Wireless Quantum Key Distribution in Indoor Environments

Osama H Mohamed El Mabrok

University of Leeds

School of Electronic and Electrical Engineering

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

27th June 2018

Declaration

The candidate confirms that the work submitted is his own, except where work which has formed 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 the work submitted is his own and that appropriate credit has been given within the thesis where reference has been made to the work of others.

The work in chapter 4 has appeared in the following publications:

1. Elmabrok, O. and Razavi, M. (2015). Feasibility of wireless quantum key distribution in indoor environments. In Globecom Workshops (GC Wkshps), 2015 IEEE, 1-2, IEEE.
2. Elmabrok, O. and Razavi, M. (2018). Wireless quantum key distribution in indoor environments. J. Opt. Soc. Am. B, 35, 197-207.

The work in chapter 5 has appeared in the following publication:

1. Elmabrok, O. and Razavi, M. (2016). Quantum-classical access networks with embedded optical wireless links. In IEEE GLOBECOM 2016 Conference Proceedings, IEEE.
2. Elmabrok, O., Ghalaii, M. and Razavi, M. (2018). Quantum-classical access networks with embedded optical wireless links. J. Opt. Soc. Am. B, 35, 487-499.

The work in chapter 6 has been submitted to Qcrypt 2018, Shanghai, China.

This is to confirm that the candidate has contributed solely to the technical parts and writing of the papers above under the guidance of his co-authors. All publication listed above were accomplished under the supervision of Dr Mohsen Razavi.

This thesis is dedicated to my parents and my small family, for their endless support and encouragement.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisor Dr Mohsen Razavi for his guidance, help, and support in many ways throughout my PhD study. Thank you for giving me this great opportunity to work in such an interesting field.

Many thanks to Dr Sima Bahrani for her remarks and help, particularly in chapter 6. I would also like to thank my colleagues, Masoud Ghalaii and Guillermo Currás Lorenzo for their help and support.

I am grateful to University of Benghazi and Ministry of Higher Education and Scientific Research in Libya for supporting with a scholarship. Part of this research has also been funded by the UK Quantum Communications Hub under the EPSRC Grant EP/M013472/1.

Last, but not least, I would like to thank my wife for her support and understanding during my study.

Abstract

Among all emerging quantum information technologies, quantum key distribution (QKD) is one of the most developed techniques. QKD harnesses the intrinsic laws of quantum mechanics to provide a method for distributing secret random keys, which can be used for data encryption and decryption between two intended users. QKD has already been demonstrated in different scenarios over optical fibre and in atmospheric channels. QKD has also been used for security assurance in several network settings, in addition of being commercially available today. Despite remarkable progress in QKD systems, convenient access to the developing quantum communications networks is still missing. Adopting QKD in mobile devices would enable such a service, particularly, in indoor environments. This is in line with the recent advancement in fabricating microchip-scale QKD devices, which would ease this incorporation into mobile devices. This work focuses on the access networks, and, in particular, it addresses the wireless mode of access in *indoor environments* for QKD networks. We find a practical regime of operation, where, in the presence of external light sources and loss, secret keys can be exchanged. We then propose practical configurations that would enable wireless access to hybrid quantum-classical networks. The proposed setups would allow an indoor wireless user, equipped with a QKD-enabled mobile device, to communicate securely with a remote party on the other end of the access network. We account for adverse effects of the background noise induced by Raman scattered light on the QKD receivers due to the transmission of both quantum and classical signals over the same fibre. In addition, we consider the loss and the background noise that arise from indoor environments. We consider a number of discrete and continuous-variable QKD protocols and study their performance in different scenarios. In our analysis we consider the asymptotic scenario, as well as the finite-size key effects. In the former case, an infinite number of signals are assumed to be exchanged between the sender and the recipient, whereas in the latter, which represents the practical scenario, a finite number of signals are exchanged between the two users. Our results indicate that a feasible regime of operation for wireless QKD exists. This makes the QKD technologies available to end users of a communications network.

Abbreviations

APD	Avalanche Photo Diode
AWG	Arrayed Waveguide Grating
BER	Bit Error Rate
BN	Background Noise
BRS	Backward Raman Scattering
CV-QKD	Continuous Variable-Quantum Key Distribution
DD	Direct Detection
DS	Decoy State
DV-QKD	Discrete Variable-Quantum Key Distribution
DWDM	Dense Wavelength Division Multiplexing
FOV	Field of View
FRS	Forward Raman Scattering
IM	Intensity Modulation
IR	Infrared
LD	Laser Diode
LED	Light Emitting Diode
Li-Fi	Light Fidelity
LO	Local Oscillator
LOS	Line of Sight
MDI-QKD	Measurement-Device-Independent Quantum Key Distribution
MZI	Mach-Zehnder Interferometer
NA	Numerical Aperture
NLOS	Non-LOS
OTP	One-Time Pad
OWC	Optical Wireless Communications
PBS	Polarizing Beam Splitter
PIN	Positive-Intrinsic-Negative
PM	Phase Modulator
P&M	Prepare and Measure
PNS	Photon-Number-Splitting
PON	Passive Optical Network
PSD	Power Spectral Density
QBER	Quantum Bit Error Rate
Qubit	Quantum Bit
RF	Radio Frequency
RFI-QKD	Reference Frame Independent Quantum Key Distribution
SPP	Single-Photon Pulse
TBN	Total Background Noise
WDM	Wavelength Division Multiplexing

Contents

List of Figures

Chapter 1

Introduction

1.1 Background

Information and communications technologies have an enormous impact on our daily lives. In particularly, data security is a significant issue, especially when dealing with smart adversaries who have powerful tools. Cryptographic techniques can achieve the goal of data protection by converting data into a format inaccessible to an unauthorised party. Such techniques today are based on the Kerckhoffs' concept Petitcolas [2011], in which, except for the key, an attacker is assumed to have a full knowledge of the cryptographic algorithm being used. In this case, in order to have a successful cryptographic scheme, we need to guarantee the security of its ingredients, such as the underlying key. Yet, there are many cases in which data security has been compromised. In fact, the security in many cryptography systems is currently based on the complexity of computations. That would urge us to find a better solution to guarantee the security of our data communication. In principle, in order to ensure the security, the key must be random (unpredictable to an eavesdropper), unique, and distributed in a secure way. Fortunately, such criteria can be fulfilled in practice using quantum key distribution (QKD) techniques. This technique allows two remote users to establish a sequence of secure bits, called a secret key. The resulted keys can then be used for securing the transmission of classical information. This thesis is an attempt to make QKD technologies available to a wide group of users.

Cryptography is an essential tool for data security in many aspects of our daily life, such as online banking services. From ancient times to present days, the cryptography has been used as an effective means to guarantee the confidentiality in data exchange. It is thought that the Romans began the idea of cryptography to convey a message securely to its intended destination. They used a simple means of encryption by replacing each letter in the original message with a letter three positions along in the alphabet to hide the content of the plaintext Dusek *et al.* [2006]. In 1926, the American scientist, Gilbert Vernam, invented a cryptographic approach known as one-time pad (OTP) Vernam [1926], which would provide unconditional security by assuming that the legitimate parties have previously shared a secret key. Yet, the distribution of keys in a secure way remains to be a challenge. Since then, cryptography has evolved gradually until attaining the existing advanced methods. The problem in the current cryptographic systems is that the security depends on the computational hardness, so the security of such systems will be always threatened. Alternatively, quantum cryptography, particularly QKD, is being developed nowadays to achieve unlimited security due to its dependence on the properties of quantum mechanics. As a result, QKD can generate and distribute a secret key even in the presence of an eavesdropper, Eve, who assumed to have an unlimited computational power.

The concept of quantum cryptography goes back to 1969, when a graduate student, Steven Wiesner, came up with the idea of quantum money Wiesner [1983]. The original manuscript, which passed unnoticed, was written circa 1970. By exploiting the properties of quantum mechanics, Wiesner decided to create bank notes which cannot be counterfeited. Even though his idea was not implemented in practice Imre & Gyongyosi [2012], it was the main motivation to Bennett and Brassard who introduced the first QKD protocol in 1984 Bennett [1984]. Nowadays, QKD has become the most popular technique among quantum communication technologies. It provides, in principle, an absolute secure method for keys distribution in comparison with the existing classical schemes.

The current dominant approach for ensuring data security over the Internet is based on a combination of public-key cryptography, e.g., the Rivest-Shamir-Adleman (RSA) protocol Rivest *et al.* [1978], for exchanging a secret key/seed, and symmetric-key cryptography protocols, such as advanced encryption standard (AES) or secure hash algorithm, for encryption, decryption, and authentication. The security of RSA is, however, based on the computational complexity of the factoring problem. The latter does not have any known efficient solutions on classical computers, but there exists a quantum algorithm using which one can solve the factoring problem in polynomial time Shor [1994]. This is a huge threat to the security of our online communications, such as email correspondence and banking transactions, especially considering the progress made in the past few years in quantum computing Barends *et al.* [2016], Johnson *et al.* [2011], Moran [2016], Shor [1994]. Note that, although symmetric-key algorithms such as AES may now be considered safe against quantum attacks Campagna *et al.* [2015], the initial input keys to such algorithms are currently distributed between two remote users using public-key schemes, which are vulnerable to quantum attacks. This would necessitate the implementation of alternative solutions, such as QKD, at large scale to offer data security to every individual user.

It is then important to utilize the advantages of this scheme not only in niche markets but also for the general public Razavi [2011, 2012]. This necessitates developing hybrid quantum-classical networks that support many users. This requires revisiting the requirements at both access and core parts of the network. Indeed, future communications networks must offer improved security features against possible attacks enabled by quantum computing technologies. One possible solution is to develop quantum-classical networks that allow any two users to, not only exchange data, but also share secret key bits using QKD techniques. Despite the recent progress in QKD systems, more work needs to be done to make QKD conveniently available to the end users of communications networks. This can be possibly achieved by combing QKD with optical wireless communications (OWC).

The OWC technology has boomed and become a competitive method to radio techniques to connect computers and personal devices wirelessly Ramirez-Iniguez *et al.* [2008]. Due to its impressive properties, especially the higher bandwidth, optical wireless systems are utilized in many applications, such as hospitals and banks. One possible challenge of using OWC for QKD purposes is the existence of background noise caused by the artificial sources, as well as the sunlight, all affecting the performance of the underlying QKD system. This work focuses on the access networks, and, in particular, it addresses the wireless mode of access in indoor environments to the developing QKD networks.

1.2 Quantum key distribution overview

In conventional QKD protocols, an eavesdropper, Eve, cannot intercept the key without disturbing the system, and accordingly having her presence discovered. Furthermore, because of the no-cloning theorem Wootters & Zurek [1982], Eve cannot copy unknown quantum states. Based on these two principles, Bennett and Brassard in 1984 came up with their BB84 protocol in which single photons were carrying the key-bit information from Alice to Bob Bennett [1984]. Over the time, more practical protocols have been developed that allow us to use weak laser pulses to approximate single-photon pulses. Nevertheless, most QKD protocols will still rely on the few photon regime of operation, which makes them vulnerable to loss and background noise. This will make the implementation of QKD especially challenging in wireless mobile environments in which background noise is strong and alignment options are limited Elmabrok & Razavi [2015], Elmabrok *et al.* [2018].

In the original BB84 protocol Bennett [1984], the light source was assumed to emit perfect single photons, but it is not the case in practice. The progress with single-photon detectors has also been tremendous with quantum efficiencies as high as 93% and dark counts as low as one per second are now achievable Marsili *et al.* [2013]. Such developments have resulted in QKD being demonstrated over both optical fiber and free-space channels Korzh *et al.* [2015] Schmitt-Manderbach *et al.* [2007]. Today, various QKD systems are also commercially available. Examples are Clavis by ID Quantique in Switzerland idq [2010] and various products by QuantumCTek in China Qua [2012], which contributes to the 2000-km-long QKD link between Beijing and Shanghai. The latter is an example of QKD networks that are being developed across the world, in order to support a wider group of end users. It is clear that the focus of most of these efforts is, however, mainly on the core networks Sasaki *et al.* [2011], or the wired access to such a backbone Fröhlich *et al.* [2013]. This thesis, however, widens the QKD adoption by looking into *wireless* indoor QKD.

1.3 Wireless indoor QKD

Wireless access to a communications network is often taken for granted. This is not the case, however, for quantum communications. Most of QKD experiments are fiber-based in which point-to-point communication is established. In addition, the single photons enjoy traveling through a very low-loss channel. Through-the-air QKD experiments have also been point to point, therefore not offering mobility, and often require expensive and bulky optics equipment. However, nowadays, wireless connection is a necessity because of its convenience and also, because of the ever increasing use of handheld devices. In order that QKD will ever become ubiquitously used, wireless mobile QKD needs to be developed. While it is hard to envisage, at the moment, that wireless quantum access can be offered anywhere anytime, there are certain scenarios in which wireless QKD can be both possible and beneficial. For instance, customers in a bank office may wish to exchange secret keys with the bank wirelessly without the need for waiting for a teller or a cash machine, and without being worried about their data privacy due to skimming frauds Duligall *et al.* [2006]. Handheld prototypes have already been made, which enable a user to securely exchange a key with a cash machine Chun *et al.* [2017], Duligall *et al.* [2006]. It would be desirable to remove the constraint of being in the vicinity of a bank machine. In such a scenario, wireless indoor QKD is an attractive solution. In the long term, such indoors solutions can be part of a home network, which is equipped with wireless optical communications and is connected via fiber to its main service provider Elmabrok & Razavi [2016]. This is in line with the developing Li-Fi technologies in data communications connected to passive optical networks (PONs) for high data rate transmissions. Our proposed wireless QKD link will be using the same infrastructure while complementing the range of services offered to the user by adding quantum enabled security.

Wireless indoor QKD would not be without its own implementation challenges. Such a system is expected to suffer from the background noise, loss, and the implications of the mobility requirement. Ambient light, caused by the sun and artificial sources of light, is the primary hindrance to the successful operation of QKD in indoor environments. Essentially, QKD is a noise-dependent scheme, in which a secret key cannot be exchanged when the noise level exceeds a certain level. Another possible downside of indoor environments is the existence of severe loss, in comparison to fiber-based QKD, when the transmitted beam angle is wide. For instance, the non-directed line-of-sight configuration, which suits most a mobile user, would suffer most from the background noise and loss. This is because, in this configuration, the receiver's field of view (FOV) should be sufficiently wide in order to collect sufficient power to operate. This could result in more background noise to sneak in. A wide beam angle at the transmitter would also result in a high channel loss, which may not be tolerable in the single-photon regime that QKD must operate. Beam steering could be a possible solution to such problems, but it would add to the complexity of the system and the cost of handheld devices.

Wireless indoor QKD is an interesting solution aiming to facilitate the access to the QKD networks, where the range is limited as in the case of PONs. Long distance wireless QKD can, however, be achieved using satellite-based QKD. The latter is one of the most interesting applications of free-space QKD. In this case, secure keys are being exchanged between a ground station, typically consists of a large-size telescope (diameter on the order of 1 m) and accurate tracking and pointing systems, and a satellite typically on the low-earth orbit. Such a setup can enable key exchange between two ground stations via a satellite, possibly far away by thousands of kilometres Liao *et al.* [2018]. This would help in providing a global network where secure data exchange is guaranteed. Our work on an indoor setup is a pre-cursor to a large-scale satellite network as one can simulate some aspects of satellite communications in an indoor setup under controlled conditions.

1.4 Research objectives and challenges

We aim to enable users equipped with a QKD-enabled mobile device in indoor environments to access a hybrid quantum-classical network. This would help end users to exchange quantum and classical data with service providers. However challenging, embedding QKD capability into mobile/handheld devices is an attractive solution for exchanging sensitive data in a safe and convenient manner. Initial prototypes have already been made, which enable a handheld device to exchange secret keys with an ATM without being affected by skimming frauds Chun *et al.* [2017], Duligall *et al.* [2006]. As another application, it would be desirable to enable a user working in a public space, such as an airport or a cafe, to exchange secret keys with its service provider via possibly untrusted nodes. Similarly, once fiber-to-the-home infrastructure is widely available, home users should benefit from such wireless links that connect them, via a PON, to other service provider nodes. In this case, the connection to the PON can be via an internal QKD node trusted by the user. Note that, in all cases above, we are dealing with a wireless link in an indoor environment, which may offer certain advantages, as compared to a general outdoor setup, in terms of ease of implementation. It is, nevertheless, a good starting point for offering wireless QKD services as we study here.

In this thesis, we first assess the feasibility of employing QKD in indoor environments by using the known techniques in OWC. This is done for QKD in a single-room single-user scenario. Multiple users can also be supported by using relevant multiple-access techniques Razavi [2012] Bahrani *et al.* [2015]. The system is mainly examined in the presence of background noise induced by an artificial lighting source, as well as the loss in indoor environments. We also account for possible imperfections in the encoder and decoder modules. After assessing the applicability, we propose practical configurations of trusted and untrusted links, that would enable wireless access to QKD networks. The proposed setups require hybrid links on which both data and quantum signals can travel in both wireless and wired modes. A QKD system run on such a hybrid quantum-classical link would then face certain challenges. First, the background light in the wireless environment can sneak into the fiber system and increase error rates of the QKD setup. Furthermore, due to nonlinear effects in optical fibers such as four-wave mixing and Raman scattering Eraerds *et al.* [2010], the data channels that travel alongside QKD channels on the same fiber can induce additional background noise on QKD systems. In particular, the impact of the Raman scattered light can be severe Eraerds *et al.* [2010], because its spectrum can overlap with the frequency band of QKD channels. By using extensive filtering in time and frequency domains, the impact of this noise can be mitigated Bahrani *et al.* [2016a], Patel *et al.* [2012, 2014b] and even maximally reduced Bahrani *et al.* [2016b], but it cannot be fully suppressed. By considering various sources of noise, four setups for embedding wireless indoor QKD links into quantum-classical access networks are then investigated. In each case, we find the corresponding key generation rate for relevant QKD protocols. We use the decoy state BB84 (DS-BB84) Ma *et al.* [2005], which relies on weak laser pulses, and measurement-device-independent QKD (MDI-QKD) Lo *et al.* [2012] protocols in our setups. MDI-QKD protocol can provide a trust-free link, as required in the case of a user in a public space, between the wireless user and the central office in an access network. The price to pay, however, is possible reduction in the rate. We also consider the GG02 protocol Grosshans & Grangier [2002], as a continuous-variable (CV) QKD scheme, and compare it with our discrete-variable (DV) protocols in terms of resilience to background noise and loss Kumar *et al.* [2014], Lasota *et al.* [2017]. In our analysis, we consider the asymptotic case, as well as the finite size scenario.

1.5 Novel contributions of the thesis

- We find a practical regime of operation for wireless QKD in indoor environments.

- We study the feasibility in different scenarios for the QKD source and receiver. Some results were presented in IEEE GLOBECOM 2015 Elmabrok & Razavi [2015].

- In the analysis, we estimate the background noise caused by a LED lighting source. We consider different scenarios where the QKD source is perfect or with known/unknown flaws. The results are published in Elmabrok *et al.* [2018].

- We examine embedding wireless indoor QKD in hybrid quantum-classical networks. We propose practical configurations that would enable wireless access to such networks Elmabrok & Razavi [2016, 2018].

- We assess the performance in practical scenarios where a finite size of data is assumed to be exchanged between two legitimate users.

1.6 Thesis outline

The rest of this thesis is organized as follows:

- In Chapter 2, we review relevant QKD techniques. We first introduce the principal properties of quantum mechanics and the key ideas behind QKD. Next, the DV (CV) QKD protocols being used in our study, will be explained.
- In Chapter 3, optical wireless communications is discussed. We provide the model and configuration used to characterise the channel in indoor environments.
- In Chapter 4, we present and discuss the feasibility aspects of wireless indoor QKD.
- In Chapter 5, we present and discuss the proposed configurations that would enable a convenient access to QKD networks.
- In Chapter 6, we present and discuss the finite-key analysis for wireless indoor QKD.
- In Chapter 7, the conclusions and future work are presented.

Chapter 2

Quantum key distribution

2.1 Introduction

The field of quantum information science has received much attention in recent years for its applications in cryptography. In particular, QKD, which is realizable today idq [2010] Qua [2012], has the capacity to generate perfect security in data exchange between parties. Since Bennett and Brassard introduced the BB84 scheme Bennett [1984], several QKD protocols have been presented, and the experimental implementation phase was the driver for many manufacturers to make QKD commercially available. Fortunately, quantum security systems are compatible with the standard optical networks as the main infrastructure in use. To date, a number of QKD protocols have been introduced and implemented over optical fibre or through free space, which could make QKD a strong competitor to classical cryptography in the future, due to its unconditional security. However, certain aspects such as rate and range, need to be enhanced before a full industrial deployment. Thus, significant efforts are being made to improve the key rate and to produce suitable devices for quantum cryptography.

The security of QKD has already been proven and remarkable experiments have illustrated the possibility of applying it in the real world Korzh *et al.* [2015] Schmitt-Manderbach *et al.* [2007]. QKD through free space is applicable, provided a line-of-sight link between the transmitter and the receiver is established. In contrast to fibre-based QKD, where standard telecommunication wavelengths are used, wavelengths in the range of 780-880 nm can also be utilized in atmospheric links rates. One of the interesting applications of free space-QKD is a key exchange between two ground stations via a satellite. For instance, in this scheme, a telescope on one of those ground stations receives polarized light pulses from a sender on a satellite to exchange a secret key, K_1. Correspondingly, the same scenario would be applied for the second ground station to obtain K_2. The satellite can then securely send K_1 to the second ground station by encrypting it using K_2. This can be done by performing bitwise XOR operation $K_1 \oplus K_2 = C$ and sending C to the ground station. Air turbulence is one of the problems that reduces the effective reception of the telescopes. In this case, a large telescope is used to collect as many of attenuated pulses as possible Prawer & Aharonovich [2014]. In 2007, the idea of a decoy state was implemented over 144 km between stations in the Canary Islands of Tenerife and La Palma Schmitt-Manderbach *et al.* [2007]. Similarly the Zeilinger Group, at the University of Vienna, achieved the same distance of 144 km by sending entangled photons instead Ursin *et al.* [2006].

While quantum optical fundamentals are generally the same as free space, fibre based-QKD uses the standard telecommunication wavelengths (1300 and 1550) nm instead. The downside of employing such wavelengths is the high noise and low efficiency of some of the currently used single photon detectors Prawer & Aharonovich [2014]. Recent developments of superconducting detectors has led a group from the University of Geneva to implement QKD over a distance of 307 km Korzh *et al.* [2015]. Interestingly, for the sake of future long-distance quantum communications, research is being conducted to develop quantum repeaters. This is because of the fiber loss that would result in limiting the transmission distances, as well as the secret key rates. Such repeaters rely on transmitting entangled quantum states between the repeater nodes. Satellite links could be used alternatively in order to have long-distance quantum communications, but this solution might be costly in comparison with optical links using quantum repeaters. Here, our focus is on the access network and how different QKD protocols and settings would adapt themselves into wireless indoor QKD.

QKD systems are classified by modulation into two main approaches, that is, discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD) Scarani *et al.* [2009]. In DV-QKD, the key distribution is achieved by utilizing certain degrees of freedom of light, that are discrete in nature, whereas in CV-QKD, it is accomplished by exploiting continuous ones. For instance in DV-QKD, the information can be encoded using the polarization of single photons. In contrast, CV-QKD encodes data by modifying the electric field quadrature amplitudes, $\hat{X}$ and $\hat{P}$. At the receiver, DV-QKD requires single-photon detectors to measure the received quantum states, whereas in CV-QKD protocols, coherent receivers, such as homodyne and heterodyne are in use. In this work, DV-QKD and CV-QKD protocols will be studied to draw a clear comparison about the feasibility and performance of different protocols. QKD systems are also classified by source into prepare and measure (P&M), which is assumed to be used in this study, and entanglement based. In P&M, the sender prepares quantum states using one of the encoding techniques, and send them to the recipient, who performs the measurement. In entanglement based KD, however, both users, perform the measurement, but the sender could be Alice or a third party.

In the following, in order to explain how QKD works, we first highlight, in short, the fundamentals of quantum mechanics and the relevant notions to QKD. Next, the key ideas behind QKD will be presented, and finally, the used DV(CV)-QKD protocols in this work are explained.

2.2 Quantum mechanics: fundamental concepts

Quantum mechanics is a mathematical framework that describes and explains the behaviour of quantum systems, such as electrons and photons. A quantum system is completely described by its state space, which provides all possible states of the system. In quantum mechanics, the state of a quantum object, such as the polarisation of a photon, is described by a vector in a complex vector space known as a Hilbert space. A qubit represents the simplest state in quantum information. QKD relys on intrinsic properties of quantum mechanics, such as superposition, uncertainty, and non-cloning theorem. For instance, the latter theorem states that unknown quantum states cannot be cloned perfectly. It would be possible, however, to make copies of a quantum state if you prepare a quantum object in a particular state. In quantum physics, entanglement is a special kind of correlation that exists between two quantum systems. This feature is crucial in certain QKD schemes. In the following, some important concepts related to QKD are explained.

2.2.1 Qubit

In classical computing theory, the bit is the basic unit of information, which has two possible values of 0 or 1. Qubit is the corresponding unit in quantum information that is expressed by states $|0\rangle$ and $|1\rangle$ or a superposition of them as shown below:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where $|0\rangle$ and $|1\rangle$ are called the computational basis states. α and β are complex amplitudes satisfying the normalization condition Nielsen & Chuang [2002]:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.2}$$

A qubit state can then be defined as a unit vector in a two dimensional complex vector space. In (2.2), $|\alpha|^2$ represents the probability of finding $|\psi\rangle$ in $|0\rangle$ if a measurement in $|0\rangle - |1\rangle$ basis is performed. $|\beta|^2$ represents the probability of finding $|\psi\rangle$ in state $|1\rangle$ upon such measurements.

Polarisation and time-bin of a single photon could be used to create a qubit in DV-QKD for information encoding. In time-bin degree of freedom, for instance, the photon generated by the source, is split into two time slots using an unbalanced interferometer, and sent to the recipient; see Fig. 2.1. The phase difference between the two slots can also be used to encode/decode the information.

2.2.2 Superposition and the measurement principle

The concept of quantum superposition is commonly explained by the ”Schrodinger’s cat” as shown in Fig. 2.2, where the cat may be alive and dead at the same time before opening the box in case of breaking a flask of poison. Quantum systems can similarly exist in a superposition (linear combination) of states, in which a measurement would cause a state to be collapsed into a single state with a certain probability.

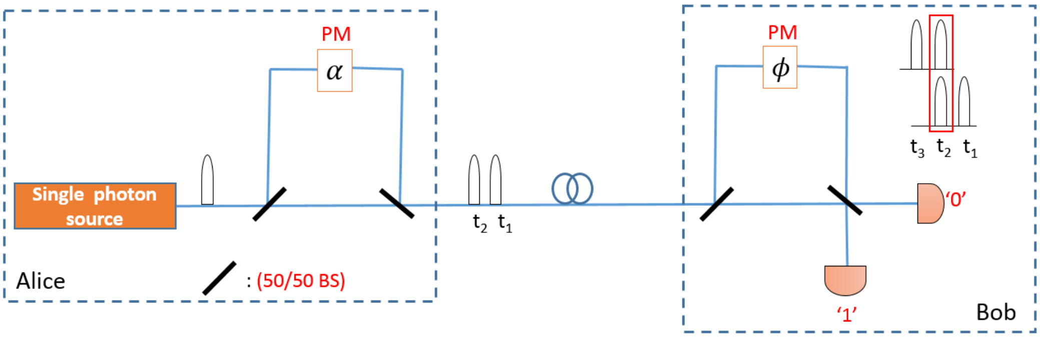

Figure 2.1: Time slot implementation of a qubit. BS: beamsplitter Diamanti [2006]. The photon can be either in time slot t_1 or t_2.

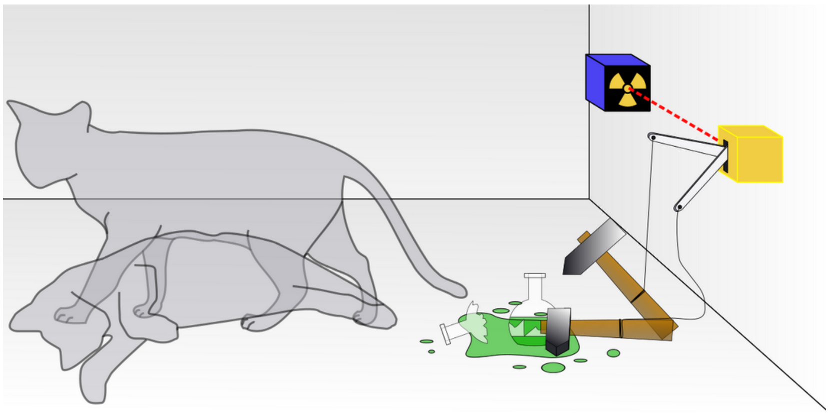

Figure 2.2: Schrodinger's Cat represents the concept of quantum superposition. We cannot be sure whether it is alive or dead before opening the box in case of breaking a flask of poison.

For instance, one manifestation of (2.1) is the polarisation state of a single photon, which can be described as follows:

$$|\psi\rangle = \alpha|H\rangle + \beta|V\rangle, \tag{2.3}$$

where $|H\rangle$ ($|V\rangle$) represents a single photon with horizontal (vertical) polarization. In this case, if we measure it using a polarising beam splitter followed by single photon detectors, the state would collapse either to H or V depending on which detector clicks, as shown in Fig 2.3. In the particular case of a diagonal

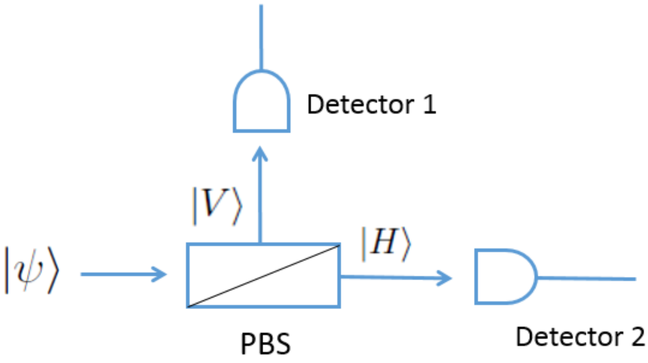

Figure 2.3: The quantum state $|\psi\rangle$ would collapse either to $|H\rangle$ or $|V\rangle$ depending to which detector clicks.

polarization (+45 or -45),

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle), \tag{2.4}$$

it is equally likely to get $|H\rangle$ or $|V\rangle$ in the above measurement.

The measurement principle plays a fundamental role in quantum cryptography. It states that, if a measurement is carried out at the quantum level, it can change the state of the observed particle in an irreversible way. For instance, in the case of the state in (2.4), the result of H-V measurement does not reveal the initial state. In QKD, after performing the measurement by Bob, the quantum states sent by Alice will be converted to classical bits after the distillation process. Such bits can then be used for secure communication and authentication tasks.

2.2.3 Uncertainty principle

Uncertainty principle, also called Heisenberg's uncertainty principle, states that there is an uncertainty relation between two observables such as position and momentum. It means that if one of the observables is measured, the measurement outcome of the second observable would be affected. The product of uncertainties of two observables, such as the position and momentum, can always be at a certain limit: $\Delta x \Delta y \geqslant \frac{\hbar}{2}$. In QKD, particularly in CV-QKD, this principle is essential in ensuring the security, since Eve cannot precisely measure both quadratures, $\hat{X}, \hat{P}$, simultaneously.

2.2.4 Entanglement

Entanglement is an interesting feature in quantum mechanics where particles can be correlated in some way that yields correlation between their measurement outcomes. This remarkable property was exploited by Ekert to introduce E91 protocol Ekert [1991]. Assume that, we have two single photons, labelled 1 and 2 , and they are in the following state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2]. \tag{2.5}$$

In (2.5), if we measure the polarization of the first photon, the result would be H or V. Suppose that the result is horizontal; then the collapsed state of the system would be:

$$|\psi\rangle = |H\rangle_1|H\rangle_2. \tag{2.6}$$

Even though we measure just the first photon, the second photon will have the same state in this case, so we say that the two photons are entangled, in which a measurement on one affects the other. A nonlinear optical material is used to generate entangled photons using the process of spontaneous Parametric Down Conversion (SPDC).

2.3 QKD key ideas

The basic structure of a QKD system is generally similar to an optical communication system, which means that it needs a light source, such as a laser diode, an optical channel, and a photodetector at the receiver. Yet with QKD, since we deal primarily with single photons, this would often necessitate a single photon source and a single-photon detector. In DV-QKD systems, single-photon detectors are necessary in comparison with CV-QKD. In the following, a brief description is provided about QKD source, QKD receiver, and the channel types in QKD. In addition, we define quantum bit error rate (QBER) and the role of Eve.

2.3.1 QKD source

Ideally, it is assumed that QKD source would emit single photons, however, the actual source in real-life QKD is the highly attenuated laser. Such an imperfect single photon source produces weak coherent states. In quantum mechanics, quantum harmonic oscillator has a specific state, called coherent state. This state resembles a classical light field, as it has relatively well-defined amplitude and phase with minimum fluctuations. Coherent states follow a Poisson photon number distribution:

$$p(n) = \frac{\mu^n}{n!} e^{-\mu}, \tag{2.7}$$

where μ is the mean number of photons in a time period τ. For instance, if μ=0.5, the probability of detecting a single photon, $p(n = 1)$, in a pulse with width τ, is 0.3.

2.3.2 QKD receiver

A single-photon detector at the QKD receiver is required in DV-QKD, whereas in CV-QKD an ordinary photodetctor is used. This is because the detection in CV-QKD is based on measuring the field quadratures, $\hat{X}$ and $\hat{P}$, using homodyne or heterodyne receivers, rather than measuring the quantized intensity in DV-QKD.

In single-photon detectors, the background noise has an adverse impact on the system performance, as it increases the error probability. One source of background noise is detector's dark current, whereby the detector tends to click despite the absence of light. The dark count rate (γ_{dc}), which is an intrinsic property of the detector, varies from one detector to another. For instance, it ranges from (100-1000)/s for an APD, to (1-100)/s for superconducting detectors Dusek *et al.* [2006]. The average dark count n_D over a period τ is: $\gamma_{dc}.\tau$.

While DV-QKD requires single-photon detectors, CV-QKD protocols are compatible with standard telecommunication technologies for coherent optical communications, namely, that of homodyne and heterodyne receivers Diamanti & Leverrier [2015]. CV-QKD has also, in certain regimes, the possible advantage of being more resilient to the background noise induced in WDM networks than DV-QKD Qi *et al.* [2010a]. This is due to the intrinsic filtration of photons that

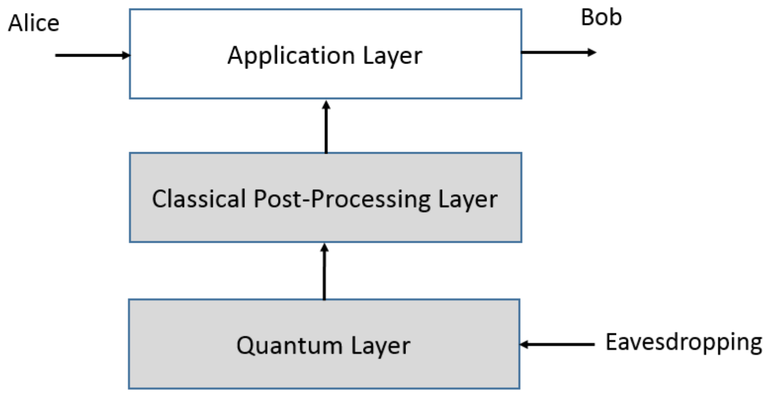

Figure 2.4: In QKD, an insecure quantum channel for exchanging quntum states and an authenticated classical channel for achieving error correction and privacy amplification. Eve attacks the quantum layer Imre & Gyongyosi [2012].

do not match the spatio-temporal and polarization mode of the local oscillator (LO) in homodyne receivers Kumar *et al.* [2014].

2.3.3 QKD channel

QKD is carried out over an insecure quantum channel and an authenticated classical channel; see Fig 2.4. The former could be free space or an optical fiber, in order to exchange quantum states, such as polarized single photons. The latter channel, which could be a telephone line, the internet, or any other classical channels, is employed for post processing steps. After such steps, we ensure achieving perfectly secret key at the expense of shortening the key rate. In Fig 2.4, Eve, the eavesdropper, tries to gain information about the key. In general, the channel distance in QKD is limited due to the loss, as the carriers are single photons, which have a low chance to survive over long distances.

2.3.4 Quantum bit error rate (QBER)

In QKD protocols, particularly in discrete variable QKD (DV-QKD), QBER refers to the error probability in the remaining keys distributed between Alice and Bob through a quantum channel. The remaining bits, which called the sifted keys, are resulted after reconciling the used bases between the two parties, and discarding the lost photons. QBER is a crucial quantity, since it allows both parties to decide whether to continue further to the post processing step or to abort the protocol in case Eve has gained more information about the key than Bob. QBER represents the discrepancy between the sifted keys and is given by:

$$QBER = \frac{false\ counts}{total\ counts}, \tag{2.8}$$

where $total\ counts$ is the total number of sifted key bits, and $false\ counts$ is the number of incorrect sifted key bits between Alice and Bob. The presence of Eve in DV-QKD schemes can typically be discovered if the QBER exceed a certain limit. In CV-QKD, however, channel loss and excess noise are essential quantities to characterise the quantum channel in this context.

2.3.5 Eve's role

Eve has an adversary role, in which she attempts to interfere and gain information about the key throughout the process of key generation. She is assumed to have unlimited computational power only bound by quantum mechanical laws, which gives her the ability to intercept the quantum channel. In order to clarify how Eve intercepts the link between Alice and Bob, we explain the intercept and resend attack. Suppose that Alice sends a horizontally polarized photon and Bob employs a linear basis (H/V) for measurement. As for Eve, she would use either a rectilinear or a diagonal basis to make the measurements. Whatever she measures, she will resend to Bob. If Eve utilizes a linear polarizer, she would obtain an exact result as Bob, in which case, Bob cannot realize her presence. On the other hand, if Eve measures using the diagonal basis, there would be 50% chance to get $|+45\rangle$ or $|-45\rangle$ state. Accordingly, Bob would get an equally likely outcome of a horizontal or a vertical polarization. Therefore, the average error rate over the link is 25% Dusek *et al.* [2006].

If Alice and Bob observe such a high amount of error, they should abort the protocol and start over. Since it is not possible for Eve to attack the quantum channel and distinguish between non-orthogonal states without perturbing the channel, the security of QKD system is guaranteed. In addition to the above attack, there are other types of attacks that Eve can perform. These include

(a) probing attacks, where Eve can collect information from both parties, Alice and Bob, by attacking equipment directly. In particular, using a probe, she can emit light into receiver/transmitter boxes and collect back the reflected signal; (b) Side-channel attacks, in which case, Eve can collect the leaked information from devices Jain *et al.* [2016].

2.4 Discrete variable QKD (DV-QKD)

In DV-QKD protocols, discrete degrees of freedom of optical signals are exploited to encode each bit of secret information. One fundamental QKD protocols that uses such an encoding is the BB84 protocol, in which the polarization of single photons is used to generate a secret key between two intended parties. In the following, we first introduce the standard BB84 protocol, as it shows generally how QKD protocols work. Then, we present other important DV-QKD protocols considered in our analysis, namely, decoy-state BB84, reference frame independent quantum key distribution (RFI-QKD), and measurement-device-independent quantum key distribution (MDI-QKD).

2.4.1 The standard BB84 protocol

In 1984, Bennett and Brassard invented BB84, which is the first QKD protocol Bennett [1984]. Later, within a few years, a practical demonstration was conducted at IBM, yet the transmission distance was only 32 cm Bennett *et al.* [1992a]. In the standard BB84 protocol, the polarization of single photons is used to generate a secret key between two intended parties. The protocol, see Fig. 2.6, is illustrated in the following steps:

Raw key generation

Firstly, Alice creates a random a sequence of bits, each of which is encoded in the so-called Z-basis (H, V polarisation) or, the X-basis (+45°, −45° polarisation); see Fig. 2.5. The encoding basis is changed randomly during qubit transmission. She transmits the polarized photons or qubits over a quantum channel to the recipient. On the reception side, Bob selects randomly one of the two bases to

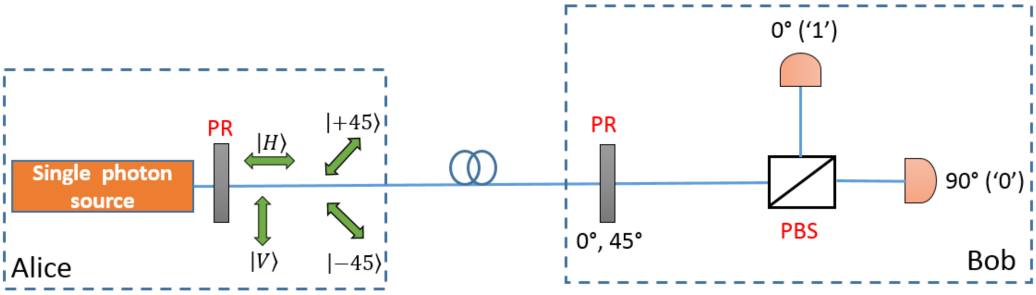

Figure 2.5: A schematic view of polarisation encoding in BB84 protocol. PR: Polarization Rotator.PBS: Polarizing Beamsplitter.

measure and record the corresponding binary string of bits Dusek *et al.* [2006]. He uses single photon detectors in order to convert the received pulses into electronic ones for the next classical processing step.

Sifted key

If the two bases are chosen equally likely, there is a 50% probability that the bases chosen by Alice and Bob will be nonidentical. Therefore 50% of the key bits would be discarded due to basis mismatching. In addition, some photons might have not reached the receiver. The remaining sequence of bits constitute the sifted key.

Error correction

The post processing step consists of error correction and privacy Amplification. Such steps would result in distilling a secure key provided that the quantum noise has not exceeded a specific limit. In order to obtain an identical secure key between Alice and Bob, we need to carry out an error correction process to get rid of any errors due to the noise in the quantum channel and/or because of Eve's intrusion. Alice and Bob reveal a chosen subset of n bits from the sifted key and/or perform parity comparisons to estimate the amount of errors. In some cases, if the error exceeds a certain threshold, they would decide to abort the protocol and start a new session; otherwise they carry on with the error-correction

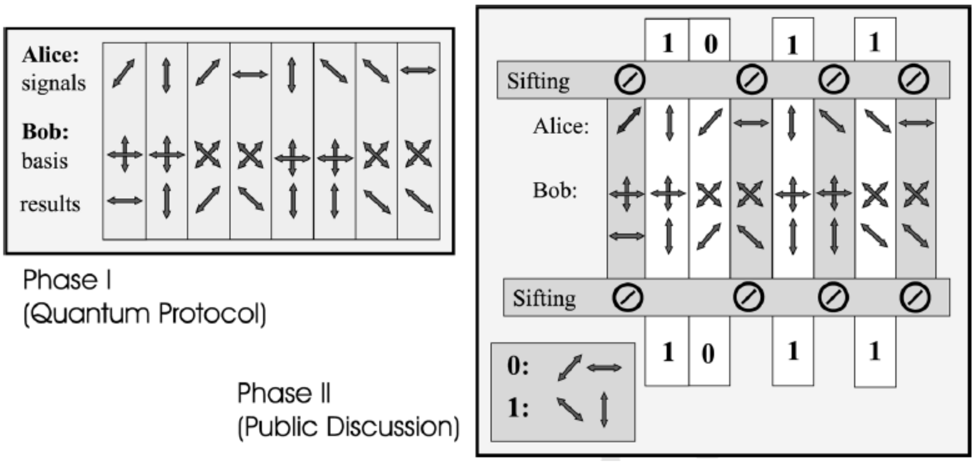

Figure 2.6: The two phases of the BB84 protocol Lütkenhaus [2007].

procedure until obtaining an identical sequence of bits on both sides Bhandari [2014].

Privacy amplification

Even though the objective of error correction is to obtain an identical stream of bits between Alice and Bob, privacy amplification is needed to prevent any possibility for Eve to gain any information about the key. In general, privacy amplification is performed by using appropriate hashing functions, in which the input stream will be shortened according to a proper factor Lütkenhaus [2007].

2.4.2 The decoy-state BB84 protocol

In the ideal scenario of the BB84 protocol Bennett [1984], explained in 2.4.1, it is assumed that Alice, the sender, uses a single-photon source. However, this is not necessarily the case in practice. The actual alternative source is a highly attenuated laser that produces weak coherent states, as mentioned previously. The problem with using such sources is the possibility of experiencing the photon-number-splitting (PNS) attack Brassard *et al.* [2000] as each pulse might contain more than one photon. That is, Eve can siphon a photon and forward the rest to Bob. Later, after public announcement of the bases by Alice and Bob, Eve can measure exactly the state of the photon without revealing her presence. The decoy-state (DS) technique Ma *et al.* [2005], which was proposed first by Hwang Hwang [2003], beats this kind of attack. The idea is to use several different light intensities, instead of one, so that any attempts by Eve to intrude on the link is more likely to be detected. This helps to gather more information from the quantum channel in order to discover the presence of Eve. The security analysis of PNS loophole due to device imperfections in real-life QKD, was originally considered by Gottesman-Lo-Lütkenhaus-Preskill (GLLP) Gottesman *et al.* [2004]. However, the obtained key rate and secure transmission distance are limited Ma [2006]. The decoy-state method Ma *et al.* [2005] was proposed to tackle effectively the limitations in GLLP analysis. Decoy-state QKD can accomplish a higher key generation rate, in comparison with non-decoy protocols, in addition of improving the transmission distances Ma [2008], Ma *et al.* [2005].

In the decoy-state technique the transmission of both signal and decoy states between Alice and Bob would help to estimate the quantum channel parameters. The signal states are used to generate the secret keys, while the objective of the decoy signals is to characterize the quantum channel Zhang *et al.* [2017b]. Roughly speaking, as compared to the signal pulses, decoy pulses often have a lower multi-photon component, due to having a lower average number of photon per pulse as compared to the signal pulses. In this case, if Eve launches the PNS attack, Bob would receive a different portion of decoy pulses than signal pulses. As a result, if Alice and Bob examine separately both the decoy and signal pulses, the attack can be detected.

The issue of eavesdropping is a matter of whether we can detect Eve or not. If Eve uses PNS attacks, the estimated value of the error rate in single-photon states, e_1, and QBER, could be so high that no secret key can be generated. The important thing about decoy states is that they enable us to accurately estimate the single-photon gain, Q_1, and e_1. If we use only one intensity, we cannot properly estimate these parameters, but with multiple decoy states, we can better estimate their values. Knowing e_1 and Q_1 becomes important at the privacy amplification stage, as it turns out that we can get a secure key only from those key bits that have been generated from single photon components at the source.

In our key-rate analysis, we use the efficient version of DS-BB84 Lo *et al.* [2005], where Z basis is chosen more frequently than the X basis. We also assume that time-bin encoding is in use. In such an encoding approach, time slot implementations are used; see Fig 2.1. The information is encoded in the relative phase of the two time slots. The modes can then be defined corresponding to the two time slots, t_1 and t_2. After the unbalanced interferometer, the qubit state can then be written as Diamanti [2006]:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\mathrm{t}_1\rangle + e^{i\alpha} \, |\mathrm{t}_2\rangle\right). \tag{2.9}$$

In Fig. 2.1, at Bob receiver's, the two pulses would interfere with each other at t_2, which is the detection timeslot. By changing the phase shift ϕ, the measurement can be performed in any desired basis. The results will be identified according to which detector has clicked. In this encoding, the Z basis is spanned by the single-photon states corresponding to each time-bin, whereas the X eigenbases are the superposition of such states. In Appendix A, the lower bound for the key generation rate in the limit of an infinitely long key Ma *et al.* [2005], is explained.

2.4.3 The reference frame independent-quantum key distribution (RFI-QKD) protocol

In most QKD schemes, two remote users have to share a reference frame to align their used bases Liang *et al.* [2014]. This alignment is performed actively over a classical channel Sheridan *et al.* [2010]. For instance, QKD systems that use polarization encoding techniques must maintain the alignment of polarized states between Alice and Bob. Such an indispensable alignment would require extra cost and time to be performed Liang *et al.* [2014]. RFI-QKD protocol was proposed by Laing et al Laing *et al.* [2010a] to break such a restriction. The idea of RFI-QKD was originally about how to maintain the state of linearly polarized qubits that sent by mobile devices equipped with QKD Wabnig *et al.* [2013]. In RFI-QKD protocol, two users employ three bases for qubits encoding. In this case, only one basis should be well-aligned between users for secret key generation, while the other two bases are used for channel characterization Laing *et al.* [2010a].

There are another proposed ideas to address the issue of reference frame misalignment. For example, qubits can be encoded within larger systems, in which many entangled photons are necessitated Bartlett *et al.* [2003], Zhang *et al.* [2014]. However, this poses a technical challenge in terms of generation, manipulation, and detection Zhang *et al.* [2014]. Another alternative solution is by utilizing spatial modes of light for encoding information Spedalieri [2006]. This may be functional through wireless communication, but due to mode dispersion, transmitted modes would be affected when sent over fiber Zhang *et al.* [2014]. Plug-and-play system is another possibility, such a system is used to compensate the polarization deviation. This is performed by sending the received light pulse in backward and forward directions over the same fiber. This is achieved by using Faraday mirror in order to to cancel out the birefringence Muller *et al.* [1997], Zhang *et al.* [2014]. A downside to this system is the possibility that error rate is increased due to Rayleigh backscattering Zhang *et al.* [2014].

RFI-QKD protocol, in particular, is practical in cases where the alignment of reference frames between remote parties is not observed and may vary in time Laing *et al.* [2010a]. In this protocol, Bob receives a qubit that prepared in an eigenstate of three orthogonal bases X, Y, and Z, which chosen randomly by Alice Laing *et al.* [2010a]Sheridan *et al.* [2010]. Z basis is supposed to be well aligned, i.e., $Z_A = Z_B$, for acquiring the raw key. X and Y bases, in contrast, are used to bound Eve's information assuming that they vary slowly with time so that they can be assumed fixed for one round of QKD operation Zhang *et al.* [2014]. After the measurement outcomes are announced over a public channel, Alice and Bob follow the typical sifting and post processing procedures to come up with a shared secret key. The estimated key generation rate for RFI-QKD with decoy-state technique is given in Appendix B. We assume that the efficient version of DS-BB84 is in use.

2.4.4 The measurement device independent-quantum key distribution (MDI-QKD) protocol

QKD schemes are not perfect in practice, and this would encourage Eve to do some interception activities. In practical QKD systems, even without launching any attacks on the quantum channel or the users' devices, Eve can still obtain information about the key by exploiting the leaked information from Alice and Bob devices Jain *et al.* [2016]. As a result, neither user would be able to discover the presence of Eve. Such a scenario is called side-channel attack Jaina *et al.* [2015]. Device-independent QKD (DI-QKD) Mayers & Yao [1998] was proposed as a solution to such a loophole of security. With certain assumptions, the devices of Alice and Bob are described as "black boxes", which means that neither parties require to know the way their devices work Xu *et al.* [2015]. One possible downside of DI-QKD is , however, its low key generation rate on the order of 10^{-10} over practical distances Curty & Moroder [2011], Gisin *et al.* [2010], Xu *et al.* [2015]. Interestingly, the MDI-QKD protocol Lo *et al.* [2012] provides an alternative solution to remove all detector side-channel attacks. This protocol can enhance the performance in comparison with DI-QKD. In MDI-QKD, the measurement is performed by a third party, Charlie, who is not necessarily trusted. In such a protocol, Charlie performs a Bell-state measurement (BSM) on Alice and Bob's signals. The security of MDI-QKD protocol is based on the reverse-EPR protocol Biham *et al.* [1996].

In the original MDI-QKD protocol Lo *et al.* [2012], in each QKD transmitter at Alice and Bob, weak coherent pulses (WCPs) are randomly encoded to different BB84 polarization states by using a polarization modulator. Decoy states generated by an intensity modulator and signals are then sent by both parties to the QKD receiver, where BSM module is located; see Fig. 2.7. This essential module consists of a 50:50 beam splitter (BS), where the signals from Alice and Bob are interfered. BS is followed by a polarizing beam splitter (PBS) in order to project the incoming photons into a horizontal (H) or a vertical (V) polarizations states Lo *et al.* [2012].

In our study, however, we assume that both users have a DS-BB84 time-bin encoder Ma & Razavi [2012], Ma *et al.* [2012b]. We also again assume that the efficient version of DS-BB84 is in use. After Charlie announces the measurement outcomes of the successful events over a public channel, Alice and Bob follow the typical sifting and post processing procedures to come up with a shared secret key.

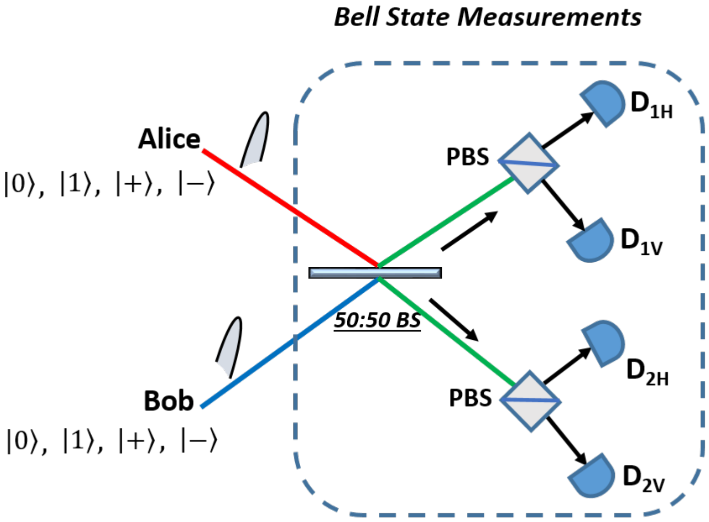

Figure 2.7: a Bell-state measurement (BSM) on Alice and Bob's signals.

2.5 Continuous variable QKD (CV-QKD): GG02 protocol

Amplitude and phase quadratures of the electric field, $\hat{X}$ and $\hat{P}$, are noncommuting variables used for encoding in CV-QKD. These quadratures describe the real and imaginary parts of the complex amplitude, $\hat{a}$, and they are given by: $\hat{X} = \frac{1}{\sqrt{2}}(\hat{a}^{\dagger} + \hat{a})$, and $\hat{P} = \frac{1}{\sqrt{2}}(\hat{a}^{\dagger} - \hat{a})$. In CV-QKD, Alice encodes the bits to be distributed by specifying such quadrature amplitudes in a coherent state. At the receiver, Bob would measure one of the quadratures, or both, using coherent receivers, such as homodyne or heterodyne. CV-QKD, as mentioned previously, is more tolerable to the background noise induced in WDM networks than DV-QKD due to the mode selectivity of the local oscillator (LO) in homodyne receivers. However, for secure communication, CV-QKD may only be practical for short distances in comparison with DV-QKD Jouguet *et al.* [2013], Lodewyck *et al.* [2007]. This is because of the excess noise and loss in the optical channels, as well as the limited efficiency of the classical reconciliation Madsen *et al.* [2012]. In our analysis, we consider GG02 as a CV-QKD protocol, in order to draw a clear comparison with DV-QKD protocols.

The GG02 protocol is introduced by Grosshans and Grangier Grosshans & Grangier [2002]. It is the counterpart of the BB84 protocol in the CV prepare and measure schemes. In contrast to BB84, which relies on discrete variables, such as the polarization of single photons, GG02 exploits the quadratures of coherent states for encoding the information. In GG02, two random numbers, X_A and P_A are drawn by Alice according to two independent zero-mean Gaussian distributions with variance V_A, in shot noise unit. The coherent state $|X_A + \mathrm{i}P_A\rangle$ is then prepared, using amplitude and phase modulators, by Alice and sent to Bob, who randomly measures one of the two quadratures. After this stage both users acquire correlated random data. The error reconciliation and the privacy amplification are then performed in order to obtain the final secure key Grosshans & Grangier [2002]. We assume here that reverse reconciliation Grosshans *et al.* [2003] is in use.

2.6 Summary

An overview of the key ideas in QKD was presented, starting from the fundamental concepts in quantum mechanics, through to the basic QKD protocols. This includes a description of the encoding techniques in QKD, namely, DV-QKD and CV-QKD. In the following chapter, we review optical wireless communications, in which channel modelling and link configurations are described.

Chapter 3

Optical wireless communications

3.1 Introduction

The advantages of wireless technologies are not restricted to mobility and flexibility for users' terminals. Users can also gain noticeable reductions in cost and time in many applications Ramirez-Iniguez *et al.* [2008]. With respect to optical wireless communications (OWC), since Gfeller and Bapst proposed this significant technology in 1979, its implementations have spread to become available in homes and offices, starting from TV remote controls all the way to the modern personal devices Qazi [2006]. Although infrared is commonly used for indoor wireless communications, other transmission bands like visible spectrum can also be utilized. This is why the technology is generally called wireless optical communications" rather than wireless infrared communications Carruthers [2003]. Indoor OWC has had great development recently, especially in the visible light regime communications where lighting sources, for example LEDs, can be exploited for data transmission; nevertheless, infrared applications are still the predominant choice.

Due to its remarkable properties such as high bandwidth, unlicensed spectrum, low cost, easy implementation, and being free of interference, OWC is becoming an interesting alternative means to the radio frequency (RF) for short ranges Ghassemlooy *et al.* [2012]. In fact, radio and infrared are considered complementary to each other instead of being presented as competitive carriers, which can be clearly seen in the availability of bandwidth Ghassemlooy & Hayes [2003].

Ambient noise and multipath dispersion are the major causes for degrading the signal quality in indoor environments, consequently limiting the high data rates. This implies that, a system design is a key point especially in terms of selecting an appropriate link configuration and a modulation technique, in addition to using a suitable light source and a photodetector. QKD is expected to be a good choice in terms of data security for indoor optical wireless communications. This combination of classical and quantum systems has not been studied yet, and clearly, the feasibility of the implementation would be a great challenge due to the ambient noise in indoor environment.

In the following, we first describe OWC channels in terms of time and frequency responses. Next, the categories of OWC links are explained based on the degree of directionality and the propagation method between the sender and the recipient. Finally, channel modelling in OWC and background are presented.

3.2 Indoor optical wireless channels

The structure of optical wireless communication schemes is generally similar to an optical communication system. It consists of an optical emitter, free space or air as the channel, and an optical receiver. Light emitting diodes (LEDs) or laser diodes (LDs) are typically used as light sources, by which the electrical signal is converted into an optical signal, and then lenses are used for beam focusing through the medium. At the receiving side, the electrical signal is retrieved back by a photodiode (PIN or APD), after being filtered and concentrated Elgala *et al.* [2011]. It is preferable to employ wavelengths in the range of 780-950 nm, because of the availability of cheap optoelectronic components within those bands Ma [2008].

In practice, Intensity Modulation/Direct Detection (IM/DD) is the main transmission approach for all indoor applications. While in RF communication schemes, the three quantities of a carrier, i.e., the amplitude, frequency, and phase, are modulated to convey information, in optical schemes, the intensity of an optical carrier is commonly modulated Ghassemlooy & Hayes [2003].

The intensity of the optical power, $x(t)$, is modulated by altering the drive current, then at the receiver, a photocurrent, $y(t)$, is resulted, which is classically

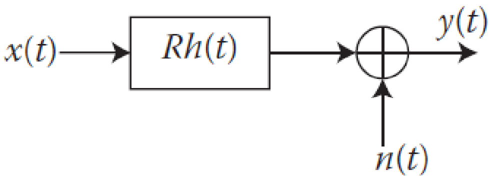

Figure 3.1: Baseband model of OWC channels.

proportional to the instantaneous optical power that strikes the photodetector. The usable frequencies' range for most indoor optical wireless schemes extends from DC to tens of MHz. For this reason, a baseband model is used to represent the system; see. Fig. 3.1.

In Fig. 3.1, $y(t)$ represents the output photoelectric current and is given by:

$$y(t) = Rx(t) \otimes h(t) + n(t) = \int_{-\infty}^{\infty} Rx(\tau)h(t-\tau)dt + n(t), \tag{3.1}$$

where $x(t) \geq 0$ is the instantaneous optical power at T_{x}, $\otimes :$ convolution, R is the photodetector responsivity (A/W), $h(t)$ is baseband channel impulse response, and $n(t)$ is the background shot noise Ghassemlooy *et al.* [2012].

In (3.1), $h(t)$ is used to demonstrate the impact of multipath dispersion in indoor OWC channel, as shown in Fig. 3.2. The frequency response of the channel is given by:

$$H(f) = \int_{-\infty}^{\infty} h(t)e^{-2j\pi ft}dt. \tag{3.2}$$

Infrared channels has a quite flat frequency response near DC, and so channel DC gain or $H(0)$ is really helpful to describe the channel Kahn & Barry [1997]. The DC gain determines the portion of the transmitted power that will be detected at the receiver. By substituting $f = 0$ in (3.2), we end up with:

$$H(0) = \int_{-\infty}^{\infty} h(t)dt. \tag{3.3}$$

3.3 Optical link categories

In OWC, a link can be generally classified based on two criteria, firstly, the degree of directionality between the transmitter and the receiver, and, secondly, whether the propagation is in line of sight (LOS) or non-LOS.

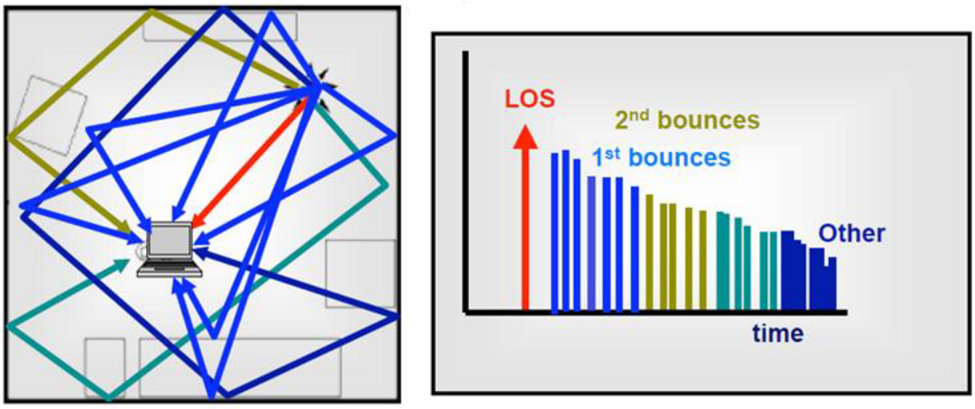

Figure 3.2: Ray representation and impulse response $h(t)$ for multipath propagation.

3.3.1 First criterion: directionality

With respect to the directionality, by employing a directed transmitter and receiver, a link is established with benefits of superior power efficiency and lower levels in multipath dispersion and path loss. However, it suffers from the existence of shadowing, and the limitation in the average transmitted power due to eye safety concerns. Alternatively, if the beam angle and field of view (FOV) of the transmitter and receiver respectively were wider, there would be a non-directed link providing the feature of terminals' mobility. Moreover, a hybrid configuration can be accomplished by combining different degrees of directionality between transmitters and receivers Kahn & Barry [1997].

3.3.2 Second criterion: line of sight

In LOS links, it is essential to maintain an aligned path between the sender and recipient for data exchange with higher power efficiency, whereas in non-LOS, the receiver depends on the reflected light from the roof, walls, or other reflective surfaces. For non-LOS, like diffuse links, the link's robustness is increased and the convenience of use is enhanced. In this case, the operation can continue, even with barriers between the sender and receiver Ghassemlooy *et al.* [2012]. However, this would not help in QKD operation, as we deal with single photons that necessitate maintaining a LOS link to be distributed between two parties without being absorbed or lost.

3.4 Channel modelling in OWC

Mathematical models are used to approximate the behaviour of different OWC channels where many variables are taken into account to estimate channels' DC-gains, and accordingly to calculate the received average power. Here, we review how the DC for a directed LOS channel is derived using the Lambertian model.

3.4.1 Directed LOS

A directed topology tends to provide maximum efficacy at the expense of mobility restrictions. Now, the Lambertian model offers an interesting approach for $H(0)$ $(=H_{DC})$ calculation. For the line-of-sight link between the transmitter and receiver, the DC-gain is given by Kahn & Barry [1997]:

$$H_{\mathrm{DC}} = \begin{cases} \frac{A(m+1)}{2\pi d^2} \cos(\phi)^m T_s(\psi) g(\psi) \cos(\psi), & 0 \leq \psi \leq \Psi_c, \\ 0 & \text{elsewhere}, \end{cases} \tag{3.4}$$

where d is the distance between the source and the receiver; ψ represents the incidence angle with reference to the receiver axis, while ϕ specifies the irradiance angle; see Fig. 3.3. These two parameters specify the relative location and orientation of the transmitter and receiver modules. $T_s(\psi)$ is the filter signal transmission; m and $g(\psi)$ are, respectively, the Lambert's mode number used to specify the directivity of the source beam and the concentrator gain, given by

$$m = \frac{-\ln 2}{\ln\Big(\cos\big(\Theta_{1/2}\big)\Big)} \tag{3.5}$$

and

$$g(\psi) = \begin{cases} \frac{n^2}{\sin^2(\Psi_c)}, & 0 \leq \psi \leq \Psi_c \\ 0 & \psi > \Psi_c \end{cases}, \tag{3.6}$$

where n is the refractive index of the concentrator, Ψ_c is the receiver's FOV, and $\Theta_{1/2}$ is the semi-angle at half power of the light source. We neglect here the reflected pulses from the walls, which will arrive at a later time.

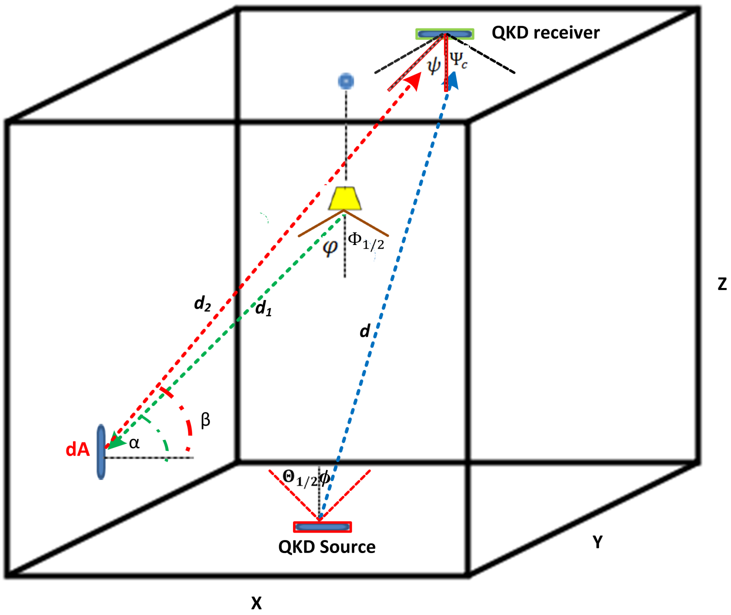

Figure 3.3: A wireless QKD link in an indoor setup. The transmitter is mobile, while the QKD receiver is fixed on the ceiling. For illustration purposes, the QKD receiver is depicted away from the centre. In practice, it should be optimally placed at the centre of the ceiling.

3.4.2 Non-directed LOS

In the case of non-directed LOS, see Fig. 3.3, the model would be slightly different, since the reflected paths are taken into account in calculation. The portion of this reflected light that may enter the receiver is estimated by calculating the DC-gain for the reflected beam, H_{Ref}, off a surface element of size dA, and is given by Gfeller & Bapst [1979] Ghassemlooy *et al.* [2012]:

$$H_{\mathrm{Ref}} = \begin{cases} \frac{A(m_1+1)}{2\pi^2 d_1^2 d_2^2}\cos(\varphi)^{m_1} r T_s(\psi) g(\psi) & \\ \times dA\cos(\alpha)\cos(\beta)\cos(\psi), & 0 \leq \psi \leq \Psi_c, \\ 0 & \text{elsewhere}, \end{cases} \tag{3.7}$$

where φ is the incidence angle with respect to the lighting source axis; d_1 and d_2 are, respectively, the distance from the lighting source to the surface element, and from there to the receiver; r is the reflection coefficient of the wall or the

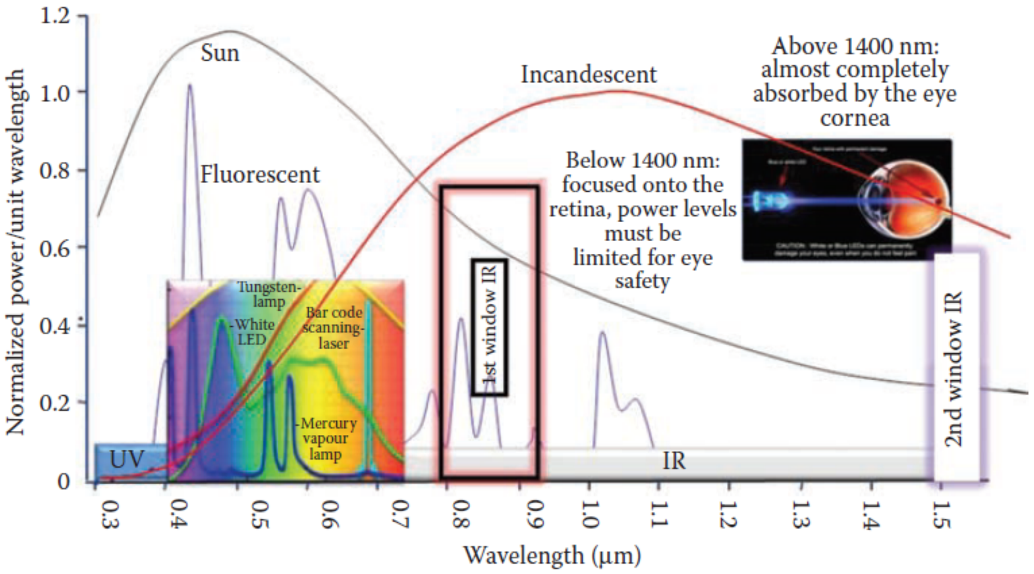

Figure 3.4: Optical power spectra of common ambient infrared sources Ghassemlooy *et al.* [2012].

floor; and m_1 is the Lambert's mode number, which is calculated from Eq. (3.5), but with semi-angle at half power of $\Phi_{1/2}$ for the lighting source (rather than $\Theta_{1/2}$). In order to calculate the collected power at the receiver, one then needs to integrate over the entire reflection area.

3.5 Background noise

The downside of indoor communications is the existence of severe ambient light. In essence, shot noise is induced in the photodiode by the irradiance of sunlight and artificial lamps. These sources radiate substantially in the band of low cost sources, which affects the scheme's performance. In addition, there is thermal noise in the receiver, which is modelled by the Boltzmann formula, and also dark current noise which varies between photodetectors, depending on the manufacturing technology Dusek *et al.* [2006]. Such noise would accordingly increase the error probability. In Fig. 3.4, ambient light that caused by the Sun and an incandescent lamp emit continuously over a wide range of wavelengths. In contrast, some common artificial sources send out a radiation mostly within the visible spectrum, which may extend to the first window of IR. With reference to eye safety, a careful attention should be given to the employed power level when employing wavelengths below 1400 nm; see Fig. 3.4. To reduce the effects of ambient light, it is important to realize higher SNR values at the receiver.

3.6 Summary

In this chapter, a short description of OWC is provided. This includes OWC channel descriptions, links categories, channel modelling in OWC, and background noise. The latter poses a challenge for QKD, however, as the transmitted power is limited to about that of a single photon per pulse. It would be interesting to see if we can operate QKD in indoor environments despite the high background noise in such channels as we describe in the following chapter.

Chapter 4

The feasibility of wireless QKD in indoor environments

4.1 Introduction

Nowadays, there is an increasing demand for data security in numerous aspects of data exchange. Users are tending to use their personal devices to connect wirelessly to obtain many services. Remote access from offices or residential places to services such as mobile banking requires a high level of security. This issue worries people about their information security, since data security has been compromised in many cases. QKD can provide a revolutionary cryptographic technique with the aim of achieving security in data transmission. QKD effectively use quantum mechanics to provide a secret method for distributing random keys between two remote users over an optical channel. Here, we aim to fascilitate the access part of hybrid quantum-classical networks by enabling users to exchange both quantum and classical signals from indoor environments. This is accomplished by adopting a regime of operation in which wireless indoor QKD is feasible.

In the following, we first describe the system of wireless QKD in indoor environments. This is followed by a preliminary step towards the feasibility assessment, which is evaluating the level of background noise and loss in such environments. A proper key rate analysis is explained next. This is to estimate the achievable key rate in different cases where the QKD source is perfect or with known/unknown flaws. Finally, the numerical results and summary are presented.

4.2 System Description

In this section, we describe the setup and the components used in our wireless QKD system. Here we consider a particular scenario in which we have an empty window-less room of $X \times Y \times Z$ dimensions, which has been illuminated by an artificial source of light; see Fig. 3.3. While this may not be exactly the case in a practical scenario, this particular setting allows us to properly study the resilience of the system to background noise. More realistic cases can also be investigated by properly adjusting the lighting source characteristics. The lighting source is assumed to be a Lambertian one with a semi-angle at half power of $\Phi_{1/2}$ located at the centre of the ceiling. The contribution of the light source is calculated via its power spectral density (PSD), denoted by S, at the operating wavelength of the QKD link, denoted by λ.

We assume that the QKD link is composed of two components. The QKD receiver, or Bob's box, is fixed and located at the centre of the ceiling, while the QKD transmitter, or Alice's device, can be anywhere on the floor with a semi-angle at half power of $\Theta_{1/2}$. With regards to the QKD receiver and the artificial light source, we assume that the QKD receiver would just receive the reflected light from the walls and the floor and no light would enter the receiver directly from the bulb. This is achievable in practice by using certain reflectors that confine the radiation of the light source toward the floor. For simplicity, however, we assume that the lamp position is at the same level of the ceiling as the QKD receiver, and that the path between QKD transmitter and receiver is not blocked. We also implicitly assume that the QKD source shines light in an upward direction toward the ceiling. This requires a minimal alignment, which can be done by the users the same way that a mobile user may avoid being in a deep fading point when using their mobile phones or given by instructions given on the screen. If the light beams used are not too narrow, then the total performance is expected to be tolerant of some movements. If they are narrow, however, then active beam steering would be required. We will see what range of beam angles we can use in our numerical results section. We assume that the QKD receiver has a detection area A and an optical filter bandwidth $\Delta\lambda$. The unwanted light is filtered out best if the filter's bandwidth matches $1/T$, where T is the width of the transmitted pulses by the QKD user.

We assume that the decoy-state variation of the BB84 protocol is in use Ma *et al.* [2005]. The key advantage of the decoy-state protocol is in allowing us to use weak laser pulses, instead of ideal single photon sources, at the source. This, while being immune to potential photon-number splitting (PNS) attacks Brassard *et al.* [2000], offers a practical inexpensive solution for QKD encoders. We employ time-bin encoding Brendel *et al.* [1999], rather than polarization, to implement the BB84 protocol. In this scheme, the information is encoded onto the phase difference between two consecutive pulses, see Sec. 2.2.1. The possible advantage over polarization encoding is that we do not need to establish an identical polarization reference frame between a mobile device and the receiver. This can much simplify the alignment requirement and would allow us to use wider beams at the transmitter.

We consider three cases with regards to the QKD encoders. We first assume that the QKD encoding is carried out perfectly; that is, the phase difference between the two consecutive pulses is exactly as the protocol requires. We consider both cases of infinitely many and weak+vacuum Ma *et al.* [2005] decoy states in this scenario. We also consider the case of using imperfect encoders. In this scenario, we assume that the device can be either characterized, in the sense that the QKD source has known flaws Tamaki *et al.* [2014], or uncharacterized but has a fixed deviation from the ideal setting. In the latter case, we use RFI-QKD protocol (see Sec. 2.4.3) Laing *et al.* [2010b], which has also been used in recent demonstrations of polarization-encoded handheld QKD Chun *et al.* [2017], Duligall *et al.* [2006]. The difference here is that, in the latter experiments, we need to at least know the reference for one polarization axis. In time-bin encoding protocols, the equivalent requirement would be to have two distinct time bins known to the receiver. The latter requirement is expected to be easier to achieve in practice for users that carry and move their QKD encoders. In section 4.4, the secret key rate analysis for each case will be given.

We consider the regime of operation when the reflected pulses off the walls are not overlapping in time with the main direct signal. This happens when the transmitted pulses are short in comparison to the transmission delay. This is the case in the practical regime of operation when high rate communications is desired. In this case, we neglect to collect the reflected QKD signals off the walls. We also assume that none of these reflected pulses will interfere with the forthcoming QKD pulses. That would imply that the repetition rate of the QKD link must be on the order of 100 MHz or lower, which is suitable for our scheme.

Two scenarios are considered in this work. We first look at the case where the lighting source is turned off in which case, the background noise is assumed to be isotropic ambient light noise with a spectral irradiance denoted by p_n. The variation in the receiver's FOV in this case would affect the corresponding value of the channel transmittance of the QKD link. In the second scenario, we consider the effect of the artificial light source by accounting for the reflections from the walls and the floor, whose reflection coefficients are denoted by r_1 and r_2, respectively. The background noise at the QKD receiver, from the lighting source, will go up with increase in S, the power spectral density (PSD), while the loss in the channel would increase with the receiver FOV. The latter would determine how much mobility may be allowed. We therefore look at the trade-off between these two parameters in determining the secure versus insecure regimes of operations. Before doing that, in the following section, we first employ the propagation models in OWC for estimating path loss and background noise in the room.

4.3 Channel Characterization

Indoor environments can impose severe conditions for the operation of a QKD system, such as that in Fig. 3.3. This includes the issues of path loss, especially if a wide beam needs to be used, and the background noise, which also affects the performance of the scheme by increasing the error rate. In this section, we estimate the path loss and the background noise collected by the QKD receiver using established OWC models.

4.3.1 Path Loss Estimation

Due to path loss, the recipient, Bob, would receive a portion of the photons sent by the sender, Alice. As pointed out in Ch. 3, this is estimated by the channel DC-gain, denoted by H_{DC}, in OWC channels. The received power depends on the distance between the sender and the receiver, as well as the degree of directionality and the alignment. For the line-of-sight link between the QKD transmitter and receiver, the DC-gain is given by Eq. (3.4) Kahn & Barry [1997].

4.3.2 Background Noise Analysis

Two sources of background noise are accounted for in our analysis. Ambient light noise is considered first, which is due to black body radiation in the surrounding environment. The ambient light is assumed to be isotropic. The second source of background noise is the artificial lighting source in the room.

Let us first assume that the lighting source is off. The background noise in this case is due to isotropic ambient light. The received power for such isotropic ambient light is given by Kahn & Barry [1997]:

$$P_{\mathrm{n,isotropic}}(\lambda) = p_n(\lambda)\Delta\lambda T_s A n^2. \tag{4.1}$$

The average number of detected photons per mode for a pulse with duration τ is given by:

$$n_B^{(1)} = \frac{P_{\mathrm{n,isotropic}}(\lambda)\tau\eta_d/2}{hc/\lambda}, \tag{4.2}$$

where c is the speed of light in the vacuum, η_d is the single-photon detector efficiency, and h is Planck's constant.

Next, the background noise at the QKD receiver due to the lighting source is calculated. The light from the source can indirectly enter our QKD receiver via reflections off the walls and the floor. We obtain the amount of reflected power that may enter the QKD receiver by partitioning the floor and the walls into surface elements of area dA and then calculating the contribution from each of these elements at the QKD receiver. The walls and the floor are modelled as diffuse reflectors, and we use the model presented in Gfeller & Bapst [1979] to approximate the reflection pattern of the walls and the floor. Suppose the incident and reflected angles that the beams make with respect to the wall and the floor normal are α and β, respectively; see Fig. 3.3. The reflected beams would enter the QKD receiver if the receiving angle, ψ, with respect to the receiver normal, is less than Ψ_c. The portion of this reflected light that may enter the receiver is estimated by calculating the DC-gain for the reflected beam, H_{Ref}, as already computed in Eq. (3.7).

By integrating over the walls and the floor, the average number of detected photons, per detector, at the QKD receiver due to the lighting source is then given by:

$$n_B^{(2)} = \frac{S(\lambda)\Delta\lambda\tau\eta_d/2}{hc/\lambda} \int\int_{\text{walls,floor}} H_{\text{Ref}}. \tag{4.3}$$

Different sources of background noise have different spectral irradiance over different ranges of wavelength. The ambient light caused by the Sun or an incandescent lamp covers a wide range of wavelengths and could generate a large number of background photons within a pulse period. In contrast, some artificial light sources, such as white LED bulbs, transmit mostly within the visible spectrum, possibly extended to the first window of infrared. For QKD systems operating at 880 nm or 1550 nm of wavelengths, the latter can then be a more tolerable source of noise.

In order to accurately estimate the impact of white LED bulbs, we measured the irradiance of two randomly selected white LED bulbs, with an equivalent brightness to a 60-W incandescent lamp. The measurements were conducted by Photometric and Optical Testing Services. Spectral irradiance measurements have been done at a distance of 50 cm from the centre of each bulb, from which the bulb's PSD has been calculated; see Fig. 4.1. The latter is measured to be on the order of 10^{-5} (W/nm) at 880 nm. In this case, for the parameter values in Table 4.1, the estimated value in Eq. (4.3), at FOV=20°, is equal to 1.8×10^{-5}. This is comparable to the dark count rate and it turns out, as will be shown later, that QKD operation can be feasible for such levels of external noise. The spectral irradiance for the sun is three orders of magnitude higher than that of the LED bulbs, hence the QKD system may only work under daylight exposure if the FOV is extremely narrow. In windowless room, however, The typical room-temperature black-body radiation from objects in the room is orders of magnitude

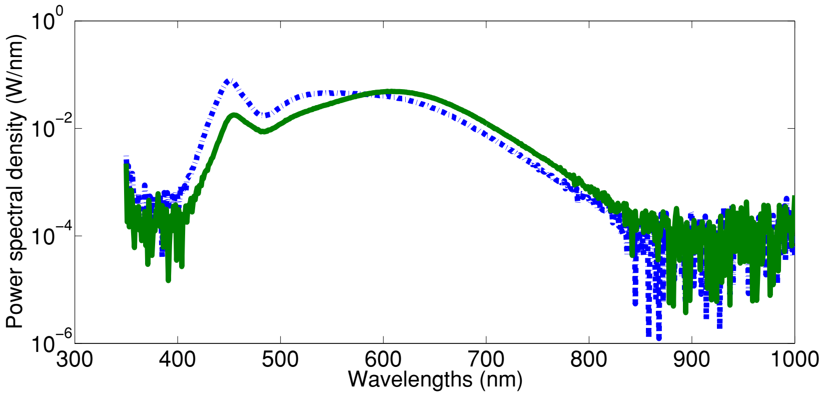

Figure 4.1: Power spectral density of two LED bulbs, equivalent to a 60-W incandescent lamp: A 650-lumen cool white LED manufactured by AURAGLOW (dashed), and a 805-lumen warm white LED bulb manufactured by INTEGRAL (solid). The wriggly form of the curves at the two far ends of the spectrum is due to the measurement precision.

weaker than that of LED bulbs and it is often negligible, as we show later in this chapter.

4.4 Secret-Key Rate Analysis

In this section, we present the rate analysis for our QKD system. The secret key generation rate, defined here as the probability of obtaining a secret key bit per transmitted quantum signal, is one of the key figures of merit for QKD systems. It will be affected by the amount of noise or eavesdropping activities, modeled by QBER of the system. The latter depends on the ambient noise and eavesdropping activities. QBER is defined as the probability of having non-identical bits in the sifted bits of Alice and Bob. In QKD protocols, if QBER is above a certain level, the protocol is aborted. In this section, we calculate the relevant key rate parameters for the three encoding techniques described in section 4.2, in the normal operating mode of the system, when there is no eavesdropper present.

4.4.1 Decoy-state BB84 with perfect encoders

Here, we assume that Alice uses a perfect encoder, where decoy-state BB84 protocol is in use. The decoy-state technique, as mentioned earlier in Sec. 2.4.2, was proposed to combat the PNS attack Brassard *et al.* [2000].

The secret key generation rate for the employed decoy-state protocol is lower bounded by Ma *et al.* [2005]

$$R \geq q\{-Q_\mu f h(E_\mu) + Q_1[1 - h(e_1)]\}, \tag{4.4}$$

where all new parameters are defined in Appendix A. If we use a two-decoy-state protocol, such as vacuum+weak, Y_1, Q_1, and e_1 can be bounded by the techniques presented in Ma *et al.* [2005], and explained in Appendix A.

4.4.2 Decoy-state QKD with known source flaws

We investigate here the case of using non-ideal QKD encoders, for which the extent of imperfection state preparation is assumed to be known. This concerns a user/manufacturer that have characterized the QKD devices. In order to obtain a fair comparison with other cases we consider, we assume that the quantum states in the Z basis, by which the secret keys are generated, are well aligned. In this basis, $|0\rangle_Z$ and $|1\rangle_Z$ represent single-photon states corresponding to the first and second time bin, respectively. For the sake of modeling the source flaws, however, we assume that the basis states in the X basis, $|0\rangle_X$ and $|1\rangle_X$, are, respectively, given by $\cos\left(\frac{\pi}{4} + \frac{\delta}{2}\right)|0\rangle_Z + \sin\left(\frac{\pi}{4} + \frac{\delta}{2}\right)|1\rangle_Z$ and $\cos\left(\frac{\pi}{4} + \frac{\delta}{2}\right)|0\rangle_Z - \sin\left(\frac{\pi}{4} + \frac{\delta}{2}\right)|1\rangle_Z$, where δ models the deviation from the ideal state. At $\delta = 0$, $|0\rangle_X$ and $|1\rangle_X$ describe two consecutive pulses with phase differences of 0° and 180°, respectively.

The asymptotic key rate in this case is given by Tamaki *et al.* [2014]

$$R = Q_1[1 - h(e_x^{(1)})] - Q_\mu f h(E_\mu), \tag{4.5}$$

where Q_1, Q_μ, and E_μ are the same as those given for the decoy-state BB84. The phase error rate $e_x^{(1)}$ is expressed in terms of the conditional probabilities as Tamaki *et al.* [2014]

$$e_x^{(1)} = \frac{Y_{1_X|0_X} + Y_{0_X|1_X}}{Y_{1_X|0_X} + Y_{0_X|1_X} + Y_{1_X|1_X} + Y_{0_X|0_X}}, \tag{4.6}$$

where, $Y_{s_X|j_X}$, for single-photon states, of our channel model is given by

$$\begin{aligned} Y_{s_X|j_X} &= \eta[P_{s_X|j_X}(1-n_N) + \frac{1}{2}n_N] \\ &\quad + (1-\eta)[n_N(1-n_N) + n_N^2/2], \end{aligned} \tag{4.7}$$

where $P_{0_X|0_X} = P_{1_X|1_X} = \frac{1}{2}[1 + \sin\left(\frac{\pi}{2}+\delta\right)]$ and $P_{0_X|1_X} = P_{1_X|0_X} = \frac{1}{2}[1 - \sin\left(\frac{\pi}{2}+\delta\right)]$.

4.4.3 Decoy state QKD with partially unknown source flaws

If the encoder imperfections are unknown, but fixed, we can use the RFI-QKD protocol Laing *et al.* [2010b], instead of BB84, with the decoy-state technique. This case corresponds to scenarios where the users cannot characterize their devices and/or the manufacturers have not specified the extent of possible imperfections in the encoders. In the RFI-QKD protocol, one basis, Z, is supposed to be known and identical to both users, while X and Y bases can be different. In our time-bin encoding, the Z basis is defined by each of the time-bin modes, whereas X and Y eigenstates are, respectively, given by superposition states $(|0\rangle_Z \pm |1\rangle_Z)/\sqrt{2}$ and $(|0\rangle_Z \pm i|1\rangle_Z)/\sqrt{2}$. We model the difference between the X (Y) operator on Alice side, X_A (Y_A), and that of Bob's side X_B (Y_B) by a rotation parameter ξ, which gives us the following:

$$X_B = \cos(\xi)X_A + \sin(\xi)Y_A \quad \text{and} \quad Y_B = \cos(\xi)Y_A - \sin(\xi)X_A. \tag{4.8}$$

The estimated key generation rate for RFI-QKD with decoy-state technique is given by Wang *et al.* [2015b]

$$R \geqslant -Q_\mu f h(E_\mu) + Q_1(1-I_E), \tag{4.9}$$

where Q_μ, E_μ, e_1, and Q_1 are the same as those given for the decoy-state BB84 protocol (Appendix A), and other parameters are defined in Appendix B.

4.5 Numerical Results

In this section, we numerically study the feasibility of wireless indoor QKD by looking at different scenarios. Table 4.1 summarizes the nominal values used in our numerical results. These parameter values are based on the available technology for QKD systems. For instance, the values used for detector efficiency and dark count can be achieved by silicon APDs Hadfield [2009]. Recent GHz-rate QKD demonstrations have also used pulse durations on the order of hundreds of ps with a correspondingly narrow filter at the receiver Patel *et al.* [2014a]. We use 0.5 photons per signal pulse, which is the near optimal value for μ in the decoy-state BB84 protocol. The room dimensions are representing a typical room with higher reflections from the walls than the floor, which might have carpeting. In a large partitioned office space, this can represent one cubicle in the room, or the area that can be covered by one QKD receiver. We also assume a rather large semi-angle at half power for both the lighting source and the QKD source, which overestimates the errors we may have in a practical setup. The latter will, however, be crucial for mobility features.

Before analyzing the key rate performance, let us start by illustrating how the position of the QKD source and its beam size, as well as the receiver's FOV, would affect the path loss. Figure 4.2 shows that the position of the QKD source with respect to its receiver can harshly affect the channel loss. In our case, moving from the centre of the room to one of its corners adds nearly 10 dB to the channel loss. This is partly because of the additional distance, but mainly because of the loose alignment we have adopted for our system. In our setup, we have assumed that the QKD source emits light upward, at a right angle with the floor, to the ceiling. There is also the interplay between the source semi-angle and the total loss. The lower the source semi-angle is the larger m would be in Eq. (3.4). This means that for small values of ϕ, i.e., when the QKD source is near the centre of the room, there may be some gain in the channel loss proportional to $m + 1$, but once ϕ increases, by moving toward the corners, that benefit may be washed away by the $\cos(\phi)^m$ term in Eq. (3.4). The receiver's FOV would also affect the loss in a negative way. One may assume that a larger FOV would result in higher power collection, but, quite the opposite, because of the concentrator

Table 4.1: Nominal values used for our system parameters.

Symbol	Parameter	Values
$\Phi_{1/2}$	Semi-angle at half power of the bulb	70°
$\Theta_{1/2}$	Semi-angle at half power of QKD source	30°
λ	Wavelength of QKD source	880 nm
X, Y, Z	Room size	4,4,3 m
r_1, r_2	Reflection coefficients of the walls and floor	0.7 , 0.1
η_d	Detector efficiency	0.6
τ	Pulse width	100 ps
$\Delta\lambda$	Optical filter bandwidth	$\frac{\lambda^2}{\tau c}$
A	Detector area	1 cm^2
n	Refractive index of the concentrator	1.5
T_s	Optical filter transmission	1
n_D	Dark count	1000τ
μ	Average no. of photons per signal pulse	0.5
ν_1, ν_2	Ave. no. of photons/pulse for decoy states	$0.1, 0$
f	Inefficiency of error correction	1.16
e_d	Relative-phase distortion probability	0

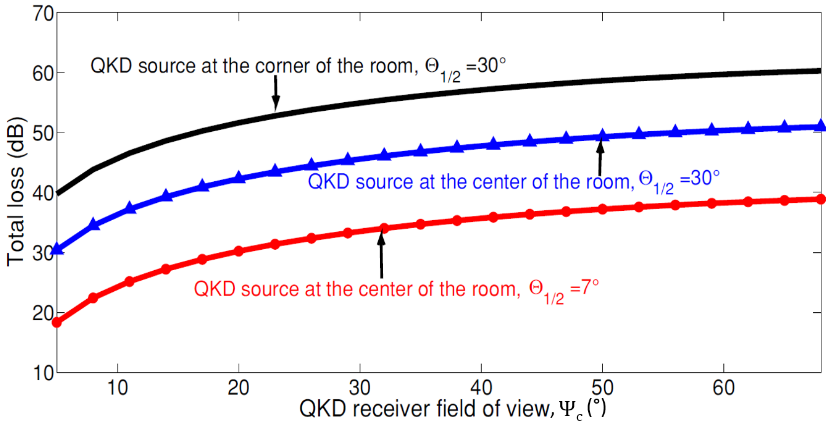

Figure 4.2: Total loss, $-10\log_{10}(\eta_d H_{\mathrm{DC}}/2)$, for the QKD source in centre and corner positions. Path loss depends on the semi-angle at half power, the position of the QKD source, and the receiver's FOV, Ψ_c.

gain, the larger the FOV is, the higher the channel loss would be. This is evident from all the curves in Fig. 4.2. A larger FOV would, however, enable the QKD source to be seen over a wider range. That advantage could, however, come with additional background noise that may sneak into the receiver. Overall, Fig. 4.2 indicates that, without beam steering, the QKD system may need to tolerate a large amount of propagation loss in the wireless channel.

In the following, we first assess the in-principle feasibility of wireless QKD using the decoy-state BB84 protocol with perfect encoders. We then consider the effect of encoder imperfections in our analysis.

4.5.1 Secure versus Insecure Regions

In this section, two scenarios of wireless QKD in indoor environments are examined, and the corresponding key generation rates are obtained using loss and background noise calculations in the previous sections. In the first scenario, only the background noise due to the isotropic ambient light is included. The key generation rate is then presented versus a range of FOVs as the latter has an impact on path loss as shown in Fig. 4.2. In the second scenario, we account for the background noise induced by the lighting source. In such a case, the amount of background noise would depend on the PSD of the lighting source and the QKD

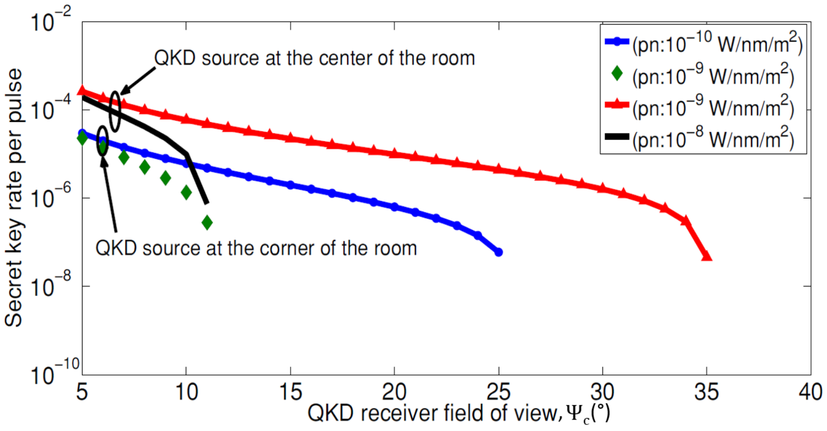

Figure 4.3: Secret key rate per transmitted pulse when the lighting source is off, and the background noise is only due to the ambient noise that has spectral irradiance denoted by p_n. The QKD source is sending light upward with 30°. The decoy-state BB84 protocol with an infinite number of decoy states and perfect encoders are employed here.

receiver's FOV. In both cases, we use the decoy-state encoding with infinitely many decoy states as described in Sec. 4.4.1.

Figure 4.3 shows the secret key generation rate in a dark room when the QKD transmitter is either at the centre of the room, or at a corner. In both cases, the QKD receiver is fixed at the centre of the ceiling. When the QKD source is located at the centre of the room, the system would tolerate spectral irradiance of ambient noise on the order of 10^{-8} W/nm/m^2, as shown in Fig. 4.3. Due to additional loss, the scheme would tolerate less ambient noise when the QKD source is located at a corner of the room. The ambient light noise considered in this case is due to black body radiation in the surrounding environment, whose effect is calculated via (4.2). This implies that the resulting background noise is constant in this case, and the drop in rate in Fig. 4.3 is merely because of the loss in the system as seen in Fig. 4.2. The spectral intensity emitted at room temperature (300 K) from objects, such as the human body, is expected to be low at the operating wavelength of our scheme. According to Planck's formula, the spectral irradiance at room temperature at 880 nm is on the order of 10^{-18} W/nm/m^2, which is far below the tolerable amount of ambient noise in

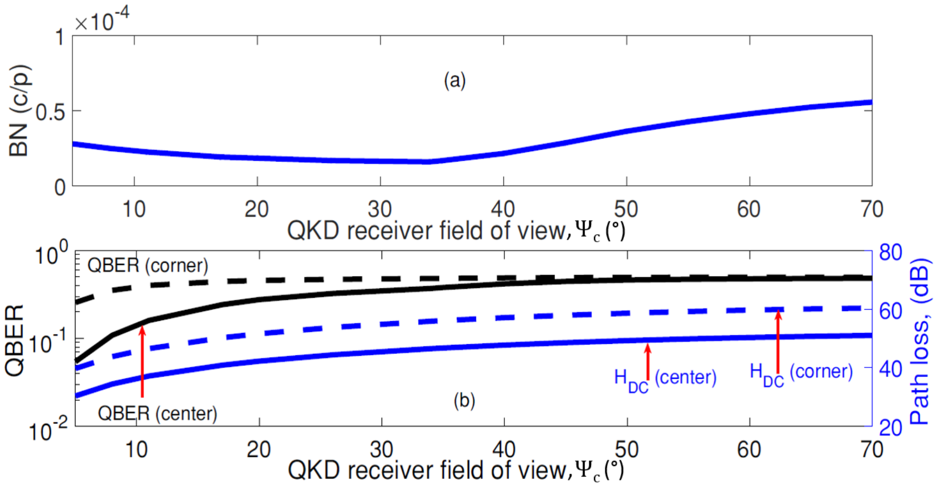

Figure 4.4: (a) Background noise (BN) in count per pulse (c/p), generated by the artificial light source, collected by the QKD receiver versus FOV, Ψ_c. (b) The channel loss, $1/H_{\mathrm{DC}}$, and QBER, E_μ, versus FOV. The QKD source is located either at the centre or corner of the room floor. The PSD of the bulb is 10^{-5} W/nm.

our scheme. This is mainly because we assume that there would be no sun light in the room, which can adversely affect system performance. In the case of our window-less room, however, it is safe to neglect the effect of isotropic ambient noise in our system. We next consider the effect of the lighting source on our QKD operation.

When the lighting source is on, additional background noise would sneak into the QKD receiver. The choice of FOV to some extent affects the amount of background noise. Figure 4.4 shows the effect of FOV on the background noise, as well as on H_{DC} and the overall QBER, E_μ. It is interesting to see that, at the beginning, the background noise would slightly drop until FOV reaches near 34°, from which point it gradually increases with FOV. For narrow FOVs, the concentrator gain is rather high, but it sharply approaches n^2 when FOV increases. This can be seen in the behavior of H_{DC} as well. The drop in the concentrator gain can justify the initial decline of the background noise. Another contributing factor is that for FOV $< 34°$, the collected power at the QKD receiver is mainly induced by the reflection from the floor, whereas for FOV $> 34°$, the reflection from the four walls would also matter. We have chosen much higher reflection coefficient from the walls (0.7) than the floor (0.1), which justifies the increase in the background noise. From the QBER curves in Fig. 4.4 it can be seen that the QBER is larger than its acceptable threshold for large FOVs. It is then fair to assume that within the region of interest for the FOV, the background noise is nearly constant while the channel gain drops with the increase in the FOV.

Figure 4.5 shows the secret key generation rate per transmitted pulse when the lighting source is on and the QKD source is placed at the centre of the room's floor facing up toward the receiver. The figure shows the trade-off between the receiver's FOV and the PSD of the light source. The higher the PSD is, the lower the FOV should be in order to improve the signal to noise ratio at the QKD receiver. This restriction partitions the x-y plane in Fig. 4.5 into secure and insecure regions. The insecure region is when the lower bound on the key rate is zero, i.e, when the secure exchange of keys cannot be guaranteed. The secure region then specifies when QKD operation is feasible within the setting in our setup. Figure 4.5 implies that with a PSD of 10^{-5} W/nm, corresponding to white LED bulbs, the QKD receiver's FOV should be less than 7°.

Figure 4.6 shows the secret key generation rate per transmitted pulse when the transmitter has moved to a corner of the room. We assume that the QKD source has a rather large transmission angle (30°), in which case a portion of its beam has the chance to be received by the receiver. This can possibly be achieved by a diffuser, if the source beam is too narrow. We assume that the source is again sending light up toward the ceiling. Being at the corner of the room, the channel DC-gain is lower than that of a transmitter at the centre of the room. This would imply that lower amounts of background noise can be tolerated in this case. The trade-off between the FOV and PSD has been shown in Fig. 4.6. In this case, at a PSD of 10^{-5} W/nm, the QKD receiver's FOV should be less than 4°.

Figures 4.5 and 4.6 imply that while there are certain regions in which secret key exchange is possible with minimal beam alignment, additional beam steering can substantially improve the system performance. At the source, this can

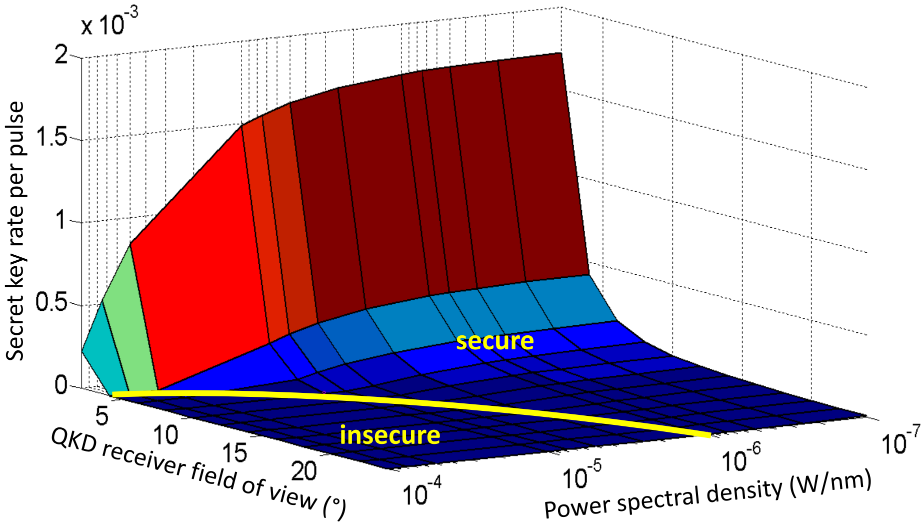

Figure 4.5: Secret key rate per transmitted pulse vesus power spectral density and QKD receiver's field of view, Ψ_c, for a QKD source ($\Theta_{1/2} = 30°$) at the centre of the floor in the presence of a lighting source. The decoy-state BB84 protocol with an infinite number of decoy states and perfect encoders are assumed here.

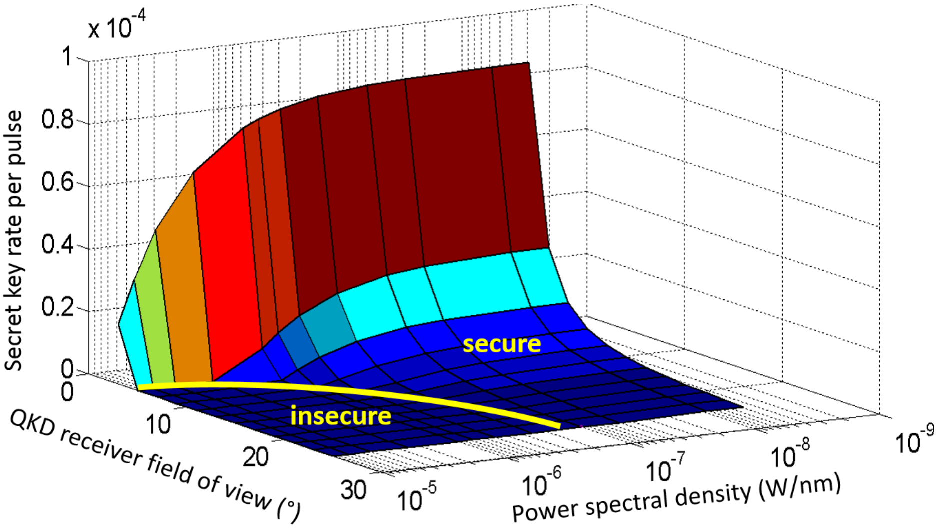

Figure 4.6: Secret key rate per transmitted pulse vesus power spectral density and QKD receiver's field of view, Ψ_c, for a QKD source with ($\Theta_{1/2} = 30°$) in a corner of the room in the presence of a lighting source. The decoy-state BB84 protocol with an infinite number of decoy states and perfect encoders are employed.

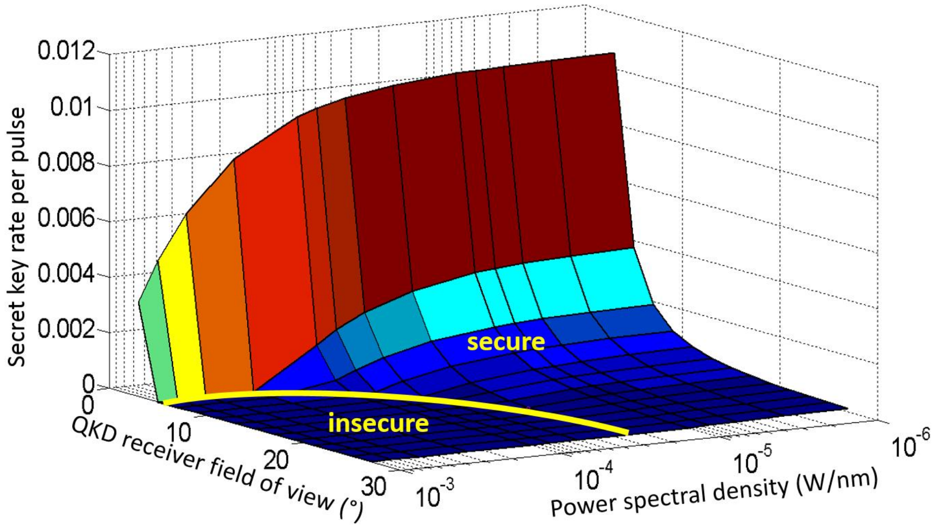

Figure 4.7: Secret key rate per transmitted pulse vesus power spectral density and QKD receiver's field of view, Ψ_c, for the QKD source in a corner of the room with additional beam steering. The QKD beam is directed into the receiver with $\Theta_{1/2} = 5°$. The decoy-state BB84 protocol with an infinite number of decoy states and perfect encoders are employed.

be achieved by narrowing the light beam and directing it toward the QKD receiver Gomez *et al.* [2015]. Here, we simulate this effect by directing a beam with $\Theta_{1/2} = 5°$ toward the QKD receiver, while the receiver's telescope orientation is fixed facing downward. As shown in Fig. 4.7, the system can now tolerate a larger amount of PSD in comparison to Fig. 4.6, where the QKD source is sending light in a non-direct manner with respect to the QKD receiver. Alternatively, in this case, one can use a larger FOV at the receiver, which allows us to cover a larger area for a mobile user.

4.5.2 More practical encoding techniques

After assessing the feasibility of wireless indoor QKD using perfect encoders, here we study the practical cases presented in Sec. 4.2. We consider the vacuum+weak decoy-state QKD, QKD with known source flaws, and RFI-QKD when the source flaws are partially known. We use the results of Sec. 4.4 to calculate the key rate in each case. Figures 4.8(a) and (b) show the secret key generation rate in each case where the QKD source is, respectively, at the centre and the corner of the room. There is only loose alignment between the source and the receiver, but here we have assumed a lower PSD for the lighting source at 10^{-6} W/nm. In the case of known source flaws we have assumed 10% error in the X basis, whereas in the RFI-QKD curve X and Y bases are rotated by a fix, but unknown, phase. In Fig. 4.8(a), when the source is at the centre of the room, the performance in all cases with an imperfect encoder is very close to the perfect case. This is expected as this case is less vulnerable to the alignment condition. When the source moves to the corner of the room, the sensitivity to the FOV becomes higher, but still with an FOV of 7°, it is still possible to exchange secret keys. At this FOV, the drop in key rate, is less than one order of magnitude when we, instead of perfect encoders, use RFI-QKD. This implies that by the proper choice of protocol we can make the system quite resilient to possible imperfections at its encoders.

The above cases illustrate the possibility of using QKD in certain indoor environments. Whether or not we need to employ extensive beam steering in our scheme would depend on the application scenario and its target key rate. One can think of certain scenarios in which the amount of keys generated by loose beam steering would still be sufficient for the application in mind. For instance, consider a bank customer that uses an advanced encryption standard (AES) protocol, supplemented by QKD generated seeds, for his/her banking transactions. Assuming that each session roughly requires 1 kb of secret key, the user can store the amount of keys required for nearly 600 sessions within 100 s in one trip to the bank, where according to Fig. 4.5, a key rate of 6 kbps, at a pulse repetition rate of 100 MHz, can be achieved when the receiver's FOV and PSD are, respectively, 5° and 10^{-5} W/nm. For applications with higher key usage, e.g., secure video streaming, one may need higher key rates only achievable if the transmitter-receiver pair are fully aligned. In such cases, one possible solution is to use docking stations, which ensures alignment without implementing all the necessary optical elements on a portable/mobile device.

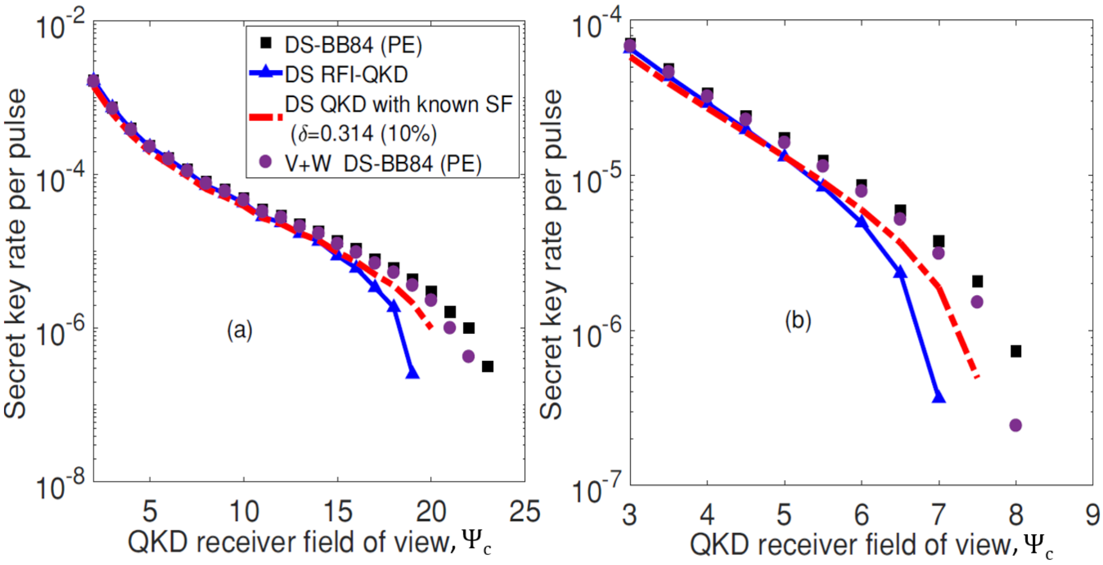

Figure 4.8: Secret key rate per transmitted pulse versus the QKD receiver FOV, for different QKD protocols (PE, perfect encoding; DS, decoy state; SF, source flaw; V + W, vacuum + weak). (a) The QKD source is located at the centre of the room. (b) The QKD source is located at a corner of the room. The PSD of the bulb is 10^{-6} W/nm.

4.6 Summary

We studied and analysed the feasibility of wireless QKD in indoor environments. We exploited the known OWC models to estimate the loss and background noise in such environments. We considered different scenarios in which the QKD source is perfect or with known/unknown flaws. Despite the severe loss and background noise in indoor environments, we showed that a practical wireless indoor QKD could exist. This would enable end users to exchange secret keys with other network users in a convenient way, as we will show in the following chapter.

Chapter 5

Wireless access to a hybrid quantum-classical network

5.1 Introduction

QKD will possibly be the most imminent application of quantum technologies in our daily life. There are, however, certain problems we have to resolve before making such a technology available to everyone. By adopting wireless indoor QKD links and embedding them into fiber-based PONs, users would be able to access conveniently to hybrid quantum-classical networks. Scenarios of interest include utilizing it in banks and public places to exchange data securely with service providers. Untrusted relay points, can be used in public places, to link a wireless end user and the corresponding central office, when MDI-QKD protocol is in use.

In this chapter, we address wireless access to a hybrid quantum-classical network. We propose practical configurations that would enable wireless access to such networks. In the following, we first provide a system description, which includes the proposed setups. This is followed by characterizing the channel, namely, the indoor optical wireless channel and optical fiber link. Next, key rate analysis is explained, where DV and CV-QKD protocols are considered. Finally, the numerical results and summary are presented

5.2 System Description

In this section, we describe our proposed setups for hybrid quantum-classical access networks comprised of optical wireless and fiber-optic links. Such setups can wirelessly connect a mobile user, in indoor environments, to the central office in access networks; see Fig. 5.1. We assume a total of N end users, which are connected to the central office via a dense wavelength-division multiplexing (DWDM) PON. The corresponding wavelengths assigned to quantum and classical data channels are, respectively, denoted by $Q = \{\lambda_{q_1},\ \lambda_{q_2},\ ...,\lambda_{q_N}\}$, $D = \{\lambda_{d_1},\ \lambda_{d_2},\ ...,\lambda_{d_N}\}$. The kth user, $k = 1, \ldots, N$, employs wavelength λ_{q_k} (λ_{d_k}) to communicate his/her quantum (classical) signals to the central office, as shown in Fig. 5.1. The same wavelengths are also used for the downlink. In order to heuristically reduce the Raman noise effect, we assume that the lower wavelength grid is allocated to the QKD channels, while the upper grid is assigned to data channels Bahrani *et al.* [2016a]. For instance, for the lower wavelength grid, wavelengths of 1530.8 nm, 1531.6 nm, ...,1555.62 nm, with 100 GHz channel spacing, are assumed to be used Eraerds *et al.* [2010]. In principle, one can use an optimised algorithm to minimise the Raman noise Bahrani *et al.* [2018].

For our wireless user, we consider a particular indoor environment, in which it has been shown that wireless QKD is feasible Elmabrok & Razavi [2015], Elmabrok *et al.* [2018]; see chapter 4. In this setting, a window-less room, of $X \times Y \times Z$ dimensions, is lit by an artificial light source. The possibly mobile QKD transmitter is placed on the floor and it transmits light toward the ceiling. The transmitter module may or may not be equipped with beam steering tools. In the former case, we assume that a minimal manual alignment is in place, by which the QKD source is facing the ceiling. This can be achieved by providing some instructions for the end user during the QKD protocol. The QKD receiver or the signal collector is fixed at the centre of the room's ceiling; see Fig. 5.1. We assume that, by using some dynamic beam steering, maximum possible power is collected from the QKD source. This may be achieved by using additional beacon pulses. The collected light may go through a non-imaging optical concentrator, such as a compound parabolic collector, and then be filtered by a bandpass filter before being detected or sent out toward its final destination.

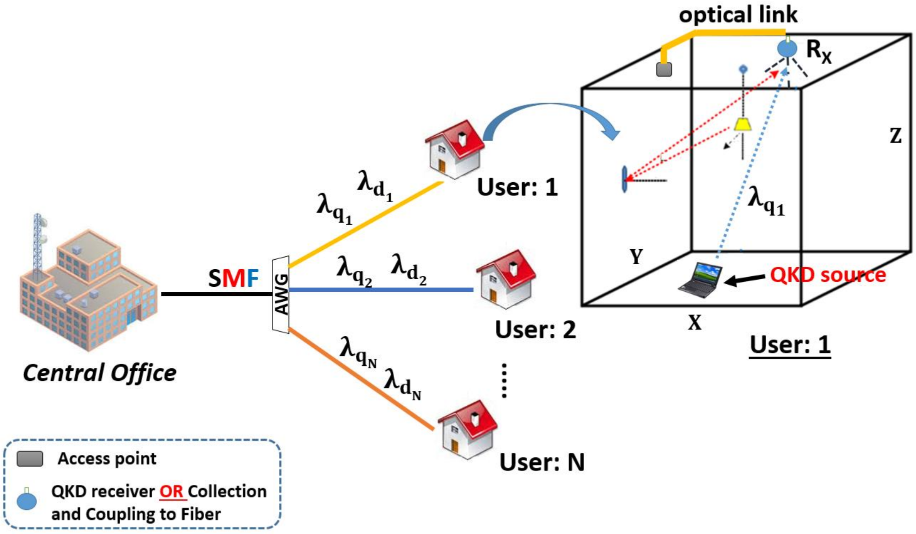

Figure 5.1: Schematic view of exchanging secret keys between an indoor wireless user with a central office at the end of an access network. The transmitter is mobile, while the QKD receiver or the collection point is fixed on the ceiling.

In each setup, we particularly study three different cases regarding the position of the mobile QKD device. Case 1 refers to the scenario when the QKD transmitter is placed at the centre of the room's floor and emits light upward with semi-angle at half power of $\Phi_{1/2}$. In case 2, the same QKD transmitter as in case 1 is moved to a corner of the room in order to assess the mobility features. These cases will represent the best and the worst case scenarios in terms of channel loss, when minimal beam alignment is used at the transmitter end. In case 3, the light beam at the QKD source is narrowed and is directed toward the QKD receiver or the coupling element. This would correspond to the worst case scenario when beam alignment is available at both the source and the receiver. In all cases, we assume a static channel in our analysis, that is we assume that the channel does not change during the key exchange procedure. The real mobile user is then expected to experience a quality of service bounded by the worst and best-case scenarios above.

We use a number of discrete and continuous-variable QKD protocols to investigate the performance of the proposed configurations. In the case of DV protocols, we use the time-bin encoding, in which the information is encoded onto the phase difference between two successive pulses Brendel *et al.* [1999]. We assume that the gap between the two pulses is sufficiently short that similar phase distortions would be applied to both time bins while traversing the channel. Possible discrepancies are modeled by a relative-phase error term e_d. The QKD protocols considered here are already explained in Chapter 2. In the following, we first describe our proposed setups and the QKD protocols used in each case, followed by a description of the channel models.

5.2.1 The proposed setups

We consider four setups in which an indoor wireless user, Alice, equipped with a QKD-enabled mobile device, would exchange secret keys with a remote party, Bob, located at the central office. In order to keep the mobile user's device simple, we assume that Alice is only equipped with the QKD encoder. That would imply that certain QKD schemes, such as entanglement-based QKD Bennett *et al.* [1992b], are not suitable for our purpose if they require measuring single photons at the mobile user's end. Bob, however, represents the service provider node and could be equipped with the encoder and/or the decoder module as needed. Based on these assumptions, here, we consider several settings depending on the existence or non-existence of a trusted/untrusted relay point between the wireless user and Bob at the central office. In all setups, a data channel will be wavelength multiplexed with the quantum one to be sent to the central office. We assume that classical data is being modulated at a constant rate throughout the QKD operation.

Setup 1 with a trusted relay point

Setup 1 is applicable whenever a trusted node between the sender and the recipient exists. For instance, in a bank, we can physically secure a QKD relay node inside the building with which the wireless QKD users in the room can exchange secret keys. In Fig. 5.2, such a node is located on the ceiling and it is comprised of Rx and Tx boxes. In this setup, the secret key exchange between Alice and Bob is accomplished in two steps: a secret key, K_1, is generated between Alice and the Rx box in Fig. 5.2; also, independently but in parallel, another secure

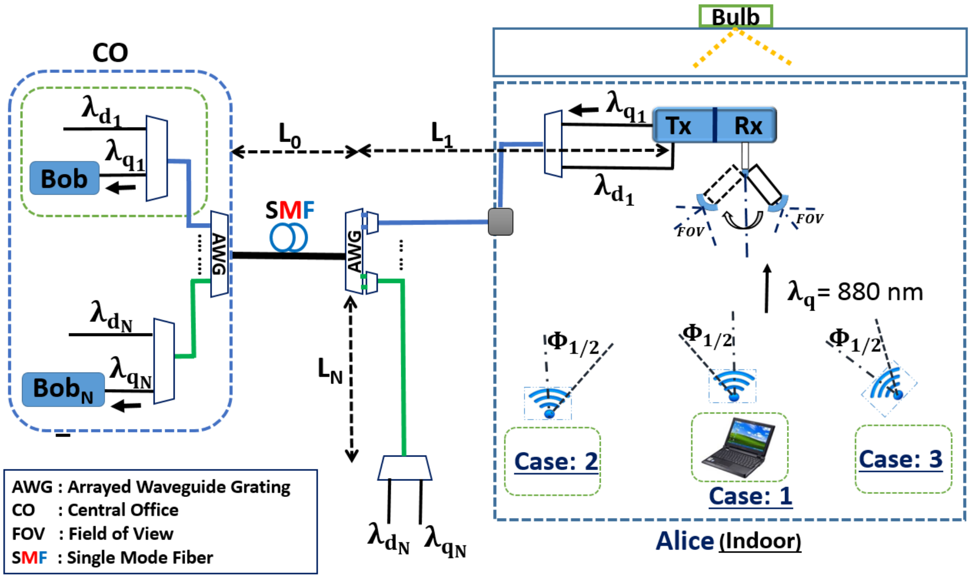

Figure 5.2: Setup 1, where secret key exchange between Alice and Bob is achieved in two steps. K_1 is generated between Alice and Rx, while K_2 is generated between Tx and Bob. The resultant key is computed by taking the XOR of K_1 and K_2. Three cases are examined according to the position and alignment of the QKD transmitter. The DS-BB84 and GG02 protocols will be examined in this setup. Dynamic beam steering is used at the Rx node.

key, K_2, is exchanged between Tx and the relevant Bob in the central office. The final secret key is then obtained by applying an exclusive-OR (XOR) operation to K_1 and K_2. Note that in this setup both links are completely run separately; therefore, the wavelength used in the wireless link does not need to be the same as the wavelength used in the fiber link. In fact, for the wireless link, we use 880 nm range of wavelength, for which efficient and inexpensive single-photon detectors are available. For the fiber link, conventional telecom wavelengths are used. DS-BB84 and GG02 protocols will be used for this setup.

Setup 2 without a relay point

In this setup, we remove the need for having a relay point altogether. As shown in Fig. 5.3, the signals transmitted by Alice are collected by a telescope and coupled to a single-mode fiber to be sent to the central office. QKD measurements will

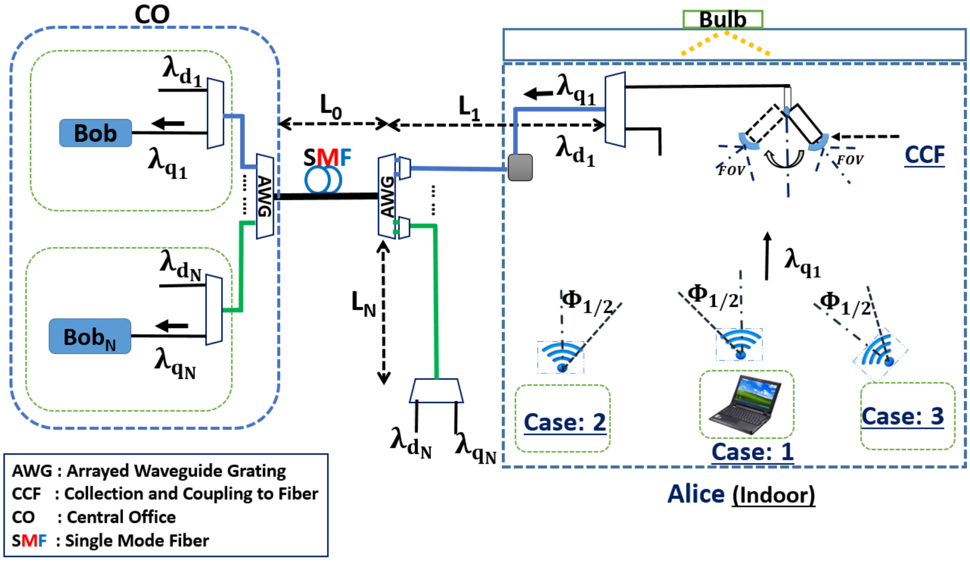

Figure 5.3: Setup 2, where secret keys are exchanged between Alice and Bob using the DS-BB84 and GG02 protocols. The latter is only used in case 3. The QKD signals are collected and coupled to the fiber and sent to Bob, where the measurement is performed. Dynamic beam steering is used at the collection node.

then be performed at the central office. Because of this coupling requirement, the wireless signals undergo an additional coupling loss in setup 2. To reduce the coupling loss, in this setup, and, for fairness, in all others, we assume that the telescope at the collection point can focus on the QKD source. This can be achieved by additional beacon beams and MEMs steering mirrors Chun *et al.* [2017]. In order to efficiently couple this photon to the fiber, the effective FOV at the collection point should match the numerical aperture of a single-mode fiber. That requires us to use FOVs roughly below 6°, although, in practice, much lower values may be needed. In this setup, DS-BB84 and GG02 can be suitable protocols and will be examined in the following sections.

Setups 3 and 4 with untrusted relay points

The setups in Figs. 5.4 and 5.5 are of interest whenever the indoor environment the wireless user is working at is not trustworthy. For instance, if the user is working at a public place, such as a coffee shop or an airport, s/he may not

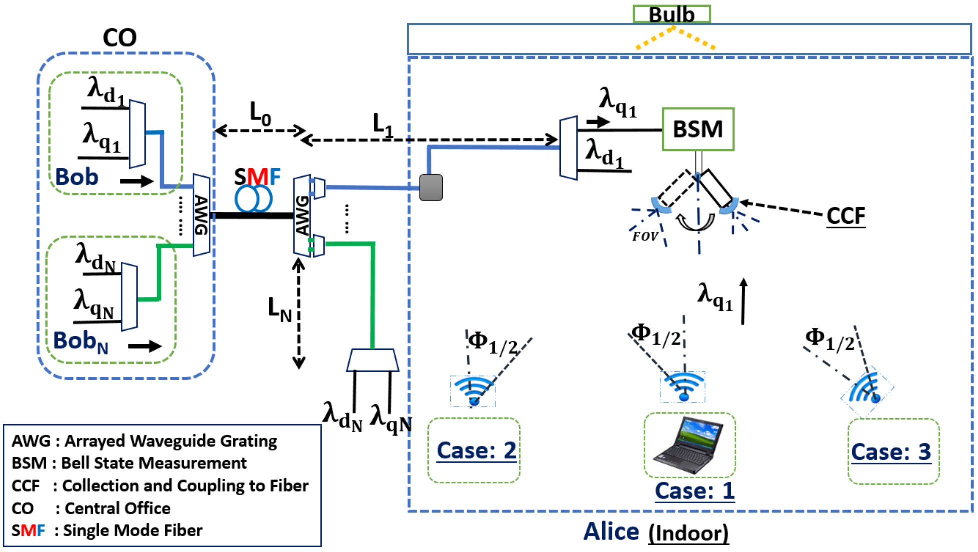

Figure 5.4: Setup 3, where secret keys are exchanged between Alice and Bob using the MDI-QKD protocol. The BSM is performed at the user's end in this setup.

necessarily trust the owners of the local system. In such setups, we can use the MDI-QKD technique Lo *et al.* [2012] to directly interfere the quantum signal sent by the users with that of the central office. This can be accomplished by, if necessary, coupling the wireless signal into the fiber and performing a Bell-state measurement (BSM) on the photons sent by Alice and Bob at either the user's end (setup 3), or at a certain place located between the sender and the recipient at the central office (setup 4). In setup 4, we use the splitting terminal of a PON to implement such BSMs. Note that in setups 3 and 4 we need to interfere a single-mode signal traveling in fiber with a photon that has traveled through the indoor channel. In order to satisfy the BSM indistinguishability criterion, we then need to collect only one spatial mode from the wireless channel. The flexible beam steering used at the collection node should then satisfy this requirement.

Here, we use a probabilistic setup for the BSM operation, as shown in Fig. 5.6. In this setup, we interfere the light coming from the two users at a 50:50 (fiber-based) beam splitter and then detect the outgoing signals using single-photon detectors. This simple setup is suitable for time-bin encoding techniques in QKD,

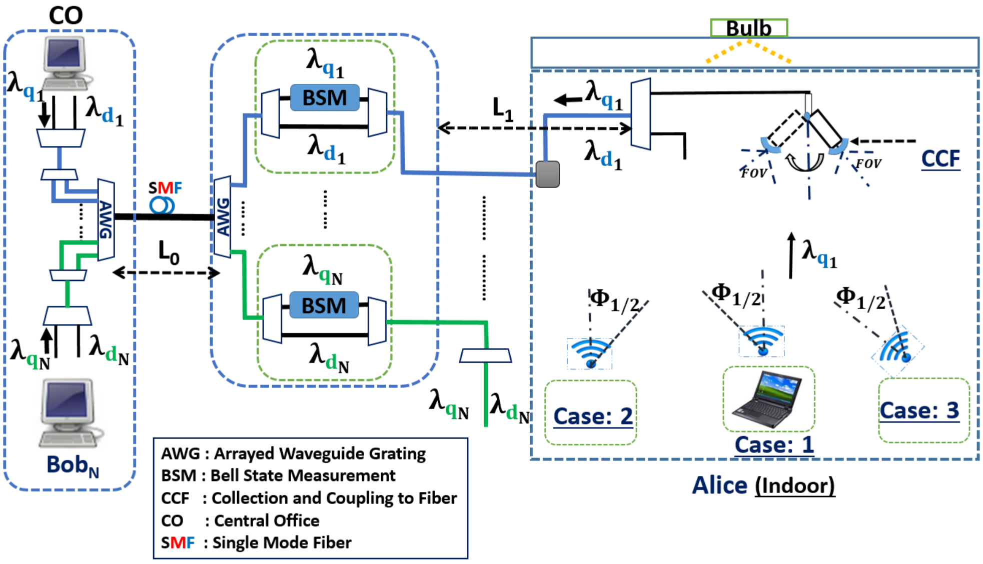

Figure 5.5: Setup 4, where secret keys are exchanged between Alice and the central office using the MDI-QKD protocol. The BSM is performed at the splitting point of the DWDM PON.

which offer certain advantages in both fiber and free-space QKD systems. In particular, they may suffer less from alignment issues as compared to polarization-based encoding in wireless environments. Note that two successive clicks, one corresponding to each time bin, is required to have a successful BSM. That would require fast single-photon detectors with sub-nanosecond deadtimes. This is achievable using self-difference feedback techniques developed recently Yuan *et al.* [2007]. If such detectors are not available, one can rely on one click on each detector, which roughly corresponds to declaring half of the success cases.

5.2.2 Channel Characterization

In this section, we model the two parts of our communication link, i.e., the wireless and fiber-based components, and find out how much loss or background noise they may introduce.

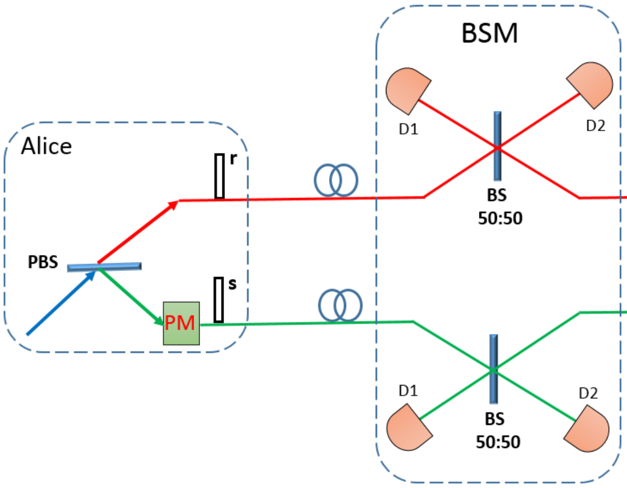

Figure 5.6: The Bell-state measurement (BSM) module used in setups 3 and 4. This module works for time-bin encoded QKD signals. If fast detectors are available, as assumed here, we can do two consecutive measurements on each time bin. if not, we can still measure one out of four Bell states by relying on a single click in total on each detector. BS: beamsplitter. PBS: Polarizing Beamsplitter. PM: Phase modulator Ma *et al.* [2012a].

Indoor optical wireless channel

Because of path loss, Bob would receive a random portion of the polarized photons that have been sent by Alice. The fraction of the transmitted power is estimated by channel DC-gain H_{DC} explained in Eq. (3.4).

Optical fiber link

As for the optical link, we make the following assumptions. We consider a loss coefficient α in dB/km in the single-mode fiber. We also assume that the loss contributed by each multi-port DWDM multiplexer, labeled as AWG (arrayed waveguide grating) in Figs. 5.2–5.5 is Λ in dB. We neglect the loss associated with two-to-one multiplexers.

As we mentioned earlier, the main source of background noise in QKD channels in a fiber link is Raman scattering. The Raman noise generated by a strong classical signal spans over a wide range of frequencies, hence can populate the

QKD receivers with unwanted signals Eraerds *et al.* [2010]. The receivers can be affected by forward and backward scattered light depending on their locations and the direction of light propagation Bahrani *et al.* [2016b]. For a classical signal with intensity I at wavelength λ_d, the power of Raman noise at a QKD receiver with bandwidth $\Delta\lambda$ centred at wavelength λ_q is given by Eraerds *et al.* [2010], Patel *et al.* [2012]

$$I_R^f(I, L, \lambda_d, \lambda_q) = I e^{-\alpha_r L} L \Gamma(\lambda_d, \lambda_q) \Delta\lambda \tag{5.1}$$

for forward scattering and

$$I_R^b(I, L, \lambda_d, \lambda_q) = I \frac{(1 - e^{-2\alpha_r L})}{2\alpha_r} \Gamma(\lambda_d, \lambda_q) \Delta\lambda \tag{5.2}$$

for backward scattering, where L is the fiber length and $\Gamma(\lambda_d, \lambda_q)$ is the Raman cross section (per unit of fiber length and bandwidth), which can be measured experimentally. In our work, we have used the results reported in Eraerds *et al.* [2010] for $\lambda_d = 1550$ nm and have used the prescription in Bahrani *et al.* [2016b] to adapt it to any other wavelengths in the C band. In our numerical analysis, we assume that the latter band (1530 - 1565 nm), is mainly used for 32 quantum channels with 100 GHz channel spacing Eraerds *et al.* [2010].

The transmitted power I is also set to secure a bit error rate (BER) of no more than 10^{-9} for all data channels. The QKD receiver would then collect a total average number of photons, due to forward and backward scattering, respectively, given by

$$\mu_R^f = \frac{\eta_d I_R^f \lambda_q T_d}{hc} \tag{5.3}$$

and

$$\mu_R^b = \frac{\eta_d I_R^b \lambda_q T_d}{hc}, \tag{5.4}$$

where T_d, η_d and h, respectively, represent the detectors' gate duration, their quantum efficiency and Planck's constant with c being the speed of light in the vacuum.

5.3 Key Rate Analysis

In this section, the secret key rate analysis for our proposed setups is presented considering non-idealities in the system. The secret key rate is defined as the asymptotic ratio between the number of secure bits and sifted bits. Without loss of generality, we only calculate the rate for user 1 assuming that there is no eavesdropper present. The DS-BB84 Ma *et al.* [2005] and GG02 protocols are used for setups 1 and 2, while the MDI-QKD protocol Lo *et al.* [2012], Ma & Razavi [2012] is employed for setups 3 and 4.

5.3.1 Setups 1 and 2

DS-BB84 protocol

The lower bound for the key generation rate in the limit of an infinitely long key is given by Ma *et al.* [2005]

$$R \geq q\{-Q_\mu f h(E_\mu) + Q_1[1 - h(e_1)]\}, \tag{5.5}$$

where all new parameters are defined in Appendix A. There, we show that the expected value for these parameters in our loss and background induced model for the channel mainly depends on two parameters: the overall efficiency of each link η, and the total background noise per detector, denoted by n_N. Here, n_N accounts for both dark counts and background noise in the link. In the following, we specify how these parameters can be calculated in each setup.

In setup 1, we have two links, a wireless link and a wired link. In the following, the parameter values for each link will be calculated separately.

Setup 1, wireless link: For the wireless channel, we assume that the background noise due to the artificial lighting source is denoted by n_{B_1}, which can be calculated using the methodology proposed in chapter 4 Elmabrok *et al.* [2018]. In our calculations, we upper bound n_{B_1} by considering the case where the QKD receiver is focused on the centre of the room. The total noise per detector, n_N, is then given by $n_{B_1}\eta_{d_1}/2 + n_{dc}$, where η_{d_1} is the detector efficiency, for the detector in the Rx box, and n_{dc} is the dark count rate per pulse for each detector in the Rx box in Fig. 5.2. We neglect the impact of the ambient noise in our windowless room Elmabrok *et al.* [2018]. The total transmissivity is also given by $\eta = H_{\rm DC}\eta_{d_1}/2$. The factor 1/2 represents the loss in the passive time-bin decoder consisted of a Mach-Zehnder interferometer.

Setup 1, fiber link: As for the fiber-based link, the background noise is mainly induced by the Raman scattered light. In this setup, where Bob's receiver is at the central office, forward scattered light is generated because of the classical signals sent by the users and backward scattered light is due to the signals sent by the central office. The total power of Raman noise, at wavelength λ_{q_1}, for forward and backward scattering are, respectively, given by

$$I_{T1}^f = [I_R^f(I, L_0 + L_1, \lambda_{d_1}, \lambda_{q_1}) + \sum_{k=2}^{N} I_R^f(Ie^{-\alpha_r L_k}, L_0, \lambda_{d_k}, \lambda_{q_1})]10^{-2\Lambda/10}$$

and

$$I_{T1}^b = [I_R^b(I, L_0 + L_1, \lambda_{d_1}, \lambda_{q_1}) + \sum_{k=2}^{N} I_R^b(I, L_0, \lambda_{d_k}, \lambda_{q_1})]10^{-2\Lambda/10},$$

where L_0 is the total distance between the central office and the AWG box at the users' splitting point and L_k is the distance of the kth user to the same AWG in the access network. In the above equations, we have neglected the out-of-band Raman noise that will be filtered by relevant multiplexers in our setup. For instance, in calculating I_{T1}^f, we account for the effect of the forward Raman noise by the data signal generated by User 1 over a total distance of $L_0 + L_1$, but, a similar effect by other users is only accounted for over a distance L_0. That is because the AWG box filters most of the Raman noise at λ_{q_1} generated over distances L_k and their effect can be neglected. By substituting the above equations in 5.3 and 5.4, the total background noise per detector, at the Bob's end in Fig. 5.2, is given by

$$n_N = \frac{\eta_{d_2}\lambda_{q_1}T_d}{2hc}(I_{T1}^f + I_{T1}^b) + n_{dc}, \tag{5.6}$$

where η_{d_2} is the detector efficiency at the Bob's receiver. Note that in setup 1 we consider two different values for η_{d_1} and η_{d_2}. The reason is that the former corresponds to the available silicon APD single-photon detectors at 880 nm, while the latter could be for InGaAs APD single-photon detectors within the 1550 nm band.

The total transmissivity η for the fiber link is given by $\eta_{\text{fib}}\eta_{d_2}/2$, where η_{fib} is the optical fiber channel transmittance including the loss associated with AWGs given by $\eta_{\text{fib}} = 10^{-[\alpha(L_1+L_0)+2\Lambda]/10}$.

Setup 2: In setup 2, the total Raman noise power for forward and backward scattering, denoted by I^f_{T2} and I^b_{T2} are given by I^f_{T1} and I^b_{T1}, respectively. The total background noise per detector at Bob's end in Fig. 5.3 is then given by

$$n_N = \frac{\eta_{d_2}}{2}\left[\frac{\lambda_{q_1}T_d}{hc}\left(I^f_{T2} + I^b_{T2}\right) + n_{B_1}\eta_{\text{fib}}\eta_{\text{coup}}\right] + n_{dc}, \tag{5.7}$$

where η_{coup} is the additional air-to-fiber coupling loss that the indoor background photons, generated by the bulb, will experience before reaching the QKD receiver. The total channel transmittance between the sender and the recipient in this setup is given by $\eta = H_{\text{DC}}\eta_{\text{coup}}\eta_{\text{fib}}\eta_{d_2}/2$.

GG02 protocol

The secure key rate for GG02 with reverse reconciliation under collective attacks is given by Fossier *et al.* [2009]

$$K = \beta I_{AB} - \chi_{BE}, \tag{5.8}$$

where β is the reconciliation efficiency. I_{AB} and χ_{BE} are, respectively, the shared information between Alice and Bob, and the amount of information obtained by the adversary in reverse reconciliation. More details can be found in Appendix D.

GG02 is characterized by the channel loss η_{ch} and the excess noise ε. For estimating the latter, we need to consider the contribution of the bulb, ε_b, as well as the Raman scattering, ε_r. The total excess noise, ε, is then given by $\varepsilon_b + \varepsilon_r + \varepsilon_q$, where ε_q is any other additional noise observed in the experiment. In the Appendix D formulation, the excess noise terms must be calculated at the input. For chaotic sources of light, if the average noise count at the end of a channel with transmissivity η_t is given by n, the corresponding excess noise at the input would be given by $2n/\eta_t$ Kumar *et al.* [2015], Qi *et al.* [2010b]. Below, we use this expression to calculate ε_b and ε_r assuming that both the Raman noise and the bulb-induced background noise are of chaotic-light nature.

Setup 1, wireless link: In setup 1, the background noise due to the bulb is denoted by n_{B_1}. This is the total background noise at the Rx box input. Given that the LO would pick a single spatio-temporal mode with matching polarization, the corresponding count that sneaks into the homodyne receiver would be $n_{B_1}/2$. The corresponding excess noise would then be given by $\varepsilon_b = n_{B_1}/H_{\text{DC}}$ and $\varepsilon = \varepsilon_b + \varepsilon_q$. In this case, $\eta_{\text{ch}} = H_{\text{DC}}$. In an experiment, ε_q is often calculated by measuring the corresponding parameter, $\varepsilon_q^{\text{rec}}$, at the receiver. In this case, $\varepsilon_q = \varepsilon_q^{\text{rec}}/(\eta_{\text{ch}}\eta_B)$, where η_B is Bob's receiver overall efficiency.
Setup 1, fiber link: In this case, $\eta_{\text{ch}} = \eta_{\text{fib}}$, $\varepsilon_b = 0$, and $\varepsilon_r = n_r/\eta_{\text{ch}}$, where

$$n_r = \frac{\lambda_{q_1} T_d}{hc}(I_{T1}^f + I_{T1}^b). \tag{5.9}$$

Setup 2: In setup 2, $\eta_{\text{ch}} = H_{\text{DC}}\eta_{\text{coup}}\eta_{\text{fib}}$, $\varepsilon_b = n_{B_1}/H_{\text{DC}}$, and $\varepsilon_r = n_r/\eta_{\text{ch}}$, where

$$n_r = \frac{\lambda_{q_1} T_d}{hc}\left(I_{T2}^f + I_{T2}^b\right). \tag{5.10}$$

In all CV-QKD setups, we assume that a phase reference for the LO is available at the receiver.

5.3.2 Setups 3 and 4 with MDI-QKD protocol

The secret key rate for the MDI-QKD setup is given in Appendix C. The key parameters to find for this scheme are η_a and η_b, which, respectively, correspond to the total transmissivity seen by Alice and Bob channels, as well as n_N, which is the total background noise per detector. Here we find these parameters for Setups 3 and 4.
Setup 3: The total forward and backward Raman noise power for setup 3 at wavelength λ_{q_1} are, respectively, given by

$$I_{T3}^f = [I_R^f(I, L_0 + L_1, \lambda_{d_1}, \lambda_{q_1}) + e^{-\alpha_r L_1}\sum_{k=2}^{N} I_R^f(I, L_0, \lambda_{d_k}, \lambda_{q_1})]10^{-2\Lambda/10},$$

and

$$I_{T3}^b = [I_R^b(I, L_0 + L_1, \lambda_{d_1}, \lambda_{q_1}) + e^{-\alpha_r L_1}\sum_{k=2}^{N} I_R^b(Ie^{-\alpha_r L_k}, L_0, \lambda_{d_k}, \lambda_{q_1})]10^{-2\Lambda/10}.$$

The total noise per detector, n_N, for setup 3 is then given by

$$n_N = \frac{\eta_{d_2}}{4}\left[\frac{\lambda_{q_1}T_d}{hc}\left(I^f_{T3}+I^b_{T3}\right)+n_{B_1}\eta_{\text{coup}}\right]+n_{dc}, \tag{5.11}$$

where we account for one particular polarization entering the BSM module.

In setup 3, $\eta_a = H_{\text{DC}}\eta_{d2}\eta_{\text{coup}}/2$ and $\eta_b = \eta_{d2}\eta_{\text{fib}}/2$, assuming an average loss factor of 1/2 for polarization mismatch. Note that the two modes interfering at the BSM must have matching polarizations. This can be achieved passively by using polarization filters before the 50:50 beam splitter in the BSM, in which case, an average loss of 1/2 is expected, or, alternatively, we need to use active polarization stabilizer, for which the corresponding loss factor approaches one.

Setup 4: The total forward and backward Raman noise power for setup 4 at wavelength λ_{q_1} are, respectively, given by

$$I^f_{T4} = [I^f_R(I,L_0,\lambda_{d_1},\lambda_{q_1})+\sum_{k=2}^{N}I^f_R(I,L_0,\lambda_{d_k},\lambda_{q_1})]\times 10^{-2\Lambda/10}+I^f_R(I,L_1,\lambda_{d_1},\lambda_{q_1}),$$

and

$$I^b_{T4} = [I^b_R(Ie^{-\alpha_r L_1},L_0,\lambda_{d_1},\lambda_{q_1})+\sum_{k=2}^{N}I^b_R(Ie^{-\alpha_r L_k},L_0,\lambda_{d_k},\lambda_{q_1})+I^b_R(Ie^{-\alpha_r L_0},L_1,\lambda_{d_1},\lambda_{q_1})]10^{-2\Lambda/10}.$$

The total noise per detector, n_N, for setup 4 is as follows

$$n_N = \frac{\eta_{d_2}}{4}\left[\frac{\lambda_{q_1}T_d}{hc}\left(I^f_{T4}+I^b_{T4}\right)+n_{B_1}\eta_{\text{coup}}10^{-\alpha L_1/10}\right]+n_{dc}. \tag{5.12}$$

In setup 4, $\eta_a = H_{\text{DC}}\eta_{d_2}\eta_{\text{coup}}10^{-\alpha L_1/10}/2$ and $\eta_b = \eta_{d_2}10^{-[\alpha L_0+2\Lambda]/10}/2$.

5.4 Numerical Results

In this section, we provide some numerical results for secret key rates in the four proposed setups. We use a DWDM scheme with 100 GHz channel spacing in the C-band with 32 users. We define Q = {1530.8 nm, 1531.6 nm,...,1555.62 nm} and D = {1560.4 nm, 1561.2 nm,...,1585.2 nm} for quantum and classical channels, respectively. We assume that λ_{q_1} is 1555.62 nm and the corresponding λ_{d_1} is 1585.2 nm. The classical data is transmitted with launch power I =

$10^{(-3.85+\alpha L/10+2\Lambda/10)}$ mW, which corresponds to receiver sensitivity of -38.5 dB guaranteeing a BER $< 10^{-9}$ Bahrani *et al.* [2016b]. In all setups, we assume that $L_1 = L_2 = \cdots = L_N$ all equal to 500 m.

Other nominal parameter values used in our simulation are summarized in Table 5.1. These are based on values that are technologically available today. In particular, for DV-QKD systems, we assume silicon-based single-photon detectors are used in the 800 nm regime (setup 1, indoor channel), whereas GaAs detectors may need to be used in the 1550 nm regime (all other setups). The former often have higher quantum efficiencies than the latter. That is why in our numerical parameters, η_{d1} is twice as big as η_{d2}. The dark count rate in such detectors varies from (100–1000)/s for an APD, to (1–100)/s for superconducting detectors Dusek *et al.* [2006]. The average dark count rate considered here is 1000/s, which, over a period of 100 ps, will result in $n_{dc} = 10^{-7}$. In the CV-QKD system, η_B is Bob's receiver overall efficiency, which includes detector efficiencies and any insertion loss in the homodyne receiver. The parameter β is the efficiency of our post-processing, which nowadays exceeds 95% Jouguet *et al.* [2011]. The parameter values chosen for the receiver electronic noise and excess noise correspond to the observed values in recent CV-QKD experiments Jouguet *et al.* [2013]. Based on the values chosen for our system parameters, relevant parameters in Sec. 5.3, such as η_{fib} and η_{ch}, can be calculated from which parameter η for each setup is obtained. The noise parameter n_N, for each setup, can similarly be found. The Raman noise terms, in particular, have been calculated by extracting the Raman cross section from the experimental measurements reported in Eraerds *et al.* [2010]. Note that, in our numerical calculations, we often vary the coupling loss to study system performance.

In each setup, three cases are considered for the light beam orientation of the QKD source. In the first case, the semi-angle at half power of the QKD source is $\Phi_{1/2} = 20°$ while the QKD source is placed at the centre of the room's floor. With the same $\Phi_{1/2}$, the QKD source is moved to the corner of the room in the second case. We use $\Phi_{1/2} = 1°$ in the third case where the QKD source is located at the corner of the room, as in the second case, but the beam is directed and focused toward the QKD receiver or the collection element. A full alignment is assumed in the third case, while in the other two cases the QKD source is sending light upward to the ceiling with a wider beam angle. As for the receiver, we assume that its telescope is dynamically rotating to collect the maximum power from the user in the three cases. We assume that the effective receiver's FOV would correspond to the numerical aperture (NA) of a single-mode fiber. For single-mode fibres, NA is about 0.1, which means that the corresponding FOV that can be coupled to the fiber is around 6°. Here, the QKD receiver's FOV is assumed to be 6° in order to maximize the collected power.

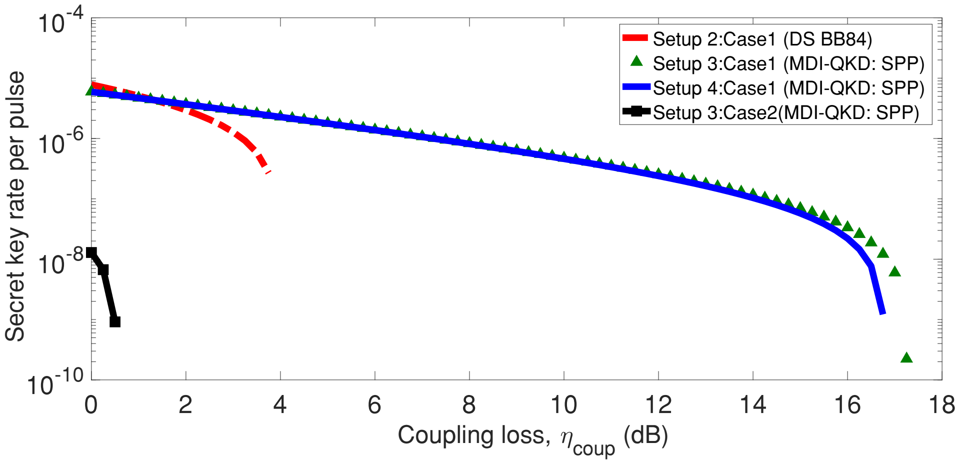

Figure 5.7: The secret key rate per pulse versus the coupling loss, η_{coup}, in dB, in setups 2, 3 and 4 in cases 1 and 2. The QKD source is placed at the centre of the room in case 1, while it is moved to a corner of the room in case 2, with semi-angle at half power of $\Phi_{1/2} = 20°$ in both cases. Receiver's FOV is 6°. The decoy-state and MDI-QKD protocols are used for secret key rate analysis. The bulb's PSD in cases 1 and 2 is 10^{-7} W/nm and 10^{-8} W/nm, respectively. The fiber length (L_0) is 10 km. (DS: Decoy state; SPP: Single-photon pulse.)

The first thing we study here is whether the loose alignment in cases 1 and 2 would be sufficient for the proper operation of a networked wireless link. The short answer turns out to be negative for setups 2–4. We already know the result for setup 1 from the previous work in chapter 4 Elmabrok *et al.* [2018], in which we show that, if the only source of lighting in the room is an LED bulb with a PSD on the order of 10^{-5}–10^{-6} W/nm, then there will be regions over which even in cases 1 and 2 the wireless user can exchange secret keys with the Rx box.

This seems to no longer necessarily hold if we remove the trusted relay node in the room. In Fig. 5.7, we have plotted the secret key rate versus the coupling loss for setups 2 to 4. While for a user in the centre of the room, it may be marginally possible to exchange keys at PSD = 10^{-7} W/nm, once the user moves to the corner, the required PSD drops to 10^{-8} W/nm. This is not strange as in setups 2–4, we have more loss and additional sources of noise as compared to setup 1. The required parameter values may not, however, be achievable in practical settings, and that implies that dynamic beam steering may be needed at both the transmitter and the receiver side of a wireless QKD link.

There are several other observations that can be made from Fig. 5.7. We have verified that the MDI-QKD with DS has a rather poor performance, and in order to tolerate substantial coupling loss, we need to use nearly ideal single-photon sources. It can also be seen that the performance of setups 3 and 4 is more or less the same. As expected, moving the BSM module around does not make a big difference in the key rate. Setup 3 has slightly better performance for the parameter values chosen here, partly because setup 4 might have slightly more Raman noise, as will be shown later. But, overall, if one needs to go with a trust-free relay node, its position can be decided based on the operational convenience without sacrificing much of the performance. In forthcoming graphs, we then only present the results for setup 3.

The situation is much more optimistic if full alignment, with $\Phi_{1/2} = 1°$, between the wireless QKD receiver and transmitter is attained (case 3). In this case, the QKD source is located at a corner of the room and transmits directly to the QKD receiver or the collector. The full alignment for this narrow beam would highly improve the channel transmissivity. Figure 5.8(a) shows key rate versus coupling loss at a PSD of 10^{-5} W/nm. It can be seen that coupling loss as high as 35 dB can be tolerated in certain setups. That leaves a large budget for loss in different elements of the system. As compared to Fig. 5.7, the rate has also improved by around three orders of magnitude. For a fixed coupling loss of 10 dB, Fig. 5.8(b) shows how the remaining loss budget can be used to reach farther central offices. It seems that tens of kilometers are reachable with practical decoy-state signals in all setups. In this figure, we have also shown the total key rate for setup 1, which can serve as a benchmark for other setups. For

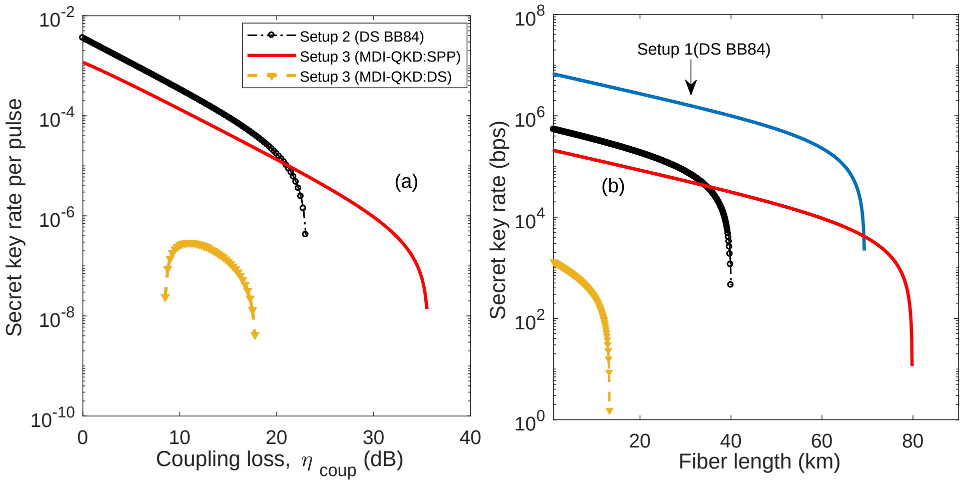

Figure 5.8: The secret key rate for setups 1–3 in case 3, in which the full alignment between the QKD node on the ceiling and wireless transmitter is obtained. The QKD source is placed at a corner of the room's floor, with semi-angle at half power $\Phi_{1/2} = 1°$. Receiver's FOV is 6°. (a) The secret key rate per pulse versus the coupling loss, η_{coup}, in dB. Fiber length is $L_0 = 10$ km and PSD is 10^{-5} W/nm. (b) The total secret key rate in bps versus L_0 when the coupling loss is 10 dB, PSD is 10^{-5} W/nm, and the repetition rate is 1 GHz. (DS: Decoy state; SPP: Single-photon pulse.)

a repetition rate of 1 GHz, keys can be exchanged at a total rate ranging from kbps to Mbps at moderate distances.

There are additional interesting, but somehow puzzling, points in Fig. 5.8. For instance, in Fig. 5.8(a), the MDI-QKD curve with DS implies that no secret keys can be exchanged at low coupling losses. This is counter-intuitive. But, we have verified that the same behavior is seen in asymmetric MDI-QKD systems, when one user's, let's say Alice, signal is accompanied by a background noise. Such a background noise would therefore undergo the same amount of loss as the Alice signal. In a particular regime, where the background noise is comparable to Bob's rate of photon arrival at the BSM module, such background photons could masquerade Bob's photons and cause errors. In setup 3, the background noise that accompanies Alice's signal is that of the bulb noise. If we make the coupling loss very low, such a noise would easily get into our BSM module and

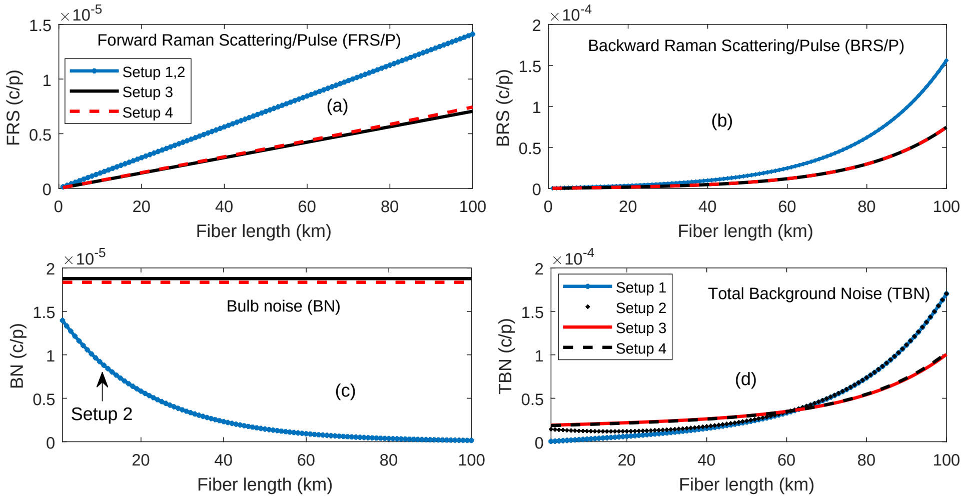

Figure 5.9: Noise counts per detector due to (a) forward Raman scattering, (b) backward Raman scattering, (c) the artificial lighting source, and (d) the total background noise n_N, all in count per pulse (c/p), versus L_0. The bulb's PSD is 10^{-5} W/nm and η_{coup} is 10 dB.

can cause errors. This explains the strange behavior of the MDI-QKD curve in Fig. 5.8(a). Another detailed point is in Fig. 5.8(b), in which the maximum security distance for setup 2, with 10 dB of coupling loss, is 40 km. In that case, one may expect that the security distance for setup 1, with no coupling loss should be 50 km (corresponding to 10 dB of fiber loss) longer, i.e., 90 km. The difference is, however, around 25 km. This turns out to be because of the additional Raman noise at longer distances. In order to understand this and the previous observation better, we need to explore the noise characteristic of the system, as we do next.

In Fig. 5.9, we have plotted the noise counts per detector due to (a) forward Raman scattering (FRS), (b) backward Raman scattering (BRS), (c) the lighting source bulb, and (d) the total background noise n_N for each setup. In each setup, the (a)–(c) noise components have been obtained from the corresponding expression for n_N by breaking it into its individual terms. There are several observations to be made. In terms of order of magnitude, all three sources of noise in Figs. 5.9(a)-(c), are larger or comparable to dark count noise per pulse, where the latter in our setup is 10^{-7}/pulse. This proves the relevance of our analysis that accounts for Raman and background noises. In Fig. 5.9(a,b), the FRS and BRS increase with distance. This is because of the launch power control scheme in use, which requires the data transmitters to send a larger amount of power proportional to the channel loss. The effect of FRS is, however, less than that of BRS, which is roughly one order of magnitude higher than FRS. BRS increases with fiber length because of the power control scheme, and will be the major source of noise in long distances. This increase in BRS justifies the shorter-than-expected security distances in Fig. 5.8(b). Finally, it can be seen that why MDI-QKD setups are more vulnerable to bulb noise than the DS system of setup 2. The bulb noise would enter the BSM module in setups 3 and 4 by mainly being attenuated by the coupling loss, whereas in setup 2, it will be further attenuated by the channel loss. That is partly why the rate in setup 2 can be higher than that of setups 3 and 4. Based on these results, one can conclude that, if the MDI property is not a crucial design factor, setup 2 could offer a reasonable practical solution to the scenarios where a trusted relay is not available. In the rest of this section, we will then compare the performance of different protocols that can be run in setup 2.

Figure 5.10 compares the GG02 performance in setups 1 and 2 with DS-BB84. In Fig. 5.10(a) we study the resilience of either scheme against background noise at low values of coupling loss. As has been shown for fibre-based systems Qi *et al.* [2010a], CV-QKD can tolerate a higher amount of background noise in this regime due to the intrinsic filtering properties of its local oscillator. That benefit would however go away if the coupling loss roughly exceeds 8 dB in our case; see Fig. 5.10(b). This implies that full beam steering is definitely a must when it comes to CV-QKD. Depending on the setting of the system, the operator can decide whether a DV or a CV scheme is the better option.

Figure 5.11 shows the relevant regimes of operation for DV and CV-QKD schemes in a different way. In Fig. 5.11(a), we have looked at the maximum coupling loss tolerated by each of the two schemes for a given background noise. It is clear that while for low values of coupling loss, CV-QKD can tolerate more noise, at high values of coupling loss DV-QKD is the only option, although it can tolerate less noise. There is therefore a trade-off between the amount of coupling loss versus background noise the system can tolerate. In Fig. 5.11(b), we have

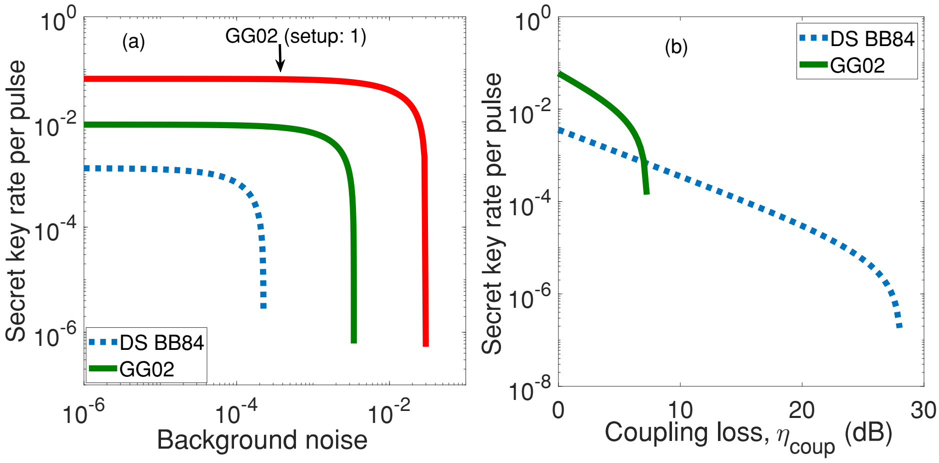

Figure 5.10: Comparison of the GG02 and DS-BB84 protocols for setup 2 and case 3 (except for the curve labeled GG02 (setup 1)). (a) Secret key rate per pulse versus total background noise. The latter is assumed to be per detector for DV-QKD, while it is per spatio-temporal mode for CV-QKD. (b) Secret key rate per pulse versus coupling loss, η_{coup}, in dB. The coupling loss in (a) is 5 dB for setup 2 and 0 dB for setup 1. The keys exchange in setup 1 is performed via a trusted relay point between the sender and the recipient, as explained in section 5.2.1. In setup 2, however, it is accomplished without a relay point, in the sense that the signals transmitted by Alice are collected by a telescope and coupled to a single-mode fiber to be sent to the central office. There is therefore no coupling loss (0 dB) in setup 1, whereas 5 dB is assumed for setup 2. The shared fiber length (L_0) is 10 km. The used bulb's PSD is 10^{-5} W/nm.

compared the two systems from the clock rate point of view. CV-QKD is often practically constrained by its low repetition rate. In Fig. 5.11(b), we have fixed the CV repetition rate to 25 MHz Wang *et al.* [2015a] and have found out at what clock rate the DV system offers a higher total key rate than the CV one. For numerical values used in our simulation this cross-over rate is around 200 MHz, which is achievable for today's DV-QKD systems. The ultimate choice between DV and CV would then depend on the characteristics of the system, such as loss and noise levels, as well as the clock rate available to the QKD system.

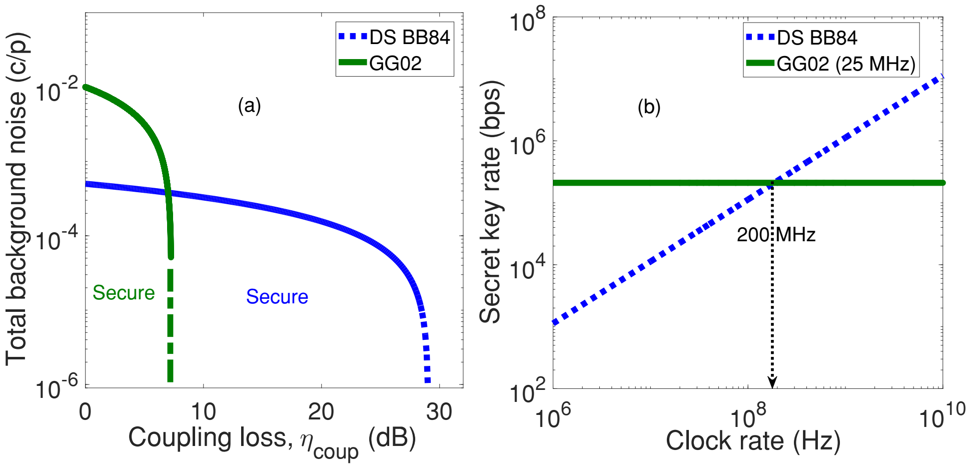

Figure 5.11: (a) Regions of secure operation for DV-QKD (DS-BB84) and CV-QKD (GG02) protocols for setup 2 (case 3). The curves show the maximum tolerable background noise at different values of coupling loss, η_{coup}, in dB. The background noise is calculated per detector for DV-QKD, while it is per spatio-temporal mode for CV-QKD. (b) Comparison of the two systems from the clock rate point of view when the CV repetition rate is fixed to 25 MHz. In (a) and (b), $L_0 = 10$ km. In (b), coupling loss is 5 dB and PSD is 10^{-5} W/nm.

5.5 Summary

We proposed four practical setups that would facilitate the access part in a hybrid quantum-classical network. This included scenarios of trusted relay, direct coupling and untrusted relay between the sender and the recipient. We considered DV and CV-QKD protocols for the secret key analysis. We considered the fiber background noise induced by Raman scattering, as well as the loss and background noise in indoor environments. The asymptotic scenario of an infinite number of signals was assumed in our analysis. It is important now to study the practical case where a finite number of signals are exchanged between two legitimate users. This will be studied in the following chapter.

Table 5.1: Nominal values used for our system parameters.

System Parameters	**Nominal value**
Number of users, N	32
Fiber attenuation coefficient, α, α_r	0.2 dB/km, 0.046 /km
AWG insertion loss, Λ	2 dB
Room size, X,Y,Z	$(4 \times 4 \times 3)$ m^3
Semi-angle at half power of the bulb	70°
Reflection coefficients of the walls and floor	0.7
Detector area	1 cm^2
Refractive index of the concentrator	1.5
Semi-angle at half power of QKD source, $\Phi_{1/2}$	20°, 1°
DV-QKD Parameters	**Nominal value**
Average number of photons per signal pulse, $\mu = \nu$	0.5
Error correction inefficiency, f	1.16
Dark count per pulse, n_{dc}	10^{-7}
Detector gate width, T_d	100 ps
Relative-phase error probability, e_d	0.033
Quantum efficiency of detector, η_{d1}, at 880 nm	0.6
Quantum efficiency of detector, η_{d2}, at 1550 nm	0.3
CV-QKD Parameters	**Nominal value**
Reconciliation efficiency, β	0.95
Receiver overall efficiency, η_B	0.6
Electronic noise (shot noise units), v_{elec}	0.015
Excess noise (shot noise units), $\varepsilon_q^{\mathrm{rec}}$	0.002

Chapter 6

Finite Size Analysis

6.1 Introduction

In the previous chapters, we considered the asymptotic scenario where infinitely many signals we assumed to be exchanged between Alice and Bob. The assumption of emitting signals for an infinitely long time is impractical, but it would help us compare the performance and the feasibility of different protocols. In the asymptotic regime, all required key parameters can, in principle, be obtained from the observed measurement results without any statistical errors. For instance, if we are interested in estimating error probability, in the asymptotic limit, the ratio between the number of bits in error and the total number of transmitted bits would give us the corresponding probability. In real-life QKD, however, Alice would send out a finite number of signals over a certain period of time, and that will cause statistical fluctuations in parameter estimation. It is thus important to account for such fluctuations when a finite size of signals is considered in comparison with the asymptotic limit. In this chapter, we study such a finite-size key scenario by comparing the performance of DV and CV-QKD for different data block sizes for wireless indoor QKD. We specify the minimum block size of keys that offers practical indoor services. Based on our proposed setups, explained in the previous chapter, we will investigate the implications this issue in AES systems that rely on QKD for refreshing their seed keys.

QKD can be used to change the session key of AES in a practical setting. The key feature of the latter algorithm is that it can encrypt a large volume of data with a short key. This is interesting in contrast to OTP, for which the length of encryption key has to be the same as the message to be sent. AES keys need to be refreshed by a certain frequency as required by the application. That would have implications on the QKD system that supports such an AES application. For instance, for a 256-bit AES with a key refresh rate of 100 times per second, we would need a secure key rate of 25.6 kbps for the QKD system. In the following, after describing the system, we provide some numerical results for secret key rates in setup 2 (case 3) in Fig. 5.3 by taking into account finite size effects for DV and CV-QKD protocols

6.2 System description

We continue on analysing the same proposed setups, particularly, setup 2 in Fig. 5.3, and apply the finite-key analysis. As explained earlier, Alice, the sender, is located in a window-less room of $X \times Y \times Z$ dimensions, lit by an artificial light source. The mobile QKD transmitter is placed on the floor and it transmits light toward the ceiling. The signal collector is fixed at the center of the room's ceiling; see Fig. 5.1. We consider setup 2 (case 3) in the settings where full alignment between the collector and the transmitter is attained. This alignment is advantageous, as it would highly improve the channel transmissivity. In setup 2, the signals transmitted by Alice are collected by a telescope and coupled to a single-mode fiber to be sent to the central office. QKD signals, sent through wireless indoor channels, are combined with classical ones and sent over shared fiber links to the QKD receiver using DWDM. For encoding the quantum states, we assume that time-bin encoding techniques is in use, as they offer certain advantages in both fiber and free-space QKD systems. In particular, they may suffer less from alignment issues as compared to polarization-based encoding in wireless environments.

Setup 2 is of interest to be studied in Chapter 6, as it is the most practical solution when the relay node cannot be trusted. This is the case when the user is in a public space, e.g., a cafe, a bank, or an airport. The MDI-QKD solution in setups 3 and 4 imposes demanding conditions on the quality of source and channel stabilisation as it requires photon indistinguishability for the BSM part.

We also focus on case 3, which is somehow the worst location for the user, hence our results would indicate the minimum key rate that can be obtained. As we have shown earlier, the performance would highly be enhanced if beam steering is in use, which is what we assume to improve the channel transmittance after undergoing additional coupling loss.

The performance of finite-size DV-QKD protocol is quantified here by applying the secret key rate analysis in Zhang *et al.* [2017b]. This paper provides a tight bound for the decoy-state method (see the Appendix E.1). A rigorous statistical fluctuation analysis has been presented in order to account for the finite-size effects. As for CV-QKD, we use the analysis in Zhang *et al.* [2017a], where the finite-size effects have been accounted for in a simple way; see Appendix E.2. The nominal parameter values used in our simulation are summarized in Table 5.1. In the following, we present some results for both protocols when different block sizes of data are considered.

6.3 Results and discussion

The results in this section are the extension of the work in the previous chapters, but with examining the finite-key scenario. We consider the adverse effects of the background noise induced by Raman-scattered light on the QKD receivers due to integration with classical channels. In addition, we consider the loss and the background noise that arise from indoor environments, as already explained. In our numerical results, we optimise a set of parameters, which could be tuned experimentally, in order to bound the optimal secure key rate. The optimization is important, since for instance, if the average number of photons per pulse, μ, set to be too high, this would result in dropping the key rate due to the potential multiphoton states. Similarly, the corresponding key rate would drop when μ, set to be very low. This is due to the increase in the ratio between the dark counts and the signal states. As a result, μ must be optimised in order to obtain the best possible performance.

Figs. 6.1 and 6.2 show the secret key rate per pulse versus the coupling loss (dB) for different block sizes of data, when the fiber link is $L_0 = 10$ km and the bulb's PSD is 10^{-5} W/nm. The two figures depict the results of the relevant regimes of operation for DV and CV-QKD schemes, respectively. As we saw before, the key rate in CV-QKD, see Fig. 6.2, is higher than its counterpart in Fig. 6.1 at low values of coupling loss. This is because that, in CV-QKD, there is always an output due to the homodyne measurement, while, in DV-QKD, the transmitted photon must arrive in order to be accounted for. In DV-QKD, the detector efficiency has a major impact on the generated key rate in comparison with CV-QKD where the detection efficiency does not have a noticeable effect on the key rate. In addition, it is apparent that CV-QKD is less tolerant to loss than DV-QKD. The impact of loss on CV-QKD systems is severe since the difference between Alice and Eve information about Bob's key quickly drops and unless we have super efficient post-processing schemes, we cannot extract a secret key out of the difference. A short block size would, however, make the margin of acceptable coupling loss within which CV-QKD can operate even narrower.

In Table 6.1, we show how the size of data can affect the time spent for key exchange. The figures in the table are based on the DV-QKD rates in Fig. 6.1, when the coupling loss is 10 dB and the repetition rate is 1 GHz. We show the length of the secure key and time spent for exchanging such keys. From a practical point of view, DV-QKD would be better in comparison with CV-QKD; see Fig. 6.2. This is because that it is less vulnerable to the loss, as well as having a reasonable acquisition time for a practical size of data. Indeed, the acquisition time is an important factor, and its practicality depends on the application in use. For example, a bank customer that uses an AES protocol, supplemented by QKD generated seeds, for banking transactions, waiting for a few seconds could be reasonable. In that sense, the numbers in Table 6.1 suggest that our proposed wireless indoor QKD systems can provide a sufficient number of key bits within a sensible duration.

It is clear from Table 6.1, that the required time to collect the transmitted data is increasing proportionally to the block size of data. In which case, the higher block size of data, the longer acquisition time for data collection. From a practical point of view, it might be better to exchange a small block size between intended users in certain applications. This is important, as it results in establishing a session of key exchange in a short practical time with a reasonable secret key rate.

Block size (bits)	$N = 10^9$	$N = 10^{10}$	$N = 10^{12}$	$N = \infty$
Key rate/pulse	4.65×10^{-5}	1.01×10^{-4}	1.53×10^{-4}	1.83×10^{-4}
Length (secure) key	46.5 kbits	1.01 Mbits	153 Mbits	∞
Acquisition time	1 sec	10 sec	1000 sec	∞

Table 6.1: Comparison between different block sizes and the corresponding secret key rate, as well as the time spent for exchanging the key for DV-QKD. We consider a repetition rate of 1 GHz. We assume that the coupling loss is 10 dB and the length of the shared fiber length (L_0) is 10 km.

The minimum block size of keys that offers practical indoor services for the practical scheme, DV-QKD, would be $N = 10^9$. This is the minimum block size that would tolerate the loss including the coupling loss. It is clear that for setup 2, DV-QKD is more practical, as it would tolerate more loss in comparison to CV-QKD. In addition, DV-QKD is more practical due to the availability of high clock rates. For instance, for $N = 10^9$, the acquisition time for DV-QKD, when the clock rate is 1 GHz, is 1 s; see Table 6.1. However, for CV-QKD, where the clock rate is limited Wang *et al.* [2015a], Zhang *et al.* [2017a], the acquisition time might be much longer.

6.4 Summary

We studied a practical scenario for wireless indoor QKD, where a finite size of data is exchanged between remote users. We assessed and compared the performance of DV and CV-QKD protocols. This is done by considering different block sizes, and computing the corresponding secret key rate, as well as the time spent for exchanging the keys. We conclude that using DV-QKD we can establish a sufficiently long key in a reasonable time of a few seconds. This further indicates the practicality of wireless indoor QKD setups.

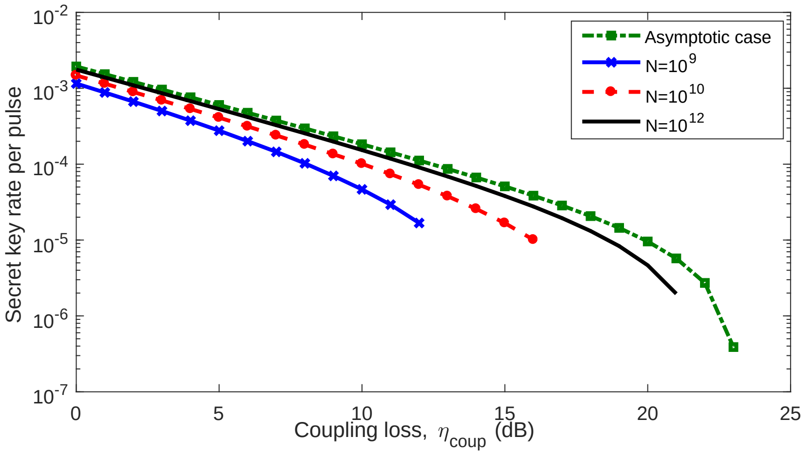

Figure 6.1: The secret key rate per pulse versus the coupling loss (dB) for setup 2 (case 3), considering different block sizes using DV-QKD (DS-BB84). The QKD source is placed at a corner of the room's floor, with semi-angle at half power $\Phi_{1/2} = 1°$, and receiver's FOV is 6°. Fiber length is $L_0 = 10$ km and the bulb's PSD is 10^{-5} W/nm.

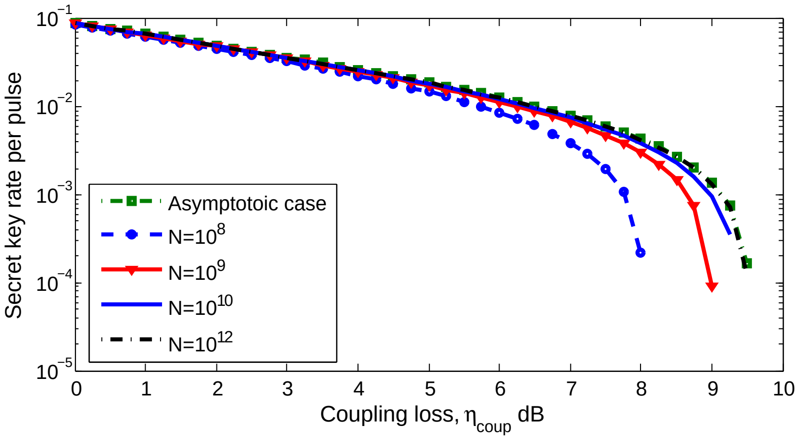

Figure 6.2: The secret key rate per pulse versus the coupling loss (dB) for setup 2 (case 3), considering different block sizes using CV-QKD (GG02). The QKD source is placed at a corner of the room's floor, with semi-angle at half power $\Phi_{1/2} = 1°$, and receiver's FOV is 6°. Fiber length is $L_0 = 10$ km and the bulb's PSD is 10^{-5} W/nm.

Chapter 7

Conclusions and future work

7.1 Conclusions

We studied the feasibility of wireless indoor QKD in a window-less room lit by an artificial source. Such systems could provide the first link within a larger quantum network or facilitate the use of QKD in common areas for many users. We showed that there would exist a practical regime of operation within which such a wireless QKD system could generate secret keys in indoor environments. We used optical wireless communications models to characterize the path loss and background noise in the channel. Our results showed that with even mild assumptions on the alignment of the QKD transmitter and receiver, it would be possible to exchange secret keys if the room is lit by white LED bulbs. Such light sources have very little power spectral density at the operating wavelengths of interest for a QKD system, and because of their low energy consumption are expected to be ubiquitously used in the future. Our results further showed that additional enhancement could be obtained if beam steering techniques were employed.

The type of equipment needed for the above setup is within reach of our current quantum and classical technologies. With recent progress in integrated QKD devices Ma *et al.* [2016], Sibson *et al.* [2017], Vest *et al.* [2015], it is possible to think of a portable device equipped with QKD capabilities. A handheld QKD prototype has, in fact, already been implemented for short-range handheld-to-ATM key exchange Chun *et al.* [2017], Duligall *et al.* [2006]. Because of high path loss in integrated optics systems, the integration requirement for time-bin encoding may be harsher than that of polarization encoding. One can, however, think of hybrid solutions where an integrated dual-rail setup is used for the initial encoding, which will then be converted to a single-rail time bin encoding using an external delay line. We also need random number generators. In many scenarios, we can generate random bits offline, store them on the device, and use them during the key-exchange protocol. As for the QKD receiver, we can use some of the existing technologies for Li-Fi for collection and alignment. For instance, we can use a non-imaging optical concentrator, such as a compound parabolic collector, followed by a bandpass filter at the receiver. The output of the phase-decoding interferometer is then passed to one of the two single-photon avalanche diodes. Such detectors have also been considered for use in Li-Fi systems Chitnis & Collins [2014]. Overall, with the progress made toward implementing QKD modules with integrated optics along with the progress in beam steering in classical optical communications Gomez *et al.* [2015], our proposed system can enable high-rate wireless access to future quantum-classical networks Elmabrok & Razavi [2016].

We also proposed and studied four configurations that enabled wireless access to hybrid quantum-classical networks. All these setups included an initial wireless indoor link that connected a quantum user to the network. Each user in the access network could also communicate classically with the central office via another wavelength in the same band. We considered setups in which a local relay point could be trusted as well as setups where such trust was not required. We showed that with proper beam alignment it was possible, in both DV- and CV-QKD, to achieve positive key rates for both trusted and untrusted relay points in certain indoor environments.

The choice of the optimum setup would depend on various system parameters, which we studied in our analysis. For instance, we found that our MDI-QKD setups, which offered trust-free QKD immune to measurement attacks, were mostly insensitive to the positions of their measurement modules, but could suffer harshly from the background noise generated in the indoor environment. If immunity to measurement attacks was not required, we could simply collect QKD signals at the ceiling and couple them into optical fibers along with other data channels. With decoy-state techniques, we showed that we could tolerate up to 30 dB of coupling loss in such a setting, provided that full alignment is achieved. At long distances, the Raman noise induced by the data channels would also take its toll on the maximum secure distance, limiting it to tens of kilometers. Both Raman noise and the background noise due to the artificial light source in the indoor environment could be orders of magnitude larger than the static dark count of single-photon detectors. We also showed that in the low-coupling-loss regime, CV-QKD could offer higher rates and more resilience to background noise than DV-QKD systems. But, overall, DV-QKD schemes could offer a more stable and flexible operation adaptable to a wider range of scenarios. In short, using our analytical results, we can identify the winner in realistic setups that enable high-rate wireless access to future quantum networks.

In order to have a practical system, we need to apply the finite-key analysis to our proposed configurations. We compared the performance of DV and CV-QKD in setup 2 (case 3) over a range of data block sizes. We show that to what extent the block size of keys can be practical in wireless indoor QKD. It turns out that DV would outperform CV-QKD. The reason is that DV-QKD is less vulnerable to the loss, as well as having a reasonable acquisition time for a practical size of data.

7.2 Future work

Setups 1 and 3 should be examined with a finite size of data, to evaluate their practicality. These setups are useful for end users in certain scenarios as already explained. Setup 1 is of interest whenever a trusted node between the sender and the recipient exists. This can be inside a building where a QKD relay node can be physically secured. Setup 3, however, is applicable whenever the relay point in indoor environment is not secure for wireless users. This is in places such as a coffee shop or an airport, where users may not necessarily trust the owners of the local system. It is interesting if a wireless localization system Raharijaona *et al.* [2017], Zhang *et al.* [2010] is considered in such places. This is important to improve the channel transmittance and also to reduce the impact of background noise, due to the established alignment. A new direction of this research could be by employing indoor positioning systems for wireless indoor QKD. This would involve reference wireless nodes which are placed in fixed positions, a QKD receiver in our case, and mobile nodes, such as laptops, in which a QKD source is embedded. A real-time tracking system Dardari *et al.* [2015] can also be exploited for freely movable users.

The secret key rate for a QKD scheme is essential for assessing its performance. For the sake of improving the key rate, quantum information can be encoded using the orbital angular momentum (OAM) of light. This degree of freedom of a single photon is exploited for multidimensional QKD Djordjevic [2013], where qudits are mapped into a single photon. As a result, a single photon can transfer more than 1 bit of information. For wireless indoor QKD, digital micro-mirror devices (DMD) can be used to generate rapidly the desired spatial modes for a high dimensional QKD system Mirhosseini *et al.* [2015]. This can be accomplished by diffracting individual photons from a plane-wave state produced by a normal laser. Another possible solution to improve the key rate is by employing existing schemes such as multiple-input and multiple-output (MIMO) technique for QKD Gabay & Arnon [2006]. Both methods would allow many independent data streams to be transmitted over the same spatial wireless channel.

Our results could be the motivate to researchers for experimental realization of wireless indoor QKD, to be ready for commercial applications. Many QKD experiments have been implemented, such as Bacco *et al.* [2013], Zhao *et al.* [2006], and the main ingredients, from attenuated laser pulses to single photon detectors, are already available. It has been shown in recent work Rusca *et al.* [2018] that using the 1-decoy approach Rusca *et al.* [2018] is advantageous in comparison with the 2-decoy system Ma *et al.* [2005]. The 1-decoy state QKD protocol would simplify the QKD encoder and make it cheaper. Indoor optical wireless communications with a higher capacity, has also been implemented Gomez *et al.* [2015]. This would ease the full implementation of combining QKD and OWC.

Appendix A

DS-BB84 key rate analysis

In this appendix, the secret key generation rate of the DS-BB84 protocol is calculated. The lower bound for the key rate, in the limit of an infinitely long key, is given Ma *et al.* [2005]

$$R_{\text{decoy}} \geqslant q\{Q_1(1 - h(e_1) - fQ_\mu h(E_\mu)\}, \tag{A.1}$$

where q is the basis-sift factor, which is equal to $1/2$ in the original BB84 protocol. This is due to discarding half of the detection events in X and Z bases after the sifting procedure. Here, we use the efficient BB84 protocol Lo *et al.* [2005], which allows us to choose unevenly between X and Z bases, in which case q can approach 1. If infinite number of decoy states are used, the parameters in (A.1) are given as follows: Q_1, which is called the single-photon gain, is the probability that Bob gets a click and Alice has sent one photon, and it is given by:

$$Q_1 = Y_1 \mu e^{-\mu}, \tag{A.2}$$

where μ is the average number of photons per pulse for the signal state and Y_1 is the yield of single photons. The latter is defined as the probability of getting a click provided that Alice has sent exactly a single photon, which is given by:

$$Y_1 = 1 - (1 - \eta)(1 - n_N)^2, \tag{A.3}$$

where η is the total system transmittance given by $\eta_d H_{\text{DC}}/2$ (the factor $1/2$ represents the loss incurred in a passive time-bin decoder), and n_N is the total noise per detector given by n_B+n_D, where n_D is the dark count rate per pulse for each of the two single-photon detectors at the Bob's receiver. As for dark count noise or dark current noise, the detector tends to click despite the absence of light. The dark count rate (γ_{dc}) varies from one detector to another. For instance, it ranges from (100-1000)/s for an APD, to (1-100)/s for superconducting detectors Dusek *et al.* [2006]. The average dark count over a period (τ) is then: $n_D = \gamma_{dc}.\tau$. $n_B = n_B^{(1)} + n_B^{(2)}$; e_1 is the error probability in the single-photon case, and is given by:

$$e_1 = \frac{e_0 Y_1 - (e_0 - e_d)\eta(1 - n_N)}{Y_1}, \tag{A.4}$$

where $e_0 = 1/2$ and e_d models the error, caused by channel distortions, in the relative phase between the two pulses generated by the phase encoder; Q_μ is the probability that Bob gets a click, when Alice has sent a coherent state with an average number of photons μ, and, it is given by Panayi *et al.* [2014]:

$$Q_\mu = 1 - e^{-\eta\mu}(1 - n_N)^2. \tag{A.5}$$

In (A.1), the overall QBER is represented by E_μ, and it is given by

$$E_\mu = \frac{e_0 Q_\mu - (e_0 - e_d)(1 - e^{-\eta\mu})(1 - n_N)}{Q_\mu}. \tag{A.6}$$

Finally, $h(x)$ is the Shannon binary entropy function given by

$$h(x) = -x\log_2 x - (1 - x)\log_2(1 - x). \tag{A.7}$$

If we use a two-decoy-state protocol, such as vacuum+weak, Y_1, Q_1, and e_1 are, respectively, bounded by Ma *et al.* [2005]

$$\begin{aligned} Y_1 \geqslant Y_1^{L,\nu_1,\nu_2} = &\frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}[Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} \\ &- \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)], \end{aligned} \tag{A.8}$$

$$\begin{aligned} Q_1 \geqslant Q_1^{L,\nu_1,\nu_2} = &\frac{\mu^2 e^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}[Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} \\ &- \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)], \end{aligned} \tag{A.9}$$

and

$$e_1 \leq e_1^{U,\nu_1,\nu_2} = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^{L,\nu_1,\nu_2}}, \tag{A.10}$$

where ν_1 and ν_2 are the average number of photons per pulse for the decoy states signals; Q_{ν_1} and Q_{ν_2} can be obtained from (12); E_{ν_1} and E_{ν_2} are the overall QBER for decoy-state signals given by (13). In the above equations, Y_0 is the probability of having a click due to the background and/or dark count noise, whose lower bound is given by

$$Y_0 \geqslant Y_0^L = \max\{\frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0\}. \tag{A.11}$$

The above lower (L) or upper (U) bounds can be used in (A.1) to find a lower bound on the key rate.

Appendix B

RFI-QKD key rate analysis

In RFI-QKD, the correlation quantity, C, is used to estimate Eve's information, and it is defined by Laing *et al.* [2010b]

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2, \tag{B.1}$$

which can be written as Wang *et al.* [2015b]

$$C = (1 - 2E_{XX})^2 + (1 - 2E_{XY})^2 + (1 - 2E_{YX})^2 + (1 - 2E_{YY})^2, \tag{B.2}$$

where E terms represent error rates in different scenarios. It can be shown that C is independent of ξ. For our numerical analysis, ξ is then assumed to be zero. In this case, we can assume that $E_{XY} = E_{YX} = 1/2$, and $E_{XX} = E_{YY} = E_{ZZ} = e_1$, where e_1 is the error probability in the single-photon case as calculated in (A.4). The parameter C can then be calculated by

$$C = 2(1 - 2e_1)^2. \tag{B.3}$$

Eve's information is bounded by Laing *et al.* [2010b]

$$I_E = (1 - e_1)h[\frac{1 + \nu_{\max}}{2}] + e_1 h[\frac{1 + f(\nu_{\max})}{2}], \tag{B.4}$$

where $\nu_{\max}$ and $f(\nu_{\max})$, respectively, are given by

$$\nu_{\max} = \min[\frac{1}{1 - e_1}\sqrt{C/2}, 1], \tag{B.5}$$

and

$$f(\nu_{\max}) = \frac{\sqrt{C/2 - (1-e_1)^2\nu_{\max}^2}}{e_1}. \tag{B.6}$$

By substituting (B.3) in the above equations, I_E is then given by

$$I_E = e_1 + (1-e_1)h[(1-3e_1/2)(1-e_1)]. \tag{B.7}$$

The estimated key generation rate for RFI-QKD with decoy-state technique is then given by Wang *et al.* [2015b]

$$R \geqslant -Q_\mu f h(E_\mu) + Q_1(1-I_E), \tag{B.8}$$

where Q_μ, E_μ, e_1, and Q_1 are the same as those given for the decoy-state BB84 protocol.

Appendix C

MDI-QKD key rate analysis

In this appendix, we summarize the secret key rate of the MDI-QKD protocol. The rates for the ideal single-photon source and the decoy-state protocols, respectively, are

$$R^{\mathrm{SPP}}_{\mathrm{MDI-QKD}} = Y_{11}[1 - h(e_{11:X}) - fh(e_{11:Z})] \tag{C.1}$$

and

$$R^{\mathrm{DS}}_{\mathrm{MDI-QKD}} = Q_{11}(1 - h(e_{11;X})) - fQ_{\mu\nu;Z}h(E_{\mu\nu;Z}). \tag{C.2}$$

In the above, Q_{11} is the gain of the single-photon states given by

$$Q_{11} = \mu\nu e^{-\mu-\nu}Y_{11}, \tag{C.3}$$

where μ (ν) is the mean number of photons in the signal state sent by Alice (Bob) and Y_{11} is the yield of the single-photon states given by

$$\begin{aligned} Y_{11} =&(1 - n_N)^2[\eta_a\eta_b/2 + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)n_N \\ &+ 4(1 - \eta_a)(1 - \eta_b)n_N^2], \end{aligned} \tag{C.4}$$

where n_N represents the total noise per detector and η_a and η_b are, respectively, the total transmittance between Alice and Bob sides and that of Charlie Panayi *et al.* [2014]. In (C.1) and (C.2), $e_{11;Z}$, $e_{11;X}$, $Q_{\mu\nu;Z}$ and $E_{\mu\nu;Z}$, respectively, represent the QBER in the Z basis for single-photon states, the phase error for single-photon states, the overall gain and the QBER in the Z-basis, which are given by Panayi *et al.* [2014]:

$$\begin{aligned}
e_{11;X}Y_{11} =& Y_{11}/2 - (1/2 - e_d)(1 - n_N)^2\eta_a\eta_b/2, \\
e_{11;Z}Y_{11} =& Y_{11}/2 - (1/2 - e_d)(1 - n_N)^2(1 - 2n_N)\eta_a\eta_b/2, \\
Q_{\mu\nu;Z} =& Q_C + Q_E, \\
E_{\mu\nu;Z}Q_{\mu\nu;Z} =& e_dQ_c + (1 - e_d)Q_E,
\end{aligned} \tag{C.5}$$

where

$$\begin{aligned}
Q_C =& 2(1 - n_N)^2e^{-\mu^{'}/2}[1 - (1 - n_N)e^{-\eta_a\mu/2}] \\
& \times [1 - (1 - n_N)e^{-\eta_b\nu/2}] \\
Q_E =& 2n_N(1 - n_N)^2e^{-\mu^{'}/2}[I_0(2x) - (1 - n_N)e^{-\mu^{'}/2}],
\end{aligned} \tag{C.6}$$

with $x = \sqrt{\eta_a\mu\eta_b\nu}/2$, $\mu^{'} = \eta_a\mu + \eta_b\nu$ and I_0 being the modified Bessel function.

Appendix D

GG02 key rate analysis

The secret key rate for GG02 with reverse reconciliation, under collective attacks, is given by Fossier *et al.* [2009]

$$K = \beta I_{AB} - \chi_{BE}, \tag{D.1}$$

where β is the reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, which, for a Gaussian channel, is given by

$$I_{AB} = \frac{1}{2}\log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \tag{D.2}$$

where V and χ_{tot} are, respectively, the total variance and the total noise given by

$$V = V_A + 1, \tag{D.3}$$

with V_A being the variance of Alice's quadrature modulation and

$$\chi_{tot} = \chi_{line} + \chi_{hom}/\eta_{\text{ch}}, \tag{D.4}$$

in which

$$\begin{aligned} \chi_{line} &= \frac{1-\eta_{\text{ch}}}{\eta_{\text{ch}}} + \varepsilon, \\ \chi_{hom} &= \frac{1-\eta_B}{\eta_B} + \frac{v_{elec}}{\eta_B}, \end{aligned} \tag{D.5}$$

are, respectively, the noise due to the channel and the noise stemming from homodyne detection. Also, the parameters η_B, v_{elec}, ε and η_{ch}, are, respectively, Bob's overall efficiency, electronic noise variance induced by homodyne electronic board, excess noise, and the channel transmittance.

In (D.1), χ_{BE} is the Holevo information between Eve and Bob, and it is given by

$$\chi_{BE} = g(\Lambda_1) + g(\Lambda_2) - g(\Lambda_3) - g(\Lambda_4), \tag{D.6}$$

where

$$g(x) = (\frac{x+1}{2})\log_2(\frac{x+1}{2}) - (\frac{x-1}{2})\log_2(\frac{x-1}{2}), \tag{D.7}$$

with

$$\begin{aligned}\Lambda_{1/2} &= \sqrt{(A \pm \sqrt{A^2 - 4B})/2},\\ \Lambda_{3/4} &= \sqrt{(C \pm \sqrt{C^2 - 4D})/2}.\end{aligned} \tag{D.8}$$

In the above equations:

$$\begin{aligned}A =& V^2(1 - 2\eta_{\text{ch}}) + 2\eta_{\text{ch}} + \eta_{\text{ch}}^2(V + \chi_{line})^2,\\ B =& \eta_{\text{ch}}^2(V\chi_{line} + 1)^2,\\ C =& \frac{V\sqrt{B} + \eta_{\text{ch}}(V + \chi_{line}) + A\chi_{hom}}{\eta_{\text{ch}}(V + \chi_{tot})},\\ D =& \sqrt{B}\frac{V + \sqrt{B}\chi_{hom}}{\eta_{\text{ch}}(V + \chi_{tot})}.\end{aligned} \tag{D.9}$$

Appendix E

Finite-Key Analysis

E.1 Decoy-State BB84

The secret key rate for decoy-state BB84, when a finite number of data is considered, is given by Zhang *et al.* [2017b]

$$K^z \geqslant M_1^{szL}[1 - h(e_1^{pszU})] - M^{sz} f h(E^{sz}), \tag{E.1}$$

where M^{sz} and E^{sz} are, respectively, the overall gain and QBER for a given block size of data, N. f is inefficiency of error correction and $h(x)$ is the Shannon binary entropy function given in A.7.

In E.1, in order to compute M_1^{szL} and e_1^{pszU}, which are, respectively, the single-photon gain and the error probability in the single-photon case, we need first to estimate M_1^L and e_1^U. The former is given by

$$M_1^L = Y_1^{*L} N(e^{-\mu}\mu q^s + e^-\nu q^w), \tag{E.2}$$

where q^s and q^w are the rate that Alice encodes a signal state and a decoy state with μ and ν, respectively. N is the block size of data, and Y_1^* is given by

$$Y_1^* \geqslant Y_1^{*L} = \frac{\mu}{\mu\nu - \mu\nu^2}\left(\mathbb{E}^L[Q^w]e^{\nu} - \mathbb{E}^U[Q^s]e^{\mu}\frac{\nu^2}{\mu^2} \quad - \frac{\mu^2 - \nu^2}{\mu^2}\mathbb{E}^U[Q^v]\right). \tag{E.3}$$

In E.3, $\mathbb{E}^L$ and $\mathbb{E}^U$ are the expected values for lower and upper bounds of the measurable quantities. Q^s, Q^w, and Q^v represent the overall gain for signal, decoy, and vacuum states, respectively Zhang *et al.* [2017b].

In order to compute $\mathbb{E}^L$ and $\mathbb{E}^U$ in E.3, we use Chernoff bound Zhang *et al.* [2017b]. In this case, for a measurement result χ, and a failure probability, ε, if χ=0, we use

$$\begin{aligned} \mathbb{E}^L(\chi) &= 0, \\ \mathbb{E}^U(\chi) &= \beta, \end{aligned} \tag{E.4}$$

where $\beta = -\ln(\varepsilon/2)$. If $\chi > 0$, we use

$$\begin{aligned} \mathbb{E}^L(\chi) &= \frac{\chi}{1+\delta^L}, \\ \mathbb{E}^U(\chi) &= \frac{\chi}{1-\delta^U}, \end{aligned} \tag{E.5}$$

where δ^L and δ^U can be obtained by solving

$$\begin{aligned} \left[\frac{e^{\delta^L}}{(1+\delta^L)^{1+\delta^L}}\right]^{\chi/(1+\delta^L)} &= \frac{1}{2}\varepsilon, \\ \left[\frac{e^{-\delta^U}}{(1-\delta^U)^{1-\delta^U}}\right]^{\chi/(1-\delta^U)} &= \frac{1}{2}\varepsilon. \end{aligned} \tag{E.6}$$

If $\chi \geq 6\beta$, δ^L and δ^U in E.6, are computed as

$$\delta^L = \delta^U = \frac{3\beta + \sqrt{8\beta\chi + \beta^2}}{2(\chi - \beta)}. \tag{E.7}$$

By substituting Y_1^* in E.2, M_1^L ia found. Then, in E.1, M_1^{szL}=χ^L for $\overline{\chi} = p_1^s M_1^L$. $\chi^L = (1-\delta)\overline{\chi}$, where

$$\delta = \frac{-\ln(\varepsilon/2) + \sqrt{[\ln(\varepsilon/2)]^2 - 8\ln(\varepsilon/2)\overline{\chi}}}{2\overline{\chi}}. \tag{E.8}$$

In the above equations, a measurement result χ for signals states, can be computed as $M^s = Q^s q^s N$, where Q^s is the overall gain, in a certain basis. The same thing is applicable for decoy and vacuum states. In this case, in E.3, $\mathbb{E}^U[Q^s]$=$\mathbb{E}^U[M^s]/(q^s N)$.

In E.1, the upper bound of the phase error rate e_1^{psz} is given by

$$e_1^{pszU} = e_1^{bxU} + \theta. \tag{E.9}$$

where θ accounts for the error in estimating e_1 Zhang *et al.* [2017b], and e_1^{bxU} can be computed as

$$e_1^U = \frac{(e_1 M_1)^U}{M_1^L} = \frac{(e_1 Y_1^*)^U}{Y_1^{*L}} = \frac{\mathbb{E}^U[E^w Q^w]e^\nu - \mathbb{E}^L[E^v Q^v]}{Y_1^{*L}\nu}, \tag{E.10}$$

where

$$(e_1 M_1)^U = (e_1 Y_1 *)^U N(e^{-\mu}\mu q^s + e^{-\nu}\nu q^w). \tag{E.11}$$

In E.10, $\mathbb{E}^U[E^w Q^w] = \mathbb{E}^U[E^w M^w]/q^w N$, and similarly for $\mathbb{E}^L[E^v Q^v]$.

E.2 GG02

the secret key rate, bounded by collective attacks, is given by Zhang *et al.* [2017a]

$$K = (1-\alpha)(1-FER)[\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{E.12}$$

where $\Delta(n)$ is related to the security of the privacy amplification, and it is computed using Eq. 4 in Leverrier *et al.* [2010], FER is the frame error rate related to the reconciliation efficiency, and α is the system overhead. I_{AB} and χ_{BE} are given in Appendix D.

References

(2010). Id quantique.

(2012). Quantumctek.

Bacco, D., Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. (2013). Experimental quantum key distribution with finite-key security analysis for noisy channels. *Nature communications*, **4**, 2363.

Bahrani, S., Razavi, M. & Salehi, J.A. (2015). Orthogonal frequency-division multiplexed quantum key distribution. *Journal of Lightwave Technology*, **33**, 4687–4698.

Bahrani, S., Razavi, M. & Salehi, J.A. (2016a). Crosstalk reduction in hybrid quantum-classical networks. *Scientia Iranica. Transaction D, Computer Science & Engineering, Electrical*, **23**, 2898.

Bahrani, S., Razavi, M. & Salehi, J.A. (2016b). Orthogonal frequency division multiplexed quantum key distribution in the presence of raman noise. In *SPIE Photonics Europe*, 99001C–99001C, International Society for Optics and Photonics.

Bahrani, S., Razavi, M. & Salehi, J.A. (2018). Wavelength assignment in hybrid quantum-classical networks. *Scientific reports*, **8**, 3456.

Barends, R., Shabani, A., Lamata, L., Kelly, J., Mezzacapo, A., Las Heras, U., Babbush, R., Fowler, A., Campbell, B., Chen, Y. *et al.* (2016). Digitized adiabatic quantum computing with a superconducting circuit. *Nature*, **534**, 222–226.

Bartlett, S.D., Rudolph, T. & Spekkens, R.W. (2003). Classical and quantum communication without a shared reference frame. *Physical review letters*, **91**, 027901.

Bennett, C.H. (1984). Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, 175–179.

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. (1992a). Experimental quantum cryptography. *Journal of cryptology*, **5**, 3–28.

Bennett, C.H., Brassard, G. & Mermin, N.D. (1992b). Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, **68**, 557–559.

Bhandari, R. (2014). Quantum error correcting codes and the security proof of the bb84 protocol. *arXiv preprint arXiv:1409.1452*.

Biham, E., Huttner, B. & Mor, T. (1996). Quantum cryptographic network based on quantum memories. *Physical Review A*, **54**, 2651.

Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B.C. (2000). Limitations on practical quantum cryptography. *Physical Review Letters*, **85**, 1330.

Brendel, J., Gisin, N., Tittel, W. & Zbinden, H. (1999). Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, **82**, 2594.

Campagna, M., Chen, L., Dagdelen, O., Ding, J., Fernick, J., Gisin, N., Hayford, D., Jennewein, T., Lütkenhaus, N., Mosca, M. *et al.* (2015). Quantum safe cryptography and security: an introduction, benefits, enablers and challengers. Tech. rep., Technical report, ETSI (European Telecommunications Standards Institute) June 2015. http://www. etsi. org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper. pdf.

Carruthers, J.B. (2003). Wireless infrared communications. *Encyclopedia of telecommunications*.

Chitnis, D. & Collins, S. (2014). A spad-based photon detecting system for optical communications. *Journal of Lightwave Technology*, **32**, 2028–2034.

Chun, H. *et al.* (2017). Handheld free space quantum key distribution with dynamic motion compensation. *Optics Express*, **25**, 6784–6795.

Curty, M. & Moroder, T. (2011). Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Physical Review A*, **84**, 010304.

Dardari, D., Closas, P. & Djurić, P.M. (2015). Indoor tracking: Theory, methods, and technologies. *IEEE Transactions on Vehicular Technology*, **64**, 1263–1278.

Diamanti, E. (2006). *Security and implementation of differential phase shift quantum key distribution systems*. Stanford University.

Diamanti, E. & Leverrier, A. (2015). Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy*, **17**, 6072–6092.

Djordjevic, I.B. (2013). Multidimensional qkd based on combined orbital and spin angular momenta of photon. *IEEE Photonics Journal*, **5**, 7600112–7600112.

Duligall, J.L., Godfrey, M.S., Harrison, K.A., Munro, W.J. & Rarity, J.G. (2006). Low cost and compact quantum key distribution. *New Journal of Physics*, **8**, 249.

Dusek, M., Lutkenhaus, N. & Hendrych, M. (2006). Quantum cryptography. *Progress in Optics*, **49**, 381 – 454.

Ekert, A.K. (1991). Quantum cryptography based on bell's theorem. *Physical review letters*, **67**, 661.

Elgala, H., Mesleh, R. & Haas, H. (2011). Indoor optical wireless communication: potential and state-of-the-art. *IEEE Communications Magazine*, **49**.

Elmabrok, O. & Razavi, M. (2015). Feasibility of wireless quantum key distribution in indoor environments. In *Globecom Workshops (GC Wkshps), 2015 IEEE*, 1–2, IEEE.

Elmabrok, O. & Razavi, M. (2016). Quantum-classical access networks with embedded optical wireless links. In *IEEE GLOBECOM 2016 Conference Proceedings*, IEEE.

Elmabrok, O. & Razavi, M. (2018). Wireless quantum key distribution in indoor environments. *JOSA B*, **35**, 197–207.

Elmabrok, O., Ghalaii, M. & Razavi, M. (2018). Quantum-classical access networks with embedded optical wireless links. *JOSA B*, **35**, 487–499.

Eraerds, P. *et al.* (2010). Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, **12**, 063027.

Fossier, S., Diamanti, E., Debuisschert, T., Villing, A., Tualle-Brouri, R. & Grangier, P. (2009). Field test of a continuous-variable quantum key distribution prototype. *New Journal of Physics*, **11**, 045023.

Fröhlich, B., Dynes, J.F., Lucamarini, M., Sharpe, A.W., Yuan, Z. & Shields, A.J. (2013). A quantum access network. *Nature*, **501**, 69–72.

Gabay, M. & Arnon, S. (2006). Quantum key distribution by a free-space mimo system. *Journal of lightwave technology*, **24**, 3114–3120.

Gfeller, F.R. & Bapst, U. (1979). Wireless in-house data communication via diffuse infrared radiation. *Proceedings of the IEEE*, **67**, 1474–1486.

Ghassemlooy, Z. & Hayes, A. (2003). Indoor optical wireless communication systems–part i. *School of Engineering, Northumbria University, Newcastle upon Tyne, UK*.

Ghassemlooy, Z., Popoola, W. & Rajbhandari, S. (2012). *Optical wireless communications: system and channel modelling with Matlab®*. CRC Press.

Gisin, N., Pironio, S. & Sangouard, N. (2010). Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Physical review letters*, **105**, 070501.

Gomez, A., Shi, K., Quintana, C., Sato, M., Faulkner, G., Thomsen, B.C. & O'Brien, D. (2015). Beyond 100-Gb/s indoor wide field-of-view optical wireless communications. *IEEE Photonics Technology Letters*, **27**, 367–370.

Gottesman, D., Lo, H.K., Lütkenhaus, N. & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, 136, IEEE.

Grosshans, F. & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical review letters*, **88**, 057902.

Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N.J. & Grangier, P. (2003). Quantum key distribution using gaussian-modulated coherent states. *Nature*, **421**, 238–241.

Hadfield, R.H. (2009). Single-photon detectors for optical quantum information applications. *Nature Photonics*, **3**, 696–705.

Hwang, W.Y. (2003). Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, **91**, 057901.

Imre, S. & Gyongyosi, L. (2012). *Advanced quantum communications: an engineering approach*. John Wiley & Sons.

Jain, N., Stiller, B., Khan, I., Elser, D., Marquardt, C. & Leuchs, G. (2016). Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, **57**, 366–387.

Jaina, N., Stillera, B., Khana, I., Elsera, D., Marquardta, C. & Leuchsa, G. (2015). Introductory review article. *arXiv preprint arXiv:1512.07990*.

Johnson, M., Amin, M., Gildert, S., Lanting, T., Hamze, F., Dickson, N., Harris, R., Berkley, A., Johansson, J., Bunyk, P. *et al.* (2011). Quantum annealing with manufactured spins. *Nature*, **473**, 194–198.

Jouguet, P., Kunz-Jacques, S. & Leverrier, A. (2011). Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A*, **84**, 062317.

Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. (2013). Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, **7**, 378–381.

Kahn, J.M. & Barry, J.R. (1997). Wireless infrared communications. *Proceedings of the IEEE*, **85**, 265–298.

Korzh, B., Lim, C.C.W., Houlmann, R., Gisin, N., Li, M.J., Nolan, D., Sanguinetti, B., Thew, R. & Zbinden, H. (2015). Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, **9**, 163–168.

Kumar, R., Qin, H. & Alléaume, R. (2014). Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense dwdm classical channel. In *CLEO: QELS_Fundamental Science*, FM4A–1, Optical Society of America.

Kumar, R., Qin, H. & Alléaume, R. (2015). Coexistence of continuous variable qkd with intense DWDM classical channels. *New Journal of Physics*, **17**, 043027.

Laing, A., Scarani, V., Rarity, J.G. & O'Brien, J.L. (2010a). Reference-frame-independent quantum key distribution. *Physical Review A*, **82**, 012304.

Laing, A., Scarani, V., Rarity, J.G. & O'Brien, J.L. (2010b). Reference-frame-independent quantum key distribution. *Physical Review A*, **82**, 012304.

Lasota, M., Filip, R. & Usenko, V.C. (2017). Robustness of quantum key distribution with discrete and continuous variables to channel noise. *Physical Review A*, **95**, 062312.

Leverrier, A., Grosshans, F. & Grangier, P. (2010). Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, **81**, 062343.

Liang, W.Y., Wang, S., Li, H.W., Yin, Z.Q., Chen, W., Yao, Y., Huang, J.Z., Guo, G.C. & Han, Z.F. (2014). Proof-of-principle experiment of reference-frame-independent quantum key distribution with phase coding. *Scientific reports*, **4**, 3617.

Liao, S.K., Cai, W.Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Rauch, D., Fink, M., Ren, J.G., Liu, W.Y. *et al.* (2018). Satellite-relayed intercontinental quantum network. *Physical review letters*, **120**, 030501.

Lo, H.K., Chau, H.F. & Ardehali, M. (2005). Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, **18**, 133–165.

Lo, H.K., Curty, M. & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical review letters*, **108**, 130503.

Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tualle-Brouri, R., McLaughlin, S.W. *et al.* (2007). Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, **76**, 042305.

Lütkenhaus, N. (2007). Theory of quantum key distribution (qkd). *Lectures on Quantum Information*, 271–284.

Ma, C., Sacher, W.D., Tang, Z., Mikkelsen, J.C., Yang, Y., Xu, F., Thiessen, T., Lo, H.K. & Poon, J.K.S. (2016). Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica*, **3**, 1274–1278.

Ma, X. (2006). Unconditional security at a low cost. *Physical Review A*, **74**, 052325.

Ma, X. (2008). Quantum cryptography: from theory to practice.

Ma, X. & Razavi, M. (2012). Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A*, **86**, 062319.

Ma, X., Qi, B., Zhao, Y. & Lo, H.K. (2005). Practical decoy state for quantum key distribution. *Physical Review A*, **72**, 012326.

Ma, X., Fung, C.H.F. & Razavi, M. (2012a). Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Physical Review A*, **86**, 052305.

Ma, X., Fung, C.H.F. & Razavi, M. (2012b). Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A*, **86**, 052305.

Madsen, L.S., Usenko, V.C., Lassen, M., Filip, R. & Andersen, U.L. (2012). Continuous variable quantum key distribution with modulated entangled states. *Nature Communications*, **3**, 1083.

Marsili, F., Verma, V.B., Stern, J.A., Harrington, S., Lita, A.E., Gerrits, T., Vayshenker, I., Baek, B., Shaw, M.D., Mirin, R.P. *et al.* (2013). Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, **7**, 210–214.

Mayers, D. & Yao, A. (1998). Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, 503–509, IEEE.

Mirhosseini, M., Magaña-Loaiza, O.S., O'Sullivan, M.N., Rodenburg, B., Malik, M., Lavery, M.P., Padgett, M.J., Gauthier, D.J. & Boyd, R.W. (2015). High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, **17**, 033033.

MORAN, C.C. (2016). Quintuple: a python 5-qubit quantum computer simulator to facilitate cloud quantum computing. *arXiv preprint arXiv:1606.09225*.

MULLER, A., HERZOG, T., HUTTNER, B., TITTEL, W., ZBINDEN, H. & GISIN, N. (1997). "plug and play" systems for quantum cryptography. *Applied Physics Letters*, **70**, 793–795.

NIELSEN, M.A. & CHUANG, I. (2002). Quantum computation and quantum information.

PANAYI, C., RAZAVI, M., MA, X. & LÜTKENHAUS, N. (2014). Memory-assisted measurement-device-independent quantum key distribution. *New Journal of Physics*, **16**, 043005.

PATEL, K. *et al.* (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, **2**, 041010.

PATEL, K.A., DYNES, J.F., LUCAMARINI, M., CHOI, I., SHARPE, A.W., YUAN, Z.L., PENTY, R.V. & SHIELDS, A.J. (2014a). Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Applied Physics Letters*, **104**, 051123.

PATEL, K.A. *et al.* (2014b). Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks. *Applied Physics Letters*, **104**, 051123.

PETITCOLAS, F.A.P. (2011). *Kerckhoffs' Principle*, 675–675. Springer US, Boston, MA.

PRAWER, S. & AHARONOVICH, I. (2014). *Quantum information processing with diamond: Principles and applications*. Elsevier.

QAZI, S. (2006). Challenges in outdoor and indoor optical wireless communications. In *ICWN*, 448–458.

QI, B., ZHU, W., QIAN, L. & LO, H.K. (2010a). Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, **12**, 103042.

QI, B., ZHU, W., QIAN, L. & LO, H.K. (2010b). Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, **12**, 103042.

RAHARIJAONA, T., MAWONOU, R., NGUYEN, T.V., COLONNIER, F., BOYRON, M., DIPERI, J. & VIOLLET, S. (2017). Local positioning system using flickering infrared leds. *Sensors*, **17**, 2518.

RAMIREZ-INIGUEZ, R., IDRUS, S.M. & SUN, Z. (2008). *Optical wireless communications: IR for wireless connectivity*. CRC press.

RAZAVI, M. (2011). Multiple-access quantum-classical networks. In *Quantum Communication, Measurement and Computing (QCMC): The Tenth International Conference*, vol. 1363, 39–42, AIP Publishing.

RAZAVI, M. (2012). Multiple-access quantum key distribution networks. *IEEE Transactions on Communications*, **60**, 3071–3079.

RIVEST, R.L., SHAMIR, A. & ADLEMAN, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21**, 120–126.

RUSCA, D. *et al.* (2018). Finite-key analysis on the 1-decoy state qkd protocol. *arXiv preprint arXiv:1801.03443*.

SASAKI, M. *et al.* (2011). Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, **19**, 10387–10409.

SCARANI, V., BECHMANN-PASQUINUCCI, H., CERF, N.J., DUŠEK, M., LÜTKENHAUS, N. & PEEV, M. (2009). The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**, 1301–1350.

SCHMITT-MANDERBACH, T., WEIER, H., FÜRST, M., URSIN, R., TIEFENBACHER, F., SCHEIDL, T., PERDIGUES, J., SODNIK, Z., KURTSIEFER, C., RARITY, J.G. *et al.* (2007). Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phy. Rev. Lett.*, **98**, 010504.

SHERIDAN, L., LE, T.P. & SCARANI, V. (2010). Finite-key security against coherent attacks in quantum key distribution. *New Journal of Physics*, **12**, 123019.

SHOR, P.W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, 124–134, IEEE.

SIBSON, P., ERVEN, C., GODFREY, M., MIKI, S., YAMASHITA, T., FUJIWARA, M., SASAKI, M., TERAI, H., TANNER, M.G., NATARAJAN, C.M., HADFIELD, R.H., O'BRIEN, J.L. & THOMPSON, M.G. (2017). Chip-based quantum key distribution. *Nature Commun.*, **8**, 13984.

SPEDALIERI, F.M. (2006). Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum. *Optics communications*, **260**, 340–346.

TAMAKI, K., CURTY, M., KATO, G., LO, H.K. & AZUMA, K. (2014). Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A*, **90**, 052314.

URSIN, R., TIEFENBACHER, F., SCHMITT-MANDERBACH, T., WEIER, H., SCHEIDL, T., LINDENTHAL, M., BLAUENSTEINER, B., JENNEWEIN, T., PERDIGUES, J., TROJEK, P. *et al.* (2006). Free-space distribution of entanglement and single photons over 144 km. *arXiv preprint quant-ph/0607182*.

VERNAM, G.S. (1926). Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, **45**, 109–115.

VEST, G., RAU, M., FUCHS, L., CORRIELLI, G., WEIER, H., NAUERTH, S., CRESPI, A., OSELLAME, R. & WEINFURTER, H. (2015). Design and evaluation of a handheld quantum key distribution sender module. *IEEE Journal of Selected Topics in Quantum Electronics*, **21**, 131–137.

WABNIG, J., BITAULD, D., LI, H., LAING, A., O'BRIEN, J. & NISKANEN, A. (2013). Demonstration of free-space reference frame independent quantum key distribution. *New Journal of Physics*, **15**, 073001.

Wang, C., Huang, D., Huang, P., Lin, D., Peng, J. & Zeng, G. (2015a). 25 mhz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Scientific reports*, **5**.

Wang, C., Sun, S.H., Ma, X.C., Tang, G.Z. & Liang, L.M. (2015b). Reference-frame-independent quantum key distribution with source flaws. *Physical Review A*, **92**, 042319.

Wiesner, S. (1983). Conjugate coding. *ACM Sigact News*, **15**, 78–88.

Wootters, W.K. & Zurek, W.H. (1982). A single quantum cannot be cloned. *Nature*, **299**, 802–803.

Xu, F., Curty, M., Qi, B. & Lo, H.K. (2015). Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, **21**, 148–158.

Yuan, Z., Kardynal, B., Sharpe, A. & Shields, A. (2007). High speed single photon detection in the near infrared. *Applied Physics Letters*, **91**, 041114–041114.

Zhang, D., Xia, F., Yang, Z., Yao, L. & Zhao, W. (2010). Localization technologies for indoor human tracking. In *Future Information Technology (FutureTech), 2010 5th International Conference on*, 1–6, IEEE.

Zhang, P., Aungskunsiri, K., Martín-López, E., Wabnig, J., Lobino, M., Nock, R., Munns, J., Bonneau, D., Jiang, P., Li, H. *et al.* (2014). Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. *Physical review letters*, **112**, 130501.

Zhang, Y.C. *et al.* (2017a). Continuous-variable qkd over 50km commercial fiber. *arXiv:1709.04618*.

Zhang, Z., Zhao, Q., Razavi, M. & Ma, X. (2017b). Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Physical Review A*, **95**, 012333.

Zhao, Y., Qi, B., Ma, X., Lo, H.K. & Qian, L. (2006). Experimental quantum key distribution with decoy states. *Physical review letters*, **96**, 070502.