_{\text{vir}1} = c_{0_Z|\text{vir}1}Y^{0_X}_{0_Z} + c_{1_Z|\text{vir}1}Y^{0_X}_{1_Z} + c_{0_X|\text{vir}1}Y^{0_X}_{0_X}, \tag{1.23}$$

where the yields on the RHS are directly observable from the protocol, and the coefficients $c_{i|\text{vir}j}$ are real and known. Thus, using this method, the phase-error rate can be estimated precisely, and the protocol is *loss tolerant* to SPFs, i.e. Eve cannot hide behind channel loss to perform an undetected USD attack.

The finite-key security of the loss-tolerant protocol was first demonstrated in Ref. [46], and more recently in Ref. [47], where we derived significantly tighter finite-key security bounds, see Section 1.2.1.4. Moreover, recent works have shown that the protocol is also secure in the presence of additional source imperfections, such as information leakage or pulse correlations, as long as their magnitude is sufficiently small [48, 49].

1.2.1.3 Countermeasures against measurement flaws

In general, detectors are much more difficult to secure against side-channel attacks than sources. Using optical isolation devices, Alice can typically prepare her signals in a protected environment outside the reach of the eavesdropper, and by verifying a random sample of these signals, she can in principle characterise her source. Neither of these hold for Bob's measurement device: he cannot be isolated from the outside world, as he must receive and measure the incoming pulses; and it is extremely difficult to characterise his measurement, since Eve may send any kind of signal to him, including strong optical pulses and even x-rays or neutrinos. Thus, the majority of hacking attacks that have been theoretically proposed and/or experimentally demonstrated against QKD systems exploit flaws in its detectors [50, 51], and while suitable countermeasures have been found to close some of these, the fact remains that they are typically the weakest

spot in the security of a QKD system. Fortunately, as we will see next, there is a class of protocols in which neither Alice nor Bob perform any measurement on quantum states, and are thus not vulnerable to any detector side-channel attack.

Measurement-device-independent QKD The first protocol of this kind was measurement-device-independent (MDI) QKD [52], see also Ref. [53], and the class of protocols is sometimes referred to as MDI-type. In MDI-QKD, Alice and Bob both send BB84-encoded states to an untrusted middle node Charlie, who (if honest) performs a Bell state measurement (BSM) on the incoming pulses, see Fig. 1.3, and announces the result. If Charlie truly performs a BSM, he will learn whether the users' bits are correlated or anti-correlated, but will not gain any information about their specific bit values. The users can then use the announced correlation information to correct errors in their keys. If Charlie is dishonest, and tries to learn some information about the encoded bit values, he will inevitably introduce some errors in at least one of the two bases. The security proof of MDI-QKD does not make any assumption on Charlie's measurement, treating him as a black box, and thus the protocol is not vulnerable to any detector side-channel attack.

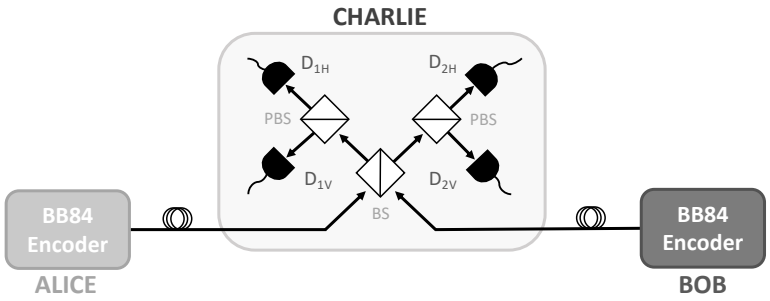


Figure 1.3: Schematic diagram of MDI-QKD [52]. Alice and Bob send polarisation-encoded BB84 pulses to a middle node Charlie, who performs a BSM based solely on linear optics components, which is able to project the incoming pulses onto two out of the four Bell states. A click in $D_{1\mathrm{H}}$ and $D_{1\mathrm{V}}$, or in $D_{2\mathrm{H}}$ and $D_{2\mathrm{V}}$, indicates a projection onto the Bell state $|\Psi^+\rangle = \frac{1}{2}(|HV\rangle + |VH\rangle)$; thus, the users' bits should be correlated (anti-correlated) if they both selected the X (Z) basis. A click in $D_{1\mathrm{H}}$ and $D_{2\mathrm{V}}$, or in $D_{2\mathrm{H}}$ and $D_{1\mathrm{V}}$, indicates a projection onto the Bell state $|\Psi^-\rangle = \frac{1}{2}(|HV\rangle - |VH\rangle)$; the users' bits should be anti-correlated if they both selected the same basis.

The main experimental challenge of MDI-QKD is performing high-visibility two-

photon interference between photons arising from independent and far-away laser sources. One must ensure that both photons are close to identical, which requires the use of feedback mechanisms to compensate for the different time-dependent polarisation rotations and propagation delays in the two independent optical fibres [51]. Moreover, since MDI-QKD requires two detectors to click, its key rate is more vulnerable to low detector efficiencies [54] than that of BB84, although this can be mitigated by the use of SNSPD detectors, whose efficiency can be as high as 93% [55]. Also, the need for two-fold coincidence detector events makes the protocol more resilient to dark counts, allowing it to reach longer distances. In fact, Ref. [56] implemented MDI-QKD over a 404 km total distance, a record at the time.

The original MDI-QKD scheme used polarisation encoding, but alternative phase-encoding schemes have been proposed [57, 58]. Moreover, some recently introduced MDI-type protocols can improve key-rate scaling with distance, the best known of which are memory-assisted QKD and twin-field QKD; we introduce these in Section 1.2.2.1 and Section 1.2.2.2. Note that, when implementing MDI-QKD, one still needs to deal with all the flaws associated with the user sources. In fact, these can have an even bigger impact in MDI-type protocols, since each flaw may now be present in both users, rather than just Alice. Fortunately, MDI-QKD can be combined with essentially all the source countermeasures introduced in Section 1.2.1.1 and Section 1.2.1.2, including the decoy-state method and the loss-tolerant protocol [45].

1.2.1.4 Asymptotic assumption and finite-key security

As we have seen in Section 1.1.3, to prove the security of a QKD protocol, one typically needs to estimate the phase-error rate, which can be used to bound the amount of information that may have leaked to an eavesdropper. This parameter is defined as the error rate that Alice and Bob would have obtained if they had run the virtual protocol instead of the actual protocol, and must be statistically bounded using data obtained in the actual protocol. For simplicity, many security proofs assume the asymptotic limit of $N_{\text{tot}} \to \infty$, in which case one can often obtain a perfect estimate of the phase-error rate, since all statistical deviation terms vanish. However, real QKD experiments must run for a finite number of rounds, and the more-complex finite-key security proofs consider the statistical fluctuations that inevitably arise in its estimation. How these are accounted for can have an important impact in the secret-key rate obtainable.

As pointed out in Section 1.1.2.1, when one considers security against coherent attacks, the detection statistics of a given round may depend on the choices made and outcomes obtained in other rounds, i.e. Eve's attack is not necessarily IID between different rounds of the protocol. However, as seen in Section 1.1.3.2, for simple protocols that rely on two mutually unbiased encoding bases, the statistical fluctuation task can be trivially reduced to a random sampling problem. This problem can then be solved using concentration bounds for sums of independent random variables, such as Chernoff bounds [59], even if Eve performs a coherent attack. This is because, when the encoding bases are mutually unbiased, Eve does not have any information about Alice's basis choice; one can even think of an equivalent fictitious scenario in which the choice is made *after* Eve's attack. However, many protocols do not rely on mutually unbiased encoding bases, either because they take into account source imperfections, see Section 1.2.1.2, or because of the inherent design of the protocol. In these cases, finite-key regime proofs become more complex, and often employ Azuma's inequality [60] to deal with the dependency between different rounds of the protocol that may exist due to a coherent attack. However, Azuma's inequality is typically less tight than Chernoff bounds, which results in lower secret-key rates.

The issue of statistical fluctuations is especially important for decoy-state protocols. In the asymptotic regime, one can in principle obtain perfect estimates of the single-photon yield Y_1^Z and phase-error rate e_1^X, but in the finite-key regime, one must apply a complex statistical fluctuation analysis to obtain bounds on these parameters. Several works have considered the finite-key security of decoy-state BB84 [61, 62] and MDI-QKD [63, 64].

Our contribution [47]: Finite-key analysis of loss-tolerant QKD based on random sampling theory In the asymptotic regime, the loss-tolerant protocol presented in Section 1.2.1.2 can obtain a perfect estimation of the phase-error rate, and consequently provides an almost identical performance to an ideal BB84 protocol in the presence of SPFs. However, since the loss-tolerant protocol does not rely on mutually unbiased encoding bases, its finite-key phase-error rate estimation task cannot be trivially reduced to a random sampling problem, as in the case of the BB84 protocol. The previous finite-key analysis of the protocol in Ref. [46] relied on the application of

Azuma's inequality to estimate the phase-error rate, which results in a worse performance than random sampling inequalities.

In Ref. [47], presented in Chapter 2, we show that, if Alice probabilistically assigns tags to her detected emissions, the phase-error rate estimation of the loss-tolerant protocol can be non-trivially reduced to a random sampling problem, which can be tightly solved using Chernoff bounds. In doing so, we obtain significantly better secret-key rates than the previous analysis based on Azuma's inequality. This has important implications for existing and future implementations of loss-tolerant QKD, and also for the security of QKD in general, since it shows that one may use random sampling techniques to prove the security of protocols for which it was not thought possible.

1.2.2 Challenge II: Improving key-rate scaling with loss

The first and best-known QKD protocol, BB84, is a prepare-and-measure *point-to-point* protocol: Alice sends encoded single photons to Bob through a direct quantum channel, such as an optical fibre, and then Bob performs a measurement on these photons. While theoretically simple and relatively easy to implement, these protocols have a fundamental practical problem: they cannot be performed over long distances, at least over standard optical fibre. The reason is that, in optical fibres, the channel transmittance η decreases exponentially with its length. With a moderate channel length of 100 km, around one in every hundred photons emitted by Alice reach Bob's lab. Over a 300-km channel, achievable by today's BB84 implementations [65], the rate of photon arrivals drops to around one in a million. If one increases the channel length to 1000 km, which falls short of covering the Earth's circumference, only around one in 10^{20} photons survives: even with a very ambitious source repetition rate of 10 GHz, it would take Bob hundreds of years to receive just one single photon from Alice. Fundamental bounds show that the secret-key rate of point-to-point QKD protocols cannot exceed $-\log_2(1-\eta)$ [66], which is approximately equal to $\frac{\eta}{\ln 2}$ for low values of η. In other words, point-to-point protocols have at best $O(\eta)$ secret-key rate scaling.

The theoretical solution to this problem has been known for many years, in what is known as quantum repeaters [67], see Fig. 1.4. Conventionally, they are based on entanglement swapping: given an entangled state between A and C_1 and another entangled state between B and C_2, one can entangle systems A and B by performing a BSM on C_1 and C_2. Thus, if one wants to create an entangled state over a long

distance L, one can generate two entangled states over half the distance, $L/2$, and then perform entanglement swapping. Similarly, the entanglement over a distance $L/2$ can be created by swapping two entangled states generated over a distance $L/4$, and so on. In a quantum repeater setup, the long channel separating Alice and Bob is divided into many smaller segments, and a node is placed between each of them. The nodes must be equipped with two quantum memories (QMs), one connected to each link, while the end users, Alice and Bob, must have one QM each. The idea is that, if one manages to generate entanglement over all the elementary links, then one can perform successive entanglement swapping rounds until Alice and Bob themselves end up becoming entangled.

To generate the elementary entanglement, each node can simply generate an entangled pair locally, store half of the pair in one of their QMs, and send the other half over its respective segment. Of course, it is possible that, in any of these emissions, the photon does not arrive to the destination. If so, the emitter generates another entangled state locally, replaces the state in his QM by half of the new pair, and emits the other half, repeating this step until the receiver confirms that a photon has arrived and their associated QM has been loaded. If the original channel had a transmissivity of η, then each of the n segments has now a transmissivity of $\sqrt[n]{\eta}$, and the probability that all of the photons survive path loss in the first trial is $(\sqrt[n]{\eta})^n = \eta$, exactly the same as the probability that a single photon will survive path loss through the entire Alice-Bob channel. However, the key is that it is not necessary for all the photons to survive path loss in the same round: the QMs can store the surviving photons while the unsuccessful emissions are retried.

Thanks to this, a quantum repeater scheme with ideal QMs can provide exponentially better quantum communication rates than direct transmission. Unfortunately, state-of-the-art QMs are far from ideal, and their coherence times are not good enough to implement a quantum repeater setup. However, the fact remains that point-to-point protocols have at best $O(\eta)$ scaling, and to overcome this limitation a protocol needs to have at least one middle node. Interestingly, this is not a sufficient condition: the MDI-QKD protocol introduced in Section 1.2.1.3 is a well-known counterexample. In MDI-QKD, both of Alice's and Bob's photons need to survive path loss in the same round, which happens with probability $(\sqrt{\eta})^2 = \eta$. Thus, while offering other advantages, standard MDI-QKD cannot improve key-rate scaling with respect to a BB84

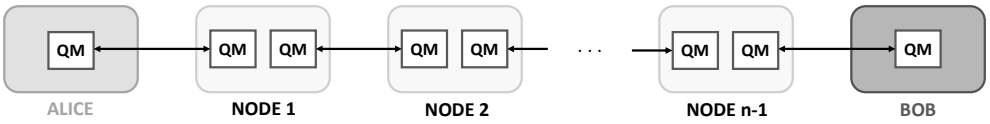


Figure 1.4: Example of a quantum repeater. The first step is to attempt to generate entanglement between each QM pair linked by a double-headed arrow, using a heralded entanglement distribution scheme [67–69]. Each QM pair repeats this step until the entanglement has been successfully generated. The repetition rate is limited by the transmission delay over the corresponding elementary link. When all QM pairs have become entangled, there will be successive rounds of entanglement swapping, in which the nodes in the middle perform a BSM, and announce the result. At the end of the process, Alice and Bob's QMs will be entangled.

protocol. However, as we will see next, some recently-proposed MDI-type protocols can achieve $O(\sqrt{\eta})$ scaling, and can thus potentially reach longer distances.

1.2.2.1 Memory-assisted QKD

The reason why MDI-QKD has $O(\eta)$ scaling is that, to obtain a successful BSM, both Alice's and Bob's photons need to survive path loss in the same round. If Charlie could interfere photons that have survived on different rounds, the scaling would be improved to $O(\sqrt{\eta})$. Memory-assisted (MA) QKD [70, 71] achieves this by placing two QMs on Charlie's setup, see Fig. 1.5. This way, a surviving photon on, say, Alice's side can be stored until one photon survives on Bob's side, after which both photons can be retrieved and interfered.

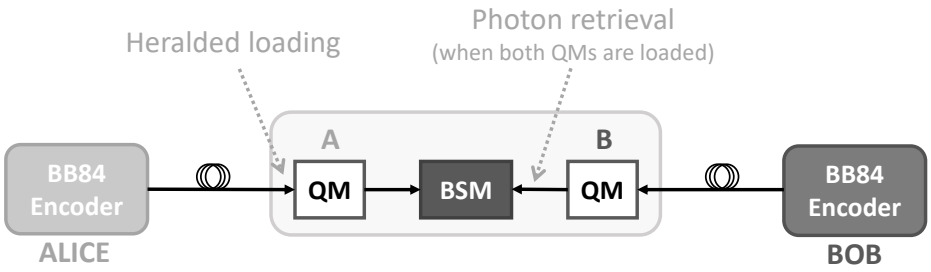


Figure 1.5: Schematics of MA-QKD [70, 71]. The setup is similar to that of MDI-QKD, see Fig. 1.3, with the addition of two quantum memories on Charlie's setup.

MA-QKD is similar to a quantum repeater with a single node, but there are impor-

tant differences between the two setups. In the latter, Alice and Bob would generate an entangled state locally, store half of the pair in their own QM, and send the other pair to Charlie, repeating this procedure until Charlie's associated QM has been loaded. Then, once both of Charlie's QMs are loaded, he would retrieve the states, perform a BSM, and communicate the result to Alice and Bob, after which the state on Alice's and Bob's QMs should be entangled. At that point, if their goal is to perform QKD, Alice and Bob can measure their QM randomly in either the Z or X basis. Note that, in this single-node repeater setup, the performance of Alice's and Bob's QMs is clearly the bottleneck, since they have to store their quantum states since the beginning. On the other hand, Charlie's early-loaded QM needs to store the quantum state until his late QM is loaded, while the late QM is read immediately after loading. The idea behind MA-QKD is that, if Alice's and Bob's goal is to perform QKD, they do not actually need to wait until the end of the protocol to perform the measurement on their local state; they can measure in the very beginning, eliminating the need for a QM. In fact, Alice and Bob do not actually need to generate an entangled pair and measure half of it. They can simply encode BB84 states, which is equivalent; see discussion around Eq. (1.11). Another related difference is the protocol repetition rate. In a single-node quantum repeater, Alice (Bob) needs to wait for Charlie to announce whether his QM has been loaded to initiate another attempt, since to do so she (he) must store half of a newly generated entangled pair in their QM, destroying the previous state. However, in MA-QKD, Alice and Bob can emit photons as fast as they can be stored in Charlie's QM. The potentially faster repetition rate can significantly reduce the average storage time of Charlie's early QM, making MA-QKD an attractive alternative to a single-node quantum repeater.

Because of these differences, MA-QKD places far less stringent demands on QMs than even a single-node quantum repeater. However, despite these reduced requirements, it is not clear if state-of-the-art QMs are sufficiently advanced for MA-QKD to provide an advantage over a memory-less MDI-QKD setup in realistic conditions. Reference [72] has recently reported an MA-QKD experiment over a total loss of 70 dB, equivalent to around 350 km of real optical fibre, although Alice and Bob were located in the same lab. This proof-of-principle demonstration obtained a higher secret-key rate than that of an ideal memory-less MDI-QKD setup. However, the comparison may not be entirely fair, since the MA-QKD setup had to be run at a relatively low repetition

rate of 1 MHz, while standard MDI-QKD has achieved clock rates of 1 GHz [73]. In terms of secret-key bits per second, the improved scaling with loss cannot offset the 10^3 times lower repetition rate. Still, given that its main limitation is the performance of QMs, which are rapidly improving, MA-QKD is a promising protocol to perform QKD at longer distances. In fact, it could potentially offer higher key rates at longer distances than its main alternative, twin-field QKD, which we will shortly discuss in Section 1.2.2.2. Moreover, theoretical and experimental work on MA-QKD brings us closer to the ultimate goal of worldwide trust-free quantum communications, since it is the stepping stone between point-to-point QKD and a full quantum repeater.

All-photonic alternative MA-QKD improves the key-rate scaling of MDI-QKD because it allows Charlie to interfere pulses that have survived in different rounds. The same $O(\eta)$ scaling could be achieved if each of Alice and Bob were connected to Charlie through multiple channels, and Charlie could combine pulses that have survived in different channels, rather than in different rounds. Based on this idea, Ref. [74] proposed an all-photonic protocol in which Charlie performs QND measurements to check on which channels the signals have arrived, and then passes them through optical switches to interfere the surviving pulses. While certainly interesting, this protocol is far from being implementable with current technology [75].

Our contribution [76]: Finite-key analysis of decoy-state MA-QKD Previous theoretical work [70, 71, 77, 78] on MA-QKD had compared its performance with that of memory-less MDI-QKD under idealistic experimental conditions. Namely, they assumed that the users employed single-photon sources and considered only the asymptotic regime in which the protocol is run for an infinite number of rounds. Their results suggested that, using state-of-the-art QMs, MA-QKD can only provide a modest secret-key rate advantage for a small window of distances, around 350 km to 450 km, which is still difficult to implement experimentally.

In Ref. [76], presented in Chapter 3, we have analysed the performance of MA-QKD under more realistic conditions: (1) assuming that the users employ weak coherent pulse (WCP) sources, in combination with the decoy-state method; and (2) taking into account the statistical fluctuations that arise from running the protocol for a finite number of rounds. Our results suggest that MA-QKD is significantly more resilient

to decoy-state finite-key effects than an equivalent MDI-QKD system, and can thus outperform the latter at much shorter distance regimes when these effects are taken into account. This has important implications for MA-QKD experiments that aim to demonstrate a key-rate advantage with respect to memory-less setups.

1.2.2.2 Twin-field QKD

Recently, Lucamarini *et al.* [79] devised a more practical approach to obtain $O(\sqrt{\eta})$ scaling, known as twin-field (TF) QKD. The idea is to substitute the two-photon interference of MDI-QKD by single-photon interference, which requires only one photon to survive path loss, hence the $O(\sqrt{\eta})$ scaling. In TF-QKD, Charlie's measurement setup may be regarded as an imperfect BSM in the qubit space spanned by vacuum ($|0\rangle$) and single-photon ($|1\rangle$) states, and requires only standard optical elements, see Fig. 1.6. The original proposal only proved the security of TF-QKD against restricted eavesdropping attacks, but a later work proved its security against general attacks [80]. Moreover, since then, several variants of the scheme have been proposed and also proven to be secure against general attacks [81–84]. The main experimental challenge of TF-QKD is the precise phase stability needed to perform single-photon interference with pulses originating from two remote independent lasers. Thus, in the first proof-of-principle TF-QKD experiments [85–88], Alice and Bob were located in the same lab, which facilitated the implementation of the feedback mechanisms needed to phase-lock their respective lasers. Nevertheless, later experiments [89, 90] implemented TF-QKD with independent lasers over 502 km and 509 km of ultra-low-loss fibre, obtaining higher secret-key rates than the fundamental bounds on point-to-point QKD. A recent experiment has performed TF-QKD over a record-breaking 605 km of optical fibre [91].

TF-QKD with single-photon sources Practical variants of TF-QKD rely on WCP sources, typically in combination with the decoy-state method. However, the idea behind TF-QKD is perhaps best understood by looking at a single-photon version of

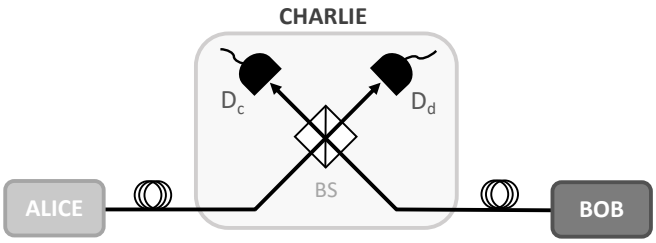


Figure 1.6: Schematic view of Charlie's measurement in TF-QKD. A click on detector D_{c} (D_{d}) is associated with constructive (destructive) interference at the 50:50 beamsplitter (BS). The states emitted by Alice and Bob depend on the specific TF-QKD variant.

it [83], in which Alice and Bob prepare the states

$$\begin{aligned} |Z_0\rangle &= |0\rangle && \text{with prob. } q \\ |Z_1\rangle &= |1\rangle && \text{with prob. } 1-q \\ |X_0\rangle &= \sqrt{q}\,|0\rangle + \sqrt{1-q}\,|1\rangle && \text{with prob. } 1/2 \\ |X_1\rangle &= \sqrt{q}\,|0\rangle - \sqrt{1-q}\,|1\rangle && \text{with prob. } 1/2. \end{aligned} \tag{1.24}$$

Note that these states do not define two mutually unbiased bases; for starters, the X-basis states are not even orthogonal to one another. However, the two bases can still be regarded as *complementary*, since the state preparation could have been replaced by the generation of the entangled state

$$|\Psi\rangle = \sqrt{q}\,|0\rangle_F\,|Z_0\rangle + \sqrt{1-q}\,|1\rangle_F\,|Z_1\rangle = \frac{1}{\sqrt{2}}(|+\rangle_F\,|X_0\rangle + |-\rangle_F\,|X_1\rangle) \tag{1.25}$$

followed by either a Z-basis or a X-basis measurement on the fictitious qubit ancilla F. Thus, if one extracts the key from the detected Z-basis emissions, one can directly estimate the phase-error rate using the bit-error rate of the detected X-basis emissions, and vice-versa, with a similar argument as for the BB84 protocol in Section 1.1.3.2.

In the Z basis, events in which Alice and Bob send the same state and Charlie reports a success are considered an error. In order to keep the error rate low, it is important that $\frac{1}{2} \ll q \lesssim 1$. Emissions of $|0\rangle\,|0\rangle$ are very common, but they should produce very few clicks on Charlie's detectors, while emissions of $|1\rangle\,|1\rangle$ are unlikely to happen, since $(1-q)^2$ is very low; thus, the bulk of the detections should be due to emissions of $|1\rangle\,|0\rangle$ and $|0\rangle\,|1\rangle$, the error-free terms. An emission of $|1\rangle\,|0\rangle$ ($|0\rangle\,|1\rangle$) results in a detection if the photon survives path loss over the Alice-Charlie (Bob-Charlie)

channel, which happens with probability $\sqrt{\eta}$. This implies that the protocol has $O(\sqrt{\eta})$ scaling. In the X basis, the definition of an error depends on the specific detector that has clicked. When Charlie reports a click on detector D_c (D_d), an emission of $|X_0\rangle|X_1\rangle$ or $|X_1\rangle|X_0\rangle$ ($|X_0\rangle|X_0\rangle$ or $|X_1\rangle|X_1\rangle$) is considered to be an error, since these should result in destructive (constructive) interference. Note that both bases have errors that are inherent to the protocol, i.e. they occur even if the devices and channel are ideal. This stands in contrast with MDI-QKD, where, in the absence of Eve, all errors occur due to imperfections in the channel, sources or measurement. Despite this, TF-QKD can offer better key rates than MDI-QKD in the long-distance regime, due to its $\sqrt{\eta}$ scaling.

The version of the protocol presented here uses the Z and X basis to encode. However, the users could have substituted either of these by the Y basis,

$$\begin{aligned} |Y_0\rangle &= \sqrt{q}\,|0\rangle - i\sqrt{1-q}\,|1\rangle \quad \text{with prob. } 1/2, \\ |Y_1\rangle &= \sqrt{q}\,|0\rangle + i\sqrt{1-q}\,|1\rangle \quad \text{with prob. } 1/2, \end{aligned} \tag{1.26}$$

equivalent to measuring the ancilla F of Eq. (1.25) in the Y basis.

Curty-Azuma-Lo variant The single-photon TF-QKD protocol presented above has a simple theoretical description, and it is useful to understand the idea behind TF-QKD. However, $|X_0\rangle$ and $|X_1\rangle$ are superpositions of vacuum and single-photon states, which are very difficult to generate in practice. Thus, most proposals, including the original proposal in Ref. [79], approximate the above single-photon idea using WCP sources. Here, we focus on the variant proposed in Ref. [83], which approximates the X-basis states $|X_0\rangle$ and $|X_1\rangle$ by the coherent states

$$\begin{aligned} |\alpha\rangle &= \sum_{n=0}^{\infty} c_n\,|n\rangle = c_0\,|0\rangle + c_1\,|1\rangle + c_2\,|2\rangle + c_3\,|3\rangle + \ldots, \\ |-\alpha\rangle &= \sum_{n=0}^{\infty} (-1)^n c_n\,|n\rangle = c_0\,|0\rangle - c_1\,|1\rangle + c_2\,|2\rangle - c_3\,|3\rangle + \ldots, \end{aligned} \tag{1.27}$$

which differ from $|X_0\rangle$ and $|X_1\rangle$ only in the presence of multi-photon components $n > 1$. To prove the security of a key generated by emitting these states, one needs to consider the equivalent entanglement-based scenario in which the users prepare

$$|\Psi_X\rangle = \frac{1}{\sqrt{2}}(|0_X\rangle_F\,|\alpha\rangle + |1_X\rangle_F\,|-\alpha\rangle). \tag{1.28}$$

In particular, one needs to estimate the phase-error rate that the users would obtain if they had measured the ancillas in Eq. (1.28) in the Z basis, rather than in the X basis. One can rewrite Eq. (1.28) as

$$|\Psi_X\rangle = \frac{1}{2}|0_Z\rangle_F(|\alpha\rangle + |-\alpha\rangle) + \frac{1}{2}|1_Z\rangle_F(|\alpha\rangle - |-\alpha\rangle). \tag{1.29}$$

This imples that the virtual protocol is equivalent to a scenario in which the users emit the even and odd cat states

$$\begin{aligned} |C_0\rangle &\propto {}_F\langle 0_Z|\Psi_X\rangle = \sum_{n \text{ even}} c_n |n\rangle, \\ |C_1\rangle &\propto {}_F\langle 1_Z|\Psi_X\rangle = \sum_{n \text{ odd}} c_n |n\rangle, \end{aligned} \tag{1.30}$$

with probabilities $p_{C_0} = \|{}_F\langle 0_Z|\Psi_X\rangle\|^2$ and $p_{C_1} = \|{}_F\langle 1_Z|\Psi_X\rangle\|^2$, respectively. As in the single-photon version, a phase-error occurs when the users send the same Z-basis state, i.e. $|C_0\rangle|C_0\rangle$ or $|C_1\rangle|C_1\rangle$, and the round is detected.

Ideally, Alice and Bob would estimate the phase-error rate directly by emitting these cat states. However, they are very difficult to generate experimentally. Instead, Ref. [83] proposed to bound the detection rates of the cat states indirectly. Assuming the asymptotic regime and collective attacks, and applying the Cauchy-Schwarz inequality, they showed that

$$Y_{C_jC_j} \leq \frac{1}{p_{C_j}^2}\left[\sum_{n+m\in\mathbb{N}_j} c_n c_m \sqrt{Y_{nm}}\right]^2, \tag{1.31}$$

where $j \in \{0,1\}$, $\mathbb{N}_0$ ($\mathbb{N}_1$) is the set of non-negative even (odd) numbers, $Y_{C_jC_j}$ is the yield probability of $|C_j\rangle|C_j\rangle$, and Y_{nm} is the yield probability of $|n\rangle|m\rangle$. The only step missing is to estimate Y_{nm}, which can be done by emitting PRCS and applying the decoy-state method.

A similar protocol with a slightly different security proof was independently proposed by Ref. [84]. In the literature, these two closely-related variants are sometimes referred to as no-phase-postselection TF-QKD.

Our work [92]: Finite-key security analysis of TF-QKD The protocol proposed by Ref. [83] has a simple experimental setup, and also a relatively-simple asymptotic security proof. However, its extension to the finite-key regime is not trivial. For

starters, their analysis assumes collective attacks. As mentioned in Section 1.1.2.1, in the asymptotic regime, security against collective attacks implies security against general attacks, but in the finite-key regime, it does not. Moreover, the protocol clearly does not rely on two complementary encoding bases, since the detection statistics of the cat states are estimated indirectly, and thus does not admit the simple statistical fluctuation analysis based on random sampling introduced in Section 1.1.3.2. Also, the asymptotic formula in Eq. (1.31) is a function of infinitely many yield probabilities Y_{nm}. In practice, one can only obtain good bounds for the lower order terms, and the authors proposed to trivially upper bound the rest by one. In the finite-key regime, however, one does not deal with yield probabilities, but rather with actual measurement results, and it is not possible to apply this trivial upper bound.

In Ref. [92], presented in Chapter 4, after carefully accounting for all the difficulties above, we prove the finite-key security of the protocol against general attacks. In doing so, we show that the protocol can overcome the fundamental bounds on point-to-point QKD with around 10^{10} transmitted signals, corresponding to around 10 s, assuming a repetition rate of 1 GHz.

Our work [40]: Security of TF-QKD with discrete phase randomisation As mentioned above, many variants of TF-QKD have been proposed to implement the basic single-photon interference idea with WCP sources. Essentially, all of them rely on the decoy-state method in one way or another. For example, the protocol explained above relies on it to estimate the detection statistics of photon-number states, an important step in estimating the phase-error rate. The decoy-state method assumes that the users can emit WCPs with a fully-random continuous phase. However, as explained in Section 1.2.1.1, these states are very difficult to generate in practice, and essentially impossible to certify. It is much easier to randomise the phase of a pulse discretely, using a random number generator and a phase modulator, and this approach is commonly used in practice. However, by doing so, one breaks the assumptions of the existing security proofs, and the implementation may not be secure.

In Ref. [40], presented in Chapter 5, we introduce and prove the security of a TF-QKD variant that relies exclusively on discrete-phase randomisation. The quantum phase of our variant is similar to that of Ref. [83], but uses discrete, rather than continuous, phase randomisation in the test mode. Surprisingly, our discretely-randomised

protocol can actually provide higher secret-key rates than the proposal by Ref. [83]. The reason is that discrete randomisation allows the users to post-select the events in which they chose exactly the same phase, and the post-selected data provides a tighter estimation of the phase-error rate. This shows that, although it is typically treated as a source flaw, discrete phase randomisation can actually offer advantages in some scenarios.

1.3 Structure of the thesis

In Chapter 2, we provide an alternative finite-key analysis for the loss-tolerant protocol. In Chapter 3, we present our analysis of the performance of decoy-state MA-QKD in the finite-key regime. In Chapter 4, we prove the finite-key security of the TF-QKD variant introduced in Ref. [83]. In Chapter 5, we present a TF-QKD variant that relies exclusively on discrete phase randomisation, and prove its security. In Chapter 6, we conclude this thesis.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978. 2

[2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Comput.*, vol. 26, pp. 1484–1509, Oct. 1997. 3

[3] C. Pomerance, "A tale of two sieves," in *Notices Amer. Math. Soc*, Citeseer, 1996. 3

[4] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, Oct. 2019. 3

[5] G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," *Trans. Am. Inst. Electr. Eng.*, vol. XLV, pp. 295–301, Jan. 1926. 3

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949. 4

[7] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982. 5

[8] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984. 5

[9] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, pp. 78–88, Jan. 1983. 5

[10] H.-K. Lo, H. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *J Cryptology*, vol. 18, pp. 133–165, Apr. 2005. 7

[11] C.-H. F. Fung, X. Ma, and H. F. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A*, vol. 81, p. 012318, Jan. 2010. 9, 11, 17

[12] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "Using quantum key distribution for cryptographic purposes: A survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, Dec. 2014. 9

[13] D. Stebila, M. Mosca, and N. Lütkenhaus, "The Case for Quantum Key Distribution," in *Quantum Communication and Quantum Networking* (A. Sergienko, S. Pascazio, and P. Villoresi, eds.), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, (Berlin, Heidelberg), pp. 283–296, Springer, 2010. 9

[14] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pp. 136–145, Oct. 2001. 10

[15] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The Universal Composable Security of Quantum Key Distribution," in *Theory of Cryptography* (J. Kilian, ed.), Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 386–406, Springer, 2005. 10

[16] R. Renner and R. König, "Universally Composable Privacy Amplification Against Quantum Adversaries," in *Theory of Cryptography* (J. Kilian, ed.), Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 407–425, Springer, 2005. 10

[17] N. Lütkenhaus, "Estimates for practical quantum cryptography," *Phys. Rev. A*, vol. 59, pp. 3301–3319, May 1999. 11

[18] M. Hayashi and T. Tsurumaru, "Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths," *New J. Phys.*, vol. 14, p. 093014, Sept. 2012. 11, 13, 14, 17

[19] R. Renner, "Symmetry of large physical systems implies independence of subsystems," *Nat. Phys.*, vol. 3, pp. 645–649, Sept. 2007. 12

[20] M. Christandl, R. König, and R. Renner, "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography," *Phys. Rev. Lett.*, vol. 102, p. 020504, Jan. 2009. 12

[21] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, pp. 351–406, May 2001. 13

[22] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, July 2000. 13

[23] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, p. 045018, Apr. 2009. 13, 18

[24] R. Renner, *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, Sept. 2005. 13

[25] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nat. Commun.*, vol. 3, p. 634, Jan. 2012. 13, 17

[26] T. Tsurumaru, "Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3465–3484, 2020. 13

[27] M. Koashi and J. Preskill, "Secure Quantum Key Distribution with an Uncharacterized Source," *Phys. Rev. Lett.*, vol. 90, p. 057902, Feb. 2003. 18

[28] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sept. 2009. 19

[29] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug. 2000. 20

[30] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr. 2000. 20, 21

[31] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, vol. 4, pp. 325–360, 2004. 20

[32] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug. 2003. 21

[33] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, June 2005.

[34] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Phys. Rev. Lett.*, vol. 94, p. 230503, June 2005. 21

[35] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, July 2005. 21

[36] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Express, OE*, vol. 20, pp. 12366–12377, May 2012. 22

[37] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Opt. Express, OE*, vol. 22, pp. 1645–1654, Jan. 2014. 22

[38] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," *Appl. Phys. Lett.*, vol. 117, p. 144003, Oct. 2020. 22

[39] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New J. Phys.*, vol. 17, p. 053014, May 2015. 22

[40] G. Currás-Lorenzo, L. Wooltorton, and M. Razavi, "Twin-Field Quantum Key Distribution with Fully Discrete Phase Randomization," *Phys. Rev. Applied*, vol. 15, p. 014016, Jan. 2021. 22, 38

[41] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Info. Comput.*, vol. 7, pp. 431–458, July 2007. 23

[42] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," *Phys. Rev. X*, vol. 5, p. 031030, Sept. 2015. 23

[43] K. Tamaki, M. Curty, and M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," *New J. Phys.*, vol. 18, p. 065008, June 2016. 23

[44] W. Wang, K. Tamaki, and M. Curty, "Finite-key security analysis for quantum key distribution with leaky sources," *New J. Phys.*, vol. 20, p. 083027, Aug. 2018. 23

[45] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A*, vol. 90, p. 052314, Nov. 2014. 24, 27

[46] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources," *New J. Phys.*, vol. 17, p. 093011, Sept. 2015. 25, 28

[47] G. Currás-Lorenzo, A. Navarrete, M. Pereira, and K. Tamaki, "Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory," *Phys. Rev. A*, vol. 104, p. 012406, Jul 2021. 25, 28, 29

[48] M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," *npj Quantum Inf.*, vol. 5, pp. 1–12, July 2019. 25

[49] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, "Quantum key distribution with correlated sources," *Sci. Adv.*, vol. 6, p. eaaz4487, Sept. 2020. 25

[50] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemp. Phys.*, vol. 57, pp. 366–387, July 2016. 25

[51] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, p. 25002, 2020. 25, 27

[52] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar. 2012. 26

[53] S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, Mar. 2012. 26

[54] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics*, vol. 8, pp. 595–604, Aug. 2014. 27

[55] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nat. Photonics*, vol. 7, pp. 210–214, Mar. 2013. 27

[56] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou,

X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, p. 190501, Nov. 2016. 27

[57] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, "Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw," *Phys. Rev. A*, vol. 85, p. 042307, Apr. 2012. 27

[58] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 062319, Dec. 2012. 27

[59] H. Chernoff, "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations," *Ann. Math. Stat.*, vol. 23, pp. 493–507, Dec. 1952. 28

[60] K. Azuma, "Weighted sums of certain dependent random variables," *Tohoku Math. J.*, vol. 19, pp. 357–367, Jan. 1967. 28

[61] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A*, vol. 89, p. 022307, Feb. 2014. 28

[62] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A*, vol. 95, p. 012333, Jan. 2017. 28

[63] X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 052305, Nov. 2012. 28

[64] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature Communications*, vol. 5, p. 3732, Apr. 2014. 28

[65] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, pp. 163–168, Mar. 2015. 29

[66] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, p. 15043, Apr. 2017. 29

[67] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar. 2011. 29, 31

[68] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413–418, Nov. 2001.

[69] M. Razavi and J. H. Shapiro, "Long-distance quantum communication with neutral atoms," *Phys. Rev. A*, vol. 73, p. 042303, Apr. 2006. 31

[70] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 16, p. 043005, Apr. 2014. 31, 33

[71] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Phys. Rev. A*, vol. 89, p. 012301, Jan. 2014. 31, 33

[72] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, pp. 60–64, Apr. 2020. 32

[73] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nat. Photonics*, vol. 10, pp. 312–315, May 2016. 33

[74] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nat. Commun.*, vol. 6, p. 6787, Apr. 2015. 33

[75] R. Trényi, K. Azuma, and M. Curty, "Beating the repeaterless bound with adaptive measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 21, p. 113052, Nov. 2019. 33

[76] G. Currás-Lorenzo and M. Razavi, "Finite-key analysis for memory-assisted decoy-state quantum key distribution," *New J. Phys.*, vol. 22, p. 103005, Oct. 2020. 33

[77] N. Lo Piparo, N. Sinclair, and M. Razavi, "Memory-assisted quantum key distribution resilient against multiple-excitation effects," *Quantum Sci. Technol.*, vol. 3, p. 014009, Dec. 2017. 33

[78] N. Lo Piparo, M. Razavi, and W. J. Munro, "Memory-assisted quantum key distribution with a single nitrogen-vacancy center," *Phys. Rev. A*, vol. 96, p. 052313, Nov. 2017. 33

[79] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, May 2018. 34, 36

[80] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound," *arXiv preprint arXiv:1805.05511*, Sept. 2018. 34

[81] X. Ma, P. Zeng, and H. Zhou, "Phase-Matching Quantum Key Distribution," *Phys. Rev. X*, vol. 8, p. 031043, Aug. 2018. 34

[82] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A*, vol. 98, p. 062323, Dec. 2018.

[83] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Inf.*, vol. 5, pp. 1–6, July 2019. 35, 36, 37, 38, 39

[84] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-Field Quantum Key Distribution without Phase Postselection," *Phys. Rev. Applied*, vol. 11, p. 034053, Mar. 2019. 34, 37

[85] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nat. Photonics*, vol. 13, pp. 334–338, May 2019. 34

[86] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System," *Phys. Rev. X*, vol. 9, p. 021046, June 2019.

[87] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending," *Phys. Rev. Lett.*, vol. 123, p. 100505, Sept. 2019.

[88] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 123, p. 100506, Sept. 2019. 34

[89] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nat. Photonics*, vol. 14, pp. 422–425, July 2020. 34

[90] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, p. 070501, Feb. 2020. 34

[91] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, "600 km repeater-like quantum communications with dual-band stabilisation," *arXiv preprint arXiv:2012.15099*, Dec. 2020. 34

[92] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, "Tight finite-key security for twin-field quantum key distribution," *npj Quantum Inf.*, vol. 7, pp. 1–9, Feb. 2021. 37, 38

Chapter 2

Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory

2.1 Abstract

The core of security proofs of quantum key distribution (QKD) is the estimation of a parameter that determines the amount of privacy amplification that the users need to apply in order to distill a secret key. To estimate this parameter using the observed data, one needs to apply concentration inequalities, such as random sampling theory or Azuma's inequality. The latter can be straightforwardly employed in a wider class of QKD protocols, including those that do not rely on basis independent sources, such as the loss-tolerant (LT) protocol. However, when applied to real-life finite-length QKD experiments, Azuma's inequality typically results in substantially lower secret-key rates. Here, we propose an alternative security analysis of the LT protocol against general attacks, for both its prepare-and-measure and measurement-device-independent versions, that is based on random sampling theory. Consequently, our security proof provides considerably higher secret-key rates than the previous finite-key analysis based on Azuma's inequality. This work opens up the possibility of using random sampling theory to provide alternative security proofs for other QKD protocols.

2.2 Introduction

Quantum key distribution (QKD) allows two distant users, Alice and Bob, to generate a shared secret key in the presence of an eavesdropper, Eve, with unbounded computational power [1, 2]. To prove the security of QKD, we often consider the error rate that Alice and Bob would have obtained in a fictitious scenario, known as the phase-error rate, which directly bounds the amount of sifted-key information that could have leaked to Eve, and determines the amount of privacy amplification that the users need to apply to distill a secret key [3–6]. Since Alice and Bob cannot directly observe the phase-error rate, they must estimate it using the data collected in the test rounds, i.e. the detected rounds which are not used to generate the sifted key. For this estimation, it is indispensable to employ statistical techniques. For example, in the case of the BB84 protocol [7] without source flaws, one can use the fact that Alice's source is basis independent to estimate the Z-basis phase-error rate from the X-basis bit-error rate, and vice-versa, using random sampling theory [8, 9]. In protocols where the user sources are basis dependent, the detection statistics of a particular round may depend on the basis choices made in previous rounds, and Azuma's inequality [10] has been typically applied to deal with this dependency [11–14]. However, recently, Maeda *et al.* [15] have successfully applied a non-trivial security analysis based on random sampling theory to a twin-field QKD variant in which the users do not employ a basis independent source. This work raises the obvious question of whether random sampling theory could also be applied to other protocols that do not use a basis independent source, and whose security proofs currently rely on Azuma's inequality. Since the estimation of Eve's side information is the core of QKD security proofs, investigating the possibility of using different estimation techniques deepens our understanding of QKD protocols and their security. Moreover, it has important experimental implications, in terms of the secret-key rate obtainable, since concentration bounds for *independent* random variables, such as the Chernoff bound, are typically tighter than those for *dependent* random variables, such as Azuma's inequality.

One obvious candidate to investigate is the loss-tolerant (LT) protocol [12], a three state protocol that is resistant to state preparation flaws (SPFs), which arise from the finite precision of modulation devices. Earlier attempts to address SPFs [16] resulted in a performance that degraded very quickly with moderate-to-high channel losses.

Conversely, even in the presence of large SPFs and high losses, the performance of the LT protocol is close to that of a perfect four-state BB84 protocol, at least in the limit of infinitely-long keys [12]. Recent works [17–19] have shown that one can prove the security of the LT protocol in the presence of additional source imperfections, such as mode dependencies, Trojan horse attacks or pulse correlations, as long as one can ensure that their magnitude is sufficiently small. Also, the LT protocol can be combined with measurement-device-independent (MDI) QKD [20] to guarantee the security in the presence of arbitrarily flawed detectors. Moreover, the LT protocol is highly practical and can be implemented with off-the-shelf devices. In fact, several experiments have implemented the LT protocol [21, 22], and a variation of it [23] set a fibre QKD distance record. For these reasons, a deep understanding of its security is of theoretical and practical interest.

Clearly, in the LT protocol, Alice's source is not basis independent. For starters, in its standard three-state formulation, Alice only emits one of the two X-basis states. However, even if one were to apply the LT idea to a four-state protocol, the source would still be basis dependent, due to the SPFs. Thus, Azuma's inequality has been used in both the asymptotic [12] and finite-key [13] security proofs of the LT protocol. In the asymptotic regime, the specific statistical technique employed does not affect the performance, since the deviation terms vanish in the limit of infinitely-long keys. However, choosing the tightest statistical technique available does have an impact on the key rate obtainable in (existing and future) real-life finite-length implementations of the LT protocol.

In this paper, we show how the finite-key security of the LT protocol against general attacks can be reduced to a random sampling problem, for both its original prepare-and-measure (P&M) version and its MDI version. This random sampling problem can be solved using concentration inequalities for sums of independent random variables, which results in tighter bounds than those of a previous analysis [13] based on Azuma's inequality. Our paper is structured as follows. In Section 2.3, we present our general statistical analysis, inspired by that of Ref. [15], and apply it to a generic scenario. In Section 2.4, we show how this analysis can be used to estimate the phase-error rate of the P&M LT protocol, and in Section 2.5, we do the same for the MDI LT protocol. In Section 2.6, we give an expression for the secret-key rate obtainable in both protocols. In Section 2.7, we simulate the secret-key rate obtainable for different values of the

block size, and compare it with that of alternative analyses. Finally, in Section 2.8, we conclude our paper.

2.3 General statistical analysis

In this section, we present our general estimation procedure and apply it to a generic scenario, which we denote as the Tagged Virtual Protocol (TVP). Its name refers to the fact that, as we will see in Sections 2.4 and 2.5, one can draw an equivalence between the TVP and the virtual protocols of both LT P&M QKD and LT MDI QKD, once the users probabilistically assign tags to their emissions.

In the TVP, the users emit, amongst others, the states ρ_{vir}, ρ_{pos} and ρ_{neg}, with probabilities p_{vir}, p_{pos} and p_{neg}. These may be states sent by Alice, in the P&M protocol, or joint states sent by Alice and Bob, in the MDI protocol. Also, ρ_{vir} is one of the virtual states, emitted only in the virtual protocol, while ρ_{pos} and ρ_{neg} are actual states, emitted also in the actual protocol. These states satisfy

$$\rho_{\text{vir}} = c_{\text{pos}}\rho_{\text{pos}} - c_{\text{neg}}\rho_{\text{neg}} \tag{2.1}$$

where c_{pos} and c_{neg} are some non-negative coefficients such that $c_{\text{pos}} - c_{\text{neg}} = 1$. For reasons that will become clear later on, we assume that the users assign a tag of $t \in \{\text{vir}, \text{pos}, \text{neg}\}$ to each emission of ρ_t. That is, each emission of ρ_{vir} is trivially assigned a tag $t = \text{vir}$, and so on. In the quantum communication phase of the protocol, some of these emissions will be detected. Here, a "detection" refers to any process that depends on Eve's attack and distinguishes some emissions from others. For the P&M protocol, we will define a detection as an event in which Bob obtained a particular measurement result, and for the MDI protocol, as an event in which Charlie reports a projection to a particular Bell state. We denote by N_t the number of detected emissions with a tag of t, i.e., the number of detected emissions of ρ_t. In the actual protocol, the outcome of the random variables N_{pos} and N_{neg} can be directly observed by the users, but the outcome of N_{vir} cannot, and must be estimated. Thus, the objective of the analysis is to find a statistical relationship between N_{vir}, N_{pos} and N_{neg}; more specifically, we want to find a function f such that $\Pr[N_{\text{vir}} > f(N_{\text{pos}}, N_{\text{neg}}; \varepsilon)] \leq \varepsilon$, where ε can be made arbitrarily small.

The starting point of the analysis is Eq. (2.1), which we now rewrite as

$$\rho_{\text{pos}} = p_{\rho_{\text{vir}}|\text{pos}}\rho_{\text{vir}} + p_{\rho_{\text{neg}}|\text{pos}}\rho_{\text{neg}}, \tag{2.2}$$

where $p_{\rho_{\text{vir}}|\text{pos}} = 1/c_{\text{pos}}$ and $p_{\rho_{\text{neg}}|\text{pos}} = c_{\text{neg}}/c_{\text{pos}}$. Equation (2.2) implies that sending ρ_{pos} is equivalent to sending ρ_{vir} with probability $p_{\rho_{\text{vir}}|\text{pos}}$ and ρ_{neg} with probability $p_{\rho_{\text{neg}}|\text{pos}}$. That is, the TVP is indistinguishable from the following scenario:

- The users select tag $t \in \{\text{vir}, \text{pos}, \text{neg}\}$ with probability p_t.
- If $t = \text{pos}$, the users emit ρ_{vir} with probability $p_{\rho_{\text{vir}}|\text{pos}}$, or ρ_{neg} with probability $p_{\rho_{\text{neg}}|\text{pos}}$.
- If $t \in \{\text{vir}, \text{neg}\}$, the users emit ρ_t.

In the above scenario, some emissions of ρ_{vir} will have a tag of "vir", and some will have a tag of "pos", but they are otherwise identical. The same is true for emissions of ρ_{neg} with tags of "neg" and "pos". Thus, one can go even further, and think of another equivalent scenario in which the users first decide the quantum state that they emit, and then probabilistically assign a tag to it. Namely:

Modified scenario

- The users select and emit the state $\rho_x \in \{\rho_{\text{vir}}, \rho_{\text{neg}}\}$ with probability $\tilde{p}_{\rho_x} := p_x + p_{\text{pos}}p_{\rho_x|\text{pos}}$.
- Next, they assign their emission the tag $t = x$ with probability $\tilde{p}_{x|\rho_x} := p_x/\tilde{p}_{\rho_x}$, or the tag $t = \text{pos}$ with probability $\tilde{p}_{\text{pos}|\rho_x} := 1 - \tilde{p}_{x|\rho_x}$.

This modified scenario is equivalent to the TVP in terms of tags, because:

1. The overall probability to assign a particular tag $t \in \{\text{vir}, \text{pos}, \text{neg}\}$ is the same in both scenarios, i.e. p_t.

2. The quantum state emitted given a particular tag t is the same in both scenarios, i.e. ρ_t.

In the modified scenario, let $\tilde{N}_t^{\rho_x}$ be the number of detected emissions of ρ_x with a tag of t, $\tilde{N}^{\rho_x} = \sum_t \tilde{N}_t^{\rho_x}$ be the total number of detected emissions of ρ_x, and $\tilde{N}_t = \sum_x \tilde{N}_t^{\rho_x}$ be the total number of detected emissions with a tag of t. That is, $\tilde{N}_{\text{vir}} = \tilde{N}_{\text{vir}}^{\rho_{\text{vir}}}$,

$\tilde{N}_{\text{pos}} = \tilde{N}_{\text{pos}}^{\rho_{\text{vir}}} + \tilde{N}_{\text{pos}}^{\rho_{\text{neg}}}$, and $\tilde{N}_{\text{neg}} = \tilde{N}_{\text{neg}}^{\rho_{\text{neg}}}$. The equivalence above implies that, for any attack by Eve, the set of random variables $\{N_{\text{vir}}, N_{\text{pos}}, N_{\text{neg}}\}$ in the TVP has an identical distribution as the set $\{\tilde{N}_{\text{vir}}, \tilde{N}_{\text{pos}}, \tilde{N}_{\text{neg}}\}$ in the modified scenario. Hence, if we find a function f such that $\Pr\left[\tilde{N}_{\text{vir}} > f(\tilde{N}_{\text{pos}}, \tilde{N}_{\text{neg}}; \varepsilon)\right] \leq \varepsilon$ in an execution of the modified scenario, then it must also be the case that $\Pr\left[N_{\text{vir}} > f(N_{\text{pos}}, N_{\text{neg}}; \varepsilon)\right] \leq \varepsilon$ in an execution of the TVP. The equivalence between the two scenarios is shown in Fig. 2.1.

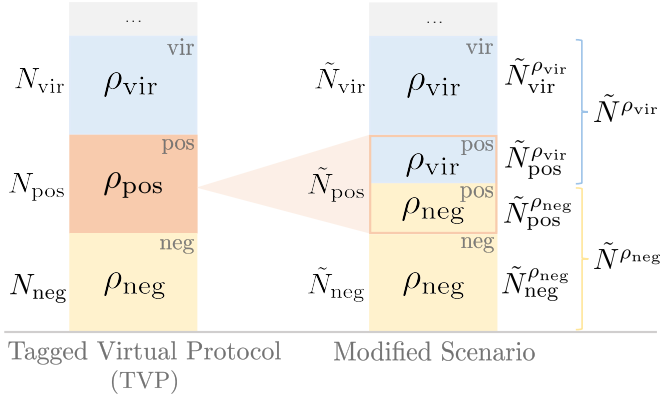


Figure 2.1: Relationship between the Tagged Virtual Protocol (TVP) and the modified scenario. In the modified scenario, each emission of ρ_{vir} (ρ_{neg}) is assigned a tag of either "vir" ("neg") or "pos" with a fixed probability, in such a way that emissions with a tag of $t \in \{\text{vir}, \text{neg}, \text{pos}\}$ are equivalent to emissions of ρ_t in the TVP. In the modified scenario, the detection statistics of each emission must be independent of the tag assigned to it, since Eve does not have any tag information. Hence, each of the $\tilde{N}^{\rho_{\text{vir}}}$ ($\tilde{N}^{\rho_{\text{neg}}}$) detected emissions of ρ_{vir} (ρ_{neg}) is assigned a tag of either "vir" ("neg") or "pos" with the *a priori* fixed probability. This allows us to find a statistical relationship between the random variables $\tilde{N}_{\text{vir}} := \tilde{N}_{\text{vir}}^{\rho_{\text{vir}}}$, $\tilde{N}_{\text{pos}} := \tilde{N}_{\text{pos}}^{\rho_{\text{vir}}} + \tilde{N}_{\text{pos}}^{\rho_{\text{neg}}}$ and $\tilde{N}_{\text{neg}} := \tilde{N}_{\text{neg}}^{\rho_{\text{neg}}}$ using a random sampling analysis, see Eq. (2.5). Since the TVP is equivalent to the modified scenario, the same relationship must hold for the random variables N_{vir}, N_{pos} and N_{neg} in the TVP, see Eq. (2.6).

The random tag assignments in the modified scenario allow us to find a bound on $\tilde{N}_{\text{vir}}$ by using a random sampling analysis. The key idea is that the probability to assign a particular tag to a particular emission must be independent of whether the emission is detected or not, since the tag assignment does not change the emitted quantum state, and Eve does not have any tag information. Thus, each of the $\tilde{N}^{\rho_{\text{vir}}}$ detected emissions of ρ_{vir} is assigned a random tag of "vir" or "pos" with probabilities

$\tilde{p}_{\text{vir}|\rho_{\text{vir}}}$ and $\tilde{p}_{\text{pos}|\rho_{\text{vir}}} = 1 - \tilde{p}_{\text{vir}|\rho_{\text{vir}}}$, respectively. This implies that $\tilde{N}_{\text{vir}}^{\rho_{\text{vir}}}$ is a random sample of a population of $\tilde{N}^{\rho_{\text{vir}}} = \tilde{N}_{\text{vir}}^{\rho_{\text{vir}}} + \tilde{N}_{\text{pos}}^{\rho_{\text{vir}}}$ elements, where each item is sampled with probability $\tilde{p}_{\text{vir}|\rho_{\text{vir}}}$. In Appendix A, we show that this implies that, except with probability $\varepsilon/2$,

$$\tilde{N}_{\text{vir}}^{\rho_{\text{vir}}} \leq g_U \left(\tilde{N}_{\text{pos}}^{\rho_{\text{vir}}}, \tilde{p}_{\text{vir}|\rho_{\text{vir}}}, \varepsilon/2 \right), \tag{2.3}$$

where g_U is defined in Eq. (2.38). Similarly $\tilde{N}_{\text{pos}}^{\rho_{\text{neg}}}$ is the size of a random sample of a population of $\tilde{N}^{\rho_{\text{neg}}} = \tilde{N}_{\text{pos}}^{\rho_{\text{neg}}} + \tilde{N}_{\text{neg}}^{\rho_{\text{neg}}}$ elements, where each item is sampled with probability $\tilde{p}_{\text{pos}|\rho_{\text{neg}}}$. This implies that, except with probability $\varepsilon/2$,

$$\tilde{N}_{\text{pos}}^{\rho_{\text{neg}}} \geq g_L \left(\tilde{N}_{\text{neg}}, \tilde{p}_{\text{pos}|\rho_{\text{neg}}}, \varepsilon/2 \right), \tag{2.4}$$

where g_L is defined in Eq. (2.38).

Using the relations $\tilde{N}_{\text{vir}} = \tilde{N}_{\text{vir}}^{\rho_{\text{vir}}}$, $\tilde{N}_{\text{pos}} = \tilde{N}_{\text{pos}}^{\rho_{\text{vir}}} + \tilde{N}_{\text{pos}}^{\rho_{\text{neg}}}$, and $\tilde{N}_{\text{neg}} = \tilde{N}_{\text{neg}}^{\rho_{\text{neg}}}$, in combination with Eqs. (2.3) and (2.4), we have that

$$\begin{aligned} \tilde{N}_{\text{vir}} &\leq g_U \left(\tilde{N}_{\text{pos}} - \tilde{N}_{\text{pos}}^{\rho_{\text{neg}}}, \tilde{p}_{\text{vir}|\rho_{\text{vir}}}, \varepsilon/2 \right) \\ &\leq g_U \left(\tilde{N}_{\text{pos}} - g_L \left(\tilde{N}_{\text{neg}}, \tilde{p}_{\text{pos}|\rho_{\text{neg}}}, \varepsilon/2 \right), \tilde{p}_{\text{vir}|\rho_{\text{vir}}}, \varepsilon/2 \right), \end{aligned} \tag{2.5}$$

except with probability ε, where in the first inequality we have used Eq. (2.3), and in the second inequality we have used Eq. (2.4) and the fact that g_U is an increasing function with respect to its first argument.

As explained above, the random variables $\{N_{\text{vir}}, N_{\text{pos}}, N_{\text{neg}}\}$ in the TVP are identically distributed as the random variables $\{\tilde{N}_{\text{vir}}, \tilde{N}_{\text{pos}}, \tilde{N}_{\text{neg}}\}$ in the modified scenario. Thus, Eq. (2.5) implies that, in the virtual protocol

$$N_{\text{vir}} \leq g_U \left(N_{\text{pos}} - g_L \left(N_{\text{neg}}, \tilde{p}_{\text{pos}|\rho_{\text{neg}}}, \varepsilon/2 \right), \tilde{p}_{\text{vir}|\rho_{\text{vir}}}, \varepsilon/2 \right) := f(N_{\text{pos}}, N_{\text{neg}}; \varepsilon), \tag{2.6}$$

except with probability ε, as required. Since N_{pos} and N_{neg} are observables of the actual protocol, Alice and Bob can use their observed values to obtain an upper bound on N_{vir}.

In Sections 2.4 and 2.5, we explain how to apply this statistical analysis to the LT protocol, for both its P&M and MDI versions. In this protocol, the virtual states and the actual states are all in the same qubit space. Because of this, each virtual state can be expressed as an operator-form linear function of the actual states. However, this linear function does not necessarily have one positive term and one negative term, as in

Eq. (2.1). To apply the analysis above, the users will first probabilistically assign tags of "pos" and "neg" to some of their emissions, in such a way that the average state with a tag of $t \in \{\text{pos}, \text{neg}\}$ is ρ_t. After these tag assignments, the resulting *tagged* virtual protocol will be equivalent to the TVP, shown on the left side of Fig. 2.1.

2.4 Prepare-and-measure protocol

In this section, we apply our analysis to the P&M LT protocol [12]. For each round, Alice sends Bob a pure state $|\psi_j\rangle_a$ with probability p_j, $j \in \{0_Z, 1_Z, 0_X\}$, where emissions of $|\psi_{0_X}\rangle_a$ ($|\psi_{0_Z}\rangle_a$ and $|\psi_{1_Z}\rangle_a$) are considered to belong to the X (Z) basis. The only assumption needed to apply our analysis is that Alice's states are characterised and linearly dependent, i.e. they are all in the same qubit space. For simplicity, in this discussion we assume that the states are in the XZ plane of the Bloch sphere; in Section 2.B, we show how to apply our results in the general case. Bob measures the incoming signals in the Z or in the X basis, with probabilities p_{Z_B} and p_{X_B}, respectively. We do not need to assume that Bob's measurement bases are mutually unbiased, but we do assume that his choice of basis is fully random, and that the detection efficiency is the same for both bases. Afterwards, Bob reveals which rounds were detected, and both users reveal their basis choice in those rounds. The sifted key is generated from the detected events in which Alice and Bob both chose the Z basis. The detected rounds in which Bob chose the X basis are considered to be test rounds. In these, Bob will reveal his measurement result. The full protocol description is given in Section 2.C.

The objective of the security analysis is to estimate the number of phase errors in the sifted key, using the test data. To define this quantity, we consider an equivalent entanglement-based virtual protocol, in which Alice replaces the key emissions by the generation of the entangled state

$$|\Psi_Z\rangle_{Aa} = \frac{1}{\sqrt{2}}\big(\,|0_Z\rangle_A\,|\psi_{0_Z}\rangle_a + |1_Z\rangle_A\,|\psi_{1_Z}\rangle_a\,\big), \tag{2.7}$$

where a is the photonic system sent to Bob and A is Alice's fictitious qubit ancilla, which she keeps in her lab. For simplicity, in Eq. (2.7), we have assumed that $p_{0_Z} = p_{1_Z}$. The key generated in the actual protocol is equivalent to the key that Alice and Bob would obtain by performing a Z-basis measurement on the systems A and a of the detected rounds in which Alice generated $|\Psi_Z\rangle_{Aa}$. The number of phase errors is defined as the

number of errors that Alice and Bob would have observed if they had measured these systems A and a in the X basis instead. This is equivalent to a scenario in which, in the key rounds, Alice sends Bob the virtual states

$$|\psi_{\mathrm{vir}_\alpha}\rangle_a = \frac{|\psi_{0_Z}\rangle_a + (-1)^\alpha |\psi_{1z}\rangle_a}{\sqrt{2(1-(-1)^\alpha \langle\psi_{0_Z}|\psi_{1_Z}\rangle_a)}}, \tag{2.8}$$

with probabilities

$$p_{\mathrm{vir}_\alpha} = \frac{1}{2} p_{Z_A}(1-(-1)^\alpha \langle\psi_{0_Z}|\psi_{1_Z}\rangle_a), \tag{2.9}$$

and Bob measures these states in the X basis. Here, p_{Z_A} is the probability that Alice selects the Z basis, and $\alpha \in \{0,1\}$. Thus, Alice's choice of state in the virtual protocol can be equivalently described by assuming that she fictitiously prepares the entangled state

$$\begin{aligned}|\Psi_{\mathrm{vir}}\rangle_{Sa} =& \sqrt{p_{\mathrm{vir}_0} p_{Z_B}}\,|0\rangle_S\,|\psi_{\mathrm{vir}_0}\rangle_a + \sqrt{p_{\mathrm{vir}_1} p_{Z_B}}\,|1\rangle_S\,|\psi_{\mathrm{vir}_1}\rangle_a + \sqrt{p_{0_Z} p_{X_B}}\,|2\rangle_S\,|\psi_{0_Z}\rangle_a \\ &+ \sqrt{p_{1_Z} p_{X_B}}\,|3\rangle_S\,|\psi_{1_Z}\rangle_a + \sqrt{p_{0_X} p_{X_B}}\,|4\rangle_S\,|\psi_{0_X}\rangle_a + \sqrt{p_{0_X} p_{Z_B}}\,|5\rangle_S\,|\psi_{0_X}\rangle_a\,,\end{aligned} \tag{2.10}$$

and then performs a measurement on system S. Note that S holds information about Alice's and Bob's setting choices. For instance, $|2\rangle_S$ represents the events in which Alice selects the virtual state $|\psi_{0_Z}\rangle_a$ and Bob chooses the X basis. In the right-hand side of Eq. (2.10), the first two terms are associated with virtual events. That is, the events in which Alice and Bob select the Z basis in the actual protocol, but their basis choice is replaced by the X basis in the virtual protocol. All the other terms in Eq. (2.10) correspond to actual events that occur in the actual protocol.

In the virtual protocol that we have just defined, the occurrence of a phase error is defined as an event in which Alice measures system S, obtains the outcome 0 (1), and Bob's X-basis measurement outputs the bit value 1 (0). The measurement statistics associated with these events cannot be directly observed, since the virtual states are never sent in the actual protocol. However, as we show in Section 2.B, one can exploit the fact that the virtual states and the actual states live in the same qubit space to find an operator-form linear relationship between the virtual states and the actual states. Namely,

$$\begin{aligned}\rho_{\mathrm{vir}_0} &= c_{0_Z|\mathrm{vir}_0}\rho_{0_Z} + c_{1_Z|\mathrm{vir}_0}\rho_{1_Z} + c_{0_X|\mathrm{vir}_0}\rho_{0_X}\,, \\ \rho_{\mathrm{vir}_1} &= c_{0_Z|\mathrm{vir}_1}\rho_{0_Z} + c_{1_Z|\mathrm{vir}_1}\rho_{1_Z} + c_{0_X|\mathrm{vir}_1}\rho_{0_X}\,,\end{aligned} \tag{2.11}$$

where $\rho_{\mathrm{vir}_\alpha} \equiv |\psi_{\mathrm{vir}_\alpha}\rangle\langle\psi_{\mathrm{vir}_\alpha}|_a$, $\rho_j \equiv |\psi_j\rangle\langle\psi_j|_a$, and the coefficients $c_{j|\mathrm{vir}_\alpha}$ can be positive, negative or zero depending on the form of the actual states $\{|\psi_j\rangle_a\}$. For example, when there are no SPFs, the emitted states are $|\psi_{0_Z}\rangle_a = |0_Z\rangle_a$, $|\psi_{1_Z}\rangle_a = |1_Z\rangle_a$ and $|\psi_{0_X}\rangle_a = |0_X\rangle_a$; and Eq. (2.11) becomes $\rho_{\mathrm{vir}_0} = \rho_{0_X}$ and $\rho_{\mathrm{vir}_1} = \rho_{0_Z} + \rho_{1_Z} - \rho_{0_X}$. Next, in order to employ the analysis in Section 2.3, we rewrite Eq. (2.11) as

$$\rho_{\mathrm{vir}_0} = c_{\mathrm{pos}_0}\rho_{\mathrm{pos}_0} - c_{\mathrm{neg}_0}\rho_{\mathrm{neg}_0}, \tag{2.12}$$

$$\rho_{\mathrm{vir}_1} = c_{\mathrm{pos}_1}\rho_{\mathrm{pos}_1} - c_{\mathrm{neg}_1}\rho_{\mathrm{neg}_1}, \tag{2.13}$$

where, for $t \in \{\mathrm{pos}, \mathrm{neg}\}$ and $\alpha \in \{0, 1\}$,

$$c_{t_\alpha} = \sum_{j \in \mathcal{S}_{t_\alpha}} |c_{j|\mathrm{vir}_\alpha}|, \tag{2.14}$$

$$\rho_{t_\alpha} = \sum_{j \in \mathcal{S}_{t_\alpha}} p_{j|t_\alpha} |\psi_j\rangle\langle\psi_j|_a . \tag{2.15}$$

In Eq. (2.15), $\mathcal{S}_{\mathrm{pos}_\alpha}$ ($\mathcal{S}_{\mathrm{neg}_\alpha}$) is the set of indices j such that c_j^α is positive (negative), and

$$p_{j|t_\alpha} = \frac{|c_{j|\mathrm{vir}_\alpha}|}{c_{t_\alpha}}. \tag{2.16}$$

Now, each of Eqs. (2.12) and (2.13) is identical to Eq. (2.1), the starting point of the statistical fluctuation analysis introduced in Section 2.3. We will apply this analysis to estimate the detection statistics of each virtual state, separately. Recall that, in the TVP defined in Section 2.3, the states sent are ρ_{vir}, ρ_{pos} and ρ_{neg} (see Fig. 2.1). However, in the virtual protocol defined above, Alice does not emit the states ρ_{pos_0}, ρ_{pos_1}, ρ_{neg_0} and ρ_{neg_1}. Instead, Alice will probabilistically assign tags of $t_0 \in \{\mathrm{pos}_0, \mathrm{neg}_0\}$ and $t_1 \in \{\mathrm{pos}_1, \mathrm{neg}_1\}$ to some of her emissions, in such a way that the average state with a tag of t_0 (t_1) is ρ_{t_0} (ρ_{t_1}). After doing so, we can draw an equivalence between the virtual protocol and the TVP.

More concretely, let us consider the events in which Alice emits $|\psi_j\rangle_a$, $j \in \{0_Z, 1_Z, 0_X\}$, and Bob chooses the X basis, corresponding to measuring system S of Eq. (2.10) in 2, 3 or 4. Each of these events occurs with probability $p_{j,X_B} = p_j p_{X_B}$, and is assigned a tag of $t_\alpha \in \{\mathrm{pos}_\alpha, \mathrm{neg}_\alpha\}$ with probability

$$p_{t_\alpha|j,X_B} = \frac{p_{t_\alpha} p_{j|t_\alpha}}{p_j p_{X_B}}, \tag{2.17}$$

or a tag of $t_\alpha = \text{junk}_\alpha$ otherwise; where $\alpha \in \{0,1\}$, $p_{j|t_\alpha}$ is given by Eq. (2.16), and p_{t_α} is the total probability of assigning tag t_α. Note that the assignment of tag t_0 and of tag t_1 is done independently: each of these emissions will have both a tag of t_0 and a tag of t_1. This is allowed because our key idea relies only on a probabilistic assignment of a tag, and even if multiple assignments are made for a single pulse, the argument still holds. In Eq. (2.17), the conditional probabilities $p_{t_\alpha|j,X_B}$ become fixed once one chooses the value of p_{t_α}, which must be such that $p_{t_\alpha} \leq p_j p_{X_B}/p_{j|t_\alpha}$ for all $j \in \{0_Z, 1_Z, 0_X\}$, since $p_{t_\alpha|j,X_B} \leq 1$. In order to waste as few test rounds as possible, and thus obtain a tight estimate of the number of phase errors, we assume that Alice chooses the largest possible value of p_{t_α}, given by

$$p_{t_\alpha} = \min_j \frac{p_j p_{X_B}}{p_{j|t_\alpha}}. \tag{2.18}$$

Moreover, in the virtual protocol, Alice assigns a deterministic tag of $t_0 = \text{vir}_0$ ($t_1 = \text{vir}_1$) to each emission of $|\psi_{\text{vir}_0}\rangle_a$ ($|\psi_{\text{vir}_1}\rangle_a$), corresponding to $S = 0$ ($S = 1$).

After these tag assignments, an emission with a tag of t_α is equivalent to an emission of ρ_{t_α}. Thus, if Alice disregards the outcome of her measurement of system S, and considers only the tags of t_α that she assigns, the virtual protocol becomes equivalent to a scenario in which Alice actually emits ρ_{t_α} with probability p_{t_α}, and then trivially assigns her emission a tag of t_α. This scenario, which we denote as the the Tagged Virtual Protocol α and depict on the right side of Fig. 2.2, is identical to the TVP defined in Section 2.3 and shown on the left side of Fig. 2.1.

Let $N_{t_0}^{1_X}$ ($N_{t_1}^{0_X}$) be the number of detected events with a tag of t_0 (t_1) in which Bob obtained measurement result 1_X (0_X). Equation (2.6) of Section 2.3 implies that, in the Tagged Virtual Protocol 0, it holds that, except with probability $\varepsilon/2$,

$$N_{\text{vir}0}^{1_X} \leq g_U\left(N_{\text{pos}0}^{1_X} - g_L\left(N_{\text{neg}0}^{1_X}, \tilde{p}_{\text{pos}0|\rho_{\text{neg}0}}, \varepsilon/4\right), \tilde{p}_{\text{vir}0|\rho_{\text{vir}0}}, \varepsilon/4\right), \tag{2.19}$$

and in the Tagged Virtual Protocol 1, it holds that, except with probability $\varepsilon/2$,

$$N_{\text{vir}1}^{0_X} \leq g_U\left(N_{\text{pos}1}^{0_X} - g_L\left(N_{\text{neg}1}^{0_X}, \tilde{p}_{\text{pos}1|\rho_{\text{neg}1}}, \varepsilon/4\right), \tilde{p}_{\text{vir}1|\rho_{\text{vir}1}}, \varepsilon/4\right), \tag{2.20}$$

where, for $\alpha \in \{0,1\}$, $\tilde{p}_{\text{vir}\alpha|\rho_{\text{vir}\alpha}} = p_{\text{vir}\alpha}/(p_{\text{vir}\alpha} + p_{\text{pos}\alpha}/c_{\text{pos}\alpha})$ and $\tilde{p}_{\text{pos}\alpha|\rho_{\text{neg}\alpha}} = 1 - p_{\text{neg}\alpha}/(p_{\text{neg}\alpha} + p_{\text{pos}\alpha}c_{\text{neg}\alpha}/c_{\text{pos}\alpha})$. Moreover, since the virtual protocol is equivalent to the Tagged Virtual Protocol 0 (1), in terms of the assigned tags of t_0 (t_1), Eq. (2.19)

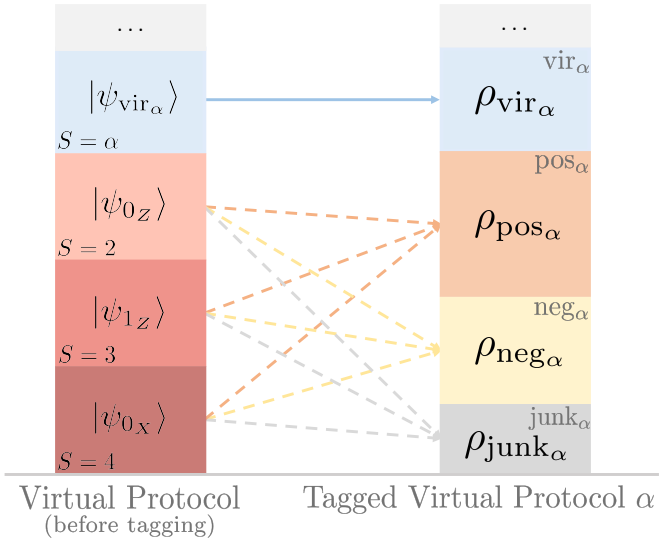


Figure 2.2: Relation between the virtual protocol and the Tagged Virtual Protocol α, where $\alpha \in \{0,1\}$, for the P&M scheme. In the virtual protocol, events for which $S \in \{2,3,4\}$ are probabilistically assigned a tag of $t_\alpha \in \{\mathrm{pos}_\alpha, \mathrm{neg}_\alpha, \mathrm{junk}_\alpha\}$ (dashed arrows), in such a way that the average state with a tag of t_α is ρ_{t_α}. Events for which $S = \alpha$ are deterministically assigned a tag of $t_\alpha = \mathrm{vir}_\alpha$ (solid arrow). If one considers only the tags of t_α that Alice has assigned, the virtual protocol becomes equivalent to the Tagged Virtual Protocol α. The ellipses at the top of the diagram represent events which are identical in both scenarios, but which are not relevant for the analysis.

(Eq. (2.20)) must also hold for the virtual protocol. Thus, combining Eqs. (2.19) and (2.20), we have that, in the virtual protocol, the number of phase errors $N_{\mathrm{ph}} := N^{1X}_{\mathrm{vir0}} + N^{0X}_{\mathrm{vir1}}$ satisfies

$$\begin{aligned} N_{\mathrm{ph}} \leq\ & g_U\left(N^{1X}_{\mathrm{pos0}} - g_L\left(N^{1X}_{\mathrm{neg0}}, \tilde{p}_{\mathrm{pos0}|\rho_{\mathrm{neg0}}}, \varepsilon/4\right), \tilde{p}_{\mathrm{vir0}|\rho_{\mathrm{vir0}}}, \varepsilon/4\right) \\ & + g_U\left(N^{0X}_{\mathrm{pos1}} - g_L\left(N^{0X}_{\mathrm{neg1}}, \tilde{p}_{\mathrm{pos1}|\rho_{\mathrm{neg1}}}, \varepsilon/4\right), \tilde{p}_{\mathrm{vir1}|\rho_{\mathrm{vir1}}}, \varepsilon/4\right), \end{aligned} \tag{2.21}$$

except with probability ε.

In order to use Eq. (2.21) to prove the security, the quantities $N^{1X}_{t_0}$ and $N^{0X}_{t_1}$, for $\alpha \in \{0,1\}$ and $t_\alpha \in \{\mathrm{pos}_\alpha, \mathrm{neg}_\alpha\}$, must be observables in an actual implementation of the protocol. Thus, the probabilistic tag assignments defined in Eq. (2.17) must happen in the actual protocol too. However, note the following: (1) the tag assigned to a particular emission must be independent of Bob's measurement result, since the tag assignment does not change the emitted quantum state; and (2) the assignment of tag

t_α is only relevant for the analysis if Bob happens to obtain a measurement outcome of $(\alpha\oplus 1)_X$ in that round. This implies that it is only necessary for Alice to probabilistically assign a tag of t_0 (t_1) to the events in which she sent $|\psi_j\rangle_a$, $j \in \{0_Z, 1_Z, 0_X\}$, and Bob obtained measurement result 1_X (0_X). For a full description of the protocol, including the tagging step, see Section 2.C.

2.5 Measurement-device-independent protocol

In this section, we apply our analysis to the LT MDI QKD protocol. For each round, Alice (Bob) selects the state $|\psi_j\rangle_a$ ($|\psi'_s\rangle_b$) with probability p_j (p'_s), where j (s) $\in \{0, 1, \tau\}$, and sends it to an untrusted middle node Charlie. As in the P&M case, the only assumption required to apply our analysis is that all states emitted by Alice (Bob) are in the same qubit space. For simplicity, in this discussion we assume that all states lie in the XZ plane of the Bloch sphere; in Appendix D, we show how to treat the case in which they do not. Emissions for which $j \in \{0, 1\}$ ($s \in \{0, 1\}$) are considered to belong to the Z basis, and for simplicity their selection probability is assumed to be equal, i.e. $p_0 = p_1 = p_Z/2$ ($p'_0 = p'_1 = p'_Z/2$). We denote Alice and Bob's joint state by $|\psi_{j,s}\rangle_{ab} \equiv |\psi_j\rangle_a \otimes |\psi'_s\rangle_b$, and its associated probability by $p_{j,s} \equiv p_j p'_s$.

Alice and Bob expect Charlie to perform a Bell state measurement on each incoming joint pulse, and announce the result. In most MDI protocols, including the original MDI QKD proposal [20], Charlie may obtain a projection to one of two Bell states. However, for simplicity, for now we assume that Charlie attempts to obtain a projection to only one of the four Bell states, and that if he is successful (unsuccessful), he reports the round as "detected" ("undetected"). At the end of the section, we show how to generalise the analysis to the case in which Charlie may report a projection to two or more different Bell states. Also, note that Charlie is untrusted, and may even be fully controlled by Eve. Thus, in what follows, we directly assume that it is Eve who performs the measurements and announces the results. Importantly, Eve is not limited to measuring each round independently: if she performs a coherent attack, her full set of announcements may depend on an arbitrary general measurement acting jointly on the photonic systems of all the rounds in the protocol.

After Eve's announcements, Alice and Bob reveal, for each round, whether or not they used the Z basis, thus learning whether or not $(j, s) \in \mathcal{Z} :=$

$\{(0,0),(0,1),(1,0),(1,1)\}$. The rounds for which $(j,s) \notin \mathcal{Z}$ are automatically considered to belong to the set of test emissions, which we denote as $\mathcal{T}$. The rounds for which $(j,s) \in \mathcal{Z}$ receive a special treatment: with probability $p_{\mathcal{K}|\mathcal{Z}}$ they are considered key emissions, and with probability $p_{\mathcal{T}|\mathcal{Z}}$ they are considered test emissions, where $\mathcal{K}$ is the set of key emissions, and $p_{\mathcal{K}|\mathcal{Z}} + p_{\mathcal{T}|\mathcal{Z}} = 1$. This is needed because we want to use data from some $\mathcal{Z}$-rounds to estimate the phase-error rate. The resulting scenario is shown on the left-hand side of Fig. 2.3. For all rounds in $\mathcal{T}$, Alice and Bob reveal their choice of (j,s).

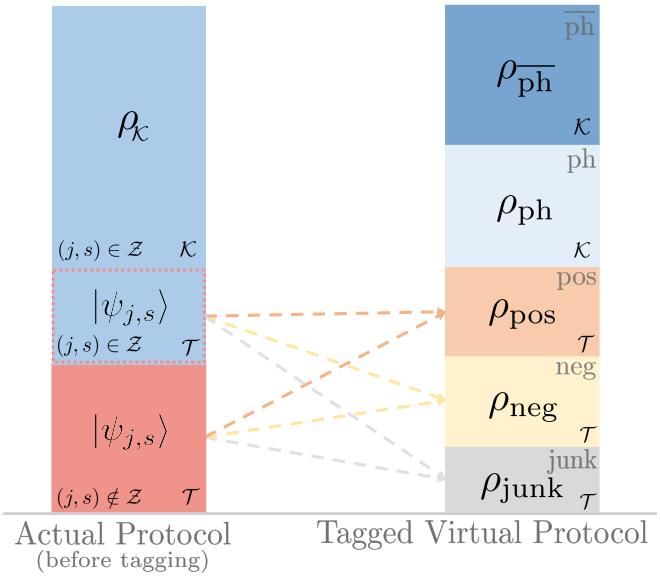


Figure 2.3: Relationship between the actual protocol and the Tagged Virtual Protocol in the MDI scenario. In the actual protocol, shown on the left, emissions such that $(j,s) \in \mathcal{Z}$ are probabilistically assigned to either $\mathcal{K}$ or $\mathcal{T}$, while emissions such that $(j,s) \notin \mathcal{Z}$ are always assigned to $\mathcal{T}$. In both the actual and virtual protocols, events in $\mathcal{T}$ are probabilistically assigned a tag of $t \in \{\text{pos}, \text{neg}, \text{junk}\}$, in such a way that the average state with a tag of t is ρ_t. The dashed arrows represent this tagging process. In the virtual protocol, $\mathcal{K}$-emissions are substituted by emissions of ρ_{ph} and $\rho_{\overline{\text{ph}}}$, and are assigned tags of "ph" and "$\overline{\text{ph}}$", respectively. If Alice and Bob consider only the tags that they have assigned, the virtual protocol becomes equivalent to the *tagged* virtual protocol, shown on the right.

Alice (Bob) defines her (his) sifted key as her (his) choices of j (s) in the detected rounds in $\mathcal{K}$. The objective of the analysis is to use the detection statistics of the

$\mathcal{T}$-rounds to estimate the number of phase errors in their sifted keys. This quantity is defined as the number of errors that Alice and Bob would have obtained if they had run a virtual scenario in which they replaced the $\mathcal{K}$-emissions by the generation of the virtual state $|\Psi_{\mathcal{K}}\rangle = \frac{1}{2}\sum_{j,s=0,1} |j_Z, s_Z\rangle_{AB} |\psi_{j,s}\rangle_{ab}$, followed by an X-basis measurement on their local ancillas A and B. Let Π_{AB}^{ph} be the projector onto the phase-error subspace in AB. Note that the definition of a phase error depends on the particular Bell state onto which Charlie is supposed to project the incoming pulses. The average state of a key emission may be written as

$$\rho_{\mathcal{K}} = \frac{1}{4}\sum_{j,s=0,1} |\psi_{j,s}\rangle\langle\psi_{j,s}|_{ab} = p_{\text{ph}|\mathcal{K}}\rho_{\text{ph}} + p_{\overline{\text{ph}}|\mathcal{K}}\rho_{\overline{\text{ph}}}, \tag{2.22}$$

where ρ_{ph} and $\rho_{\overline{\text{ph}}}$ are quantum states such that $p_{\text{ph}|\mathcal{K}}\rho_{\text{ph}} = \text{Tr}_{AB}[\Pi_{AB}^{\text{ph}} |\Psi_{\mathcal{K}}\rangle\langle\Psi_{\mathcal{K}}|]$ and $p_{\overline{\text{ph}}|\mathcal{K}}\rho_{\overline{\text{ph}}} = \text{Tr}_{AB}[(\mathbb{I} - \Pi_{AB}^{\text{ph}}) |\Psi_{\mathcal{K}}\rangle\langle\Psi_{\mathcal{K}}|]$. Thus, the virtual protocol may be regarded as the following scenario: the users jointly select $\mathcal{K}$ or $\mathcal{T}$ with probabilities $p_{\mathcal{K}} = p_{\mathcal{Z}}p_{\mathcal{K}|\mathcal{Z}}$ and $p_{\mathcal{T}} = 1 - p_{\mathcal{K}}$, respectively, and

- If they select $\mathcal{K}$, they emit ρ_{ph} and $\rho_{\overline{\text{ph}}}$ with probabilities $p_{\text{ph}|\mathcal{K}}$ and $p_{\overline{\text{ph}}|\mathcal{K}}$, respectively.
- If they select $\mathcal{T}$, they emit $|\psi_{j,s}\rangle_{ab}$ with probability $p_{j,s|\mathcal{T}} = p_{j,s}p_{\mathcal{T}|j,s}/p_{\mathcal{T}}$, where $p_{\mathcal{T}|j,s} = p_{\mathcal{T}|\mathcal{Z}}$ if $(j,s) \in \mathcal{Z}$ and $p_{\mathcal{T}|j,s} = 1$ if $(j,s) \notin \mathcal{Z}$.

The number of phase errors, N_{ph}, is defined as the number of detected emissions of ρ_{ph} that Alice and Bob would have observed if they had run this virtual protocol. To estimate this quantity, we use again the random sampling analysis of Section 2.3. To apply this analysis, however, we need to first show that ρ_{ph} can be written in the form of Eq. (2.1), i.e.,

$$\rho_{\text{ph}} = c_{\text{pos}}\rho_{\text{pos}} - c_{\text{neg}}\rho_{\text{neg}}, \tag{2.23}$$

and then add a tagging step to the protocol, so that it becomes equivalent to a scenario in which the states ρ_{pos} and ρ_{neg} are actually emitted. In Section 2.B, we show that ρ_{ph} can be expressed as an operator-form linear function of the actual states, that is

$$\rho_{\text{ph}} = \sum_{j,s} c_{j,s}\rho_{j,s}, \tag{2.24}$$

where $\rho_{j,s} \equiv |\psi_{j,s}\rangle\langle\psi_{j,s}|_{ab}$ and the coefficients $c_{j,s}$ are real and can be negative. Thus, if we denote by $\mathcal{S}_{\text{pos}}$ ($\mathcal{S}_{\text{neg}}$) the set of pairs (j,s) such that $c_{j,s}$ is positive (negative), and, for $t \in \{\text{pos}, \text{neg}\}$, we set

$$c_t = \sum_{j,s\in\mathcal{S}_t} |c_{j,s}|, \tag{2.25}$$

$$\rho_t = \sum_{j,s\in\mathcal{S}_t} p_{j,s|t}\rho_{j,s}, \tag{2.26}$$

where

$$p_{j,s|t} := \begin{cases} |c_{j,s}|/c_t & \text{if } (j,s) \in \mathcal{S}_t, \\ 0 & \text{otherwise,} \end{cases} \tag{2.27}$$

we obtain Eq. (2.23).

In the tagging step, Alice and Bob need to probabilistically assign tags of "pos" and "neg" to their emissions in $\mathcal{T}$, in such a way that the average state with a tag of t is ρ_t. To achieve this, in the actual protocol, Alice and Bob must assign a tag of $t \in \{\text{pos}, \text{neg}\}$ to each emission of $|\psi_{j,s}\rangle_{ab}$ in $\mathcal{T}$ with probability

$$p_{t|j,s,\mathcal{T}} = \frac{p_{t|\mathcal{T}} p_{j,s|t}}{p_{j,s|\mathcal{T}}}, \tag{2.28}$$

where $p_{j,s|t}$ is given by Eq. (2.27), and $p_{t|\mathcal{T}}$ is the probability that a round in $\mathcal{T}$ is assigned a tag of t. Note that the assignment probabilities $p_{t|j,s,\mathcal{T}}$ become fixed once one chooses $p_{t|\mathcal{T}}$. From Eq. (2.28), it follows that the value of $p_{t|\mathcal{T}}$ must be such that $p_{t|\mathcal{T}} \leq p_{j,s|\mathcal{T}}/p_{j,s|t}$, $\forall (j,s) \in \mathcal{S}_t$. Hence, its maximum possible value is

$$p_{t|\mathcal{T}} = \min_{j,s\in\mathcal{S}_t} \frac{p_{j,s|\mathcal{T}}}{p_{j,s|t}}, \tag{2.29}$$

and we assume that Alice and Bob choose this value, in order to waste as few $\mathcal{T}$-rounds as possible and thus obtain a tight estimate of the phase-error rate. Finally, Alice and Bob assign the tag "junk" to all the remaining rounds in $\mathcal{T}$ that have not been tagged as "pos" or "neg".

Since $\mathcal{T}$-emissions are identical in the actual and virtual protocols, the previous tag assignments can be regarded as taking place in both protocols. Besides, let us further assume that, in the virtual protocol, Alice and Bob assign trivial tags of "ph" and "$\overline{\text{ph}}$" to each emission of ρ_{ph} and $\rho_{\overline{\text{ph}}}$, respectively. Then, if Alice and Bob disregard their choice of state, and consider only the tags that they have assigned, the resulting *tagged* virtual protocol becomes equivalent to the scenario depicted in the right-hand side of

Fig. 2.3, in which Alice and Bob emit ρ_t, $t \in \{\text{ph}, \overline{\text{ph}}, \text{pos}, \text{neg}, \text{junk}\}$, with probability p_t; where $p_t = p_{\mathcal{K}} p_{t|\mathcal{K}}$ for $t \in \{\text{ph}, \overline{\text{ph}}\}$, and $p_t = p_{\mathcal{T}} p_{t|\mathcal{T}}$ for $t \in \{\text{pos}, \text{neg}, \text{junk}\}$. This scenario is identical to the starting point of the random sampling analysis in Section 2.3, the TVP shown on the left side of Fig. 2.1. The only differences are that here we have denoted the virtual state of interest as ρ_{ph}, not ρ_{vir}; and that we have some extra emissions of $\rho_{\overline{\text{ph}}}$ and ρ_{junk}, which we simply ignore in the analysis. Using Eq. (2.6), we have that, except with probability ε, the number of phase errors N_{ph} satisfies

$$N_{\text{ph}} \leq g_U \left(N_{\text{pos}} - g_L\Big(N_{\text{neg}}, \tilde{p}_{\text{pos}|\rho_{\text{neg}}}, \varepsilon/2\Big), \tilde{p}_{\text{ph}|\rho_{\text{ph}}}, \varepsilon/2 \right), \tag{2.30}$$

where N_t is the number of detected events with a tag of t, $\tilde{p}_{\text{ph}|\rho_{\text{ph}}} = p_{\text{ph}}/(p_{\text{ph}} + p_{\text{pos}}/c_{\text{pos}})$ and $\tilde{p}_{\text{pos}|\rho_{\text{neg}}} = 1 - p_{\text{neg}}/(p_{\text{neg}} + p_{\text{pos}} c_{\text{neg}}/c_{\text{pos}})$.

In the analysis above, we have assumed that Alice and Bob reveal their choice of basis for all rounds, and then probabilistically assign all events such that $(j, s) \in \mathcal{Z}$ to either $\mathcal{T}$ or $\mathcal{K}$ with probabilities $p_{\mathcal{T}|\mathcal{Z}}$ and $p_{\mathcal{K}|\mathcal{Z}}$. However, note the following: (1) the probability to assign a particular emission to $\mathcal{T}$ or $\mathcal{K}$ must be independent of whether or not it is detected, since Eve has no information about this assignment when she makes her announcements; and (2) the set assigned to the undetected rounds is irrelevant, since their data is not used at any point in the analysis. This implies that it is only necessary for Alice and Bob to reveal their choice of basis in the detected rounds, and then assign each detected event such that $(j, s) \in \mathcal{Z}$ to either $\mathcal{T}_{\text{d}}$ or $\mathcal{K}_{\text{d}}$ with probabilities $p_{\mathcal{T}|\mathcal{Z}}$ and $p_{\mathcal{K}|\mathcal{Z}}$, respectively, where $\mathcal{T}_{\text{d}}$ ($\mathcal{K}_{\text{d}}$) is the set of detected test (key) rounds. By a similar argument, we conclude that Alice and Bob only need to reveal their choice of (j, s) for the emissions in $\mathcal{T}_{\text{d}}$, and then assign each of them a tag of $t \in \{\text{pos}, \text{neg}\}$ with probability $p_{t|j,s,\mathcal{T}}$. For a full description of the protocol, including these assignments, see Section 2.D.

Case in which Charlie reports several projections

The analysis above can be easily generalised to the case in which Charlie may report a projection to two or more Bell states. Essentially, the procedure is simply repeated separately for each successful projection announcement Ω. Note that, because the definition of a phase error depends on Ω, so does the operator associated with a phase error, which we now denote as ρ_{ph_Ω}. By repeating the procedure in Eqs. (2.23) to (2.27), we define the operators ρ_{pos_Ω} and ρ_{neg_Ω}, and the coefficients c_{pos_Ω} and c_{neg_Ω}, for

each Ω. Then, we imagine that, for all Ω, Alice and Bob assign a tag $t_\Omega \in \{\text{pos}_\Omega, \text{neg}_\Omega\}$ to each emission in $\mathcal{T}$ with probability $p_{t_\Omega|j,s,\mathcal{T}}$, defined similarly to Eq. (2.29), in such a way that the average state with a tag of t_Ω is ρ_{t_Ω}. In the virtual protocol, we also imagine that Alice and Bob assign a tag $t_\Omega = \text{ph}_\Omega$ to each emission of ρ_{ph_Ω}. Then, if Alice and Bob look only at the assigned tag of t_Ω, the scenario becomes equivalent to the "Tagged Virtual Protocol Ω", in which Alice and Bob emit ρ_{t_Ω} with probability p_{t_Ω}. Let N_{t_Ω} be the number of events with a tag of t_Ω in which Charlie announced Ω. Applying the results of Section 2.3 to the "Tagged Virtual Protocol Ω", we have that, except with probability ε_Ω,

$$N_{\text{ph}_\Omega} \leq g_U\left(N_{\text{pos}_\Omega} - g_L\left(N_{\text{neg}_\Omega}, \tilde{p}_{\text{pos}_\Omega|\rho_{\text{neg}_\Omega}}, \varepsilon_\Omega/2\right), \tilde{p}_{\text{ph}_\Omega|\rho_{\text{ph}_\Omega}}, \varepsilon_\Omega/2\right) := N^{\text{U}}_{\text{ph}_\Omega}, \tag{2.31}$$

and because of the equivalence between the "Tagged Virtual Protocol Ω" and the virtual protocol, Eq. (2.31) must also hold for the latter, for all Ω. Thus, the total number of phase errors is upper bounded by

$$N_{\text{ph}} \leq \sum_\Omega N^{\text{U}}_{\text{ph}_\Omega}, \tag{2.32}$$

except with probability $\varepsilon = \sum_\Omega \varepsilon_\Omega$. By a similar argument as in the main analysis above, we deduce that, in the actual protocol: (1) Alice and Bob only need to reveal their choice of basis in the detected rounds, and then assign each detected event such that $(j,s) \in \mathcal{Z}$ to either $\mathcal{T}_\text{d}$ or $\mathcal{K}_\text{d}$ with probabilities $p_{\mathcal{T}|\mathcal{Z}}$ and $p_{\mathcal{K}|\mathcal{Z}}$, respectively, where $\mathcal{T}_\text{d}$ ($\mathcal{K}_\text{d}$) is the set of detected test (key) rounds; and (2) Alice and Bob only need to reveal their choice of (j,s) for the emissions in $\mathcal{T}_\text{d}$, and then assign each of them a tag of $t_\Omega \in \{\text{pos}_\Omega, \text{neg}_\Omega\}$ with probability $p_{t_\Omega|j,s,\mathcal{T}}$, where Ω is Charlie's announcement on that round.

2.6 Secret-key rate and security parameter

In Sections 2.4 and 2.5, we have shown how to obtain an upper bound N^{U}_{ph} on the number of phase errors N_{ph} such that

$$\Pr\left[N^{\text{U}}_{\text{ph}} > N_{\text{ph}}\right] \leq \varepsilon. \tag{2.33}$$

After calculating this bound, Alice and Bob perform error correction, error verification, and privacy amplification. They obtain a secret key of length

$$K = N_{\mathrm{s}}(1 - h(N_{\mathrm{ph}}/N_{\mathrm{s}})) - \lambda_{\mathrm{EC}} - \log_2 \frac{1}{\epsilon_{\mathrm{c}}} - \log_2 \frac{1}{\xi}, \tag{2.34}$$

where N_{s} is the length of the sifted key, λ_{EC} is the number of bits revealed in the error correction step, and ϵ_{c} is the probability that Alice and Bob's keys will not be identical after the error verification step. It is known [5, 15] that, if the number of phase errors is bounded as in Eq. (2.33) and the secret-key length is set as in Eq. (2.34), then the protocol is ϵ_{s}-secret, with $\epsilon_s = \sqrt{2}\sqrt{\varepsilon + \xi}$. Since the protocol is also ϵ_{c}-correct, then it is ϵ_{sec}-secure, with $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{c}} + \epsilon_{\mathrm{s}}$.

2.7 Numerical results

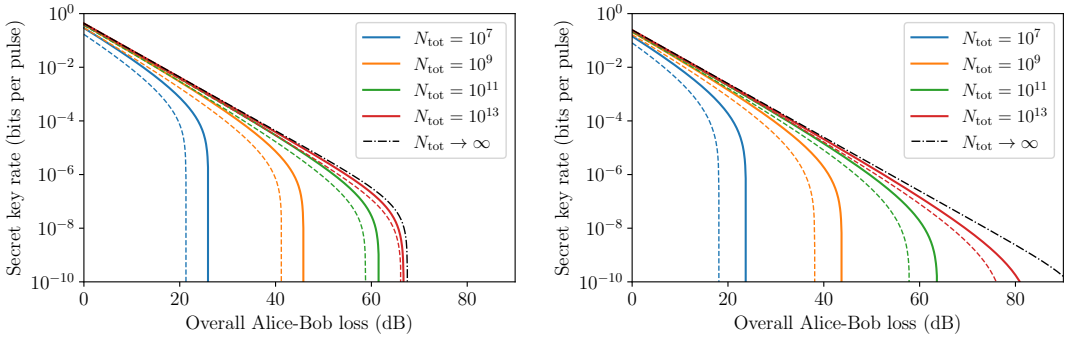
In this section, we simulate the secret key obtainable for both the P&M and MDI LT protocols, using the analysis introduced in the previous sections. As usual, we assume the nominal scenario in which no eavesdropper is present. Moreover, we assume that the users' sources emit three different imperfectly-encoded single-photon states in the form

$$|\psi_j\rangle = \cos(\theta_j)\,|0_Z\rangle + \sin(\theta_j)\,|1_Z\rangle\,, \tag{2.35}$$

where $\{|0_Z\rangle, |1_Z\rangle\}$ forms a qubit basis, and $\theta_j \in [0, 2\pi)$ is the encoded phase. For the P&M scheme, we assume that Alice's states satisfy $\theta_{0Z} = 0$, $\theta_{1Z} = \kappa\pi/2$, and $\theta_{0X} = \kappa\pi/4$, where $\kappa = 1 + \delta/\pi$ and δ quantifies the magnitude of the SPFs. For the MDI setup, we assume that Alice's and Bob's states satisfy $\theta_0 = \theta'_0 = 0$, $\theta_1 = \theta'_1 = \kappa\pi/2$, $\theta_\tau = \kappa\pi/4$ and $\theta'_\tau = -\kappa\pi/4$, where θ_j (θ'_s) denotes the angle of Alice's (Bob's) state when she (he) emits state j (s).

To simulate the data that would be obtained in an experiment, we use the channel model in Ref. [17] for the P&M protocol, and the channel model in Section 2.E for the MDI protocol. For simplicity, in the latter we assume that Charlie only announces a detection if he obtains a projection to the Bell state Ψ^-. The experimental parameters considered are: SPF's parameter $\delta = 0.126$, error correction inefficiency $f = 1.16$, dark count probability of the detectors $p_d = 10^{-8}$ and fiber loss coefficient $\alpha = 0.2$ dB/km. Moreover, we select the correctness and secrecy parameters to be $\epsilon_c = 10^{-8}$

and $\epsilon_s = 10^{-8}$, respectively, and for simplicity we set $\xi = \varepsilon$ in Eq. (2.34), which means that $\varepsilon = \epsilon_s^2/4$. In our simulations, we optimise over Alice and Bob's basis selection probabilities, and in the MDI protocol, we also optimise over the value of $p_{\mathcal{T}|\mathcal{Z}}$. Also, we consider different values of the block size N_{tot}, which represents the total number of rounds in the protocol. Finally, we assume an error-correction leakage of $\lambda_{\text{EC}} = fh(e_Z)$ bits, where e_Z is the bit-error rate of the sifted key. The results for the P&M and the MDI LT protocols are shown in Fig. 2.4(a) and Fig. 2.4(b), respectively.



(a) P&M Protocol

(b) MDI Protocol

Figure 2.4: Secret-key rate obtainable using our analysis based on random sampling theory (solid lines), for the P&M (a) and MDI (b) LT protocols, as a function of the overall channel loss and for different values of the block size N_{tot}. For comparison, we include the secret-key rate obtainable using an alternative analysis based on Azuma's inequality (dashed lines), similar to that of Ref. [13]. For both LT protocols, our analysis clearly outperforms the alternative analysis based on Azuma's inequality.

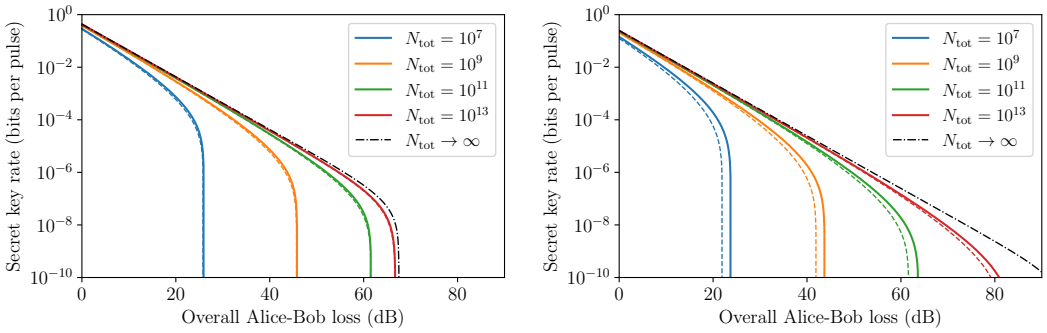
For completeness, we compare our results with those of an alternative analysis based on the application of Azuma's inequality. This alternative analysis, presented in Section 2.F, is essentially a simplified version of the security proof in Ref. [13], which considers the emission of weak coherent pulses rather than single photons. The results in Fig. 2.4 show that our analysis based on random sampling offers significantly higher performances for both the P&M and MDI LT protocols. The difference in performance is larger for lower values of N_{tot}, while as N_{tot} increases, the two analyses slowly converge. In the case $N_{\text{tot}} \to \infty$, both analyses provide a perfect estimation of the phase-error rate, and thus offer the same secret-key rate.

We note that a novel concentration inequality for sums of dependent random variables has been recently uploaded to a preprint server by Kato [24]. This result can be regarded as an improved version of Azuma's inequality that is much tighter when the success probability of the random variables is low. In Section 2.F, we give a statement of the result, and use it to substitute Azuma's inequality in the alternative finite-key analysis of the LT protocol. However, it must be said that, when applied to QKD protocols, Kato's inequality requires an extra condition that is not needed in either our analysis based on random sampling or analyses based on Azuma's inequality. Namely, it requires users to attempt to predict the results that they expect to obtain in the experiment, before they actually run the experiment. This is an important step, since the inequality is only tight when the actual experimental data was reasonable close to their predictions [25].

In Fig. 2.5, we compare the performance of our analysis based on random sampling theory with that of our alternative analysis based on Kato's inequality. For simplicity, in the alternative analysis, we assume that the users could perfectly predict the experimental data that they obtain in the experiment, which maximises the secret-key rate obtainable. Fig. 2.5(a) shows that, in the case of the P&M protocol, the difference between the two analyses vanishes almost completely. Conversely, Fig. 2.5(b) shows that, in the case of the MDI protocol, our analysis based on random sampling still retains an advantage, although significantly smaller than that observed in Fig. 2.4(b). We emphasise that, unlike the alternative analysis based on Kato's inequality, our analysis based on random sampling does not require the users to make any prediction before running the experiment.

2.8 Discussion

In this work, we have proved the finite-key security of the loss-tolerant (LT) QKD protocol against general attacks, for both its prepare-and-measure and measurement-device-independent versions. Our security analysis reduces the parameter estimation task to a classical random sampling problem, which can be solved using Chernoff bounds, and provides higher secret-key rates than previous results based on the application of Azuma's inequality [13].



(a) P&M Protocol

(b) MDI Protocol

Figure 2.5: Comparison between the secret-key rate obtainable using our random sampling analysis (solid lines) and our alternative analysis based on the application of a novel concentration inequality for dependent random variables (dashed lines), for both the P&M (a) and MDI (b) versions of the LT protocol and different values of the block size $N_{\rm tot}$. For the P&M protocol, the performance of the two security proofs is almost identical, while for the MDI protocol, our analysis based on random sampling provides slightly better secret-key rates.

Although we have assumed single-photon sources, we believe that our analysis can be extended to the case in which the users employ weak coherent sources, as long as the single-photon components of the three encoded pulses satisfy the requirements of our proof, i.e. they are characterised and belong to the same qubit space. In that case, the users should assign tags to their emissions in such a way that Eq. (2.1) holds for their single-photon components; i.e. $\rho^{(1)}_{\rm vir} = c_{\rm pos}\rho^{(1)}_{\rm pos} - c_{\rm neg}\rho^{(1)}_{\rm neg}$, where $\rho^{(1)}_t$ is the average quantum state of a single-photon pulse with a tag of t. If so, Eq. (2.6) holds, although it now has the form $N^{(1)}_{\rm vir} \leq f(N^{(1)}_{\rm pos}, N^{(1)}_{\rm neg}; \varepsilon)$, where $N^{(1)}_t$ denotes the number of detected single-photon pulses with a tag of t. Note that now $N^{(1)}_{\rm pos}$ and $N^{(1)}_{\rm neg}$ are not directly observable, since the users do not know the photon number of their emissions. However, by using different laser intensities μ, they are able to observe the values $\{N^{\mu}_{\rm pos}\}$ and $\{N^{\mu}_{\rm neg}\}$ for all μ, where N^{μ}_t is the number of detected emissions with a tag of t that originated from intensity μ. Thus, they can apply the decoy-state method [26–29] to obtain an upper (lower) bound on $N^{(1)}_{\rm pos}$ ($N^{(1)}_{\rm neg}$), using for example the numerical techniques introduced in Ref. [30].

Also, in our random sampling analysis, we have assumed that the three encoded

states live in the same qubit space. In a future work, it would be interesting to consider if our security proof can be extended to the case in which the qubit assumption is not satisfied, due to additional imperfections such as mode dependencies [17] or correlations between different rounds of the protocol [18, 19]. In that case, one can no longer derive an operator equality between the virtual and the actual states, such as e.g. Eq. (2.11). Instead, one needs to find an operator dominance condition [15] between them, which is non-trivial if the side-channel states are not characterised, as assumed by Refs. [17–19].

Acknowledgements

We thank Mohsen Razavi and Marcos Curty for valuable discussions. G.C.-L. and M.P. acknowledge support from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement number 675662 (project QCALL). A.N. acknowledges support from a FPU scholarship (FPU 15/03668) from the Spanish Ministry of Science, Innovation and Universities (MCIU). K.T. acknowledges support from JSPS KAKENHI Grant Numbers JP18H05237 18H05237 and JST-CREST JPMJCR 1671. All data generated can be reproduced by the equations and the methodology introduced in this paper.

2.A Random sampling analysis

Here, we prove the statements in Eqs. (2.3) and (2.4), and give an expression for the functions g_L and g_U. Let us assume that we have a population of n items, where n is unknown. Each item is assigned to either $\mathcal{K}_1$ with probability p or to $\mathcal{K}_2$ with probability $1-p$. We know the value of $K_2 = |\mathcal{K}_2|$ and we would like to obtain bounds on $K_1 = |\mathcal{K}_1|$.

Let $\xi_i = 1$ if the i-th trial is assigned to $\mathcal{K}_2$ and $\xi_i = 0$ otherwise. We have that

$$\sum_{i=1}^{n} \xi_i = K_2. \tag{2.36}$$

Clearly, $\mathbb{E}[K_2] = (1-p)n$, and therefore $n = \mathbb{E}[K_2]/(1-p)$. Using the inverse multiplicative Chernoff bound [25, 31, 32], we have that

$$\begin{aligned} \mathbb{E}[K_2] &\geq -K_2 W_0\left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right) \\ \mathbb{E}[K_2] &\leq -K_2 W_{-1}\left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right) \end{aligned} \tag{2.37}$$

where W_0 and W_{-1} are branches of the Lambert W function, and each of the bounds fails with probability at most ε. From this and the fact that $n = K_1 + K_2$, we have that

$$\begin{aligned} K_1 = n - K_2 = \frac{\mathbb{E}[K_2]}{1-p} - K_2 &\geq \max\left(-\frac{K_2 W_0\left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right)}{1-p} - K_2,\, 0\right) =: g_L(K_2, p, \varepsilon), \\ K_1 = n - K_2 = \frac{\mathbb{E}[K_2]}{1-p} - K_2 &\leq -\frac{K_2 W_{-1}\left(-e^{\frac{\ln\varepsilon - K_2}{K_2}}\right)}{1-p} - K_2 =: g_U(K_2, p, \varepsilon), \end{aligned} \tag{2.38}$$

where each of the bounds fails with probability ε. It can be shown that g_U is an increasing function of K_2. Note that Eq. (2.38) is only valid for $K_2 > 0$. In the special case $K_2 = 0$, we have that [31]

$$\begin{aligned} g_L(0, p, \varepsilon) &:= 0 \\ g_U(0, p, \varepsilon) &:= -\frac{\ln\varepsilon}{1-p}. \end{aligned} \tag{2.39}$$

We note that this random sampling problem can also be solved using the method introduced in Ref. [15].

2.B Operator-form linear relationship between the virtual and actual states

In this Appendix, we show how to find an operator-form linear relationship between the virtual states and the actual states, see Eq. (2.11) and Eq. (2.24). For simplicity, we provide first the procedure for the P&M protocol; then, at the end of this Appendix, we show how to extend it to the MDI case. The only assumption on Alice's emitted states, $|\psi_j\rangle_a$ for $j \in \{0_Z, 1_Z, 0_X\}$, is that they are linearly dependent, i.e. all three states live in the same qubit space. However, the analysis simplifies significantly if they are all in the same standard basis plane of the Bloch sphere, such as the XZ, XY or ZY plane. First, we consider this simpler case, and then provide the analysis for the general case.

2.B.1 Case in which all states are in a standard basis plane

Without loss of generality, we assume that the three states are in the XZ plane of the Bloch sphere, i.e. they can be expressed as

$$|\psi_j\rangle_a = \cos(\theta_j)\,|0_Z\rangle_a + \sin(\theta_j)\,|1_Z\rangle_a\,, \tag{2.40}$$

where $\theta_j = (-\pi, \pi]$. Alice generates her sifted key from the detected emissions of $|\psi_{0_Z}\rangle_a$ and $|\psi_{1_Z}\rangle_a$. To prove the security of the sifted key, we consider an entanglement-based virtual protocol in which Alice prepares the state

$$|\Psi_Z\rangle_{Aa} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_A\,|\psi_{0_Z}\rangle_a + |1_Z\rangle_A\,|\psi_{1_Z}\rangle_a\right). \tag{2.41}$$

In this virtual protocol, Alice measures her local ancilla A in the complementary basis $\{|0_X\rangle_A, |1_X\rangle_A\}$, where $|\alpha_X\rangle_A = 1/\sqrt{2}\,[|0_Z\rangle_A + (-1)^\alpha\,|1_Z\rangle_A]$ for $\alpha \in \{0,1\}$. If Alice obtains $|\alpha_X\rangle_A$, she effectively emits the virtual state

$$|\psi_{\mathrm{vir}_\alpha}\rangle_a = \frac{1}{\sqrt{p_{\mathrm{vir}_\alpha|Z}}}\left(\,|\psi_{0_Z}\rangle_a + (-1)^\alpha\,|\psi_{1_Z}\rangle_a\,\right), \tag{2.42}$$

where $p_{\mathrm{vir}_\alpha|Z} = \left\||\psi_{0_Z}\rangle_a + (-1)^\alpha\,|\psi_{1_Z}\rangle_a\right\|^2/4 = (1+(-1)^\alpha\cos(\theta_{0_Z} - \theta_{1_Z}))/2$ is the probability that Alice obtains $|\alpha_X\rangle_A$. Since $|\psi_{0_Z}\rangle_a$ and $|\psi_{1_Z}\rangle_a$ are in the XZ plane, $|\psi_{\mathrm{vir}_\alpha}\rangle_a$ is also in the XZ plane.

Let $[S_j^Z, S_j^X, S_j^Y]$ be the Bloch vector of the state $|\psi_j\rangle_a$. We have that $S_j^Z = \cos(2\theta_j)$, $S_j^X = \sin(2\theta_j)$ and $S_j^Y = 0$. Thus, in operator form, the state $|\psi_j\rangle_a$ can be

expressed as

$$\rho_j \equiv |\psi_j\rangle\langle\psi_j|_a = \frac{1}{2}\big(\sigma_I + S_j^Z\sigma_Z + S_j^X\sigma_X\big), \tag{2.43}$$

where σ_I is the identity operator and σ_K, for $K \in \{Z, X, Y\}$, is a Pauli operator. It is useful to see Eq. (2.43) as a system of linear equations, with three unknowns (σ_I, σ_Z, σ_X) and three equations (one for each $|\psi_j\rangle_a$). We can write this system in matrix form:

$$\boldsymbol{\rho} = \boldsymbol{S}\boldsymbol{\sigma}, \tag{2.44}$$

where $\boldsymbol{\rho} = [\rho_{0_Z}, \rho_{1_Z}, \rho_{0_X}]^{\mathrm{T}}$, $\boldsymbol{\sigma} = [\sigma_I, \sigma_Z, \sigma_X]^{\mathrm{T}}$, and

$$\boldsymbol{S} := \frac{1}{2}\begin{bmatrix} 1 & S_{0_Z}^Z & S_{0_Z}^X \\ 1 & S_{1_Z}^Z & S_{1_Z}^X \\ 1 & S_{0_X}^Z & S_{0_X}^X \end{bmatrix}; \tag{2.45}$$

and express its solution as

$$\boldsymbol{\sigma} = \boldsymbol{S}^{-1}\boldsymbol{\rho}. \tag{2.46}$$

Equation (2.46) essentially says that the operators σ_I, σ_Z, σ_X can be expressed as a linear combination of the actual states ρ_j. This implies that every state that can be expressed as a linear combination of σ_I, σ_Z, σ_X (i.e., every state in the XZ plane) can also be expressed as a linear combination of ρ_j. In particular, the virtual states $|\psi_{\mathrm{vir}_\alpha}\rangle_a$ are in the XZ plane, and in operator form they can be expressed as

$$\rho_{\mathrm{vir}_\alpha} \equiv |\psi_{\mathrm{vir}_\alpha}\rangle\langle\psi_{\mathrm{vir}_\alpha}|_a = \frac{1}{2}\big(\sigma_I + S_{\mathrm{vir}_\alpha}^Z\sigma_Z + S_{\mathrm{vir}_\alpha}^X\sigma_X\big), \tag{2.47}$$

where $S_{\mathrm{vir}_0}^Z = -S_{\mathrm{vir}_1}^Z = \cos(\theta_{0_Z} + \theta_{1_Z})$ and $S_{\mathrm{vir}_0}^X = -S_{\mathrm{vir}_1}^X = \sin(\theta_{0_Z} + \theta_{1_Z})$. Or equivalently,

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{\sigma}, \tag{2.48}$$

where $\boldsymbol{S}_{\mathrm{vir}_\alpha} = \frac{1}{2}\big[1, S_{\mathrm{vir}_\alpha}^Z, S_{\mathrm{vir}_\alpha}^X\big]^{\mathrm{T}}$. Combining Eqs. (2.46) and (2.48), we have that

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}\boldsymbol{\rho} = \boldsymbol{f}_\alpha\boldsymbol{\rho}, \tag{2.49}$$

where $\boldsymbol{f}_\alpha := \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}$ is a row vector. If we express $\boldsymbol{f}_\alpha$ as $\boldsymbol{f}_\alpha = [c_{0_Z|\alpha}, c_{1_Z|\alpha}, c_{0_X|\alpha}]$, we obtain Eq. (2.11), i.e.

$$\rho_{\mathrm{vir}_\alpha} = c_{0_Z|\mathrm{vir}_\alpha}\rho_{0_Z} + c_{1_Z|\mathrm{vir}_\alpha}\rho_{1_Z} + c_{0_X|\mathrm{vir}_\alpha}\rho_{0_Z}, \tag{2.50}$$

for $\alpha \in \{0, 1\}$, as required.

2.B Operator-form linear relationship between the virtual and actual states

In our numerical simulations, we assume that the three states emitted by Alice are in the XZ plane, and that when written as in Eq. (2.40), their phases satisfy $\theta_{0_Z} = 0$, $\theta_{1_Z} = \kappa\pi/2$ and $\kappa\pi/4$, for some κ. For this particular case, an analytical expression for the coefficients is given by

$$\begin{aligned} c_{0_Z|\mathrm{vir}_0} &= c_{1_Z|\mathrm{vir}_0} = 0, \\ c_{0_X|\mathrm{vir}_0} &= 1, \\ c_{0_Z|\mathrm{vir}_1} &= c_{1_Z|\mathrm{vir}_1} = \csc^2(\kappa\pi/4))/2, \\ c_{0_X|\mathrm{vir}_1} &= -\cot^2(\kappa\pi/4)). \end{aligned}$$

2.B.2 General case

Here, we consider the case in which the three states are not all in the same standard basis plane. Formally, we assume that for all $K \in \{Z, X, Y\}$, there is at least one j such that $S_j^K \neq 0$. Therefore Eq. (2.43) becomes

$$\rho_j \equiv |\psi_j\rangle\langle\psi_j|_a = \frac{1}{2}\big(\sigma_I + S_j^Z\sigma_Z + S_j^X\sigma_X + S_j^Y\sigma_Y\big), \tag{2.51}$$

and now we have a system of three equations with four unknowns. We have to find a way to modify Eq. (2.51) such that it becomes a system with three unknowns.

For any basis $\{|0_U\rangle_a, |1_U\rangle_a\}$ of the qubit space, Alice's emitted states can be expressed as

$$|\psi_j\rangle_a = e^{i\gamma_j}\left(\sqrt{u_j}\,|0_U\rangle_a + e^{i\phi_j}\sqrt{1-u_j}\,|1_U\rangle_a\right). \tag{2.52}$$

where $0 \leq u_j \leq 1$, $\gamma_j \in [0, 2\pi)$, $\phi_j \in [0, 2\pi)$. Since the end points of the three Bloch vectors associated to Alice's emitted states form a plane, there must be a basis U such that u_j has the same value $\forall j$. Expressed in this basis, which we denote as $\tilde{Y}$, the states are

$$|\psi_j\rangle_a = e^{i\gamma_j}\left(\sqrt{\tilde{y}}\,|0_{\tilde{Y}}\rangle_a + e^{i\phi_j}\sqrt{1-\tilde{y}}\,|1_{\tilde{Y}}\rangle_a\right), \tag{2.53}$$

for some $0 \leq \tilde{y} \leq 1$. Let V be a unitary operator such that $V|0_Y\rangle_a = |0_{\tilde{Y}}\rangle_a$ and $V|1_Y\rangle_a = |1_{\tilde{Y}}\rangle_a$. V can be regarded as a transformation from the set of mutually unbiased bases Z, X, Y to the set of mutually unbiased bases $\tilde{Z}$, $\tilde{X}$, $\tilde{Y}$. Let us define the modified Pauli operators $\tilde{\sigma}_K = V\sigma_K V^\dagger$, for $K \in \{Z, X, Y\}$, and express the actual states in terms of these, i.e.

$$\rho_j = \frac{1}{2}\big(\sigma_I + \tilde{S}_Z^j\tilde{\sigma}_Z + \tilde{S}_X^j\tilde{\sigma}_X + \tilde{S}_Y^j\tilde{\sigma}_Y\big). \tag{2.54}$$

2.B Operator-form linear relationship between the virtual and actual states

Note that the three states have the same $\tilde{Y}$ component, i.e. $\tilde{S}_Y^j = \tilde{S}_Y := 2\tilde{y} - 1$, $\forall j$. This allows us to define the operator $\tilde{\sigma}_O = \sigma_I + \tilde{S}_Y \tilde{\sigma}_Y$, and rewrite Eq. (2.54) as

$$|\psi_j\rangle\langle\psi_j|_a = \frac{1}{2}\big(\tilde{\sigma}_O + \tilde{S}_Z^j \tilde{\sigma}_Z + \tilde{S}_X^j \tilde{\sigma}_X\big), \tag{2.55}$$

which has a similar form as Eq. (2.43), i.e. it can be regarded as a linear system of three equations and three unknowns. If we define $\boldsymbol{\rho} = [\rho_{0_Z}, \rho_{1_Z}, \rho_{0_X}]^{\mathrm{T}}$, $\boldsymbol{\sigma} = [\tilde{\sigma}_O, \tilde{\sigma}_Z, \tilde{\sigma}_X]^{\mathrm{T}}$, and

$$\boldsymbol{S} := \frac{1}{2}\begin{bmatrix} 1 & \tilde{S}_{0_Z}^Z & \tilde{S}_{0_Z}^X \\ 1 & \tilde{S}_{1_Z}^Z & \tilde{S}_{1_Z}^X \\ 1 & \tilde{S}_{0_X}^Z & \tilde{S}_{0_X}^X \end{bmatrix}; \tag{2.56}$$

we have that $\boldsymbol{\rho} = \boldsymbol{S}\boldsymbol{\sigma}$, and therefore,

$$\boldsymbol{\sigma} = \boldsymbol{S}^{-1}\boldsymbol{\rho}. \tag{2.57}$$

The previous equation implies that the modified Pauli operators $\tilde{\sigma}_O$, $\tilde{\sigma}_Z$, $\tilde{\sigma}_X$ can be expressed as a linear combination of the actual states ρ_j. Therefore, any state that can be expressed as a linear combination of $\tilde{\sigma}_O$, $\tilde{\sigma}_Z$, $\tilde{\sigma}_X$ (i.e. any state whose $\tilde{Y}$-component is $\tilde{S}_Y$) can also be expressed as a linear combination of the ρ_j.

If we define the virtual states as in Eq. (2.42), it is likely that they will not satisfy the condition that their $\tilde{Y}$-component is $\tilde{S}_Y$. However, note that to obtain Eq. (2.42), we have assumed that Alice measures the ancilla A of the entangled state in Eq. (2.41) in the X basis. In reality, Alice could have decided to measure it in any other basis that is mutually unbiased with Z. Equivalently, we can express this degree of freedom by assuming that Alice does measure in the X basis, but defines the entangled state as

$$|\Psi_Z\rangle_{Aa} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_A |\psi_0\rangle_a + e^{i\phi}|1_Z\rangle_A |\psi_1\rangle_a\right), \tag{2.58}$$

for some $\phi \in [0, 2\pi)$. Thus, the virtual states now become

$$|\psi_{\mathrm{vir}_\alpha}\rangle_a = \frac{1}{\sqrt{p_{\mathrm{vir}_\alpha|Z}}}\big(|\psi_0\rangle_a + (-1)^\alpha e^{i\phi}|\psi_1\rangle_a\big), \tag{2.59}$$

where $p_{\mathrm{vir}_\alpha|Z} = \big\||\psi_0\rangle_a + (-1)^\alpha e^{i\phi}|\psi_1\rangle_a\big\|^2/4$ is the probability that Alice obtains $|\alpha_X\rangle_A$. Substituting Eq. (2.53) in Eq. (2.59), one can easily show that if Alice chooses $\phi = \gamma_{0_Z} - \gamma_{1_Z} + (\phi_{0_Z} - \phi_{1_Z})/2$, then the modified Bloch vector of the virtual state $|\psi_{\mathrm{vir}_\alpha}\rangle_a$, $[\tilde{S}_{\mathrm{vir}_\alpha}^Z, \tilde{S}_{\mathrm{vir}_\alpha}^X, \tilde{S}_Y^{\mathrm{vir}_\alpha}]$, satisfies $\tilde{S}_Y^{\mathrm{vir}_\alpha} = \tilde{S}_Y$ for both $\alpha \in \{0, 1\}$. Therefore

$$\rho_{\mathrm{vir}_\alpha} = \frac{1}{2}\big(\tilde{\sigma}_O + \tilde{S}_{\mathrm{vir}_\alpha}^Z \tilde{\sigma}_Z + \tilde{S}_{\mathrm{vir}_\alpha}^X \tilde{\sigma}_X\big), \tag{2.60}$$

or equivalently,

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{\sigma}, \tag{2.61}$$

where $\boldsymbol{S}_{\mathrm{vir}_\alpha} = \frac{1}{2}\big[1,\, \tilde{S}^Z_{\mathrm{vir}_\alpha},\, \tilde{S}^X_{\mathrm{vir}_\alpha}\big]^{\mathrm{T}}$. Combining Eqs. (2.57) and (2.61), we have that

$$\rho_{\mathrm{vir}_\alpha} = \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}\boldsymbol{\rho} := \boldsymbol{f}_\alpha\boldsymbol{\rho}, \tag{2.62}$$

where $\boldsymbol{f}_\alpha := \boldsymbol{S}_{\mathrm{vir}_\alpha}\boldsymbol{S}^{-1}$ is a row vector. If we express $\boldsymbol{f}_\alpha$ as $\boldsymbol{f}_\alpha = [c_{0_Z|\alpha},\, c_{1_Z|\alpha},\, c_{0_X|\alpha}]$, we obtain Eq. (2.11), i.e.

$$|\psi_{\mathrm{vir}_\alpha}\rangle\langle\psi_{\mathrm{vir}_\alpha}|_a = c_{0_Z|\alpha}\,|\psi_{0_Z}\rangle\langle\psi_{0_Z}|_a + c_{1_Z|\alpha}\,|\psi_{1_Z}\rangle\langle\psi_{1_Z}|_a + c_{0_X|\alpha}\,|\psi_{0_X}\rangle\langle\psi_{0_X}|_a\,, \tag{2.63}$$

for $\alpha \in \{0,1\}$, as required.

2.B.3 MDI protocol

In the MDI scenario, we essentially perform the above procedure separately for Alice's and Bob's states. Let $|\psi_j\rangle_a$ ($|\psi'_s\rangle_b$), with j (s) $\in \{0,1,\tau\}$, denote Alice's (Bob's) states, and let $\rho_j \equiv |\psi_j\rangle\langle\psi_j|$ ($\rho'_s \equiv |\psi'_s\rangle\langle\psi'_s|$) denote their operator form. Using the analysis in the previous sections, we have that

$$\begin{aligned}\rho_{\mathrm{vir}_\alpha} &= c_{0|\mathrm{vir}_\alpha}\rho_0 + c_{1|\mathrm{vir}_\alpha}\rho_1 + c_{0|\mathrm{vir}_\alpha}\rho_\tau,\\ \rho'_{\mathrm{vir}_\beta} &= c'_{0|\mathrm{vir}_\beta}\rho'_0 + c'_{1|\mathrm{vir}_\beta}\rho'_1 + c'_{0|\mathrm{vir}_\beta}\rho'_\tau;\end{aligned} \tag{2.64}$$

where $\alpha,\beta \in \{0,1\}$, and $\rho_{\mathrm{vir}_\alpha}$ ($\rho'_{\mathrm{vir}_\beta}$) denotes one of Alice's (Bob's) virtual states, emitted with probability $p_{\mathrm{vir}_\alpha|\mathcal{K}}$ ($p'_{\mathrm{vir}_\beta|\mathcal{K}}$). We can define Alice and Bob's joint virtual states as

$$\rho_{\mathrm{vir}_{\alpha,\beta}} = \rho_{\mathrm{vir}_\alpha} \otimes \rho'_{\mathrm{vir}_\beta} = \sum_{j,s} c_{j,s|\mathrm{vir}_{\alpha,\beta}}\rho_{j,s}, \tag{2.65}$$

emitted with probability $p_{\mathrm{vir}_{\alpha,\beta}|\mathcal{K}} = p_{\mathrm{vir}_\alpha|\mathcal{K}}p'_{\mathrm{vir}_\alpha|\mathcal{K}}$; where $c_{j,s|\mathrm{vir}_{\alpha,\beta}} = c_{j|\mathrm{vir}_\alpha}c'_{s|\mathrm{vir}_\beta}$. Depending on Charlie's Bell state report, the definition of a phase error will change. If Charlie reports a projection to either Ψ^- or Φ^-, the phase-error operator is defined as

$$\rho_{\mathrm{ph}} = (p_{\mathrm{vir}_{0,0}}\rho_{\mathrm{vir}_{0,0}} + p_{\mathrm{vir}_{1,1}}\rho_{\mathrm{vir}_{1,1}})/p_{\mathrm{ph}}, \tag{2.66}$$

where $p_{\mathrm{ph}} = p_{\mathrm{vir}_{0,0}} + p_{\mathrm{vir}_{1,1}}$. Conversely, if he reports a projection to either Ψ^+ or Φ^+, the phase-error operator is defined as

$$\rho_{\mathrm{ph}} = (p_{\mathrm{vir}_{0,1}}\rho_{\mathrm{vir}_{0,1}} + p_{\mathrm{vir}_{1,0}}\rho_{\mathrm{vir}_{1,0}})/p_{\mathrm{ph}}, \tag{2.67}$$

where $p_{\text{ph}} = p_{\text{vir}_{0,1}} + p_{\text{vir}_{1,0}}$. In any case, one can express the phase-error operator as

$$\rho_{\text{ph}} = \sum_{j,s} c_{j,s}\rho_{j,s}, \tag{2.68}$$

where the coefficients $c_{j,s}$ are a linear function of the coefficients $c_{j,s|\alpha,\beta}$, and can be obtained by substituting Eq. (2.65) in either Eq. (2.66) or Eq. (2.67).

In our numerical simulations we assume that Alice and Bob's states are in the XZ plane, and that when written as in Eq. (2.40), their phases satisfy $\theta_0 = \theta'_0 = 0$, $\theta_1 = \theta'_1 = \kappa\pi/2$, $\theta_\tau = -\theta'_\tau = \kappa\pi/4$. For this particular case, we have that Alice's virtual states satisfy

$$\begin{aligned} c_{0|\text{vir}_0} &= c_{1|\text{vir}_0} = 0, \\ c_{0|\text{vir}_0} &= 1, \\ c_{0|\text{vir}_1} &= c_{1|\text{vir}_1} = \csc^2(\kappa\pi/4))/2, \\ c_{\tau|\text{vir}_1} &= -\cot^2(\kappa\pi/4); \end{aligned} \tag{2.69}$$

while Bob's virtual states satisfy

$$\begin{aligned} c'_{0|\text{vir}_0} &= 1, \\ c'_{1|\text{vir}_0} &= -c'_{\tau|\text{vir}_0} = \frac{1}{1+2\cos(\kappa\pi/2)}, \\ c'_{0|\text{vir}_1} &= -\frac{\cos(\kappa\pi/2)\csc^2(\kappa\pi/4)}{2}, \\ c'_{1|\text{vir}_1} &= \frac{\cos(\kappa/2)\csc(\kappa\pi/4)\csc(3\kappa\pi/4)}{2}, \\ c'_{\tau|\text{vir}_1} &= \frac{\cot^2(\kappa\pi/4)}{1+2\cos(\kappa\pi/2)}. \end{aligned} \tag{2.70}$$

2.C Description of the P&M protocol

(1) *Preparation*

For each round, Alice chooses a pure state $|\psi_j\rangle_a$ with probability p_j, where $j \in \{0_Z, 1_Z, 0_X\}$, and sends it to Bob through the quantum channel. Emissions of $|\psi_{0_X}\rangle_a$ ($|\psi_{0_Z}\rangle_a$ and $|\psi_{1_Z}\rangle_a$) are considered to belong to the X (Z) basis.

(2) *Detection*

Bob measures the incoming signals in either the Z or the X basis, which he chooses with probabilities p_Z and $p_X = 1 - p_Z$, respectively.

(3) *Sifting*

Bob announces which rounds were detected, and Alice and Bob reveal their basis choices in those rounds. Let $\mathcal{K}_Z$ be the set of detected rounds in which both users employed the Z basis, and let $\mathcal{T}_X$ be the set of detected rounds in which Bob employed the X basis. Then,

(3.1) Alice (Bob) defines her (his) sifted key as the bit values associated with her emissions (his measurement results) in the rounds in $\mathcal{K}_Z$.

(3.2) For all rounds in $\mathcal{T}_X$, Bob announces his measurement result.

(4) *Tag assignment*

Alice probabilistically assigns a tag to all rounds in $\mathcal{T}_X$, depending on her choice of state and Bob's measurement result. Namely, if she chose the state $|\psi_j\rangle_a$ and Bob obtained measurement result $(\alpha \oplus 1)_X$, for $\alpha \in \{0,1\}$, she assigns a tag of $t_\alpha \in \{\text{pos}_\alpha, \text{neg}_\alpha\}$ with probability $p_{t_\alpha|j,X_B}$, given by Eq. (2.17). Then, she calculates $N_{t_\alpha}^{(\alpha\oplus 1)_X}$, the number of detected events with a tag of t_α in which Bob obtained measurement result $(\alpha \oplus 1)_X$.

(5) *Parameter estimation*

Alice uses the values of $\{N_{t_\alpha}^{(\alpha\oplus 1)_X}\}$ to obtain an upper bound N_{ph}^{U} on N_{ph}, the number of phase errors in her sifted key, using Eq. (2.21).

(6) *Postprocessing*

(6.1) *Error correction*: Alice sends Bob a pre-fixed amount λ_{EC} of syndrome information bits through an authenticated public channel, which Bob uses to correct errors in his sifted key.

(6.2) *Error verification*: Alice and Bob compute a hash of their error-corrected keys using a random universal hash function, and check whether they are equal. If so, they continue to the next step; otherwise, they abort the protocol.

(6.3) *Privacy amplification:* Alice and Bob extract a secret key pair (S_A, S_B) of length $|S_A| = |S_B| = \ell$ from their error-corrected keys using a random two-universal hash function.

2.D Description of the MDI protocol

(1) *Quantum communication*

For each round, Alice (Bob) selects the state $|\psi_j\rangle_a$ ($|\psi'_s\rangle_b$) with probability p_j (p'_s), where j (s) $\in \{0, 1, \tau\}$, and sends it to an untrusted middle node Charlie, who announces whether or not he obtained a successful projection to a Bell state. Emissions for which $j \in \{0, 1\}$ ($s \in \{0, 1\}$) are considered to belong to the Z basis.

(2) *Sifting*

Alice and Bob announce their basis choices in the detected rounds. Then, they assign all detected rounds in which at least one of them used the X basis to set $\mathcal{T}_{\rm d}$. Also, for each detected round in which both chose the Z basis, they assign it to set $\mathcal{K}_{\rm d}$ with probability $p_{\mathcal{K}|\mathcal{Z}}$, or to set $\mathcal{T}_{\rm d}$ with probability $p_{\mathcal{T}|\mathcal{Z}} = 1 - p_{\mathcal{K}|\mathcal{Z}}$. Then, they announce these assignments, and

(2.1) Alice (Bob) defines her (his) sifted key as her (his) choices of j (s) in the rounds in $\mathcal{K}_{\rm d}$.

(2.2) For all rounds in $\mathcal{T}_{\rm d}$, Alice and Bob announce their choice of j and s.

(3) *Tag assignment*

Alice and Bob assign a tag $t \in \{\text{pos}, \text{neg}\}$ to each round in $\mathcal{T}_{\rm d}$ with probability $p_{t|j,s,\mathcal{T}}$, give by Eq. (2.29). Then, they calculate N_t, the number of detected events with a tag of t.

(4) *Parameter estimation*

Alice and Bob substitute the values of $N_{\rm pos}$ and $N_{\rm neg}$ in Eq. (2.30) to obtain an upper bound $N_{\rm ph}^{\rm U}$ on $N_{\rm ph}$, the number of errors in the sifted key.

(5) *Postprocessing*

(5.1) *Error correction*: Alice sends Bob a pre-fixed amount $\lambda_{\rm EC}$ of syndrome information bits through an authenticated public channel, which Bob uses to correct errors in his sifted key.

(5.2) *Error verification*: Alice and Bob compute a hash of their error-corrected keys using a random universal hash function, and check whether they are equal. If so, they continue to the next step; otherwise, they abort the protocol.

(5.3) *Privacy amplification:* Alice and Bob extract a secret key pair (S_A, S_B) of length $|S_A| = |S_B| = \ell$ from their error-corrected keys using a random two-universal hash function.

2.E Channel model for the MDI protocol

In this Appendix, we present the channel model used in our simulations of the MDI LT protocol, which is based on the single-photon version of the original MDI QKD scheme [20]. Specifically, we assume that Alice and Bob prepare polarised single-photon states in the form of Eq. (2.35), where here $|0_Z\rangle$ and $|1_Z\rangle$ denote the horizontally and vertically polarised single-photon states, respectively. After the preparation, Alice (Bob) sends the transmitted states to the intermediate party Charlie through a lossy quantum channel of transmittance η_A (η_B), who interferes the two incoming signals in a 50:50 beamsplitter, which has on each output port a polarising beamsplitter (PBS) that separates the horizontal and vertical modes. Now, let h_1 and v_1 (h_2 and v_2) be the threshold detectors placed at horizontal and vertical output port of the first (second) PBS, respectively, and let p_d be the dark-count probability of each detector. After the measurement, Charlie announces the Bell state Ψ^+ (Ψ^-) if he observes clicks in h_1 and v_1, or h_2 and v_2 (h_1 and v_2, or h_1 and v_2). Then, it is easy to prove that the conditional probability that Charles announces the Bell state $\Psi^\pm$ given that Alice and Bob selected the states $|\psi_j\rangle_a$ and $|\psi_s\rangle_b$, respectively, is

$$\begin{aligned} \mathrm{P}_{j,s}^{\Psi^\pm} = (1-p_d)^2 \Bigg[& \frac{\eta_A \eta_B}{2} \sin^2(\kappa(\theta_j \pm \theta'_s)) + p_d \frac{\eta_A \eta_B}{2} (1 + \cos(2\kappa\theta_j) \cos\big(2\kappa\theta'_s\big)) \\ & + p_d(1-\eta_A)\eta_B + p_d \eta_A (1-\eta_B) + 2p_d^2(1-\eta_a)(1-\eta_b) \Bigg]. \end{aligned} \tag{2.71}$$

2.F Alternative analysis using concentration inequalities for dependent random variables

In this Appendix, we present an alternative analysis that requires the application of a concentration inequality for sums of dependent Bernoulli random variables. This alternative analysis is a simplified version of that of Ref. [13], which considers the emission of weak coherent pulses rather than single photons. In Ref. [13], Azuma's inequality [10] is the concentration inequality applied. Here, we also present a new security proof based on the application of the recently proposed Kato's inequality [24]. First, we introduce the concentration inequalities that we consider, and then we provide the analysis.

2.F.1 Concentration inequalities

Let $\xi_1, ..., \xi_N$ be a sequence of Bernoulli random variables, and let $\Lambda_l = \sum_{u=1}^{l} \xi_u$. Let $\mathcal{F}_l$ be its natural filtration, i.e. the σ-algebra generated by $\{\xi_1, ..., \xi_l\}$.

2.F.1.1 Azuma's inequality

According to Azuma's inequality [10],

$$\begin{aligned} \Pr\left[\Lambda_n - \sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) \geq b\sqrt{N}\right] &\leq \exp\left[-\frac{b^2}{2}\right], \\ \Pr\left[\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) - \Lambda_n \geq b\sqrt{N}\right] &\leq \exp\left[-\frac{b^2}{2}\right]. \end{aligned} \tag{2.72}$$

Equating the right hand sides to to ε_{A} and solving for b, we have that

$$\begin{aligned} \sum_{u=1}^{N} \Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) &\leq \Lambda_N + \Delta_{\mathrm{A}}, \\ \Lambda_N &\leq \sum_{u=1}^{N} \Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) + \Delta_{\mathrm{A}}, \end{aligned} \tag{2.73}$$

except with probability at most ε_{A} for each of the bounds, where $\Delta_{\mathrm{A}} = \sqrt{2N \ln \varepsilon_{\mathrm{A}}^{-1}}$.

2.F.1.2 Kato's inequality

According to Kato's inequality [24], for any n, and any a, b such that $b \geq |a|$,

$$\Pr\left[\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) - \Lambda_N \geq \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}\right] \leq \exp\left[\frac{-2(b^2-a^2)}{(1+\frac{4a}{3\sqrt{N}})^2}\right]. \quad (2.74)$$

By replacing $\xi_l \to 1 - \xi_l$ and $a \to -a$ in Eq. (2.74), we also derive [25]

$$\Pr\left[\Lambda_N - \sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) \geq \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}\right] \leq \exp\left[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{N}})^2}\right]. \quad (2.75)$$

By isolating Λ_N in Eq. (2.75), we derive,

$$\Pr\left[\Lambda_N \geq \frac{N}{\sqrt{N}-2a}\left(\frac{1}{\sqrt{N}}\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) + b - a\right)\right] \leq \exp\left[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{N}})^2}\right], \quad (2.76)$$

which holds when $a \leq \sqrt{N}/2$.

In the following, we will use Eq. (2.74) to obtain an upper bound on $\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1})$, Eq. (2.75) to obtain a lower bound on $\sum_{u=1}^{N} \Pr(\xi_u = 1|\mathcal{F}_{u-1})$, and Eq. (2.76) to obtain an upper bound on Λ_N.

Upper bound on the sum of probabilities

Before running the protocol, one should use previous knowledge of the channel to come up with a prediction $\tilde{\Lambda}_N$ of the value of Λ_N that one expects to obtain. Then, one calculates the values of a and b that would minimise the deviation term in Eq. (2.74) if the realisation of Λ_N equalled $\tilde{\Lambda}_N$, for a fixed failure probability ε_{K}. These are the solution of the optimisation problem

$$\begin{aligned} \min_{a,b} \quad & \left[b + a\left(\frac{2\tilde{\Lambda}_N}{N} - 1\right)\right]\sqrt{N} \\ \text{s.t.} \quad & \exp\left[\frac{-2(b^2-a^2)}{(1+\frac{4a}{3\sqrt{N}})^2}\right] = \varepsilon_{\mathrm{K}}, \\ & b \geq |a|, \end{aligned} \quad (2.77)$$

which can be expressed as

$$\begin{aligned} a &= \frac{3\left(72\sqrt{n}\tilde{\Lambda}_N(n-\tilde{\Lambda}_N)\ln\varepsilon_{\mathrm{K}} - 16N^{3/2}\ln^2\varepsilon_{\mathrm{K}} + 9\sqrt{2}(N-2\tilde{\Lambda}_N)\sqrt{-N^2\ln\varepsilon_{\mathrm{K}}(9\tilde{\Lambda}_N(n-\tilde{\Lambda}_N) - 2N\ln\varepsilon_{\mathrm{K}})}\right)}{4(9N - 8\ln\varepsilon_{\mathrm{K}})(9\tilde{\Lambda}_N(n-\tilde{\Lambda}_N) - 2N\ln\varepsilon_{\mathrm{K}})}, \\ b &= \frac{\sqrt{18a^2N - (16a^2 + 24a\sqrt{n} + 9N)\ln\varepsilon_{\mathrm{K}}}}{3\sqrt{2N}}. \end{aligned} \quad (2.78)$$

Then, we have that

$$\sum_{u=1}^{N} \Pr\left(\xi_u = 1 | \xi_1, ..., \xi_{u-1}\right) \leq \Lambda_N + \Delta_K^{\mathrm{U}}, \tag{2.79}$$

except with probability ε_{K}, where

$$\Delta_K^{\mathrm{U}} = \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}. \tag{2.80}$$

Lower bound on the sum of probabilities

Similarly to the previous case, one should use previous knowledge of the channel to come up with a prediction $\tilde{\Lambda}_N$ of the value of Λ_N that one expects to obtain after running the protocol. Then, one calculates the values of a and b that would minimise the deviation term in Eq. (2.75) if the realisation of Λ_N equalled $\tilde{\Lambda}_N$, for a fixed failure probability ε_{K}. These are the solution of the optimisation problem

$$\begin{aligned} \min_{a,b} \quad & \left[b + a\left(\frac{2\tilde{\Lambda}_N}{N} - 1\right)\right]\sqrt{N} \\ \text{s.t.} \quad & \exp\left[\frac{-2(b^2 - a^2)}{(1 - \frac{4a}{3\sqrt{N}})^2}\right] = \varepsilon_{\mathrm{K}}, \\ & b \geq |a|, \end{aligned} \tag{2.81}$$

which can be expressed as

$$\begin{aligned} a &= \frac{3\left(-72\sqrt{N}\tilde{\Lambda}_N(n - \tilde{\Lambda}_N)\ln\varepsilon_{\mathrm{K}} + 16N^{3/2}\ln^2\varepsilon_{\mathrm{K}} + 9\sqrt{2}(N - 2\tilde{\Lambda}_N)\sqrt{-N^2\ln\varepsilon_{\mathrm{K}}(9\tilde{\Lambda}_N(n - \tilde{\Lambda}_N) - 2N\ln\varepsilon_{\mathrm{K}})}\right)}{4(9N - 8\ln\varepsilon_{\mathrm{K}})(9\tilde{\Lambda}_N(n - \tilde{\Lambda}_N) - 2N\ln\varepsilon_{\mathrm{K}})}, \\ b &= \frac{\sqrt{18a^2N - \left(16a^2 - 24a\sqrt{n} + 9N\right)\ln\varepsilon_{\mathrm{K}}}}{3\sqrt{2N}}. \end{aligned} \tag{2.82}$$

Then, we have that

$$\sum_{u=1}^{N} \Pr\left(\xi_u = 1 | \mathcal{F}_{u-1}\right) \geq \Lambda_N - \Delta_K^{\mathrm{L}}, \tag{2.83}$$

except with probability ε_{K}, where

$$\Delta_K^{\mathrm{L}} = \left[b + a\left(\frac{2\Lambda_N}{N} - 1\right)\right]\sqrt{N}. \tag{2.84}$$

Upper bound on the actual value

In this case, we assume that we have an upper bound S_N on the sum of probabilities $\sum_{u=1}^{N} \Pr\left(\xi_u = 1 | \mathcal{F}_{u-1}\right)$, and we want to obtain an upper bound on Λ_N. Before running the protocol one should use previous knowledge to come up with a prediction $\tilde{S}_N$ of the value of the upper bound S_N that one expects to obtain. Then, one calculates the values of a and b that would minimise the deviation term in Eq. (2.76) if the prediction comes true. These are the solution of the optimisation problem

$$\begin{aligned} \min_{a,b} \quad & \frac{N}{\sqrt{N}-2a}\left(\frac{1}{\sqrt{N}}\tilde{S}_N + b - a\right) \\ \text{s.t.} \quad & \exp\left[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{N}})^2}\right] = \varepsilon_{\mathrm{K}}, \\ & b \geq |a|, \end{aligned} \tag{2.85}$$

whose analytical solution is

$$\begin{aligned} a &= \frac{3\sqrt{N}\left(9\ln\varepsilon_{\mathrm{K}}\left(3N^2 - 8N\tilde{S}_N + 8\tilde{S}_N^2\right) + 9(N-2\tilde{S}_N)\sqrt{N\ln\varepsilon_{\mathrm{K}}(N\ln\varepsilon_{\mathrm{K}} + 18\tilde{S}_N(\tilde{S}_N - N))} + 4n\ln^2(\varepsilon_{\mathrm{K}})\right)}{4\left(36\ln\varepsilon_{\mathrm{K}}\left(N^2 - 2N\tilde{S}_N + 2\tilde{S}_N^2\right) + 4N\ln^2\varepsilon_{\mathrm{K}} + 81N\tilde{S}_N(N-\tilde{S}_N)\right)}, \\ b &= \frac{\sqrt{18a^2N - \left(16a^2 - 24a\sqrt{N} + 9N\right)\ln\varepsilon_a}}{3\sqrt{2N}}. \end{aligned} \tag{2.86}$$

Then, we have that,

$$\Lambda_N \geq \frac{N}{\sqrt{N}-2a}\left(\frac{1}{\sqrt{N}}S_N + b - a\right), \tag{2.87}$$

except with probability ε_{K}.

2.F.2 Analysis

We assume a virtual protocol in which Alice prepares N_{tot} copies of the entangled state in Eq. (2.10), and sends all subsystems B to Bob through the untrusted quantum channel. Then, Bob performs a quantum non-demolition measurement on each system B, learning which rounds produce a click on his detectors, and saving the system B of these detected rounds in a quantum memory. Let N be the number of detected rounds. For each detected round $u = \{1, 2, \ldots, N\}$, Alice measures her ancilla S, and Bob measures B in the X basis; except if Alice obtained $S = 5$, in which case Bob measures B in the Z basis. Let $\xi_u = (i, j)$ represent the event "Alice learns that she emitted i and

Bob obtains measurement result j". More specifically, Alice learns that she emitted $i = \{\text{vir}_0, \text{vir}_1, 0_Z, 1_Z, 0_X\}$ if she obtained $S = \{0, 1, 2, 3, 4\}$ in her measurement of system S, respectively. Events in which she obtained $S = 5$ are ignored in the analysis. Then, using the fact that the virtual states can be written as an operator-form linear function of the actual states as in Eq. (2.11), one can show that

$$\begin{aligned}&\sum_{u=1}^{N} \Pr[\xi_u = (\text{vir}_\alpha,\, \alpha \oplus 1)|\mathcal{F}_{u-1}] \\ &\quad = \sum_{i=\{0_Z,1_Z,0_X\}} \frac{p_{\text{vir}_\alpha} p_{Z_B} c_{i|\text{vir}_\alpha}}{p_i p_{X_B}} \sum_{u=1}^{N} \Pr[\xi_u = (i,\, \alpha \oplus 1)|\mathcal{F}_{u-1}],\end{aligned} \tag{2.88}$$

where $\mathcal{F}_{u-1}$ is the σ-algebra generated by $\{\xi_1, ..., \xi_{u-1}\}$. Now one needs to apply a concentration bound for sums of dependent random variables to substitute the sums of probabilities in Eq. (2.88) by the actual values.

2.F.2.1 Using Azuma's inequality

Applying Eq. (2.73) to Eq. (2.88), we have that

$$N_{\text{vir}_\alpha}^{\alpha\oplus 1} \leq \sum_{i=\{0_Z,1_Z,0_X\}} \frac{p_{\text{vir}_\alpha} p_{Z_B} c_{i|\text{vir}_\alpha}}{p_i p_{X_B}} (N_i^{\alpha\oplus 1} + \delta_i) + \Delta_{\text{A}} := \overline{N}_{\text{vir}_\alpha}^{\alpha\oplus 1}, \tag{2.89}$$

except with probability $4\varepsilon_{\text{A}}$, where ε_{A} is the failure probability of each aplication of Azuma's inequality, which has been applied four times; and $\delta_i = \Delta_{\text{A}}$ ($\delta_i = -\Delta_{\text{A}}$) if $c_{i|\text{vir}_\alpha}$ is positive (negative). Then, the number of phase errors is upper bounded by

$$N_{\text{ph}} \leq \overline{N}_{\text{vir}_0}^{1} + \overline{N}_{\text{vir}_1}^{0}, \tag{2.90}$$

except with probability $\varepsilon = 8\varepsilon_{\text{A}}$.

Using a similar analysis, for the MDI protocol, we have that

$$N_{\text{ph}} \leq \sum_{j,s} \frac{p_{\text{ph}} c_{j,s}}{p_{j,s,\mathcal{T}}} (N_{j,s,\mathcal{T}} + \delta_{j,s}) + \Delta_{\text{A}} \tag{2.91}$$

except with probability $\varepsilon = 9\varepsilon_{\text{A}}$, where $N_{j,s,\mathcal{T}}$ is the number of detected test rounds in which the user emitted $|\psi_{j,s}\rangle_{a,b}$, and $\delta_{j,s} = \Delta_{\text{A}}$ ($\delta_{j,s} = -\Delta_{\text{A}}$) if $c_{j,s}$ is positive (negative).

2.F.2.2 Using Kato's inequality

Applying Eq. (2.79) and Eq. (2.83) to Eq. (2.88), we have that

$$\sum_{u=1}^{N} \Pr[\xi_u = (\mathrm{vir}_\alpha, \alpha \oplus 1) | \mathcal{F}_{u-1}] \leq \sum_{i=\{0_Z, 1_Z, 0_X\}} \frac{p_{\mathrm{vir}_\alpha} p_{Z_B} c_{i|\mathrm{vir}_\alpha}}{p_i p_{X_B}} (N_i^{\alpha\oplus 1} + \delta_i) := S_{\mathrm{vir}_\alpha}, \tag{2.92}$$

except with probability $3\varepsilon_{\mathrm{K}}$, where $\delta_i = \Delta_{\mathrm{K}}^{\mathrm{U}}$ ($\delta_i = -\Delta_{\mathrm{K}}^{\mathrm{L}}$) if $c_{i|\mathrm{vir}_\alpha}$ is positive (negative). Substituting $S_n \to S_{\mathrm{vir}_\alpha}$ and $\Lambda_n \to N_{\mathrm{vir}_\alpha}^{\alpha\oplus 1}$ in Eq. (2.87), we obtain an upper bound $\overline{N}_{\mathrm{vir}_\alpha}^{\alpha\oplus 1}$ which fails with probability $4\varepsilon_{\mathrm{K}}$. Then, the number of phase errors is upper bounded by

$$N_{\mathrm{ph}} \leq \overline{N}_{\mathrm{vir}_0}^{1} + \overline{N}_{\mathrm{vir}_1}^{0}, \tag{2.93}$$

except with probability $\varepsilon = 8\varepsilon_{\mathrm{K}}$.

Similarly, for the MDI protocol, we have that

$$\sum_{u=1}^{N} \Pr[\xi_u = \mathrm{ph} | \mathcal{F}_{u-1}] \leq \sum_{j,s} \frac{p_{\mathrm{ph}} c_{j,s}}{p_{j,s,\mathcal{T}}} (N_{j,s,\mathcal{T}} + \delta_{j,s}) := S_{\mathrm{ph}} \tag{2.94}$$

except with probability $\varepsilon = 8\varepsilon_{\mathrm{A}}$, where $\delta_{j,s} = \Delta_{\mathrm{K}}^{\mathrm{U}}$ ($\delta_{j,s} = -\Delta_{\mathrm{K}}^{\mathrm{L}}$) if $c_{j,s}$ is positive (negative). Then, substituting $S_n \to S_{\mathrm{ph}}$ and $\Lambda_n \to N_{\mathrm{ph}}$ in Eq. (2.87), we obtain an upper bound on N_{ph} which fails with probability $9\varepsilon_{\mathrm{K}}$.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, p. 1301, 2009. 51

[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics*, vol. 8, pp. 595–604, 2014. 51

[3] M. Koashi, "Complementarity, distillable secret key, and distillable entanglement," *arXiv:0704.3661*, 2007. 51

[4] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, p. 045018, 2009.

[5] M. Hayashi and T. Tsurumaru, "Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths," *New J. Phys.*, vol. 14, no. 9, p. 093014, 2012. 68

[6] T. Tsurumaru, "Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3465–3484, 2020. 51

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984. 51

[8] C.-H. F. Fung, X. Ma, and H. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A*, vol. 81, no. 1, p. 012318, 2010. 51

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nat. Commun.*, vol. 3, p. 634, 2012. 51

[10] K. Azuma, "Weighted sums of certain dependent random variables," *Tohoku Math. J.*, vol. 19, pp. 357–367, 1967. 51, 83

[11] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, "Unconditional security of a three state quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 94, no. 4, p. 040503, 2005. 51

[12] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A*, vol. 90, no. 5, p. 052314, 2014. 51, 52, 57

[13] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources," *New J. Phys.*, vol. 17, p. 093011, Sept. 2015. 52, 69, 70, 83

[14] A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H.-K. Lo, and K. Tamaki, "Quantum key distribution with setting-choice-independently correlated light sources," *npj Quantum Inf.*, vol. 5, no. 1, pp. 1–8, 2019. 51

[15] K. Maeda, T. Sasaki, and M. Koashi, "Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit," *Nat. Commun.*, vol. 10, no. 1, pp. 1–8, 2019. 51, 52, 68, 72, 73

[16] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, vol. 4, pp. 325–360, 2004. 51

[17] M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," *npj Quantum Inf.*, vol. 5, no. 1, p. 62, 2019. 52, 68, 72

[18] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, "Quantum key distribution with correlated sources," *Sci. Adv.*, vol. 6, p. eaaz4487, Sept. 2020. 72

[19] Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, "Practical Quantum Key Distribution That is Secure Against Side Channels," *Phys. Rev. Applied*, vol. 15, p. 034072, Mar. 2021. 52, 72

[20] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, 2012. 52, 62, 82

[21] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, "Experimental quantum key distribution with source flaws," *Phys. Rev. A*, vol. 92, p. 032305, 2015. 52

[22] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, "Experimental measurement-device-independent quantum key distribution with imperfect sources," *Phys. Rev. A*, vol. 93, p. 042308, 2016. 52

[23] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, p. 190502, 2018. 52

[24] G. Kato, "Concentration inequality using unconfirmed knowledge," *arXiv:2002.04357*, 2020. 70, 83, 84

[25] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, "Tight finite-key security for twin-field quantum key distribution," *npj Quantum Information*, vol. 7, pp. 1–9, Feb. 2021. 70, 73, 84

[26] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003. 71

[27] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, 2005.

[28] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, p. 230503, 2005.

[29] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, 2005. 71

[30] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nat. Commun.*, vol. 5, no. 1, pp. 1–7, 2014. 71

[31] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A*, vol. 95, p. 012333, Jan. 2017. 73

[32] S. Bahrani, O. Elmabrok, G. Currás Lorenzo, and M. Razavi, "Wavelength assignment in quantum access networks with hybrid wireless-fiber links," *J. Opt. Soc. Am. B*, vol. 36, p. B99, Feb. 2019. 73

Chapter 3

Finite-key analysis for memory-assisted decoy-state quantum key distribution

3.1 Abstract

Memory-assisted quantum key distribution (MA-QKD) systems are among novel promising solutions that can improve the key-rate scaling with channel loss. By using a middle node with quantum storage and measurement functionalities, they offer the same key-rate scaling with distance as a single-node quantum repeater. However, the distance at which they can surpass the nominal key rate of repeaterless systems, in terms of bits per second, is typically long, owing to the efficiency and/or interaction time issues when one deals with quantum memories. This crossover distance can be a few hundred kilometres, for instance, when one relies on the exchange of infinitely many key bits for the key-rate analysis. In a realistic setup, however, we should account for the finite-key effects in our analysis. Here, we show that accounting for such effects would actually favour MA-QKD setups, by reducing the crossover distance to the regime where realistic implementations can take place. We demonstrate this by rigorously analysing a decoy-state version of MA-QKD, in the finite-key regime, using memory parameters already achievable experimentally. This provides us with a better understanding of the advantages and challenges of working with memory-based systems.

3.2 Introduction

Quantum key distribution (QKD) has made a lot of progress as part of the solution package for secure communications in the quantum era [1]. But, when it comes to long distances, quantum technologies still have a long way to go before they can replicate the same functionalities that public-key cryptography offers. In terrestrial networks, such as the infrastructure that today's Internet is based on, the biggest challenge to overcome is perhaps the exponential growth of loss in optical fibres [2]. This makes it extremely difficult to perform QKD at long distances without trusted middle nodes. Quantum repeaters are potential solutions, but none of their theoretical architectures can currently be implemented experimentally to the full effect [3]. For instance, probabilistic quantum repeaters [4–6] would require quantum memory (QM) modules with high coupling efficiencies to light and with coherence times exceeding the transmission delays, which are hard to achieve together [7]. That said, even if the current QMs are not sufficiently advanced for quantum repeaters, they may still be used to offer key-rate improvements in some of the existing QKD systems. Working on such memory-assisted QKD (MA-QKD) systems paves the way for future scalable quantum repeaters. This work studies the secret key rate for decoy-state MA-QKD systems in the practical regime where only a finite block of data is exchanged among QKD users.

MA-QKD setups [7, 8] are based on the measurement-device-independent QKD (MDI-QKD) protocol [9], in which Alice and Bob send BB84-encoded pulses to a middle node, Charlie, who performs a Bell-state measurement (BSM). In MDI-QKD, a raw key bit can be generated if both pulses survive the channel loss in the same round and the BSM is successful. In MA-QKD, however, Charlie employs two QMs to store the quantum state of the users' pulses, and only performs the BSM when both memories have been loaded. This will allow the pulses that arrive in different rounds to be combined to produce a key bit. Thus, the key-rate scaling is improved from η^2 in MDI-QKD to η in MA-QKD [7], where η is the transmittance of the channel between Alice/Bob and Charlie. Together with the recently introduced twin-field QKD (TF-QKD) [10], MA-QKD is a strong contender to beat the current rate versus distance records in QKD. Such an advantage has recently been demonstrated experimentally using silicon vacancy centres [11].

Offering advantage in a realistic setup that relies on imperfect QMs is not without its own challenges. For instance, photon-memory coupling can introduce additional loss in the setup. Some memories have also a long photon-memory interaction time that requires users to employ a low source repetition rate. The better scaling with channel loss can only offset these effects after a certain distance, which we refer to as the crossover distance. If this distance happens to be long, it would then be difficult to experimentally implement a stable system that benefits from such an advantage. Other effects, such as decoherence in the QMs, also need to be taken into account when evaluating system performance [7] and they typically exacerbate the situation. Additionally, in realistic setups, we should consider the effect of using weak laser pulses by the users in conjunction with finite-key effects. In this work, we develop a security analysis that accounts for all the above, and, in particular, quantify the interplay between the crossover distance and other parameters of the system.

Several analyses of MA-QKD have already been carried out, under varying assumptions and for different implementations of QMs. However, most of them [8, 12, 13] assume single-photon sources, which are difficult to attain in practice. In many QKD experiments, attenuated laser sources are used, instead. The multi-photon components in the signals generated by these sources introduce security loopholes, and they need to be dealt with [14]. The decoy-state method [15] is often used to bound the leaked information from these multi-photon signals, thus closing the loophole. This method involves the statistical estimation of channel probabilities, based on data collected from the use of different laser intensities. This statistical characterisation of the channel would only be perfect if one could collect an infinite amount of data by using the channel infinitely many times. In practice, a QKD experiment will run for a fixed amount of time, and a finite-size dataset will be generated [16]. By using statistical analyses based on concentration inequalities, it has been shown that a bound on the leaked information can be computed [16, 17], thus a secret key can still be distilled, with a failure probability that can be made arbitrarily small. However, as the total number of signals exchanged (the block size) gets smaller, the obtainable secret key rate is reduced. In fact, if the block size is too small, no secret key rate may be obtained at all.

In this paper, we provide the first analysis of a decoy-state MA-QKD setup that accounts for the statistical fluctuations that arise from generating a finite-size key.

Previous work [7] on MA-QKD has only considered the asymptotic limit in which the users exchange an infinite number of signals, and under simplified assumptions on the loading of QMs with attenuated laser sources. In our finite-key analysis, we compare MA-QKD performance with that of a no-memory MDI-QKD system, by using parameters from state-of-the-art experiments on quantum memories [12]. We find that MA-QKD is inherently more resistant to finite-key effects, and it experiences a lower reduction in secret key rate than MDI-QKD. In particular, we see that once these effects are considered, the distance from which MA-QKD offers an advantage is reduced. This would make it easier for experimentalists to implement a decoy-state MA-QKD setup that outperforms, in terms of secret key rate versus distance, the equivalent decoy-state BB84 or MDI-QKD setups.

In terms of key rate, MA-QKD may not outperform the recently introduced TF-QKD, at least with state-of-the-art quantum memories. However, one should be careful when comparing systems that have different requirements. For instance, the single-photon interference of TF-QKD demands phase stability over long channels, which is experimentally difficult, and which MA-QKD does not need. We believe that comparing MA-QKD with MDI-QKD is the fairest when it comes to the requirements of each system. We note that there exists some recent work on memory assisted TF-QKD [18], which specifies under what circumstances adding quantum memories to TF-QKD setups can be advantageous. Moreover, we believe that MA-QKD is of special interest as is the very first step toward building memory-based quantum repeaters. Unlike TF-QKD, or other no-memory systems, these offer a scalable solution for long distance quantum communications. Any practical progress with quantum repeaters would be based on fully understanding and implementing MA-QKD as the simplest memory-based repeater system. Our findings for MA-QKD systems suggest that memory-based quantum repeaters may also be resilient to finite-key effects, at least when users access them with decoy-state sources.

The rest of the paper is organised as follows. In Section 3.3, we describe the analysed setup, placing an emphasis on the QM modules, and the different parameters that are used for modelling them. In Section 3.4, we explain how different system parameters affect the secret-key rate. In Section 3.5, we compare the secret key rate achievable in decoy-state MA-QKD and decoy-state MDI-QKD with examples from warm vapour

and cold atomic ensembles. Section 3.6 concludes the paper with our interpretation of the results.

3.3 System description

In this section, we describe our MA-QKD setup and the assumptions we make on different devices and components of the system.

Figure 3.1 shows the schematic of the MA-QKD setup considered in this work. Here, in each round, Alice and Bob each send decoy-state BB84 states in their chosen basis. Charlie verifies the receipt of the transmitted signal by generating an entangled photon pair (EPP) on each side to effectively teleport the state of the users to a local photon on his site. The side BSMs in Fig. 3.1 would herald the success of such an event, in which case the remaining photon of the EPP source will be written to the corresponding QM. That is, its photonic state is transferred to the memory, and will be kept there until the state of the other user is also successfully received and teleported to its respective QM. At this point, the two QMs will be read, i.e., their states will be transferred to photons on which the middle BSM is performed. At the end of the protocol, Charlie announces his measurement results, and Alice and Bob would follow with conventional steps for sifting and post-processing of their key bits.

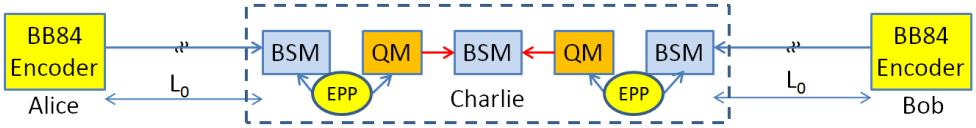


Figure 3.1: The schematic of an MA-QKD system. The two users Alice and Bob use decoy-state BB84 encoders to generate polarisation/phase encoded signals. Charlie, in the middle, uses entangled photon pair (EPP) sources to teleport the state sent by the users to the corresponding memories. When both memories are loaded, their states are converted back to photons and combined in the middle BSM. For an example of the BSM module, see Fig. 3.4 of Appendix 3.A.

Note that the teleportation scheme used here to herald and transfer the state of photons is not an ideal one. In an ideal teleportation setting, the users have to send ideal single photons, whereas here they are using weak laser pulses. The effect of the

multi-photon components has then to be taken into account. We analyse the memory-loading procedure for weak laser pulses in Appendix 3.A. In this scheme, we are also delaying the writing of the second photon of the EPP until we learn about the success of teleportation. While there is a chance that the transfer of this photonic state to the QM may fail, this delayed writing process has the advantage that the QM initialisation is not necessary in each round [12], but only when a writing procedure has been attempted. This helps with maximising the repetition rate of the protocol especially when the initialisation phase is time consuming. We account for the failure in transferring a local single photon to the memory by the memory writing efficiency parameter.

Finally, while, in practice, an ideal EPP source as assumed here may not be realistic, it would help us obtain the key features of our finite-key analysis without overly complicating the calculations. The former issue can be managed by techniques introduced in Ref. [12], where they propose a quasi-EPP scheme based on single-photon sources, instead. It is also possible to create a photon-QM entangled pair in certain QMs [13, 19]. In all cases, we should be careful with the possible multiple excitations we may locally create at Charlie's node to not violate the conditions for the proper operation of MA-QKD systems [12, 20]. Under above considerations, we believe that the main result from our paper, i.e., the resilience of the decoy-state MA-QKD to finite-key effects, should still hold.

In the following, we describe the key components of our system in more detail.

3.3.1 Quantum memories

We model QMs using a few relevant parameters to our setup, while keeping our model as general as possible:

- The writing efficiency, denoted as η_w, is the probability of successfully transferring a single-photon state to the quantum memory. We refer to this process by the term "loading".

- The reading efficiency, denoted as η_r, is the probability to transfer the qubit state stored in the QM back to a single photon. We assume that, at time t after loading, $\eta_r(t) = \eta_{r0} \exp[-t/T_1]$, where η_{r0} denotes the reading efficiency at time $t = 0$ and T_1 is the decay time constant of the QM.

- The QM decoherence time constant is denoted by T_2. We consider two decoherence processes: dephasing and depolarisation. In the case of dephasing, for an initial state $\rho(0)$ of the QM, the state at a time t after loading will be

$$\rho(t) = p(t)\rho(0) + [1 - p(t)]\sigma_z\rho(0)\sigma_z, \tag{3.1}$$

  where $p(t) = [1 + \exp(-t/T_2)]/2$. Dephasing will only affect X-basis states. For a depolarisation process, we assume

$$\rho(t) = p(t)\rho(0) + \frac{1 - p(t)}{3}[\sigma_z\rho(0)\sigma_z + \sigma_x\rho(0)\sigma_x + \sigma_y\rho(0)\sigma_y]. \tag{3.2}$$

  In both cases, we treat the QM state as a qubit for which σ_x, σ_y, and σ_z are its corresponding Pauli operators.

- We denote the interaction time with single photons as τ_{int}, for both reading and writing procedures. We denote the initialisation time of the QM as τ_{init}. Because of our delayed-writing assumption, a writing procedure will always be followed by a reading procedure, and the QM only needs to be initialised after reading.

- The writing time is denoted as τ_w, and the reading time is denoted as τ_r. For our delayed writing procedure, we assume $\tau_w = \tau_{\text{int}}$ and $\tau_r = \tau_{\text{int}} + \tau_{\text{init}}$. We effectively neglect the required time for measurement in both cases.

- We denote as τ_p the pulse duration of both the user sources and the EPP sources, which are assumed to have matching pulse shapes. We assume $\tau_p = \tau_w$ to maximize the writing efficiency into the memory. The MA-QKD system is to be run at a repetition rate of $R_s = 1/\tau_p$.

3.3.2 Channel and source model

Similarly, we present our assumptions on the channel and the users sources:

- We assume that the user sources produce phase-randomised coherent states, and that the intensity of the pulse can be perfectly tuned in each round. The users select a random intensity, in terms of mean number of photons, from the set $\{z, w_1, w_2, v\}$ with probability $\{p_z, p_{w_1}, p_{w_2}, p_v\}$. Emissions with the z intensity will be encoded in the Z basis, and they will be used to generate the raw key.

Emissions with any other intensity will be encoded in the X basis, and they will be used to estimate the single-photon counts and their corresponding phase-error rate. We will refer to z as the signal intensity, and to $\{w_1, w_2, v\}$ as the decoy intensities. Our model can work with either polarisation or phase encoding. We denote the source repetition rate as R_s.

- We assume non-resolving detectors with efficiency η_d and a dark count rate γ_{dc}. The latter includes intrinsic effects as well as background photons in the channel. The dark count probability per detector per round of the protocol is $p_{\text{dc}} = \gamma_{dc}\tau_p$.

- We denote the total length of the channel separating Alice and Bob by L. We assume that the central node is located exactly halfway between the users. We denote the attenuation length of the channel by L_{att}. The transmission coefficient for each leg of the channel is given by $\eta_{\text{ch}} = \exp\left(\frac{-L}{2L_{\text{att}}}\right)$.

- We consider the effect of setup misalignment between the user sources and the measurement devices in the central node. The standard way to model misalignment in QKD is by a misalignment probability e_{mis}, and previous analyses of MA-QKD have also modelled it that way [7]. However, as explained in Appendix 3.A, such a model is not directly applicable when considering the indirect loading of QMs with weak laser pulses. Here, we model misalignment by assuming that the encoding modes, e.g., horizontal and vertical polarisations, have been rotated from their ideal settings by a random angle θ. We then average over θ to find parameters of interest.

- In our setup, we allow for the usage of frequency converters to match the frequency of the telecom signals sent by the users with that of the EPP source. The EPP source, in one leg, should generate a beam that interacts with the QM. For a degenerate EPP source, this would typically require us to downconvert the frequency of the other beam to the telecom band. One can, in principle, design a non-degenerate EPP source, but we should then be careful with the extent of multiple excitations in the source [20]. We account for the efficiency of frequency converters by including additional loss in our setup.

3.4 Key-rate analysis

In this section, we find the secret key generation rate for our decoy-state MA-QKD setup, in both the asymptotic and finite-key regimes. We assume the nominal mode of operation in which no eavesdropper is present, and the system is only affected by device imperfections. Also, for simplicity, we assume that the sources used by Alice and Bob, and the channels connecting them to the middle node are identical.

3.4.1 Asymptotic case

In this subsection, we calculate the key rate obtainable in the limit that the users exchange an infinite number of signals. In this regime, we can assume that the signal intensity is used with probability $p_z \simeq 1$, and that the decoy-state analysis provides a perfect estimate of the single-photon channel probabilities. Under these assumptions, the secret key rate is lower bounded by [7]

$$R \geq R_s \left[Q_{11}^Z \left(1 - h(e_{\text{ph}})\right) - f Q_Z h(e_Z) \right], \tag{3.3}$$

where Q_Z is the probability of generating a sifted key bit per round of the protocol, and e_Z is the error rate of the sifted key. Also, Q_{11}^Z is the single-photon contribution to Q_Z, and e_{ph} is the phase-error rate of these single-photon components.

Our objective here is to calculate what Alice and Bob would observe in a nominal experiment for directly measurable parameters Q_Z and e_Z, and their corresponding estimation for Q_{11}^Z and e_{ph} after using the decoy state method. For this, we mainly use the method introduced in [7], but we adjust it as needed to account for the specific components of our model. In particular, in the case of weak laser pulses at the source, we need to pay special attention to the modelling of misalignment in the channel. We also extend the results of [7] to depolarising channels.

Appendix 3.A provides a detailed and self-contained description of our analysis. In short, we first obtain the exact expression for loading probability p_{load}^{μ} and loading error rate e_{load}^{μ} when Alice/Bob sends a phase-randomised coherent state with intensity μ under a generic model for channel misalignment. This parameter would then allow us to calculate the average number of rounds needed to load both memories, and the corresponding state of the memories after a heralded loading. We will then account for memory decoherence and decay processes and calculate the rate of success, and

the corresponding error rate, for the middle BSM. Section 3.A.2.1, in Appendix 3.A, provides the analytical form for all parameters needed in Eq. (3.3).

3.4.2 Finite-key regime

Now, we calculate the secret key rate in the more realistic scenario where the number of signals exchanged by the users is finite. In this regime, we still derive the secret key from the data points for which both users have used the Z basis, but we also need to take into account the rounds in which the users employ decoy intensities. In this case, we can no longer assume that the decoy-state analysis provides a perfect estimate of the single-photon statistics Q_{11}^Z and e_{ph}. Instead, we use a statistical analysis to bound them. Under our new assumptions, the total secret key length K satisfies

$$K \geq M_{11}^Z[1 - H(e_{\text{ph}})] - M_Z H(e_Z), \tag{3.4}$$

where M_Z is the length of the sifted key, generated from the events in which both users selected the Z basis (i.e., the z intensity), and e_Z is its bit error rate; M_{11}^Z is the number of bits in this sifted key that originated from single-photon emissions, and e_{ph} is their phase-error rate.

In an experimental implementation of the protocol, the measurable observables available to us are the sets $\{M^{ab}\}$ and $\{E^{ab}\}$, where M^{ab} is the total number of measurement counts when Alice has used intensity a *and* Bob has used intensity b, while E^{ab} is the number of such events that result in error. The objective of Alice and Bob is to use this data to obtain statistical bounds on M_{11}^Z and e_{ph}.

The full description of our statistical analysis appears in Appendix 3.B. We use the idea in [21] to perform our statistical fluctuation analysis using X-basis data only. This would make our statistical estimation procedure more efficient. By applying tight multiplicative Chernoff bounds [16], we are then able to use the measured counts M^{ab} and E^{ab} to set linear constraints on the possible values that M_{11}^Z and e_{ph} could take. These constraints enable us to express the desired bounds on these quantities as the solution to two linear programs. We use the analytical estimation procedure introduced in [17] to solve these programs.

For our numerical simulations, we still need to make some assumptions on the obtained measurement results in a nominal experiment. For this purpose, we use the

expected values for relevant parameters using the corresponding probability in the asymptotic regime, derived in the previous subsection. That is, we assume

$$M^{ab} = NQ^{ab} \quad \text{and} \quad E^{ab} = e_{ab}M^{ab}, \tag{3.5}$$

where N is the total number of rounds, i.e., the number of transmitted pulses by Alice/Bob, in the protocol, Q^{ab} is the probability of having a successful measurement originating from intensities a, for Alice, and b, for Bob, and e_{ab} is the probability that this measurement results in an error. Section 3.A.2.2, in Appendix 3.A, provides the derivation and the analytical form for all these parameters.

In our finite-key analysis, we have only considered the effect of statistical fluctuations on parameter estimation. Thus, in our key rate formula in Eq. (3.4), we have neglected some of the less significant terms that usually appear in a rigorous finite-key analysis. The latter is to adhere to the universal composable framework [22, 23]; e.g., we direct the reader to Eq. (1) of [17]. We have neglected these terms for simplicity, as they are, in practice, only on the order of tens of bits, and because their effect is identical for the memory-assisted and no-memory systems, which the present work aims to compare.

3.5 Numerical results

In this section, we use the results of Section 3.4 to simulate the secret key rate that can be achieved with the decoy-state MA-QKD scheme in Fig. 3.1, in both the asymptotic and finite-key regimes. We use two types of memories for our analysis: Warm vapour atomic ensembles, which often offer high bandwidth, hence high repetition rates, but a rather low coherence time; and cold atomic ensembles, which are often slower but benefit from longer coherence times. Table 3.1 summarises the relevant memory parameters used in our simulation based on the experimentally reported values in [24], for warm vapours, and [25], for cold atomic ensembles. In our simulations, we have assumed $T_1 = T_2$.

We compare the MA-QKD system with a no-memory MDI-QKD setup, run at a repetition rate of 1 GHz, as a reference point, and study how finite-key effects change the crossover distance under different circumstances. Section 3.A.3 in Appendix 3.A provides the analytical expressions used for simulating the MDI-QKD system. MDI-QKD

	WV [24]	CA [25]	SV [11]
Writing-reading efficiency, $\eta_w\eta_{r0}$	0.05	0.76	0.423
Decay time, T_1	120 µs	220 ms	200 μs
Interaction time, τ_{int}	1.43 ns	240 ns	142 ns
Repetition rate, R_s	518 MHz	4.2 MHz	7.04 MHz

Table 3.1: Parameter values of recently demonstrated warm vapour (WV) and cold atom (CA) ensembles [12], as well as silicon vacancy (SV) centres, used in the simulations in this work. For simplicity, in our simulations, we assume $T_2 = T_1$.

is the closest no-QM system to MA-QKD, which enables us to make this comparison as fair as possible. They both offer measurement-device-independent features and they can both be run with minimal requirements on the source or channel phase stabilisation. The latter property is needed for advanced twin-field QKD systems, whose rate-versus-distance scaling is similar to MA-QKD, but are expected to offer higher rates if properly implemented [26–28].

In all cases, we use the system parameters listed in Table 3.2, which are attainable by today's technologies [29]. In all graphs, we optimise over the values of the intensities $\{z, w_1, w_2\}$, and assume a vacuum intensity of $v = 0.5 \cdot 10^{-3}$, since the optimal value $v = 0$ may be difficult to achieve in practice. We also optimise over their selection probabilities $\{p_z, p_{w_1}, p_{w_2}, p_v\}$. In our finite-key analysis, we assume a failure probability of $\varepsilon = 0.5 \cdot 10^{-11}$ for each of the concentration bounds used in Section 3.B; the total failure probability of the estimation process is $20\varepsilon = 10^{-10}$.

In Fig. 3.2, we show the performance of the warm vapour memory in Ref. [24], for different values of the block size N, which represents the total number of signals sent by Alice (or Bob) in that run of the protocol. We can see that, at low distances, the key rate of MA-QKD is lower than that of MDI-QKD. This is partly due to the lower repetition rate for MA-QKD, but also due to the additional loss effects introduced by the QM's less-than-one writing and reading efficiencies. At longer distances, however, the improved key-rate scaling of MA-QKD with channel loss may overcome these effects.

In Fig. 3.2(a), we can see that in the asymptotic regime (black curves), the MA-QKD protocol can only offer a small advantage over MDI-QKD from around 340 km to 430 km. However, once we use a finite block size N (colour curves), the crossover distance moves to the left to shorter channel lengths, and even approaches 100 km at

Attenuation length of the channel, L_{att}	22 km
Detector efficiency, η_d	93%
Detector dark count rate, γ_{dc}	1 count/s
Misalignment error probability, e_{mis}	0.5%
Conversion efficiency, η_c	0.5, 1

Table 3.2: System parameter values used for the simulations in this work. For no-memory MDI-QKD, we assume that the channel misalignment, in their respective leg of the channel, flips the state sent by each user with probability e_{mis}. For MA-QKD, we assume that channel misalignment rotates the states sent by the users by an angle θ that follows a uniform distribution of width $2\sqrt{3e_{\text{mis}}}$; see Eq. (3.28), and the explanation preceding it.

$N = 10^{10}$. This suggests that in order to see the advantages of MA-QKD over no-QM MDI-QKD we only need to demonstrate such systems over much shorter distances than one may require in the asymptotic regime. With record distances for entanglement distribution between two QMs being around 50 km [30], one can hope that such a demonstration can take place in near future.

While a slight shift to the left, due to finite-key effects, might be expected in Fig. 3.2, the considerable change in the crossover distance may come as a surprise. A naive thinking may suggest that in order to see the benefits in the finite-key setting, we need to have larger count numbers in MA-QKD, as compared to MDI-QKD, to reduce statistical errors in our parameter estimation. But, so long as, in the asymptotic case, the key rate for MDI-QKD is higher than that of MA-QKD, we may expect that the corresponding counts will also remain larger in the finite-key setting, hence no considerable change may be expected in the crossover distance. This argument, however, fails to give us an accurate picture of what is happening in the MA-QKD case. Below, we explain two key reasons for why the finite-key setting may benefit the MA-QKD setup, hence shifting the crossover distance to much shorter channel lengths.

- **Self-purification of multi-photon terms:** The MA-QKD system can by design get rid of some of the erroneous terms that would otherwise be present in the no-QM setup. Let us compare the two setups when Alice selects a non-vacuum intensity s, in the X basis, and Bob selects the vacuum intensity v. In no-QM MDI-QKD, there is a single BSM module, in which Alice's and Bob's emissions

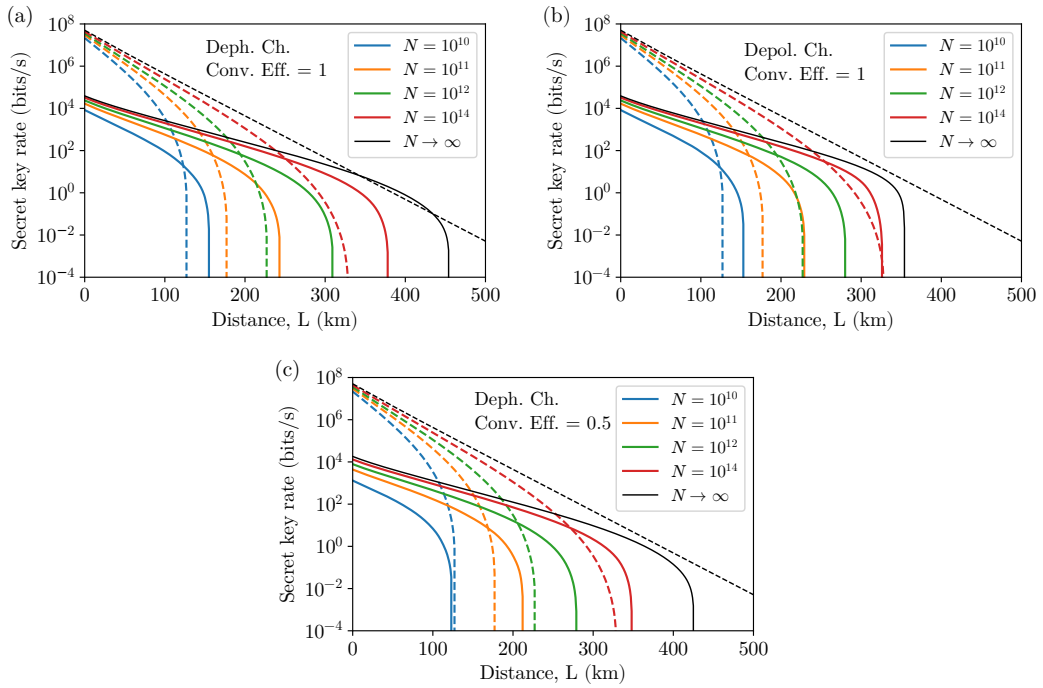


Figure 3.2: Secret key generation rate, in b/s, for a MA-QKD setup using warm vapour quantum memories [24] (solid lines), in comparison with no-memory MDI-QKD (dashed lines), for different values of the block size N. In (a) and (c) a dephasing channel is used to model memory decoherence, whereas, in (b), a depolarisation channel is used. The efficiency of the frequency converter is assumed ideal in (a) and (b), whereas, in (c), it is 50%.

are directly combined. A successful BSM, in polarisation encoding, is declared if two detectors corresponding to different polarisations click. In the event that Bob sends a vacuum state, a successful BSM could happen because of the multi-photon terms in Alice's signal. This increases M^{sv} and E^{sv} counts, which add to the uncertainty in estimating e_{ph}. In MA-QKD, such counts are much lower. Charlie will declare that Bob's QM has been loaded when his corresponding side BSM is successful. For a vacuum input, such an event could only happen if one of the detectors clicks because of the dark count, assuming that the EPP source can only cause a click in one of the detectors. For low dark count rates, as we assume here, the measurement counts M^{sv}, as well as its corresponding terms in error will be close to zero in MA-QKD. Around the crossover distance, this makes

the upper bound on e_{ph} lower for MA-QKD even if its corresponding value in the asymptotic case is higher than that of MDI-QKD. That is, MA-QKD enjoys less noisy statistics that helps us obtain tighter bounds on our parameters of interest.

- **Efficient use of decoy states:** In both MDI-QKD and MA-QKD, the secret key is extracted from events in which both users select the signal intensity z. The rounds in which they both employ the decoy intensities are used for parameter estimation only. The points that one user uses the Z basis and the other uses the X basis, are then somehow "wasted" and will be sifted out. MA-QKD can help with better sifting efficiency. This is partly because of the main advantage of MA-QKD with respect to MDI-QKD in that the key rate scales with the transmissivity of one leg of the channel, rather than the entire channel. To better understand this point, let us consider the effect of employing the vacuum intensity, v. Suppose that Alice and Bob are using either an MDI-QKD or an MA-QKD setup with a channel transmittance per leg of η, and that they use intensity z with probability $p_z \simeq 1$, as they do in the infinite key regime. Charlie will report a successful detection with probability Q_z. Now suppose that they use the same scheme as above, except that they now employ a (fictitious) finite-key scheme, in which they employ the vacuum intensity v with probability $p_v = p_z = 1/2$. The effect of this is equivalent to using a channel with transmittance per leg of $\eta/2$, since the effective transmittance of each user's link has been reduced by one half. Since MDI-QKD scales with η^2, Q_z will be reduced by a factor of 4. However, since MA-QKD scales with η, Q_z will only be reduced by a factor of 2. In reality, Alice and Bob will use additional decoy intensities other than the vacuum intensity. But since the decoy states will typically have larger vacuum components than the signal intensity z, they will have a similar effect as adding loss to the system, which MA-QKD tolerates better.

Another important factor in our finite-key comparison is the amount of time needed to collect data for a block size N. In the case of MDI-QKD, we can typically run the system at a high repetition rate on the order of GHz for very long periods of time. The stability of the memory-based system may, however, require us to stop collecting data after a certain period of time. It would be interesting to see how the two systems compare if, instead of the block size, one fixes the total data collection time T_{col},

instead. This corresponds to a block size of $N = R_s T_{\text{col}}$, for each system, and gives a considerable advantage to the faster system in collecting more data at an identical time. This would not make much a difference in the case of warm vapours as we can already run the system at sub-GHz rates. But, in the case of cold atomic ensembles or silicon vacancy centres, which represent slower memories, this would be interesting to study.

Figure 3.3 (a)-(c) show the performance of MA-QKD using the cold atom QM reported in Ref. [25], with a repetition rate of 4.2 MHz, at different collection times. This means that, at an identical collection time, the MDI-QKD system can collect almost 250 times more data than the MA-QKD setup. It is interesting to see that, even under these harsher conditions, the MA-QKD system can offer a similar advantage as we saw in Fig. 3.2 over the no-QM MDI-QKD setup. As shown in Fig. 3.3(a), for a dephasing channel, in the asymptotic regime (black curves), the MA-QKD system can only offer a small advantage in the range from 300 km to 430 km. However, if the experiment is run for an hour (orange curves), MA-QKD can generate more key after 230 km, and, while MDI-QKD dies off at about 250 km, MA-QKD can generate a key up to 350 km. If the experiment is run for just a minute (blue curves), MA-QKD can offer an advantage after a distance of just 170 km. In Fig. 3.3(d), we show a similar graph for the silicon vacancy centres used in the recent MA-QKD experiment reported in [11]. This system has a slightly higher repetition rate, but a lower coherence time. The latter is the main reason why the cut-off distance is shorter in Fig. 3.3(d) compared with Fig. 3.3(a).

Note that it may not be possible to use a memory-based system continuously for a long period of time without applying certain calibrations or cooling techniques. This could reduce the time available for data collection, reducing the effective block size for an MA-QKD system. One key technique that may mitigate this problem in the setup considered in this work is the delayed writing procedure, in which we only attempt to interact with the memory if the corresponding side-BSM is successful. This means that the memory is kept in a ready-to-go initial state until we know a photon has survived the path loss, in which case its state is teleported to the memory. Given that at long distances the chance of the latter event is low, this suggests that the external interaction with the memory is not that frequent, and the time between any two such events can be used to bring the memory back to a solid initial state. In the case of

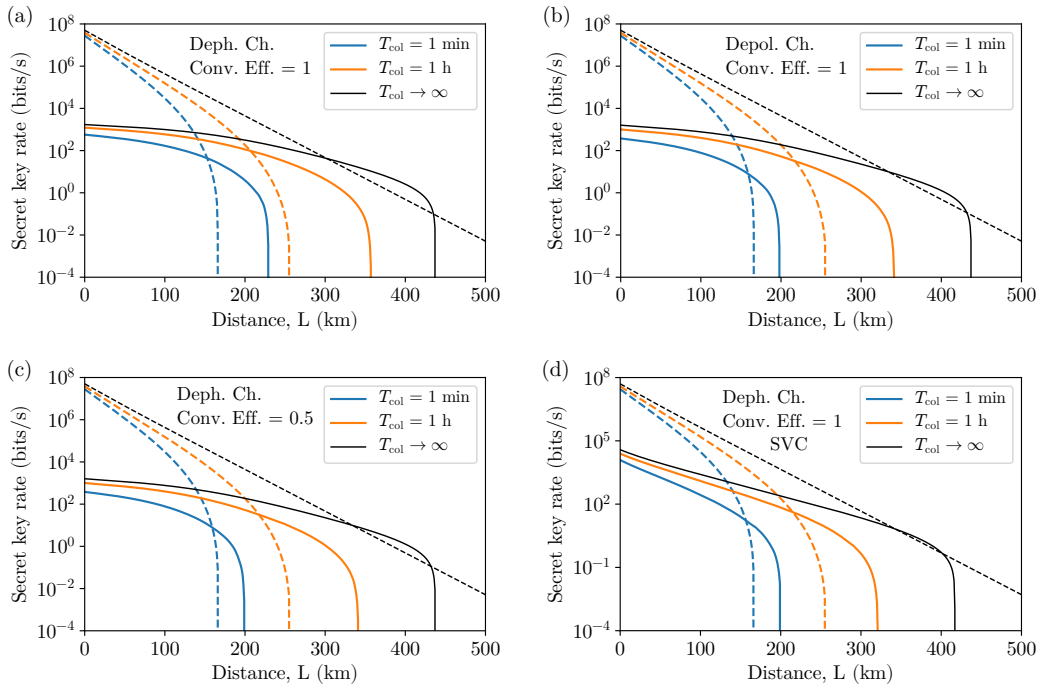


Figure 3.3: Secret key generation rate, in b/s, for a MA-QKD setup (solid lines) using (a)–(c) cold atom quantum memories, reported in [25], and (d) silicon vacancy centres, reported in [11], in comparison with no-memory MDI-QKD (dashed lines), if we collect data for one minute (blue), one hour (orange), or with no time limit (black). In (a), (c), and (d) a dephasing channel is used to model memory decoherence, whereas, in (b), a depolarisation channel is used. The efficiency of the frequency converter is assumed ideal in (a), (b), and (d), whereas, in (c), it is 50%.

memories reported in [24] and [25], we also have the additional advantage that after reading the memory, it automatically goes back to its initial state. Nevertheless, it is easy in our analysis to consider the effect of possible interruptions in data collection by modifying the block size. For instance, for CA ensembles, we have verified that the advantage shown in Fig. 3.3(a) will remain even if we can only collect data a quarter of the experiment time.

Finally, we have looked at how different system parameters can affect the conclusion we draw above. In Fig. 3.2(b) and Fig. 3.3(b), we have used a depolarising channel to model the decoherence effect. In comparison to Fig. 3.2(a) and Fig. 3.3(a), where a dephasing model is used, we see that the warm vapour system, which has lower T_2

values, is more adversely affected than the cold atom system. We observe the same behaviour when we change the frequency converter efficiency from one to to 0.5 as can be seen in Fig. 3.2(c) and Fig. 3.3(c). This can simply be a ramification of having noisier data in the case of warm vapours as compared to the cold atom case. This would result in less tight bounds on system parameters at the same block size or collection time, hence sharper drop in key rates. The overall effect would nevertheless suggest that MA-QKD systems can offer competitive performances in the finite-key regime irrespective of the memory or other relevant system parameters. This would be an essential observation in the early demonstrations of memory-based systems and how we benchmark them against their rival counterparts.

3.6 Conclusions

By borrowing ideas from quantum repeaters, MA-QKD can improve the scaling of repeaterless QKD systems. However, the common imperfections in memory-based systems such as their coupling efficiency to photonic systems, or their finite coherence times, may make it difficult for them to offer any practical advantage as compared to their no-memory counterparts. In particular, previous analyses suggest that any advantage in the total key rate would often come only after a crossover distance that is still challenging to implement experimentally. In this work, we showed that once we considered the finite-key effects in the key rate analysis, the crossover distance in such systems was reduced to a point that an experimental implementation could be foreseen in the near future. This effect was attributed to two features of decoy-state MA-QKD systems. First is their ability to purify some of the errors that result from multi-photon terms in weak laser pulses, and the other relates to a more efficient sifting of signal and decoy states. It is essential, however, for MA-QKD systems to keep all sources of noise near the memory units low, as they otherwise would translate into erroneous measurements in the middle site. As such are the multiple excitation terms in the memories, or sources that drive them, or additional background noise that may enter the setup. All these issues are manageable with careful design and they are all precursors to implementing longer quantum communications links relying on quantum memory units. In particular, we believe that the results of this work would be applicable to possible architectures for future quantum networks, in which end users are only equipped with

simple equipment, such as decoy-state BB84 encoders, but the core of the network has advanced memory-based repeater chains [31].

We should note that there are no-memory QKD systems, such as twin-field (TF) QKD [10], that offer a similar rate-vs-distance scaling as MA-QKD, and they have already been implemented at record distances [28]. An MA-QKD system may not be currently able to offer higher key rates or reach longer distances than those achieved by TF-QKD systems. But, it is important to recognise that the expertise and skills in both MA-QKD and TF-QKD would be required to implement scalable quantum repeater systems that go beyond the current rate-versus-distance records. In this respect, this work makes us one step closer to the final goal of implementing long-distance quantum communications systems.

Acknowledgements

We thank William Munro and Koji Azuma for valuable discussions. This work was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement number 675662 (QCALL). All data generated can be reproduced by the equations and the methodology introduced in this paper.

3.A Simulation model

In this appendix, we describe our simulation model, starting with our analysis of the indirect-loading of QMs with attenuated laser sources. Here, we assume that Charlie is honest, there is no eavesdropper, and we are only interested in finding the relevant parameters in a realistic setting.

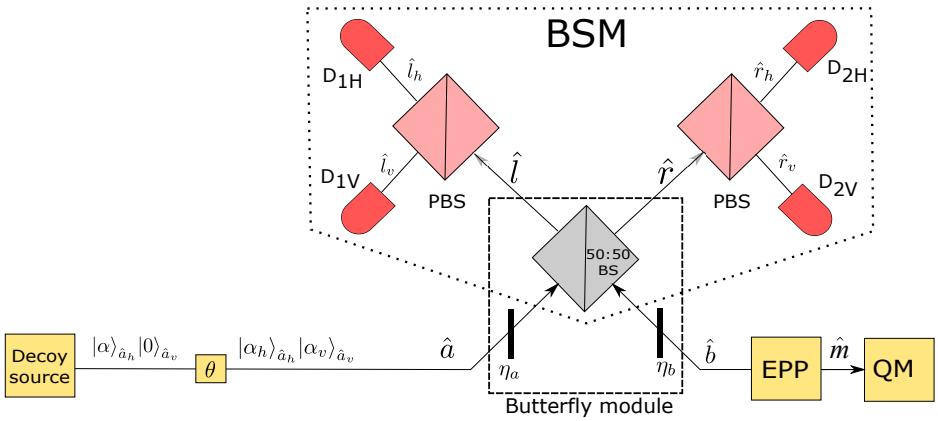


Figure 3.4: Loading of a QM with a Z-encoded weak coherent pulse, in a round with a misalignment angle of θ. The module in the dotted box represents a partial Bell-state measurement (BSM) on polarisation-encoded photons. We refer to the module in the dashed box as the butterfly module, in which η_a models the channel transmissivity and the quantum efficiency of a single-photon detector, whereas η_b captures the coupling and frequency conversion efficiencies as well as the quantum efficiency of a single-photon detector. The quantum efficiency of photodetectors in the BSM module is then assumed to be one.

Figure 3.4 shows a schematic view of our memory loading model for a single user, say Alice, in the polarisation encoding case. We model the loss in the channel, the measurement devices, and possible frequency converters as two beam splitters of transmissivity $\eta_a = \eta_{\text{ch}}\eta_d$ and $\eta_b = \eta_c\eta_d$ located at each input port of the 50:50 beam splitter of the BSM module. Here, η_{ch} models the transmissivity of the Alice-Charlie channel, η_c models the frequency conversion and/or coupling efficiency, and η_d represents the efficiency of the single-photon detectors. Note that by assuming the same efficiency η_d for all detectors, we are able to analyse its effects at the input ports of the BSM, simplifying our model. We do not need to consider the effect of the QM's writing effi-

ciency, η_w, at the loading stage. Instead, we modify the reading efficiency η_r by an η_w factor, allowing us to analyse its effect at the reading stage. In Fig. 3.4, the EPP source is assumed to generate an ideal entangled state in the form $\frac{1}{\sqrt{2}}(|HH\rangle_{\hat{b}\hat{m}} + |VV\rangle_{\hat{b}\hat{m}})$, where $\hat{b}$ and $\hat{m}$, respectively, represent the two output modes of the EPP source heading toward the BSM module and the QM.

We also consider setup misalignment between the user sources and the central node, which, in polarisation encoding, we model as a random rotation of the horizontal and vertical modes. For simplicity, we assume that the rotation angle θ is independent and identically distributed between different rounds of the protocol, and for the two legs of the system. Also, we assume that polarisation maintenance schemes are in place, so that the reference frames at the user sources and the central node are the same on average. It is reasonable then to assume, as we do in this work, that the probability density function (PDF) $f(\theta)$ is an even function of θ. One can use a similar formulation when other types of encoding, e.g. time-bin, are used.

In the following, in Sec. 3.A.1, we first find the post-measurement state of the loaded memory, the loading probability, and the its corresponding error rate under above considerations. The particular issue of misalignment turns out to complicate the analysis when we use weak laser pulses (WCPs) as compared to single-photon sources. Previous analyses of MA-QKD either assume no channel misalignment [8, 12] or model it as an error probability e_{mis} [7, 20], which is effectively given by $\int_{-\pi}^{\pi} f(\theta)\sin^2(\theta)\mathrm{d}\theta$. In our case, while the analysis is more cumbersome, the end result, in terms of the form of the post-measurement state of the QM, is similar to the single-photon case. This allows us to replicate most of the analysis in [7] in Sec. 3.A.2, and extend it to the case of depolarisation channels. In the last section of this Appendix, we have summarised the key rate relationships used for the no-QM MDI-QKD as a reference point.

3.A.1 Memory loading

Here, we calculate the post-measurement state of the QM, its loading probability and error rate, in the two cases of Z and X bases.

3.A.1.1 Analysis for Z basis

Without loss of generality, let us consider the case that the user generates a horizontally polarised WCP of intensity μ. Ideally, the state generated is of the form $|\alpha\rangle_{\hat{a}_h}|0\rangle_{\hat{a}_v}$,

where $\alpha = \sqrt{\mu}$ and $\hat{a}_h$ and $\hat{a}_v$ represent, respectively, the horizontal and vertical modes of the transmitted light in Fig. 3.4. In a particular round with a misalignment angle of θ, the misaligned state, at the input of the butterfly module, is given by

$$|\psi\rangle_{\hat{a}}^{\theta} = |\alpha_h\rangle_{\hat{a}_h} |\alpha_v\rangle_{\hat{a}_v} , \tag{3.6}$$

where $\alpha_h = \alpha \cos\theta$ and $\alpha_v = \alpha \sin\theta$. Meanwhile, the joint state of the two output modes of the EPP source, i.e., $\hat{b}$ and $\hat{m}$, is given by

$$\left|\Phi^+\right\rangle_{\hat{b}\hat{m}} = \tfrac{1}{\sqrt{2}}(|HH\rangle_{\hat{b}\hat{m}} + |VV\rangle_{\hat{b}\hat{m}}) = \tfrac{1}{\sqrt{2}}(|10H\rangle_{\hat{b}_h\hat{b}_v\hat{m}} + |01V\rangle_{\hat{b}_h\hat{b}_v\hat{m}}), \tag{3.7}$$

where in the last equality, we have divided $\hat{b}$ into, respectively, horizontal and vertical modes $\hat{b}_h$ and $\hat{b}_v$. After reordering modes, and averaging over θ, the joint input state to the butterfly module is given by

$$\hat{\rho}_{\text{in}} = \int_{-\pi}^{\pi} f(\theta) \hat{\rho}_{\text{in}}^{\theta} \mathrm{d}\theta, \tag{3.8}$$

where

$$\begin{aligned} \hat{\rho}_{\text{in}}^{\theta} = |\psi\rangle_{\hat{a}}^{\theta}\langle\psi| \otimes \left|\Phi^+\right\rangle_{\hat{b}\hat{m}}\left\langle\Phi^+\right| = &\frac{1}{2} |\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h} |1\rangle\langle 1|_{\hat{b}_h} |\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v} |0\rangle\langle 0|_{\hat{b}_v} |H\rangle\langle H|_{\hat{m}} \\ &+ \frac{1}{2} |\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h} |0\rangle\langle 0|_{\hat{b}_h} |\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v} |1\rangle\langle 1|_{\hat{b}_v} |V\rangle\langle V|_{\hat{m}} \\ &+ \frac{1}{2} |\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h} |1\rangle\langle 0|_{\hat{b}_h} |\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v} |0\rangle\langle 1|_{\hat{b}_v} |H\rangle\langle V|_{\hat{m}} \\ &+ \frac{1}{2} |\alpha_h\rangle\langle\alpha_h|_{\hat{a}_h} |0\rangle\langle 1|_{\hat{b}_h} |\alpha_v\rangle\langle\alpha_v|_{\hat{a}_v} |1\rangle\langle 0|_{\hat{b}_v} |V\rangle\langle H|_{\hat{m}} , \end{aligned} \tag{3.9}$$

and $|\psi\rangle\langle\psi|_{\hat{a}}$ is our shorthand notation for $|\psi\rangle_{\hat{a}\hat{a}}\langle\psi|$.

We are interested in the state projected to the QM after a successful loading, i.e., when exactly an H detector and a V detector click in the BSM module. To model this measurement process, we should find the output state of the butterfly module, with an input state as in Eq. (3.8), and then find the post-measurement state for the desired measurement outcome. The key to calculate this is to realise that the horizontal and vertical modes will interact separately at the 50:50 beam splitter of the butterfly module, and will cause clicks in the horizontal and vertically polarised detectors, respectively. Thus, we can split the overall transformation $\hat{B}$ for the butterfly module in Fig. 3.4, and the overall POVM operator $\hat{M}$ in horizontal and vertical operators as

follows:

$$\hat{B} = \hat{B}_h \otimes \hat{B}_v \tag{3.10}$$

$$\hat{M} = \hat{M}_h \otimes \hat{M}_v. \tag{3.11}$$

Here, the butterfly operators $\hat{B}_h$ and $\hat{B}_v$ in Fig. 3.4 only differ in their input and output modes: $\hat{B}_h$ will take modes $\hat{a}_h$ and $\hat{b}_h$ to modes $\hat{l}_h$ and $\hat{r}_h$, while $\hat{B}_v$ will take modes $\hat{a}_v$ and $\hat{b}_v$ to modes $\hat{l}_v$ and $\hat{r}_v$. The measurement operators (POVMs) are also identical for both the horizontal and vertical modes, and are given by

$$\begin{aligned}\hat{M}_x = (1-p_{\mathrm{dc}}) \left[\left(\hat{I}_{\hat{l}_x} - (1-p_{\mathrm{dc}}) \left|0\right\rangle\!\left\langle 0\right|_{\hat{l}_x} \right) \otimes \left|0\right\rangle\!\left\langle 0\right|_{\hat{r}_x} \right] \\ + (1-p_{\mathrm{dc}}) \left[\left|0\right\rangle\!\left\langle 0\right|_{\hat{l}_x} \otimes \left(\hat{I}_{\hat{r}_x} - (1-p_{\mathrm{dc}}) \left|0\right\rangle\!\left\langle 0\right|_{\hat{r}_x} \right) \right],\end{aligned} \tag{3.12}$$

for $x \in \{h, v\}$, where $\hat{I}$ is the identity operator for the corresponding mode. $\hat{M}_x$ represents the event of getting a click in the x-polarised left detector and no click on the x-polarised right detector, or vice-versa.

Using the above notation, the post-measurement state of the QM, after a successful loading, is given by

$$\hat{\rho}_{\hat{m}} = \frac{\mathrm{Tr}_{\hat{l}_h,\hat{l}_v,\hat{r}_h\hat{r}_v}\left[\hat{B}^\dagger \hat{\rho}_{\mathrm{in}} \hat{B} \hat{M}\right]}{\mathrm{Tr}\left[\hat{B}^\dagger \hat{\rho}_{\mathrm{in}} \hat{B} \hat{M}\right]} = \frac{1}{p^{\mu}_{\mathrm{load}}} \int_{-\pi}^{\pi} f(\theta) \mathrm{Tr}_{\hat{l}_h,\hat{l}_v,\hat{r}_h\hat{r}_v}\left[\hat{B}^\dagger \hat{\rho}^{\theta}_{\mathrm{in}} \hat{B} \hat{M}\right] \mathrm{d}\theta \tag{3.13}$$

where

$$\mathrm{Tr}_{\hat{l}_h,\hat{l}_v,\hat{r}_h\hat{r}_v}\left[\hat{B}^\dagger \hat{\rho}^{\theta}_{\mathrm{in}} \hat{B} \hat{M}\right] = c_{HH}(\theta) \left|H\right\rangle\!\left\langle H\right| + c_{VV}(\theta) \left|V\right\rangle\!\left\langle V\right| + c_{HV}(\theta) \left|H\right\rangle\!\left\langle V\right| + c_{VH}(\theta) \left|V\right\rangle\!\left\langle H\right|, \tag{3.14}$$

with

$$\begin{aligned} c_{HH}(\theta) &= \frac{1}{2} \mathrm{Tr}\left[\hat{B}_h^\dagger \left|\alpha_h\right\rangle\!\left\langle\alpha_h\right|_{\hat{a}_h} \left|1\right\rangle\!\left\langle 1\right|_{\hat{b}_h} \hat{B}_h \hat{M}_h\right] \mathrm{Tr}\left[\hat{B}_v^\dagger \left|\alpha_v\right\rangle\!\left\langle\alpha_v\right|_{\hat{a}_v} \left|0\right\rangle\!\left\langle 0\right|_{\hat{b}_v} \hat{B}_v \hat{M}_v\right] \\ c_{VV}(\theta) &= \frac{1}{2} \mathrm{Tr}\left[\hat{B}_h^\dagger \left|\alpha_h\right\rangle\!\left\langle\alpha_h\right|_{\hat{a}_h} \left|0\right\rangle\!\left\langle 0\right|_{\hat{b}_h} \hat{B}_h \hat{M}_h\right] \mathrm{Tr}\left[\hat{B}_v^\dagger \left|\alpha_v\right\rangle\!\left\langle\alpha_v\right|_{\hat{a}_v} \left|1\right\rangle\!\left\langle 1\right|_{\hat{b}_v} \hat{B}_v \hat{M}_v\right] \\ c_{HV}(\theta) &= \frac{1}{2} \mathrm{Tr}\left[\hat{B}_h^\dagger \left|\alpha_h\right\rangle\!\left\langle\alpha_h\right|_{\hat{a}_h} \left|1\right\rangle\!\left\langle 0\right|_{\hat{b}_h} \hat{B}_h \hat{M}_h\right] \mathrm{Tr}\left[\hat{B}_v^\dagger \left|\alpha_v\right\rangle\!\left\langle\alpha_v\right|_{\hat{a}_v} \left|0\right\rangle\!\left\langle 1\right|_{\hat{b}_v} \hat{B}_v \hat{M}_v\right] \\ c_{VH}(\theta) &= \frac{1}{2} \mathrm{Tr}\left[\hat{B}_h^\dagger \left|\alpha_h\right\rangle\!\left\langle\alpha_h\right|_{\hat{a}_h} \left|0\right\rangle\!\left\langle 1\right|_{\hat{b}_h} \hat{B}_h \hat{M}_h\right] \mathrm{Tr}\left[\hat{B}_v^\dagger \left|\alpha_v\right\rangle\!\left\langle\alpha_v\right|_{\hat{a}_v} \left|1\right\rangle\!\left\langle 0\right|_{\hat{b}_v} \hat{B}_v \hat{M}_v\right], \end{aligned} \tag{3.15}$$

and

$$p^{\mu}_{\mathrm{load}} = \mathrm{Tr}\left[\hat{B}^\dagger \hat{\rho}_{\mathrm{in}} \hat{B} \hat{M}\right] = \int_{-\pi}^{\pi} f(\theta)[c_{HH}(\theta) + c_{VV}(\theta)] \mathrm{d}\theta \tag{3.16}$$

is the probability of a successful loading for a WCP with intensity μ.

Every individual trace term in Eq. (3.15) involves either horizontal or vertical modes, and is equivalent to the probability of having exactly one detector click in the corresponding polarisation. Such terms have already been calculated in Table III of [31], which here we reuse, after making necessary adjustments, to obtain

$$\begin{aligned}
c_{HH}(\theta) &= (1-p_{\mathrm{dc}})^2\left(1-\mathrm{e}^{-1/2\,\eta_a\left(\sin^2\theta\right)\mu}\,(1-p_{\mathrm{dc}})\right)\times \\
&\quad\left(\left(\eta_b\,\left(\cos^2\theta\right)\mu\,\eta_a-2\,\eta_b+4\right)\mathrm{e}^{1/2\,\eta_a\left(\cos^2\theta\right)\mu}-4\,(1-\eta_b)\,(1-p_{\mathrm{dc}})\right)\mathrm{e}^{-1/2\,\eta_a\,\mu\left(\left(\cos^2\theta\right)+1\right)}, \\
c_{VV}(\theta) &= (1-p_{\mathrm{dc}})^2\Big[(1-p_{\mathrm{dc}})\left(\eta_b\,\cos^2\theta\mu\,\eta_a-\eta_b\,\eta_a\,\mu+2\,\eta_b-4\right)\mathrm{e}^{-1/2\,\eta_a\,\mu\left(\cos^2\theta+1\right)} \\
&\quad-4\,(1-\eta_b)\,(1-p_{\mathrm{dc}})\,\mathrm{e}^{1/2\,\eta_a\,\mu\left(\cos^2\theta-2\right)}-\left(\eta_b\,\cos^2\theta\mu\,\eta_a-\eta_b\,\eta_a\,\mu+2\,\eta_b-4\right)\mathrm{e}^{-1/2\,\eta_a\,\mu} \\
&\quad+4\,\mathrm{e}^{-\eta_a\,\mu}\,(-1+p_{\mathrm{dc}})^2\,(1-\eta_b)\Big],
\end{aligned} \tag{3.17}$$

and

$$c_{HV}(\theta)=c_{VH}(\theta)=\frac{1}{4}\cos\theta\sin\theta(1-p_{\mathrm{dc}})^2(\eta_a\eta_b\mu e^{-\eta_a\mu}). \tag{3.18}$$

It is interesting that, in the above, the diagonal terms c_{HV} and c_{VH} are odd functions of θ. Under our assumption that $f(\theta)$ is an even function, we have that

$$\int_{-\pi}^{\pi} f(\theta)c_{HV}(\theta)\mathrm{d}\theta=\int_{-\pi}^{\pi} f(\theta)c_{VH}(\theta)\mathrm{d}\theta=0, \tag{3.19}$$

implying that these terms vanish when considering the average post-measurement state $\hat{\rho}_{\hat{m}}$ in Eq. (3.13). Thus, $\hat{\rho}_{\hat{m}}$ can be expressed as

$$\rho_{\hat{m}}=e^{\mu}_{\mathrm{load}}\,|H\rangle\langle H|+(1-e^{\mu}_{\mathrm{load}})\,|V\rangle\langle V|\,, \tag{3.20}$$

where

$$e^{\mu}_{\mathrm{load}}=\frac{1}{p^{\mu}_{\mathrm{load}}}\int_{-\pi}^{\pi} f(\theta)c_{HH}(\theta)\mathrm{d}\theta \tag{3.21}$$

is the probability of loading the memory with the wrong state. In our case, when we send H-polarised light, a successful BSM in Fig. 3.4 suggests that the $\hat{b}$ mode is V-polarised. The state stored in the memory, for an EPP source with $|\Phi^+\rangle_{\hat{b}\hat{m}}$ as its initial state, is then also expected to be V-polarised. That is why the coefficient for $|H\rangle\langle H|$, in Eq. (3.20), represents the loading error probability, in Z basis, for a WCP with intensity μ.

Due to the symmetry of the setup, if the user sends vertically polarised light, the loading probability p^{μ}_{load} would be the same, but the post-measurement state is given by $\rho_{\hat{m}}=(1-e^{\mu}_{\mathrm{load}})\,|H\rangle\langle H|+e^{\mu}_{\mathrm{load}}\,|V\rangle\langle V|$.

3.A.1.2 Analysis for X basis

Without loss of generality, let us assume that Alice generates the plus state given by

$$\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\hat{a}_h}\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\hat{a}_v}. \tag{3.22}$$

In a particular round with a misalignment angle θ, the butterfly module will receive the state

$$|\psi\rangle_{\hat{a}}^{\theta}=\left|\frac{\alpha}{\sqrt{2}}(\sin\theta+\cos\theta)\right\rangle_{\hat{a}_h}\left|\frac{\alpha}{\sqrt{2}}(\sin\theta-\cos\theta)\right\rangle_{\hat{a}_v}, \tag{3.23}$$

while the output state of the EPP source can be written as

$$\left|\Phi^{+}\right\rangle_{\hat{b}\hat{m}}=\tfrac{1}{\sqrt{2}}(|DD\rangle_{\hat{b}\hat{m}}+|AA\rangle_{\hat{b}\hat{m}})=\tfrac{1}{\sqrt{2}}\left((|10\rangle+|01\rangle)\left|D\right\rangle+(|10\rangle-|01\rangle)\left|A\right\rangle\right))_{\hat{b}_h\hat{b}_v\hat{m}}, \tag{3.24}$$

where $|D\rangle=(|H\rangle+|V\rangle)/\sqrt{2}$ and $|A\rangle=(|H\rangle-|V\rangle)/\sqrt{2}$.

The analysis is similar to the one for the Z basis. After going through similar steps, we find that the probability to successfully load the memory is given by

$$\begin{aligned}p_{\text{load}}^{\mu}=\int_{-\pi}^{\pi}f(\theta)\frac{1}{2}\,(1-p_{\text{dc}})^{2}\Big(&(1-p_{\text{dc}})\left(\cos\theta\sin\left(\theta\right)\mu\eta_a\,\eta_b-1/2\,\eta_b\,\mu\eta_a+6\,\eta_b-8\right)\\&\mathrm{e}^{-1/2\,\eta_a\,\mu(\cos\theta\sin(\theta)+3/2)}-(1-p_{\text{dc}})\left(\cos\theta\sin\left(\theta\right)\mu\eta_a\,\eta_b+1/2\,\eta_b\,\mu\eta_a-6\,\eta_b+8\right)\\&\mathrm{e}^{\eta_a\,\mu(2\,\cos(\theta)\sin(\theta)-3)/4}+\left(\eta_b\,\mu\eta_a-4\,\eta_b+8\right)\mathrm{e}^{-\eta_a\,\mu/2}+8\,\mathrm{e}^{-\eta_a\,\mu}\left(1-p_{\text{dc}}\right)^{2}\left(1-\eta_b\right)\Big)\mathrm{d}\theta,\end{aligned} \tag{3.25}$$

and, under our assumption that $f(\theta)$ is even, the post-measurement state of the memory can be written as

$$\rho_{\hat{m}}=e_{\text{load}}^{\mu}\left|D\right\rangle\!\left\langle D\right|+(1-e_{\text{load}}^{\mu})\left|A\right\rangle\!\left\langle A\right|, \tag{3.26}$$

where

$$\begin{aligned}e_{\text{load}}^{\mu}=\frac{1}{p_{\text{load}}^{\mu}}\int_{-\pi}^{\pi}f(\theta)\frac{1}{4}\,(-1+p_{\text{dc}})^{2}\Big(&(1-p_{\text{dc}})\left(\cos\left(\theta\right)\sin\left(\theta\right)\mu\eta_a\,\eta_b-\eta_b\,\mu\eta_a/2+6\,\eta_b-8\right)\\&\mathrm{e}^{-1/2\,\eta_a\,\mu(\cos(\theta)\sin(\theta)+3/2)}-(1-p_{\text{dc}})\left(\cos\left(\theta\right)\sin\left(\theta\right)\mu\eta_a\,\eta_b+1/2\,\eta_b\,\mu\eta_a-6\,\eta_b+8\right)\\&\mathrm{e}^{1/4\,\eta_a\,\mu(2\,\cos(\theta)\sin(\theta)-3)}+\left(2\,\eta_b\,\mu\eta_a-2\,\left(\cos^{2}\theta\right)\mu\eta_a\,\eta_b-4\,\eta_b+8\right)\mathrm{e}^{-1/2\,\eta_a\,\mu}\\&+8\,\mathrm{e}^{-\eta_a\,\mu}\left(1-p_{\text{dc}}\right)^{2}\left(1-\eta_b\right)\Big)\mathrm{d}\theta.\end{aligned} \tag{3.27}$$

Finally, note that we calculate the integrals in Eqs. (3.16), (3.21), (3.25) and (3.27) numerically as a closed form expression for them could not be found. In our simulations,

to compute p^{μ}_{load} and e^{μ}_{load}, we assume that $f(\theta)$ follows a uniform distribution over $[-\Theta, \Theta]$. To have a fair comparison with no-memory MDI-QKD, we choose $\Theta = \sqrt{3e_{\text{mis}}}$, where e_{mis} is the misalignment error probability in one leg of a symmetric MDI-QKD setup. This is motivated by the fact that

$$\frac{1}{2\sqrt{3e_{\text{mis}}}} \int_{-\sqrt{3e_{\text{mis}}}}^{\sqrt{3e_{\text{mis}}}} \sin^2\theta \mathrm{d}\theta \approx \frac{1}{2\sqrt{3e_{\text{mis}}}} \int_{-\sqrt{3e_{\text{mis}}}}^{\sqrt{3e_{\text{mis}}}} \theta^2 \mathrm{d}\theta = e_{\text{mis}}, \tag{3.28}$$

which implies that the chosen $f(\theta)$ would cause a misalignment error of approximately e_{mis} in the MDI-QKD setup.

3.A.2 Key rate simulation

In Sec. 3.A.1, we showed that the post-measurement QM state after a successful loading is a mixture of the desired and undesired states for the QM; see Eq. (3.20) and Eq. (3.26). In effect, it is as if the state of QM has flipped with a probability e^{μ}_{load}. This is similar to how misalignment acts on a single photon state, because of which we can think of the whole loading process as a channel with an effective misalignment of e^{μ}_{load}. This would also make it possible to use the methodology in Ref. [7] to calculate the required parameters of the key rate formula. In particular, the photonic states retrieved from the two QMs turn out to also have a similar form to a misaligned photon, although at a higher error rate to account for the dephasing/depolarisation process.

In the following, we explain how to simulate all terms in the key-rate formula, in both the asymptotic and finite-key regimes. Given that in MA-QKD, one of the memories will be read immediately after loading, only one of the QMs would undergo the decay process. That implies that the middle BSM in Fig. 3.1 can be thought as an asymmetric MDI-QKD setup, with possibly different transmissivities η_l and η_r for, respectively, its left and right legs [7]. We can then use the yield and error rate formulas, summarised below, of asymmetric single-photon MDI-QKD for our rate calculation:

$$Y_{11}^{\text{MDI}}(\eta_l, \eta_r) = (1-p_d)^2 \left[\frac{\eta_l\eta_r}{2} + (2\eta_l + 2\eta_r - 3\eta_l\eta_r)p_d + 4(1-\eta_l)(1-\eta_r)p_d^2\right], \tag{3.29}$$

$$e_{11;X}^{\text{MDI}}(\eta_l, \eta_r, e_d) Y_{11}^{\text{MDI}}(\eta_l, \eta_r) = e_0 Y_{11}^{\text{MDI}}(\eta_l, \eta_r) - (e_0 - e_d)(1-p_d)^2\eta_l\eta_r/2, \tag{3.30}$$

$$e_{11;Z}^{\text{MDI}}(\eta_l, \eta_r, e_d) Y_{11}^{\text{MDI}}(\eta_l, \eta_r) = e_0 Y_{11}^{\text{MDI}}(\eta_l, \eta_r) - (e_0 - e_d)(1-p_d)^2(1-2p_d)\eta_l\eta_r/2, \tag{3.31}$$

where $e_0 = 1/2$ and e_d is the total misalignment probability in the asymmetric MDI-QKD setup, i.e., the probability that exactly one of the photons is misaligned.

3.A.2.1 Asymptotic regime

In this case, the key-rate formula is given by Eq. (3.3). In this regime, we assume that the signal intensity z, encoded in the Z-basis, is chosen with probability approaching one, and the parameter estimation provides perfect estimates of the single-photon terms Q_{11}^Z and e_{ph}. We only then need to simulate the values of Q_Z, e_Z, Q_{11}^Z and e_{ph} under nominal mode of operation. The procedure we use to calculate these terms is very similar to that of [7]. The main differences are our new model for the memory-loading with WCPs, developed earlier in this Appendix, and the inclusion of the depolarising channel for memory decoherence.

To compute Q_Z, we divide it into two parts: (1) the probability of having the two memories loaded and available to read in a given round, denoted by P_{side}, and (2) the probability that the middle BSM is successful, given that the QMs are ready, denoted by P_{mid}. Then,

$$Q_Z = P_{\text{side}} P_{\text{mid}}. \tag{3.32}$$

To find P_{side}, we first estimate the probability to load the QM with a Z-encoded WCP, given by p_{load}^z in Eq. (3.16). Then, we compute the average number of rounds N_L that it takes to load both memories, substituting η_A and η_B by p_{load}^z in Eq. (C.3) of [7], to obtain

$$N_L = \frac{3 - 2p_{\text{load}}^z}{p_{\text{load}}^z(2 - p_{\text{load}}^z)}. \tag{3.33}$$

Then, we have that

$$P_{\text{side}} = \frac{1}{N_L + N_r}. \tag{3.34}$$

where N_r is the number of rounds it takes to read the memory, which we assume to be one.

The second term is given by

$$P_{\text{mid}} = Y_{11}^{\text{MDI}}(\eta_m, \eta_{m'}), \tag{3.35}$$

where $\eta_m = \eta_w \eta_{r0} \eta_d$ is the effective reading efficiency of the QM loaded later, and $\eta_{m'}$ is the average effective reading efficiency of the QM loaded earlier, given by [7]

$$\eta_{m'} = \frac{(1 + e^{T/T_1} - p_{\text{load}}^z)p_{\text{load}}^z}{(2 - p_{\text{load}}^z)(e^{T/T_1} + p_{\text{load}}^z - 1)} \eta_m, \tag{3.36}$$

where T_1 is the time constant for the decay process of the QM.

The single-photon component Q_{11}^Z is given by

$$Q_{11}^Z = Q_Z \frac{(p_{\text{load}}^{\text{SP}})^2}{(p_{\text{load}}^z)^2} z^2 e^{-2z}, \tag{3.37}$$

where $p_{\text{load}}^{\text{SP}}$ is the probability to load the QM when a single photon is sent, given by [7]

$$p_{\text{load}}^{\text{SP}} = Y_{11}^{\text{MDI}}(\eta_{ch}\eta_d, \eta_c\eta_d). \tag{3.38}$$

To find e_{ph}, we first calculate the misalignment-error probability for loading the QM with an X-basis single photon, which is given by [7]

$$e_{\text{load}}^{X,\text{SP}} = e_{11;X}^{\text{MDI}}(\eta_{ch}\eta_d, \eta_c\eta_d, e_{\text{mis}}). \tag{3.39}$$

Then, we obtain

$$e_{\text{ph}} = e_{11;X}^{\text{MDI}}(\eta_m, \eta_m', \mathrm{E}\left\{e_{\text{QM}}^{\text{SP}}\right\}), \tag{3.40}$$

where $\mathrm{E}\left\{e_{\text{QM}}^{\text{SP}}\right\}$ is the total misalignment probability, given by

$$\mathrm{E}\left\{e_{\text{QM}}^{\text{SP}}\right\} = 2e_{\text{load}}^{X,\text{SP}} + 2\beta\mathrm{E}\left\{e_{\text{deph}}\right\} - 2e_{\text{load}}^{X,\text{SP}} e_{\text{load}}^{X,\text{SP}} - 4\beta\mathrm{E}\left\{e_{\text{deph}}\right\} e_{\text{load}}^{X,\text{SP}}, \tag{3.41}$$

with

$$\mathrm{E}\left\{e_{\text{deph}}\right\} = 1 - \frac{p_{\text{load}}^z}{1-(1-p_{\text{load}}^z)^2} - \frac{(p_{\text{load}}^z)^2(1-p_{\text{load}}^z e^{-T/T_2})}{[1-(1-p_{\text{load}}^z)e^{-T/T_2}][1-(1-p_{\text{load}}^z)^2]}, \tag{3.42}$$

in the case of dephasing memories, and by

$$\mathrm{E}\left\{e_{\text{QM}}^{\text{SP}}\right\} = 2e_{\text{load}}^{X,\text{SP}} + 2\beta\mathrm{E}\left\{e_{\text{depol}}\right\} - 2e_{\text{load}}^{X,\text{SP}} e_{\text{load}}^{X,\text{SP}} - 4\beta\mathrm{E}\left\{e_{\text{depol}}\right\} e_{\text{load}}^{X,\text{SP}}, \tag{3.43}$$

with

$$\mathrm{E}\left\{e_{\text{depol}}\right\} = \frac{2}{3}\mathrm{E}\left\{e_{\text{deph}}\right\}, \tag{3.44}$$

in the case of depolarising memories.

To calculate e_Z, we use

$$e_Z = e_{11;Z}^{\text{MDI}}(\eta_m, \eta_m', \mathrm{E}\left\{e_{\text{QM}}\right\}), \tag{3.45}$$

where $\mathrm{E}\left\{e_{\text{QM}}\right\}$ is the average total misalignment-error probability between the two QMs, which depends on the specific model used for decoherence. In the dephasing

model, the Z-basis QM states will not be affected by the decoherence, therefore, the probability that exactly one state is misaligned is as follows

$$\mathrm{E}\left\{e_{\mathrm{QM}}\right\} = e_{\mathrm{QM}} = 2e^z_{\mathrm{load}}(1 - e^z_{\mathrm{load}}), \tag{3.46}$$

where e^z_{load} is given by Eq. (3.21). For the depolarisation model, we have

$$\mathrm{E}\left\{e_{\mathrm{QM}}\right\} = 2e^z_{\mathrm{load}} + 2\beta\mathrm{E}\left\{e_{\mathrm{depol}}\right\} - 2e^z_{\mathrm{load}}e^z_{\mathrm{load}} - 4\beta\mathrm{E}\left\{e_{\mathrm{depol}}\right\}e^z_{\mathrm{load}}, \tag{3.47}$$

where $\beta = 1 - 2e^z_{\mathrm{load}}$.

To derive Eq. (3.47) and Eqs. (3.41) to (3.44), we have used a similar analysis as in Appendix D of Ref. [7].

3.A.2.2 Finite-key regime

In this case, we need to calculate the sets $\{M^{ab}\}$ and $\{E^{ab}\}$, where M^{ab} is the total number of measurement counts when Alice (Bob) has used intensity a (b), while E^{ab} is the number of such events that also result in an error. Note that intensity z is encoded in the Z basis and intensities $\{w_1, w_2, v\}$ are encoded in the X basis; we are only interested in estimating $\{M^{ab}\}$ and $\{E^{ab}\}$ when a, b are encoded in the same basis.

For our numerical simulations, we still need to make some assumptions on the obtained measurement results in a nominal experiment. For this purpose, we use the expected values for relevant parameters using the corresponding probability in the asymptotic regime. That is, we assume

$$M^{ab} = NQ^{ab} \quad \text{and} \quad E^{ab} = e_{ab}M^{ab}, \tag{3.48}$$

where N is the total number of rounds, i.e., the number of transmitted pulses by Alice/Bob, in the protocol, Q^{ab} is the probability of having a successful measurement originating from intensities a, for Alice, and b, for Bob, and e_{ab} is the probability that this measurement results in an error.

To calculate Q_{ab}, we first compute the total gain Q_{tot}, using the same procedure as for Q_Z in the asymptotic case, with the difference that Q_{tot} is now a function of the average memory-loading probability given by

$$\bar{p}_{\mathrm{load}} = \sum_a p_a p^a_{\mathrm{load}}, \tag{3.49}$$

where p_a is the probability of selecting intensity $a \in \{z, w_1, w_2, v\}$; and p^a_{load} is the probability of a successful loading when the user selects intensity a, given by either Eq. (3.21) or Eq. (3.27), depending on whether intensity a is encoded in the Z or X basis. Then, we have that

$$N_L = \frac{3 - 2\bar{p}_{\text{load}}}{\bar{p}_{\text{load}}(2 - \bar{p}_{\text{load}})}, \tag{3.50}$$

$$\eta_{m'} = \frac{(1 + e^{T/T_1} - \bar{p}_{\text{load}})\bar{p}_{\text{load}}}{(2 - \bar{p}_{\text{load}})(e^{T/T_1} + \bar{p}_{\text{load}} - 1)}\eta_m, \tag{3.51}$$

$$P_{\text{side}} = \frac{1}{N_L + N_r} \tag{3.52}$$

$$P_{\text{mid}} = Y_{11}^{\text{MDI}}(\eta_m, \eta_{m'}), \tag{3.53}$$

$$Q_{\text{tot}} = P_{\text{side}} P_{\text{mid}}, \tag{3.54}$$

where $N_r = 1$ and $\eta_m = \eta_w \eta_{r0} \eta_d$. Now, Q^{ab} is the fraction of Q_{tot} that originated from intensities a, b. Note that after a successful loading, the state projected to the QM is always a misaligned qubit. The probability that the middle BSM is successful only depends on the loss coefficients η_m and $\eta_{m'}$, and it is independent of the intensities a, b that caused the loading. Thus, Q^{ab} only depends on how likely intensities a, b are to cause a successful loading, that is,

$$Q^{ab} = Q_{\text{tot}} p_a p_b \frac{p^a_{\text{load}} p^b_{\text{load}}}{\bar{p}^2_{\text{load}}}. \tag{3.55}$$

For e_{ab}, we have that

$$e_{zz} = e^{\text{MDI}}_{11;Z}(\eta_m, \eta'_m, \mathrm{E}\left\{e^{\text{QM}}_{zz}\right\}), \tag{3.56}$$

$$e_{ab} = e^{\text{MDI}}_{11;X}\left(\eta_m, \eta'_m, \mathrm{E}\left\{e^{\text{QM}}_{ab}\right\}\right), \quad a, b \in \{w_1, w_2, v\} \tag{3.57}$$

where $\mathrm{E}\left\{e^{\text{QM}}_{ab}\right\}$ is the total average misalignment error probability between the two QMs, and depends on whether one considers a dephasing or depolarisation model. The former has no effect on Z-basis states, and therefore

$$\mathrm{E}\left\{e^{\text{QM}}_{zz}\right\} = e^{\text{QM}}_{zz} = 2e^z_{\text{load}}(1 - e^z_{\text{load}}). \tag{3.58}$$

For the X-basis intensities, we have that

$$\begin{aligned}\mathrm{E}\left\{e^{\text{QM}}_{ab}\right\} = {} & e^a_{\text{load}} + e^b_{\text{load}} + \beta_a \mathrm{E}\left\{e_{\text{deph}}\right\} + \beta_b \mathrm{E}\left\{e_{\text{deph}}\right\} - 2e^a_{\text{load}} e^b_{\text{load}} \\ & - 2\beta_a \mathrm{E}\left\{e_{\text{deph}}\right\} e^b_{\text{load}} - 2\beta_b \mathrm{E}\left\{e_{\text{deph}}\right\} e^a_{\text{load}},\end{aligned} \tag{3.59}$$

where $\beta_k = 1 - 2e^k_{\text{load}}$, and

$$\mathrm{E}\left\{e_{\text{deph}}\right\} = 1 - \frac{\bar{p}_{\text{load}}}{1-(1-\bar{p}_{\text{load}})^2} - \frac{\bar{p}^2_{\text{load}}(1-\bar{p}_{\text{load}}e^{-T/T_2})}{[1-(1-\bar{p}_{\text{load}})e^{-T/T_2}][1-(1-\bar{p}_{\text{load}})^2]}, \tag{3.60}$$

using a similar analysis to the one that results in Eq. (D.8) of [7].

For a depolarisation channel, we have that, for all intensities

$$\begin{aligned}\mathrm{E}\left\{e^{\text{QM}}_{ab}\right\} = e^a_{\text{load}} + e^b_{\text{load}} + \beta_a \mathrm{E}\left\{e_{\text{depol}}\right\} + \beta_b \mathrm{E}\left\{e_{\text{depol}}\right\} - 2e^a_{\text{load}}e^b_{\text{load}} \\ - 2\beta_a \mathrm{E}\left\{e_{\text{depol}}\right\} e^b_{\text{load}} - 2\beta_b \mathrm{E}\left\{e_{\text{depol}}\right\} e^a_{\text{load}},\end{aligned} \tag{3.61}$$

where

$$\mathrm{E}\left\{e_{\text{depol}}\right\} = \frac{2}{3}\mathrm{E}\left\{e_{\text{deph}}\right\}. \tag{3.62}$$

3.A.3 MDI-QKD without QMs

Here, we give the formulas that we have used to simulate the no-memory MDI-QKD with WCP sources.

In general, if Alice and Bob encode in the Z basis and choose intensities a and b, respectively, the gain and error-rate formulas are given by [32]

$$Q^{ab} = Q_c + Q_e, \tag{3.63}$$

$$e_{ab} = e_d Q_c + (1-e_d)Q_e, \tag{3.64}$$

where e_d represents the total misalignment error probability given by $e_d = 2e_{\text{mis}}(1-e_{\text{mis}})$, and

$$\begin{aligned}Q_c &= 2(1-p_d)^2 e^{-\zeta/2}(1-(1-p_d)e^{-\eta a/2})(1-(1-p_d)e^{-\eta b/2}) \\ Q_e &= 2p_d(1-p_d)^2 e^{-\zeta/2}[I_0(2x) - (1-p_d)e^{-\zeta/2}] \\ x &= \eta\sqrt{ab}/2 \\ \zeta &= \eta(a+b),\end{aligned} \tag{3.65}$$

where I_0 is the modified Bessel function of the first kind and $\eta = \eta_{\text{ch}}\eta_d$ is the total attenuation between each user and the middle node. If they encode in the X basis, they are given by [32]

$$Q^{ab} = 2y^2[1 + 2y^2 - 4yI_0(x) + I_0(2x)], \tag{3.66}$$

$$e_{ab} = \frac{Q^{ab}}{2} - (1-2e_d)y^2[I_0(2x) - 1], \tag{3.67}$$

where

$$y = (1-p_d)e^{-\zeta/4}. \tag{3.68}$$

3.A.3.1 Asymptotic regime

In the asymptotic regime, the key rate formula is given by

$$R \leq R_s \left[Q_{11}^Z \left(1 - h(e_{\text{ph}})\right) - f Q_Z h(e_Z) \right]. \tag{3.69}$$

Q_Z and e_Z are given by Eqs. (3.63) and (3.64), respectively, by substituting $a = b = z$. In the asymptotic regime, we assume that the users are able to obtain perfect estimates of Q_{11}^Z and e_{ph}, which are given by

$$Q_{11}^Z = z^2 e^{-2z} Y_{11}, \tag{3.70}$$

$$e_{\text{ph}} = e_{11;X}^{\text{MDI}}(\eta, \eta, e_d) = \frac{1}{2} - \frac{1}{Y_{11}}(1/2 - e_d)(1 - p_d)^2(1 - 2p_d)\frac{\eta^2}{2}, \tag{3.71}$$

where

$$Y_{11} = Y_{11}^{\text{MDI}}(\eta, \eta) = (1 - p_d)^2 \left[\frac{\eta^2}{2} + (4\eta - 3\eta^2)p_d + 4(1 - \eta)^2 p_d^2 \right]. \tag{3.72}$$

3.A.3.2 Finite-key regime

We need to simulate the sets $\{M^{ab}\}$ and $\{E^{ab}\}$. In our simulations, we assume that all measurement counts equal their expected values, that is,

$$M^{ab} = N p_{ab} Q^{ab} \quad \text{and} \quad E^{ab} = e_{ab} M^{ab}, \tag{3.73}$$

where Q_{ab} and e_{ab} are given by Eq. (3.63) and Eq. (3.64) for Z-encoded intensities, and by Eq. (3.66) and Eq. (3.67) for X-encoded intensities, and p_{ab} is the probability that Alice and Bob choose intensities a and b, respectively.

3.B Finite-key analysis

In this Appendix, we explain the detailed procedure for finding a lower bound on M_{11}^Z and an upper bound on e_{ph} in Eq. (3.4). For our finite-key analysis of MDI-QKD and MA-QKD, we use the analytical estimation procedure introduced in [17], together with the tighter multiplicative Chernoff bounds introduced in [16]. Also, as in [21], we estimate the total single photon measurement counts M_{11} in both bases using data in the X basis only. We then link it with M_{11}^{zz} via random sampling analysis. This allows us to encode decoy intensities in the X basis only, thus wasting fewer rounds for statistical estimation.

3.B.1 Background

In the protocol, Alice and Bob emit phase-randomised coherent states of a random intensity $a \in \{z, w_1, w_2, v\}$, where the z intensity is encoded in the Z basis and the rest of the intensities are encoded in the X basis. Without knowing the basis information, the output state corresponding to intensity a can be written as

$$\rho_a = \sum_{n=0}^{\infty} p_{n|a} \left|n\right\rangle\!\left\langle n\right|, \tag{3.74}$$

where $p_{n|a}$ is the probability that a pulse of intensity a contains n photons, and $|n\rangle$ is the n-photon Fock state. For weak laser pulses, we can typically assume a Poisson distribution for the photon number, in which case, $p_{n|a} = a^n e^{-a}/n!$. While most of our analysis does not depend on the choice of the probability distribution, we also use the Poisson assumption for our numerical results. Based on the above diagonal form, for a pulse encoded in a given basis, the only information available to Eve is its photon number n. This implies that, instead of the actual protocol, Alice and Bob could have run the equivalent *virtual* scenario in which

- Alice (Bob) sends a Z-encoded n-photon Fock state with probability $p_{n,Z} = p_z p_{n|z}$.
- Alice (Bob) sends an X-encoded n-photon Fock state with probability $p_{n,X} = \sum_{a\in\{w_1,w_2,v\}} p_a p_{n|a}$.

In this virtual scenario, Alice and Bob can wait until after Eve's attack to assign each emission of an X-encoded n-photon Fock state to intensity $a \in \{w_1, w_2, v\}$ with probability

$$p_{a|n,X} = \frac{p_a p_{n|a}}{p_{n,X}}, \tag{3.75}$$

and then "reveal" their intensity choices in the appropriate step of the protocol, so that Eve cannot tell which scenario (actual or virtual) is being performed.

Note that Fock states encoded in different bases are in general partially distinguishable to Eve, so Alice and Bob must decide their encoding basis before their emission, even in the virtual scenario. There is one important exception, however: single-photon signals encoded in either the X or Z bases are indistinguishable once averaged by their selection probabilities, since

$$\rho_1 = \frac{1}{2}\left|H\right\rangle\!\left\langle H\right| + \frac{1}{2}\left|V\right\rangle\!\left\langle V\right| = \frac{1}{2}\left|D\right\rangle\!\left\langle D\right| + \frac{1}{2}\left|A\right\rangle\!\left\langle A\right|. \tag{3.76}$$

This implies that the users could have replaced their single-photon emissions by the following purification of ρ_1

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|H\rangle + |1\rangle|V\rangle\right) = \frac{1}{\sqrt{2}}\left(|+\rangle|D\rangle + |-\rangle|A\rangle\right), \tag{3.77}$$

where the first qubit, in $|0\rangle$-$|1\rangle$ basis, is held by the users and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. This allows us to alter our virtual scenario in the following way: when Alice and Bob both decide to send a single-photon state, they replace their respective emissions by the generation of $|\psi_1\rangle$, and then wait until after Eve's attack to decide in which basis to measure their ancilla. This delayed basis choice will allow us to estimate the statistics of Z-encoded single-photon emissions using X-basis data.

3.B.2 Estimation of M_{11}^Z

The estimation is divided in two steps:

1. Estimation of M_{11}, the total single-photon measurement counts in both basis, using the decoy state analysis.

2. Estimation of M_{11}^Z from M_{11}, via a random sampling analysis.

3.B.2.1 Estimation of M_{11}

In our virtual scenario, the users have replaced their decoy-state emissions by Fock states, which are only assigned to a particular intensity after Eve's attack. Let $\mathcal{M}_{nm}^X$, with $(n,m) \neq (1,1)$, be the set of rounds in which Alice (Bob) chooses the X basis, sends n (m) photons, and Charlie reports a successful detection. Also, let $M_{nm}^X = \left|\mathcal{M}_{nm}^X\right|$. After her reports, Alice and Bob will assign each event in $\mathcal{M}_{nm}^X$ to intensities $a, b \in \{w_1, w_2, v\}$ with probability

$$p_{ab|nm,X} = p_{a|n,X}p_{b|m,X} = \frac{p_a p_{n|a}}{p_{n,X}}\frac{p_b p_{m|b}}{p_{m,X}}, \tag{3.78}$$

where $p_{n,X} = \sum_{a\in\{w_1,w_2,v\}} p_a p_{n|a}$ by the law of total probability. As explained above, Alice and Bob have also delayed their choice of basis on those rounds in which both sent a single photon. Let $\mathcal{M}_{11}$ be the set of rounds in which Alice and Bob sends a

single photon and Charlie reports a successful detection, and let $M_{11} = |\mathcal{M}_{11}|$. The probability that they assign each event in $\mathcal{M}_{11}$ to intensities $a, b \in \{z, w_1, w_2, v\}$ is

$$p_{ab|11} = p_{a|1} p_{b|1} = \frac{p_a p_{1|a}}{p_1} \frac{p_b p_{1|b}}{p_1} \tag{3.79}$$

where $p_1 = \sum_{a \in \{z, w_1, w_2, v\}} p_a p_{n|a}$ by the law of total probability. Let M^{ab} denote the number of rounds assigned to intensities $a, b \in \{w_1, w_2, v\}$. Its expected value is

$$\mathrm{E}[M^{ab}] = p_{ab|00,X} M_{00}^X + p_{ab|01,X} M_{01}^X + p_{ab|11} M_{11} + \sum_{(m,n) \in S} p_{ab|mn,X} M_{mn}^X, \tag{3.80}$$

where $S = \{(m,n) | m, n \in \mathbb{Z}, m, n \geq 0\} - \{(0,0), (0,1), (1,1)\}$. Each of these intensity assignments is a Bernoulli random variable, and therefore $\mathrm{E}[M^{ab}]$ is the average value of the sum of some Bernoulli random variables. The values of M^{ab} measured by Alice and Bob correspond to an instance of this sum of Bernoulli random variables.

Let $\chi = \sum_{i=1}^{n} \chi_i$ be the outcome of the sum of n independent Bernoulli random variables $\chi_i \in \{0, 1\}$. Given the observation of the outcome χ, its expectation value $E[\chi]$ can be bounded by [16]

$$\begin{aligned} \mathrm{E}^{\mathrm{L}}[\chi] &= \frac{\chi}{1 + \delta^{\mathrm{L}}}, \\ \mathrm{E}^{\mathrm{U}}[\chi] &= \frac{\chi}{1 - \delta^{\mathrm{U}}}, \end{aligned} \tag{3.81}$$

except with probability ϵ, where δ^{L} and δ^{U} are the solutions of the equations

$$\begin{aligned} \left[\frac{e^{\delta^{\mathrm{L}}}}{(1 + \delta^{\mathrm{L}})^{1 + \delta^{\mathrm{L}}}} \right]^{\chi/(1+\delta^{\mathrm{L}})} &= \frac{1}{2} \varepsilon \\ \left[\frac{e^{-\delta^{\mathrm{U}}}}{(1 - \delta^{\mathrm{U}})^{1 - \delta^{\mathrm{U}}}} \right]^{\chi/(1-\delta^{\mathrm{U}})} &= \frac{1}{2} \varepsilon. \end{aligned} \tag{3.82}$$

These solutions can be expressed in terms of the Lambert W function, the inverse of $f(z) = ze^z$, as follows

$$\begin{aligned} \delta^{\mathrm{L}} &= W_0(-e^{\ln(\varepsilon/2 - \chi)}/\chi) \\ \delta^{\mathrm{U}} &= W_{-1}(-e^{\ln(\varepsilon/2 - \chi)}/\chi), \end{aligned} \tag{3.83}$$

which is useful for their quick numerical computation.

We use Eq. (3.81) to find bounds on $E[M^{ab}]$, which by Eq. (3.80) will set constraints on the values of M_{nm}^X and M_{11}. Since we are interested in M_{11}^{L}, our analysis can be reformulated as the optimization problem: Find min M_{11} such that

$$\mathrm{E}^{\mathrm{L}}[M^{ab}] \leq p_{ab|00,X} M_{00}^{X} + p_{ab|01,X} M_{01}^{X} + p_{ab|11} M_{11} + \sum_{(m,n)\in S} p_{ab|mn,X} M_{mn}^{X} \leq \mathrm{E}^{\mathrm{U}}[M^{ab}] \tag{3.84}$$

$\forall a, b \in \{w_1, w_2, v\}$. This problem can be solved using linear optimisation techniques [17]. In this work, however, we use the computationally faster analytical estimation method laid out in the Supplementary Note 1 of [17], for Poisson distributed input signals. Note that to use this analytical method, one needs to define the term $\hat{M}_{11}^{X}$ such that

$$p_{ab|11} M_{11} = p_{ab|11,X} \hat{M}_{11}^{X}, \tag{3.85}$$

where $p_{ab|11,X}$ is given by Eq. (3.78), and substitute $p_{ab|11} M_{11}$ by $p_{ab|11,X} \hat{M}_{11}^{X}$ in Eq. (3.84). Then, one can use the results of [17] to find a lower bound on $\hat{M}_{11}^{X}$, and reuse Eq. (3.85) to turn it into a lower bound M_{11}^{L} on M_{11}.

3.B.2.2 Estimation of M_{11}^{Z} from M_{11}

Let $\mathcal{M}_{11}^{Z}$ be the subset of $\mathcal{M}_{11}$ in which both users employ the Z basis, and let $M_{11}^{Z} = \left|\mathcal{M}_{11}^{Z}\right|$. By the delayed basis argument, Alice and Bob could decide which events in $\mathcal{M}_{11}$ belong to $\mathcal{M}_{11}^{Z}$ after Eve's attack. They assign each event in $\mathcal{M}_{11}$ to $\mathcal{M}_{11}^{Z}$ with probability

$$p_{zz|11} = \left(\frac{p_z p_{1|z}}{p_1}\right)^2. \tag{3.86}$$

Let $\chi = \sum_{i=1}^{n} \chi_i$ be the outcome of the sum of n independent Bernoulli random variables $\chi_i \in \{0, 1\}$. Given the expectation value $E[\chi]$, the outcome χ can be lower-bounded by [16]

$$\begin{aligned} \chi &\geq \chi^{\mathrm{L}} = (1-\delta)\bar{\chi} \\ \delta &= \frac{-\ln(\varepsilon) + \sqrt{[\ln(\varepsilon)]^2 - 8\ln(\varepsilon)\bar{\chi}}}{2\bar{\chi}}, \end{aligned} \tag{3.87}$$

except with probability ε.

The lower bound on M_{11}^{Z} is then given by $(M_{11}^{Z})^{L} = (1-\delta)\bar{\chi}$, where $\bar{\chi} = p_{zz|11} M_{11}^{\mathrm{L}}$ and δ is given by Eq. (3.87).

3.B.3 Estimation of e_{ph}

The upper bound on e_{ph} is given by

$$e_{\text{ph}}^{\text{U}} = \frac{(E_{11}^{Z})^{\text{U}}}{(M_{11}^{Z})^{\text{L}}}, \tag{3.88}$$

where E_{11}^{Z} is the number of phase errors in $\mathcal{M}_{11}^{Z}$, that is, the number of bit errors that Alice and Bob would have obtained if they had encoded their Z basis single-photon emissions in the X basis. The estimation of this quantity is divided in two steps:

1. Estimation of E_{11}, the total amount of phase-flip errors in all single-photon emissions.

2. Estimation of E_{11}^{Z} from E_{11}, via a random sampling analysis.

3.B.3.1 Estimation of E_{11}

Let us imagine that, in the virtual scenario, Alice and Bob measure all their pairs of ancillas in $\mathcal{M}_{11}$ in the X basis, even those that they have assigned to $\mathcal{M}_{11}^{Z}$. Let $\mathcal{E}_{11}$ be the subset of $\mathcal{M}_{11}$ in which they find a phase-flip error, and let $E_{11} = |\mathcal{E}_{11}|$. Each event in $\mathcal{E}_{11}$ is assigned to intensity $a, b \in \{z, w_1, w_2, v\}$ with probability $p_{ab|11}$ defined in Eq. (3.79).

Also, let $\mathcal{E}_{nm}^{X}$, with $(n, m) \neq (1, 1)$, be the subset of $\mathcal{M}_{nm}^{X}$ in which Alice and Bob obtain a phase-flip error. Each event in $\mathcal{E}_{nm}^{X}$ is assigned to intensity $a, b \in \{w_1, w_2, v\}$ with probability $p_{ab|nm,X}$ defined in Eq. (3.78). For $a, b \in \{w_1, w_2, v\}$, the expected value of E_{ab} with respect to these assignments is

$$\text{E}[E^{ab}] = p_{ab|00,X} E_{00}^{X} + p_{ab|01,X} E_{01}^{X} + p_{ab|11} E_{11} + \sum_{(m,n)\in S} p_{ab|mn,X} E_{mn}^{X}. \tag{3.89}$$

From Eqs. (3.81)–(3.83), we obtain bounds $\text{E}^{\text{L}}[E^{ab}], \text{E}^{\text{U}}[E^{ab}]$, and redefine our analysis as the optimization problem: Find max E_{11} such that

$$\text{E}^{\text{L}}[E^{ab}] \leq p_{ab|00,X} E_{00}^{X} + p_{ab|01,X} E_{01}^{X} + p_{ab|11} E_{11} + \sum_{(m,n)\in S} p_{ab|mn,X} E_{mn}^{X} \leq \text{E}^{\text{U}}[E^{ab}], \tag{3.90}$$

$\forall a, b \in \{w_1, w_2, v\}$. Again, this problem can be solved using linear programming techniques, but we use the analytical estimation method in the Supplementary Note 1 of

[17]. Note that to use this analytical method, one needs to define a term $\hat{E}_{11}^{X}$ such that

$$p_{ab|11}E_{11} = p_{ab|11,X}\hat{E}_{11}^{X}, \tag{3.91}$$

where $p_{ab|11,X}$ is given by Eq. (3.78), and substitute $p_{ab|11}E_{11}$ by $p_{ab|11,X}\hat{E}_{11}^{X}$ in Eq. (3.90). Then, one can use the results of [17] to find an upper bound on $\hat{E}_{11}^{X}$, and reuse Eq. (3.91) to turn it into an upper bound E_{11}^{U} on E_{11}.

3.B.3.2 Estimation of E_{11}^{Z} from E_{11}

By the delayed basis argument, each event in E_{11} will be assigned to E_{11}^{Z} with probability $p_{zz|11}$, defined in Eq. (3.86).

Let $\chi = \sum_{i=1}^{n}\chi_i$ be the outcome of the sum of n independent Bernoulli random variables $\chi_i \in \{0,1\}$. Given the expectation value $E[\chi]$, the outcome χ can be upper-bounded by [16]

$$\begin{aligned} \chi &\leq \chi^{\mathrm{U}} = (1+\delta)\bar{\chi} \\ \delta &= \frac{-\ln(\varepsilon) + \sqrt{[\ln(\varepsilon)]^2 - 8\ln(\varepsilon)\bar{\chi}}}{2\bar{\chi}}, \end{aligned} \tag{3.92}$$

except with probability ε.

Finally, an upper bound on E_{11}^{Z} is given by $(E_{11}^{Z})^{\mathrm{U}} = (1+\delta)\bar{\chi}$, where $\bar{\chi} = p_{zz|11}E_{11}^{\mathrm{U}}$ and δ is given by Eq. (3.92).

References

[1] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, "Advances in quantum cryptography," *arXiv preprint arXiv:1906.01645*, 2019. 94

[2] N. Gisin, "How far can one send a photon?," *Frontiers of Physics*, vol. 10, no. 6, p. 100307, 2015. 94

[3] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Scientific reports*, vol. 6, p. 20463, 2016. 94

[4] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, p. 413, 2001. 94

[5] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[6] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 123–130, May 2015. 94

[7] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 16, no. 4, p. 043005, 2014. 94, 95, 96, 100, 101, 113, 118, 119, 120, 121, 123

[8] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Physical Review A*, vol. 89, no. 1, p. 012301, 2014. 94, 95, 113

[9] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical review letters*, vol. 108, no. 13, p. 130503, 2012. 94

[10] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, p. 400, 2018. 94, 111

[11] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, *et al.*, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, no. 7801, pp. 60–64, 2020. 94, 104, 108, 109

[12] N. L. Piparo, N. Sinclair, and M. Razavi, "Memory-assisted quantum key distribution resilient against multiple-excitation effects," *Quantum Science and Technology*, vol. 3, no. 1, p. 014009, 2017. 95, 96, 98, 104, 113

[13] N. L. Piparo, M. Razavi, and W. J. Munro, "Memory-assisted quantum key distribution with a single nitrogen-vacancy center," *Physical Review A*, vol. 96, no. 5, p. 052313, 2017. 95, 98

[14] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, p. 136, IEEE, 2004. 95

[15] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005. 95

[16] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Physical Review A*, vol. 95, no. 1, p. 012333, 2017. 95, 102, 124, 127, 128, 130

[17] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature communications*, vol. 5, p. 3732, 2014. 95, 102, 103, 124, 128, 130

[18] F. Schmidt and P. van Loock, "Memory-assisted long-distance phase-matching quantum key distribution," *arXiv preprint arXiv:1910.03333*, 2019. 96

[19] H. Takahashi, E. Kassa, C. Christoforou, and M. Keller, "Strong coupling of a single ion to an optical cavity," *Phys. Rev. Lett.*, vol. 124, p. 013602, Jan 2020. 98

[20] N. L. Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories," *IEEE Journal of selected topics in quantum electronics*, vol. 21, no. 3, pp. 138–147, 2015. 98, 100, 113

[21] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Physical Review A*, vol. 93, no. 4, p. 042324, 2016. 102, 124

[22] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," in *Theory of Cryptography Conference*, vol. 3378, pp. 386–406, Springer, 2005. 103

[23] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography Conference*, vol. 3378, pp. 407–425, Springer, 2005. 103

[24] R. M. Camacho, P. K. Vudyasetu, and J. C. Howell, "Four-wave-mixing stopped light in hot atomic rubidium vapour," *Nature Photonics*, vol. 3, no. 2, p. 103, 2009. 103, 104, 106, 109

[25] S.-J. Yang, X.-J. Wang, X.-H. Bao, and J.-W. Pan, "An efficient quantum light–matter interface with sub-second lifetime," *Nature Photonics*, vol. 10, no. 6, p. 381, 2016. 103, 104, 108, 109

[26] K. Maeda, T. Sasaki, and M. Koashi, "Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit," *Nature Communications*, vol. 10, p. 3140, Jul 2019. 104

[27] G. C. Lorenzo, A. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, "Tight finite-key security for twin-field quantum key distribution," *arXiv preprint arXiv:1910.11407*, 2019.

[28] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, p. 070501, Feb 2020. 104, 111

[29] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, *et al.*, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics*, vol. 7, no. 3, pp. 210–214, 2013. 104

[30] Y. Yu, F. Ma, X.-Y. Luo, B. Jing, P.-F. Sun, R.-Z. Fang, C.-W. Yang, H. Liu, M.-Y. Zheng, X.-P. Xie, W.-J. Zhang, L.-X. You, Z. Wang, T.-Y. Chen, Q. Zhang, X.-H. Bao, and J.-W. Pan, "Entanglement of two quantum memories via fibres over dozens of kilometres," *Nature*, vol. 578, no. 7794, pp. 240–245, 2020. 105

[31] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 123–130, 2014. 111, 116

[32] X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," *Physical Review A*, vol. 86, no. 5, p. 052305, 2012. 123

Chapter 4

Tight finite-key security for twin-field quantum key distribution

4.1 Abstract

Quantum key distribution (QKD) offers a reliable solution to communication problems that require long-term data security. For its widespread use, however, the rate and reach of QKD systems must be improved. Twin-field (TF) QKD is a step forward toward this direction, with early demonstrations suggesting it can beat the current rate-versus-distance records. A recently introduced variant of TF-QKD is particularly suited for experimental implementation, and has been shown to offer a higher key rate than other variants in the asymptotic regime where users exchange an infinite number of signals. Here, we extend the security of this protocol to the finite-key regime, showing that it can overcome the fundamental bounds on point-to-point QKD with around 10^{10} transmitted signals. In many practical regimes of interest, our analysis offers higher key rates than those of alternative variants. Moreover, some of the techniques we develop are applicable to the finite-key analysis of other QKD protocols.

4.2 Introduction

Quantum key distribution (QKD) enables two remote parties, Alice and Bob, to generate a shared secret key in the presence of an eavesdropper, Eve, who may have

unbounded computational power at her disposal [1–3]. While, ideally, the two parties can be at any distance, in practice, due to the loss and noise in the channel, point-to-point QKD is limited to a certain maximum distance at which secret key bits can securely be exchanged. In fact, the longest distance achieved to date in a terrestrial QKD experiment is about 400 km [4, 5]. The main limitation is the exponential decrease of the transmittance, η, with the channel length in optical fibres. Even with a high repetition rate of 10 GHz, it would take an average of about two minutes to send a single photon over a distance of 600 km of standard optical fibres, and about 300 years to send it over 1000 km [6]. Indeed, fundamental bounds [7–11] on the private capacity of *repeaterless* point-to-point QKD protocols show that their secret-key rate scales at best approximately linearly with η. A protocol that aims to overcome this linear scaling must then include at least one middle node. Interestingly, this is not a sufficient condition. A well-known counterexample is the so-called measurement-device independent QKD (MDI-QKD) [12], which uses the middle node for an *untrusted* Bell-state measurement operation. There are, however, extensions of MDI-QKD that can improve its rate scaling from η to $\sqrt{\eta}$ by either using quantum memories [13, 14] or quantum non-demolition measurements [15]. Such setups can, in fact, be considered to be the simplest examples of quantum repeaters [6, 16], which are the ultimate solution to trust-free long-distance quantum communications [17]. However, even these simple versions may need more time to be efficiently implemented in practice [18, 19].

Remarkably, the recently proposed twin-field QKD (TF-QKD) [20] can also overcome this linear scaling while using a relatively simple setup. TF-QKD is related to MDI-QKD, and it inherits its immunity to detector side-channels. However, it relies on single-photon, rather than two-photon, interference for its entanglement swapping operation. The secret-key rate of this protocol was first conjectured [20] and then proven [21, 22] to scale with $\sqrt{\eta}$ too, making this approach a strong candidate to beat the current QKD records [23–26] with today's technology. The main experimental challenge is that single-photon interference needs very precise phase stability, which makes it more demanding than two-photon interference. Also, some of its current security proofs [21, 22] need Alice and Bob to randomly choose a global phase, and then post-select only those rounds in which their choices match, which causes a drop in the secret key rate. Since the original proposal, several variants of TF-QKD have been developed [27–30], sharing the single-photon interference idea and its consequent $\sqrt{\eta}$ scaling, but

differing in their experimental setups and security proofs. Moreover, some of these variants have been shown to be robust against phase reference mismatch [28–30], which simplifies their experimental implementation.

In this paper, we focus on the TF-QKD variant introduced in [28], which has two key features: (i) it does not need phase post-selection, which results in a higher secret-key rate; and (ii) it is a convenient option for experimental implementation. Indeed, many of the current TF-QKD experiments use this variant [23, 24, 26]. One of its defining characteristics is its unconventional security proof; specifically, its estimation of the phase-error rate, a parameter needed to bound the amount of key information that may have leaked to an eavesdropper. In many QKD protocols, the phase-error rate of the single-photon emissions in one basis can be directly estimated by bounding the bit-error rate of the single-photon emissions in the other basis. In the above TF-QKD variant, however, the encoding bases are not mutually unbiased. To estimate the phase-error rate, the authors in [28] use the complementarity [31] between the "phase" and the "photon-number" of a bosonic mode. In this case, the security of a bit encoded in the relative phase of two coherent pulses can be related to the detection statistics of photon-number states. More specifically, in the *asymptotic* regime, the phase-error rate can be bounded by a non-linear function of infinitely many yield probabilities for even photon-number states [28], which can be estimated via the decoy-state method [32–34].

While, in the asymptotic regime, the protocol in [28] can offer a higher key rate than its counterparts, it is not obvious if this advantage will still hold in a practical setting where only a finite number of pulses is sent. In the finite-key regime, one should account for possible statistical fluctuations between the true phase-error rate and the measurement data used to estimate it. There are, however, two challenges in doing so. The first challenge is that the phase-error rate of the protocol is related to the measurement statistics of infinitely many combinations of photon-number states; in practice, one can only obtain bounds for a finite number of them, and dealing with the unbounded components is not as straightforward as in the asymptotic regime. The second challenge is that, unlike in many other QKD protocols, the encoding bases are not mutually unbiased. This opens the possibility that, under a coherent attack by Eve, the detection statistics of a particular round may depend on the basis choices

made in previous rounds. Accounting for these correlations makes the analysis quite cumbersome.

In this work, we provide a rigorous security proof for the protocol in [28] that accounts for these two issues in the finite-key setting. Our security proof provides a tight bound on the key rate against general coherent attacks. To overcome the two main challenges mentioned above, we borrow ideas from the finite-key analysis of MDI-QKD [35] and the loss-tolerant protocol [36, 37], as well as introduce several methods of our own. To obtain a tighter result, we employ a recent technique to bound the deviation between a sum of correlated random variables and its expected value [38], which can be much tighter than the widely employed Azuma's inequality [39] when the success probability is low. Importantly, our numerical simulations show that the protocol can overcome the repeaterless bounds [8–10] for a block size of around 10^{10} transmitted signals in nominal working conditions.

During the preparation of this manuscript, an alternative finite-key security analysis for an identical protocol setup has been reported in [40], using an interesting, but different, approach. We would like to highlight that our analysis imposes fewer conditions on the setup parameters than that of Ref. [40], and results in a higher key rate in most practical regimes. In the Discussion section, we compare both approaches. We also compare our results with those of the sending-or-not-sending TF-QKD protocol introduced in [30], whose security has recently been extended to the finite-key regime [41]. We find that for reasonably large block sizes, and sufficiently low phase reference mismatch errors, the asymptotic key rate advantage of the scheme in [28] is maintained in the finite-key regime, for most practical ranges of distance.

Results

Protocol description

The setup of the TF-QKD protocol in [28] is illustrated in Fig. 4.1 and its step-by-step description is given below. Alice and Bob generate quantum signals and send them to a middle node, Charlie, who would ideally couple them at a balanced 50:50 beamsplitter and perform a photodetection measurement. For simplicity, we assume the symmetric scenario in which the Alice-Charlie and Bob-Charlie quantum channels are identical. We note, however, that our analysis can be straightforwardly extended

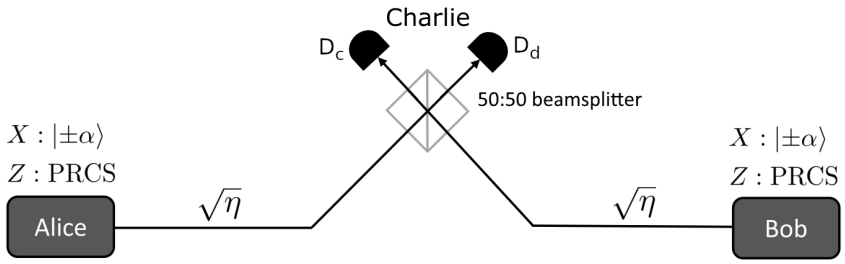


Figure 4.1: **Setup of the simple TF-QKD protocol [28] considered in this work.** Alice and Bob generate their sifted key from the rounds in which they both select the X basis and Charlie declares that a single detector has clicked. The key bit is encoded in the phase of their coherent state. When the users select the same (a different) bit, the constructive (destructive) interference at Charlie's 50:50 beamsplitter should cause a click in detector D_c (D_d). The Z-basis PRCSs are only used to estimate the phase-error rate of the X-basis emissions.

to the asymmetric scenario recently considered in Refs. [42, 43]. The emitted quantum signals belong to two bases, selected at random. In the X basis, Alice and Bob send phase-locked coherent states $|\pm\alpha\rangle$ with a random phase of either 0 or π with respect to a pre-agreed reference. In the Z basis, Alice and Bob generate phase-randomised coherent states (PRCSs), which are diagonal in the Fock basis. The X-basis states are used to generate the key, while the Z-basis data is used to estimate the detection statistics of Fock states, in combination with the decoy-state method. This is a crucial step in estimating the phase-error rate of the key, thus bounding the information that could have been leaked to a potential eavesdropper. The detailed steps of the protocol are:

(1) *Preparation*

Alice (Bob) chooses the key-generation basis X with probability p_X or the parameter-estimation basis Z with probability $p_Z = 1 - p_X$, and

(1.1) If she (he) chooses the X basis, she (he) generates a random bit b_A (b_B), prepares an optical pulse in the coherent state $\left|(-1)^{b_A}\alpha\right\rangle$ ($\left|(-1)^{b_B}\alpha\right\rangle$), and sends it to Charlie.

(1.2) If she (he) chooses the Z basis, she (he) sends an optical pulse in a PRCS of intensity μ, selected from the set $\underline{\mu} = \{\mu_0, \mu_1, \ldots, \mu_{d-1}\}$ with probability p_μ, where d is the number of decoy intensities used.

They repeat step (1) for N rounds.

(2) *Detection*

An honest Charlie measures each round separately by interfering Alice and Bob's signals at a 50:50 beamsplitter, followed by threshold detectors D_c and D_d placed at the output ports corresponding to constructive and destructive interference, respectively. After the measurement, Charlie reports the pair $(k_c,\ k_d)$, where $k_c = 1$ ($k_d = 1$) if detector D_c (D_d) clicks and $k_c = 0$ ($k_d = 0$) otherwise. If he is dishonest, Charlie can measure all rounds coherently using an arbitrary quantum measurement, and report N pairs $(k_c,\ k_d)$ depending on the result. A round is considered successful (unsuccessful) if $k_c \neq k_d$ ($k_c = k_d$).

(3) *Sifting*

For all successful rounds, Alice and Bob disclose their basis choices, keeping only those in which they have used the same basis. Let $\mathcal{M}_X$ ($\mathcal{M}_Z$) be the set of successful rounds in which both users employed the X (Z) basis, and let $M_X = |\mathcal{M}_X|$ ($M_Z = |\mathcal{M}_Z|$) be the size of this set. Alice and Bob disclose their intensity choices for the rounds in $\mathcal{M}_Z$ and learn the number of rounds $M^{\mu\nu}$ in $\mathcal{M}_Z$ in which they selected intensities $\mu \in \underline{\mu}$ and $\nu \in \underline{\mu}$, respectively. Also, they generate their sifted keys from the values of b_A and b_B corresponding to the rounds in $\mathcal{M}_X$. For those rounds in which $k_c = 0$ and $k_d = 1$, Bob flips his sifted key bit.

(4) *Parameter estimation*

Alice and Bob apply the decoy-state method to $M^{\mu\nu}$, for $\mu, \nu \in \underline{\mu}$, obtaining upper-bounds M^{U}_{nm} on the number of rounds M_{nm} in $\mathcal{M}_Z$ in which they sent n and m photons, respectively. They do this for all $n, m \geq 0$ such that $n + m$ is even and $n + m \leq S_{\mathrm{cut}}$ for a prefixed parameter S_{cut}. Then, they use this data to obtain an upper bound $N^{\mathrm{U}}_{\mathrm{ph}}$ on the number of phase errors, N_{ph}, in their sifted keys.

(5) *Postprocessing*

(5.1) *Error correction*: Alice sends Bob a pre-fixed amount λ_{EC} of syndrome information bits through an authenticated public channel, which Bob uses to correct errors in his sifted key.

(5.2) *Error verification*: Alice and Bob compute a hash of their error-corrected keys using a random universal hash function, and check whether they are equal. If so, they continue to the next step; otherwise, they abort the protocol.

(5.3) *Privacy amplification:* Alice and Bob extract a secret key pair (S_A, S_B) of length $|S_A| = |S_B| = \ell$ from their error-corrected keys using a random two-universal hash function.

4.2.1 Parameter estimation and Secret-key rate analysis

The main contribution of this work—see Methods for the details—is a procedure to obtain a tight upper-bound $N_{\mathrm{ph}}^{\mathrm{U}}$ on the total number of phase errors N_{ph} in the finite-key regime for the protocol described above. Namely, we find that, except for an arbitrarily small failure probability ε, it holds that

$$\begin{aligned} N_{\mathrm{ph}} \leq N_{\mathrm{ph}}^{\mathrm{U}} :=& \frac{p_X^2}{p_Z^2} \sum_{j=0}^{1} \Bigg[\sum_{\substack{n,m\in\mathbb{N}_j \\ n+m\leq S_{\mathrm{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}} \sqrt{M_{nm}^{\mathrm{U}} + \Delta_{nm}} \\ &+ \sqrt{M_Z + \Delta} \sum_{\substack{n,m\in\mathbb{N}_j \\ n+m> S_{\mathrm{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}} \Bigg]^2 + \Delta, \end{aligned} \tag{4.1}$$

where $p_{nm|X}$ ($p_{nm|Z}$) is the probability that Alice and Bob's joint X (Z) basis pulses contain n and m photons, respectively, given by

$$p_{nm|X} = |\langle\alpha|n\rangle|^2 |\langle\alpha|m\rangle|^2, \tag{4.2}$$

$$p_{nm|Z} = \sum_{\mu,\nu\in\underline{\mu}} p_\mu p_\nu p_{n|\mu} p_{m|\nu}, \tag{4.3}$$

with $p_{n|\mu} = \mu^n \exp(-\mu)/n!$ being the Poisson probability that a PRCS pulse of intensity μ will contain n photons; $\mathbb{N}_0$ ($\mathbb{N}_1$) is the set of non-negative even (odd) integers; and Δ and Δ_{nm} are statistical fluctuation terms defined in step 4 of subsection "Instructions for experimentalists", where we provide a step-by-step instruction list to apply our

results to the measurement data obtained in an experimental setup. The rest of the parameters have been introduced in the protocol description.

When it comes to finite-key analysis, there is one key difference between the protocol considered in this work and several other protocols, such as, for example, decoy-state BB84 [44], decoy-state MDI-QKD [35], and sending-or-not-sending TF-QKD [41]. In all the latter setups, when there are no state-preparation flaws, the single-photon components of the two encoding bases are mutually unbiased; in other words, they look identical to Eve once averaged by the bit selection probabilities. This implies that such states could have been generated from a maximally entangled bipartite state, where one of its components is measured in one of the two orthogonal bases, and the other half represents an encoded key bit. In fact, the user(s) could even wait until they learn which rounds have been successfully detected to decide their measurement basis, effectively delaying their choice of encoding basis. This possibility allows the application of a random sampling argument: since the choice of the encoding basis is independent of Eve's attack, the bit error rate of the successful X-basis emissions provides a random sample of the phase-error rate of the successful Z-basis emissions, and vice-versa. Then, one can apply tight statistical results such as the Serfling inequality [45] to bound the phase-error rate in one basis using the measured bit-error rate in the other basis. This approach, however, is not directly applicable to the protocol considered here, in which the secret key is extracted from all successfully detected X-basis signals, not just from their single-photon components. Moreover, the encoding bases are not mutually unbiased: the Z-basis states are diagonal in the Fock basis, while the X-basis states are not. This will require a different, perhaps more cumbersome, analysis as we highlight below.

To estimate the X-basis phase-error rate from the Z-basis measurement data, we construct a virtual protocol in which the users learn their basis choice by measuring a quantum coin after Charlie/Eve reveals which rounds were successful. Note that, because of the biased basis feature of the protocol, the statistics of the quantum coins associated to the successful rounds could depend on Eve's attack. This means that the users cannot delay their choice of basis, which prevents us from applying the random sampling argument. Still, it turns out that the quantum coin technique now allows us to upper-bound the average number of successful rounds in which the users had selected the X basis and obtained a phase error. This bound is a non-linear function

of the average number of successful rounds in which they had selected the Z basis and respectively sent n and m photons, with $n+m$ even. More details can be found in the Methods Section; see Eq. (4.19).

The main tool we use to relate each of the above average terms to their actual occurrences, $N_{\rm ph}$ and M_{nm}, is Azuma's inequality [39], which is widely used in security analyses of QKD to bound sums of observables over a set of rounds of the protocol (in our case, the set of successful rounds after sifting), when the independence between the observables corresponding to different rounds cannot be guaranteed. When using Azuma's inequality, the deviation term Δ scales with the square root of the number of terms in the sum. In our case, Δ scales with $\sqrt{M_{\rm s}}$, where $M_{\rm s}$ is the number of successful rounds after sifting. For parameters of comparable magnitude to $M_{\rm s}$, this provides us with a reasonably tight bound. Whenever the parameter of interest is small, however, the provided bound could instead be loose. This is the case for the crucial term $M_{00}^{\rm U}$ in Eq. (4.1), as vacuum states are unlikely to result in successful detection events, and thus the bound obtained with Azuma's inequality can be loose. This is important because, in Eq. (4.1), the coefficient associated to the vacuum term is typically the largest. To obtain a better bound for this term, we employ a remarkable recent technique to bound the deviation between a sum of dependent random variables and its expected value [38]. This technique provides a much tighter bound than Azuma's inequality when the value of the sum is much lower than the number of terms in the sum. In particular, it provides a tight upper-bound for the vacuum component M_{00}. In Methods, we provide a statement of the result and we explain how we apply it to our protocol.

Having obtained the upper-bound $e_{\rm ph}^{\rm U} := N_{\rm ph}^{\rm U}/M_X$ on the phase-error rate, we show in Supplementary Note A that, if the length of the secret key obtained after the privacy amplification step satisfies

$$\ell \leq M_X \left[1 - h(e_{\rm ph}^{\rm U})\right] - \lambda_{\rm EC} - \log_2 \frac{2}{\epsilon_{\rm c}} - \log_2 \frac{1}{4\epsilon_{\rm PA}^2}, \tag{4.4}$$

the protocol is guaranteed to be $\epsilon_{\rm c}$-correct and $\epsilon_{\rm s}$-secret, with $\epsilon_{\rm s} = \sqrt{\varepsilon} + \epsilon_{\rm PA}$; where ε is the failure probability associated to the estimation of the phase-error rate, $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon binary entropy function, and $\lambda_{\rm EC}$ is number of bits that are spent in the error-correction procedure. Here, our security analysis follows the universal composable security framework [46, 47], according to which a protocol is $\epsilon_{\rm sec}$-secure if it is both $\epsilon_{\rm c}$-correct and $\epsilon_{\rm s}$-secret, with $\epsilon_{\rm sec} \leq \epsilon_{\rm c} + \epsilon_{\rm s}$.

4.2.2 Instructions for experimentalists

Here, we provide a step-by-step instruction list to apply our security analysis to a real-life experiment:

(1) Set the security parameters ϵ_{c} and ϵ_{PA}, as well as the failure probabilities ε_{c} and ε_{a} for the inverse multiplicative Chernoff bound and the concentration bound for sums of dependent random variables, respectively. Set S_{cut}. Calculate the overall failure probability ε of the parameter estimation process, which depends on the number of times that the previous two inequalities are applied. In general, $\varepsilon = d^2\varepsilon_{\mathrm{c}} + \left(\lfloor \frac{S_{\mathrm{cut}}}{2} \rfloor + 1\right)^2 \varepsilon_{\mathrm{a}} + \varepsilon_{\mathrm{a}}$, where d is the number of decoy intensities employed by each user. For $S_{\mathrm{cut}} = 4$ and three decoy intensities, we have that $\varepsilon = 9\varepsilon_{\mathrm{c}} + 10\varepsilon_{\mathrm{a}}$.

(2) Use prior information about the channel to obtain a prediction $\tilde{M}_{00}^{\mathrm{U}}$ on M_{00}^{U}, the upper bound on the number of Z-basis vacuum events that will be obtained after applying the decoy-state method.

(3) Run steps 1-3 of the protocol, obtaining a sifted key of length M_X, and Z-basis measurement counts $M^{\mu\nu}$ for $\mu, \nu \in \underline{\mu}$. Let $M_{\mathrm{s}} = M_X + M_Z$ be the number of successful rounds after sifting.

(4) Use the analytical decoy-state method included in the Supplementary Note B and the measured values of $M^{\mu\nu}$ to obtain upper bounds M_{nm}^{U}, for all n, m such that $n + m$ is even and $n + m \leq S_{\mathrm{cut}}$. Alternatively, use the numerical estimation method introduced in the Supplementary Notes of [35].

(5) Set $\Delta = \sqrt{\frac{1}{2} M_{\mathrm{s}} \ln \varepsilon_{\mathrm{a}}^{-1}}$ and $\Delta_{nm} = \Delta$ for all n, m except for $m = n = 0$. Substitute $\tilde{\Lambda}_n \to \tilde{M}_{00}^{\mathrm{U}}$ in Eq. (4.32) to find parameters a and b. Set

$$\Delta_{00} = \left[b + a \left(\frac{2M_{00}^{\mathrm{U}}}{M_{\mathrm{s}}} - 1 \right) \right] \sqrt{M_{\mathrm{s}}}, \tag{4.5}$$

(6) Use Eq. (4.1) to find $N_{\mathrm{ph}}^{\mathrm{U}}$ and set $e_{\mathrm{ph}}^{\mathrm{U}} = N_{\mathrm{ph}}^{\mathrm{U}} / M_X$.

(7) Use Eq. (4.4) to specify the required amount of privacy amplification and to find the corresponding length of the secret key that can be extracted. The key obtained is ϵ_{sec}-secure, with $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{c}} + \epsilon_{\mathrm{s}}$ and $\epsilon_{\mathrm{s}} = \sqrt{\varepsilon} + \epsilon_{\mathrm{PA}}$.

4.3 Discussion

In this section, we analyse the behaviour of the secret-key rate as a function of the total loss. We simulate the nominal scenario in which there is no Eve and Charlie is honest. In this case, the total Alice-Bob loss includes the loss in the quantum channels as well as the inefficiency of Charlie's detectors. We compare the key rate for the protocol in Fig. 4.1, using the finite-key security analysis introduced in the previous section, with that of the sending-or-not-sending TF-QKD protocol [30, 41], as well as with the finite-key analysis presented in Ref. [40]. We also include the asymptotic secret key capacity for repeaterless QKD systems over lossy channels, known as the PLOB bound [9], for comparison. It is given by $-\log_2(1-\eta)$, where η is the transmittance of the Alice-Bob quantum channel, which includes the efficiency of Charlie's detectors. While specific bounds for the finite-key setting have recently been studied [10, 48], in the practical regimes of interest to this work, they numerically offer a negligible difference to the PLOB bound. The latter has then been used in all relevant graphs for consistency. To simulate the data that would be obtained in all protocols, we use the simple channel model described in Supplementary Note C, which accounts for phase reference mismatch and polarisation misalignment. Also, we assume that both users employ three decoy-state intensities $\mu_0 > \mu_1 > \mu_2$. Since the optimal value $\mu_2 = 0$ is typically difficult to achieve in practice, we set $\mu_2 = 10^{-4}$ and optimise the secret-key rate over the value of μ_0 and μ_1. We also optimise it over the selection probabilities, as well as over p_X and α.

In our simulations, we model the phase reference mismatch between Alice and Bob's pulses by shifting Bob's signals by an angle $\phi = \delta_{\text{ph}}\pi$, where $\delta_{\text{ph}} = 9.1\%$. This corresponds to a QBER of around 2% for most attenuations, matching the experimental results in [23]. For brevity, we do not consider the effect of polarisation misalignment in our numerical results, but one can use the provided analytical model to study different scenarios of interest. In principle, even if the mechanism used for polarisation stability is not perfect, one can use polarisation filters to ensure that the same polarisation modes are being coupled at the 50:50 beamsplitter, at the cost of introducing additional loss. We assume a per-pulse dark count probability $p_{\text{d}} = 10^{-8}$ for each detector. We assume an error correction leakage of $\lambda_{\text{EC}} = fM_X h(e_X)$, where e_X is the bit error rate of the

sifted key, and f is the error correction inefficiency, which we assume to be $f = 1.16$. For the security bounds, we set $\epsilon_c = \epsilon_s = 10^{-10}$, and for simplicity we set $\varepsilon = \epsilon_{PA} = \epsilon_s/3$.

In Fig. 4.2, we display the secret key rate per pulse achievable for different values of the block size, N, of transmitted signals. It can be seen that the protocol could outperform the repeaterless bound for a block size of around 10^{10} transmitted signals per user, at an approximate total loss of 50 dB. For standard optical fibres, this corresponds to a total distance of 250 km, if we neglect the loss in the photodetectors. At a 1 GHz clock rate, it takes only around ten seconds to collect the required data. For a block size of 10^{11} transmitted signals, the protocol can already outperform the repeaterless bound for a total loss ranging from 45 dB to over 80 dB. By increasing N, we approach the asymptotic performance of the protocol. We note that our choice of dark count probability, $p_d = 10^{-8}$, may be conservative, since a dark count rate of 1 c.p.s, corresponding to $p_d = 10^{-9}$ with a repetition rate of 1 GHz, which may be achievable with state-of-the-art SSPD [49]. In Supplementary Note D, we show an additional graph for of $p_d = 10^{-9}$. We find that, for sufficiently large block sizes, the maximum distance increases when the dark count probability decreases. Interestingly, however, this is not the case for $N = 10^{10}$, for which the two curves are almost identical.

The dependence of the secret key rate on the block size N has been shown in Fig. 4.3, at a fixed total loss of 50 dB and for several values of the phase reference mismatch δ_{ph}. In all cases, there is a minimum required block size to obtain a positive key rate. This minimum block size can be even lower than 10^9 in the ideal case of no phase reference mismatch, and it goes up to around 10^{10} at $\delta_{ph} = 20\%$. There is a sharp increase in the secret key rate once one goes over this minimum required block size, after which one slowly approaches the key rate in the asymptotic limit. The latter behaviour is likely due to the use of Azuma's inequality. One can, nevertheless, overcome the repeaterless bound at a reasonable block size in a practical regime where $\delta_{ph} \leq 15\%$. At higher values of total loss this crossover happens at even larger values of δ_{ph}.

In Fig. 4.4, we compare the performance of our protocol with that of the sending-or-not-sending TF-QKD protocol presented in [30, 41]. To compute the results of the sending-or-not-sending protocol, we have used the analysis in [41], after correcting a mistake present in Appendix A of that work. Namely, according to Eqs. (S14) to (S19) of Ref. [50], if the failure probability of the phase-error rate estimation is $\bar{\varepsilon}$, then the smooth max entropy term in the left-hand side of Eq. (A5) should be $H_{\max}^{\sqrt{\bar{\varepsilon}}}$ instead

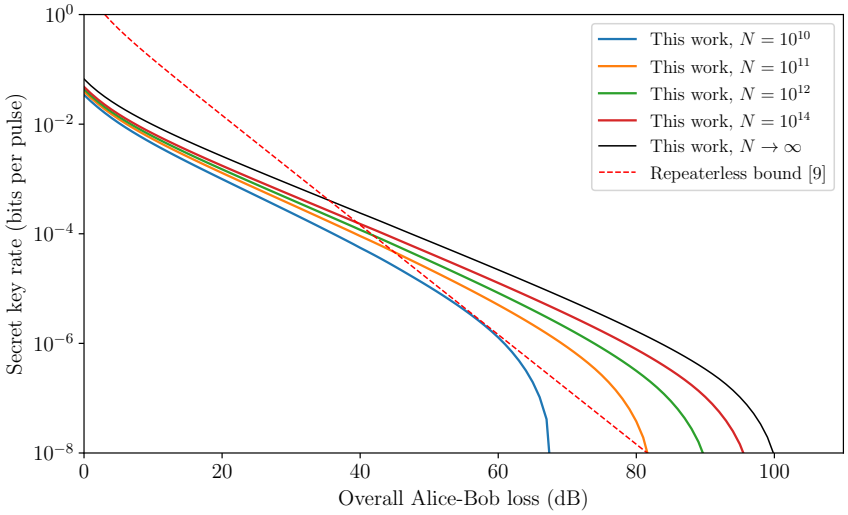


Figure 4.2: **Secret key rate obtainable as a function of the channel loss.** We consider different values of the block size N, which represents the total number of rounds in the protocol. The overall Alice-Bob loss includes the loss in both quantum channels and in Charlie's detectors. The simulation parameters are stated in the main text.

of $H_{\max}^{\bar{\varepsilon}}$. In the asymptotic regime, the protocol considered in this work outperforms the sending-or-not-sending protocol at all values of total loss. For a block size of 10^{12} transmitted signals, this is still the case up to 80 dB of total loss, after which the key rate is already lower than 10^{-6} bits per pulse for both protocols. For a block size of 10^{10} transmitted signals, however, the curves for the two protocols cross at around 55 dB, after which the sending-or-not-sending protocol offers a better performance. This behaviour is due to the different statistical fluctuation analyses applied to the two protocols. As explained in the Result section, the single-photon components in the sending-or-not-sending protocol are mutually unbiased, allowing for a simpler and tighter estimation of the phase-error rate. This is not the case for our TF-QKD protocol, for which this estimation involves the application of somewhat looser bounds for several terms in Eq. (4.1). We conclude that for sufficiently large block sizes, and a sufficiently low phase reference mismatch, the protocol considered in this work maintains its better key-rate performance over the sending-or-not sending variant. We note that for smaller block sizes and higher values of phase reference mismatch, this comparative advantage

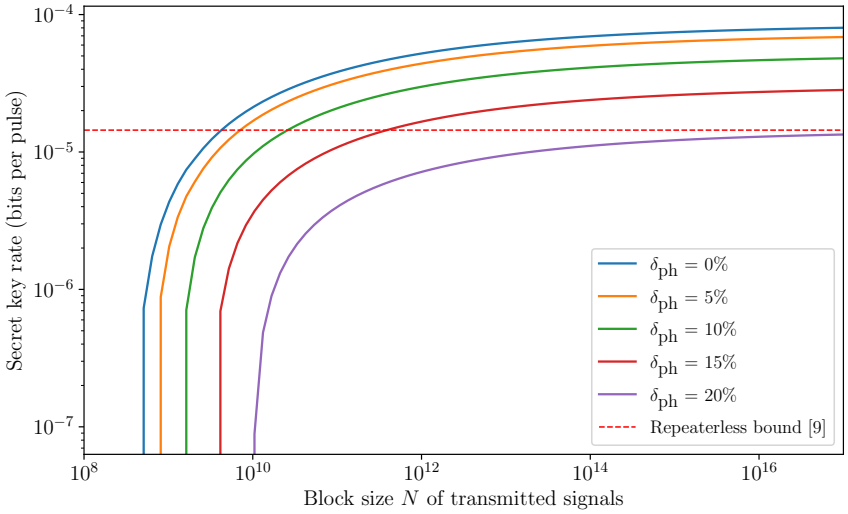


Figure 4.3: **Secret key rate obtainable as a function of the block size N.** We assume a total loss of 50 dB and consider several values of the phase reference mismatch δ_{ph}. All other simulation parameters are stated in the main text.

is reduced, or even inverted in some regimes. For completeness, in Supplementary Note D, we provide additional simulation results for a broader range of parameter values.

Finally, in Fig. 4.5, we compare our results with those of the alternative analysis in [40]. To compute the secret-key rate of the latter, we use the code provided by the authors, except for the adjustments needed to match it to the channel model described in Supplementary Note C. It can be seen that, in most regimes, the analysis introduced in this paper provides a higher key rate than that of [40]. Moreover, we remark that the security proof presented in [40], in its current form, is only applicable when the state generated by the weakest decoy intensity μ_2 is a perfect vacuum state of intensity $\mu_2 = 0$. The security analysis presented in this work, however, can be applied to any experimental value of μ_2, and we assume a value of $\mu_2 = 10^{-4}$, which may be easier to achieve in practice. That said, the security proof in [40] adopts an interesting approach that results in a somehow simpler statistical analysis. In particular, unlike in the analysis presented in this paper, the authors in [40] do not estimate the detection statistics of photon-number states as an intermediate step to bounding the phase-error rate. Instead, they show that the operator corresponding to a phase-error can be bounded by a linear combination of the Z-basis decoy states. While this linear bound is

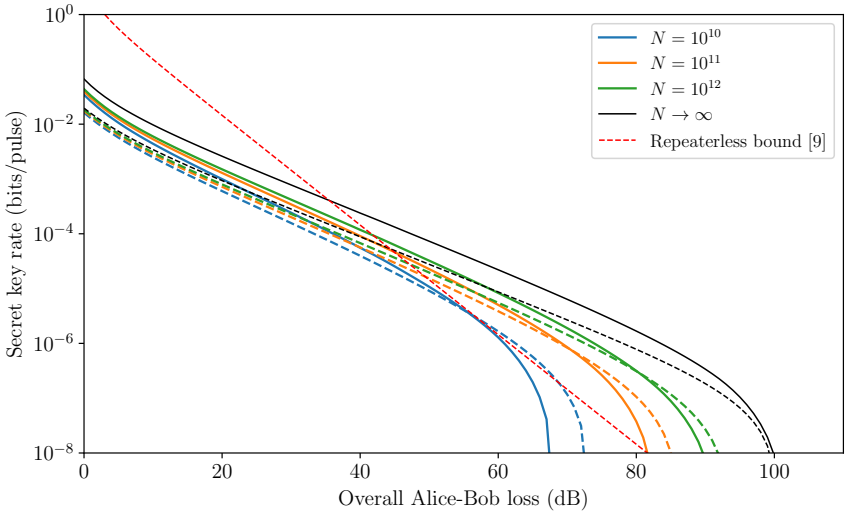


Figure 4.4: **Comparison between this work (solid) and sending-or-not-sending TF-QKD [30, 41] (dashed).** We consider different values for the block size N of transmitted signals. All other simulation parameters are stated in the main text.

asymptotically looser than the non-linear formula in Eq. (4.1), it allows the application of a simpler statistical analysis based on a double use of Bernoulli sampling. Given that the finite-key analysis of a protocol could be part of the software package of a product, we believe that the additional key rate achievable by our analysis in many regimes justifies its slightly more complex approach.

In conclusion, we have proven the security of the protocol proposed in Ref. [28], in the finite-key regime and against coherent attacks. Our results show that, under nominal working conditions experimentally achievable by today's technology, this scheme could outperform the repeaterless secret-key rate bound in a key exchange run of around ten seconds, assuming a 1 GHz clock rate. In terms of key rate, it would also outperform other TF-QKD variants, as well as alternative security proofs, in many practical regimes of interest.

4.4 Methods

In this section, we introduce the procedure that we use to prove the security of the protocol, referring to the Supplementary Notes when appropriate. For notation clarity,

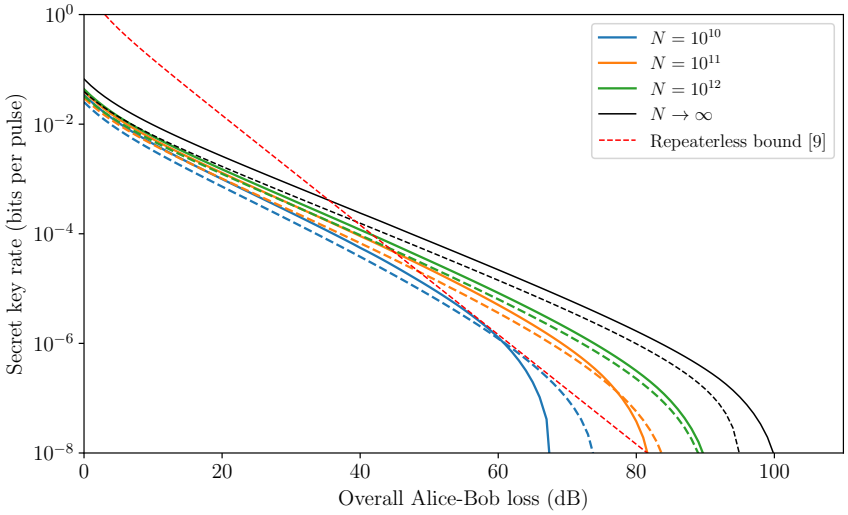


Figure 4.5: **Comparison between this work (solid) and the alternative analysis in [40] (dashed).** We consider different values for the block size N of transmitted signals. All other simulation parameters are stated in the main text.

we assume the symmetric scenario in which Alice and Bob employ the same X-basis amplitude α and the same set of Z-basis intensities $\underline{\mu}$, which is optimal when the Alice-Charlie and Bob-Charlie channels are identical. However, the analysis can be applied as well to the asymmetric scenario [42, 43] by appropriately redefining the parameters $p_{nm|X}$ and $p_{nm|Z}$.

4.4.1 Virtual protocol

To bound the information leakage to Eve, we construct an entanglement-based virtual protocol that is equivalent to the actual protocol. In this virtual protocol, Alice and Bob measure their local ancilla systems in a basis that is conjugate to that used to generate the key. We refer to the error rate of the virtual protocol as the phase-error rate e_{ph}. The objective of the security analysis is to find an upper-bound e_{ph}^{U} such that $\Pr\left(e_{\text{ph}} > e_{\text{ph}}^{\text{U}}\right) \leq \varepsilon$. In Supplementary Note A, we show how this can be used to prove the security of the key obtained in the actual protocol.

In the virtual protocol, Alice replaces her X-basis emissions by the preparation of the state

$$|\psi_X\rangle_{Aa} = \frac{1}{\sqrt{2}}(|+\rangle_A |\alpha\rangle_a + |-\rangle_A |-\alpha\rangle_a), \tag{4.6}$$

where A is an ancilla system at Alice's lab, a is the photonic system sent to Eve, and $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$; while Bob replaces his X basis emissions are by a similarly defined $|\psi_X\rangle_{Bb}$. After Eve's attack, Alice and Bob measure systems A and B in the Z basis $\{|0\rangle, |1\rangle\}$, which is conjugate to the X basis $\{|+\rangle, |-\rangle\}$ that they would use to generate the key. It is useful to write the state in Eq. (4.6) as

$$|\psi_X\rangle_{Aa} = |0\rangle_A |C_0\rangle_a + |1\rangle_A |C_1\rangle_a , \tag{4.7}$$

where $|C_0\rangle$ and $|C_1\rangle$ are the (unnormalised) cat states

$$|C_0\rangle = \frac{1}{2}(|\alpha\rangle + |-\alpha\rangle), \qquad |C_1\rangle = \frac{1}{2}(|\alpha\rangle - |-\alpha\rangle). \tag{4.8}$$

Alice's Z-basis emissions are diagonal in the Fock basis, and the virtual protocol replaces them by their purification

$$|\psi_Z\rangle_{Aa} = \sum_{n=0}^{\infty} \sqrt{p_{n|Z}} |n\rangle_A |n\rangle_a , \tag{4.9}$$

where $p_{n|Z} = \sum_{\mu \in \underline{\mu}} p_\mu p_{n|\mu}$ is the probability that Alice's Z basis pulse contains n photons, averaged over the selection of μ. Unlike in the actual protocol, in the virtual protocol Alice and Bob learn the photon number of their signals by measuring systems A and B after Eve's attack.

Lastly, Alice's emission of $|\psi_X\rangle_{Aa}$ with probability p_X and $|\psi_Z\rangle_{Aa}$ with probability p_Z is replaced by the generation of the state

$$|\psi\rangle_{A_c Aa} = \sqrt{p_X} |0\rangle_{A_c} |\psi_X\rangle_{Aa} + \sqrt{p_Z} |1\rangle_{A_c} |\psi_Z\rangle_{Aa} , \tag{4.10}$$

where A_c is a quantum coin ancilla at Alice's lab; while Bob's is replaced by an equally defined $|\psi\rangle_{B_c Bb}$. Alice and Bob measure systems A_c and B_c after Eve's attack, delaying the reveal of their basis choice. The full description of the virtual protocol is the following:

(1) *Preparation*

Alice and Bob prepare N copies of the state $|\phi\rangle = |\psi\rangle_{A_c Aa} \otimes |\psi\rangle_{B_c Bb}$ and send all systems a and b to Eve over the quantum channel.

(2) *Detection*

Eve performs an arbitrary general measurement on all the subsystems a and b of $|\phi\rangle^{\otimes N}$ and publicly announces N bit pairs (k_c, k_d). Without loss of generality, we assume that there is a one-to-one correspondence between her measurement outcome and her set of announcements. A round is considered successful (unsuccessful) if $k_c \neq k_d$ ($k_c = k_d$). Let $\mathcal{M}$ ($\bar{\mathcal{M}}$) represent the set of successful (unsuccessful) rounds.

(3) *Virtual sifting*

For all rounds, Alice and Bob jointly measure the systems A_{c} and B_c, learning whether they used the same or different bases, but not the specific basis they used. Let $\mathcal{M}_{\mathrm{s}}$ ($\mathcal{M}_{\mathrm{d}}$) denote the set of successful rounds in which they used the same (different) bases.

(4) *Ancilla measurement*

(4.1) For all rounds in $\mathcal{M}_{\mathrm{s}}$, Alice (Bob) first measures the system A_{c} (B_c) in $\{|0\rangle, |1\rangle\}$, learning her (his) choice of basis. If the result is $|0\rangle_{A_{\mathrm{c}}}$ ($|0\rangle_{B_c}$), she (he) measures system A (B) in $\{|0\rangle, |1\rangle\}$; if the result is $|1\rangle_{A_{\mathrm{c}}}$ ($|1\rangle_{B_c}$), she (he) measures system A (B) in the Fock basis.

(4.2) For all rounds in $\mathcal{M}_{\mathrm{d}}$, Alice (Bob) measures the systems A_{c} (B_c) and A (B), using the same strategy as in step 4.1.

(5) *Intensity assignment*

For all rounds in $\mathcal{M}$ in which Alice (Bob) obtained $|1\rangle_{A_{\mathrm{c}}}$ ($|1\rangle_{B_c}$), she (he) assigns each n-photon state to intensity μ with probability $p_{\mu|n}$.

(6) *Classical communication*

For all rounds in $\mathcal{M}$, Alice and Bob announce all their basis and intensity choices over an authenticated public channel.

(7) *Estimation of the number of phase errors*

Alice and Bob calculate an upper bound on N_{ph} using their Z basis measurement data.

Two points from the virtual protocol above require further explanation. The first is that, in the real protocol, Bob flips his key bit when Eve reports $k_c = 0$ and $k_d = 1$. This step is omitted from the virtual protocol, since the X-basis bit flip gate σ_z has no effect on Bob's Z-basis measurement result. The second point concerns step 5, which may appear to serve no purpose, but it is needed to ensure that the classical information exchanged between Alice and Bob is equivalent to that of the real protocol. The term $p_{\mu|n}$ is the probability that Alice's (Bob's) Z-basis n-photon pulse originated from intensity μ, and it is given by

$$p_{\mu|n} = \frac{p_\mu p_{n|\mu}}{\sum_{\mu\in\underline{\mu}} p_\mu p_{n|\mu}}. \tag{4.11}$$

4.4.2 Phase-error rate estimation

We now turn our attention to Alice and Bob's measurements in step (4.1) of the virtual protocol. Let $u \in \{1, 2, ..., M_s\}$ index the rounds in $\mathcal{M}_s$, and let ξ_u denote the measurement outcome of the u-th round. The possible outcomes are $\xi_u = X_{ij}$, corresponding to $|00\rangle_{A_cB_c}|ij\rangle_{AB}$, where $i, j \in \{0, 1\}$; and $\xi_u = Z_{nm}$, corresponding to $|11\rangle_{A_cB_c}|n, m\rangle_{AB}$, where n and m are any non-negative integers. Note that the outcomes $|10\rangle_{A_cB_c}$ and $|01\rangle_{A_cB_c}$ are not possible due to the previous virtual sifting step. A phase error occurs when $\xi_u \in \{X_{00}, X_{11}\}$. In Supplementary Note E, we prove that the probability to obtain a phase error in the u-th round, conditioned on all previous measurement outcomes in the protocol, is upper-bounded by

$$\Pr\left(\xi_u \in \{X_{00}, X_{11}\}|\mathcal{F}_{u-1}\right) \leq \frac{p_X^2}{p_Z^2}\sum_{j=0}^{1}\left[\sum_{n,m\in\mathbb{N}_j}\sqrt{\frac{p_{nm|X}}{p_{nm|Z}}\Pr\left(\xi_u = Z_{nm}|\mathcal{F}_{u-1}\right)}\right]^2, \tag{4.12}$$

where $\mathcal{F}_{u-1}$ is the σ-algebra generated by the random variables $\xi_1, ..., \xi_{u-1}$, $\mathbb{N}_0$ ($\mathbb{N}_1$) is the set of non-negative even (odd) numbers, and the probability terms $p_{nm|X}$ and $p_{nm|Z}$ have been defined in Eqs. (4.2) and (4.3). In Eq. (4.12), for notation clarity, we have omitted the dependence of all probability terms on the outcomes of the measurements performed in steps (2) and (3) of the virtual protocol.

Applying the concentration bound in Eq. (4.30), we have that, except with probability ε_a,

$$N_{ph} \leq \sum_{u=1}^{M_s}\Pr\left(\xi_u \in \{X_{00}, X_{11}\}|\mathcal{F}_{u-1}\right) + \Delta, \tag{4.13}$$

where N_{ph} is the number of events of the form $\xi_u \in \{X_{00}, X_{11}\}$ in $\mathcal{M}_{\text{s}}$, and $\Delta = \sqrt{\frac{1}{2} M_{\text{s}} \ln \varepsilon_{\text{a}}^{-1}}$ is a deviation term. Similarly, from Eq. (4.30), we have that, except with probability ε_{a},

$$\sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u = Z_{nm} | \mathcal{F}_{u-1}\right) \leq M_{nm} + \Delta, \tag{4.14}$$

where M_{nm} is the number of events of the form $\xi_u = Z_{nm}$ in $\mathcal{M}_{\text{s}}$. As we will explain later, this bound is not tight when applied to the vacuum counts M_{00}. For this term, we use the alternative bound in Eq. (4.33), according to which, except with probability ε_{a},

$$\sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u = Z_{00} | \mathcal{F}_{u-1}\right) \leq M_{00} + \Delta_{00}. \tag{4.15}$$

In this case, the deviation term is given by

$$\Delta_{00} = \left[b + a\left(\frac{2M_{00}}{M_{\text{s}}} - 1\right)\right] \sqrt{M_{\text{s}}}, \tag{4.16}$$

where a and b can be found by substituting $\tilde{\Lambda}_n$ by $\tilde{M}_{00}^{\text{U}}$ in Eq. (4.31).

Now we will transform Eq. (4.12) to apply Eqs. (4.13) to (4.15). Let us denote the right-hand side of Eq. (4.12) as $f(\vec{p}_u)$, where $\vec{p}_u$ is a vector of probabilities composed of $\Pr(\xi_u = Z_{nm} | \mathcal{F}_{u-1})\ \forall n, m$. If we expand the square in $f(\vec{p}_u)$, we can see that all addends are positive and proportional to $\sqrt{p_1 p_2}$, where p_1 and p_2 are elements of $\vec{p}_u$, implying that $f(\vec{p}_u)$ is a concave function. Thus, by Jensen's inequality [51], we have

$$\frac{1}{M_{\text{s}}} \sum_{u=1}^{M_{\text{s}}} f(\vec{p}_u) \leq f\left(\frac{1}{M_{\text{s}}} \sum_{u=1}^{M_{\text{s}}} \vec{p}_u\right). \tag{4.17}$$

After taking the average over all rounds M_{s} on both sides of Eq. (4.12), applying Eq. (4.17) on the right-hand side, and cancelling out the term $1/M_{\text{s}}$ on both sides of the inequality, we have that

$$\begin{aligned} &\sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u \in \{X_{00}, X_{11}\} | \mathcal{F}_{u-1}\right) \\ &\qquad \leq \frac{p_X^2}{p_Z^2} \sum_{j=0}^{1} \left[\sum_{n,m \in \mathbb{N}_j} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}} \sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u = Z_{nm} | \mathcal{F}_{u-1}\right)} \right]^2. \end{aligned} \tag{4.18}$$

We are now ready to apply Eqs. (4.13) to (4.15) to substitute the sums of probabilities in Eq. (4.18) by N_{ph} and M_{nm}. However, note that, in their application of the

decoy-state method, Alice and Bob only estimate the value of M_{nm} for terms of the form $n+m \leq S_{\text{cut}}$, so it is only useful to substitute Eq. (4.14) for these terms. With this in mind, we obtain

$$\begin{aligned} N_{\text{ph}} - \Delta \leq & \frac{p_X^2}{p_Z^2} \sum_{j=0}^{1} \Bigg[\sum_{\substack{n,m \in \mathbb{N}_j \\ n+m \leq S_{\text{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}} \sqrt{M_{nm} + \Delta_{nm}} \\ & + \sum_{\substack{n,m \in \mathbb{N}_j \\ n+m > S_{\text{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}} \sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u = Z_{nm} | \mathcal{F}_{u-1}\right)} \Bigg]^2, \end{aligned} \tag{4.19}$$

where $\Delta_{nm} = \Delta$ except for Δ_{00}.

We still need to deal with the sum over the infinitely many remaining terms of the form $n+m > S_{\text{cut}}$. For them, we apply the following upper bound

$$\sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u = Z_{nm} | \mathcal{F}_{u-1}\right) \leq \sum_{u=1}^{M_{\text{s}}} \Pr\left(\xi_u = Z | \mathcal{F}_{u-1}\right) \leq M_Z + \Delta, \tag{4.20}$$

where $\xi_u = Z$ denotes that Alice and Bob learn that they have used the Z basis in the uth round in $\mathcal{M}_{\text{s}}$; and M_Z is the number of events of the form $\xi_u = Z$ obtained by Alice and Bob. In the last step, we have used Eq. (4.30), using an identical argument as in Eq. (4.13). When we apply Eq. (4.20) to Eq. (4.19), we end up with the term

$$\sum_{\substack{n,m \in \mathbb{N}_j \\ n+m > S_{\text{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}} \sqrt{M_Z + \Delta} = \sqrt{M_Z + \Delta} \sum_{\substack{n,m \in \mathbb{N}_j \\ n+m > S_{\text{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}}. \tag{4.21}$$

It can be shown that the infinite sum in Eq. (4.21) converges to a finite value if

$$\max\{\underline{\mu}\} > \alpha^2. \tag{4.22}$$

Substituting Eq. (4.20) into Eq. (4.19), and isolating N_{ph}, we obtain

$$\begin{aligned} N_{\text{ph}} \leq & \frac{p_X^2}{p_Z^2} \sum_{j=0}^{1} \Bigg[\sum_{\substack{n,m \in \mathbb{N}_j \\ n+m \leq S_{\text{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}} \sqrt{M_{nm} + \Delta_{nm}} \\ & + \sqrt{M_Z + \Delta} \sum_{\substack{n,m \in \mathbb{N}_j \\ n+m > S_{\text{cut}}}} \sqrt{\frac{p_{nm|X}}{p_{nm|Z}}} \Bigg]^2 + \Delta. \end{aligned} \tag{4.23}$$

Note that the right hand side of Eq. (4.23) is a function of the measurement counts M_{nm}, which cannot be directly observed. They must be substituted by the upper

bounds M^{U}_{nm} obtained via the decoy-state analysis, as explained below. After doing so, we obtain Eq. (4.1). The failure probability ε associated to the estimation of N_{ph} is upper-bounded by summing the failure probabilities of all concentration inequalities used. That includes each application of Eqs. (4.30) and (4.33), which fail with probability ε_{a}; and each application of the multiplicative Chernoff bound in the decoy-state analysis, which fails with probability ε_{c}. In the case of three decoy intensities and $S_{\mathrm{cut}} = 4$, we have $\varepsilon = 9\varepsilon_{\mathrm{c}} + 10\varepsilon_{\mathrm{a}}$. In our simulations, we set $\varepsilon_{\mathrm{c}} = \varepsilon_{\mathrm{a}}$ for simplicity.

4.4.3 Decoy-state analysis

Since Alice and Bob's Z-basis emissions are a mixture of Fock states, the measurement counts M_{nm} have a fixed value, which is nevertheless unknown to them. Instead, the users have access to the measurement counts $M^{\mu\nu}$, the number of rounds in $\mathcal{M}_Z$ in which they selected intensities μ and ν, respectively. To bound M_{nm}, we use the decoy-state method [32–34]. This technique exploits the fact that Alice and Bob could have run an equivalent virtual scenario in which they directly send Fock states $|n, m\rangle$ with probability $p_{nm|Z}$, and then randomly assign each of them to intensities μ and ν with probability

$$p_{\mu\nu|nm} = \frac{p_{\mu\nu} p_{nm|\mu\nu}}{p_{nm|Z}}, \tag{4.24}$$

where $p_{\mu\nu} = p_\mu p_\nu$ and $p_{nm|\mu\nu} = p_{n|\mu} p_{m|\nu}$. In particular, each of the instances in which Alice and Bob chose the Z basis, sent n and m photons, and Eve announced a detection is assigned to intensities μ and ν with a fixed probability $p_{\mu\nu|nm}$, even if Eve employs a coherent attack. This implies that these assignments can be regarded as an independent Bernoulli trial, and $M^{\mu\nu}$ can be regarded as a sum of independent Bernoulli trials. The average value of $M^{\mu\nu}$ is

$$\mathbb{E}[M^{\mu\nu}] = \sum_{n,m=0}^{\infty} p_{\mu\nu|nm} M_{nm}. \tag{4.25}$$

In the actual protocol, Alice and Bob know the realisations $M^{\mu\nu}$ of these random variables. By using the inverse multiplicative Chernoff bound [52, 53], stated in Supplementary Note F, they can compute lower and upper bounds $\mathbb{E}^L[M^{\mu\nu}]$ and $\mathbb{E}^{\mathrm{U}}[M^{\mu\nu}]$ for $\mathbb{E}[M^{\mu\nu}]$. These will set constraints on the possible value of the terms M_{nm}. We are

interested in the indices (i,j) such that $i+j \leq S_{\text{cut}}$ and $i+j$ is even, and an upper bound on each M_{ij} can be found by solving the following linear optimisation problem

$$\begin{aligned} &\max M_{ij} \\ &\text{s.t. } \forall \mu,\nu \quad \mathbb{E}^{\text{U}}[M^{\mu\nu}] \geq \sum_{n,m=0}^{\infty} p_{\mu\nu|nm} M_{nm}, \\ &\qquad\qquad \mathbb{E}^{L}[M^{\mu\nu}] \leq \sum_{n,m=0}^{\infty} p_{\mu\nu|nm} M_{nm}. \end{aligned} \tag{4.26}$$

This problem can be solved numerically using linear programming techniques, as described in the Supplementary Note 2 of [35]. While accurate, this method can be computationally demanding. For this reason, we have instead adapted the asymptotic analytical bounds of [42, 54] to the finite-key scenario and used them in our simulations. The results obtained using these analytical bounds are very close to those achieved by numerically solving Eq. (4.26). This analytical method is described in Supplementary Note B.

4.4.4 Concentration inequality for sums of dependent random variables

A crucial step in our analysis is the substitution of the sums of probabilities in Eq. (4.18) by their corresponding observables in the protocol. Typically, this is done by applying the well-known Azuma's inequality [39]. Instead, we use the following recent result [38]:

Let $\xi_1, ..., \xi_n$ be a sequence of random variables satisfying $0 \leq \xi_l \leq 1$, and let $\Lambda_l = \sum_{u=1}^{l} \xi_u$. Let $\mathcal{F}_l$ be its natural filtration, i.e. the σ-algebra generated by $\{\xi_1, ..., \xi_l\}$. For any n, and any a, b such that $b \geq |a|$,

$$\Pr\left[\sum_{u=1}^{n} E(\xi_u|\mathcal{F}_{u-1}) - \Lambda_n \geq \left[b + a\left(\frac{2\Lambda_n}{n} - 1\right)\right]\sqrt{n}\right] \leq \exp\left[\frac{-2(b^2-a^2)}{(1+\frac{4a}{3\sqrt{n}})^2}\right]. \tag{4.27}$$

By replacing $\xi_l \to 1-\xi_l$ and $a \to -a$, we also derive

$$\Pr\left[\Lambda_n - \sum_{u=1}^{n} E(\xi_u|\mathcal{F}_{u-1}) \geq \left[b + a\left(\frac{2\Lambda_n}{n} - 1\right)\right]\sqrt{n}\right] \leq \exp\left[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{n}})^2}\right]. \tag{4.28}$$

In our analysis, we apply Eqs. (4.27) and (4.28) to sequences $\xi_1, ..., \xi_n$ of Bernoulli random variables, for which $E(\xi_u|\mathcal{F}_{u-1}) = \Pr(\xi_u = 1|\mathcal{F}_{u-1})$.

Now, if we set $a = 0$ on Eqs. (4.27) and (4.28), we obtain

$$\begin{aligned} \Pr\left[\Lambda_n - \sum_{u=1}^{n} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) \geq b\sqrt{n}\right] &\leq \exp\left[-2b^2\right], \\ \Pr\left[\sum_{u=1}^{n} \Pr(\xi_u = 1|\mathcal{F}_{u-1}) - \Lambda_n \geq b\sqrt{n}\right] &\leq \exp\left[-2b^2\right]. \end{aligned} \tag{4.29}$$

This is a slightly improved version of the original Azuma's inequality, whose right-hand side is $\exp\left[-\frac{1}{2}b^2\right]$. Equating the right hand sides of Eq. (4.29) to ε_{a}, and solving for b, we have that

$$\begin{aligned} \sum_{u=1}^{n} \Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) &\leq \Lambda_n + \Delta, \\ \Lambda_n &\leq \sum_{u=1}^{n} \Pr\left(\xi_u = 1|\xi_1, ..., \xi_{u-1}\right) + \Delta, \end{aligned} \tag{4.30}$$

with $\Delta = \sqrt{\frac{1}{2} n \ln \varepsilon_{\mathrm{a}}^{-1}}$, and where each of the bounds in Eq. (4.30) fail with probability at most ε_{a}.

The bound in Eq. (4.30) scales with $\sqrt{n}$, and it is only tight when Λ_n is of comparable magnitude to n. When $\Lambda_n \ll n$, one can set a and b in Eq. (4.27) appropriately to obtain a much tighter bound. To do so, one can use previous knowledge about the channel to come up with a prediction $\tilde{\Lambda}_n$ of Λ_n before running the experiment. Then, one obtains the values of a and b that would minimise the deviation term if the realisation of Λ_n equalled $\tilde{\Lambda}_n$, by solving the optimisation problem

$$\begin{aligned} \min \quad & \left[b + a\left(\frac{2\tilde{\Lambda}_n}{n} - 1\right)\right]\sqrt{n} \\ \text{s.t.} \quad & \exp\left[\frac{-2(b^2 - a^2)}{(1 + \frac{4a}{3\sqrt{n}})^2}\right] = \varepsilon_{\mathrm{a}}, \\ & b \geq |a|. \end{aligned} \tag{4.31}$$

The solution to Eq. (4.31) is

$$\begin{aligned} a &= \frac{3\left(72\sqrt{n}\tilde{\Lambda}_n(n - \tilde{\Lambda}_n)\ln\varepsilon_a - 16n^{3/2}\ln^2\varepsilon_a + 9\sqrt{2}(n - 2\tilde{\Lambda}_n)\sqrt{-n^2\ln\varepsilon_a(9\tilde{\Lambda}_n(n - \tilde{\Lambda}_n) - 2n\ln\varepsilon_a)}\right)}{4(9n - 8\ln\varepsilon_a)(9\tilde{\Lambda}_n(n - \tilde{\Lambda}_n) - 2n\ln\varepsilon_a)}, \\ b &= \frac{\sqrt{18a^2n - \left(16a^2 + 24a\sqrt{n} + 9n\right)\ln\varepsilon_a}}{3\sqrt{2n}}. \end{aligned} \tag{4.32}$$

After fixing a and b, we have that

$$\sum_{u=1}^{n} \Pr\left(\xi_u = 1 | \xi_1, ..., \xi_{u-1}\right) \leq \Lambda_n + \Delta', \tag{4.33}$$

except with probability ε_{a}, where

$$\Delta' = \left[b + a\left(\frac{2\Lambda_n}{n} - 1\right)\right]\sqrt{n}. \tag{4.34}$$

In our numerical simulations, we have found the simple bound in Eq. (4.30) to be sufficiently tight for all components except the vacuum contribution M_{00}. For this latter component, we use Eq. (4.33) instead. However, note that the users do not know the true value of M_{00}, even after running the experiment. Instead, they will obtain an upper-bound M_{00}^{U} on M_{00} via the decoy-state method, and they will apply Eq. (4.33) to this upper bound. Therefore, to optimise the bound, the users should come up with a prediction $\tilde{M}_{00}^{\mathrm{U}}$ on the value of M_{00}^{U} that they expect to obtain after running the experiment and performing the decoy-state analysis, and then substitute $\tilde{\Lambda}_n \to \tilde{M}_{00}^{\mathrm{U}}$ in Eq. (4.31) to obtain the optimal values of a and b. To find $\tilde{M}_{00}^{\mathrm{U}}$, one can simply use their previous knowledge of the channel to come up with predictions $\tilde{M}^{\mu\nu}$ of $M^{\mu\nu}$, and run the decoy-state analysis using these values to obtain $\tilde{M}_{00}^{\mathrm{U}}$.

Data availability

All data generated in this study can be reproduced using the equations and methodology introduced in this paper and its Supplementary Notes, and are available from the corresponding author upon reasonable request.

Acknowledgements

We thank Margarida Pereira, Kiyoshi Tamaki and Mirko Pittaluga for valuable discussions. We thank Kento Maeda, Toshihiko Sasaki and Masato Koashi for the computer code used to generate Fig. 4.5, as well as for insightful discussions. This work was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement number 675662 (QCALL). M.C. also acknowledges support from the Spanish Ministry of Economy and Competitiveness (MINECO), and the Fondo Europeo de Desarrollo Regional (FEDER)

through the grant TEC2017-88243-R. K.A. thanks support, in part, from PRESTO, JST JPMJPR1861. A.N. acknowledges support from a FPU scholarship from the Spanish Ministry of Education. M.R. acknowledges the support of UK EPSRC Grant EP/M013472/1. G.K. acknowledges financial support by the JSPS Kakenhi (C) No. 17K05591.

Author contributions

G.C.-L. performed the analytical calculations and the numerical simulations. A.N. constructed the analytical decoy-state estimation method. G.K. derived the security bounds in Supplementary Note A. All the authors contributed to discussing the main ideas of the security proof, checking the validity of the results, and writing the paper.

Competing interests

The authors declare no competing interests.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sept. 2009. 136

[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics*, vol. 8, pp. 595–604, July 2014.

[3] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photonics*, Feb. 2020. 136

[4] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, p. 190501, 2016. 136

[5] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, p. 190502, Nov. 2018. 136

[6] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar. 2011. 136

[7] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett.*, vol. 102, p. 050503, Feb. 2009. 136

[8] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nat. Commun.*, vol. 5, p. 5235, Oct. 2014. 138

[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, p. 15043, Apr. 2017. 145

[10] M. M. Wilde, M. Tomamichel, and M. Berta, "Converse bounds for private communication over quantum channels," *IEEE Trans. Inf. Theory*, vol. 63, pp. 1792–1817, Mar. 2017. 138, 145

[11] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, "Theory of channel simulation and bounds for private communication," *Quantum Sci. Technol.*, vol. 3, p. 035009, May 2018. 136

[12] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar. 2012. 136

[13] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 16, p. 043005, Apr. 2014. 136

[14] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Phys. Rev. A*, vol. 89, p. 012301, Jan. 2014. 136

[15] K. Azuma, K. Tamaki, and W. J. Munro, "All-photonic intercity quantum key distribution," *Nat. Commun.*, vol. 6, p. 10171, Dec. 2015. 136

[16] L.-M. Duan, M. Lukin, J. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413–418, Nov. 2001. 136

[17] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, pp. 123–130, May 2015. 136

[18] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, pp. 60–64, Apr. 2020. 136

[19] R. Trényi, K. Azuma, and M. Curty, "Beating the repeaterless bound with adaptive measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 21, p. 113052, Nov. 2019. 136

[20] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, "Overcoming the Rate–Distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, May 2018. 136

[21] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound," *arXiv preprint arXiv:1805.05511*, 2018. 136

[22] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, p. 031043, Aug. 2018. 136

[23] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nat. Photonics*, vol. 13, pp. 334–338, Mar. 2019. 136, 137, 145

[24] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Phys. Rev. Lett.*, vol. 123, p. 100506, Sept. 2019. 137

[25] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution through sending or not sending," *Phys. Rev. Lett.*, vol. 123, p. 100505, Sept. 2019.

[26] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev. X*, vol. 9, p. 021046, June 2019. 136, 137

[27] J. Lin and N. Lütkenhaus, "Simple security analysis of phase-matching measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 98, p. 042332, Oct. 2018. 136

[28] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Inf.*, vol. 5, p. 64, July 2019. 137, 138, 139, 149

[29] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection," *Phys. Rev. Appl.*, vol. 11, p. 034053, Mar. 2019.

[30] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A*, vol. 98, p. 062323, Dec. 2018. 136, 137, 138, 145, 146, 149

[31] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, p. 045018, Apr. 2009. 137

[32] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug. 2003. 137, 156

[33] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, June 2005.

[34] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, p. 230503, June 2005. 137, 156

[35] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nat. Commun.*, vol. 5, p. 3732, Apr. 2014. 138, 142, 144, 157

[36] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A*, vol. 90, p. 052314, Nov. 2014. 138

[37] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources," *New J. Phys.*, vol. 17, p. 093011, Sept. 2015. 138

[38] G. Kato, "Concentration inequality using unconfirmed knowledge," *arXiv preprint arXiv:2002.04357*, 2020. 138, 143, 157

[39] K. Azuma, "Weighted sums of certain dependent random variables," *Tohoku Math. J.*, vol. 19, no. 3, pp. 357–367, 1967. 138, 143, 157

[40] K. Maeda, T. Sasaki, and M. Koashi, "Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit," *Nat. Commun.*, vol. 10, p. 3140, July 2019. 138, 145, 148, 150

[41] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, "Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses," *Phys. Rev. Appl.*, vol. 12, p. 024061, Aug. 2019. 138, 142, 145, 146, 149

[42] F. Grasselli, Á. Navarrete, and M. Curty, "Asymmetric twin-field quantum key distribution," *New J. Phys.*, vol. 21, p. 113032, Nov. 2019. 139, 150, 157

[43] W. Wang and H.-K. Lo, "Simple method for asymmetric twin-field quantum key distribution," *New J. Phys.*, vol. 22, p. 013020, Jan. 2020. 139, 150

[44] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A*, vol. 89, p. 022307, Feb. 2014. 142

[45] R. Serfling, "Probability inequalities for the sum in sampling without replacement," *Ann. Stat.*, vol. 2, pp. 39–48, Jan. 1974. 142

[46] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," in *Theory of Cryptography Conference*, vol. 3378, pp. 386–406, Springer, 2005. 143

[47] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography Conference*, vol. 3378, pp. 407–425, Springer, 2005. 143

[48] R. Laurenza, S. Tserkis, L. Banchi, S. L. Braunstein, T. C. Ralph, and S. Pirandola, "Tight bounds for private communication over bosonic Gaussian channels based on teleportation simulation with optimal finite resources," *Phys. Rev. A*, vol. 100, p. 042301, Oct. 2019. 145

[49] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin, and S. Nam, "Detecting single infrared photons with 93% system efficiency," *Nat. Photonics*, vol. 7, pp. 210–214, Feb. 2013. 146

[50] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nat. Commun.*, vol. 3, p. 634, Jan. 2012. 146

[51] J. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Math.*, vol. 30, no. 0, pp. 175–193, 1906. 154

[52] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A*, vol. 95, p. 012333, Jan. 2017. 156

[53] S. Bahrani, O. Elmabrok, G. Currás Lorenzo, and M. Razavi, "Wavelength assignment in quantum access networks with hybrid wireless-fiber links," *J. Opt. Soc. Am. B*, vol. 36, p. B99, Feb. 2019. 156

[54] F. Grasselli and M. Curty, "Practical decoy-state method for twin-field quantum key distribution," *New J. Phys.*, vol. 21, p. 073001, July 2019. 157

Chapter 5

Twin-field quantum key distribution with fully discrete phase randomization

5.1 Abstract

Twin-field (TF) quantum key distribution (QKD) can overcome fundamental secret-key-rate bounds on point-to-point QKD links, allowing us to reach longer distances than ever before. Since its introduction, several TF-QKD variants have been proposed, and some of them have already been implemented experimentally. Most of them assume that the users can emit weak coherent pulses with a continuous random phase. In practice, this assumption is often not satisfied, which could open up security loopholes in their implementations. To close this loophole, we propose and prove the security of a TF-QKD variant that relies exclusively on discrete phase randomization. Remarkably, our results show that it can also provide higher secret-key rates than an equivalent continuous-phase-randomized protocol.

5.2 Introduction

Quantum key distribution (QKD) allows two users, Alice and Bob, to generate a shared secret key in the presence of an eavesdropper, Eve, with unlimited computational power. Despite its great potential, QKD has yet to overcome important practical problems before it is ready for widespread use. One of the most important challenges is how

to perform QKD at long distances, given that, in optical fibres, the loss increases exponentially with the channel length. Even with a GHz repetition rate, it would take 300 years to successfully send a single photon over 1000 km of standard optical fibres [1]. Another crucial issue is to guarantee that a particular implementation of a QKD protocol is secure. That is, we have to show that QKD implementations satisfy all assumptions made in their corresponding theoretical security proof, or to devise security proofs that match the realities of QKD experiments. In this work, we address the latter issue for twin-field QKD (TF-QKD) [2], one of the key candidates for improving key-rate scaling with distance.

Fundamental bounds show that the key rate of repeaterless QKD protocols scales at best linearly with η [3], where η is the transmittance of the channel connecting Alice and Bob. TF-QKD breaks this limitation, offering a key rate that scales with $\sqrt{\eta}$. The key enabling idea behind the operation of TF-QKD is to effectively generate an entangled state between the two users in the space spanned by vacuum and single-photon states. To do so, we need a repeater node that performs entanglement swapping, using single-photon interference, as well as phase stability across the channel, to make sure the generated state is in the desired superposition form. This approach requires only one photon to survive the path loss over half of the channel, thus the improved scaling with distance. Note that TF-QKD is not the only protocol that achieves this scaling. Other protocols, inspired by quantum repeater structures, can achieve the same key-rate scaling by using quantum memories [4, 5] or quantum non-demolition measurements [6]. However, TF-QKD is, experimentally, in a more advanced state than such alternatives. In fact, certain variants of TF-QKD have already been implemented [7–10], and a distance record exceeding 500 km has already been achieved [11, 12]. The issue of implementation security is crucially relevant for these experiments.

One of the main constraints on a QKD system is given by the type of optical encoder needed in the implementation of the protocol. Its corresponding security proof would then need to address such practical constraints. The single-photon version of TF-QKD has a simple theoretical description [13], but it is difficult to implement in practice. Thus, a significant research effort has focused on developing practical variants [13–16] in which the users encode weak coherent pulses (WCPs). These variants differ in their protocol descriptions and/or security proofs, but, so far, all of them rely on the decoy-state method [17]. That is, they either use decoy states in their key mode [14, 15],

i.e., to generate the key, and/or in their test mode [13, 16], i.e., to estimate Eve's side information on the key.

Conventional decoy-state techniques require the emission of phase-randomized coherent states (PRCS), and assume that the users are ideally able to randomize the phase of their pulses *continuously* and *uniformly*. This is, however, difficult to achieve in practice. Experimentally, there are two approaches to randomize the phase of a coherent pulse: passive and active. Passive randomization consists of turning the laser off and then on again to generate the PRCS. In addition to the impracticality of this approach in a high-speed QKD system, it is hard to guarantee experimentally that the generated phase genuinely follows a uniform distribution [18]. In fact, experiments have shown that, in practice, there are phase correlations between adjacent pulses [19, 20]. In an active randomization procedure, a phase modulator is used, in combination with a random number generator. This approach fits the TF-QKD variant of Refs. [13, 16] very well, since one already needs a phase modulator to produce the phase-locked coherent states emitted in the key mode. However, it randomizes the phase over a *discrete*, not *continuous*, set of values. Thus, none of these two approaches necessarily satisfy the assumptions of the decoy-state method, which could open security loopholes in the experimental implementations of TF-QKD.

In this work, we address this security loophole, by proposing and proving the security of a TF-QKD variant that relies exclusively on discrete phase randomization. Note that the use of discrete randomization has already been considered in Ref. [18], in the context of a decoy-state BB84 protocol, where it was treated as a source flaw. Its authors found that, for the decoy-state BB84 protocol, the secret key rate obtainable using discrete randomization is always strictly worse than using continuous randomization, although the former quickly approaches the latter as the number of discrete random phases increases. In fact, in that protocol, one can obtain a performance reasonably close to the continuous case using as few as ten discrete random phases. However, it is not immediately clear whether this behaviour would hold for the TF-QKD variants in [13–16], given that: (i) their security proofs are quite diverse, and some of them very different from that of decoy-state BB84; and (ii) in TF-QKD, both users emit quantum states, and thus the source flaw is present in both users. In fact, recent works have found that the security issue arising from flawed sources that leak information has a much bigger impact in measurement-device-independent (MDI) QKD [21] than in

BB84 [22]. In principle, the same could be true for other kinds of source imperfections, such as the use of discrete phase randomization.

The quantum phase of our TF-QKD variant is similar to that of Ref. [13], with the main difference being that we use discrete, not continuous, phase randomization in test mode. However, unlike in the case of decoy-state BB84 [18], we find that our key rate does not simply approach that of Ref. [13] as the number of phase slices increases. Instead, perhaps surprisingly, we can actually obtain *higher* secret-key rates than Ref. [13], with as few as eight discrete random phases. The reason is that discrete randomization allows us to postselect the test-mode rounds in which the users' phase choices exactly *matched*, i.e., they were exactly the same, or their difference was exactly π. As we will see, this postselected data allows for a tighter estimation of the phase-error rate. Intuitively, this is because, in TF-QKD, it is advantageous if the users share the same global phase reference, something that can be equivalently achieved by postselection.

We note that the concept of phase postselection has appeared in other TF-QKD variants [14, 15, 23], although in combination with continuous-phase-randomized signals. Refs. [14, 15] postselect the signals with a *similar*, not *identical*, phase. This introduces challenges in the security analysis, and it is not clear if this approach could be used for the type of TF-QKD variant considered in this work. Ref. [23] assumes that signals with an *identical* phase are postselected. While certainly interesting from a theoretical point of view, this protocol is not implementable in practice, since Alice and Bob will never choose exactly the same phase when using continuous phase randomization.

Similarly to other protocols that rely on discrete randomization [18], we use numerical techniques as part of our security proof. In particular, inspired by the work of Ref. [24], we use semidefinite programming (SDP) techniques to estimate the phase-error rate. We note that, in Ref. [24], the authors already apply their generic numerical technique to prove the security of a TF-QKD protocol with discrete phase randomization. However, in practice, their procedure can only be applied when just a few discrete random phases are used, since the number of constraints grows very quickly as the number of phase values increases. Here, we exploit the particularities of our protocol to introduce an analysis that uses a much smaller number of carefully chosen

constraints, and is efficient even with a large number of discrete phases. This allows us to investigate how the key rate improves when increasing the number of phase values.

5.3 Methods

5.3.1 Protocol description

Our protocol is very similar to that of Refs. [13, 16]. Alice and Bob send quantum signals to an untrusted middle node Charlie, who (ideally) interferes them at a balanced 50:50 beamsplitter, performs a photodetection measurement, and reports the outcome. These signals belong to one of two "modes", key and test, selected at random. Key-mode emissions are used to generate the raw key, while test-mode emissions are used to estimate Eve's side information. In key mode, the users send phase-locked coherent states $\left|\pm\sqrt{\mu}\right\rangle$. In test mode, the users send phase-randomized coherent states of different intensities. Unlike in Refs. [13, 16], the phases of the test-mode states are randomized over a *discrete* set, rather than a continuous range. The detailed protocol steps are the following:

(1) *Preparation*

Alice (Bob) randomly choose the transmission mode, key or test, and

(1.1) If she (he) chooses key mode, she (he) generates a random bit b_A (b_B), prepares an optical pulse in the coherent state $\left|(-1)^{b_A}\sqrt{\mu}\right\rangle$ ($\left|(-1)^{b_B}\sqrt{\mu}\right\rangle$), and sends it to Charlie.

(1.2) If she (he) chooses test mode, she (he) selects a random intensity β_a (β_b) $\in \{\beta_1, \ldots, \beta_{d-2}, \mu, \beta_v\}$, where d is the number of intensities, μ is the same intensity used in key mode, and $\beta_v = 0$ is a vacuum intensity. Then, she (he) selects a random phase θ_a (θ_b) $= \frac{2\pi m}{M}$, where $m \in \{0, 1, 2, \ldots, M-1\}$ and M is the number of random phases, prepares the state $\left|\sqrt{\beta_a}e^{i\theta_a}\right\rangle$ ($\left|\sqrt{\beta_b}e^{i\theta_b}\right\rangle$), and sends it to Charlie.

(2) *Detection*

An honest Charlie interferes Alice and Bob's signals at a 50:50 beamsplitter, followed by threshold detectors D_c and D_d, placed at the output ports corresponding

to constructive and destructive interference, respectively. A round is considered successful if exactly one detector clicks, and unsuccessful otherwise. After the measurement, Charlie reports whether or not the round was successful, and, if it was, he reports which specific detector clicked.

(3) *Sifting*

For all successful rounds, Alice and Bob disclose their choices of key mode or test mode, keeping only data from those in which they have used the same mode. Then,

(3.1) They calculate the gain p_{succ} of their key mode rounds, and generate their sifted keys from the values of b_A and b_B corresponding to these rounds. Then, they publicly disclose a small random subset of their sifted keys. With this information, they estimate the fraction of the sifted key, $p_{\text{same|succ}}$ ($p_{\text{diff|succ}}$), that originated from emissions in which their phase choices agreed (disagreed). Bob then flips his sifted key bits corresponding to the rounds in which D_d clicked. Based on that, Alice and Bob estimate the bit error rate e_{bit}.

(3.2) For all values of β, Alice and Bob calculate the gains $\{Q_\beta\}$ of the test mode rounds in which they both used intensity β and the same phase $\theta_a = \theta_b$. They also calculate the gains $\{Q_\beta^-\}$ of the rounds in which they both used intensity β and opposite phases $\theta_a = \theta_b \pm \pi$.

(4) *Parameter estimation*

Alice and Bob use the values of $\{Q_\beta\}$ and $\{Q_\beta^-\}$ to estimate the amount of key information I_{AE} that may have been leaked to an eavesdropper.

(5) *Postprocessing*

Alice and Bob perform error correction and privacy amplification to obtain a secret key.

Since this is a discretely-modulated MDI-type protocol, in principle, one could directly use the numerical techniques of Ref. [24] to prove its security. However, the SDP

in Ref. [24] requires one constraint, in the form of an inner product, for each combination of emitted states. The number of different states in this protocol can make such an approach infeasible in practice. Namely, since Alice and Bob send $[(d-1)M+1]^2$ different joint states [1], one needs to solve the dual problem of an SDP with $[(d-1)M+1]^4$ inner-product constraints, plus the constraints related to the measurement results of the protocol. Thus, even for $M=4$ and $d=3$, the simplest case considered in the numerical results of this paper, one needs to solve a SDP with more than 6561 constraints. For $M=12$ and $d=3$, the number of constraints grows to more than 390625. This can make the implementation of such techniques infeasible on conventional computers [25, 26].

In the following, we provide a security analysis that requires to solve the dual problem of two SDPs with only $(d-1)(d-2)M+2d+M-1$ constraints each. That is, for the examples considered above, we have SDPs with 17 and 41 constraints, respectively, which can be quickly solved using any commercial off-the-shelf laptop.

5.3.2 Security analysis

In our security analysis, we consider the asymptotic scenario in which the users emit an infinite number of signals. Also, for simplicity, we assume collective attacks. We note that, in the asymptotic regime, security against collective attacks implies security against general attacks, thanks to results such as the postselection technique [27].

We consider the virtual protocol in which Alice replaces her key mode emissions by the generation of the state

$$|\psi\rangle_{Aa} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|\sqrt{\mu}\rangle_a + |1\rangle_A|-\sqrt{\mu}\rangle_a\right), \tag{5.1}$$

where A is a virtual qubit ancilla that she keeps in her lab, and a is the photonic system sent to Charlie; and Bob replaces them by a similarly defined $|\psi\rangle_{Bb}$. We assume that Eve controls not only the quantum channels, but also the untrusted middle node Charlie, and the announcements he makes. As mentioned in the protocol description, for each round, Alice and Bob expect to receive two announcements: whether the round was successful, and, if so, whether Charlie obtained constructive or destructive

[1] To compute the number of states, note that the set of test-mode states contains the set of key-mode states, so one only needs to count the former. Also, when Alice or Bob choose the vacuum intensity, they send the same vacuum state, independently of their choice of random phase.

interference. However, the latter announcement only determines whether or not Bob flips his sifted key bit, which does not affect Eve's side information on Alice's key. Thus, from a security standpoint, we can describe Eve's collective attack as a two-outcome general measurement $\{\hat{M}_{ab}, \hat{M}^f_{ab}\}$ on the photonic systems ab, where $\hat{M}_{ab}$ ($\hat{M}^f_{ab}$) is the Kraus operator corresponding to the announcement of the round as successful (unsuccessful). Conditioned on a successful announcement, Alice and Bob obtain a state,

$$|\Psi\rangle_{AaBb} = \frac{\hat{M}_{ab}\,|\psi\rangle_{Aa}\,|\psi\rangle_{Bb}}{\sqrt{p_{\text{succ}}}}, \tag{5.2}$$

where $p_{\text{succ}} = \left\| \hat{M}_{ab}\,|\psi\rangle_{Aa}\,|\psi\rangle_{Bb} \right\|^2$ is the probability that Eve announces a key mode round as successful.

In our virtual protocol, after Eve's announcements, Alice and Bob perform the joint measurement $\{\hat{O}_{\text{same}}, \hat{O}_{\text{diff}}\}$, with $\hat{O}_{\text{same}} = |00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}$ and $\hat{O}_{\text{diff}} = |01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}$, on the ancillas corresponding to the successful rounds, learning whether they used the same or different phases. Note that this is a valid virtual protocol step, since it commutes with the Z-basis measurement that Alice and Bob would perform to generate their sifted keys. Depending on the result of their joint measurement, they will obtain one of the two post-measurement states

$$|\Psi_{\text{same}}\rangle = \frac{|00\rangle_{AB}\,\hat{M}_{ab}\left|\sqrt{\mu}\right\rangle_a\left|\sqrt{\mu}\right\rangle_b + |11\rangle_{AB}\,\hat{M}_{ab}\left|-\sqrt{\mu}\right\rangle_a\left|-\sqrt{\mu}\right\rangle_b}{2\sqrt{p_{\text{succ,same}}}}, \tag{5.3}$$

$$|\Psi_{\text{diff}}\rangle = \frac{|01\rangle_{AB}\,\hat{M}_{ab}\left|\sqrt{\mu}\right\rangle_a\left|-\sqrt{\mu}\right\rangle_b + |10\rangle_{AB}\,\hat{M}_{ab}\left|-\sqrt{\mu}\right\rangle_a\left|\sqrt{\mu}\right\rangle_b}{2\sqrt{p_{\text{succ,diff}}}}, \tag{5.4}$$

where $p_{\text{succ,same}} = p_{\text{succ}} p_{\text{same}|\text{succ}}$ ($p_{\text{succ,diff}} = p_{\text{succ}} p_{\text{diff}|\text{succ}}$) is the probability that Alice and Bob use the same (different) phases in a key mode round *and* Eve reports the round as successful. This allows us to define the quantities

$$e_{\text{ph,same}} = \|\,{}_{AB}\langle ++|\Psi_{\text{same}}\rangle\|^2 + \|\,{}_{AB}\langle --|\Psi_{\text{same}}\rangle\|^2, \tag{5.5}$$

$$e_{\text{ph,diff}} = \|\,{}_{AB}\langle ++|\Psi_{\text{diff}}\rangle\|^2 + \|\,{}_{AB}\langle --|\Psi_{\text{diff}}\rangle\|^2, \tag{5.6}$$

where $e_{\text{ph,same}}$ ($e_{\text{ph,diff}}$) is the phase-error rate of the successful key mode rounds in which Alice and Bob used the same (different) phases. Eve's side information of the sifted key (per key bit) can now be bounded by

$$I_{AE} \leq p_{\text{same}|\text{succ}} h(e_{\text{ph,same}}) + p_{\text{diff}|\text{succ}} h(e_{\text{ph,diff}}), \tag{5.7}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon binary entropy function. The secret key rate that Alice and Bob can distill is

$$R \geq p_{\text{succ}}\left[1 - I_{AE} - fh(e_{\text{bit}})\right], \tag{5.8}$$

where f is the error correction inefficiency.

The objective of our security analysis is to obtain upper bounds on $e_{\text{ph,same}}$ and $e_{\text{ph,diff}}$, using the the data obtained in the test rounds. The procedure is very similar for both terms; we will first explain $e_{\text{ph,same}}$.

5.3.2.1 Estimation of $e_{\text{ph,same}}$

First, we rewrite Eq. (5.3) as

$$|\Psi_{\text{same}}\rangle = \frac{(|{+}{+}\rangle + |{-}{-}\rangle)_{AB}\,\hat{M}_{ab}\,|\lambda_{\text{even}}\rangle_{ab} + (|{+}{-}\rangle + |{-}{+}\rangle)_{AB}\,\hat{M}_{ab}\,|\lambda_{\text{odd}}\rangle_{ab}}{2\sqrt{p_{\text{succ,same}}}}, \tag{5.9}$$

with $|\lambda_{\text{even}}\rangle_{ab}$ and $|\lambda_{\text{odd}}\rangle_{ab}$ being unnormalized states defined as

$$|\lambda_{\text{even}}\rangle_{ab} = \frac{1}{2}(|\sqrt{\mu}\rangle_a\,|\sqrt{\mu}\rangle_b + |{-}\sqrt{\mu}\rangle_a\,|{-}\sqrt{\mu}\rangle_b) = \sum_{n\in\mathbb{N}_0}\sqrt{P_{n|\mu}}\,|\lambda_n\rangle_{ab}\,, \tag{5.10}$$

$$|\lambda_{\text{odd}}\rangle_{ab} = \frac{1}{2}(|\sqrt{\mu}\rangle_a\,|\sqrt{\mu}\rangle_b - |{-}\sqrt{\mu}\rangle_a\,|{-}\sqrt{\mu}\rangle_b) = \sum_{n\in\mathbb{N}_1}\sqrt{P_{n|\mu}}\,|\lambda_n\rangle_{ab}\,, \tag{5.11}$$

where $\mathbb{N}_0$ ($\mathbb{N}_1$) is the set of non-negative even (odd) numbers, $|\lambda_n\rangle_{ab}$ is the n-photon two-mode Fock state defined by

$$|\lambda_n\rangle_{ab} = \frac{1}{\sqrt{2^n n!}}(a^\dagger + b^\dagger)^n\,|00\rangle_{ab}\,, \tag{5.12}$$

and

$$P_{n|\mu} = \frac{e^{-2\mu}(2\mu)^n}{n!}, \tag{5.13}$$

follows a Poisson distribution of average 2μ. Combining Eq. (5.5) and Eq. (5.9), we have that

$$e_{\text{ph,same}} = \frac{1}{2p_{\text{succ,same}}}\left\|\hat{M}_{ab}\,|\lambda_{\text{even}}\rangle_{ab}\right\|^2. \tag{5.14}$$

Finding a way to estimate the quantity in Eq. (5.14) is critical for our security proof. One possible approach would be to apply the Cauchy-Schwarz inequality to show that

$$\left\|\hat{M}_{ab}\,|\lambda_{\text{even}}\rangle_{ab}\right\|^2 \leq \left[\sum_{n\in\mathbb{N}_0}\sqrt{P_{n|\mu}Y_n}\right]^2, \tag{5.15}$$

where $Y_n = \left\| \hat{M}_{ab} \left| \lambda_n \right\rangle_{ab} \right\|^2$ is the yield probability of the state $\left| \lambda_n \right\rangle_{ab}$. Let us assume that Alice and Bob used continuous phase-randomization on their test mode emissions, and kept only the data from the events in which they use the same intensity and the same phase. Then, the resulting post-selected state, given that they both chose intensity β, can be expressed as

$$\frac{1}{2\pi} \int_0^{2\pi} d\theta \left| \sqrt{\beta} e^{i\theta} \right\rangle \left| \sqrt{\beta} e^{i\theta} \right\rangle \left\langle \sqrt{\beta} e^{i\theta} \right| \left\langle \sqrt{\beta} e^{i\theta} \right|_{ab} = \sum_{n=0}^{\infty} P_{n|\beta} \left| \lambda_n \right\rangle\!\left\langle \lambda_n \right|_{ab}, \tag{5.16}$$

where $P_{n|\beta}$ follows a Poisson distribution and is given by Eq. (5.13). Then, one could apply the standard decoy-state method to estimate the yield probabilities Y_n, $\forall n \in \mathbb{N}_0$, and plug these in Eq. (5.15) to estimate $e_{\text{ph,same}}$ in Eq. (5.14). Essentially, this is the approach of Ref. [23]. However, note that if Alice and Bob use continuous phase-randomization, the probability that they select exactly the same phase θ is zero, and the resulting protocol is not implementable in practice.

Here, we use the same test-mode phase-postselection idea as in Ref. [23], but we employ discrete phase randomization, which results in a protocol that is actually implementable. In this case, Eq. (5.16) becomes

$$\begin{aligned} \rho_\beta &= \frac{1}{M} \sum_{m=0}^{M-1} \left| \sqrt{\beta} e^{\frac{2i\pi m}{M}} \right\rangle \left| \sqrt{\beta} e^{\frac{2i\pi m}{M}} \right\rangle \left\langle \sqrt{\beta} e^{\frac{2i\pi m}{M}} \right| \left\langle \sqrt{\beta} e^{\frac{2i\pi m}{M}} \right|_{ab} \\ &= \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} \left| \lambda^{\beta}_{n \bmod M} \right\rangle\!\left\langle \lambda^{\beta}_{n \bmod M} \right|_{ab}, \end{aligned} \tag{5.17}$$

where ρ_β is the post-selected state when Alice and Bob both used intensity β and the same phase [18]. In Eq. (5.17), we have that

$$\left| \lambda^{\beta}_{n \bmod M} \right\rangle_{ab} = \sum_{l=0}^{\infty} \sqrt{\frac{P_{Ml+n|\beta}}{P^{\beta}_{n \bmod M}}} \left| \lambda_{Ml+n} \right\rangle_{ab}, \tag{5.18}$$

$$P^{\beta}_{n \bmod M} = \sum_{l=0}^{\infty} P_{Ml+n|\beta}. \tag{5.19}$$

and $P_{n|\beta}$ is given by Eq. (5.13). Note that for the vacuum intensity β_v, we have

$$\rho_{\beta_v} = \left| \lambda^{\beta_v}_{0 \bmod M} \right\rangle\!\left\langle \lambda^{\beta_v}_{0 \bmod M} \right|_{ab} = \left| \lambda_0 \right\rangle\!\left\langle \lambda_0 \right|_{ab}. \tag{5.20}$$

Unlike the states $\left| \lambda_n \right\rangle$ in Eq. (5.16), the states $\left| \lambda^{\beta}_{n \bmod M} \right\rangle$ in Eq. (5.17) have a slight dependence on the intensity β. Thus, their yield probabilities,

$$Y^{\beta}_{n \bmod M} = \left\| \hat{M}_{ab} \left| \lambda^{\beta}_{n \bmod M} \right\rangle_{ab} \right\|^2, \tag{5.21}$$

are not necessarily equal for two different intensities β_1 and β_2, which prevents us from applying the standard decoy-state method. Instead, we use a similar idea as in Ref. [24], defining the Gram matrix G of the set of Eve's post-measurement states, and constructing a semidefinite program in which the objective function and all the constraints are linear functions of entries of G. In our case, we define G as the Gram matrix of the vector set $\left\{\hat{M}_{ab}\left|\lambda^{\beta}_{n \bmod M}\right\rangle\right\}$, $\forall \beta \in \mathcal{T}$ and $n \in \{0, 1, ..., M-1\}$, where $\mathcal{T}$ is the set of all test-mode intensities, except vacuum. The entries of G are $G_{ij} = \langle i|j\rangle$, where $|i\rangle$ denotes the i-th element of the vector set.

Our objective function is Eq. (5.14), which we can write as

$$e_{\text{ph,same}} = \frac{1}{2p_{\text{succ,same}}} \langle \lambda_{\text{even}}|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}|\lambda_{\text{even}}\rangle \,. \tag{5.22}$$

By re-expressing $|\lambda_{\text{even}}\rangle$ and $|\lambda_{\text{odd}}\rangle$ in Eqs. (5.10) and (5.11) as

$$\begin{aligned} |\lambda_{\text{even}}\rangle_{ab} &= \sum_{\substack{n=0 \\ n\in\mathbb{N}_0}}^{M-1} \sqrt{P^{\mu}_{n \bmod M}}\, \left|\lambda^{\mu}_{n \bmod M}\right\rangle_{ab}, \\ |\lambda_{\text{odd}}\rangle_{ab} &= \sum_{\substack{n=0 \\ n\in\mathbb{N}_1}}^{M-1} \sqrt{P^{\mu}_{n \bmod M}}\, \left|\lambda^{\mu}_{n \bmod M}\right\rangle_{ab}, \end{aligned} \tag{5.23}$$

it becomes clear that the right-hand side of Eq. (5.22) is a linear function of elements of G.

Our constraints are the following:

- Taking the norm squared of both sides of Eq. (5.3), and solving for $p_{\text{succ,same}}$, we obtain

$$p_{\text{succ,same}} = \frac{1}{2} \langle \lambda_{\text{even}}|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}|\lambda_{\text{even}}\rangle + \frac{1}{2} \langle \lambda_{\text{odd}}|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}|\lambda_{\text{odd}}\rangle \,. \tag{5.24}$$

- From Eq. (5.17), we have that

$$Q_{\beta} = \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} Y^{\beta}_{n \bmod M}, \tag{5.25}$$

  where Q_{β} is the measured gain of the state ρ_{β}. Note that $Y^{\beta}_{n \bmod M}$ is a (diagonal) element of G, thus Eq. (5.25) is a linear function of elements of G.

- Using the trace distance inequality [18], we obtain

$$Y^{\beta_1}_{n \bmod M} - Y^{\beta_2}_{n \bmod M} \leq \sqrt{1 - F_n^{\beta_1,\beta_2}}, \tag{5.26}$$

where

$$F_n^{\beta_1,\beta_2} = \left| \left\langle \lambda^{\beta_1}_{n \bmod M} \middle| \lambda^{\beta_2}_{n \bmod M} \right\rangle_{ab} \right|^2 = \left[\sum_{l=0}^{\infty} \sqrt{\frac{P_{Ml+n|\beta_1}}{P^{\beta_1}_{n \bmod M}}} \sqrt{\frac{P_{Ml+n|\beta_2}}{P^{\beta_2}_{n \bmod M}}} \right]^2. \tag{5.27}$$

- Our next constraint is based on the inequality

$$\begin{aligned} Y^{\beta_1}_{n \bmod M} \leq & 1 - Y^{\beta_2}_{n \bmod M} + 2\sqrt{F_n^{\beta_1,\beta_2}(1 - F_n^{\beta_1,\beta_2})(1 - Y^{\beta_2}_{n \bmod M})Y^{\beta_2}_{n \bmod M}} \\ & + F_n^{\beta_1,\beta_2}(2Y^{\beta_2}_{n \bmod M} - 1), \end{aligned} \tag{5.28}$$

which holds when $Y^{\beta_2}_{n \bmod M} \leq F_n^{\beta_1,\beta_2}$ [28]. This bound is tighter than the trace distance inequality in Eq. (5.26), but cannot be directly added to the SDP, since it is a non-linear function of $Y^{\beta_2}_{n \bmod M}$, an element of G. The only exception is the case $n = 0$ and $\beta_2 = \beta_v$, since from Eq. (5.20), we have that

$$Y^{\beta_v}_{0 \bmod M} = Y_0 = Q_{\beta_v}, \tag{5.29}$$

and Q_{β_v}, the gain of the vacuum intensity, is directly measurable from the protocol. Thus, substituting $n = 0$, $\beta_1 = \beta$, $\beta_2 = \beta_v$ and $Y^{\beta_v}_{0 \bmod M} = Q_{\beta_v}$ in Eq. (5.28), we have the inequality

$$Y^{\beta}_{0 \bmod M} \leq 1 - Q_{\beta_v} + 2\sqrt{F_0^{\beta,\beta_v}(1 - F_0^{\beta,\beta_v})(1 - Q_{\beta_v})Q_{\beta_v}} + F_0^{\beta,\beta_v}(2Q_{\beta_v} - 1), \tag{5.30}$$

which is a linear function of $Y^{\beta}_{0 \bmod M}$. Equation (5.30) holds when $Q_{\beta_v} \leq F_0^{\beta,\beta_v}$, which should always happen in practice, since $Q_{\beta_v} \approx 0$ and $F_0^{\beta,\beta_v} \approx 1$.

- For our final constraints, we use the fact that $Y^{\beta}_{n \bmod M} \leq 1$, $\forall n, \beta$. To reduce the number of constraints, we only include the case $\beta = \mu$.

Combining everything, we have that our upper-bound on $e_{\text{ph,same}}$ is the solution of

the following SDP:

$$
\begin{aligned}
&\max_{G} \quad \frac{1}{2p_{\text{succ,same}}} \langle \lambda_{\text{even}} | \hat{M}_{ab}^{\dagger} \hat{M}_{ab} | \lambda_{\text{even}} \rangle \ \text{ s.t.} \\
&p_{\text{succ,same}} = \frac{1}{2} \langle \lambda_{\text{even}} | \hat{M}_{ab}^{\dagger} \hat{M}_{ab} | \lambda_{\text{even}} \rangle + \frac{1}{2} \langle \lambda_{\text{odd}} | \hat{M}_{ab}^{\dagger} \hat{M}_{ab} | \lambda_{\text{odd}} \rangle ; \\
&Q_{\beta} = \sum_{n=0}^{M-1} P_{n \bmod M}^{\beta} Y_{n \bmod M}^{\beta}, \quad \forall \beta \in \mathcal{T}; \\
&Y_{n \bmod M}^{\mu} \leq 1, \quad \forall n \in \{0, ..., M-1\}; \\
&Y_{n \bmod M}^{\beta_1} - Y_{n \bmod M}^{\beta_2} \leq \sqrt{1 - F_n^{\beta_1, \beta_2}}, \quad \forall \beta_1, \beta_2 \in \mathcal{T}, \ n \in \{0, ..., M-1\}; \\
&Y_{0 \bmod M}^{\beta} \leq 1 - Q_{\beta_v} + 2\sqrt{F_0^{\beta, \beta_v}(1 - F_0^{\beta, \beta_v})(1 - Q_{\beta_v}) Q_{\beta_v}} + F_0^{\beta, \beta_v}(2Q_{\beta_v} - 1), \quad \forall \beta \in \mathcal{T};
\end{aligned}
\tag{5.31}
$$

where $\mathcal{T} = \{\beta_1, \ldots, \beta_{d-2}, \mu\}$ is the set of all test-mode intensities, except vacuum.

5.3.2.2 Estimation of $e_{\text{ph,diff}}$

The procedure to estimate $e_{\text{ph,diff}}$ is very similar to that of $e_{\text{ph,same}}$. In this case, we rewrite Eq. (5.4) as

$$
|\Psi_{\text{diff}}\rangle = \frac{(|{+}{+}\rangle - |{-}{-}\rangle)_{AB} \hat{M}_{ab} |\lambda_{\text{even}}^{-}\rangle_{ab} + (|{-}{+}\rangle - |{+}{-}\rangle)_{AB} \hat{M}_{ab} |\lambda_{\text{odd}}^{-}\rangle_{ab}}{2\sqrt{p_{\text{succ,diff}}}}, \tag{5.32}
$$

where $|\lambda_{\text{even}}^{-}\rangle_{ab}$ and $|\lambda_{\text{odd}}^{-}\rangle_{ab}$ are unnormalized states defined as

$$
\begin{aligned}
|\lambda_{\text{even}}^{-}\rangle_{ab} &= \frac{1}{2}(|\sqrt{\mu}\rangle_a |{-}\sqrt{\mu}\rangle_b + |{-}\sqrt{\mu}\rangle_a |\sqrt{\mu}\rangle_b) \\
&= \sum_{n+m \in \mathbb{N}_0} c_n c_m |n\rangle_a |m\rangle_b = \sum_{n \in \mathbb{N}_0} \sqrt{P_{n|\mu}} |\lambda_n^{-}\rangle_{ab}, \qquad (5.33) \\
|\lambda_{\text{odd}}^{-}\rangle_{ab} &= \frac{1}{2}(|\sqrt{\mu}\rangle_a |{-}\sqrt{\mu}\rangle_b - |{-}\sqrt{\mu}\rangle_a |\sqrt{\mu}\rangle_b) \\
&= \sum_{n+m \in \mathbb{N}_1} c_n c_m |n\rangle_a |m\rangle_b = \sum_{n \in \mathbb{N}_1} \sqrt{P_{n|\mu}} |\lambda_n^{-}\rangle_{ab}, \qquad (5.34)
\end{aligned}
$$

$|\lambda_n^{-}\rangle_{ab}$ is the n-photon two-mode Fock state defined by

$$
|\lambda_n^{-}\rangle_{ab} = \frac{1}{\sqrt{2^n n!}} (a^{\dagger} - b^{\dagger})^n |00\rangle_{ab}, \tag{5.35}
$$

and $P_{n|\mu}$ is given by Eq. (5.13). In this case, the state after post-selecting the test mode emissions in which Alice and Bob both used intensity β and opposite phases

$\theta_a = \theta_b \pm \pi = \theta$ is

$$\begin{aligned}\rho_\beta^- &= \frac{1}{M}\sum_{m=0}^{M-1}\left|\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right\rangle\left|-\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right\rangle\left\langle\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right|\left\langle-\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right|_{ab} \\ &= \sum_{n=0}^{M-1} P^\beta_{n \bmod M}\left|\lambda^{\beta,-}_{n \bmod M}\right\rangle\!\left\langle\lambda^{\beta,-}_{n \bmod M}\right|_{ab},\end{aligned} \tag{5.36}$$

where

$$\left|\lambda^{\beta,-}_{n \bmod M}\right\rangle_{ab} = \sum_{l=0}^{\infty}\sqrt{\frac{P_{Ml+n|\beta}}{P^\beta_{n \bmod M}}}\left|\lambda^-_{Ml+n}\right\rangle_{ab}, \tag{5.37}$$

$P_{n|\beta}$ is given by Eq. (5.13), and $P^\beta_{n \bmod M}$ is given by Eq. (5.19).

Similarly as in the previous subsection, we re-express $|\lambda^-_{\text{even}}\rangle$ and $|\lambda^-_{\text{odd}}\rangle$ as

$$\begin{aligned}\left|\lambda^-_{\text{even}}\right\rangle_{ab} &= \sum_{\substack{n=0\\ n\in\mathbb{N}_0}}^{M-1}\sqrt{P^\mu_{n \bmod M}}\left|\lambda^{\mu,-}_{n \bmod M}\right\rangle_{ab}, \\ \left|\lambda^-_{\text{odd}}\right\rangle_{ab} &= \sum_{\substack{n=0\\ n\in\mathbb{N}_1}}^{M-1}\sqrt{P^\mu_{n \bmod M}}\left|\lambda^{\mu,-}_{n \bmod M}\right\rangle_{ab},\end{aligned} \tag{5.38}$$

and define

$$Y^{\beta,-}_{n \bmod M} = \left\|\hat{M}_{ab}\left|\lambda^{\beta,-}_{n \bmod M}\right\rangle_{ab}\right\|^2. \tag{5.39}$$

This time, we define G as the Gram matrix of the vector set $\left\{\hat{M}_{ab}\left|\lambda^{\beta,-}_{n \bmod M}\right\rangle\right\}$, and follow a similar procedure as in the last subsection to construct the objective function and the constraints. In the end, we have that our upper-bound on $e_{\text{ph,diff}}$ is the solution of the following SDP:

$$\begin{aligned}&\max_G \quad \frac{1}{2p_{\text{succ,diff}}}\langle\lambda^-_{\text{even}}|\hat{M}^\dagger_{ab}\hat{M}_{ab}|\lambda^-_{\text{even}}\rangle \text{ s.t.} \\ &p_{\text{succ,diff}} = \frac{1}{2}\langle\lambda^-_{\text{even}}|\hat{M}^\dagger_{ab}\hat{M}_{ab}|\lambda^-_{\text{even}}\rangle + \frac{1}{2}\langle\lambda^-_{\text{odd}}|\hat{M}^\dagger_{ab}\hat{M}_{ab}|\lambda^-_{\text{odd}}\rangle; \\ &Q^-_\beta = \sum_{n=0}^{M-1} P^\beta_{n \bmod M} Y^{\beta,-}_{n \bmod M}, \quad \forall\beta\in\mathcal{T}; \\ &Y^{\mu,-}_{n \bmod M} \le 1, \quad \forall n\in\{0,...,M-1\}; \\ &Y^{\beta_1,-}_{n \bmod M} - Y^{\beta_2,-}_{n \bmod M} \le \sqrt{1-F_n^{\beta_1,\beta_2}}, \quad \forall\beta_1,\beta_2\in\mathcal{T},\ n\in\{0,...,M-1\}; \\ &Y^{\beta,-}_{0 \bmod M} \le 1 - Q^-_{\beta_v} + 2\sqrt{F_0^{\beta,\beta_v}(1-F_0^{\beta,\beta_v})(1-Q^-_{\beta_v})Q^-_{\beta_v}} + F_0^{\beta,\beta_v}(2Q^-_{\beta_v}-1), \quad \forall\beta\in\mathcal{T};\end{aligned} \tag{5.40}$$

where $F_n^{\beta_1,\beta_2}$ is given by Eq. (5.27) and $\mathcal{T} = \{\beta_1,\ldots,\beta_{d-2},\mu\}$ is the set of all test-mode intensities, except vacuum.

5.4 Numerical results

Here, we simulate the secret key rate obtainable as a function of the overall Alice-Bob loss, which includes the inefficiency of Charlie's detectors, for different values of M, the number of random phases. For the sake of our numerical simulations, we assume that there is no eavesdropper, and we only model the imperfections in the system to simulate the values one may obtain in a real experiment. We assume a misalignment error rate of 2%, matching the results of a recent experiment [7], and a dark count probability of 10^{-8} per pulse. In all curves, we assume that Alice and Bob use three different test-mode intensities $\{\beta_1, \mu, \beta_v\}$, where $\beta_v = 0$ is a vacuum intensity and μ is the same intensity used in key mode. We optimize over the value of μ and β_1, with the condition that $\mu, \beta_1 \geq 10^{-4}$. This condition is motivated by the fact that it is experimentally difficult to produce a laser pulse with a very small, but fixed, intensity.

In our channel model, we make the additional assumption that, when Charlie obtains a click on both detectors, he announces the round as successful, and randomly chooses which detector he reports as having clicked. While this is a slight deviation from the protocol described in Section 5.3.1, it greatly simplifies all gain and yield formulas, at the cost of introducing some additional errors. In the low-loss regime, when double clicks are relatively common, this assumption slightly lowers the key rate obtainable. At medium to high losses, when the probability of a double click is almost zero, the effect vanishes. Under this assumption, we have that

$$Q_\beta = Q_\beta^- = (1-d)(1 - e^{-2\sqrt{\eta}\beta} + 2de^{-2\sqrt{\eta}\beta}), \tag{5.41}$$

where d is the dark count probability of each detector, and η is the overall Alice-Bob loss. Moreover, $p_{\text{succ}} = Q_\mu$, and $p_{\text{same}|\text{succ}} = p_{\text{diff}|\text{succ}} = 1/2$, due to the symmetry of the setup. The bit error rate of the sifted key is given by

$$e_{\text{bit}} = \frac{(1-d)e_{\text{mis}} - (e_{\text{mis}} - d)e^{-2\sqrt{\eta}\mu}}{p_{\text{succ}}}, \tag{5.42}$$

where e_{mis} is the misalignment error probability. To obtain a reliable upper bound on $e_{\text{ph,same}}$ and $e_{\text{ph,diff}}$, we need to substitute the above values in Eq. (5.31) and Eq. (5.40), and numerically solve the dual problem of each SDP [24, 29]. Note that, due to the symmetry assumed in our channel model, the SDPs in Eq. (5.31) and Eq. (5.40) end up being identical; in our simulations, we only solve their dual problem once, since its

solution provides an upper-bound on both $e_{\text{ph,same}}$ and $e_{\text{ph,diff}}$. To solve this SDP dual problem, we have written a MATLAB program that uses the CVX toolbox [30], which we run on a commercial laptop.

In Fig. 5.1, we see that the protocol can overcome the repeaterless bound [3] with as few as four random phases. For the ideal case of $M \to \infty$, we use Eq. (5.15), assuming that Alice and Bob are somehow able to estimate the exact values of Y_n, $\forall n$, using the data collected in test mode. These values are given by $Y_0 = 2d(1-d)$ and, for $n > 0$,

$$Y_n = (1-d)(1-(1-\sqrt{\eta})^2 + 2d(1-\sqrt{\eta})^n). \tag{5.43}$$

As explained in the discussion following Eq. (5.15), the case of $M \to \infty$ is not actually implementable in practice, but it provides an upper-bound on the secret key rate obtainable for finite values of M. Notably, Fig. 5.1 shows that one can get very close to this ideal scenario with only $M = 12$ random phases.

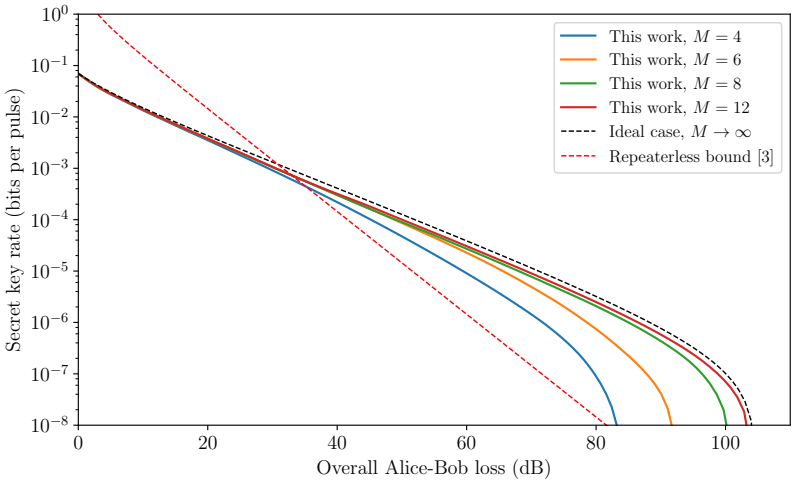


Figure 5.1: Secret key rate for our discrete-phase-randomized protocol at different values of M, in comparison to fundamental bound for repeaterless QKD systems $-\log_2(1-\eta)$, where η is the overall Alice-Bob transmissivity.

In Fig. 5.2, we compare the results of our protocol with those of Ref. [13], one of the best performing TF-QKD variants, in both the asymptotic [31] and finite-key [32] regimes. The comparison is interesting because the quantum phase of Ref. [13] is almost identical to ours, the only difference being their use of continuous phase randomization in test mode. Thus, Fig. 5.2 directly compares the performance of the discrete and

continuous randomization approaches. Remarkably, we obtain higher secret-key rates using discrete phase randomization, as long as one uses eight random phases or more. This may sound surprising at first instance, but it is justified by the fact that, for the same value of μ, we can obtain a tighter estimation of the phase-error rate in the discrete-phase version, thanks to the test-mode phase postselection. This can be seen in Fig. 5.3(a), where we compare the upper-bound on the phase-error rate of the two protocols for a fixed value $\mu = 0.06$. In a practical setting, one would optimize over the value of μ, in which case the two protocols result in similar bounds for the phase-error rate, see Fig. 5.3(b). But, this will be achieved at a higher value of μ for our protocol, see Fig. 5.3(c), which results in a higher gain, see Fig. 5.3(d), and hence a higher secret-key rate.

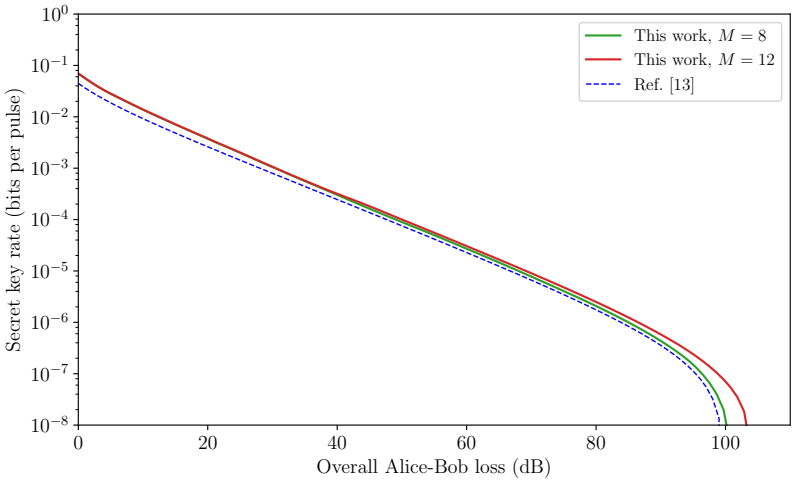


Figure 5.2: Comparison between the results of this work and those of Ref. [13], which uses continuous phase randomization in its test-mode emissions. For simplicity, to compute the results in [13], we assume that Alice and Bob's test-mode rounds provide perfect estimates of the yield probabilities Y_{nm} for $n+m \leq 4$, while the rest are upper-bounded by one. This is an ideal scenario and, as shown in [13], the results will be slightly worse once one considers the imperfect estimates that result from the use of a finite set of decoy states, as we do for the results in this work.

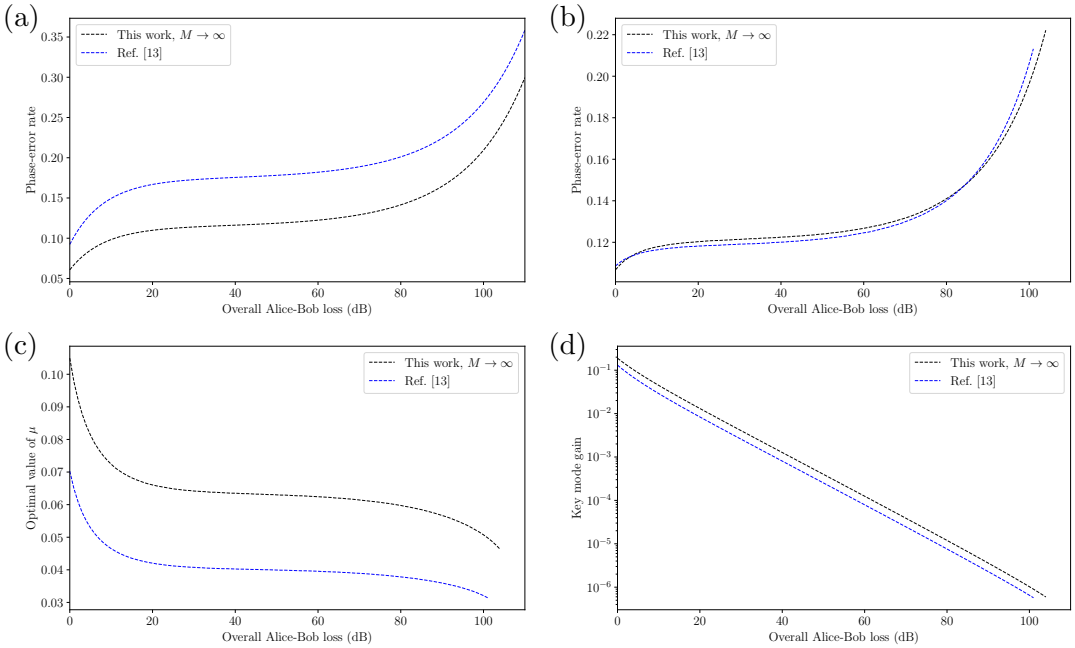


Figure 5.3: Comparison between the value of some terms in our analysis, for the ideal case $M \to \infty$, and the analysis in Ref. [13]. (a) Upper-bound on the phase-error rate, assuming a fixed value $\mu = 0.06$. (b) Upper-bound on the phase-error rate, for the value of μ that optimizes the key rate in each analysis. (c) Value of μ that optimizes the key rate in each analysis. (d) Key mode gain for the value of μ that optimizes the key rate in each analysis.

5.5 Conclusion and discussion

Most previous variants of TF-QKD have relied on the emission of weak laser pulses with a continuous random phase, which is difficult to achieve and certify in practice. Here, we have proposed a practical TF-QKD variant that uses discrete phase randomization instead. Its security proof relies on post-selecting the test-mode rounds in which the users' phase values exactly matched, which is not practically possible with a continuous randomization approach. Consequently, our discretely-randomized protocol can actually result in *higher* key rates than an equivalent protocol based on continuous randomization. This is interesting, given that discrete randomization is usually considered to be a source flaw. In fact, previous analyses of decoy-state QKD with discrete randomization [18] obtained strictly worse results than their continuous counterparts.

Our security proof relies on a customised version of numerical techniques for MDI-QKD protocols based on semidefinite programming, which has a substantially reduced complexity as compared with the generic approach.

There are several ways by which we can improve our analysis to account for additional imperfections in a real implementation. For instance, in our analysis, we assume that the users can modulate the phase of their pulses precisely. It would be interesting to find out how they key-rate bounds change when the phase modulator, while fully characterized, is imperfect. Also, we have considered the asymptotic regime in which Alice and Bob run the protocol for infinitely many rounds. It remains an open question whether discrete randomization could still offer an advantage in a finite-key setting. Since state-of-the-art numerical finite-key proofs can only prove security tightly against a restricted class of eavesdropping attacks [33, 34], important developments are needed before we can rigorously answer this question.

We note that, shortly after the first version of this manuscript was uploaded to the arXiv, Zhang et al uploaded another manuscript [35] proposing an alternative TF-QKD protocol with discrete phase randomization. The main difference seems to be that in our protocol, only two phases are encoded in key mode, while in their proposal, M phases are encoded in the key mode, i.e. as many as in the test mode. This symmetry simplifies the phase-error rate formula. However, while the secret key rate of our protocol increases with M, theirs approaches zero as M grows, due to the sifting factor.

Acknowledgements

We thank Kiyoshi Tamaki, Marcos Curty, Álvaro Navarrete, Margarida Pereira, Zhen-Qiang Yin, and Xiongfeng Ma for valuable discussions. This work was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement number 675662 (QCALL). L.W. acknowledges the support of of UK EPSRC Grant EP/SO23607/1. All data generated can be reproduced by the equations and the methodology introduced in this paper.

References

[1] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, no. 1, p. 33, 2011. 168

[2] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, p. 400, 2018. 168

[3] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.*, vol. 8, p. 15043, 2017. 168, 182

[4] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 16, no. 4, p. 043005, 2014. 168

[5] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Phys. Rev. A*, vol. 89, no. 1, p. 012301, 2014. 168

[6] K. Azuma, K. Tamaki, and W. J. Munro, "All-photonic intercity quantum key distribution," *Nat. Commun.*, vol. 6, p. 10171, 2015. 168

[7] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nat. Photonics*, vol. 13, no. 5, pp. 334–338, 2019. 168, 181

[8] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Phys. Rev. Lett.*, vol. 123, p. 100506, Sept. 2019.

[9] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution through sending or not sending," *Phys. Rev. Lett.*, vol. 123, p. 100505, Sept. 2019.

[10] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev. X*, vol. 9, no. 2, p. 021046, 2019. 168

[11] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photonics*, vol. 14, pp. 422–425, July 2020. 168

[12] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Phys. Rev. Lett.*, vol. 124, no. 7, p. 070501, 2020. 168

[13] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Inf.*, vol. 5, no. 1, pp. 1–6, 2019. xiii, 168, 169, 170, 171, 182, 183, 184

[14] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A*, vol. 98, no. 6, p. 062323, 2018. 168, 170

[15] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, no. 3, p. 031043, 2018. 168, 170

[16] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection," *Phys. Rev. Appl.*, vol. 11, no. 3, p. 034053, 2019. 168, 169, 171

[17] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, 2005. 168

[18] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," *New J. Phys.*, vol. 17, no. 5, p. 053014, 2015. 169, 170, 176, 178, 184

[19] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Express*, vol. 20, no. 11, pp. 12366–12377, 2012. 169

[20] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Opt. Express*, vol. 22, no. 2, pp. 1645–1654, 2014. 169

[21] W. Wang, K. Tamaki, and M. Curty, "Measurement-device-independent quantum key distribution with leaky sources," *arXiv:2001.08086*, 2020. 169

[22] W. Wang, K. Tamaki, and M. Curty, "Finite-key security analysis for quantum key distribution with leaky sources," *New J. Phys.*, vol. 20, no. 8, p. 083027, 2018. 170

[23] R. Wang, Z.-Q. Yin, F.-Y. Lu, S. Wang, W. Chen, C.-M. Zhang, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, "Optimized protocol for twin-field quantum key distribution," *Communications Physics*, vol. 3, p. 149, Aug. 2020. 170, 176

[24] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, "Versatile security analysis of measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 99, no. 6, p. 062332, 2019. 170, 172, 173, 177, 181

[25] Y. Ye, "Lecture notes in SDP rank reduction." https://web.stanford.edu/~yyye/sdprank-slides09.pdf, 2009. 173

[26] J. Gondzio, "Interior point methods 25 years later," *Eur. J. Oper. Res.*, vol. 218, no. 3, pp. 587–601, 2012. 173

[27] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, no. 2, p. 020504, 2009. 173

[28] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, "Quantum key distribution with correlated sources," *Sci. Adv.*, vol. 6, no. 37, p. eaaz4487, 2020. 178

[29] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," *Nat. Commun.*, vol. 7, no. 1, pp. 1–9, 2016. 181

[30] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1." http://cvxr.com/cvx, Mar. 2014. 182

[31] M. Lucamarini, "Recent progress on measurement-device-independent quantum key distribution." http://2018.qcrypt.net/wp-content/uploads/2018/slides/Wednesday/01.Marco%20Lucamarini.pdf, 2018. 182

[32] G. Currás Lorenzo, A. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, "Tight finite-key security for twin-field quantum key distribution," *arXiv:1910.11407*, 2019. 182

[33] D. Bunandar, L. C. Govia, H. Krovi, and D. R. Englund, "Numerical finite-key analysis of quantum key distribution," *arXiv:1911.07860*, 2019. 185

[34] I. George, J. Lin, and N. Lütkenhaus, "Numerical calculations of finite key rate for general quantum key distribution protocols," *arXiv:2004.11865*, 2020. 185

[35] C.-M. Zhang, Y.-W. Xu, R. Wang, and Q. Wang, "Twin-field quantum key distribution with discrete-phase-randomized sources," *arXiv:2008.05277*, 2020. 185

Chapter 6

Discussion and Conclusions

In the previous chapters, we have analysed the security and performance of novel QKD protocols in realistic conditions. Here, we summarise our main results, and identify some open lines of investigation that could be addressed in future work.

6.1 Summary

Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory

In a BB84-type protocol, when Alice's source is basis independent, one can invoke a random sampling argument to directly estimate the phase-error rate in one basis using the observed bit-error rate in the other basis. This is especially important in the finite-key regime, since it makes it very easy to deal with finite-key statistical fluctuations in the estimation of the phase-error rate. Conversely, when Alice's source is basis dependent, Eve can at least partially distinguish Alice's basis choice. Thus, under a coherent attack, Eve can cause the detection statistics of a particular round to depend on the basis choices made in other rounds. To deal with this dependency, previous works have often relied on Azuma's inequality, which offers a worse performance than concentration inequalities used to solve random sampling problems. In Chapter 2, we have introduced a technique that, for some QKD protocols with basis-dependent sources, can reduce the phase-error rate estimation task to a random sampling problem, which can be solved more tightly. In particular, we have shown that our technique can be used to prove the finite-key security of the loss-tolerant protocol [1] for both its prepare-and-measure and

measurement-device-independent versions, if the users probabilistically assign a tag to each detected emission. Our analysis obtained significantly better key rates than the previous finite-key security proof of the loss-tolerant protocol [2] based on Azuma's inequality.

Finite-key analysis for memory-assisted decoy-state quantum key distribution

In Chapter 3, we analysed the performance of MA-QKD in practical conditions that previous works [3–6] had not considered. Namely, we assumed that the users employ WCP sources, in combination with the decoy-state method, and took into account the statistical fluctuations that inevitably arise when the protocol is run for a finite number of rounds. To perform our simulations, we developed a model for the heralded loading of a QM using attenuated laser sources in the presence of polarisation misalignment. We also proposed a simple and high-performance finite-key statistical fluctuation analysis that is valid for both decoy-state MDI-QKD and decoy-state MA-QKD. Our simulation results suggested that decoy-state MA-QKD is inherently more resilient to statistical fluctuation effects than its equivalent no-memory MDI-QKD counterpart. Thus, in the finite-key regime, decoy-state MA-QKD could offer large key-rate advantages over much shorter channel lengths than previously thought, even when implemented with today's imperfect QMs. The main reason for this behaviour is that, in MDI-QKD, the multi-photon components of X-encoded weak coherent pulses can, by themselves, cause two detectors to simultaneously click in Charlie's measurement apparatus. These spurious events are interpreted and announced as successful BSM results by Charlie, which adds statistical noise to the parameter estimation task. Conversely, these events are absent in MA-QKD, allowing for a tighter estimation of the relevant parameters. This result is important for experimental groups aiming to implement a MA-QKD system that can offer a true advantage over an equivalent memory-less setup in realistic conditions.

Tight finite-key security for twin-field quantum key distribution

In Chapter 4, we considered the finite-key security of the TF-QKD variant proposed by Ref. [7]. This protocol offers high performance and is well-suited for experimental implementation, but its asymptotic security proof is non-standard and poses particularly difficult challenges when considering the finite-key regime. Namely, it does not

rely on two mutually unbiased encoding bases, which makes it difficult to consider the effect of statistical fluctuations when using the test-mode observed data to estimate the phase-error rate of the key-mode emissions. Moreover, its direct expression for the phase-error rate is a function of infinitely many estimation parameters, and it is impossible to estimate all of them in practice. The asymptotic security proof could trivially bound some of these and reduce the expression to a finite number of parameters. However, this trivial bound cannot be applied in the finite-size setting. In Chapter 4, we proposed a tight finite-key security proof for the protocol that takes into account the above challenges. In doing so, we showed that the protocol can overcome fundamental bounds on the secret-key rate of point-to-point protocols in a run of about 10^{10} transmitted signals. Moreover, we showed that the asymptotic performance advantage that this protocol offers with respect to other TF-QKD variants also holds in the finite-key regime, for many practical regimes of interest.

Twin-field quantum key distribution with fully discrete phase randomisation

The security proofs of previous TF-QKD variants [7–12] assumed that the users can emit weak coherent pulses with a continuous random phase, either to generate the key or to estimate its phase-error rate. However, in practice, this is difficult to achieve, and it is comparatively much easier to randomise the phase of the pulses discretely. In Chapter 5, we considered the security and performance of a TF-QKD variant that relies only on discrete phase randomisation. Previous work on QKD with discretely-randomised sources [9] had treated its presence as a source flaw, and focused on showing that its impact on the key rate is small when the number of random phases is sufficiently high. However, in our TF-QKD variant, we found that the use of discrete randomisation allowed us to introduce post-processing steps that are not possible in an equivalent continuously-randomised protocol. Namely, it allowed us to post-select the test-mode rounds in which the users employed exactly the same phase, which results in a better estimation of the phase-error rate. As a result, we found that our variant can achieve higher secret-key rates than the equivalent continuously-randomised protocol proposed by Ref. [7], when using eight discrete random phases or more. To prove the security of the protocol, we relied on semi-definite programming techniques.

6.2 Future work

Using semi-definite programming to prove the finite-key security of QKD

In recent years, numerical techniques based on semi-definite programming have started to be applied to prove the security of QKD protocols [13–15]. Their main advantage over analytical proofs is their flexibility, as they can be easily applied to different protocols, and even take into account device imperfections. However, they currently have some limitations that hinder their use in practical implementations. Typically, these numerical techniques work by using the observed outcomes of the protocol to restrict the space of Eve's possible attacks, and then finding the worst-case scenario that is consistent with these restrictions. Because of this, they are difficult to apply when Eve performs a general attack, since in that case, her attack is described by an operator acting on the photonic systems of all rounds in the protocol *at once*, which means that the space of Eve's possible attacks is enormous. Thus, numerical security proofs often assume collective attacks, thanks to which Eve's action can be described by an operator acting only on the photonic system(s) of a single round, which makes the space of possible attacks much smaller. As explained in Section 1.1.2.1, in the asymptotic regime, security against collective attacks often implies security against general attacks, but in the finite-key regime, it does not. In a future work, it would be interesting to consider whether semi-definite programming techniques could be used to prove the finite-key security of QKD against general attacks. To do so, one would need to find a way to reduce the problem so that it can be solved using these techniques.

Finite-key analysis of twin-field QKD with discrete phase randomisation

In Chapter 4, we proved the finite-key security of the TF-QKD variant proposed in Ref. [7], and in Chapter 5 we proved the asymptotic security of a similar variant in which the users employ discrete, rather than continuous, phase randomisation in their test-mode emissions. In a future work, it would be interesting to attempt to prove the finite-key security of the discrete TF-QKD variant introduced in Chapter 5, using the techniques developed in Chapter 4. This is complicated by the fact that discrete randomisation made it difficult to obtain a closed form expression for the phase-error rate, and we relied on numerical techniques based on semi-definite programming for our asymptotic proof. To prove the finite-key security of the protocol against general

attacks, one would either have to find a closed form expression for the phase-error rate, or to find a way to reduce the problem so that it is solvable using numerical techniques, as explained in the previous paragraph.

Addressing other imperfections in the security of TF-QKD

In this thesis, we have addressed two important points for the implementation security of TF-QKD: statistical fluctuations in realistic implementations, and the use of discrete phase randomisation. In future work, it would be interesting to consider further practical imperfections, such as preparation flaws or information leakage from the users' sources. A previous attempt to do this [16] resulted in a secret-key rate that scales with $O(\eta)$, rather than $O(\sqrt{\eta})$ as in standard TF-QKD. In future work, it would be interesting to investigate whether it is possible to account for these imperfections while maintaining the $O(\sqrt{\eta})$ scaling.

Investigating the finite-key resilience of MA-QKD

In Chapter 3, we simulated the finite-key performance of decoy-state MA-QKD, and found that the protocol is more resilient to statistical fluctuations than the corresponding memory-less MDI-QKD setup. In our simulations, we assumed a particular model for the heralded loading process of the QMs. However, there are many different quantum memory proposals, and the mechanisms to obtain a heralded loading vary considerably between these. For example, the memory loading procedure used in the recent experiment by Ref. [17] differs considerably from the model assumed in our simulations. In future works, it would be interesting to consider whether decoy-state MA-QKD's resilience to statistical fluctuation effects holds for different QM implementations and heralded loading procedures.

Applying random sampling theory to prove the finite-key security of other basis-dependent protocols

Traditionally, random sampling theory has only been applied to prove the finite-key security of protocols with a basis-independent source. However, in Chapter 2, we have shown the possibility of using random sampling results to prove the security of protocols with a basis-dependent source. In particular, we first showed how to reduce the estimation task of a simplified basis-dependent scenario to a random sampling

problem, and then showed that the loss-tolerant protocol becomes equivalent to our simplified scenario after the users assign random tags to their emissions. In future work, it would be interesting to consider whether other basis dependent protocols, such as those dealing with Trojan-horse attacks, can also be reduced to our simplified scenario.

References

[1] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A*, vol. 90, p. 052314, Nov. 2014. 190

[2] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources," *New J. Phys.*, vol. 17, p. 093011, Sept. 2015. 191

[3] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New J. Phys.*, vol. 16, p. 043005, Apr. 2014. 191

[4] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Phys. Rev. A*, vol. 89, p. 012301, Jan. 2014.

[5] N. Lo Piparo, N. Sinclair, and M. Razavi, "Memory-assisted quantum key distribution resilient against multiple-excitation effects," *Quantum Sci. Technol.*, vol. 3, p. 014009, Dec. 2017.

[6] N. Lo Piparo, M. Razavi, and W. J. Munro, "Memory-assisted quantum key distribution with a single nitrogen-vacancy center," *Phys. Rev. A*, vol. 96, p. 052313, Nov. 2017. 191

[7] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Inf.*, vol. 5, pp. 1–6, July 2019. 191, 192, 193

[8] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, May 2018.

[9] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-Field Quantum Key Distribution without Phase Postselection," *Phys. Rev. Applied*, vol. 11, p. 034053, Mar. 2019. 192

[10] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A*, vol. 98, p. 062323, Dec. 2018.

[11] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound," *arXiv preprint arXiv:1805.05511*, Sept. 2018.

[12] X. Ma, P. Zeng, and H. Zhou, "Phase-Matching Quantum Key Distribution," *Phys. Rev. X*, vol. 8, p. 031043, Aug. 2018. 192

[13] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," *Nat. Commun.*, vol. 7, p. 11712, May 2016. 193

[14] A. Winick, N. Lütkenhaus, and P. J. Coles, "Reliable numerical key rates for quantum key distribution," *Quantum*, vol. 2, p. 77, July 2018.

[15] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, "Versatile security analysis of measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 99, p. 062332, June 2019. 193

[16] Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, "Practical Quantum Key Distribution That is Secure Against Side Channels," *Phys. Rev. Applied*, vol. 15, p. 034072, Mar. 2021. 194

[17] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," *Nature*, vol. 580, pp. 60–64, Apr. 2020. 194

Appendix A

Supplementary Notes for Chapter 4

A.1 Security bounds

Let $\mathbf{X}$ ($\mathbf{X}'$) denote Alice's (Bob's) sifted key of length M_X before the post-processing step of the protocol. Through the error correction and verification steps, Bob should have turned $\mathbf{X}'$ into a copy of $\mathbf{X}$, except with a small error probability. Then, Alice and Bob apply a privacy amplification scheme based on two-universal hashing to obtain a shorter secret key of length ℓ. The objective of this Note is to prove that this key is ϵ_{s}-secret, with $\epsilon_{\mathrm{s}} \leq \sqrt{\varepsilon} + \epsilon_{\mathrm{PA}}$, where ε is the failure probability of the estimation of the phase-error rate, and ϵ_{PA} appears in the key-rate formula in Eq. (4.4) of the main text. For this, we will make use of the Quantum Leftover Hash Lemma [1, 2], according to which, for any $\epsilon > 0$,

$$\epsilon_{\mathrm{s}} \leq \epsilon + \frac{1}{2}\sqrt{2^{\ell - H^{\epsilon}_{\min}(\mathbf{X}|E')_{\rho}}}, \tag{A.1}$$

where E' represents Eve's total side information about $\mathbf{X}$, $H^{\epsilon}_{\min}(\mathbf{X}|E')$ is the ϵ-smooth min entropy of $\mathbf{X}$ conditioned on E', and ρ is the quantum state that Alice has measured to obtain $\mathbf{X}$. Let E denote Eve's side information before the error correction step. By the chain rule for smooth min-entropies [2],

$$H^{\epsilon}_{\min}(\mathbf{X}|E')_{\rho} \geq H^{\epsilon}_{\min}(\mathbf{X}|E)_{\rho} - \lambda_{\mathrm{EC}} - \log_2 \frac{2}{\epsilon_{\mathrm{c}}}, \tag{A.2}$$

where λ_{EC} ($\log_2 \frac{2}{\epsilon_{\mathrm{c}}}$) is the number of bits revealed in the error correction (verification) step of the protocol. We will also make use of the following theorem, introduced in [3],

which we reproduce here for completeness.

Theorem [3]: Let $\epsilon > 0$, ρ_{AEB} be a tripartite quantum state, $\mathbb{X} = \{M_x\}$ and $\mathbb{Z} = \{N_z\}$ be two POVMs on A, and $\mathbf{X}$ ($\mathbf{Z}$) be the result of the measurement of $\mathbb{X}$ ($\mathbb{Z}$). Then,

$$H_{\min}^{\epsilon}(\mathbf{X}|E)_{\rho} + H_{\max}^{\epsilon}(\mathbf{Z}|B)_{\rho} \geq q, \tag{A.3}$$

where $q = \log_2 \frac{1}{c}$, with

$$c = \max_{x,z} \left\| \sqrt{M_x}\sqrt{N_z} \right\|_{\infty}^2. \tag{A.4}$$

To apply this theorem, we consider a slightly modified but equivalent scenario to the virtual protocol defined in Methods. In step (4.1), we imagine that Alice and Bob now first measure all the quantum coins A_c and B_c in $\mathcal{M}_s$, learning their choice of basis. Then, for the successful rounds in which they both used the Z basis, they measure their ancillas, learning their choice of state. Let us denote by k the result of both these measurements. Conditioned on this result, the state of Alice's and Bob's X-basis ancillas A and B, together with Eve's side information E on them, will be in some state $\rho(k)$. Note that if Alice measures all her $M_X(k)$ qubits A in the X basis, she will obtain a raw key $\mathbf{X}$ that is identical to the one she would have obtained in the real protocol; while if she measures them in the Z basis, she will obtain a raw key $\mathbf{Z}$ that is identical to that of the virtual protocol.

Let $\mathbb{X} = \{M_x\}$ ($\mathbb{Z} = \{N_z\}$) denote Alice's overall POVM if she chooses to measure all her qubits A in the X (Z) basis. The elements M_x of $\mathbb{X}$ are of the form $|x_1 x_2 x_3 ...\rangle\langle x_1 x_2 x_3 ...|$, where $x_n \in \{+, -\}$ is the result of the measurement of round $n \in \{1, ..., M_X(k)\}$. Conversely, the elements N_z of $\mathbb{Z}$ are of the form $|z_1 z_2 z_3 ...\rangle\langle z_1 z_2 z_3 ...|$, with $z_n \in \{0, 1\}$. Since M_x and N_z are rank 1 projective measurements, we have that

$$\max_{x,z} \left\| \sqrt{M_x}\sqrt{N_z} \right\|_{\infty}^2 = \max_{x,z} \|\langle x_1 x_2 x_3 ...|z_1 z_2 z_3 ...\rangle\|^2 = 2^{-M_X(k)}, \tag{A.5}$$

where in the last step we have used the fact that $\|\langle x_n|z_n\rangle\|^2 = 1/2$, independently of the value of x_n and z_n. From Eq. (A.3), it follows that

$$H_{\min}^{\epsilon}(\mathbf{X}|E)_{\rho(k)} + H_{\max}^{\epsilon}(\mathbf{Z}|B)_{\rho(k)} \geq M_X(k). \tag{A.6}$$

Now, let us assume that Bob measures his systems B using POVM $\mathbb{Z}$, obtaining a string $\mathbf{Z}'$ that is identical to the one that he would obtain in the virtual protocol. Clearly, the result of a measurement of B cannot contain more information about $\mathbf{Z}$ than system B itself, and therefore

$$H_{\max}^{\epsilon}(\mathbf{Z}|\mathbf{Z}')_{\rho(k)} \geq H_{\max}^{\epsilon}(\mathbf{Z}|B)_{\rho(k)}. \tag{A.7}$$

Combining Eqs. (A.2), (A.6) and (A.7), we have that

$$H_{\min}^{\epsilon}(\mathbf{X}|E')_{\rho(k)} \geq M_X(k) - H_{\max}^{\epsilon}(\mathbf{Z}|\mathbf{Z}')_{\rho(k)} - \lambda_{\mathrm{EC}} - \log_2 \frac{2}{\epsilon_{\mathrm{c}}}. \tag{A.8}$$

Based on the outcome k, Alice and Bob will use Eq. (4.1) of the main text to estimate $N_{\mathrm{ph}}^{\mathrm{U}}(k)$ and $e_{\mathrm{ph}}^{\mathrm{U}}(k) = N_{\mathrm{ph}}^{\mathrm{U}}(k)/M_X(k)$. Let $\varepsilon(k) = \Pr\left(e_{\mathrm{ph}} > e_{\mathrm{ph}}^{\mathrm{U}}(k)\middle|k\right)$, where e_{ph} is the fraction of bits that differ between $\mathbf{Z}$ and $\mathbf{Z}'$. From [2], we have that

$$H_{\max}^{\sqrt{\varepsilon(k)}}(\mathbf{Z}|\mathbf{Z}')_{\rho(k)} \leq M_X(k) h(e_{\mathrm{ph}}^{\mathrm{U}}(k)). \tag{A.9}$$

Substituting $\epsilon = \sqrt{\varepsilon(k)}$ and Eq. (A.9) in Eq. (A.8), we have

$$H_{\min}^{\sqrt{\varepsilon(k)}}(\mathbf{X}|E)_{\rho(k)} \geq M_X(k)\left[1 - h(e_{\mathrm{ph}}^{\mathrm{U}}(k))\right] - \lambda_{\mathrm{EC}} - \log_2 \frac{2}{\epsilon_{\mathrm{c}}}. \tag{A.10}$$

Alice and Bob extract a key of length $\ell(k)$, given by Eq. (4.4) of the main text, from the state $\rho(k)$. Substituting $\ell(k)$ and Eq. (A.10) in Eq. (A.1), we have that the security parameter of the key, conditioned on the outcome k, can be upper-bounded by

$$\epsilon_{\mathrm{s}}(k) \leq \sqrt{\varepsilon(k)} + \epsilon_{\mathrm{PA}}. \tag{A.11}$$

We are interested in the overall secrecy parameter ϵ_{s}, given by the average over k of $\epsilon_{\mathrm{s}}(k)$. To bound this parameter, we first note that, in Methods, we have proven that $\Pr\left(e_{\mathrm{ph}} > e_{\mathrm{ph}}^{\mathrm{U}}\right) \leq \varepsilon$, which we now rewrite as

$$\varepsilon \geq \Pr\left(e_{\mathrm{ph}} > e_{\mathrm{ph}}^{\mathrm{U}}\right) = \sum_k p(k) \Pr\left(e_{\mathrm{ph}} > e_{\mathrm{ph}}^{\mathrm{U}}(k)\middle|k\right) = \sum_k p(k)\varepsilon(k). \tag{A.12}$$

Finally, we have

$$\begin{aligned} \epsilon_{\mathrm{s}} = \sum_k p(k)\epsilon_{\mathrm{s}}(k) &\leq \sum_k p(k)\left(\sqrt{\varepsilon(k)} + \epsilon_{\mathrm{PA}}\right) \\ &= \epsilon_{\mathrm{PA}} + \sum_k p(k)\sqrt{\varepsilon(k)} \leq \epsilon_{\mathrm{PA}} + \sqrt{\sum_k p(k)\varepsilon(k)} \leq \epsilon_{\mathrm{PA}} + \sqrt{\varepsilon}, \end{aligned} \tag{A.13}$$

where in the second to last step we have applied Jensen's inequality, and in the last step we have applied Eq. (A.12).

A.2 Analytical estimation method

In this Note, we present an analytical method to obtain the upper bounds M_{nm}^{U} in Eq. (4.1) of the main text, using the observed quantities $M^{\mu\nu}$. First, we explain the general idea behind the procedure, and then we obtain specific analytical bounds for the case of three decoy intensities and $S_{\mathrm{cut}} = 4$, which we use in our simulations. We have numerically verified that the choice of three decoy intensities is optimal for reasonable block size values below 10^{12} transmitted signals.

Our starting point is Eq. (4.25) of the main text, which we rewrite as

$$\hat{M}^{\mu\nu} = \sum_{n,m=0}^{\infty} \frac{\mu^n \nu^m}{n!m! p_{n|Z} p_{m|Z}} M_{nm}, \tag{A.14}$$

by defining $\hat{M}^{\mu\nu} = e^{\mu+\nu} \frac{\mathbb{E}[M^{\mu\nu}]}{p_\mu p_\nu}$. To obtain an upper bound for a specific term M_{ij} in Eq. (A.14), we follow a procedure analogous to Gaussian elimination, defining a linear combination

$$\Omega = \sum_{\mu,\nu} \hat{c}_{\mu\nu} \hat{M}^{\mu\nu}. \tag{A.15}$$

From Eq. (A.14), Ω can also be expressed as a linear combination of the M_{nm} terms, that is,

$$\Omega = \sum_{n,m=0}^{\infty} c_{nm} M_{nm}. \tag{A.16}$$

Then, we rewrite the R.H.S. of Eq. (A.16) as

$$\Omega = c_{ij} M_{ij} + \sum_{(n,m)\in S_+} c_{nm} M_{nm} + \sum_{(n,m)\in S_-} c_{nm} M_{nm}, \tag{A.17}$$

where we have singled out the index (i,j), ensured that $c_{ij} > 0$, and defined S_+ (S_-) as the set of pairs $(n,m) \neq (i,j)$ such that c_{nm} is a positive (negative) number. From Eq. (A.17), one can obtain the following upper bound on M_{ij}

$$\begin{aligned} M_{ij} &= \frac{1}{c_{ij}} \left[\Omega - \sum_{nm\in S_+} c_{nm} M_{nm} - \sum_{nm\in S_-} c_{nm} M_{nm} \right] \\ &\leq \frac{1}{c_{ij}} \left[\mathrm{UB}\{\Omega\} - \mathrm{LB}\{ \sum_{(n,m)\in S_+} c_{nm} M_{nm} \} + \mathrm{UB}\{ \sum_{(n,m)\in S_-} |c_{nm}| M_{nm} \} \right], \end{aligned} \tag{A.18}$$

where $\mathrm{UB}\{x\}$ ($\mathrm{LB}\{x\}$) denotes an upper (lower) bound on x.

Now, we find an expression for each of the bounds within Eq. (A.18). First, note that Ω is a linear combination of the expected values $\mathbb{E}[M^{\mu\nu}]$ as in Eq. (A.14). While these are unknown to the users, they can obtain lower and upper bounds $\mathbb{E}^{\mathrm{L}}[M^{\mu\nu}]$ and $\mathbb{E}^{\mathrm{U}}[M^{\mu\nu}]$ using the inverse multiplicative Chernoff bound presented in Appendix A.6. To obtain $\mathrm{UB}\{\Omega\}$, we simply replace each term $\mathbb{E}[M^{\mu\nu}]$ in Eq. (A.15) by either its upper or lower bound, depending on whether its coefficient in Ω is positive or negative.

Second, we use the fact that $M_{nm} \geq 0$ to find the trivial lower bound $\mathrm{LB}\{\sum_{(n,m)\in S_+} c_{nm}M_{nm}\} = 0$. For the remaining term, we note that

$$\begin{aligned}\sum_{n,m\in S_-} |c_{nm}|M_{nm} &\leq c_{\max} \sum_{n,m\in S_-} M_{nm} \\ &\leq c_{\max}(M_Z - M_{ij} - \mathrm{LB}\{\sum_{\substack{n,m\notin S_- \\ (n,m)\neq(i,j)}} M_{nm}\}),\end{aligned} \tag{A.19}$$

where we have chosen $c_{\max}$ such that $c_{\max} \geq |c_{nm}|$ for all the pairs $(n,m) \in \mathcal{S}_-$, and the last lower bound depends on the particular M_{ij} that we are trying to estimate, as we will show later. Substituting the three bounds in Eq. (A.18) and isolating M_{ij}, we obtain

$$M_{ij} \leq \frac{1}{c_{ij} + c_{\max}} \left[\mathrm{UB}\{\Omega\} + c_{\max}(M_Z - \mathrm{LB}\{\sum_{\substack{n,m\notin S_- \\ (n,m)\neq(i,j)}} M_{nm}\}) \right]. \tag{A.20}$$

Bounds for three decoy intensities

Now, we obtain explicit lower bounds for the case in which $S_{\mathrm{cut}} = 4$ and each of Alice and Bob use three different intensity settings, satisfying $\mu_0 > \mu_1 > \mu_2$ and $\nu_0 > \nu_1 > \nu_2$, respectively. For this, we take inspiration from the asymptotic analytical bounds derived in [4]. First, we define

$$K^{a_S,a_I,b_S,b_I} = \kappa_A^{a_I}\kappa_B^{b_I}\hat{M}^{a_S,b_S} - \kappa_A^{a_S}\kappa_B^{b_I}\hat{M}^{a_I,b_S} - \kappa_A^{a_I}\kappa_B^{b_S}\hat{M}^{a_S,b_I} + \kappa_A^{a_S}\kappa_B^{b_S}\hat{M}^{a_I,b_I}, \tag{A.21}$$

which is a function of some intensities that satisfy $a_S > a_I$ and $b_S > b_I$, with $a_S, a_I \in \{\mu_0, \mu_1, \mu_2\}$ and $b_S, b_I \in \{\nu_0, \nu_1, \nu_2\}$. The coefficients κ_A^{μ} and κ_B^{ν} depend on the specific M_{ij} that is to be estimated, but we have omitted this dependence from the notation

for simplicity. Using the previous equation, we now define

$$\begin{aligned}\Omega = w_A^{\mu_1\mu_2} w_B^{\nu_1\nu_2} K^{\mu_0,\mu_1,\nu_0,\nu_1} - w_A^{\mu_0\mu_1} w_B^{\nu_1\nu_2} K^{\mu_1,\mu_2,\nu_0,\nu_1} \\ - w_A^{\mu_1\mu_2} w_B^{\nu_0\nu_1} K^{\mu_0,\mu_1,\nu_1,\nu_2} + w_A^{\mu_0\mu_1} w_B^{\nu_0\nu_1} K^{\mu_1,\mu_2,\nu_1,\nu_2},\end{aligned} \tag{A.22}$$

where the coefficients $w_A^{\mu\nu}$ and $w_B^{\mu\nu}$ also depend on the particular M_{ij} that we want to estimate. If we rewrite Ω as $\Omega = \sum_{k,l=0}^{2} \hat{c}_{\mu_k\nu_l} \hat{M}^{\mu_k\nu_l}$, it is easy to prove that if the coefficients $w_A^{\mu\nu}$, $w_B^{\mu\nu}$, κ_A^{μ} and κ_B^{μ} are all positive, the coefficients $\hat{c}_{\mu_k\nu_l}$ are always positive (negative) when $k+l$ is even (odd). Thus, one can find upper (Ω^{U}) and lower (Ω^{L}) bounds on Ω by properly replacing each $\hat{M}_{\mu_k\nu_l}$ by either its upper or lower bound, as explained in the introduction of this Note.

Upper bound on M_{00}

By substituting $\kappa_A^{\mu} = \kappa_B^{\mu} = \mu$ and $w_A^{\mu\nu} = w_B^{\mu\nu} = (\mu^2\nu - \nu^2\mu)$ in Ω, we obtain the following function Ω_{00}:

$$\Omega_{00} := \Omega = c_{00}M_{00} + \sum_{n=3}^{\infty} c_{n0}M_{n0} + \sum_{m=3}^{\infty} c_{0m}M_{0m} + \sum_{\substack{n=3\\m=3}}^{\infty} c_{nm}M_{nm}, \tag{A.23}$$

where the coefficients

$$\begin{aligned} c_{nm} \;=\; & \frac{1}{m!n!p_{nm|Z}} \mu_1\nu_1 \left[\mu_0\mu_1\left(\mu_0-\mu_1\right)\mu_2^n - \mu_0\mu_2\left(\mu_0-\mu_2\right)\mu_1^n + \mu_1\mu_2\left(\mu_1-\mu_2\right)\mu_0^n\right] \\ & \times \left[\nu_0\nu_1\left(\nu_0-\nu_1\right)\nu_2^m - \nu_0\nu_2\left(\nu_0-\nu_2\right)\nu_1^m + \nu_1\nu_2\left(\nu_1-\nu_2\right)\nu_0^m\right], \end{aligned} \tag{A.24}$$

can be shown to be non-negative for all n, m [4]. Then, an upper bound on M_{00} is straightforwardly given by

$$M_{00} \leq \frac{\Omega_{00}^{\mathrm{U}}}{c_{00}}, \tag{A.25}$$

where we have lower bounded the term $\sum_{n=3}^{\infty} c_{n0}M_{n0} + \sum_{m=3}^{\infty} c_{0m}M_{0m} + \sum_{\substack{n=3\\m=3}}^{\infty} c_{nm}M_{nm}$ by zero since all the coefficients satisfy $c_{nm} \geq 0$.

Upper bound on M_{11}

By substituting $\kappa_A^{\mu} = \kappa_B^{\mu} = 1$ and $w_A^{\mu\nu} = w_B^{\mu\nu} = (\mu^2 - \nu^2)$ in Ω, we obtain the following function Ω_{11}:

$$\Omega_{11} := \Omega = c_{11}M_{11} + \sum_{n=3}^{\infty} c_{n1}M_{n1} + \sum_{m=3}^{\infty} c_{1m}M_{1m} + \sum_{\substack{n=3\\m=3}}^{\infty} c_{nm}M_{nm}, \tag{A.26}$$

where the coefficients

$$c_{nm} = \frac{\left[\mu_0^n\left(\mu_1^2-\mu_2^2\right)-\mu_1^n\left(\mu_0^2-\mu_2^2\right)+\mu_2^n\left(\mu_0^2-\mu_1^2\right)\right]\left[\nu_0^m\left(\nu_1^2-\nu_2^2\right)-\nu_1^m\left(\nu_0^2-\nu_2^2\right)+\nu_2^m\left(\nu_0^2-\nu_1^2\right)\right]}{m!n!p_{nm|Z}}, \tag{A.27}$$

can be shown to be negative for the pairs $(n,m) \in S_-$, with $S_- = \{(n,m)|n \geq 3, m = 1\} \cup \{(n,m)|n = 1, m \geq 3\}$ and non-negative for the pairs $(n,m) \in S_+$, with $S_+ = \{(n,m)|n \geq 3, m \geq 3\}$ [4]. According to Eq. (A.19), an upper bound on the sum of negative terms can be obtained by

$$\begin{aligned}\sum_{n,m\in S_-}|c_{nm}|M_{nm} &\leq c_{\max}(M_z - M_{11} - \mathrm{LB}\{\sum_{\substack{n,m\notin S_-\\(n,m)\neq(1,1)}} M_{nm}\})\\ &\leq c_{\max}(M_z - M_{11} - \mathrm{LB}\{\sum_{n,m\in S_o} M_{nm}\})\\ &\leq c_{\max}(M_z - M_{11} - \mathrm{LB}\{\sum_{n=0}^{\infty} M_{n0}\} - \mathrm{LB}\{\sum_{m=0}^{\infty} M_{0m}\} + \mathrm{UB}\{M_{00}\}),\end{aligned}$$

where $c_{\max} \geq |c_{nm}|$ for all the pairs $(n,m) \in S_-$ and $S_o = \{(n,0)|n \geq 0\} \cup \{(0,m)|m \geq 0\}$. In Eq. (A.28), the second inequality comes from the fact that we have set to zero all those terms M_{nm}, with $(m,n) \neq (1,1)$, which do not belong to S_- nor to S_o because $M_{nm} \geq 0$, $\forall n,m$. A valid $c_{\max}$ can be obtained by noticing that, for $n > s$,

$$\begin{aligned}g_\mu(n) &:= \frac{\mu_0^n\left(\mu_1^s-\mu_2^s\right)-\mu_1^n\left(\mu_0^s-\mu_2^s\right)+\mu_2^n\left(\mu_0^s-\mu_1^s\right)}{n!p_{n|Z}}\\ &\leq \frac{\mu_0^n\left(\mu_1^s-\mu_2^s\right)}{n!p_{n|Z}}\\ &\leq \frac{\left(\mu_1^s-\mu_2^s\right)}{e^{-\mu_0}p_{\mu_0}}.\end{aligned} \tag{A.28}$$

This means that, from Eqs. (A.27) and (A.28), $c_{\max}$ is given by

$$c_{\max} = \max[\frac{\left(\mu_1^2-\mu_2^2\right)}{e^{-\mu_0}p_{\mu_0}}|g_\nu(1)|, \frac{\left(\nu_1^2-\nu_2^2\right)}{e^{-\nu_0}p_{\nu_0}}|g_\mu(1)|]. \tag{A.29}$$

Finally from Eqs. (A.18) and (A.28), an upper bound on M_{11} is given by

$$M_{11} \leq M_{11}^{\mathrm{U}} = \frac{\Omega_{11}^{\mathrm{U}} + c_{\max}(M_z - M_{0A}^{\mathrm{L}} - M_{0B}^{\mathrm{L}} + M_{00}^{\mathrm{U}})}{c_{11} + c_{\max}}, \tag{A.30}$$

where M_{0A}^{L} and M_{0B}^{L} are lower bounds on the quantities $M_{0A} = \sum_{m=0}^{\infty} M_{0m}$ and $M_{0B} = \sum_{n=0}^{\infty} M_{n0}$, respectively, and we have lower bounded the term $\sum_{n,m=3}^{\infty} c_{nm}M_{nm}$ by zero. Since M_{0A} and M_{0B} depend only on a single emitter, we can estimate them

using the same method as for the vacuum component in BB84. Using the results of [5], we have that

$$M_{0A}^{\mathrm{L}} = p_0 \frac{\mu_1 \mathrm{LB}\{\hat{M}^{\mu_2}\} - \mu_2 \mathrm{UB}\{\hat{M}^{\mu_1}\}}{\mu_1 - \mu_2}, \tag{A.31}$$

$$M_{0B}^{\mathrm{L}} = p_0 \frac{\nu_1 \mathrm{LB}\{\hat{M}^{\nu_2}\} - \nu_2 \mathrm{UB}\{\hat{M}^{\nu_1}\}}{\nu_1 - \nu_2}, \tag{A.32}$$

where $\hat{M}^{\mu} = e^{\mu} \frac{\mathbb{E}[M^{\mu}]}{p_{\mu}}$, $\hat{M}^{\nu} = e^{\nu} \frac{\mathbb{E}[M^{\nu}]}{p_{\nu}}$, $M^{\mu} = \sum_{\nu} M^{\mu\nu}$ and $M^{\nu} = \sum_{\mu} M^{\mu\nu}$, with $\mu \in \{\mu_0, \mu_1, \mu_2\}$ and $\nu \in \{\nu_0, \nu_1, \nu_2\}$; and the upper and lower bounds included in Eqs. (A.31) and (A.32) are obtained accordingly to Eq. (A.64).

Upper bound on M_{22}

By substituting $\kappa_A^{\mu} = \kappa_B^{\mu} = 1$ and $w_A^{\mu\nu} = w_B^{\mu\nu} = (\mu - \nu)$ in Ω, we obtain the following function Ω_{22}:

$$\Omega_{22} := \Omega = \sum_{n,m=2}^{\infty} c_{nm} M_{nm}, \tag{A.33}$$

where the coefficients

$$c_{nm} = \frac{\left[\mu_0^n (\mu_1 - \mu_2) - \mu_1^n (\mu_0 - \mu_2) + \mu_2^n (\mu_0 - \mu_1)\right] \left[\nu_0^m (\nu_1 - \nu_2) - \nu_1^m (\nu_0 - \nu_2) + \nu_2^m (\nu_0 - \nu_1)\right]}{m! n! p_{nm|Z}}, \tag{A.34}$$

can be shown to be non-negative for all the pairs (n, m) [4]. Then, an upper bound on M_{22} is straightforwardly given by

$$M_{22} \leq M_{22}^{\mathrm{U}} = \frac{\Omega_{22}^{\mathrm{U}}}{c_{22}}, \tag{A.35}$$

where we have lower bounded the term $\sum_{\substack{n,m \geq 2 \\ n,m \neq 2}}^{\infty} c_{nm} M_{nm}$ by zero.

Upper bounds on M_{02} and M_{04}

By substituting $\kappa_A^{\mu} = \mu$, $\kappa_B^{\mu} = 1$, $w_A^{\mu_0\mu_1} = (\mu_0 - \mu_1)\mu_0$, $w_A^{\mu_1\mu_2} = (\mu_1 - \mu_2)\mu_2$ and $w_B^{\mu\nu} = (\mu - \nu)$ in Ω, we consider the following function Ω_{02}:

$$\Omega_{02} := \Omega = \sum_{m=2}^{\infty} c_{0m} M_{0m} + \sum_{\substack{n=3 \\ m=2}}^{\infty} c_{nm} M_{nm}, \tag{A.36}$$

where the coefficients

$$c_{nm} = \frac{\left[\mu_0^n \mu_1 \mu_2 (\mu_1 - \mu_2) - \mu_1^n \mu_0 \mu_2 (\mu_0 - \mu_2) + \mu_2^n \mu_0 \mu_1 (\mu_0 - \mu_1)\right] \left[\nu_0^m (\nu_1 - \nu_2) - \nu_1^m (\nu_0 - \nu_2) + \nu_2^m (\nu_0 - \nu_1)\right]}{m! n! p_{nm|Z}}, \tag{A.37}$$

can be shown to be non-negative for all pairs (n, m) [4]. Then, an upper bound on M_{02} is straightforwardly given by

$$M_{02} \leq M_{02}^{\mathrm{U}} = \frac{\Omega_{02}^{\mathrm{U}}}{c_{02}}, \tag{A.38}$$

where we have lower bounded all the terms $c_{nm} M_{nm}$ in Eq. (A.36), with the exception of $c_{02} M_{02}$, by zero. Similarly, an upper bound on M_{04} is directly given by

$$M_{04} \leq M_{04}^{\mathrm{U}} = \frac{\Omega_{02}^{\mathrm{U}}}{c_{04}}. \tag{A.39}$$

Upper bounds on M_{20} and M_{40}

By substituting $\kappa_A^{\mu} = 1$, $\kappa_B^{\mu} = \mu$, $w_A^{\mu\nu} = (\mu - \nu)$, $w_B^{\nu_0\nu_1} = (\nu_0 - \nu_1)\nu_0$ and $w_B^{\nu_1\nu_2} = (\nu_1 - \nu_2)\nu_2$ in Ω, we obtain the following function Ω_{20}:

$$\Omega_{20} := \Omega = \sum_{n=2}^{\infty} c_{n0} M_{n0} + \sum_{\substack{n=2 \\ m=3}}^{\infty} c_{nm} M_{nm}, \tag{A.40}$$

where the coefficients

$$c_{nm} = \frac{\left[\mu_0^n (\mu_1 - \mu_2) - \mu_1^n (\mu_0 - \mu_2) + \mu_2^n (\mu_0 - \mu_1)\right] \left[\nu_0^m \nu_1 \nu_2 (\nu_1 - \nu_2) - \nu_1^m \nu_0 \nu_2 (\nu_0 - \nu_2) + \nu_2^m \nu_0 \nu_1 (\nu_0 - \nu_1)\right]}{m! n! p_{nm|Z}}, \tag{A.41}$$

can be shown to be non-negative for all the pairs (n, m) [4]. Then, an upper bound on M_{20} is straightforwardly given by

$$M_{20} \leq M_{20}^{\mathrm{U}} = \frac{\Omega_{20}^{\mathrm{U}}}{c_{20}}. \tag{A.42}$$

where we have lower bounded all the terms $c_{nm} M_{nm}$ in Eq. (A.40), with the exception of $c_{20} M_{20}$, by zero. Similarly, an upper bound on M_{40} is directly given by

$$M_{40} \leq M_{40}^{\mathrm{U}} = \frac{\Omega_{20}^{\mathrm{U}}}{c_{40}}. \tag{A.43}$$

Upper bound on M_{13}

By substituting $\kappa_A^{\mu} = \kappa_B^{\mu} = 1$, $w_A^{\mu\nu} = (\mu^2 - \nu^2)$ and $w_B^{\mu\nu} = (\mu - \nu)$ in Ω, we obtain a function Ω_{13} such that:

$$-\Omega_{13} := \Omega = \sum_{m=2}^{\infty} c_{1m} M_{1m} + \sum_{\substack{n=3 \\ m=2}}^{\infty} c_{nm} M_{nm}, \tag{A.44}$$

where the coefficients

$$c_{nm} = -\frac{\left[\mu_0^n\left(\mu_1^2 - \mu_2^2\right) - \mu_1^n\left(\mu_0^2 - \mu_2^2\right) + \mu_2^n\left(\mu_0^2 - \mu_1^2\right)\right]\left[\nu_0^m\left(\nu_1 - \nu_2\right) - \nu_1^m\left(\nu_0 - \nu_2\right) + \nu_2^m\left(\nu_0 - \nu_1\right)\right]}{m!n!p_{nm|Z}}, \tag{A.45}$$

can be shown to be positive for the pairs $(n, m) \in S_+$, being $S_+ = \{(n, m)|n = 1, m \geq 2\}$ and negative for the pairs $(n, m) \in S_-$, being $S_- = \{(n, m)|n \geq 3, m \geq 2\}$ [4]. Then, by following a similar procedure to that used to derive Eq. (A.30), an upper bound on M_{13} can be obtained as

$$M_{13} \leq M_{13}^{\mathrm{U}} = \frac{c_{\max}(M_z - M_{0A}^{\mathrm{L}} - M_{0B}^{\mathrm{L}} + M_{00}^{\mathrm{U}}) - \Omega_{13}^{\mathrm{L}}}{c_{13} + c_{\max}}, \tag{A.46}$$

where $c_{\max} = \frac{(\nu_1 - \nu_2)}{e^{-\nu_0} p_{\nu_0}} \frac{\left(\mu_1^2 - \mu_2^2\right)}{e^{-\mu_0} p_{\mu_0}}$, and M_{0A}^{L} and M_{0B}^{L} are given by Eqs. (A.31) and (A.32), respectively.

Upper bound on M_{31}

By substituting $\kappa_A^{\mu} = \kappa_B^{\mu} = 1$, $w_A^{\mu\nu} = (\mu - \nu)$ and $w_B^{\mu\nu} = (\mu^2 - \nu^2)$ in Ω, we obtain a function Ω_{31} such that:

$$-\Omega_{31} := \Omega = \sum_{n=2}^{\infty} c_{n1} M_{n1} + \sum_{\substack{n=2 \\ m=3}}^{\infty} c_{nm} M_{nm}, \tag{A.47}$$

where the coefficients

$$c_{nm} = -\frac{\left[\mu_0^n\left(\mu_1 - \mu_2\right) - \mu_1^n\left(\mu_0 - \mu_2\right) + \mu_2^n\left(\mu_0 - \mu_1\right)\right]\left[\nu_0^m\left(\nu_1^2 - \nu_2^2\right) - \nu_1^m\left(\nu_0^2 - \nu_2^2\right) + \nu_2^m\left(\nu_0^2 - \nu_1^2\right)\right]}{m!n!p_{nm|Z}}, \tag{A.48}$$

can be shown to be positive for the pairs $(n, m) \in S_+$, with $S_+ = \{(n, m)|n \geq 2, m = 1\}$ and negative for the pairs $(n, m) \in S_-$, with $S_- = \{(n, m)|n \geq 2, m \geq 3\}$ [4]. Then, by following a similar procedure to that used to derive Eq. (A.30), an upper bound on M_{31} can be obtained as

$$M_{31} \leq M_{31}^{\mathrm{U}} = \frac{c_{\max}(M_z - M_{0A}^{\mathrm{L}} - M_{0B}^{\mathrm{L}} + M_{00}^{\mathrm{U}}) - \Omega_{31}^{\mathrm{L}}}{c_{31} + c_{\max}}, \tag{A.49}$$

where $c_{\max} = \frac{(\mu_1-\mu_2)}{e^{-\mu_0}p_{\mu_0}}\frac{(\nu_1^2-\nu_2^2)}{e^{-\nu_0}p_{\nu_0}}$, and M_{0A}^{L} and M_{0B}^{L} are given by Eqs. (A.31) and (A.32), respectively.

A.3 Channel model

For our simulations, we use the channel model of [6], which we summarize here. We model the overall loss between Alice (Bob) and Charlie by a beamsplitter of transmittance $\sqrt{\eta}$, which includes the channel transmissivity and the quantum efficiency of Charlie's detectors. We consider that the quantum channels connecting Alice and Bob with Charlie introduce both phase and polarisation misalignment. We model the phase reference mismatch between Alice and Bob's pulses by shifting Bob's signals by an angle $\phi = \delta_{\mathrm{ph}}\pi$. We model polarisation misalignment as a unitary operation that transforms Alice's (Bob's) polarisation input mode $a_{\mathrm{in}}^\dagger$ ($b_{\mathrm{in}}^\dagger$) into the orthogonal polarisation output modes $a_{\mathrm{out}}^\dagger$ and $a_{\mathrm{out}\perp}^\dagger$ ($b_{\mathrm{out}}^\dagger$ and $b_{\mathrm{out}\perp}^\dagger$) as follows: $a_{\mathrm{in}}^\dagger \rightarrow \cos(\theta_A)a_{\mathrm{out}}^\dagger - \sin(\theta_A)a_{\mathrm{out}\perp}^\dagger$ ($b_{\mathrm{in}}^\dagger \rightarrow \cos(\theta_B)b_{\mathrm{out}}^\dagger - \sin(\theta_B)b_{\mathrm{out}\perp}^\dagger$). The rotation angles are assumed to be $\theta_A = -\theta_B = \arcsin\left(\sqrt{\delta_{\mathrm{pol}}}\right)$.

With this channel model, it can be shown [6] that the probability that Charlie reports a successful detection, given that both users employ the X basis, is given by

$$Q_X = (1-p_{\mathrm{d}})(e^{-\gamma\Omega(\phi,\theta)} + e^{\gamma\Omega(\phi,\theta)})e^{-\gamma} - 2(1-p_{\mathrm{d}})^2 e^{-2\gamma}, \tag{A.50}$$

where $\gamma = \sqrt{\eta}\alpha^2$, $\theta = \theta_A - \theta_B$, and $\Omega(\phi,\theta) = \cos\phi\cos\theta$. The probability that Alice and Bob end up with different key bits is given by

$$e_X = \frac{e^{-\gamma\Omega(\phi,\theta)} - (1-p_{\mathrm{d}})e^{-\gamma}}{e^{-\gamma\Omega(\phi,\theta)} + e^{\gamma\Omega(\phi,\theta)} - 2(1-p_{\mathrm{d}})e^{-\gamma}}, \tag{A.51}$$

while the probability that Charlie reports a successful detection, given that both users employ the Z basis and select the intensities μ and ν, respectively, is

$$Q^{\mu\nu} = 2(1-p_{\mathrm{d}})\left[e^{-\frac{(\mu^2+\nu^2)\sqrt{\eta}}{2}} I_0(\mu\nu\sqrt{\eta}\cos\theta) - (1-p_{\mathrm{d}})e^{-(\mu^2+\nu^2)\sqrt{\eta}}\right], \tag{A.52}$$

where $I_0(z) = \frac{1}{2\pi i}\oint e^{(z/2)(t+1/t)}t^{-1}\mathrm{d}t$ is the modified Bessel function of the first kind.

In our simulations, we assume that the observed measurement counts equal their expected value, that is, we set $M_X = Np_X^2 Q_X$ and $M^{\mu\nu} = Np_Z^2 p_\mu p_\nu Q^{\mu\nu}$, where $M^{\mu\nu}$ denotes the number of successful rounds in which Alice and Bob select the Z basis and the intensities μ and ν, respectively. Also, we assume that the bit-error rate of the sifted-key equals the probability given by Eq. (A.51).

A.4 Additional simulation results

Results for $p_{\mathrm{d}} = 10^{-9}$

In Fig. A.1, we show the results obtainable for a dark count probability of 10^{-9} instead of 10^{-8}, which may be feasible using state-of-the-art SSPD detectors [7]. Compared with Fig. 4.2 in the main text, we see that, for sufficiently large block sizes, the protocol can now reach longer distances. However, for the case $N = 10^{10}$, the curve in Fig. A.1 is almost identical to that of Fig. 4.2 in the main text.

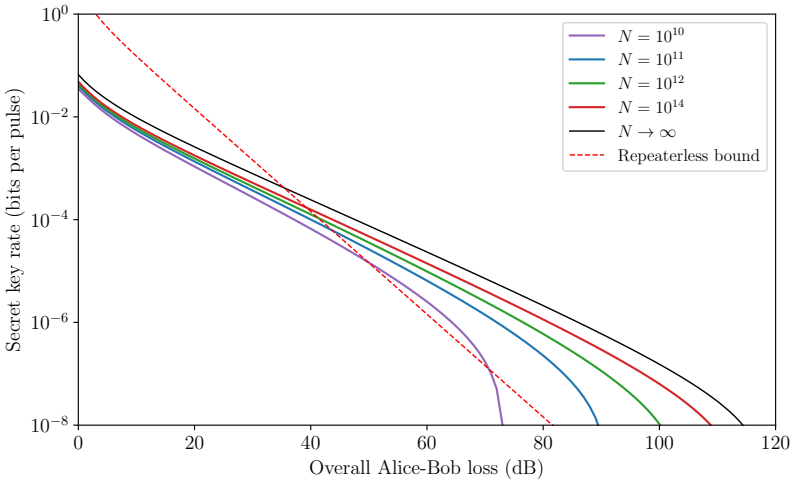


Figure A.1: Results obtainable for the channel parameters in the main text, but a dark count probability of 10^{-9}.

Comparison with sending-or-not-sending

In Fig. A.2, we provide a more in-depth comparison of the key rate obtainable for a broader range of values of the phase reference mismatch δ_{ph} and the block size N. We can see that, in general, our protocol performs better for larger block sizes and lower misalignment values, while the opposite is true for the sending-or-not-sending variant.

A.5 Proof of Equation (12) in the main text

Let us consider the evolution that the initial quantum state $|\Phi\rangle = |\phi\rangle^{\otimes N}$, where $|\phi\rangle = |\psi\rangle_{A_c A a} \otimes |\psi\rangle_{B_c B b}$ and $|\psi\rangle$ is given by Eq. (4.10) in the main text, experiences before step

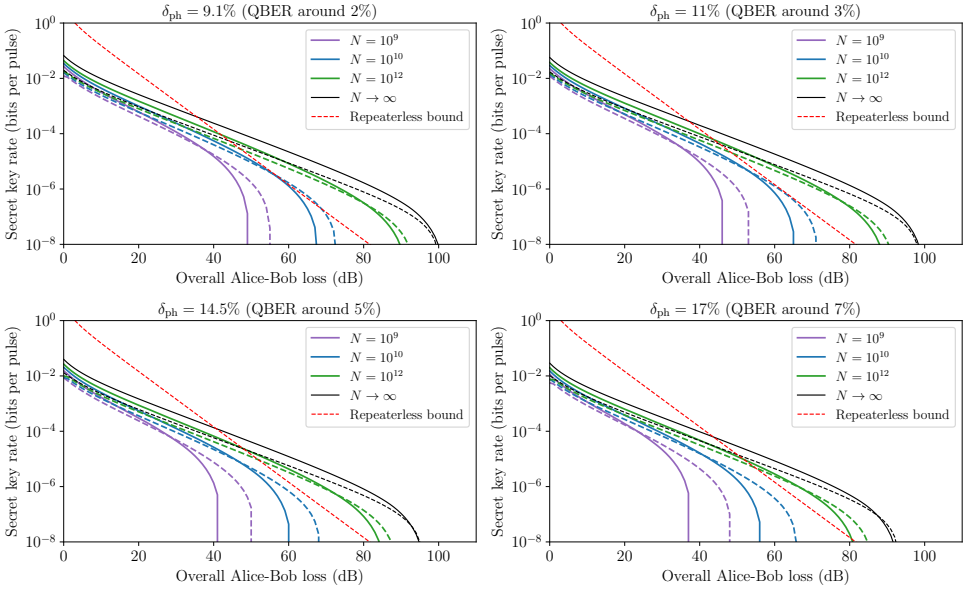


Figure A.2: Comparison between the results in this work (solid) and those of sending-or-not-sending TF-QKD [8, 9] (dashed), for several values of the phase-reference mismatch parameter δ_{ph} and the block size N. The rest of the parameters are those in the main text.

(4.1) of the virtual protocol, by taking into account all operations applied to it. After Eve's measurement in step (2), it is transformed to $\hat{M}_{\text{eve}} |\Phi\rangle$, where $\hat{M}_{\text{eve}}$ is the operator associated with her outcome. Let us reorder $|\Phi\rangle$ as $|\Phi\rangle = |\phi\rangle^{\otimes M} |\phi\rangle^{\otimes \bar{M}}$, writing first (last) the M ($\bar{M}$) successful (unsuccessful) rounds. In the virtual sifting step, Alice and Bob measure all subsystems A_c and B_c, using measurement operators $\{\hat{O}_s = |00\rangle\langle 00| + |11\rangle\langle 11|, \hat{O}_d = \mathbb{I} - \hat{O}_s\}$. Again, let us reorder $|\Phi\rangle = |\phi\rangle^{\otimes M_s} |\phi\rangle^{\otimes M_d} |\phi\rangle^{\otimes \bar{M}_s} |\phi\rangle^{\otimes \bar{M}_d}$, writing first (second) the M_s (M_d) successful rounds in which the users used the same (a different) basis, and third (fourth) the $\bar{M}_s$ ($\bar{M}_d$) unsuccessful rounds in which the users used the same (a different) basis. The unnormalised quantum state just before step (4.1) is then given by

$$\begin{aligned} \hat{O}_s^{\otimes M_s} \hat{O}_d^{\otimes M_d} \hat{O}_s^{\otimes \bar{M}_s} \hat{O}_d^{\otimes \bar{M}_d} \hat{M}_{\text{eve}} |\Phi\rangle &= \hat{M}_{\text{eve}} \hat{O}_s^{\otimes M_s} \hat{O}_d^{\otimes M_d} \hat{O}_s^{\otimes \bar{M}_s} \hat{O}_d^{\otimes \bar{M}_d} |\Phi\rangle \\ &= \hat{M}_{\text{eve}} (\hat{O}_s |\phi\rangle)^{\otimes M_s} (\hat{O}_d |\phi\rangle)^{\otimes M_d} (\hat{O}_s |\phi\rangle)^{\otimes \bar{M}_s} (\hat{O}_d |\phi\rangle)^{\otimes \bar{M}_d}, \end{aligned} \tag{A.53}$$

where we have used the fact that $\hat{M}_{\text{eve}}$ commutes with the sifting operators, as they act on different systems. Next, in step (4.1), Alice and Bob measure the registers A_c,

B_c, A and B for all rounds in $\mathcal{M}_s$, one by one. Let $u \in \{1, ..., M_s\}$ index the rounds in $\mathcal{M}_s$, let ξ_u be the outcome of the measurement of the u-th registers, and let $\hat{M}_u$ denote its associated measurement operator. Note that $\hat{M}_u \hat{O}_s = \hat{M}_u$. The unnormalised state just before their measurement of the u-th registers is

$$|\Phi_u\rangle = \hat{M}_{\text{eve}}(\otimes_{l=1}^{u-1} \hat{M}_l |\phi\rangle)(\hat{O}_s |\phi\rangle_u)(\hat{O}_s |\phi\rangle)^{\otimes(M_s-u)}(\hat{O}_d |\phi\rangle)^{\otimes M_d}(\hat{O}_s |\phi\rangle)^{\otimes \bar{M}_s}(\hat{O}_d |\phi\rangle)^{\otimes \bar{M}_d}, \tag{A.54}$$

where we have highlighted the initial quantum state of the u-th round, renaming it as $|\phi\rangle_u$. Since we are interested in the reduced state of the round u, we trace out the other rounds, which we denote by $\bar{u}$:

$$\hat{\sigma}_u = \text{Tr}_{\bar{u}}[|\Phi_u\rangle\langle\Phi_u|] = \sum_{\vec{u}} \langle \vec{u} | \Phi_u \rangle \langle \Phi_u | \vec{u} \rangle = \sum_{\vec{u}} \hat{M}_{\vec{u}} \hat{O}_s |\phi\rangle\langle\phi|_u \hat{O}_s^\dagger \hat{M}_{\vec{u}}^\dagger, \tag{A.55}$$

where

$$\hat{M}_{\vec{u}} = \langle \vec{u} | \hat{M}_{\text{eve}}(\otimes_{l=1}^{u-1} \hat{M}_l |\phi\rangle)(\hat{O}_s |\phi\rangle)^{\otimes(M_s-u)}(\hat{O}_d |\phi\rangle)^{\otimes M_d}(\hat{O}_s |\phi\rangle)^{\otimes \bar{M}_s}(\hat{O}_d |\phi\rangle)^{\otimes \bar{M}_d}, \tag{A.56}$$

and the states $\{|\vec{u}\rangle\}$ represent a basis for all the subsystems A_c, A, B_c, B, a and b of all the rounds in the protocol except the u-th round in $\mathcal{M}_s$. The operator $\hat{\sigma}_u$ is unnormalised, and its trace denotes the joint probability of all previous measurement outcomes in the protocol. This includes Eve's measurement outcomes and Alice and Bob virtual sifting results, which we collectively denote as the event $\boldsymbol{\xi}$; as well as Alice and Bob's measurement outcomes $\xi_1, ..., \xi_{u-1}$ of the previous $u-1$ registers. That is, $\text{Tr}[\hat{\sigma}_u] = \Pr(\boldsymbol{\xi}, \xi_1, ..., \xi_{u-1})$. The probability that Alice and Bob learn that they used the Z basis and sent Fock states $|n, m\rangle$ in the u-th round of $\mathcal{M}_s$, conditioned on all the

previous events, is

$$\begin{aligned}\Pr\left(\xi_u = Z_{nm}|\boldsymbol{\xi},\xi_1,...,\xi_{u-1}\right) &= \frac{\mathrm{Tr}\left[\langle 11|_{A_cB_c}\langle nm|_{AB}\,\hat{\sigma}_u\,|11\rangle_{A_cB_c}|nm\rangle_{AB}\right]}{\mathrm{Tr}[\hat{\sigma}_u]} \\ &= \frac{\mathrm{Tr}\left[\langle 11|_{A_cB_c}\langle nm|_{AB}\sum_{\vec{u}}\hat{M}_{\vec{u}}\,|\phi_u\rangle\langle\phi_u|\,\hat{M}_{\vec{u}}^\dagger\,|11\rangle_{A_cB_c}|nm\rangle_{AB}\right]}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})} \\ &= \frac{\sum_{\vec{u}}\left\|\hat{M}_{\vec{u}}\langle 11|_{A_cB_c}\langle nm|_{AB}\,|\phi\rangle_u\right\|^2}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})} \\ &= \frac{p_Z^2 p_{nm|Z}\sum_{\vec{u}}\left\|\hat{M}_{\vec{u}}\,|n\rangle_a|m\rangle_b\right\|^2}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})} \\ &= \frac{p_Z^2 p_{nm|Z}\,\langle n|_a\langle m|_b\left(\sum_{\vec{u}}\hat{M}_{\vec{u}}^\dagger\hat{M}_{\vec{u}}\right)|n\rangle_a|m\rangle_b}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})},\end{aligned} \tag{A.57}$$

where in the second equality we have used $\hat{O}_s\hat{M}_{\vec{u}} = \hat{M}_{\vec{u}}\hat{O}_s$ and $\hat{O}_s\,|11\rangle_{A_cB_c} = |11\rangle_{A_cB_c}$. Now, let $\hat{E}_u = \sum_{\vec{u}}\hat{M}_{\vec{u}}^\dagger\hat{M}_{\vec{u}}$. Since $\hat{E}_u$ is a sum of positive semi-definite operators, it is positive semi-definite. Therefore, we can decompose it as $\hat{E}_u = \sqrt{\hat{E}_u}\sqrt{\hat{E}_u}$, and rewrite Eq. (A.57) as

$$\begin{aligned}\Pr\left(\xi_u = Z_{nm}|\boldsymbol{\xi},\xi_1,...,\xi_{u-1}\right) &= \frac{p_Z^2 p_{nm|Z}\,\langle n|_a\langle m|_b\sqrt{\hat{E}_u}\sqrt{\hat{E}_u}\,|n\rangle_a|m\rangle_b}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})} \\ &= \frac{p_Z^2 p_{nm|Z}\left\|\sqrt{\hat{E}_u}\,|n\rangle_a|m\rangle_b\right\|^2}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})}.\end{aligned} \tag{A.58}$$

Using an identical approach, we can show that the probability that Alice and Bob will learn that they used the X basis and sent cat states $|C_i\rangle|C_j\rangle$ in the u-th successful round is

$$\Pr\left(\xi_u = X_{ij}|\boldsymbol{\xi},\xi_1,...,\xi_{u-1}\right) = \frac{p_X^2\left\|\sqrt{\hat{E}_u}\,|C_i\rangle_a|C_j\rangle_b\right\|^2}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})}. \tag{A.59}$$

Now, we want to relate the probability terms on the left hand side of Eqs. (A.58) and (A.59). For this, we use the approach of [6] and apply the Cauchy-Schwartz

inequality to show that

$$\begin{aligned}\left\|\sqrt{\hat{E}_u}\left|C_i\right\rangle_a\left|C_j\right\rangle_b\right\|^2 &= \sum_{\substack{n,n'\in\mathbb{N}_i\\ m,m'\in\mathbb{N}_j}} \sqrt{p_{n'm'|X}}\sqrt{p_{nm|X}}\left\langle n'\right|_a\left\langle m'\right|_b\sqrt{\hat{E}_u}\sqrt{\hat{E}_u}\left|n\right\rangle\left|m\right\rangle \\ &\leq \sum_{\substack{n,n'\in\mathbb{N}_i\\ m,m'\in\mathbb{N}_j}} \sqrt{p_{n'm'|X}}\sqrt{p_{nm|X}}\left\|\sqrt{\hat{E}_u}\left|n'\right\rangle_a\left|m'\right\rangle_b\right\|\left\|\sqrt{\hat{E}_u}\left|n\right\rangle_a\left|m\right\rangle_b\right\| \\ &= \left[\sum_{n\in\mathbb{N}_i,m\in\mathbb{N}_j}\sqrt{p_{nm|X}}\left\|\sqrt{\hat{E}_u}\left|n\right\rangle_a\left|m\right\rangle_b\right\|\right]^2 .\end{aligned} \tag{A.60}$$

Combining the three previous equations, we obtain

$$\begin{aligned}P\left(\xi_u = X_{ij}|\boldsymbol{\xi},\xi_1,...,\xi_{u-1}\right) &\leq \frac{p_X^2\left[\sum_{n\in\mathbb{N}_i,m\in\mathbb{N}_j}\sqrt{p_{nm|X}}\left\|\sqrt{\hat{E}_u}\left|n\right\rangle_a\left|m\right\rangle_b\right\|\right]^2}{\Pr(\boldsymbol{\xi},\xi_1,...,\xi_{u-1})} \\ &= \frac{p_X^2}{p_Z^2}\left[\sum_{n\in\mathbb{N}_i,m\in\mathbb{N}_j}\sqrt{\frac{p_{nm|X}}{p_{nm|Z}}\Pr\left(\xi_u = Z_{nm}|\boldsymbol{\xi},\xi_1,...,\xi_{u-1}\right)}\right]^2,\end{aligned} \tag{A.61}$$

and since a phase error occurs when $\xi_u \in \{X_{00}, X_{11}\}$, its probability is upper-bounded by

$$\begin{aligned}&\Pr\left(\xi_u \in \{X_{00},X_{11}\}|\boldsymbol{\xi},\xi_0,...,\xi_{u-1}\right) \\ &\quad\leq \frac{p_X^2}{p_Z^2}\sum_{j=0}^{1}\left[\sum_{n,m\in\mathbb{N}_j}\sqrt{\frac{p_{nm|X}}{p_{nm|Z}}\Pr\left(\xi_u = Z_{nm}|\boldsymbol{\xi},\xi_1,...,\xi_{u-1}\right)}\right]^2.\end{aligned} \tag{A.62}$$

Note that, since all probabilities are conditioned on $\boldsymbol{\xi}$, we can remove it from the conditions and work on the probability space in which the event $\boldsymbol{\xi}$ has happened. Also, to match the notation in Eqs. (4.13) to (4.15) of the main text, we rewrite Eq. (A.62) as

$$\Pr\left(\xi_u \in \{X_{00},X_{11}\}|\mathcal{F}_{u-1}\right) \leq \frac{p_X^2}{p_Z^2}\sum_{j=0}^{1}\left[\sum_{n,m\in\mathbb{N}_j}\sqrt{\frac{p_{nm|X}}{p_{nm|Z}}\Pr\left(\xi_u = Z_{nm}|\mathcal{F}_{u-1}\right)}\right]^2, \tag{A.63}$$

where $\mathcal{F}_{u-1}$ is the σ-algebra generated by $\xi_1,...,\xi_{u-1}$.

A.6 Inverse multiplicative Chernoff bound

Here, we state the result that we use to obtain the lower and upper bounds required in Eq. (4.26) of the main text. Let $\chi = \sum_{i=1}^{n} \chi_i$ be the outcome of a sum of n independent Bernoulli random variables $\chi_i \in \{0, 1\}$. Given the observation of the outcome χ, its expectation value $\mathbb{E}[\chi]$ can be lower and upper bounded by [10]

$$\begin{aligned} \mathbb{E}^{\mathrm{L}}[\chi] &= \frac{\chi}{1+\delta^{\mathrm{L}}}, \\ \mathbb{E}^{\mathrm{U}}[\chi] &= \frac{\chi}{1-\delta^{\mathrm{U}}}, \end{aligned} \tag{A.64}$$

except with a probability ε_{c}, where δ^{L} and δ^{U} are the solutions of the following equations

$$\begin{aligned} \left[\frac{e^{\delta^{\mathrm{L}}}}{(1+\delta^{\mathrm{L}})^{1+\delta^{\mathrm{L}}}}\right]^{\chi/(1+\delta^{\mathrm{L}})} &= \frac{1}{2}\varepsilon_{\mathrm{c}} \\ \left[\frac{e^{-\delta^{\mathrm{U}}}}{(1-\delta^{\mathrm{U}})^{1-\delta^{\mathrm{U}}}}\right]^{\chi/(1-\delta^{\mathrm{U}})} &= \frac{1}{2}\varepsilon_{\mathrm{c}}. \end{aligned} \tag{A.65}$$

The solutions to Eq. (A.65) satisfy [11]

$$\begin{aligned} \frac{1}{1+\delta_L} &= -W_0(-e^{(\ln(\varepsilon_{\mathrm{c}}/2)-\chi)/\chi}), \\ \frac{1}{1-\delta_U} &= -W_{-1}(-e^{(\ln(\varepsilon_{\mathrm{c}}/2)-\chi)/\chi}), \end{aligned} \tag{A.66}$$

where W_0 and W_{-1} are branches of the Lambert W function, which is the inverse of the function $f(z) = ze^z$.

References

[1] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," *IEEE Trans. Inf. Theory*, vol. 57, pp. 5524–5535, Aug. 2011. 198

[2] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nat. Commun.*, vol. 3, p. 634, Jan. 2012. 198, 200

[3] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, p. 110506, Mar. 2011. 198, 199

[4] F. Grasselli, Á. Navarrete, and M. Curty, "Asymmetric twin-field quantum key distribution," *New J. Phys.*, vol. 21, p. 113032, Nov. 2019. 202, 203, 204, 205, 206, 207

[5] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Phys. Rev. A*, vol. 89, p. 022307, Feb. 2014. 205

[6] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Inf.*, vol. 5, p. 64, July 2019. 208, 212

[7] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin, and S. Nam, "Detecting single infrared photons with 93% system efficiency," *Nat. Photonics*, vol. 7, pp. 210–214, Feb. 2013. 209

[8] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Phys. Rev. A*, vol. 98, p. 062323, Dec. 2018. 210

[9] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, "Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses," *Phys. Rev. Appl.*, vol. 12, p. 024061, Aug. 2019. 210

[10] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A*, vol. 95, p. 012333, Jan. 2017. 214

[11] S. Bahrani, O. Elmabrok, G. Currás Lorenzo, and M. Razavi, "Wavelength assignment in quantum access networks with hybrid wireless-fiber links," *J. Opt. Soc. Am. B*, vol. 36, p. B99, Feb. 2019. 214