Photonic integration of a directly phase-modulated source for Quantum Key Distribution

Innocenzo De Marco

University of Leeds

School of Electronic and Electrical Engineering

Toshiba Europe Ltd

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

November, 2020

This page intentionally left blank.

Intellectual Property Statement

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

The work in Chapter 5 of the thesis is to appear in publication as follows:

- **Innocenzo De Marco**, Robert I. Woodward, George L. Roberts, Taofiq K. Paraïso, Thomas Roger, Mirko Sanzaro, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields. *Universal Quantum Key Distribution transmitter*, in preparation.

I was responsible for setting up and performing the experiment, collecting and analysing data. I wrote the manuscript which is currently in preparation.

The work in Chapter 6 of the thesis has appeared in publication as follows:

- Taofiq K. Paraïso, **Innocenzo De Marco**, Thomas Roger, Davide G. Marangon, James F. Dynes, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields. *A modulator-free quantum key distribution transmitter chip*, npj Quantum Inf 5, 42 (2019).

I was responsible for the collection and analysis of experimental data, as well as performing simulations of the experiment concerning the key rates and photon fluxes.

The work in Chapter 7 of the thesis is to appear in publication as follows:

- Taofiq K. Paraïso, **Innocenzo De Marco**, Thomas Roger, Mirko Sanzaro, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields. *On-chip generation of decoy states for Quantum Key Distribution*, in preparation.

I was responsible for data collection and analysis.

The work in Chapter 8 of the thesis has appeared in publication as follows:

- Thomas Roger, Taofiq K. Paraïso, **Innocenzo De Marco**, Davide G. Marangon, Zhiliang Yuan, and Andrew J. Shields. *Real-time interferometric quantum random number generation on chip*, J. Opt. Soc. Am. B 36, B137-B142, (2019).

I was responsible for characterising the system and acquiring and analysing preliminary data.

Contents from published papers were presented in the following conferences:

- Thomas Roger, Taofiq K. Paraïso, **Innocenzo De Marco**, Davide G. Marangon, Zhiliang Yuan, and Andrew J. Shields. *Real-time interferometric quantum random number generation on chip.* CLEO 2019, San José, CA (USA), 2019.
- **Innocenzo De Marco**, Taofiq K. Paraïso, Thomas Roger, Davide G. Marangon, James F. Dynes, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields. *Integrated photonic technologies for quantum communications.* QCALL Early-Stage Researchers Conference, Palermo (Italy), 2019.

Acknowledgements

Writing a thesis during a global pandemic has a sort of eerie feeling to it. Nevertheless, it is a reminder that we can still fight through hard times and find some good in them. This thesis marks the end of a long journey. I would like to thank everyone who helped and supported me during these years.

First of all, I would like to thank Dr Andrew Shields, for giving me the opportunity to pursue research in a field I have always enjoyed. Thanks to Prof Mohsen Razavi, my academic supervisor, for the support with both bureaucratic and academic matters. I would also like to acknowledge QCALL, the organisation who allowed me to get in contact with fellow early-stage researchers sharing the same passion for research. Being part of such a group taught me a lot so, to every single one of you, thank you.

Thanks to Dr Taofiq Paraïso, who inspired me to "grind" through difficulties and made me a much better researcher than I though I could be. A thank you goes to the QKD chip team, Dr Thomas Roger and Dr Mirko Sanzaro, for all the discussions both on and off topic and their comments on my thesis that certainly improved its quality. Thanks to Dr Davide Marangon, for his invaluable help with all things QRNG, and the break room discussions about human rights and politics. Many thanks to Dr Zhiliang Yuan, the best group leader one could hope for, and Prof Marco Lucamarini, who was the very first person to help me acclimate in Cambridge and in Toshiba.

A very heartfelt thank you is for my current and past fellow PhD students and coworkers at Toshiba. Mirko, the best cubicle mate one could ever hope for and a fellow QCALL member. We went through a lot of pain together, but we made it! Andrea, my support bubble during these troubled times, really came through when I needed some human contact. For everyone else: you are too many to mention, but all of you have a place in my heart; you made my time here one of the best of my life, and I look forward to seeing what great things you'll do.

Mom, Dad and Gaia, you are always there for me. If I can repay you even for a fraction of what you did for me, I will be happy. Family and friends from back in Italy are and will always be a big part of my life. They shaped me into who I am now and I will always be grateful for them.

Finally, Kristina. You have been a constant in my life for the last few years, so much so that I cannot imagine my life without you. Thanks for being close despite being far. I could not have made it without you.

This page intentionally left blank.

Abstract

Quantum key distribution (QKD) is recognised as the main countermeasure against attacks to current cryptography from a quantum adversary. Despite the fact that several implementations have been already shown, the technology is still not at the stage of large-scale deployment. This is due to several factors, such as entropy loss, the high cost and space requirements for installing QKD systems. Integrated photonics is the natural solution for this: it allows for compact devices at a much lower cost, which is a step forward towards mass production. In this work I present the photonic integrated chips developed at Toshiba Europe Ltd. to which I have contributed. These include QKD transmitters and receivers, as well as integrated circuits implementing quantum random number generators (QRNG).

Firstly, after introducing the basic concepts of secure communications, I show and demonstrate the interoperability of a QKD light source based on direct phase modulation and optical injection locking with discrete optics. This will be the basis for the next experiment, as this light source is the one implemented on all our QKD chips. I then proceed to demonstrate how to perform QKD with these integrated devices, achieving record lengths for a photonic integrated circuit. This is then further enhanced by demonstrating that a chip-based transmitter can also encode decoy states. Finally, a key component of a QKD system is the capability of generating random strings to ensure the security of the key. To this end, I demonstrate a chip-based QRNG working with stand-alone electronics, achieving high generation rates and therefore being suitable for usage in QKD systems.

This work represents a step towards large-scale implementation of QKD networks.

This page intentionally left blank.

Contents

Abbreviations xvii

I Background 1

1 Introduction 3
1.1 Thesis outline . . . 3
1.2 Classical Cryptography . . . 4
1.3 Quantum cryptography . . . 8
1.4 Quantum Key Distribution . . . 9
1.4.1 Categories of QKD protocols . . . 9
1.4.2 QKD implementations . . . 11
1.4.3 Time-bin and phase encoded QKD . . . 15
1.4.4 Extracting a secure key . . . 17
1.4.5 State of the art . . . 19

2 Phase-encoded QKD protocols 21
2.1 The BB84 protocol . . . 21
2.2 The DPS protocol . . . 25
2.3 The COW protocol . . . 26

3 Photonic integrated circuits 29
3.1 Integrated photonic platforms . . . 29
3.1.1 Silicon photonic circuits . . . 31
3.1.2 Silicon-on-insulator photonic circuits . . . 32
3.1.3 Indium Phosphide photonic circuits . . . 32
3.2 Generic integration processes . . . 33
3.3 Applications of integrated photonics . . . 34
3.3.1 Photonic integrated circuits in telecommunications . . . 34
3.3.2 Integrated quantum photonics . . . 35
3.3.3 Integrated quantum communications . . . 36

II Experiments and results **39**

4 Methods **41**
4.1 Experimental apparatus . . . 41
4.2 Performing a QKD experiment . . . 45

5 Multi-protocol, multi-rate QKD transmitter **47**
5.1 Introduction and personal contributions . . . 47
5.2 Directly phase-modulated light source . . . 48
5.3 Experimental setup . . . 50
5.3.1 Protocols implementation . . . 50
5.3.2 Integrated decoding circuits . . . 52
5.4 Characterisation . . . 54
5.5 Results . . . 56
5.6 Conclusions and discussion . . . 57

6 High bit-rate QKD with integrated photonics **59**
6.1 Experimental setup . . . 59
6.1.1 Integrated photonic transmitter . . . 59
6.1.2 Layout of the experiment . . . 60
6.2 Characterisation of the transmitter . . . 62
6.2.1 Integrated lasers . . . 62
6.2.2 Variable optical attenuator . . . 63
6.2.3 Coherence transfer . . . 63
6.2.4 Differential phase encoding . . . 65
6.3 Experimental parameters and results . . . 66
6.4 Conclusions and discussion . . . 67

7 On-chip generation of decoy states for QKD **69**
7.1 Decoy state generation . . . 69
7.2 Experimental setup . . . 70
7.2.1 Integrated transmitter . . . 70
7.2.2 Layout of the experiment . . . 71
7.3 Characterisation . . . 71
7.3.1 EAM . . . 71
7.4 Results . . . 72
7.4.1 Decoy states generation . . . 72
7.4.2 QKD with decoy states . . . 73
7.5 Conclusions and discussion . . . 75

8 Real-time generation of quantum random numbers **77**
8.1 Random Number Generation 77
8.2 Phase noise in DFB lasers 79
8.3 Experimental setup 80
8.4 Characterisation 82
8.5 Results 83
8.6 Conclusions and discussion 85

III Final remarks **89**

9 Conclusions **91**

10 Future work **95**

References **97**

This page intentionally left blank.

List of Figures

1.1 Symmetric and asymmetric cryptography conceptualised 5
1.2 Public-key cryptography is used to distribute a key between two parties. . . . 7
1.3 A generic QKD system. Alice sends information to Bob through a quantum channel. 12
1.4 Poissonian distribution of the probability $P(n)$ of emitting n photons, for four different mean photon numbers. Higher mean photon numbers have higher probability of multi-photon events. 14
1.5 Time-bin encoding for the X, Y, Z bases. On the right, the Bloch sphere mapping the six states. 15
1.6 Self-interference of a pulse in a MZI. 16
1.7 Adding a delay to one of the MZI arms allows to measure the interference of two consecutive pulses. 17
1.8 The process of extracting a secure key. 18
1.9 Sifted and secure key rates, QBER as a function of the channel loss. 19

2.1 Schematic of the polarisation-encoded BB84 protocol. 22
2.2 Transmitter setup for time-bin encoded BB84. 22
2.3 Passive receiving two-interferometer setup for the BB84 protocol. 23
2.4 Histogram distribution of the intensities from interferences of uniformly distributed phase differences, in scenarios with (top) and without (bottom) classical noise. In the bottom plot, the blue, dashed line represents the noiseless case, to highlight the discrepancies. 24
2.5 Transmitter setup for the DPS protocol. 26
2.6 Experimental setup for the COW protocol. 26
2.7 Comparison between the asymptotic key rates of the decoy-state BB84, DPS and COW protocols. 27

3.1 Femtosecond laser writing: a highly focussed, pulsed laser beam is used to write waveguides on a glass substrate. 30
3.2 Basic fabrication process of a PIC using lithography. 31

3.3 Examples of basic building blocks available for photonic circuit design. 33
3.4 A 2 mm × 4 mm photonic chip for QKD. 36

4.1 Experimental setup for a QKD experiment. 42
4.2 Schematic of the probe station used to test chips. 44
4.3 Schematic of the temperature control system. 44
4.4 Setup for calibrating the photon flux sent by Alice to Bob. 45

5.1 Direct phase modulation of a DFB laser. 48
5.2 Principle of operation of OIL. 50
5.3 Injecting light into the seeded cavity generates coherent pulses. 51
5.4 Experimental setup showing optical and electronic devices used for the QTx. 51
5.5 Driving signals from phase encoding and injection locked lasers for the COW protocol. 52
5.6 Driving signals from phase encoding and injection locked lasers for the DPS protocol. 53
5.7 Driving signals for the two lasers for the BB84 protocol. 53
5.8 Jittery output from a gain-switched laser (left). Output after CW injection (right). 54
5.9 Spectra of an unseeded (left) and seeded (right) gain-switched laser. The peaks are spaced by 2 GHz. 55
5.10 Interference power output of seeded pulses from a directly phase modulated light source. 56
5.11 Cumulative interferences of phase-randomised pulses (left). Histogram of the interferences recorded at the centre of the pulse. (right). 57
5.12 Results obtained using different clock rates and protocols. 58

6.1 Principle of operation of an MMI. 60
6.2 Experimental setup to perform QKD using an integrated transmitter. 61
6.3 P-I-V curves for two different DFB lasers. 62
6.4 Spectra of the injection locked laser in pulsed mode when seeded by CW light. 63
6.5 Optical output from the phase encoding laser modulated to encode a BB84 pattern. 64
6.6 Photocurrent measured from the on-chip photodiode (converted to optical power) versus voltage applied on MZI. 64
6.7 Interference fringes at the output of the receiving interferometer. 65
6.8 Left: Incrementing modulation on phase encoding laser generates pulses with increasing phase difference. Right: expected constellation plot in the optical phase space. 66
6.9 Eye diagram (left) and constellation plot (right) of 8-level DPSK. 67

6.10 QBER and asymptotic SKR obtained for the BB84 (left) and DPS (right) protocols as a function of the channel loss. 68

7.1 Quantum-Confined Stark Effect. 70
7.2 Schematic of the EAM-decoy circuit. 71
7.3 Measured power at the output of the chip as a function of the voltage applied to the EAM. 71
7.4 Left: Emission of the EAM in forward bias, shown in the I-V curve. Right: Spectral shift of the light emitted by the injection locked laser when forward-biasing the EAM. 72
7.5 QBER over time for a QKD experiment with decoy states generated on chip. 73
7.6 EAM attenuation of decoy states at four different levels. 73
7.7 Visibility of interfering pulses. Both signal and decoy states are interfering. . 74
7.8 1 Mbit/s secure key rate achieved using decoy-state BB84. 74

8.1 Schematic representation of a QRNG. 78
8.2 Sequence of gain-switched pulses from a DFB laser. 80
8.3 Experimental setup. The yellow section is the photonic circuit, the teal section includes the electronics. 81
8.4 1000 interference events, recorded by an oscilloscope, are overlapped and plotted on the left hand side. On the right is the distribution of $\sim$ 800000 interference intensities, measured in the interval highlighted by the rectangle. 82
8.5 Autocorrelation of consecutive pulses obtained by using the plug-and-play QRNG system. 83
8.6 Histogram obtained by recording data using the plug-and-play QRNG system. 84
8.7 An FIR filter flattens and spreads the distribution across the 8-bit range. . . 84

This page intentionally left blank.

Abbreviations

ADC	analog-to-digital converter ... 80–84
AES	advanced encryption standard ... 6, 8, 9, 91
AWG	arbitrary waveform generator ... 42, 45, 50, 51, 57, 60, 71–73
BB84	Bennett-Brassard 1984 protocol . 10, 17, 21–23, 25, 27, 28, 37, 45, 50, 52, 53, 55–57, 60, 61, 63, 64, 66–69, 73–75, 92
CMOS	complementary metal-oxide-semiconductor ... 35, 48
COW	Coherent One Way ... 21, 26–28, 37, 50, 52, 56, 57
CW	continuous wave ... 20, 22, 37, 50, 54, 59, 62, 63, 71
DC	direct current ... 41–43, 50, 60, 72, 79, 80, 82
DFB	distributed feedback ... 32, 35, 48, 59, 62, 79–82
DPR	distributed phase reference ... 11, 25, 28
DPS	differential phase shift 21, 25–28, 37, 50, 52, 53, 56, 57, 60, 61, 65–68, 92
EAM	electro-absorption modulator ... 32, 41, 42, 69–75, 92, 96
EOPM	electro-optical phase modulator ... 20, 37, 69
FIR	finite impulse response ... 83, 84, 93
FPGA	field programmable gate array ... 57, 81–83, 85, 92
GS	ground-signal ... 43
GSG	ground-signal-ground ... 43
InP	Indium Phosphide ... 20, 30, 32, 34, 35, 37, 59, 81, 95
MMI	multi-mode interferometer ... 59, 60, 81
MPW	multi-project wafer ... 33, 36
MZI	Mach-Zehnder interferometer ... 16, 17, 37, 59, 63, 69, 75
aMZI	asymmetric MZI ... 16, 21, 22, 24, 25, 27, 52, 54–57, 61, 65
OIL	optical injection locking ... 49, 50, 67
OSA	optical spectrum analyser ... 62, 81, 82
PD	photodiode ...
APD	avalanche photodiode ... 61, 96
SDAPD	self-differencing APD ... 61, 67, 92, 96
PDF	probability density function ... 80

PIC	photonic integrated circuit 29, 31, 33–36, 95
PNS	photon number splitting 11, 13, 25, 75, 92
PSK	phase-shift keying 35, 65
DPSK	differential phase-shift keying 65–67
QBER	quantum bit error rate 17–19, 25, 46, 52, 56–58, 66–68, 72–75, 92
QCSE	quantum-confined Stark effect 70, 92
QKD	quantum key distribution 3, 4, 9–15, 17, 18, 20, 21, 23, 25, 36, 37, 41–43, 47, 48, 50, 54, 57, 59, 61, 66, 67, 69, 73, 75, 77, 79, 85, 91, 92, 95, 96
CV-QKD	continuous variable QKD 10, 20
DPR-QKD	distributed phase reference QKD 26
DV-QKD	discrete variable QKD 10, 11, 13
MDI-QKD	measurement-device independent QKD 10, 11, 14, 95
QRx	QKD receiver 52, 61
QTx	QKD transmitter. 41, 47, 51, 56, 59, 60, 63, 65–67, 69, 70, 72, 75, 92, 96
TF-QKD	Twin-field QKD 11, 20, 95
RF	radio frequency 41, 42, 48, 50, 60, 69, 72, 80, 81
RNG	random number generator 77
PRNG	pseudo-random number generator 77, 78
QRNG	quantum random number generator. 66, 77, 78, 82–85, 87, 92
TRNG	true random number generator 78
RSA	Rivest-Shamir-Adleman cryptosystem 6, 8, 91
SiO_xN_y	Silicon Oxy-Nitride 32
SKR	secure key rate 18, 19, 25, 27, 28, 46, 52, 56–59, 67, 68, 73–75, 92, 96
SMU	source-measure unit 41, 50, 60, 72
SOI	Silicon-on-insulator 32
SPD	single photon detector 10, 14, 18, 23, 25, 42, 61, 96
SNSPD	superconducting nanowire SPD 54, 61, 66, 67, 73, 92, 96
SSC	spot-size converter 43, 59, 62, 81
TEC	thermo-electric cooler 42–44, 60, 71
TEUR	Toshiba Europe Ltd 3, 11, 52
TOPS	thermo-optical phase shifter 37, 52
VOA	variable optical attenuator 41, 43, 56, 59, 60, 63, 64, 68, 69, 71, 72, 81

Assumptions

The following assumptions are made throughout the thesis:

- quantum mechanical laws are valid;
- Alice and Bob are able to authenticate each other;
- transmitting and receiving devices are trusted, i.e. they are not under control of an eavesdropper;
- Alice is able to transmit in only one mode: the assumption is that an optical filter is enough to suppress all other modes;
- in the case that detectors do not have identical efficiencies, a fair sampling assumption is made, i.e. all the detection events are a fair sample of all signals sent by Alice.

This page intentionally left blank.

Part I

Background

This page intentionally left blank.

Chapter 1

Introduction

In a world where everything is connected in a large, worldwide network, information security is one of the most compelling issues to address. The Internet of Things revolution is gaining momentum [1], and the number of devices sharing information is ever increasing. Data breaches in social networks have raised awareness on the subject of data security, and people are starting to become conscious of the importance of personal data.

This security is especially important when transmitting information from one point to another. Bank account information, medical records and trade-secret information are transmitted through networks continuously, so it is important to keep these data secure. Eavesdropping data in transit is sometimes easier than trying to attack a storage unit where data is securely kept, as communication involves the transmission over public channels. The need for secure communications is hence of paramount importance.

This thesis is aimed at taking steps towards large-scale deployment of secure quantum communications, particularly quantum key distribution (QKD). Currently, network employing QKD systems employ space-consuming, expensive and power-hungry instrumentation to efficiently work. Here, we show how transitioning to integrated photonics could benefit all three of the aforementioned issues, while still being able to effectively perform QKD. The work presented in this thesis was carried out by the author jointly with other researchers in Toshiba Europe Ltd (TEUR). The author's contributions are highlighted where necessary.

1.1 Thesis outline

This chapter will describe the techniques developed over time to transmit messages in a way that prevents eavesdroppers from reading them. Classical cryptography will be addressed first, outlining the current status of data security. Next, as a countermeasure to the advent of quantum computers, QKD will be introduced, with its guarantee of unconditional security: the main concepts of QKD are presented here.

Chapter 2 introduces the QKD protocols that will be used throughout this thesis.

Chapter 3 introduces the idea of integrated photonics and how generic integration processes will help speed-up the development of these technologies for both classical and quantum communications. Examples of applications for photonic integrated circuits will be presented. Chapter 5 presents a directly phase-modulated light source with multi-rate and multi-protocol capabilities. The QKD transmitter presented in this chapter is able to communicate with different hardware by simply changing the driving signals. Chapter 6 describes how such a light source performs when integrated on a photonic circuit, and shows the record results obtained by this integrated transmitter with QKD experiments. Chapter 7 expands on this, demonstrating the ability of generating decoy states on a chip-based transmitter through an electro-absorption modulator. Chapter 8 demonstrates a real-time QKD based on integrated photonics, capable of Gb/s generation rates. Finally, the last two chapters conclude the thesis with a perspective on future work in the field.

1.2 Classical Cryptography

Data travelling from one point to another is easily intercepted, regardless of the means used to transmit the message: an eavesdropper, Eve, can tap the communication channel, intercept the envelope containing the message, intercept the messengers and bribe them into revealing the message.

The usual method two parties, Alice and Bob, employ to keep their communication secure is cryptography. Alice scrambles her message (plaintext) by applying an operation (encryption) to it using an algorithm (cipher) and a secret piece of information (key). She then sends the result (ciphertext) across the communication channel. When Bob receives it, he applies the inverse operation (decryption) to retrieve the plaintext. The particular operation applied to the message depends on the protocol Alice and Bob choose to implement.

The goal is to make sure that Eve is not able to retrieve the plaintext without access to the key. Encrypting messages to prevent them being read by unwanted eavesdroppers is a challenge dating back centuries. Julius Caesar [2] used a simple encryption scheme for his private correspondence. The scheme simply consisted of substituting each letter in a message with the third letter after it, in the alphabet. This way, A becomes D, B becomes E, and so on. The Ancient Greeks in Sparta relied on a different kind of encryption, based on rearranging the letters composing the plaintext. Both of these schemes are easily breakable and result in a poor security of the information.

In time, several encryption schemes were developed and used, each one more secure and harder to break than the previous one. Each one, however, was eventually broken. The most notable example is the Enigma machine [3], a very sophisticated encoding system developed at the end of World War I by a German engineer and used by Germany during the Second World War. Such a scheme was thought to be unbreakable, until the task force of Bletchley Park, led by scientists like Alan Turing, found the flaws in the scheme and broke it, allowing

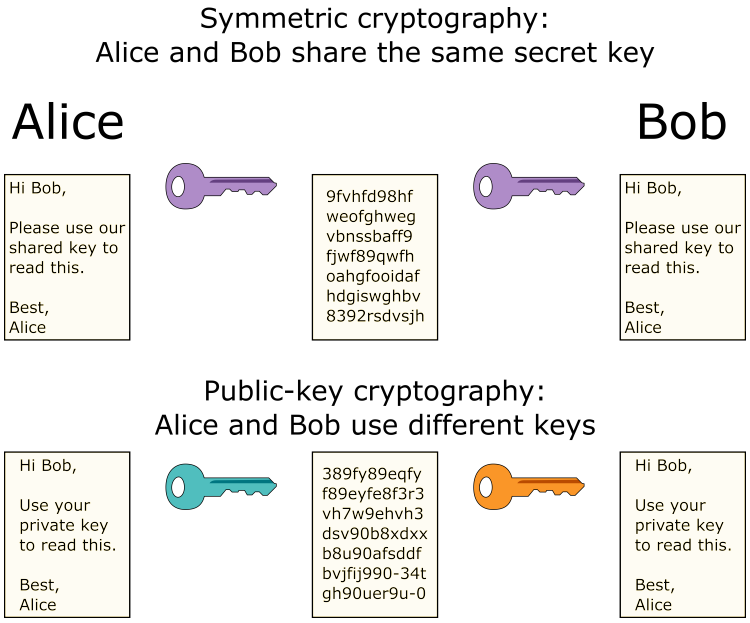

Figure 1.1: Symmetric (top) and asymmetric (bottom) cryptography conceptualised. Symmetric encryption sees Alice (left) and Bob (right) sharing the same key to encrypt and decrypt a message. Asymmetric encryption relies on Bob sharing a public key that Alice can use to encrypt her message, which will then be decrypted by Bob using his private key.

the allied forces to intercept the plans of the Axis before their execution. Many historians describe the breaking of the Enigma code as a turning point in WWII [4].

Later on, cryptography started to be approached in a mathematical and more rigorous way. Plaintexts and keys started to be represented as streams of characters (which became streams of bits with the advent of the computer era), ciphers as mathematical algorithms. This allows for a more thorough study of the security of a protocol.

Encryption schemes nowadays can be mainly categorised into two main families: asymmetric (public-key) schemes and symmetric schemes (Figure 1.1)

Asymmetric cryptography

Public-key, or asymmetric protocols [5], have been developed to perform encryption between parties not sharing a secret. They can also be used for digital signatures, i.e. a method for the recipient of a message to correctly identify the sender. In public key protocols, Bob computes a public-private key pair and discloses the public key only, which is accessible to Alice (and to eavesdroppers), for her to encrypt her message for Bob. When Bob receives the ciphertext, he retrieves the plaintext using the private key, which only he knows. The security relies on the difficulty for an attacker to infer the private key from the public key.

It is important to notice that such protocols present a high risk of being tampered

with. Eve might replace the public key and intercept the communication with Alice. To prevent this, several approaches have been proposed, the most widespread being public key infrastructures [6], relying on certificate authorities to vouch for the authenticity of public keys, and "web of trust" [7] network configurations, which authenticate public keys by comparing endorsements from different nodes in the network.

All public-key protocols rely on one-way functions: a function is called one-way if it can be computed by a polynomial-time algorithm but, for every probabilistic polynomial-time algorithm, the probability of inverting the function is negligible [8] without knowing the private key in advance. Keys obtained in this way are hence said to be *computationally secure*. This means that a normal computer is expected to take a very large amount of time to decrypt a message encrypted using public-key cryptography.

The first known public-key algorithm is the Diffie-Hellman (sometimes known as Diffie-Hellman-Merkle) key exchange algorithm [9, 10]. Such a protocol allows two parties to share a secret key over an insecure channel. The key can then be used by a symmetric-key protocol.

The Rivest-Shamir-Adleman cryptosystem (RSA) [11] is the most used public-key protocol in digital communications. It is based on the factoring problem, i.e. decomposing a large integer number into its prime factors. Such a problem is easy to compute one way (multiplying two prime numbers is easy), and it is (part of) the algorithm Bob performs to generate the public key, while it is hard to compute the inverse operation. The protocol is slower than symmetric encryption schemes, which will be explained later: for this reason, nowadays it is more commonly used to distribute encrypted keys which will then be used in faster symmetric protocols.

However, Peter Shor proved in 1994 [12] that a quantum computer can theoretically solve the factorisation problem in polynomial time. The recent experimental demonstration of quantum advantage by Google [13] may indicate the first sign of practical threats to RSA cryptography. The need for new, secure ways of encrypting data is growing.

Symmetric cryptography

Symmetric cryptography relies on both Alice and Bob to share the same secret key. The absence of a public key makes them more secure than public-key protocols, and they are routinely used in classical communications. Like asymmetric protocols, however, the majority of symmetric encryption schemes only offer computational security. The idea is to enlarge the encoding space to bound the probability of breaking the code.

The main difficulty when implementing these protocols is the key distribution. Alice and Bob have to share the same key, so there has to exist a way for them to obtain the key in a secure way. Public-key schemes such as RSA or Diffie-Hellman are generally used to distribute an encryption key between the two parties; they will then use these keys to encrypt their data using symmetric protocols (Figure 1.2).

The standard symmetric scheme used in information technology is the advanced encryp-

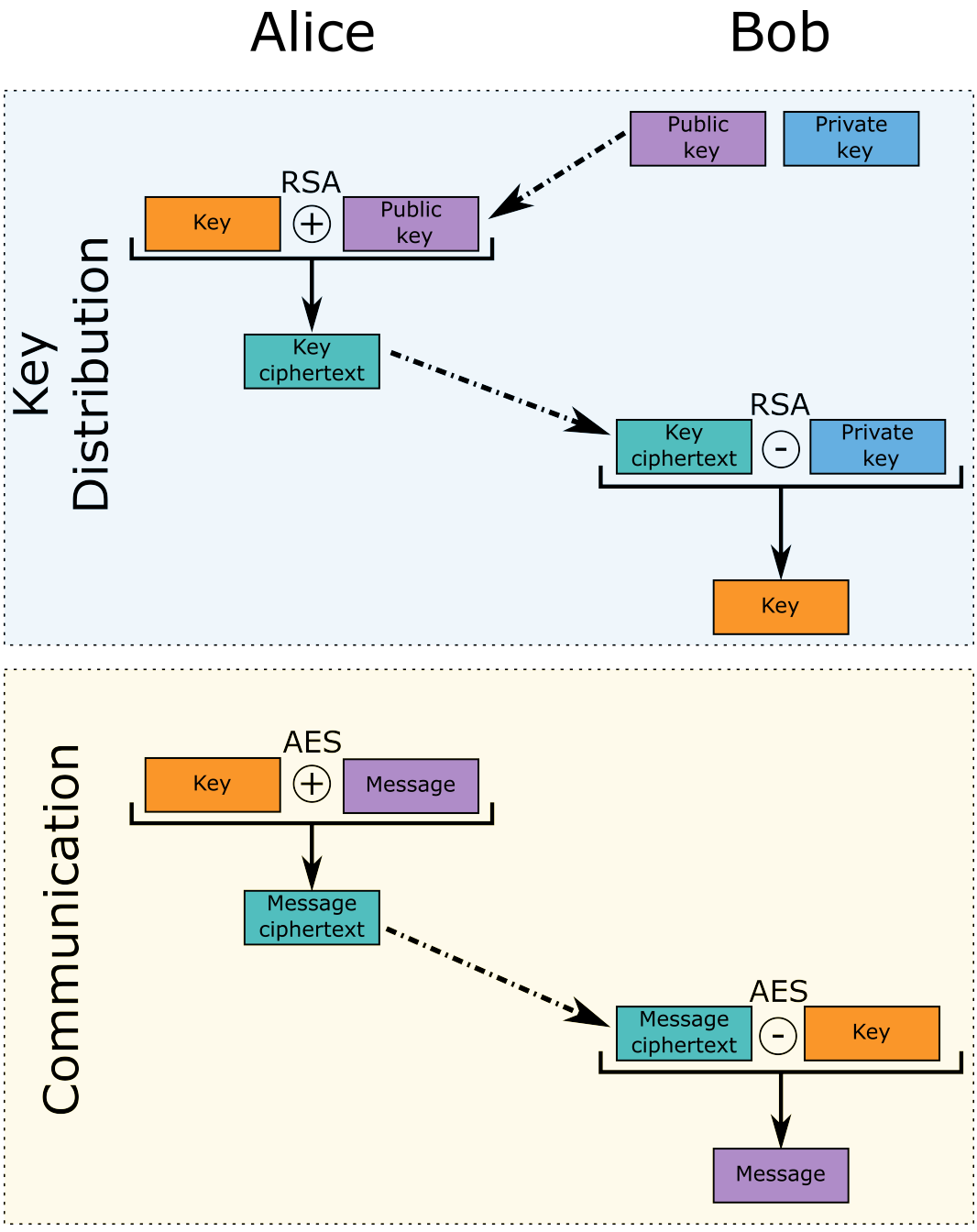

Figure 1.2: Public-key cryptography is used to distribute a key between two parties. The key will then be used to communicate using symmetric protocols. The dashed lines represent public communication between Alice and Bob, the solid lines represent the local operations of encryption and decryption. The operator signs represent the application of the AES encryption and decryption scheme.

tion standard (AES). The protocol is based on a so-called substitution-permutation network, where the plaintext gets manipulated by substituting or permuting the bits depending on the key. This is done several times: for each round of substitutions and permutations, the security of the ciphertext increases, as small changes in any of the rounds get diffused throughout the key and generate very different results. AES is considered computationally secure when the key has a sufficient length (192 or 256 bits, depending on the assumed computational power of the adversary) and enough rounds of substitutions and permutations are performed, however there have been reports of attacks that, while still not effective, could potentially become dangerous with more computational power [14]. Moreover, quantum computing can further decrease the complexity of decrypting AES by exploiting Grover's algorithm [15], although it would still remain a computationally hard problem to solve.

Claude Shannon, in 1949, proved that there is one and only one encryption protocol which is *information-theoretically secure* [16], i.e. which results in a ciphertext giving no information whatsoever about the original message. This **one-time pad** encoding, first introduced by Frank Miller in 1882 [17], is a symmetric encryption scheme. It requires a key satisfying three conditions: it has to be generated randomly, must be as long as (or longer than) the message and can only be used once (ideally, it should be destroyed after use [18]). Failing to meet any of these requirements would result in partial or total loss of security. The key will be summed to the plaintext (modulo 2 sum when dealing with binary strings; in Information Sciences, this is known as a XOR operation) and the resulting ciphertext will look random to an eavesdropper. If the key is generated completely randomly, no algorithm can reverse-engineer it: even performing a brute-force attack (i.e. trying every possible key), it will not be possible to determine which is the right message. For example, the plaintext "QKD" encrypted with a random key will look like a random string of 3 characters. Unless the eavesdropper has previous knowledge about the nature of the message, it will be impossible for them to determine whether the original message is "QKD" or "RSA" or "AES".

Quantum computing will change how we think of data security, by breaking public-key protocols. The need for Alice and Bob to share the same key, combined with the need to keep this key secret, will become a problem when RSA and AES are broken. It is of paramount importance that new key distribution schemes fill in the security gap that quantum computing could create.

1.3 Quantum cryptography

Shor proved that quantum mechanics can be used to break modern cryptographic systems. However, quantum systems can also be exploited to counter such attacks, exploiting the inherent unpredictability of the quantum realm to implement secure communications [19].

Some of the underlying principles of quantum cryptography are deeply rooted into the fundamental principles of quantum mechanics. The no-signalling theorem [20] rules out

the possibility of faster-than-light communication when measuring entangled states. The no-cloning theorem [21] states that it is not possible to create an identical copy of an unknown quantum system. The measurement problem [22] asserts that trying to measure a superposition state makes its wavefunction collapse into one of the eigenstates, effectively disrupting the quantum state. This makes it impossible for any eavesdropper to tamper with the communication without being detected, and is the basis upon which quantum cryptography relies.

While protocols for sending messages in a secure way have been proposed, such as quantum coin flipping [23] or quantum commitment protocols [24], their unconditional security is proven impossible to guarantee [25, 26]. Instead, an efficient way of encrypting information is to distribute a secret key between two parties, which can then use classical encryption protocols to communicate securely.

Quantum cryptography, especially quantum key distribution, has now been around for almost three decades. However, the technology is still at a prototyping stage: while commercial solutions are available, they are usually aimed at very niche applications. While promising, further research is still needed to make this a viable solution for mass marketing.

1.4 Quantum Key Distribution

QKD is a technique which allows the two parties, Alice and Bob, to share an encryption key with information-theoretical security, the highest level of protection, thanks to quantum physics. They can then use their shared key to encrypt and decrypt a message using the one-time pad or, if computational security is enough, AES [27]. Several protocols [19, 28–34] have been proposed and developed, each one exploiting different properties of the quantum nature of light.

Photons are the natural choice for such implementations, as they weakly interact with matter, are easy to manipulate and their quantum properties have been thoroughly studied. They can be sent through long distances using optical fibres with very little losses, and their phase and polarization can be easily manipulated using common optical elements. Moreover, classical communication networks nowadays already rely on optical fibre connections, so there is also an existing infrastructure in which quantum communications can be performed. Both phase and polarisation of photons are used in QKD, depending on the protocols to be implemented; the same protocols can sometimes be implemented in a real-life experiment using either one.

1.4.1 Categories of QKD protocols

The idea behind QKD is that measurements performed by an eavesdropper (Eve) will perturb the quantum state prepared by the legitimate users, potentially introducing errors in the transmission: if Eve performs a measurement on the system in the attempt to steal

information, Alice and Bob will be able to detect her presence from the increased noise in the communication. The noise can be used a measure of the amount of information Eve has access to. A number of errors above a certain threshold means that the attacker has gained enough information to compromise the security of the key.

The way the encoding into light is performed is used to classify QKD protocols into two main categories:

- entanglement-based QKD, where information is shared by Alice and Bob as an entangled photon pair. If Alice and Bob measure their photons individually, they can infer what the other has measured;
- prepare-and-measure QKD, where one party (conventionally Alice) encodes information into quantum properties of light and sends it to Bob who will measure it. Bob will then communicate to Alice some pieces of information (depending on the protocol) so that the two can share the same key.

For the purpose of this thesis, only prepare-and-measure protocols will be considered. These can be further categorised into two categories:

- discrete variable QKD (DV-QKD), based on encoding information into single photons;
- continuous variable QKD (CV-QKD), where information is encoded in the quadratures of the optical fields.

In this thesis, we will only focus on discrete variable QKD, as it represents a more mature field with already established protocols and security analyses.

DV-QKD

This was the first class of protocols to be developed, and the one where the most efforts are currently focussed. Indeed, the very first DV-QKD protocol, the Bennett-Brassard 1984 protocol (BB84) with its variations, is still the most used in experimental implementations of QKD. Information can be encoded in the polarisation, time-bin, or phase of single photons. Some of these protocols, which will be used in the experiments of this work, will be presented in more detail later in this thesis.

At Bob's end, fast and reliable detection of single photons is needed. This makes the receiving end of QKD systems very expensive, as single photon detectors (SPDs) are very sophisticated pieces of equipment. This also means that SPDs are more likely to present vulnerabilities, due to their complexity. Indeed, several attacks have been proposed that would allow Eve to obtain information about the key without being detected. [35, 36] Countermeasures have also been proposed [37], but it is clear that the vulnerability of SPDs constitutes a side channel that would severely hinder the security of QKD.

measurement-device independent QKD (MDI-QKD) [38–40] removes this weakness by introducing a third, untrusted party (Charlie) who is in charge of the detectors, while Alice

and Bob only have transmitting equipment. Charlie performs a Bell-state measurement on the photons sent by Alice and Bob, which interfere with each other, and reveals the result. Alice (Bob) knows what she (he) sent and what the result is, so she (he) is able to infer what Bob (Alice) has sent. This gives Charlie no information at all about the key, so eavesdroppers cannot attack the detectors to infer any information. However, since two-photon interference detection is needed, the achievable key rates decay exponentially with distance, as photons from both Alice and Bob need to be detected by Charlie in the same time bin.

In 2018, building on the concepts of MDI-QKD, a novel protocol was introduced by researchers at TEUR, called Twin-field QKD (TF-QKD) [34]. This protocol relies on optical field interference, rather than two-photon interference, and hence does not require coincidence measurements at Charlie's. This means that higher key rates are achievable, as the decay with distance is now proportional to the loss in one leg of the line. TF-QKD, in fact, is able to reach communication distances and key rates which are proven to be unreachable by standard, point-to-point QKD [41]. This generated a lot of interest in the protocol. Several variations have been proposed [42–44] and proof-of-principle experiments have indeed surpassed the so-called repeaterless bound [45, 46].

DPR-QKD

Distributed phase reference (DPR) protocols can be seen as a variant of DV-QKD protocols. However, rather than on the properties of single photons, these protocols encode information in the phase difference between coherent pulses. Among the advantages provided by protocol based on this concept, there are simple implementations, as they do not require phase randomisation, and inherent security against photon number splitting (PNS) attacks [47], as such an attack would change the photon statistics and can be detected. On the other hand, security against coherent attacks has not been proven for DPR protocols, which means there is no lower bound to the obtainable key rates.

1.4.2 QKD implementations

In prepare-and-measure QKD, Alice sends her encoded photons to Bob through a quantum channel (Figure 1.3). In order to fully characterise a system, it is important to determine the parameters that characterise Alice's light source, Bob's detection apparatus and the quantum channel itself. The following paragraphs will give some information about these elements of a QKD system.

Quantum Channels

The medium through which the information is transmitted (communication channel) plays an important role in QKD. Free space does not require any equipment, however its use is limited by the need for a clear line of sight between transmitter and receiver, as well as the

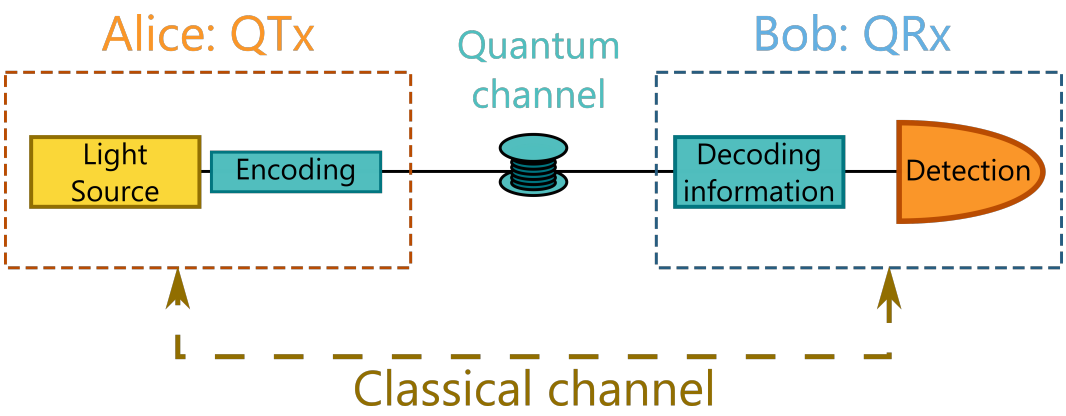

Figure 1.3: A generic QKD system. Alice sends information to Bob through a quantum channel. Communication is still needed through a classical channel for post-distribution steps such as error correction and privacy amplification.

alignment between the parties [48]. Both are influenced by weather conditions [49] (sunny weather introduces a lot of optical noise, rain introduces scattering losses) and the Earth's shape.

A lot of these issues, particularly Earth's curvature and atmospheric conditions, can be addressed by using satellite QKD. Outside of the atmosphere, photon dispersion and losses are heavily reduced, so light has to travel in these conditions only for the few km where the Earth's atmosphere is concentrated [50].

An interesting aspect when dealing with satellite QKD is the difference between sat-to-ground and ground-to-sat links. In particular, while both configurations are being investigated, a downlink configuration (i.e. where the transmitter is on the satellite and the receiver on the ground) seems to be easier to implement from an alignment point of view. This is because light in the space vacuum travels in a straight line, while the atmosphere can cause scattering, inducing losses; if the path through the atmosphere is at the beginning of the link, the beam has a longer distance to travel at a misaligned angle with respect to the detector, hence it is easier for it to be lost. However, if the transmission angle is changed at the end of the path, the beam will not end far off the detector.

The downside to satellite-based QKD is that a link to a specific satellite is only established for a few minutes a day, provided that the weather is clear. A satellite constellation might overcome this issue, however it requires trusting every satellite in the constellation.

Another choice for a quantum channel are optical fibres. They have replaced copper wires for long-distance classical communications, because of the higher bandwidths and distances they can cover. There is, hence, a massive network already in place to be used for QKD, whose signals can be multiplexed with classical information [51, 52].

A point-to-point QKD protocol usually requires two communication channels: a quantum channel, where information is encoded in quantum states, used for private communication,

and an authenticated classical channel, where public communication is performed. Both channels are supposed to be accessible by an eavesdropper with unlimited computational power. However, the key concept is that if Eve tries to attack the quantum channel, she will be detected thanks to the laws of quantum mechanics. The quantum channel will be used for the first step of QKD, i.e. the distribution of the raw keys, while communication on the public channel will be used to perform classical error correction and privacy amplification protocols to extract a secure key.

Light Sources

For DV-QKD experiments, it would be ideal to encode information into single photons. This requires high rate, high fidelity single photon sources in the C-band of telecommunication wavelengths (1530 nm–1565 nm, or 191.56 THz–195.94 THz) to be compatible with current fibre infrastructure. Such wavelengths are chosen because they are the most transparent for optical fibres, which minimises the propagation losses.

An ideal single photon source should emit one and only one photon every clock cycle. Single photon sources are available, however no ideal source has been demonstrated so far. Quantum dots [53, 54], nitrogen vacancy centres in diamonds [55] and many other technologies [56, 57] have been proposed as single photon sources, because of their low multi-photon components, however their emission wavelengths are not within the telecom transmission band.

The best performing sources for QKD, so far, are pulsed lasers attenuated to contain less than one photon per pulse [58–60]. They are cheap, easy to fabricate and can achieve mW optical outputs with low electrical power consumption. The number of photons in each pulse can be modelled by a Poissonian distribution. The probability $P(n)$ of having n photons in a pulse with a mean photon number μ is

$$P(n) = \frac{\mu^n}{n!}\mathrm{e}^{-\mu}. \tag{1.1}$$

If the photon number is higher than one, Eve could obtain more information about the key by performing a PNS attack [61]. Eve has access to the quantum channel; she can perform non-destructive measurements on the states sent by Alice to determine the number of photons in each pulse. She can then split the multi-photon pulses, keeping one photon and sending the rest of the pulse to Bob, and block all the single-photon states. Once Alice and Bob reconcile their preparation and measurement bases, Eve can perform the same measurements as Bob to obtain the same result as the two legitimate parties, without being detected.

In order to minimise the number of multi-photon events, which could potentially open this side channel, the mean number of photons per pulse must be kept low (Figure 1.4). This means, however, that the probability of emitting no photons at all is also higher, which

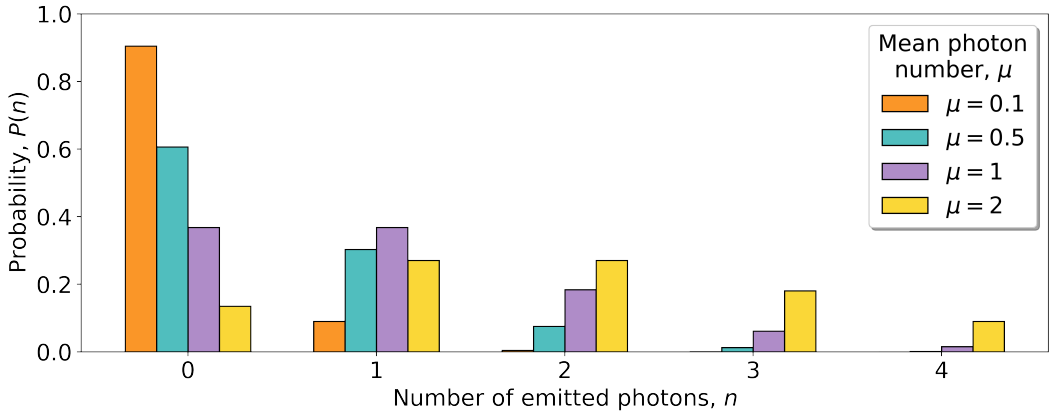

Figure 1.4: Poissonian distribution of the probability $P(n)$ of emitting n photons, for four different mean photon numbers. Higher mean photon numbers have higher probability of multi-photon events.

reduces the obtainable key rates. A solution to this issue is given by decoy states. More details on this will be given later in this thesis (Section 2.1).

Detection

Discrete variable protocols require detectors capable of detecting light at the single photon level. Compared to the ease of use of laser diodes in the transmitting node, SPDs are more complex and expensive. This makes the receiving end of a QKD system a suitable target for attacks that would go unnoticed without the appropriate countermeasures. While MDI-QKD is a way to circumvent this issue, standard point-to-point links are more practical and likely to be used first in real-life implementations. It is important to understand how the devices work in order to spot and prevent potential vulnerabilities.

The most investigated attack to a detector is the blinding attack [62]. Sending bright light into the detector switches its operating mode from the Geiger mode, the regime in which detectors usually operate for QKD, to its linear mode. Eve has now full control of the detector: she can easily control what the detector in linear mode will output. This attack can be detected by monitoring the photocurrent of the detector [35], which is macroscopically high when under blinding attacks. It is also possible to counter the attack by implementing best practices when using the detectors [37]. This reduces the leaked information below the threshold where privacy amplification is not possible.

Another proposed attack to a gated detector is the after-gate attack [63], where bright pulses arrive at the detector outside its activation time. This is thought not to have a dramatic effect on the information Eve can obtain; nevertheless, a countermeasure has been proposed for this attack as well [64].

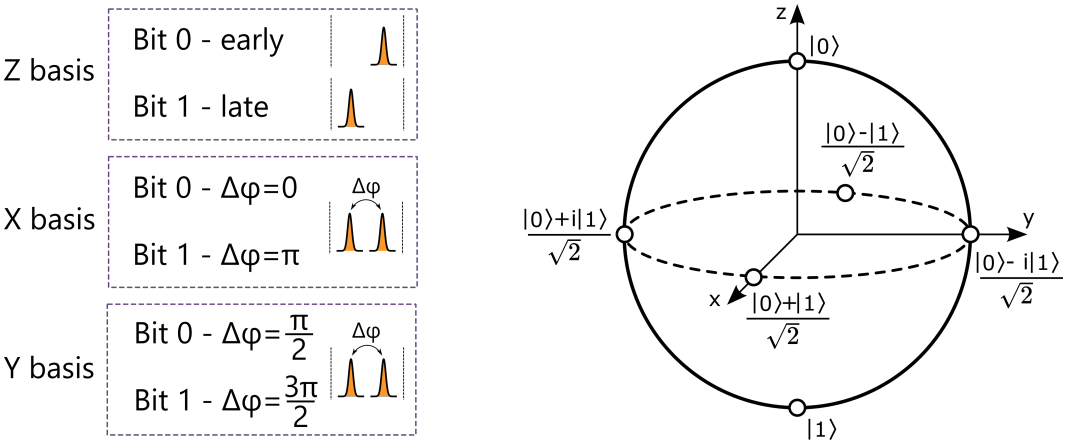

Figure 1.5: Time-bin encoding for the X, Y, Z bases. On the right, the Bloch sphere mapping the six states.

1.4.3 Time-bin and phase encoded QKD

The very first experimental demonstration of QKD was implemented in free space, over a distance of 32 cm [65]. Encoding information in the photon polarisation is a straightforward choice when dealing with free-space channels. Photons travelling through clear air interact very weakly with the environment, hence their polarisation remains stable for long distances. When employing satellites, such distances can be improved even more [66], as weather-dependent losses only affect a small fraction of the path travelled by the photons.

However, most of the research in quantum communications is focussed on fibre-based links. This is because fibre optics is already a well-established technology in classical communications, providing a ready-to-use network for QKD. When travelling through a fibre, polarisation of photons is unstable over time [67]. Even polarisation-maintaining fibres do not guarantee a stable output, especially if connected to elements like phase modulators [68, 69] or even another, slightly different fibre. This would require an active stabilisation system which is usually more complex to implement.

An alternative way of encoding information is time-bin encoding. Information is encoded into two neighbouring time bins: a pulse arriving in the early time bin is assigned to bit 0, while a pulse in the late bin will be mapped onto bit 1. Other bases will be represented as a superposition state of the two bits, $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right)$, where ϕ is the relative phase between the early and late pulses Figure 1.5.

Another approach is to encode the information directly in the phase difference of consecutive pulses. This section will describe the most common way to encode and decode information using phase.

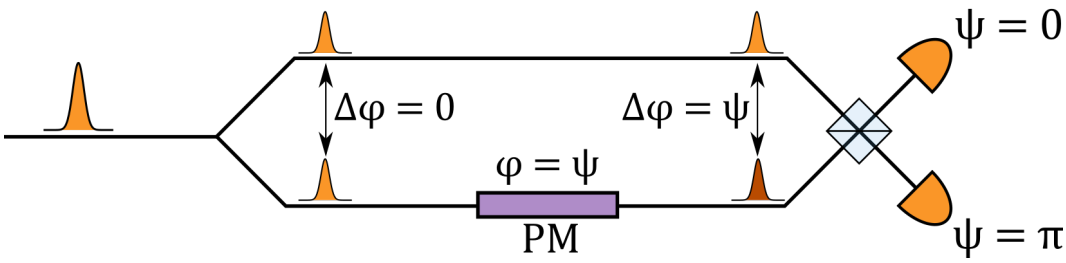

Figure 1.6: Self-interference of a pulse in a MZI. the pulse is divided in two at the first beam splitter, one of the two halves is phase-modulated, and the pulses are recombined in the second beam splitter. The phase difference between the two pulses determines which detector will click.

Phase encoding

The most popular approach to phase encoding employs phase modulators, developed using materials that change their refractive index when a voltage is applied. In particular, Lithium Niobate ($LiNbO_3$) modulators are a popular choice [70, 71]; they are easily fabricated and work on a broad band of wavelengths, as well as having a high modulation bandwidth and low half-wave voltages V_π, i.e. the voltage required to apply a π phase shift to light.

Phase decoding

Differences in phase between two pulses can be measured by having them interfere on a beam splitter: the phase difference determines the probability of the interference pulse being reflected or transmitted. A useful way to visualise this is with a pulse travelling through a Mach-Zehnder interferometer (MZI) (Figure 1.6). When the pulse arrives at the first beam splitter, it is divided into two pulses having the same phase. If one of the arms of the MZI has a phase modulator, the phase of the pulse travelling through that arm can be changed so that the interference with the non modulated pulse will be completely constructive on one arm and completely destructive on the other. Changing the voltage of the phase modulator by its V_π, the opposite behaviour will be observed.

Now, consider the case of a pulse train with a repetition rate of T. Measuring the phase difference between two consecutive pulses is achieved by delaying half of the pulse travelling through one arm by T, creating an asymmetric MZI (aMZI). The non-delayed half of the second pulse will interfere with the delayed half of the first one. If the phase modulator is set to not apply any change to the phase of the incoming pulses, the detectors will then effectively measure the original phase difference between the two consecutive pulses (Figure 1.7). If the phase modulator is applying a different phase on the pulse travelling through it, this is equivalent to performing a measurement in a different basis.

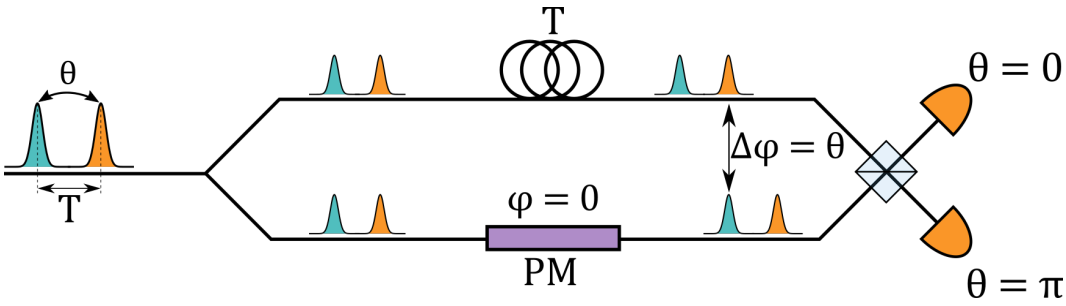

Figure 1.7: Adding a delay to one of the MZI arms allows to measure the interference of two consecutive pulses, as the delayed half-pulse from the first pulse will interfere with the non-delayed half-pulse from the second one.

1.4.4 Extracting a secure key

After the raw key distribution through the quantum channel, Alice and Bob will have to make sure that the keys they use are the same. At the same time, they want to remove all information that Eve might have acquired during the key distribution. This is possible by exploiting well-known concepts in classical communications, such as error correction and privacy amplification.

The first step after the distribution of raw keys is *basis reconciliation*. In QKD protocols that employ more than one basis (e.g. the BB84 protocol), Alice and Bob discard the events where Alice has prepared her state in one basis but Bob measured it in a different one. This way, they obtain a *sifted key*.

At this point, the keys shared by Alice and Bob may not be exactly matching. This is due to different causes such as imperfection in the encoding or decoding systems, stray photons in the channel or eavesdropping. For unconditional security, all errors are attributed to Eve, to assume a worst-case scenario. The usual error rates are in the order of a few percent, but can be reduced to less than 10^{-9}, the standard allowed error rate in classical communications, using classical error correction algorithms [72–74]. During the error correction process, Alice and Bob first estimate the amount of errors by comparing portions of their sifted keys. If the quantum bit error rate (QBER) is lower than a certain threshold (which depends on the protocol), they perform error correction algorithms (such as the CASCADE algorithm [72]) and obtain identical copies of their sifted keys. Otherwise, they abort the protocol and start a new key distribution, because the high QBER has prevented the generation of a secret key.

The last step concerns minimising the amount of information Eve has about the key. This is done by performing *privacy amplification* algorithms [75, 76]. The goal of such algorithms is to reduce Eve's information to an arbitrary small value, starting from an estimated value of Eve's information given by the phase error rate.

Parameter estimation, error correction and privacy amplification are all performed over the public, classical channel. This means that every bit used to perform them is disclosed

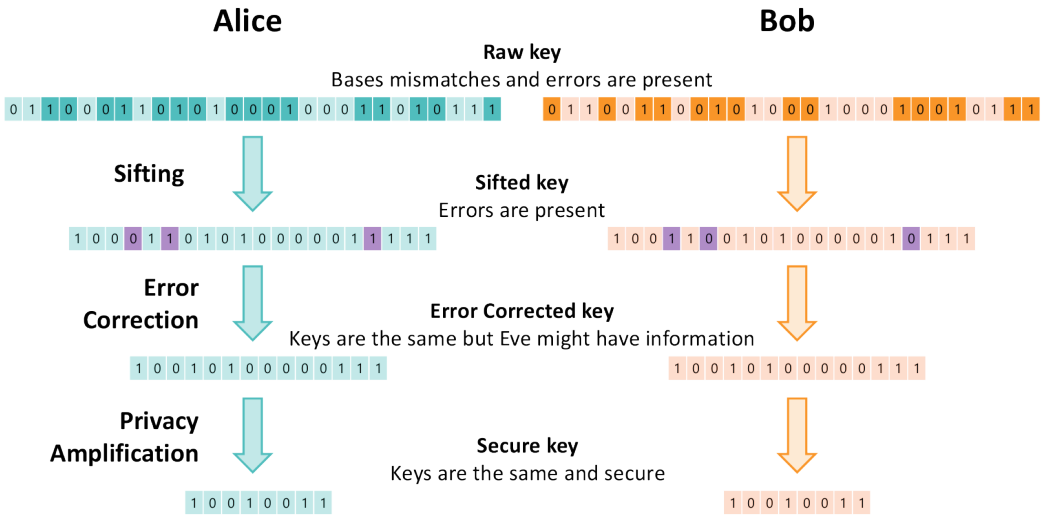

Figure 1.8: The process of extracting a secure key. Each step makes the key shorter: basis reconciliation discards all events where Alice and Bob measured in different bases; during error correction, random bits of the sifted key are made public and hence are discarded; finally, the privacy amplification algorithm further reduces the key length.

publicly, so it must be discarded. The final *secure key*, hence, will be much shorter than the sifted key (Figure 1.8).

Key rates estimation

When characterising a QKD system, it is usually impractical to go through all the steps described in the previous paragraph. The goal of the majority of experiments performed in a laboratory is to assess the capabilities of a QKD system. This can be done without actually extracting a key, but rather by estimating the *key rates* that the system is capable of generating as a function of the communication distance [77]. In such QKD experiments, the same raw key is exchanged repeatedly, and cumulative data is recorded by a SPD. The QBER is then easily computed by the number of clicks in the time bins where no click was expected, over the total number of counts.

The quantities that are usually considered when estimating key rates are the QBER, Q, which has been discussed, and the *sifted key rate*, R, which measures the amount of data recorded by Bob in the correct basis per state sent by Alice. In the asymptotic case, i.e. when considering infinite-length keys, the secure key rate (SKR) will be a simple function, depending on the protocol, of these two parameters:

$$S = f(Q, R). \tag{1.2}$$

In real scenarios, however, the key exchange will eventually stop: the key length will have a

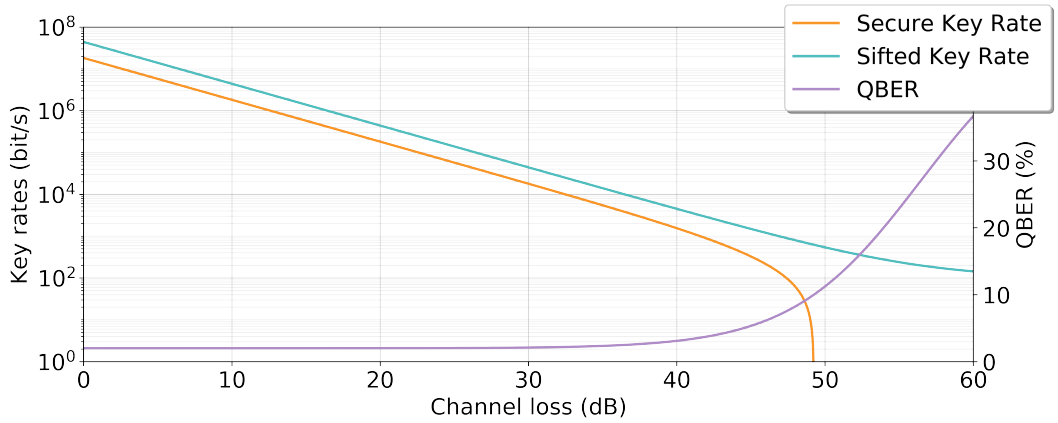

Figure 1.9: Sifted key rate, SKR and QBER as a function of the channel loss for the BB84 protocol. This simulation a clock rate of 1 GHz, a photon flux of 0.55 photons per pulse, a detector efficiency of 75%, dark count rates of 50 Hz and losses in Bob of 12 dB.

finite size. This makes the extraction of a secure key more complicated, because there will be an uncertainty in the values of Q and R [78–80]. The SKR for a raw key of size n can be calculated as:

$$S_{FS} = \xi f_{FS}(Q + \sigma_Q, R - \sigma_R) - \Delta(n, \epsilon), \tag{1.3}$$

where ξ is a factor representing the uncertainty on error correction and privacy amplification, f_{FS} is a different function than f, still depending on the protocol, and $\Delta(n, \epsilon)$ contains information about parameter estimation, error correction and probability that the protocol fails. Note that the parameters of f_{FS} also contain the standard deviations of Q and R. This is because the calculation outputs a lower bound on the SKR. Hence, the parameters used to compute it must be assumed to represent a worst-case scenario, where the error rate is higher and the sifted key rate lower than the average value.

Figure 1.9 shows an example of how the sifted and secure key rates, as well as the QBER, vary as a function of the channel loss. The QBER will start off at a base value at short distances, due to encoding imperfections and potential attacks from Eve. As the distance increases, more photons are lost in the channel. This means that detection by Bob become more likely to be caused by dark counts, rather than actual photons sent by Alice. This increases the error rate. The sifted key rate, expressed in bits per qubit, will depend on factors such as the detection efficiency and the loss of the quantum channel.

1.4.5 State of the art

Record communication lengths and key rates

Toshiba holds the current record for the highest key rates achieved over a 10 km channel, with 13.7 Mbit/s during a continuous 5-day experiment [81]. The experiment used fast detection

equipment that allows for higher rates of post-processing for sifting, error correction and privacy amplification.

The longest distance achieved in a point-to-point QKD link was achieved in 2018 by the University of Geneva [82]. They used a very optimised system with ultra-low-loss fibres and detectors with very low dark count rates, to achieve key distribution at a distance of 421 km. The previous record was held by the same group, who reached 307 km in 2015 [83], however using a protocol which is not secure against coherent attacks.

The newly introduced TF-QKD allowed to extend the maximum distance of key distribution to more than 500 km, which has been done by Hefei University reaching 509 km in 2019 [84].

Satellite QKD can reach even longer distances [85]. An experiment from Hefei University in 2017 [86] demonstrated kbit/s secure key rates over more than 1200 km using their Micius satellite as a trusted node. This also allowed for the world-first QKD-secured teleconference between the Chinese and the Austrian Academies of Sciences [87].

For CV-QKD, the record distance of 202.81 km was achieved in 2020 in Beijing [88], obtained by using an ultra-low-loss fibre link and carefully controlling the excess noise, as well as using an optimised algorithm for reconciliation.

QKD Networks and miniaturisation

Scaling QKD to reach as many users as possible is a foreseeable goal in the mid-short term. Indeed, multi-user QKD networks have already been demonstrated and some are actually active. Network implementations have been shown in the United States of America [89], Austria [90], South Africa [91], Switzerland [92], Japan [93], China [94] and England [95].

Reaching more users will require smaller and cheaper devices. In 2017, the University of Bristol demonstrated an Indium Phosphide (InP) transmitter chip for QKD capable of encoding information in different protocols [96]. The approach employed several Mach-Zehnder modulators and electro-optical phase modulators (EOPMs) to carve pulses from a continuous wave (CW), on-chip laser and modulate them to encode QKD states.

In that same year, they also demonstrated Silicon-based QKD encoders for different polarisation and phase encoded protocols [97]. This is similar to the approach followed by the Massachusetts Institute of Technology, which employed a similar encoder to perform a metropolitan test between two of their laboratories, in 2018 [98].

Chip-based QKD, which is the scope of this work, has been demonstrated to match bulk optics implementations [99]. Work has been carried out to also develop handheld devices [100–102]. These technologies will surely affect the development of secure communications in the future.

Chapter 2

Phase-encoded QKD protocols

The BB84 protocol introduced the concept of quantum cryptography and QKD. It is still the most used protocol in QKD implementations, and by using decoy states can reach even longer communication distances. After that, a plethora of new protocols were introduced, all with their on advantages and drawbacks. In particular, two of the other protocols that are often used in experiments are the differential phase shift (DPS) and the Coherent One Way (COW) protocols.

This chapter will describe these three main QKD protocols that will be used in the experiments of the thesis.

2.1 The BB84 protocol

The protocol introduced by Bennett and Brassard in 1984 [19] paved the way for the field of quantum cryptography. The original protocol relied on encoding information in the polarisation of photons, using the states $\{0, 1\}$ in the computational basis, or Z basis, and $\{+, -\}$ in the diagonal basis, or X basis (Figure 2.1). A variation of this protocol, instead of using the photon polarisation, encodes the bits in the time bins of weak coherent pulses in phase randomised pairs. The protocol relies on superposition states between time bins encoded in two non-orthogonal measurement bases, X and Y. Some other variations include a six-state encoding with the Z basis as well [103].

In the four-state scenario, the X basis $\{0, 1\}$ bits will be encoded with phase shifts of $\{0, \pi\}$ respectively, while the Y basis will have phase shifts of $\{\pi/2, 3\pi/2\}$. The usual setup for such an encoding consists of a gain-switched laser attenuated at the single photon level. Gain-switching the laser generates pulses which have a random phase (Figure 2.2). Pulses are generated at a rate $2T$, then sent through an aMZI with a delay of T. The short arm has a phase modulator to encode the bit value onto the pulse pair. The output of the aMZI is a train of pulses separated by T. Pulse pairs generated by the same initial pulse will have a coherent phase difference determined by the phase modulator. On the other hand, pulse

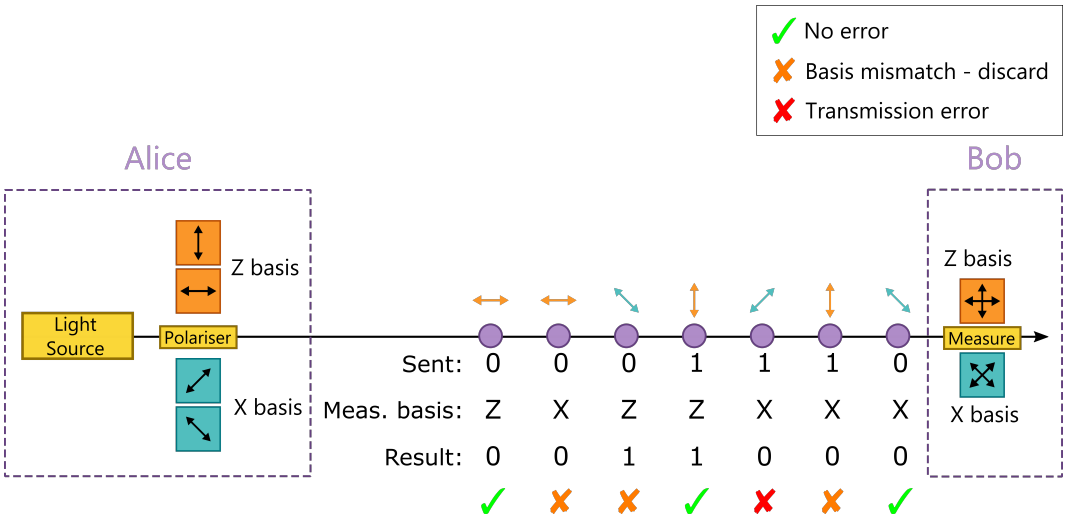

Figure 2.1: Schematic of the polarisation-encoded BB84 protocol. Alice prepares her qubits in two different bases, chosen at random, and Bob randomly chooses in which basis to measure them. They then discard the events with a basis mismatch. Eavesdropping and channel losses introduce errors when the bases are matching.

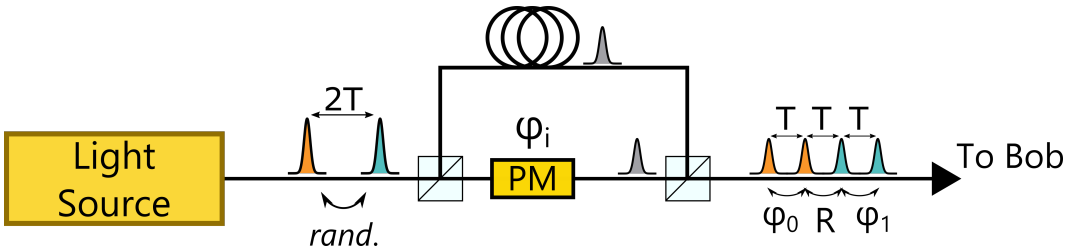

Figure 2.2: Transmitter setup for time-bin encoded BB84. Gain switched pulses are prepared and split into an early and late pulse. The pair of early-late pulses will have a coherent phase difference. Pulses belonging to different time bins will have a random phase difference.

pairs where the pulses were generated by different gain-switching events will have a random phase. This is crucial for phase randomisation, as mentioned in Section 1.4.3.

Such an approach is easily implemented, as it only requires a laser and fibre-based interferometers are relatively easy to manufacture. However, the long arm of the aMZI is more affected by phase drifts, making the alignment of the interferometer rather unstable: active stabilisation systems are needed to compensate for the phase drifts. Another approach is to use a carved CW laser beam to generate pulses, and a phase modulator to encode both the bit phases and the random phases. This requires an intensity modulator to carve the pulses, adding to the complexity of the system, and electronics working at double the speed. An alternative approach based on injection locking and direct phase modulation is presented in Chapter 5.

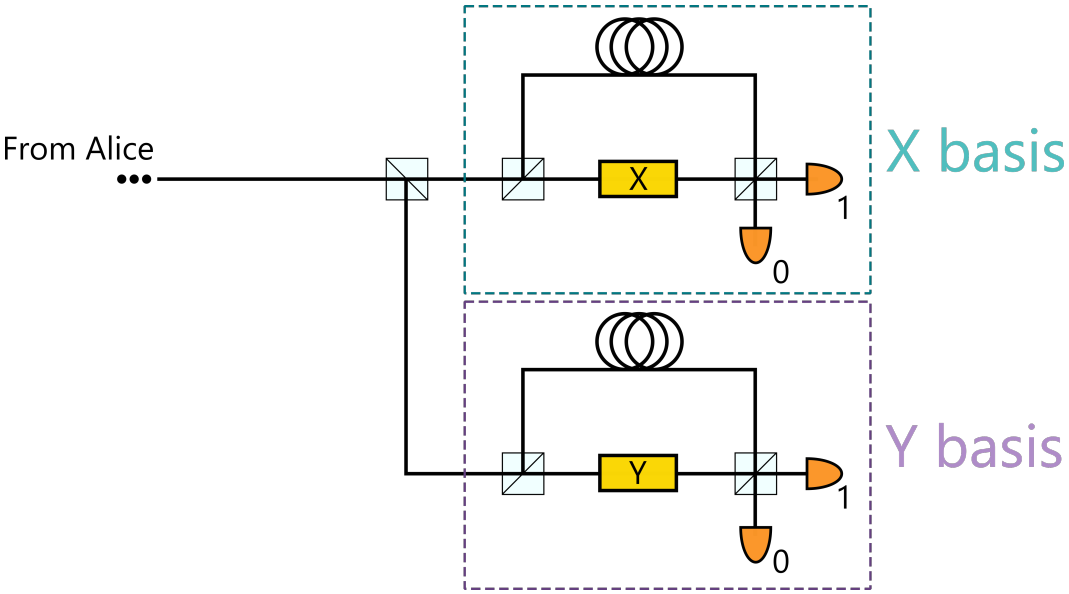

Figure 2.3: Passive receiving two-interferometer setup for the BB84 protocol. The phase modulators in the short arms determine which phase the interferometer is measuring.

At the receiving end, Bob will need to detect photons in two bases. This can be done by high-speed phase modulators actively changing the measurement basis. However, this requires high-speed electronics that would add to the complexity of the system. The usual way to go around this limitation is to measure passively in both bases, by splitting the line into two interferometers, one set to measure in the Z basis, the other in the X basis (Figure 2.3). Such a setup, however, can become hard to stabilise; moreover, SPDs are the most expensive equipment in a QKD system, so doubling the number of needed detectors can cause a large increase in costs. For proof of principle experiments, it is often sufficient to use one interferometer only, and perform measurements in the Z and X bases separately.

Phase randomisation

Another important aspect of phase modulation for the BB84 is phase randomisation. Randomness is crucial in QKD: the initial raw string sent by Alice must be random; the bases in which Alice and Bob choose to prepare and measure the states must be random; finally, the global phase of pulse pairs must be random [104], while pulses belonging to the same pair will have a fixed phase difference representing the (randomly chosen) bit and basis.

This is important because it prevents Eve from obtaining information about the key [105, 106]. A laser emits a coherent state $|\alpha\rangle$ that can be expressed as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,, \tag{2.1}$$

where $\alpha = \sqrt{\mu} e^{i\theta}$; μ is the mean photon number, θ is the phase of the pulse and $|n\rangle$ is the

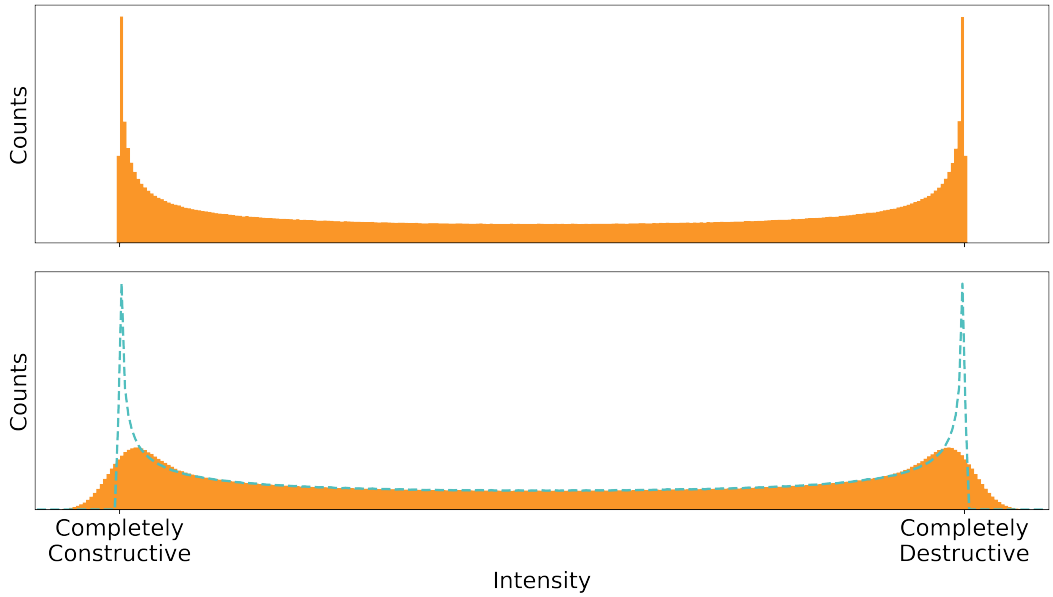

Figure 2.4: Histogram distribution of the intensities from interferences of uniformly distributed phase differences, in scenarios with (top) and without (bottom) classical noise. In the bottom plot, the blue, dashed line represents the noiseless case, to highlight the discrepancies.

Fock state with n photons. If the phase distribution is random, then the measurement result is indistinguishable from a Poissonian distribution of Fock states:

$$|\alpha\rangle\langle\alpha| = \int_0^{2\pi} \frac{d\theta}{2\pi} \left|\sqrt{\mu}e^{i\theta}\right\rangle\left\langle\sqrt{\mu}e^{i\theta}\right| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n| \,. \tag{2.2}$$

One way of measuring randomness is to send a train of phase-randomised pulses through an aMZI. If the phase difference between two consecutive pulses is random, the detectors will measure different intensities of light at every clock cycle. This intensity is proportional to $1+\cos(\Delta\varphi)$, where $\Delta\varphi$ is the phase difference between two pulses. If the phases are uniformly distributed in the interval $[0, 2\pi]$, the histogram of the intensities should be symmetrical and peaked at the values corresponding to completely constructive and destructive interferences. This U-shaped histogram (Figure 2.4, top) is one of the signatures that the system has some noise of a quantum origin.

In real devices, other sources of noise occur, such as thermal and electronic noise. When these alone are considered, they produce an intensity distribution which is gaussian. When combined with the quantum emission, this produces a U-shaped histogram whose peaks are wider and lower (Figure 2.4, bottom). The min-entropy of the generated numbers can be measured to estimate how many truly random bits can be extracted from the raw string.

Decoy states

The security of the BB84 protocol is based on the assumption that Alice is able to send Bob perfect single photon states. Unfortunately, as discussed in Section 1.4.2 (Figure 1.4), this is not the case for weak coherent pulses. The poissonian distribution of photons in pulses implies that some of the generated pulses will have more than one photon. This will enable Eve to perform a PNS attack, by blocking all the single-photon events and intercepting a photon from multi-photon states [61]. Since lowering the mean photon number would lead to a dramatic decrease in the SKR, it is necessary to find new alternatives.

Decoy states were introduced to overcome this vulnerability [107]. Alice will choose multiple intensity levels (usually 3, one signal and two decoy states) for her pulses when sending them through the quantum channel. The decoy signals are sent at a lower intensity than the signal pulses: this means that they will have a lower number of multi-photon events, hence Eve will block more decoy pulses than signal pulses. At the end of the transmission, Alice announces which intensities she has used for each qubit. If the QBER for signal and decoy states are different (net of the lower count rates for decoy states), then Alice and Bob can conclude that an eavesdropper has attempted to intercept the transmission.

The security of decoy-state BB84 has been first proven for an infinite amount of decoy states [31], allowing SKRs scaling in the same way as the ideal single-photon case [32, 108]. However, later research has shown that practical implementations only need two decoys [109–111] to achieve a SKR not far from the infinite-decoy case. For the finite-key size scenario, one decoy state has been proven to be better than two, allowing experimental implementations to be even easier to implement [112]. The introduction of decoy states has allowed QKD systems to reach record lengths [82] and key rates [81].

2.2 The DPS protocol

The DPS protocol [113] is a DPR protocol that builds on the idea of phase-encoded BB84 but eliminates the need for an aMZI at the transmitting end (Figure 2.5). The laser source generates a sequence of weak coherent pulses, all sharing a phase reference frame. Each pulse is then modulated with a phase of $\{0, \pi\}$ relative to the previous pulse, and sent to Bob.

The simpler setup allows for an easier implementation of the protocol. The need for one basis only, rather than two, and the absence of phase randomisation, make all detected photons count towards the raw key rate. This would provide a raw key 4 times longer, assuming that every pulse now is coherent (instead of having a random interference every other pulse) and that Bob and Alice do not have any basis mismatch (which causes an error 50% of the time for BB84). Measuring in one basis only also has the advantage of simplifying the receiving system: Bob needs only one passive interferometer (as previously shown in Figure 1.7) with two SPDs to measure the interference of consecutive pulses and obtain the raw key. After the transmission, Bob reveals on the public channel the times at which his

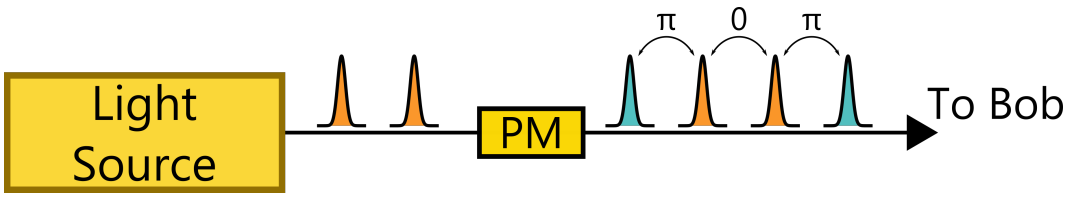

Figure 2.5: Transmitter setup for the DPS protocol. The light source is assumed to output coherent pulses. This scheme requires time synchronisation between the driving signals of the light source and the phase modulator.

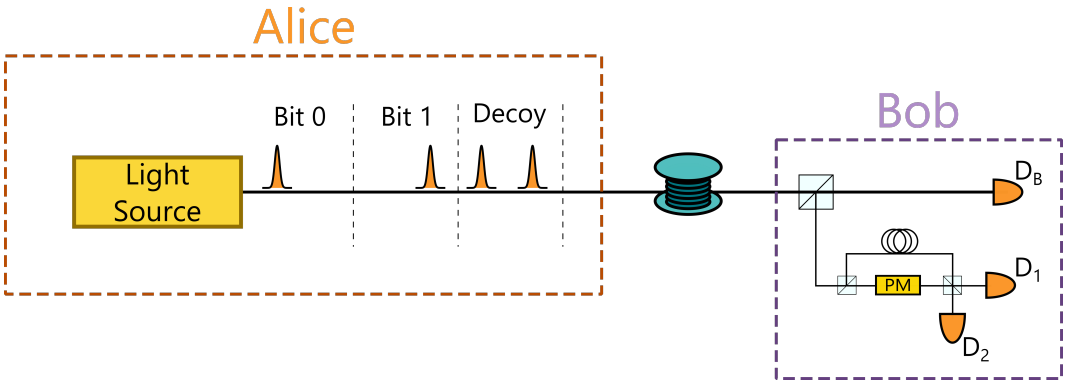

Figure 2.6: Experimental setup for the COW protocol. The light source is assumed to output coherent pulses.

detectors clicked. From that information, Alice knows which pulses have interfered and the phase difference between them: from that, she infers which detector clicked at Bob. This way both parties can agree on a raw key, as long as a click on either detector is assigned to the same bit by Alice and Bob.

The security of this protocol has been proven in the asymptotic key scenario [114, 115]. However, coherent attacks in the finite key-size scenario are a big vulnerability that makes it impossible to extract a secure key of finite length at long distances [116]. It is an open question whether this protocol is secure against general and side-channel attacks [117].

2.3 The COW protocol

Another distributed phase reference QKD (DPR-QKD) protocol that does not require phase modulation in the transmitter is the COW protocol [118]. The information is encoded in the time of arrival of coherent pulses. This removes all errors related to imperfect phase encoding.

A schematic of the protocol is shown in Figure 2.6. Alice sends coherent pulses of mean photon number μ and encodes information in the time bins of pulse pairs: a $\{\mu - 0\}$ pair represents bit 0, $\{0 - \mu\}$ encodes bit 1. A decoy pair $\{\mu - \mu\}$ is also sent for added security.

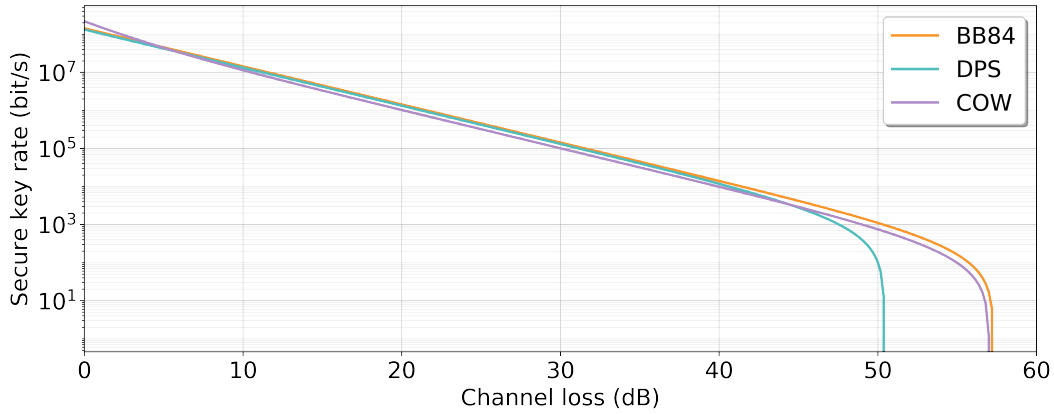

Figure 2.7: Comparison between the asymptotic key rates of the decoy-state BB84, DPS and COW protocols, with optimised parameters.

Bob measures the time of arrival on his detector D_B and, to check for eavesdropping, splits his line and sends part of it through an aMZI. Since the pulses are coherent, when consecutive pulses interfere only detector D_1 should click. A loss of coherence will make D_2 click, increasing the error rate. When estimating the key rates, this can be measured from cumulative measurements as a decrease in the contrast, V, between the two detectors:

$$V = \left| \frac{C_1 - C_2}{C_1 + C_2} \right|, \tag{2.3}$$

where C_1, C_2 are the counts on detectors 1 and 2, respectively. In this case, D_1 and D_2 are considered to have the same efficiency.

During the public discussion stage, Bob announces the times when D_B has clicked and the times when his monitoring detector D_2 has clicked. This gives Alice information on what Bob has measured and reveals the amount of information that Eve might have obtained by monitoring the statistics of detection on D_2. She announces what pulse pairs were decoys so that Bob can remove those, and Alice and Bob can proceed to extract the secure key.

A comparison between the asymptotic SKRs obtainable with the three protocols presented is shown in Figure 2.7. The BB84 assumes a decoy-state experiment with coherent attacks. For the DPS and COW protocols, collective attacks are considered instead.

The photon fluxes are optimised for each protocol to obtain the highest secure key rates. In particular, the BB84 protocol has photon fluxes of 0.55 ph/symbol, 0.05 ph/symbol, 1×10^{-6} ph/symbol for signal, decoy and vacuum states respectively; the DPS protocol features a photon flux of 0.2 ph/symbol and the COW protocol uses 0.4 ph/symbol. A symbol is defined as a pulse pair for the BB84 and COW protocol, while the DPS protocol encodes one symbol per pulse. For this reason, the same laser clock rates give a symbol rate that is twice as high for the DPS protocol. This comparison assumes a receiving system with no losses and a detector with 80% efficiency and dark count rates of 100 Hz.

For the BB84 protocol, security against coherent attacks does not cause a large decrease in the SKR. However, this is not the case for DPR-based protocols. The COW protocol has been proven to be secure against collective attacks, allowing to reach a distance of 307 km [83]. However, security proof against coherent attacks for both the DPS and the COW protocols has been produced in 2012 [116]. It was found that requiring security against this kind of attacks severely limits the maximum distance achievable by these protocols. The maximum distance obtainable in this case is around 50 km. Additionally, an upper bound was found for the COW protocol, further proving that such protocol is not suitable for long-distance communications [119].

Chapter 3

Photonic integrated circuits

Many fields, from science to telecommunications, employ lasers and all sorts of photonic devices to modify the properties of light. However, such elements quickly become hard to maintain when scaling to larger dimensions: dealing with hundreds, even thousands of optical components is a struggle both for space management and for cost effectiveness. This might prevent people from performing elaborate experiments or developing new products due to constraints on resources.

Integrated photonic can overcome these issues by allowing the miniaturisation of a plethora of components to be implemented on a small chip. A photonic integrated circuit (PIC) is a device that embeds several optical components onto a substrate (chip). The main advantages of PICs are *miniaturisation* and cost reduction: the same number of components that can be embedded in a chip would require larger space resources and increased costs of production, if assembled in bulk optics.

PICs are now used widely in classical communications, especially in fibre optic networks. Transmitters can be implemented that allow to generate Tbit/s data rates [120], and interconnects between a multitude of nodes are possible in a small amount of space [121].

The basic concepts of integrated photonics are presented in this chapter, along with a description of some of the main applications of this technology.

3.1 Integrated photonic platforms

The technology is now at a stage where photonic chips are developed on several different substrates, each providing a platform with its own features and limitations. Similar to electronic circuits, PICs provide a path (waveguide) to route light towards the components which change its properties. The way waveguides and components are implemented on a PIC depends on the specific platform.

Waveguides on borosilicate glass, for example, are fabricated by focussing a high-power laser beam on a point inside the material [122, 123]: this locally changes the index of

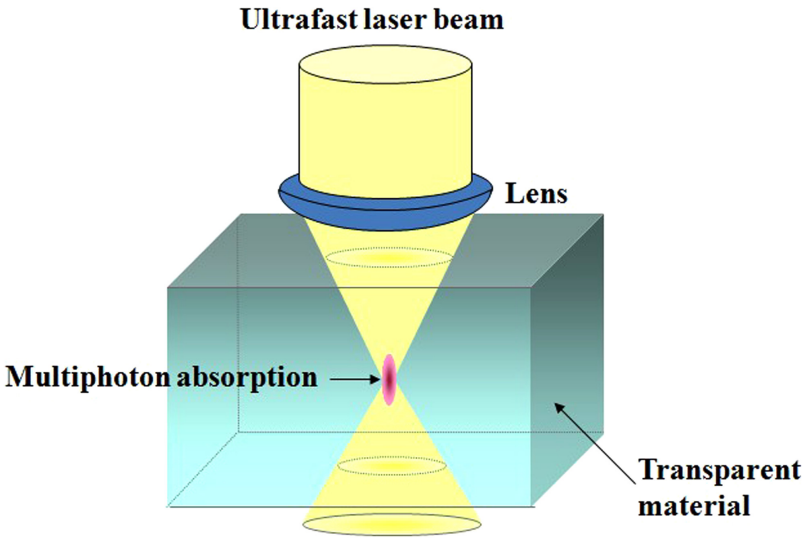

Figure 3.1: Femtosecond laser writing: a highly focussed, pulsed laser beam is used to write waveguides on a glass substrate [124].

refraction, due to nonlinear absorption processes. Moving the substrate creates paths where light will move at a different speed from the rest of the material: this allows to "write" waveguides in the glass. Changing the laser parameters (power, pulsing time, wavelength, beam profile) will give different shapes of the waveguides due to the heat diffusion from the focussed beam. This way it is possible to carefully choose parameters in order to write circular waveguides, which are polarisation insensitive. This fabrication technique also allows for 3D structures to be written. In quantum simulation, a 2D quantum walk is used to simulate a 1D system evolving over time, mapping time in one of the spatial dimensions. In the same way,being able to write 3D structures is useful when implementing 2D quantum walks (the dimension through which light propagates maps time) or to have directional couplers with different splitting ratios without modifying the phase of the photons.

Other materials, such as semiconductor-based chips, are fabricated using lithography [125, 126]: the basic procedure to fabricate a photonic chip in this way (Figure 3.2) starts with the application of a light-sensitive photoresist to the wafer; a mask of the device to be written is applied on top and ultra-violet light is shone onto the wafer. The mask shields the photoresist, while the exposed photoresist reacts to the light and gets removed using a solvent, leaving the material exposed. Finally, the exposed oxide is etched and the remaining photoresist is removed.

This process does not provide 3D capabilities, and the waveguides present high birefringence which makes polarisation independence hard to achieve, though there have been demonstrations of polarisation-independent waveguide filters fabricated in InP [127]. On the other hand, birefringence can be exploited for polarisation control techniques, such as filtering [128]. Moreover, the possibility of growing active components such as lasers and

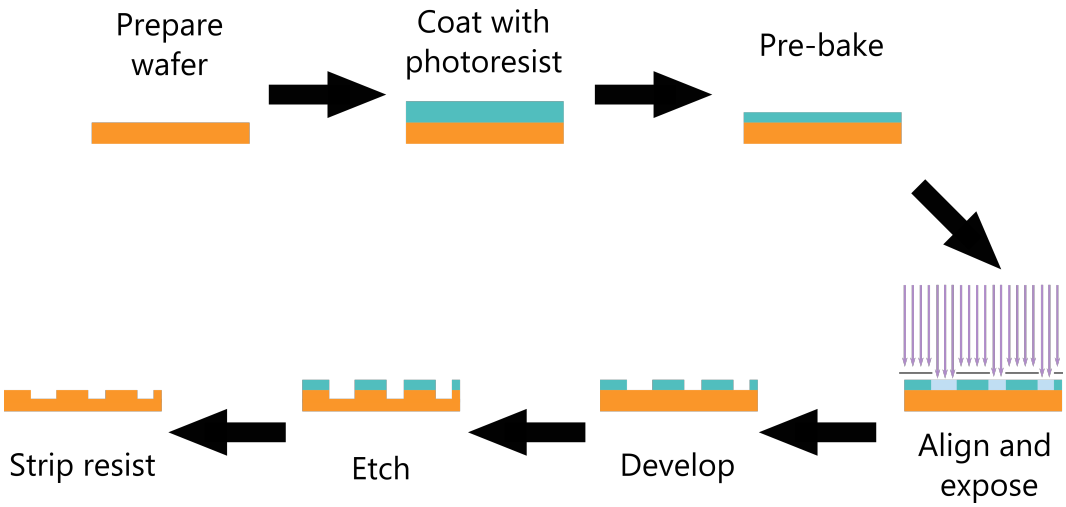

Figure 3.2: Basic fabrication process of a PIC using lithography.

high-speed components such as phase modulators directly on chip makes up for the lack of polarisation independence.

The exposing section of the process can be performed using several different techniques. Contact lithography is the most common process; a mask is put in contact with the resist and a uniform light is shone upon the wafer. Such a process is inexpensive and relatively easy to develop, however it is susceptible to defects in the mask and substrate, so it has been progressively phased out in favour of projection masks, which are smaller and projected onto the wafer many times. Based on the type of exposure the wafer goes through, different spatial resolutions can be achieved. Conventional UV or deep-UV techniques allow to reach resolutions in the order of the µm. The limitation is mainly due to diffraction as light propagates through the photoresist.

A major advantage in resolution can be achieved through electron-beam lithography. This is a form a maskless lithography that employs focussing an electron beam on the resist. The lack of a mask allows for direct writing of a pattern on the wafer. Moreover, the resolution achievable with this technique is less than 10 nm. On the other hand, e-beam systems are usually very expensive, and the serial writing makes them relatively slow compared to parallel, mask-based lithography. For this reason, e-beam lithography is generally only used for low-volume production.

3.1.1 Silicon photonic circuits

The field of microelectronics made silicon chips extremely common. Technology is at a very advanced stage, and silicon chips are now the main building block for microprocessors, memories and other electronics. The ability to process optical signals with silicon chips, hence, is very important for the industry. Integrating photonic components onto this platform will

be extremely useful to create new ways of processing information, e.g. by providing ultra-fast connection between the cores of a processor, where the bandwidth of electronic connections currently acts as a bottleneck [129]. Silicon waveguides are relatively easy to fabricate [129, 130]. Phase modulators have also been demonstrated [131], allowing for modulations of up to 40 Gbit/s [132]. Silicon Oxy-Nitride (SiO_xN_y) is a particularly good choice for photonic circuits. The platform offers low losses, <1 dB/cm, and a tight mode confinement that reduces bend losses in the waveguide: this is especially useful when fabricating circuits with long delay lines, as allowing for tighter bending radii makes the circuit more compact.

However, the indirect band gap of silicon means it is an impractical platform for the implementation of lasers and detectors at telecom wavelengths. Research is ongoing to overcome this issue, but the results so far are not encouraging. One possibility is hybrid integration [133], where a laser fabricated in another platform (usually Indium Phosphide) is bonded to a silicon chip. If having an external light source is not an issue, Raman amplification can be performed on Silicon chips, thanks to the high Raman gain and the tight waveguide confinement [134–136].

3.1.2 Silicon-on-insulator photonic circuits

An interesting platform which has gained a lot of interest in the field of integrated photonics is Silicon-on-insulator (SOI). Differently from standard Silicon devices, in SOI devices the Silicon junction is placed above an insulator: this largely reduces parasitic capacitance within the device [137] in electronic chips. In integrated photonics, the presence of an insulator enables a good light propagation in the Silicon waveguide, thanks to the high index contrast between Silicon and insulator [125].

3.1.3 Indium Phosphide photonic circuits

In applications where light generation or detection is needed in the telecom band, InP is more practical than Silicon-based platforms [138]. Active components are grown on the chips through epitaxial processes; the active regions of lasers and electro-absorption modulators (EAMs) can be fabricated with a multi-quantum well structure, which exploit exciton resonance to enhance the device performance. Already in the late 1980s, photonic chips integrating distributed feedback (DFB) lasers and EAMs were introduced [139]. Nowadays, the technology has evolved, reaching transmission data rates of >10 Gbit/s [140]. Higher bit rates are achievable by multiplexing signals from different lasers [141], and chips with over 1700 components have been fabricated to reach Tbit/s rates [142]. Among the plethora of other components InP allows to fabricate, there are wavelength-division multiplexing circuits based on Bragg gratings [143], P-I-N photodiodes for light detection [144] and polarisation mode splitters [145].

Compared to Silicon, InP is a lossier platform (∼3 dB/cm), but the high powers of the lasers, as well as the small footprints of these chips, make this issue negligible when

developing PICs. In applications where losses are a concern, hybrid integration with Silicon-based waveguides appears to be the most promising way of minimising propagation losses.

3.2 Generic integration processes

While it is easy to find similarities between electronic and photonic circuits development, it is also important to highlight the differences. Being at such an early stage, photonic circuits are now mostly built with specific applications in mind. This makes it not worth investing into low-cost manufacturing processes, which in turn makes it harder to afford photonic chips.

Such an issue is currently being addressed by the development of *generic integration processes* [146]. Much like in electronic integrated circuits, some optical components (e.g. lasers, phase modulators, photodiodes, waveguide splitters) are commonly used in almost every application: foundries can work to standardise them as basic building blocks, and provide users with a library of such elements (Figure 3.3). Users can then design their own circuits using standard components, which allows the foundry to fabricate them at once using multi-project wafers (MPWs): chips designed by different clients can be fabricated on the same wafer because they all share the same components. This dramatically cuts the costs and timescales of fabrication: foundries will not have to run dedicated fabrication process for each user, and users will share the costs of MPW runs among each other. Moreover, since a single run can manufacture a large amount of chips, production times are greatly reduced, paving the way for mass production.

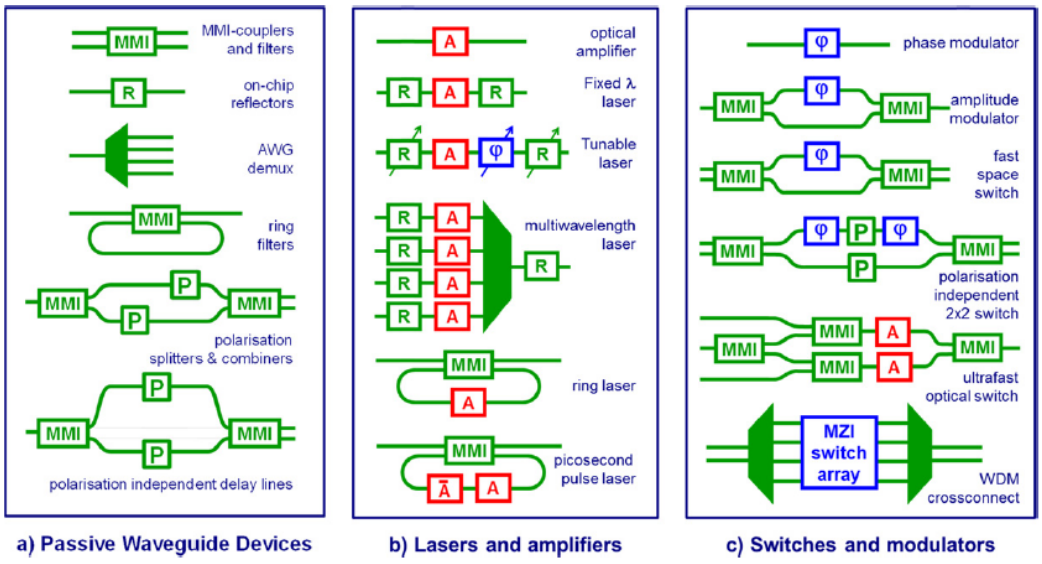

Figure 3.3: Examples of basic building blocks available for photonic circuit design [146].

It is worth noticing how, despite the development of generic integration processes, there

are still significant differences between electronic and optical integrated circuits. Notably, the development of electronic circuits has already established a world-wide standard, whereas the building blocks for optical circuits are developed individually by the foundries. Moreover, while copper is the standard platform for electronics, PICs can be fabricated using several different materials: this is important, as it highlights how the field is still at an early stage of development. Hybrid integration is once more the best candidate to fill in this gap: Silicon-based platforms can act as the equivalent of copper for waveguides and passive components, while lasers, modulators and other active components can be integrated from another platform like InP, in a similar way as components like transistors or amplifiers are placed on an electronic circuit board.

3.3 Applications of integrated photonics

Developments in photonic integrated circuits have positively affected all branches of science. Light is particularly useful for sensing purposes, a feature that has been known since the early days of RADAR technology. The possibility of having smaller devices has opened a plethora of possible applications. The automotive industry uses PIC-based radars to improve ground monitoring of traffic and safety, but also to improve the performances of driverless vehicles [147]. Different photonic-based sensors are also used for fields such as aerospace, food quality control, chemistry [148]. In life sciences, several lab-on-a-chip systems have been proposed, using optical and fluidic interfaces rather than electrical interconnects [149–151].

This section will focus on the advances in photonic circuits in the relevant fields to this thesis, i.e. telecommunications and quantum information.

3.3.1 Photonic integrated circuits in telecommunications

Among the differences between electronic and photonic circuits, the particle statistics can also be relevant depending on the application. Electronic circuits are based on interactions between electrons, which follow fermionic statistics and can be charged positively or negatively, unlike photons which are bosons. This makes it hard to efficiently store photons, which hinders the capability of fabricating devices such as random access memories (RAM) using light, although some promising early-stage results have been shown [152].

On the other hand, photons are ideal for the transmission of information: optical fibres are now the standard channel for long-distance communications, as they allow to reach larger distances and higher data rates than electric wires. The growth in number of devices that employ optical components means that the amount of data that will have to be processed will drastically increase. In particular, central nodes such as datacentres will be faced with increasing volumes of traffic that will need to be handled. As the complexity of the protocols and the traffic volumes increase, so does the need for space-saving, cost-effective devices that are able to process that amount of information. Integrated photonics has

a vast potential to replace most of the current photonic elements in telecommunications, particularly transmitters and routers.

Integrated DFB lasers are the most popular choice for a telecom transmitter: they can emit at the right wavelengths, can be more compact than other diode lasers, and are easier to fabricate. Moreover, they can easily achieve mW powers, can be operated at high speed, and have the capability of having narrow linewidths: the latter is a particularly important requirement in telecommunication technology, as information is often multiplexed into different wavelengths, and interference between channels should be avoided.

Optical transmitters encode information in different properties of light. ON-OFF keying can easily be implemented using standard components, however it has a low yield of data transmission and requires high-speed receiving hardware. On the other hand, more sophisticated techniques like phase-shift keying (PSK) or Quadrature-Amplitude Modulation (QAM) can achieve higher data rates with slower electronics, but require more elements in the transmitter. This makes integrated devices fundamental when dealing with large amounts of transmitters as it allows to drastically cut space, costs and power consumption [121].

Photonic routing is another challenge which can easily be overcome with photonic chips. Chip-based optical interconnects are able to achieve operation rates of Gbit/s, while consuming powers in the order of fJ/bit [153]. This is especially important in the Internet of Things era, where a massive amount of devices are interconnected and datacentres have to route extremely high volumes of data.

Development of new techniques for device fabrication has exponentially increased the capacity of PICs: while tens of components could be implemented on a chip in the early 2000s, photonic chips now boast numbers in the order of one thousand components [142, 154], following a trend similar to that of Moore's law for electronic devices [155].

InP chips are the natural choice for this kind of applications, as is to date the only material that can emit light at telecom wavelengths. At the same time, this platform also allows for the implementation of waveguides, high-speed modulators and photodiodes, which are also indispensable for telecommunications. On the other hand, Silicon-based platform would allow for easier integration with complementary metal-oxide-semiconductor (CMOS) electronics, which is based on the same material. Their lack of light emitting and detecting devices, however, makes it more complicated to integrate these chips with existing electronic devices.

3.3.2 Integrated quantum photonics

The cost-effectiveness and little space requirements of PICs are an attractive opportunity not only for communications, but for research in quantum optics and quantum information as well [156]. Photons' weak interactions with the environment make them ideal for tests of fundamental properties of quantum mechanics. Scaling the dimensions of these experiments is particularly useful in quantum information processing, where numbers of photons in the

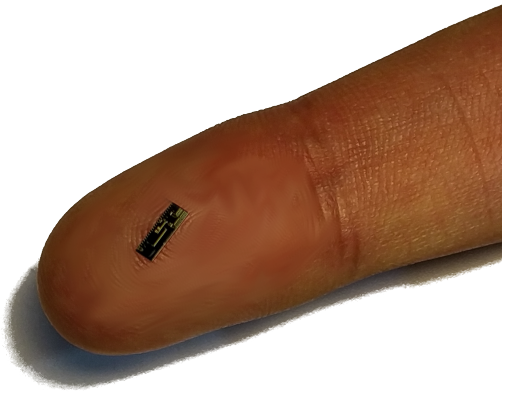

Figure 3.4: A 2 mm × 4 mm photonic chip for QKD.

order of thousands will greatly increase the complexity of the systems: such systems will most likely be impossible to implement using bulk optics, as the number of components needed would be prohibitive in terms of space and cost resources. Integrating them on PICs should make such experiments feasible. Chip-based devices have been demonstrated for applications such as testing the validity of Shor's algorithm [157].

Another area of interest for PICs is quantum simulation. Implementing quantum walks for boson sampling [158–160] is a major challenge that aims to prove how quantum mechanics is indeed more suitable for simulating physical systems than standard, classical computational models. Chip-based devices have been used to simulate processes such as Anderson localisation [159, 161] and quantum transport networks [162], as well as in applications such as quantum chemistry and molecular simulations [163]. PICs have also been present in experimental applications such as photon generation [164, 165] and detection [166], and many others.

3.3.3 Integrated quantum communications

Notably, quantum communications and QKD also have benefitted from the development of integrated photonic technologies. Usual QKD systems, like those commercially sold by IDQ or developed by Toshiba Europe Ltd, are relatively bulky: lasers, phase and intensity modulators and optical fibres occupy roughly the same space as the control electronics in a commercial QKD system, as well as being expensive, making such devices not suitable for large-scale deployment.

Integrated photonics, on the other hand, may offer a solution to this problem. The optical elements of a QKD system can be embedded on a chip which occupies a space 1 to 2 orders of magnitude smaller than its bulk-optics counterpart (Figure 3.4), and the costs can also be cut down by a significant amount thanks to MPW runs.

Implementations of chip-based QKD have been shown in recent years. The first QKD

experiment using integrated photonics was demonstrated in 2017 by the University of Bristol [96]: an InP chip is used as a transmitter, containing a laser and MZIs using EOPMs to transmit phase-encoded information. Pulses were obtained by carving a CW laser: this way all pulses are coherent with each other. Multi-protocol operation was achieved using active phase randomisation for BB84. The detection was performed on a reconfigurable Silicon-based chip to allow for low transmission losses. The rates obtained with an equivalent channel length of 20 km were 345 kbit/s, 311 kbit/s and 565 kbit/s for the BB84, COW and DPS protocols, respectively.

Polarisation and time-bin encoding have also been demonstrated by the same group in 2017 on a Silicon chip [97]. The light source is an off-chip laser, coupled to the QKD encoder. High speed operation is obtained by using carrier-depleting modulators (CDMs): these usually introduce losses in the system due to saturation, but using a thermo-optical phase shifter (TOPS) to shift the temperature allows to work in a low-loss regime for the CDM. Different protocols are encoded in different silicon chips for this experiment. The experiment reports key rates of 916 kbit/s for the time-bin encoded COW protocol, and 329 kbit/s for the polarisation-encoded BB84 protocol.

Silicon photonics is also the encoding platform chosen for a metropolitan experiment performed in Cambridge, MA (USA) in 2018 [98]. Information was transmitted over 43 km, with a channel loss of 16.4 dB. The key rate achieved over this link was 157 kbit/s, using the polarisation-encoded BB84 protocol.

This page intentionally left blank.

Part II

Experiments and results

This page intentionally left blank.

Chapter 4

Methods

This chapter will describe the experimental apparatus and the measurement methods employed throughout this thesis.

4.1 Experimental apparatus

The experimental setup for all QKD experiments is shown in Figure 4.1. Each element will be described in more detail in this section.

Alice and Bob nodes

The two communicating parties, Alice and Bob, are each allocated one desktop PC. Alice's computer is connected to the electronics and the temperature control of the transmitter devices under test, and contains all the needed software (developed in LabVIEW, Matlab and Python) to control them. The software sets the bias voltages for all devices in the QKD system (lasers, heaters, EAMs, variable optical attenuators (VOAs)) and the radio frequency (RF) waveforms which drive the lasers. A local LAN connection is set up to communicate with Bob over a classical channel.

Bob's computer is connected to the receiver apparatus. It contains software to set the voltage on the receiver interferometers (hence setting the measurement bases) and to monitor the single photon detectors. Software was also written to read data from single photon counter modules.

Transmitter electronics

The QKD transmitters (QTxs) used throughout this thesis are all driven by direct current (DC) and RF sources. The DC voltages and currents are provided by a high-precision source-measure unit (SMU), which is capable of outputting voltages up to 24 V with a precision of ∼1 mV, or currents of up to 150 mA with a precision of 1 µA. The RF waveforms are

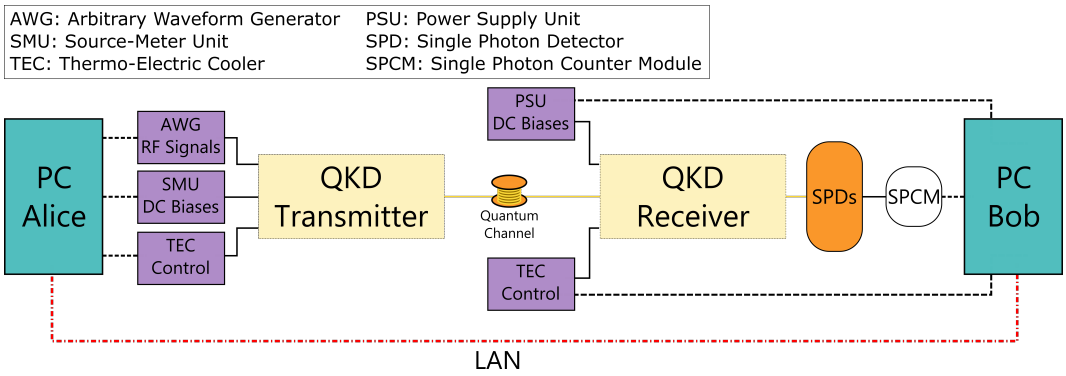

Figure 4.1: Experimental setup for a QKD experiment. Dashed, black lines represent connections between computers and instrumentation. Solid black lines represent electrical connections. Yellow lines represent fibre connections. The dashed red line represent the LAN connection between Alice and Bob.

sent from Alice's PC to an arbitrary waveform generator (AWG). This has a bandwidth of 24 GSamples/s, which translates into a resolution of ∼41.7 ps per sample. The output from the AWG must be amplified in order to reach the desired amplitude, which is about 3.5 Vpp for the lasers and about 4 Vpp for the EAMs.

In order to connect the instrumentation to the optical devices, SMA-type coaxial cables are used. These are specifically suited for high-speed operation, as standard BNC cables suffer from very high electronic noise at RF frequencies. Where DC connections are needed, they are routed to SMA cables to ensure compatibility with the probe station for chip testing. It is important to notice that, since the AWG is capable of a resolution of 24 GSamples/s, the SMA cables need to be suitable for operation at frequencies >12 GHz.

Receiving electronics

For the receiving hardware, the only electrical connections needing control from the user are the connections to the decoding interferometer. These are provided by a benchtop DC source, which is programmable and controllable remotely. The single photon detectors are connected to a single photon counter module, which outputs timestamped data from the SPDs with a resolution of 100 ps. This data can then be retrieved and used for the extraction or estimation of a secure key.

DFB lasers

All lasers employed throughout the thesis, both on and off-chip, have a bandwidth of >10 Gbit/s, which allows them to be driven correctly by the AWG. They are kept at a constant temperature by using a thermo-electric cooler (TEC), which ensures stability of the output. The output wavelength can be changed by locally heating the laser, hence changing

the refractive index of the cavity: all lasers have a DC-controlled heater that can be adjusted to shift the wavelength by a few nm. This is especially useful for the purpose of this thesis, as the wavelengths of the lasers must be precisely matched to obtain the best results (more detail about this in Chapter 5).

Chip testing

After receiving the chips from the foundry, they are tested into a custom-made probe station (Figure 4.2). This is an enclosure where the chip is secured on top of a temperature controlled metal plate. A set of different probes are used to connect the chip via its electrical pads. Depending on the component, two-pin ground-signal (GS) or three-pin ground-signal-ground (GSG) probes are used. The GS configuration is used for elements where high-speed modulation is not needed, such as heaters and VOAs. On the other hand, in order to reduce electrical reflections to a minimum, a GSG configuration guarantees a better shielding of the signal track, minimising electronic noise. Alignment of the probe tips with the chip's electrical pads is done by manually moving the probe tips by means of micropositioners. The probes are in turn connected to the driving instrumentation via SMA-type cables. Light out of the chip is coupled to a single mode optical fibre, which is aligned to the chip's spot-size converter (SSC) using servo motors and piezoelectric positioners.

Temperature control of the chips

Sending electrical signals to a chip introduces a significant quantity of heat in the system. Moreover, the condition of the room are variable: the outside temperature, the presence of people in the room, and the air conditioning system all contribute to temperature fluctuations over time. For this reason, it is important to introduce temperature control systems in place to operate in a stable environment. The temperature control system employed throughout this thesis is shown in Figure 4.3. QKD chips are mounted on a metallic interposer, which is then placed on the cold plate of a TEC, also called *Peltier cooler* [167]: the Peltier effect [168] refers to the phenomenon of heating or cooling of a p-n junction due to a flow of current.

A TEC is composed of two plates, one of which has a current flowing through it, connected by alternating p-n semiconductors. Sending current through the device sends heat from one plate to the other. The plate connected to the electrical circuit is in contact with a heatsink, in order to keep it at room temperature, while the other plate will be the one that is temperature controlled. By attaching a temperature sensor to the interposer, it is possible to calibrate the TEC current via a feedback loop to keep the overall chip temperature stable. This is done by means of a TEC controller, a device that is specifically built for this purpose. Note that local temperature variations still happen, due to the presence of heaters on the chips.

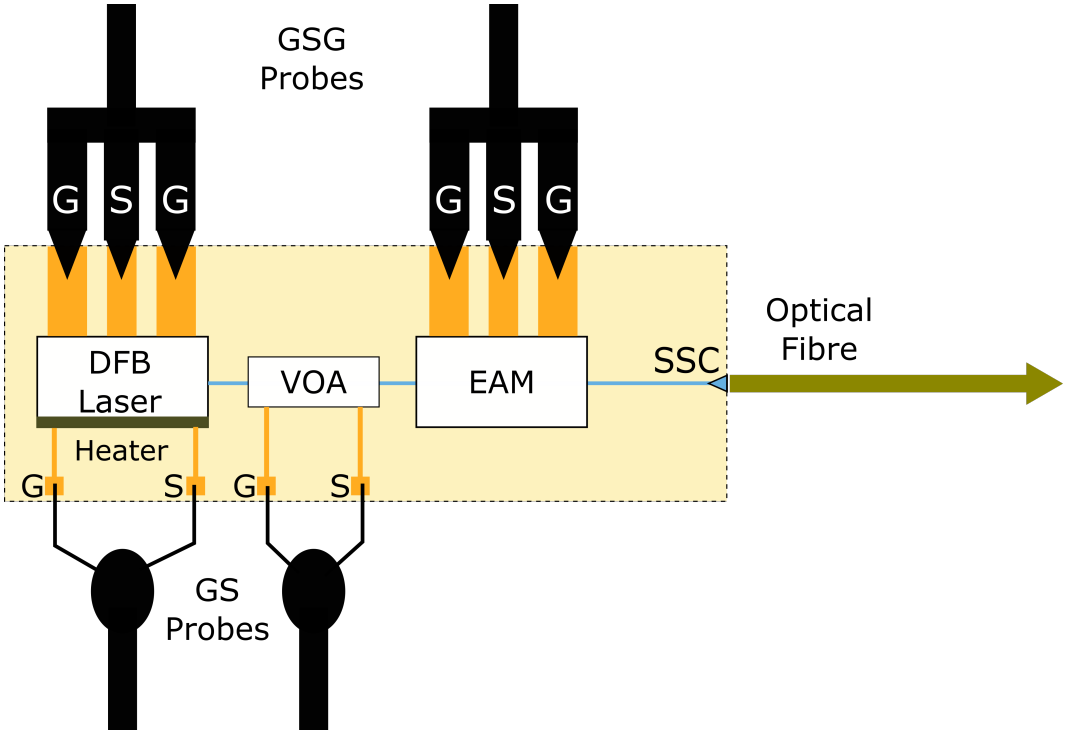

Figure 4.2: Schematic of the probe station used to test chips. The probe tips are moved and positioned on top of the electrical pads of the chip by means of micropositioners and, are connected to the instrumentation via SMA-type cables. Micropositioners are also used to align an optical fibre which collects the light out of the chip.

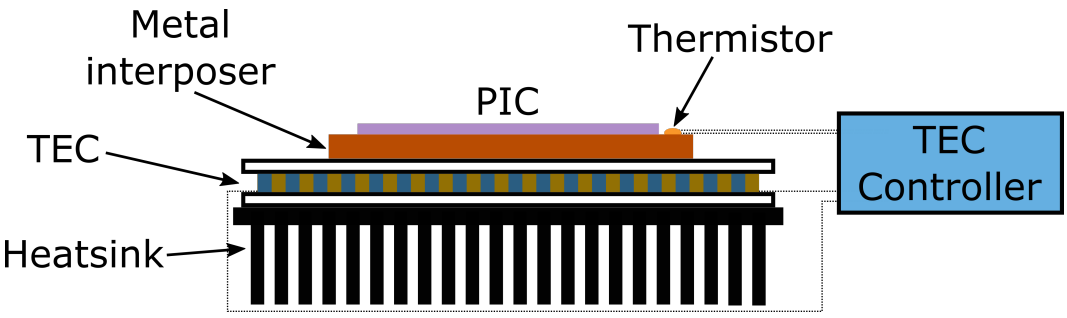

Figure 4.3: Schematic of the temperature control system. The chip is mounted on a metal interposer which, in turn, is mounted on a TEC and has a thermistor connected to it. The temperature controller reads data from the thermistor and, based on that, regulates the current sent to the TEC through a feedback loop, to maintain the overall chip temperature stable.

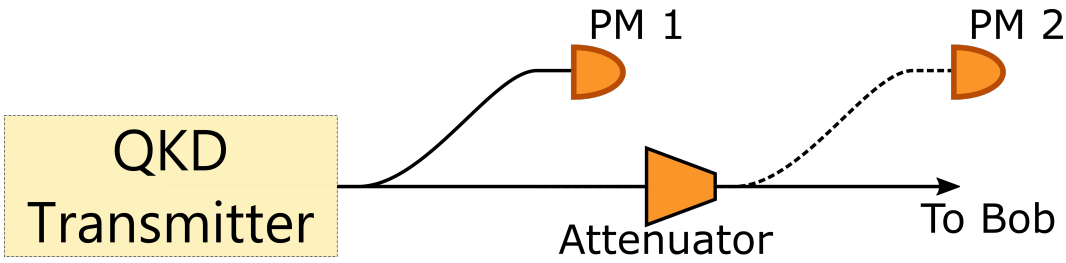

Figure 4.4: Setup for calibrating the photon flux sent by Alice to Bob. The optical path is split into two, one going to Bob and the other monitoring the optical power. By knowing the splitting ratio between the two arms (which is achievable by measuring PM2 instead of sending light to Bob - the dashed line represents the alternative optical path) it is possible to modify the attenuation according to the monitoring power to have the correct photon flux in the quantum channel.

4.2 Performing a QKD experiment

Setting the photon flux

Photon fluxes at the single photon level can be very hard to measure directly. A way around this is to measure light at a macroscopic level before attenuating it to the single photon level; splitting the optical line before this attenuation it is possible to continuously measure accurately an optical power (Figure 4.4). Then, it is possible to remove the attenuation and measure the ratio between the two arms, at which point measuring light at the monitoring arm will give an accurate indication of how much attenuation is needed to achieve the desired photon flux.

QBER and key rates estimation

The goal of all experiments described in this thesis is not to distil, but rather estimate secure key rates. For this reason, the raw key is composed by a repeating random pattern of 1024 bits encoded in the AWG driving signal. Bob's computer reads data from the single photon counter module. A trigger signal is sent at the start of each pattern, and the single photon counter module digitises the data in the form of a histogram. The histogram will show a pulse train composing the pattern. High pulses will represent '0' bits, low pulses will represent '1' bits.

For the BB84 protocol, pulses interfering with a random phase difference will result in a histogram pulse which is half of the height of a '1' bit. This is because the distribution of the interference is centered in between the completely constructive and completely destructive interference events. Similarly, pulses measured in the conjugate basis to the preparation basis will result in a half-height histogram pulse. These events will be discarded as part of the sifting and basis reconciliation.

The QBER can then be measured by counting the number of counts that were recorded in the low pulses, as in an ideal scenario there should be none, and comparing them to the total number of counts:

$$QBER = 1 - \frac{2 * C_{\mathrm{wrong}}}{C_{total}}.$$

Once a QBER is calculated, it is possible to estimate a SKR as in Section 1.4.4.

Chapter 5

Multi-protocol, multi-rate QKD transmitter

5.1 Introduction and personal contributions

QKD implementations have already achieved impressive results (Section 1.4.5). However, these are all relying on application-specific systems: this has led to the situation where different hardware is needed to implement separate protocols at different count rates. In real-life scenarios, users would likely choose their device based on considerations on performance and costs. At the same time, different vendors might sell devices operating with different protocols or at different clock rates. A multi-protocol, multi-rate transmitter is highly desirable in this scenario [169, 170].

Lack of interoperability is an issue for users and manufacturers alike. It is important to agree on a set of standards, in order for consumers to be able to use different hardware without loss of performance. At the same time, the presence of a standard in the early stages of QKD development would help manufacturers focus their efforts in the same direction. Some steps have been taken in this direction, and the development of standards for QKD is currently ongoing [171].

This chapter will explore a bulk optics QTx that addresses this issue: its multi-protocol, multi-rate capabilities are demonstrated by the reported experiment, as a first step towards fully universal QKD transmitters.

The author of this thesis was responsible for designing and carrying out the experiment, as well as analysing the experimental data. In particular, section Section 5.4 and the following sections in this chapter are based on original work.

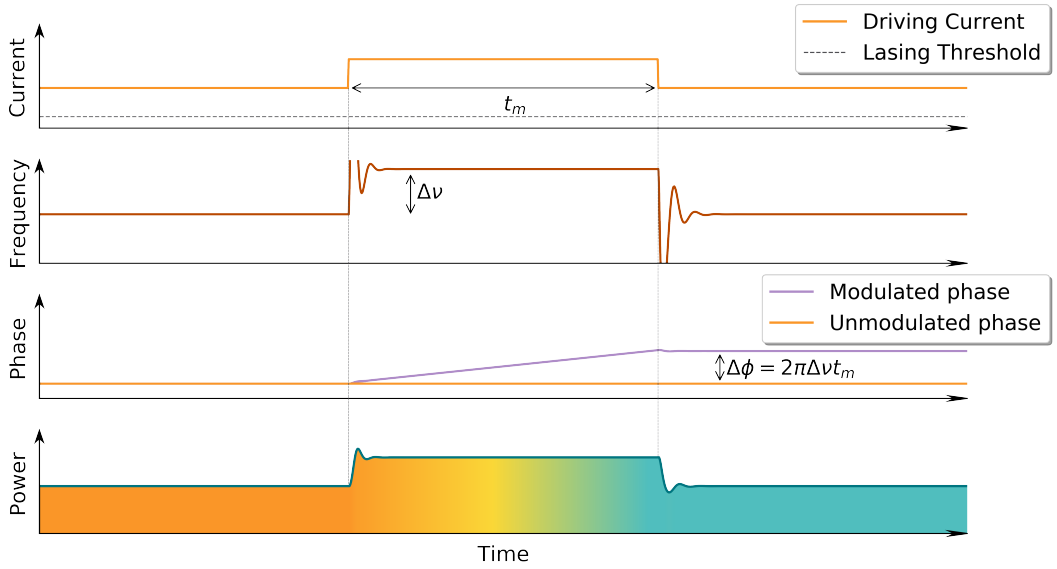

Figure 5.1: Numerical simulation of direct phase modulation of a DFB laser. Modulating the driving current for a short time induces a change in the frequency that in turn causes a change in the phase evolution (the slope of the lavender curve). The phase change in the light beam is shown in the bottom plot as the coloured plot filling.

5.2 Directly phase-modulated light source

Phase modulation is one of the most common ways of encoding information in light. By using the interference between phase-modulates pulses, we can additionally modulate other properties of light such as amplitude [172] and polarisation [173]. The usual way of modulating the phase is through external phase modulators, as discussed in Section 1.4.3. $LiNbO_3$-based modulators require amplification of the signal inputs due to the high voltages required, which are not achievable by common CMOS technology. This leads to increased cost and space requirements. Trying to reduce the required voltages by increasing the active length is not feasible due to arising issues such as losses in the electrode, phase walk-off between optical and electrical signal, travelling RF waves from the light wave or RF parasitic effects [174, 175].

Direct phase modulation [68, 176] is a simple method to change the phase of a DFB laser diode output. When modulating the driving current of a DFB laser above its lasing threshold, this directly changes its frequency, wavelength and phase evolution. A numerical simulation of this, obtained by solving the rate equations below, is shown in Figure 5.1.

This is an issue in both classical and quantum communications, as it leads to unwanted interferences due to different wavelengths travelling at different speeds in the fibre. Moreover, in QKD this leads to situations where Eve might detect the change in wavelength during the modulation to extract information about the key while remaining undetected [177].

In 2016, a novel light source [178] was introduced that combines the advantages of the well-known phenomena of direct phase modulation and optical injection locking (OIL) [179]. In this scheme, two lasers are used to separate the pulse preparation from the phase modulation.

In OIL, a phase encoding laser sends light into the cavity of an injection locked (or seeded) laser. Back reflections from the injection locked laser to the phase encoding laser are avoided by using an optical circulator (Figure 5.2). Light travelling through the injection locked laser from the phase encoding laser overcomes spontaneous emission, effectively forcing the seeded laser to emit light with the same parameters (wavelength, phase) as the injected beam. This is modelled by the rate equations for the photon number $S(t)$ and the carrier density $N(t)$ of the seeded laser, and the phase difference between the two lasers $\phi(t)$ [180]:

$$\frac{\mathrm{d}N(t)}{\mathrm{d}t} = J(t) - R(N) - \Gamma a[N(t) - N_{tr}]S(t) + F_N(t), \tag{5.1}$$

$$\begin{aligned}\frac{\mathrm{d}S(t)}{\mathrm{d}t} = &\{\Gamma a[N(t) - N_{tr}] - \gamma_p\}S(t) + \beta BN^2(t) \\ &+ \kappa\sqrt{S_{inj}S(t)}\cos\left(\phi_M - \phi(t)\right) + F_S(t),\end{aligned} \tag{5.2}$$

$$\begin{aligned}\frac{\mathrm{d}\phi(t)}{\mathrm{d}t} = &\frac{\alpha}{2}\Gamma a[N(t) - N_{tr}] - \kappa\sqrt{\frac{S_{inj}}{S(t)}}\sin\left(\phi_M - \phi(t)\right) \\ &- 2\pi\Delta\nu + F_\theta(t),\end{aligned} \tag{5.3}$$

where Γ is the confinement factor, a is the gain coefficient of the injection locked laser, N_{tr} is the carrier number at transparency, γ_p is the photon decay rate, κ is the coupling rate, S_{inj} is the number of injected photons, $J(t)$ is the injection current density for the injection locked laser, R, B are carrier recombination rates, α is the linewidth enhancement factor of the laser and $F_N(t), F_S(t), F_\theta(t)$ are Langevin noise sources modeled as Gaussian random variables, which are related to spontaneous emission [181]. These terms are negligible when the injection power is strong enough. These equations, when evaluated numerically, describe the behaviour of these quantities as shown in Figure 5.1.

The coupled elements in this equation reveal a strong link between the three quantities. In particular, the output can be tuned experimentally by changing two parameters: the injected power, hence the number of injected photons S_{inj}, and the frequency detuning $\Delta\nu$ between the two lasers. If the injection locked laser is periodically driven above and below its lasing threshold (gain-switching [182]), it generates pulses that are coherent thanks to the injection from the phase encoding laser (Figure 5.3).

At this point, one can think of integrating OIL with direct phase modulation: modulating the phase encoding laser in between two pulses from the seeded laser will cause the intensity and wavelength to go back to their previous value when the modulation is done, however the phase will have evolved: a pulse generated after the modulation will have a phase difference to the previous pulse which depends on the modulation amplitude and duration, while

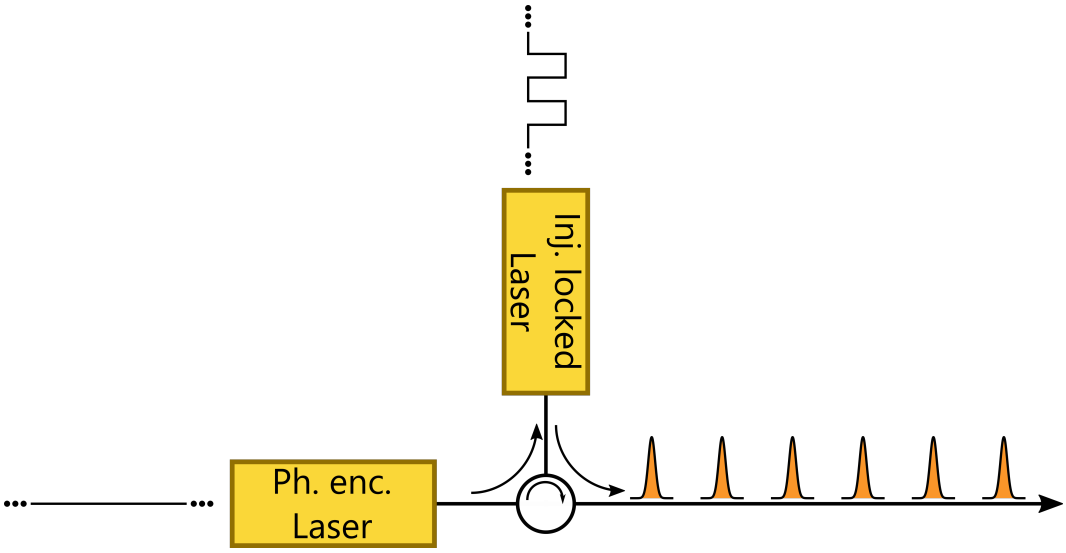

Figure 5.2: Principle of operation of OIL. The phase encoding laser injects light into a second laser which inherits the phase and frequency of the former. An optical circulator ensures that light only travels in one direction, avoiding mutual seeding.

maintaining the same intensity and frequency, because the pulse is generated after these quantities have gone back to their original levels in the cavity of the phase encoding laser. This process does not require any external phase modulators and has very low half-wave voltages compared to standard $LiNbO_3$ modulators. The pulses can now effectively be used for QKD experiments [183–186].

5.3 Experimental setup

A schematic of the experiment is shown in Figure 5.4. An AWG sends RF electrical signals to the transmitter to encode a certain protocol at a given clock rate. The phase encoding laser is driven by an AWG with high vertical resolution. The signal is sent to an amplifier before reaching the laser, in order to achieve the desired driving voltages. The injection locked laser is pulsed by using the amplified, digital marker channel of the AWG, since there is only the need for two levels. DC biases are applied to the lasers using SMUs.

5.3.1 Protocols implementation

In this experiment, the transmitter is set to encode three protocols (BB84, DPS, COW). The COW protocol is straightforward to implement (Figure 5.5): the phase encoding laser is simply driven in CW mode without being modulated, inducing a zero phase difference between consecutive pulses. A CW injection is easy to achieve, and yields a very good coherence transfer as well as a reduction of jitter. This, combined with the absence of phase

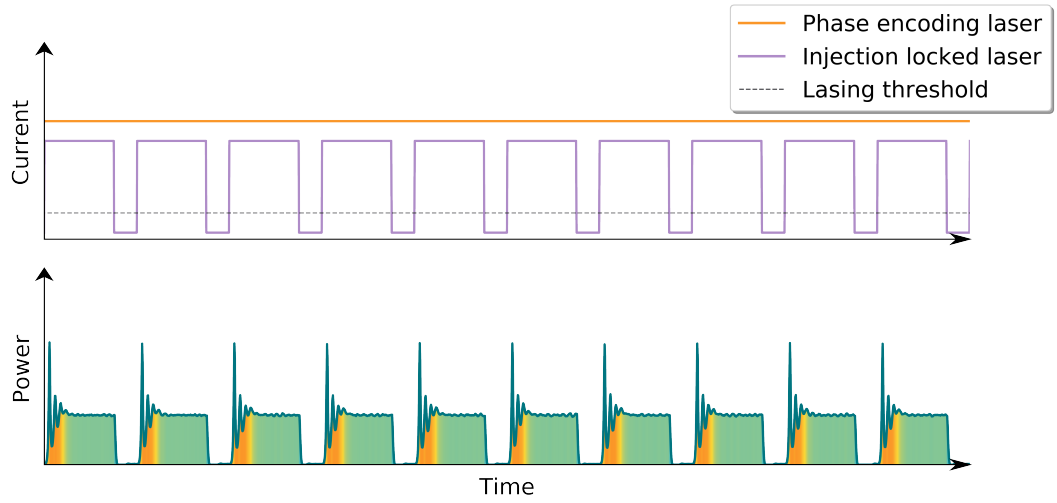

Figure 5.3: Injecting light into the seeded cavity generates coherent pulses.

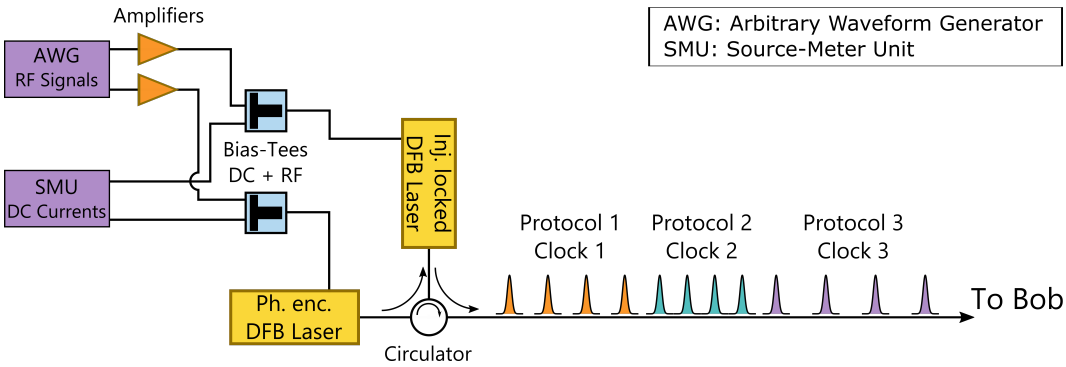

Figure 5.4: Experimental setup showing optical and electronic devices used for the QTx. The transmitter allows to encode different protocols (represented with different colours) at different clock rates, by simply changing the driving signal of the AWG. The full setup is based on the one shown in Figure 4.1.

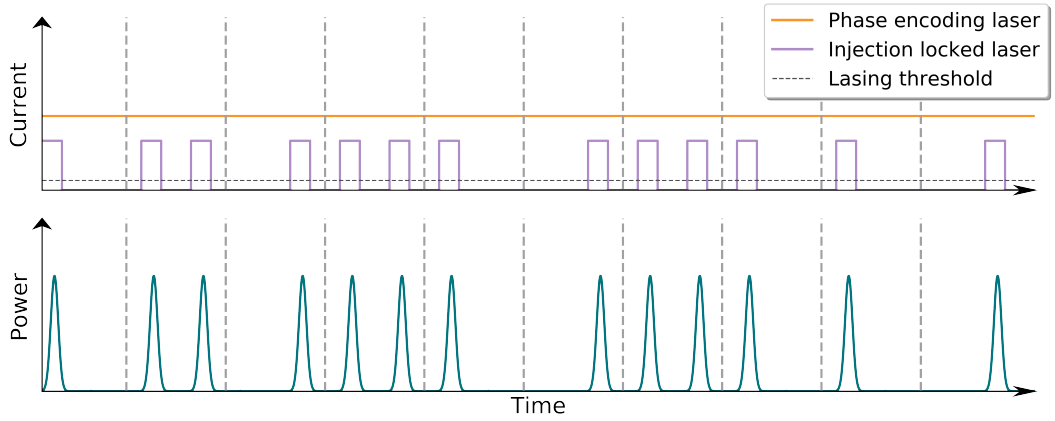

Figure 5.5: Driving signals from phase encoding and injection locked lasers for the COW protocol. The top plot represents the electrical driving signals, the bottom plot represents the optical output. Consecutive pulses have a zero phase difference.

errors, is expected to have a positive impact on the QBER, which should stay very low for this protocol. The bit encoding is implemented in pulse pairs: the pair {0, 1} is used for bit 0, {1, 0} encodes bit 1, while two full bins {1, 1} are used for decoy bits. For the DPS protocol, bits are encoded in the phase difference between consecutive pulses (Figure 5.6): the phase encoding laser is driven above threshold and modulated for a short time in between pulses to apply a π phase shift, or not modulated for a 0 shift. The BB84 protocol requires a different driving signal for the phase encoding laser. The global phase of a pulse pair, as shown in Section 1.4.3, has to be random for the protocol to be secure, while still maintaining coherence within the pulse pair. This can be done with an aMZI, but it can also be achieved by the directly-modulated transmitter (Figure 5.7): gain-switching the phase encoding laser between every pulse pair, i.e. depleting the cavity then turning the laser back on, gives the next pulse pair a global phase determined by the vacuum fluctuations in the cavity, while the two pulses generated within this modulation will have a phase corresponding to the encoded bit and basis.

For this experiment, SKRs for all three protocols will be evaluated in the asymptotic key size scenario, as finite-key size effects are beyond the scope of the experiment.

5.3.2 Integrated decoding circuits

While the transmitter is implemented with bulk optics, a first step towards miniaturisation is the integration of the receiving circuits. The QKD receiver (QRx) circuits, designed by researchers at TEUR, are implemented on Silicon-based photonic chips. Each circuit decodes a protocol at a certain clock rate (2 GHz or 2.5 GHz). The clock rate is set by the delay line in the aMZIs. The receiver chips contain multiple circuits. This is useful as it allows to decode different protocols without the need for off-chip optical switching. TOPSs modulate

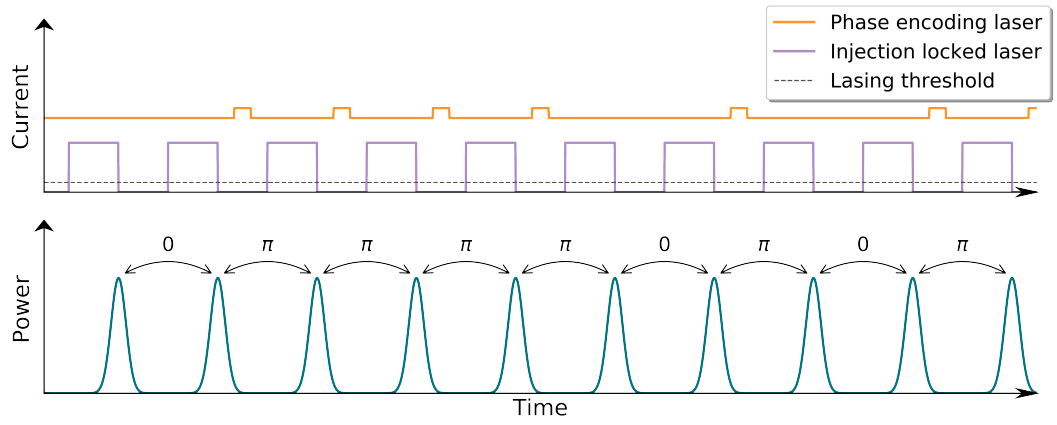

Figure 5.6: Driving signals from phase encoding and injection locked lasers for the DPS protocol. The top plot represents the electrical driving signals, the bottom plot represents the optical output.

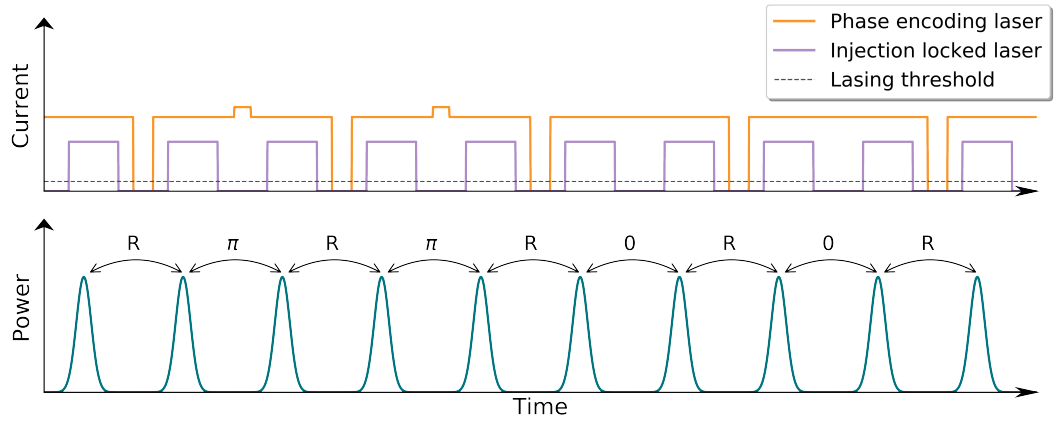

Figure 5.7: Driving signals for the two lasers for the BB84 protocol. The top plot represents the electrical driving signals, the bottom plot represents the optical output.

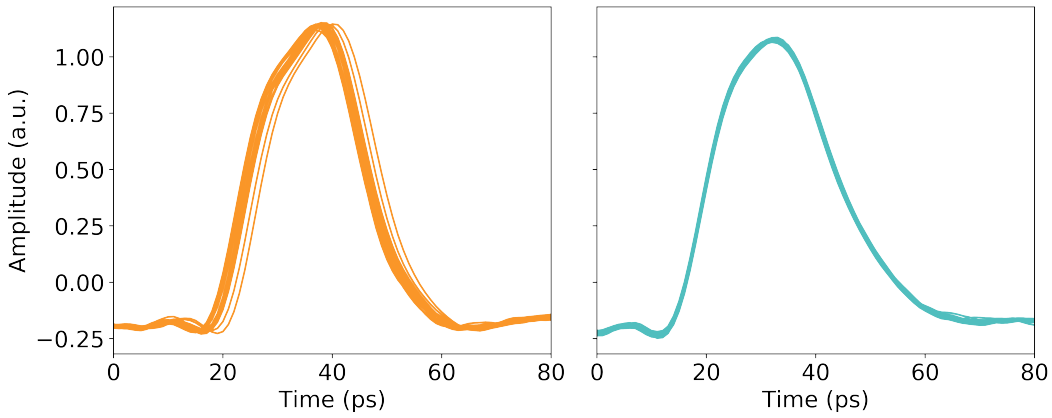

Figure 5.8: Jittery output from a gain-switched laser (left). Output after CW injection (right).

the light in the interferometers; the phase shift is proportional to the dissipated power, hence to the square of the voltage. A π phase shift is achieved with a voltage of $\sim$15 V. These phase shifts can be used to direct light towards an arm or the other of the interferometer. This is particularly useful to balance the two arms of the aMZI, since the long arm is lossier than the short one, hence it will cause a power imbalance at the output coupler. For this experiments, the 2.5 GHz chip has a measured loss of 10.1 dB, higher than the 6.7 dB of the 2 GHz chip, despite having a shorter delay line. The main contribution to the losses is indeed the propagation loss (0.2 dB/cm), however fibre coupling and imperfections in the fabrication process also have an effect, which can explain the discrepancy in the losses. The output waveguides are coupled to optical fibres, and the detection is performed by superconducting nanowire SPDs (SNSPDs) [187] with an efficiency of 55% and dark count rates of $\sim$10 Hz.

5.4 Characterisation

Pulses from a gain-switched laser suffer from high chirp and jitter, as well as having a random phase. High chirp and jitter prevent such pulses to be used for QKD, as pulses do not interfere well in these conditions, resulting in higher error rates. Optical injection is a good way of preventing this: as the emission process is triggered by injected light, spontaneous emission becomes negligible and temporal or spectral noise is suppressed (Figure 5.8).

Phase locking is achieved by injecting CW light from the phase encoding laser into the seeded laser. By changing the temperature of the phase encoding (or the seeded) laser, its emission wavelength shifts. Figure 5.9 shows how the spectrum of a seeded laser looks like, compared to the spectrum of a laser not being seeded. In seeded mode, the envelope width is much narrower, and fringes at 2 GHz appear due to the modulation, which are not visible on the unseeded spectrum due to the high jitter.

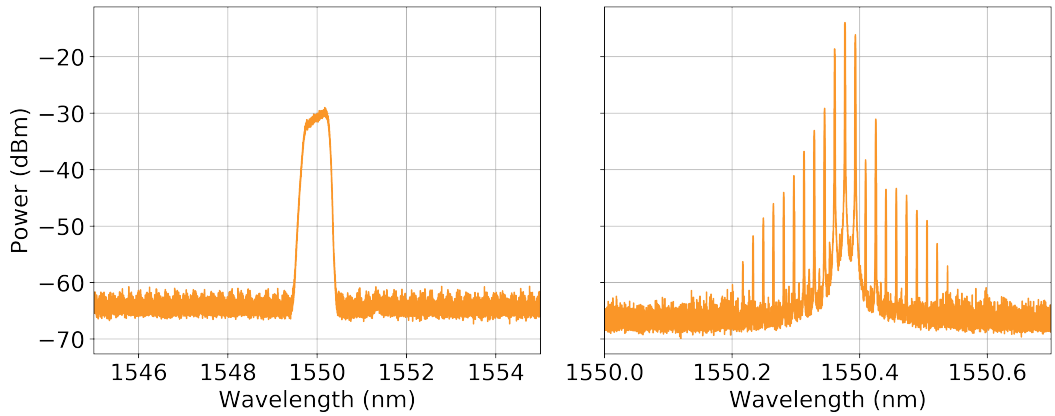

Figure 5.9: Spectra of an unseeded (left) and seeded (right) gain-switched laser. The peaks are spaced by 2 GHz.

In order to check whether the wavelengths of the two lasers are phase-locked, pulses are sent through an aMZI and consecutive pulses interfere. If the pulses are all coherent, a fixed phase shift on the aMZI should always give the same result, as the phase difference between pulses won't change. By changing the voltage applied to the phase modulator on the aMZI, hence, the proportion between constructive and destructive interference changes depending on the phase shift but is equal for all pulses. When the phase spans the whole $[0, 2\pi]$ range, a good measure of coherence transfer is the visibility between the completely constructive and completely destructive interference events, measured as

$$V = \frac{P_{max} - P_{min}}{P_{max} + P_{min}},$$

where P_{max}, P_{min} are the powers measured at the completely constructive and destructive interference events, respectively. This setup is able to obtain visibilities above 98%, which indicates a good coherence transfer (Figure 5.10).

Another important feature of the transmitter, which is important for the security of the BB84 protocol, is phase randomisation (Section 2.1). To achieve this, the phase encoding laser is modulated like in Figure 5.7. Gain-switching the phase encoding laser ensures that its phase is randomised between pulse pairs. Pulses belonging to the same pair will always interfere constructively (or destructively) and result in an output with a stable intensity, while every other pulse interference will be random. To check how well this phase randomisation happens, the interference after the aMZI is monitored using an oscilloscope. The results show that this is indeed the case: the inter-pair interference shows random output intensities due to phase randomisation. An easy way to visualise this is to take all pulses derived from the interference of phase-randomised pulses and superimpose them on the same time scale. Since the phase difference is random, the intensity of each interference will be random as well. The distribution of the intensities of these random interferences has the characteristic U-shape, derived by the physical model of phase diffusion (Section 8.1), as shown in Figure 5.11. It

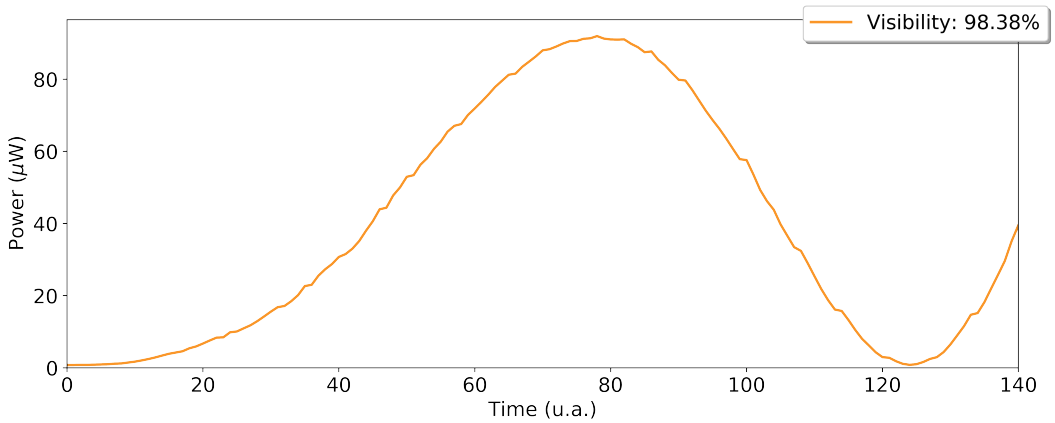

Figure 5.10: Interference power output of seeded pulses from a directly phase modulated light source. The phase modulator in the aMZI is set to continuously change the voltage, hence the measurement basis. When light is coherent, the output power after the interferometer should show events of totally constructive interference (high power) and totally destructive interference (low power). Visibility is measured by comparing these two power values.

can be noted that the shape of the histogram is not perfectly symmetric and the peaks are broader than the theoretical U-shaped histogram shown in Section 2.1. Deviations from the ideal system can be explained by taking into account electrical noise from the oscilloscope and the photodiode used to record the data, and by the fact that there is a contribution to noise given by the time jitter of the pulses. Nevertheless, this is still a good signature that the phases are uniformly distributed, which is the main factor to keep in mind when dealing with BB84.

5.5 Results

The system described in Section 5.3 is set up to measure the performance of the QTx in different conditions. Electrical driving signals are sent to the lasers according to the protocol to be implemented.

The channel loss was emulated with a VOA and set to 14 dB. For the DPS and COW, a photon rate of 0.2 ph/pulse was used; this gives an encoding rate of 0.4 ph/symbol for the COW protocol, as two pulses make up one symbol (Section 2.3).

Data acquisition returns a QBER value and a raw count rate, which are used to estimate a SKR for that data point. The QBER is calculated by comparing the string received by Bob during the acquisition time with the modulation pattern sent by Alice. A data point is recorded every 5 seconds for 20 minutes, then a signal is sent to the electronics, triggering the clock rate and/or protocol change. When this happens, a first point is recorded with a high QBER, which results in no positive key rate. This is attributed to the settling time of

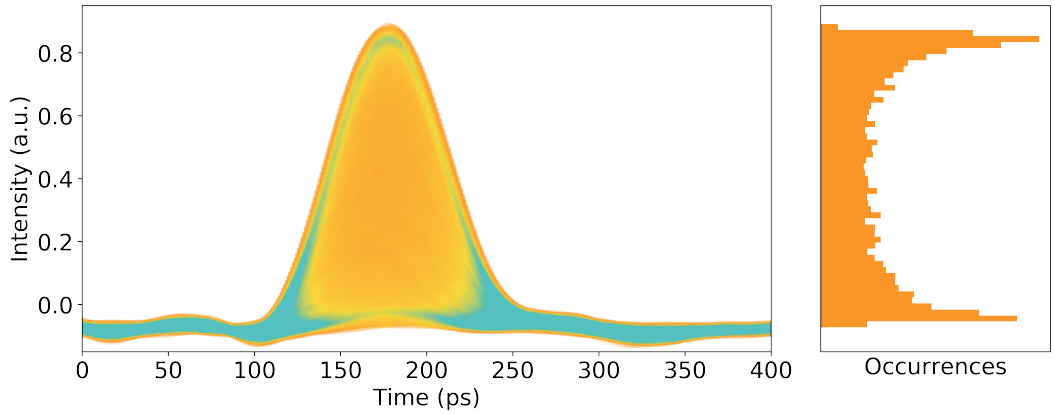

Figure 5.11: Cumulative interferences of phase-randomised pulses (left). Histogram of the interferences recorded at the centre of the pulse. (right).

the AWG, and is measured to be around 5 seconds. The stability of the system allows for a reasonably constant SKR during a 20-minute window (Figure 5.12).

The QBER is stable around 2.7% for the BB84 and DPS protocols, and around 0.7% for the COW protocol (due to the absence of phase errors). This yields secure key rates of 0.5 Mbit/s, 0.4 Mbit/s and 2.5 Mbit/s, respectively.

5.6 Conclusions and discussion

This experiment showed the feasibility of having a single transmitter communicating with receivers employing different clock rates and protocols. The effective settling time of <5 s is limited by the driving electronics needing time to settle to the desired operation regime. Reduced times can certainly be obtained by using dedicated, faster electronics, such as a field programmable gate array (FPGA) board.

This transmitter greatly simplifies the optical circuit needed for the BB84 protocol, since it only needs two laser diodes. Standard implementations of time-bin encoded BB84 require an aMZI with a high-speed phase modulator on one of the arms. This is more power consuming due to the high driving voltages of the phase modulators.

The versatility of the system and the capability of transmitter to address different hardware pave the way for large-scale deployment of QKD systems. The next step is to proceed to the miniaturisation of the optical components, which is the main goal of the next chapter.

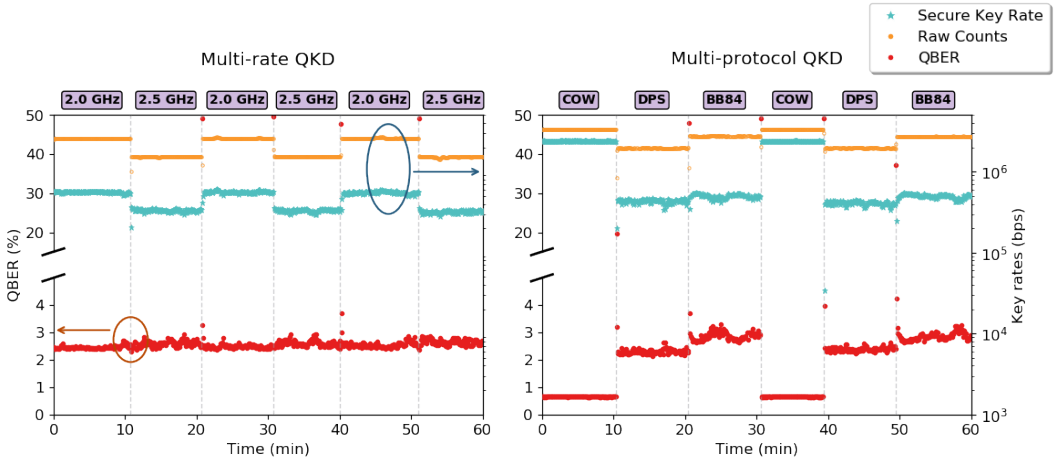

Figure 5.12: Results obtained using different clock rates and protocols. The first point after a switch, with a high QBER, does not result in a positive SKR.

Chapter 6

High bit-rate QKD with integrated photonics

After demonstrating the versatility of a transmitter based on direct phase modulation, the next step towards large-scale implementation of QKD systems is miniaturisation. Integrated photonic-based QKD has already been shown (Section 3.3.3). However, demonstrations so far heavily rely on high-speed intensity and phase modulators in order to carve pulses from a CW laser and encode information. The approach followed in this work [99] removes the need for such elements, which weigh on the power consumption of the system, by generating phase-encoded pulses using the lasers' driving electronics directly.

The author was responsible for acquiring and analysing data in this experiment, as well as setting it up. The results obtained show the highest recorded SKR for a chip-based QKD system, which is encouraging for future works.

6.1 Experimental setup

6.1.1 Integrated photonic transmitter

The QTx is an InP chip fabricated using a generic integrated process (Chapter 3). The novelty of this transmitter is in the small number of elements needed. The pair of DFB lasers and a thermally tuneable MZI are the only components that make up the transmitter. The MZI acts as a VOA to calibrate the injection power.

Light is coupled out of the chip using an optical fibre. The mismatch between the fibre mode and the waveguide mode is compensated by a SSC: the waveguide is tapered to reach a mode size comparable to that of a single-mode fibre. This guarantees low coupling losses and alignment-tolerant coupling [188].

The couplers used in the VOA are multi-mode interferometers (MMIs) [189]. These are mainly waveguides designed to propagate several modes. When light enters the coupler, its

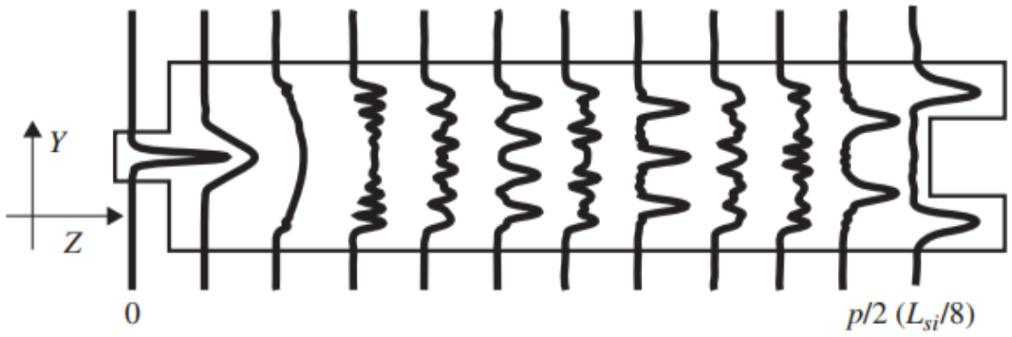

Figure 6.1: Principle of operation of an MMI [191]. Light entering the MMI is decomposed into its eigenmodes, which will interfere while propagating.

profile along the y direction is decomposed into its eigenmodes $\psi_\nu(y)$ [190]:

$$\Psi(y,0) = \sum_{\nu=0}^{m-1} c_\nu \psi_\nu(y), \tag{6.1}$$

where c_ν are the field excitation coefficients m is the number of modes that can propagate in the waveguide. Each mode travels at different velocities in the waveguide, resulting in an interference pattern that depends on the length L of the coupler (Figure 6.1):

$$\Psi(y,L) = \sum_{\nu=0}^{m-1} c_\nu \psi_\nu(y) \exp\left\{\left[i\frac{\nu(\nu+2)\pi}{3L_\pi}L\right]\right\}, \tag{6.2}$$

where L_π is the beat length of the two lowest-order modes. Choosing $L^* = \frac{p}{2}(3L_\pi)$, $p = 1, 3, 5, \ldots$ will result in duplicate images of $\Psi(y,0)$:

$$\Psi(y,L^*) = \frac{1+(-i)^p}{2}\Psi(y,0) + \frac{1-(-i)^p}{2}\Psi(-y,0). \tag{6.3}$$

An MMI coupler with this length will then effectively act as a 1x2 beam splitter.

6.1.2 Layout of the experiment

The experimental setup is shown in Figure 6.2. The QTx is driven by an AWG and SMUs as in Section 5.3, which provide the DC and RF signals needed to implement the BB84 and the DPS protocols. A Peltier TEC keeps the chip at a constant temperature: this is important, as the temperature affects the emission wavelength. For the TEC to work as efficiently as possible, the temperature detection must be performed as close to the chip as possible. This is done by placing the chip on a metal substrate and then fixing a thermistor very close to the chip, using a thermally conductive adhesive to keep it in place. The thermistor and the TEC are then connected to a controller that enables high precision temperature stability.

The quantum channel at different distances is simulated by a VOA, assuming a loss of 0.2 dB/km for a standard optical fibre. Data points have also been obtained with 75 km

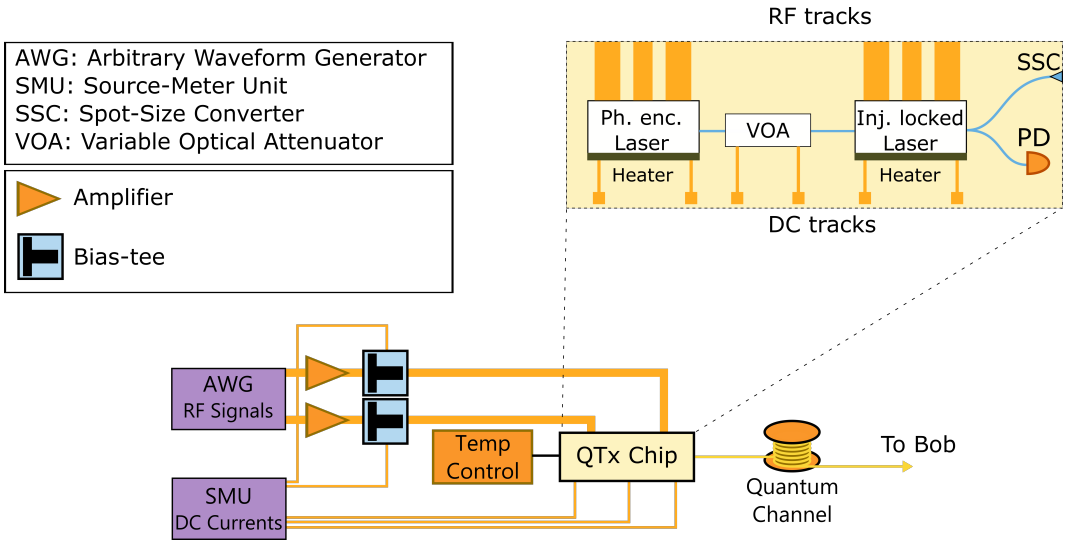

Figure 6.2: Experimental setup to perform QKD using an integrated transmitter. Optical and electrical connections are shown here. The full setup is based on the one shown in Figure 4.1.

of real fibre spool. When using real fibre links, it is important to consider not only the stability of the link, but also the temporal broadening of the pulse due to the light travelling at different, wavelength-dependent, velocities. This could cause unwanted interferences between pulses in neighbouring time bins, which severely affects the quality of the results. In order to prevent this, a special dispersion-compensating fibre was used.

After the quantum channel Bob has an integrated QRx (Section 5.3.2) based on Silicon, with an interferometric length of 2 GHz. The QRx chip has a loss of ∼6.8 dB. The circuit in the receiver is a passive aMZI (Section 1.4.3, Figure 1.7), which is enough to measure data encoded in the BB84 and DPS protocols for a proof-of-principle experiment, as discussed in Chapter 2. The QRx is then out-coupled through optical fibres to SPDs.

For this experiment, both avalanche photodiodes (APDs) and SNSPDs were used for single photon detection. The APDs are fast-gated, self-differencing APDs (SDAPDs) [192, 193], which allow fast detection rates thanks to the lower afterpulsing probabilities. Their efficiency is 18% with a dark count rate of 25.4 kHz. Such detectors are especially useful in field trials and real-life implementations of quantum links. Their low performance is compensated by their compact dimensions and the ability to work at room temperature. The SNSPDs, on the other hand, have much better performances: the detectors used for this experiment have efficiencies of ∼ 80% with dark count rates of 100 Hz. However, they require cryogenic temperatures to work, whereas SDAPDs can work at room temperature. This makes them suitable for laboratory and field experiments, but not for practical implementations at large scales.

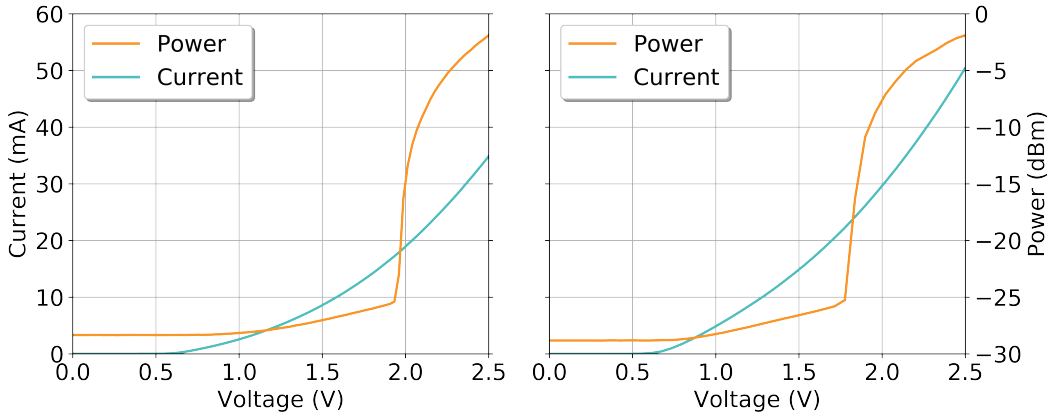

Figure 6.3: P-I-V curves for two different DFB lasers. Different lasers will have different IV characteristics due to the fabrication process while maintaining similar maximum output powers.

6.2 Characterisation of the transmitter

6.2.1 Integrated lasers

The length of the cavity in a DFB laser determines the initial wavelength of the emitted light, which can be tuned by means of a heating element. The change in temperature causes a change in the refractive index of the cavity, which in turn affects the emission wavelength. The DFB lasers chosen for this chip are designed to emit at a wavelength of ∼1550 nm.

The electrical characteristics of these lasers are measured. Depending on the chip, different voltages are required in order to begin lasing on the chip-based DFB. This is mostly dependant on factors such as the fabrication process, the length of the cavity and the position of the electrical contacts. As an example of these differences, Figure 6.3 shows a comparison between the I-V curves of two different lasers. Note how the current drawn from each laser is different at the same voltage, while the lasing power is similar.

The output power from a chip-based laser can be measured by simply coupling the SSC at the output of the chip to an optical fibre, but the measurement would not be accurate due to the coupling losses (∼2 dB) and scattering at the output facet of the chip. Instead, the photodiode on chip can be used to have a more accurate measurement of the emitted light. The photodiodes' specs are used to convert from the measured photocurrent to the actual light. The ratio for these particular photodiodes is 1 mW↔ 0.8 mA.

The CW emission of the integrated lasers has a linewidth of <30 pm, limited by the resolution of the optical spectrum analyser (OSA) used in the measurement. A narrow linewidth is especially useful when seeding with a CW-driven laser. When the injection locked laser is pulsed, the short temporal width and the pulse chirping broaden the spectral linewidth. Once the phase encoding laser is seeding the injection locked laser, the chirp is

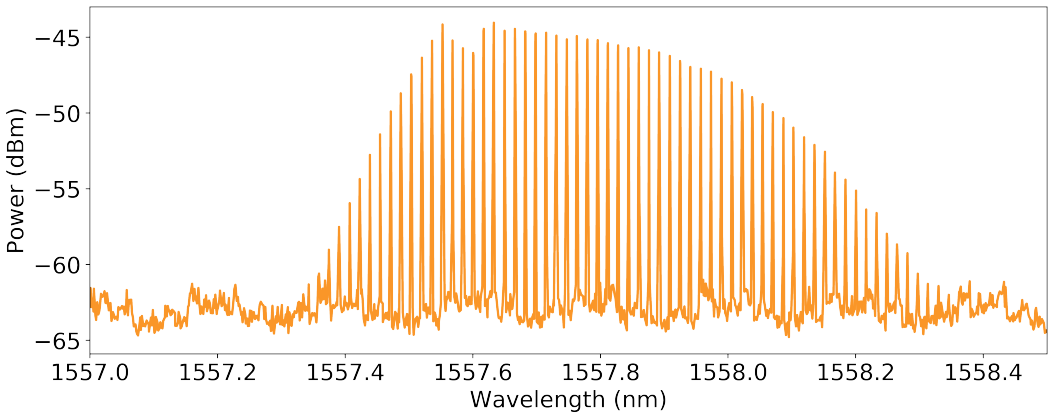

Figure 6.4: Spectra of the injection locked laser in pulsed mode when seeded by CW light. The frequency comb presents peaks separated by 2 GHz, which corresponds to the temporal frequency of the pulses.

removed and the broad spectrum now exhibits the characteristic comb structure with peaks separated by 2 GHz.

It is important to check the signal coming out of the phase encoding laser for the BB84 protocol, as it involves repeatedly turning the laser on and off. To do this, light is sent from the laser directly to the output waveguide. The waveform is then recorded by an oscilloscope (Figure 6.5). The sharp peak at the beginning of each pulse is a signature of the gain-switching phenomenon. In the absence of injection, this guarantees the phase randomisation. The second peak is the modulation that has to happen in between two seeded pulses. It is important that the signal from the injection locked falls inside the flat parts of the phase encoding laser waveform.

6.2.2 Variable optical attenuator

The VOA between the two lasers is a simple MZI. By changing the relative phase of one of the arms, constructive and destructive interferences can be tuned, effectively directing more or less light from the phase encoding laser to the seeded laser. The extinction achievable through this is measured by monitoring the photocurrent at the photodiode on the chip. The MZI is able to generate 20 dB of extinction ratio (Figure 6.6), which is more than enough for the purpose of simply tuning the injection power.

6.2.3 Coherence transfer

A series of experiments are performed to show the versatility of the QTx. The first step is to measure the coherence transfer from the phase encoding laser to the seeded laser. In order to do this, the phase encoding laser is kept above threshold in CW mode while the

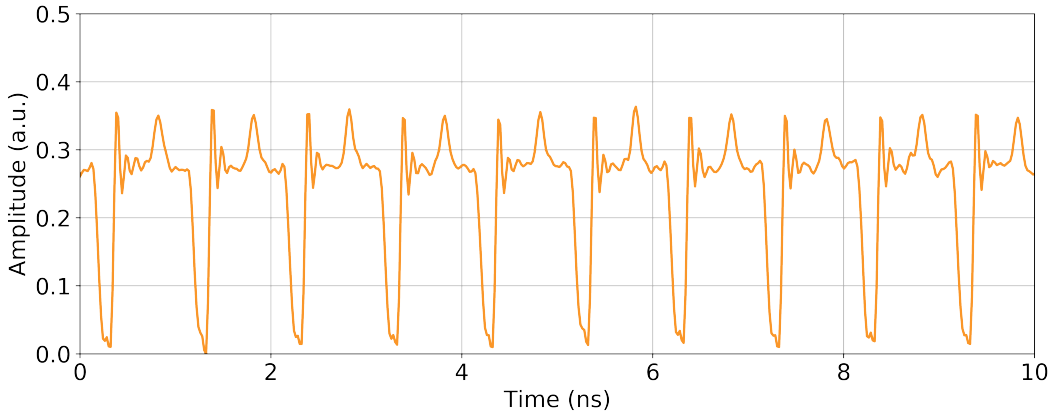

Figure 6.5: Optical output from the phase encoding laser modulated to encode a BB84 pattern. After an initial overshoot due to rapid depletion of the cavity in the gain-switching regime, the emission stabilises to a steady state. At this point, it is possible to add a modulation to the pulse to introduce a phase modulation. The amplitude of the modulation determines the phase difference.

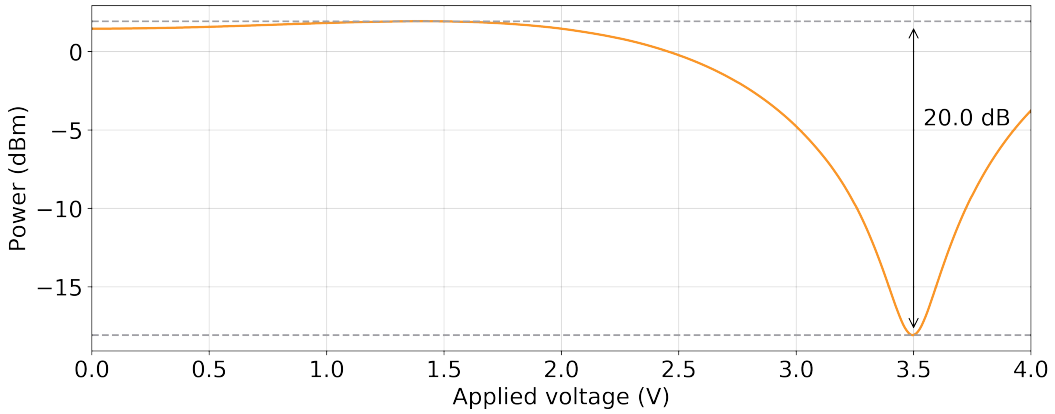

Figure 6.6: Photocurrent measured from the on-chip photodiode (converted to optical power) versus voltage applied to the VOA. This setup is able to obtain ∼20 dB of attenuation between the phase encoding laser and the injection locked laser, which is useful to minimise the power sent back to the phase encoding laser while still maintaining a good injection power in the other direction.

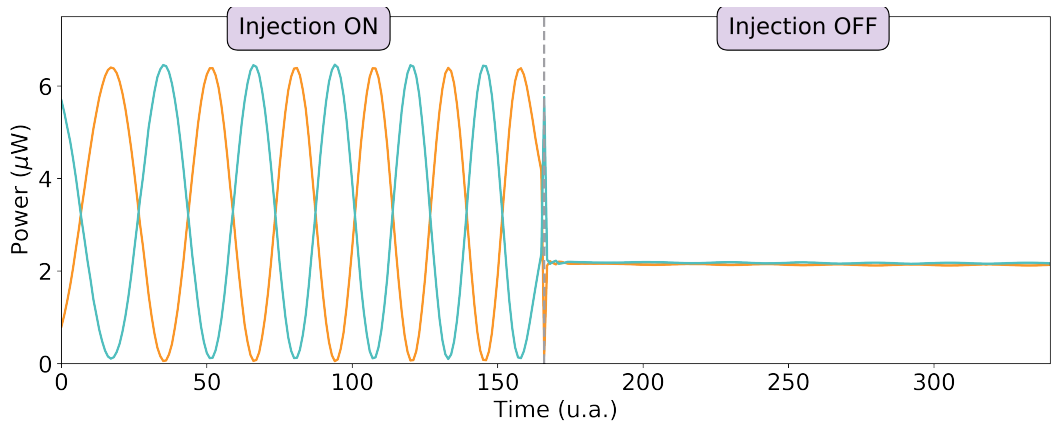

Figure 6.7: Interference fringes at the output of the receiving interferometer. A high power corresponds to a completely constructive interference on one arm, which is mirrored by a low power, destructive interference on the other arm, and vice versa. The fringes disappear once the injection from the phase encoding laser is turned off, because the pulses generated by gain switching are not coherent among each other.

injection locked laser is pulsed, and the wavelengths of the two lasers are matched. This results in pulses with a zero relative phase difference at the interference coupler. Coherence transfer is measured as in Section 5.4: pulses interfere in an aMZI, and the contrast between constructive and destructive interference is measured. The experiment showed a visibility value of 98.3% when the injection was on, while no fringes (hence no coherence) were recorded while the injection was off (Figure 6.7).

6.2.4 Differential phase encoding

In classical communications, PSK encoding protocols are widely used to transmit information. The advantage over simple ON-OFF keying is given by the ability to encode multiple bits per clock cycle, largely increasing the amount of information that can be transmitted. However, PSK encoding is subject to errors due to phase drifts in the channel that could offset the phase reference between Alice and Bob. A way around it is to encode information in the phase *difference* of pulses rather than its absolute value. This is the concept behind differential phase-shift keying (DPSK): pulses will be affected in the same way by phase drifts (which are much slower than the transmission speed), so their difference will remain constant throughout the channel. This type of modulation is similar to the one used for the DPS protocol. Information is stored in the phase difference between pulses, not the phase itself.

The phase-encoding capabilities of the transmitter can then be tested by using the QTx as a DPSK encoder. Modulating the phase encoding laser with different intensities will implement different phase shifts. Representing the pulses in the optical phase space, the

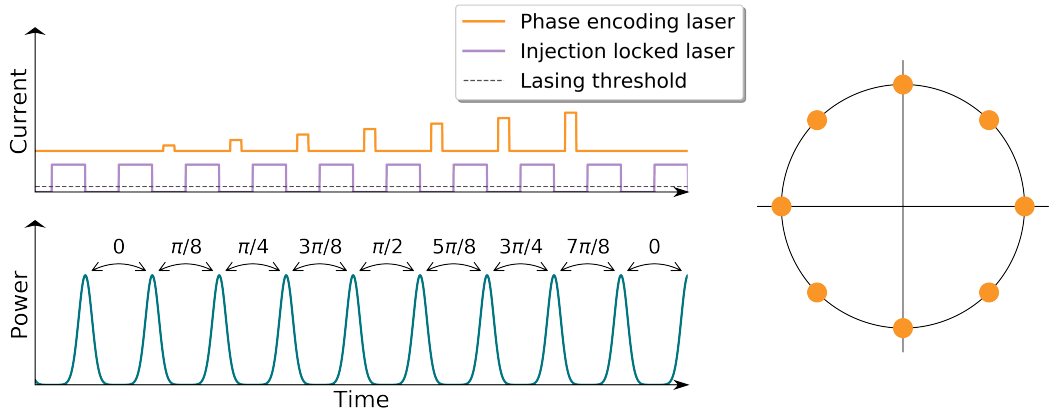

Figure 6.8: Left: Incrementing modulation on phase encoding laser generates pulses with increasing phase difference. Right: expected constellation plot in the optical phase space.

results should draw a circle around the origin. For an 8-level modulation, the result should look like Figure 6.8.

The results are compatible with the predicted outcome. This experiment shows that eight very distinct levels of phase difference can be generated (Figure 6.9). This is useful in classical communications, where DPSK is used to encode information, but also proves that the QTx is performing well for phase-encoded QKD as well.

6.3 Experimental parameters and results

The final step is to perform QKD using the chip. Results show that the chip-based QTx is able to efficiently encode QKD states. The bit sequences encoded in the pulse trains generated by the QTx are generated by a quantum random number generator (QRNG). For both BB84 and DPS protocols, using SNSPDs, the transmitter chip achieves record results (Figure 6.10), compared to similar chip-based QKD experiments [96].

The DPS protocol is implemented by modulating the phase encoding laser for ∼80 ps in between two seeded pulses at 2 GHz. The photon flux was set to 0.194 ph/pulse. The recorded QBER value is 2.5%; this results in an asymptotic key rate of 400 kbit/s at 20 dB, which is equivalent to 100 km of standard optical fibre.

The BB84 protocol encodes data into the phase difference between pulse pairs, while different pulse pairs have random global phases. These phase differences can be set to four different values, representing the Z and X bases. The phase encoding laser is gain-switched at 1 GHz with a duty cycle of 85%, to ensure coherence within the pairs and randomisation between different pairs, while an additional modulation encodes the bit values. The photon flux for the signal pulses was set to 0.2 ph/pulse. An external intensity modulator is used to encode decoy states. For this experiment, decoy states were not generated in real time.

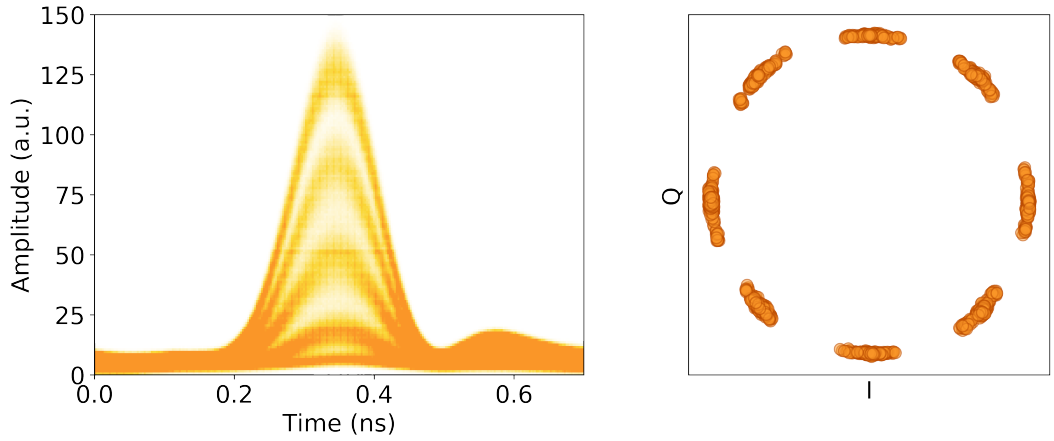

Figure 6.9: Eye diagram (left) and constellation plot in the phase space (right) of 8-level DPSK. Eight very distinct phase encodings are generated, with the potential to generate more.

Instead, the same experiment was repeated three times using three different photon fluxes (0.2 ph/pulse for signal states, 0.1 ph/pulse for decoy states and 1×10^{-5} ph/pulse for vacuum states). To estimate the key rates, the probability of sending a decoy state and the probability of sending a vacuum state are assumed to be equal at 1/16.

The QBER is 2.2%, resulting in an asymptotic key rate of 270 kbit/s at 20 dB. Fitting the experimental data with a simulated curve, it is possible to see that such a setup would yield >2 Mbit/s at 10 dB, which would be a record for integrated photonic chips. An experiment performed with 75 km of real fibre, with a measured loss of 16.7 dB (∼0.22 dB/km), shows results in line with the simulated channel loss. The QBER is 2.04%, with a raw count rate of 1.54 Mc/s and an asymptotic SKR of 618 kbit/s, which are in excellent agreement with the results of the emulated channel loss measurements.

The same experiments were then repeated using InGaAs SDAPDs. For the decoy state BB84 (DPS) protocol, a QBER of 3.2% (3.5%) and an asymptotic SKR of 840 kbit/s (125 kbit/s) at 10 dB attenuation, corresponding to 50 km of standard single-mode fibre, were obtained, which are comparable to SKRs obtained with bulk optics QTxs [178]. Using SDAPDs allowed to take measurements at a lower channel loss. This is because the count rates at 10 dB are lower, due to the lower efficiencies of these detectors. In similar conditions, the SNSPDs were not able to record data at low losses, because the high count rates saturate the detectors, which in turn shut off to prevent damage.

6.4 Conclusions and discussion

This QTx chip shows that integrated photonics is a promising area of development for QKD networks. The encoding based on direct phase modulation and OIL is able to remove the need

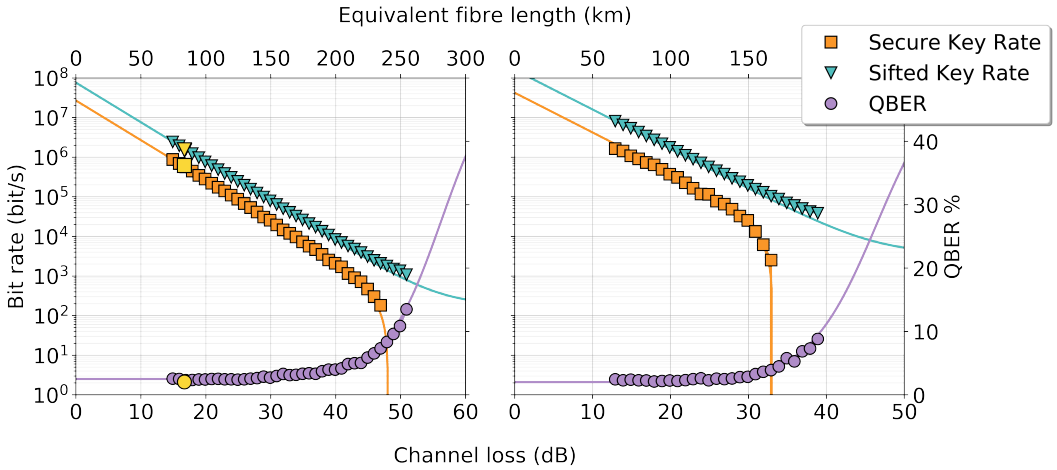

Figure 6.10: QBER and asymptotic SKR obtained for the BB84 (left) and DPS (right) protocols as a function of the channel loss. The markers represent experimental values, the solid lines the simulation results. The yellow points represent data taken on real fibre.

for power-hungry phase modulators. Record results were obtained with this chip, proving that the approach is worth exploring further for more applications.

At the same time, it is important to note that the absence of an optical circulator between the phase encoding and injection locked lasers in our integrated device severely affects the coherence transfer from the phase encoding laser. Reflections from the injection locked cavity, albeit attenuated, interfere with the light coming from the phase encoding. In extreme cases, this can make it impossible to obtain a signal that is stable and has high coherence.

One way around the lack of optical isolation in integrated chips is to carefully adjust the attenuation between the two lasers. However, it is necessary to find a trade-off: a high attenuation might give a power too low to seed efficiently the cavity; no coherence transfer is observed in these cases, and the injection locked laser behaves as in the free-running, gain-switched mode of operation. On the other hand, an attenuation too low will cause high-power pulses to be reflected from the injection locked laser back into the phase encoding cavity, affecting the coherence. In particular, the coherence transfer can be depleted to a visibility of $< 20\%$ when the VOA is not attenuating enough. For this chip the VOA was set to an attenuation of 10 dB between phase encoding and injection locked lasers. It is important to keep this in mind when designing circuits for this kind of applications.

Chapter 7

On-chip generation of decoy states for QKD

The next step for building a deployable QKD system is the use of decoy states to make the BB84 protocol more robust. This chapter shows that it is possible to use integrated devices to generate decoy states.

The author was responsible for the data acquisition and analysis. Results show that high bit rates are achievable using electro-absorption modulators to generate decoy states efficiently.

7.1 Decoy state generation

Section 2.1 gives information about how and why decoy states improve the performances of QKD systems, specifically for the BB84 protocol. For proof-of-principle experiments, generating decoy states is often simulated using a VOA. It is sufficient to perform the experiment separately at a lower photon flux to obtain the decoy parameters. For real-life applications, however, actual keys have to be extracted: efficiently generating decoy states in real time becomes an essential requirement in this scenario.

Usual implementations of decoy-state QKD employ external intensity modulators to attenuate selected pulses [192]. However, due to their high power consumption, scaling to larger systems becomes less feasible. Integrated photonics might provide a solution to this. There have been approaches that employ a MZI and high-speed EOPMs to attenuate the pulses by destructive interference [96], however this approach requires high RF driving voltages and does not reach high extinction ratios.

This chapter will investigate an alternative way of generating decoy states on chip, using an EAM to attenuate the pulses emitted by the QTx.

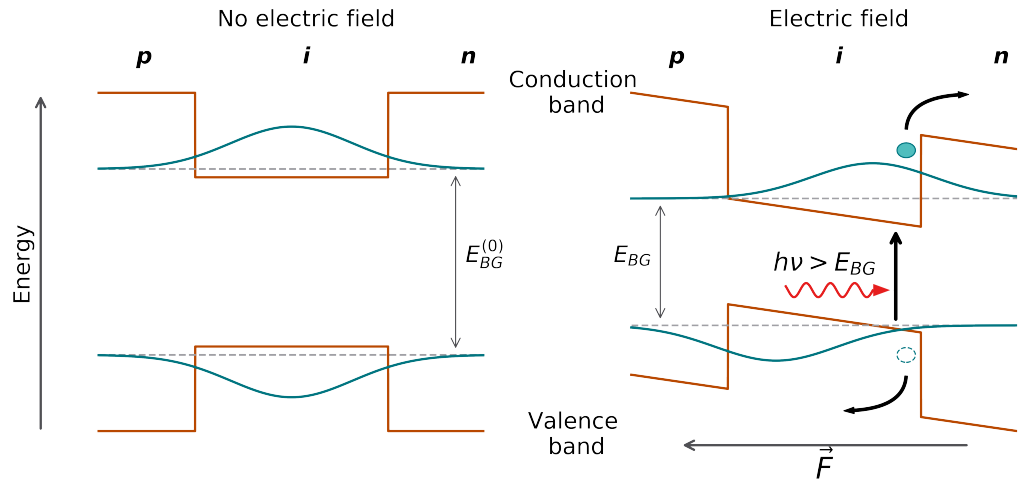

Figure 7.1: Quantum-Confined Stark Effect: applying an electric field shifts the energy bands and reduces the bandgap. A photon with a higher energy is absorbed and creates an electron-hole pair which is then swept by the electric field $\vec{F}$.

7.2 Experimental setup

7.2.1 Integrated transmitter

The chip-based transmitter resembles the circuit used for the chip-based QTx in Chapter 6, with the addition of an EAM at the output of the injection locked laser (Figure 7.2). An EAM is a device that modulates the intensity of light travelling through it via tunable absorption. The device is a P-I-N structure with multiple quantum wells; absorption is performed via carrier generation in the quantum wells.

The rate of carrier generation depends on the bandgap, which can be shifted according to the quantum-confined Stark effect (QCSE) (Figure 7.1) [194–196]. Applying an electric field in reverse bias to the device causes a decrease in the bandgap energy, which in turn changes the absorption spectrum. When light is injected, it gets absorbed and creates electron-hole pairs. These are swept to opposite sides of the quantum well by the electric field, increasing the tunnelling probability and decreasing the carrier density in the intrinsic region. In forward bias, the carriers recombine radiatively in the intrinsic region and the EAM starts behaving as a light emitting diode [197]. The emitted wavelength shifts as a function of the bias current, due to the QCSE.

Such a device is able to achieve high extinction ratios (>20 dB) at GHz speeds while still requiring significantly less power than an electro-optic modulator (2 V–3 V compared to voltages above 10 V).

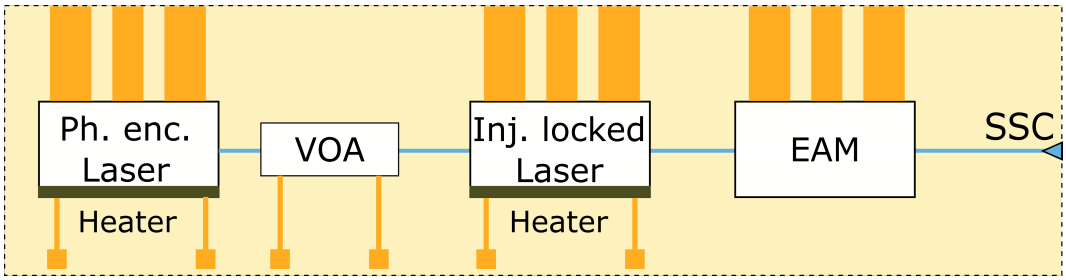

Figure 7.2: Schematic of the EAM-decoy circuit. The VOA is used to calibrate the injection power. The EAM is used to both generate decoy states and attenuate the signal to single photon level.

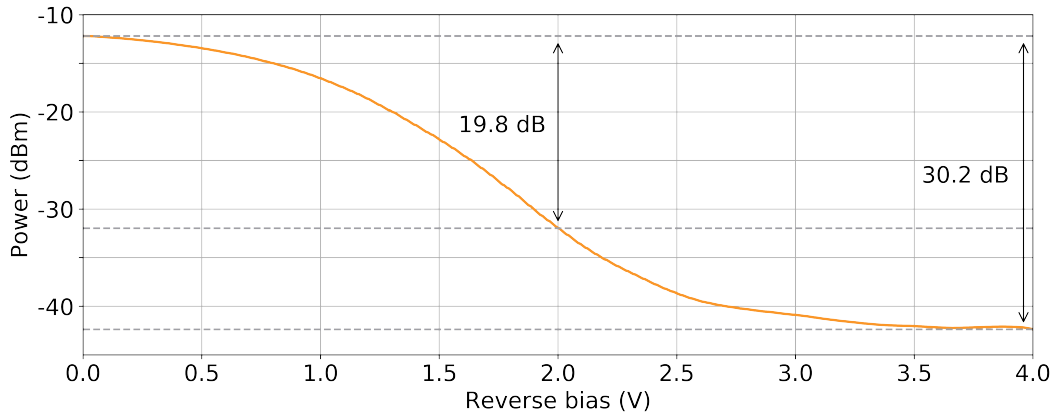

Figure 7.3: Measured power at the output of the chip as a function of the CW voltage applied to the EAM.

7.2.2 Layout of the experiment

The setup is similar to the one in Chapter 6. Two analog channels of the AWG drive the phase encoding laser and the EAM, while the injection locked laser is driven by a digital channel. A TEC is used to keep the temperature at a stable value. The receiving interferometer is the same, chip-based one used for the previous experiment.

7.3 Characterisation

7.3.1 EAM

The EAM works by increasing its absorption when in reverse bias. Strong attenuations of more than 10 dB can be achieved with as little as 2 V, as shown in Figure 7.3.

When driven with forward bias, the EAM is emitting light. It is possible to characterise the Stark shift of the wavelength by measuring the emission spectrum as a function of the

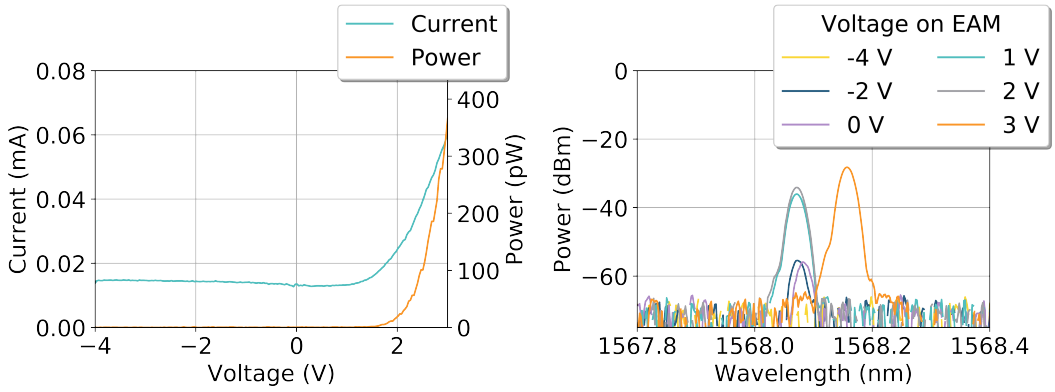

Figure 7.4: Left: Emission of the EAM in forward bias, shown in the I-V curve. Right: Spectral shift of the light emitted by the injection locked laser when forward-biasing the EAM.

applied voltage (Figure 7.4), when the injection locked laser is on as well.

This spectral shift means that the parameters of the EAM must be chosen with some care: an RF amplitude which would bring the EAM above its light emitting threshold is not desirable. This is easily adjustable by offsetting the RF amplitude with the DC bias.

To characterise the QTx performance and find the best parameters, light is not attenuated to the single photon level and is sent to a fast sampling oscilloscope. This makes it faster to acquire data and allows to see in real time what happens when parameters are adjusted. Among the variables that can be tweaked are the phase encoding laser's wavelength, which can be shifted by changing the voltage on the laser heater; the injection power, adjustable with the VOA between phase encoding and injection locked lasers; the temporal delay between the two lasers, which makes sure that the seeded pulses in a pair are coherent; the phase encoding laser's RF amplitude and duty cycle. The results here are encouraging: the QBER is below 4% (Figure 7.5). The spikes in QBER can be attributed to temperature fluctuations due to external factors (i.e. air conditioning, doors opening, movement of people). However, it is important to notice how the QBER levels for signal and decoy states are in agreement, even though the signal and decoy patterns are chosen randomly and independently from one another. This is a good sign that the EAM makes it viable to realise decoy-state intensity modulation and does not produce any residual phase modulation.

7.4 Results

7.4.1 Decoy states generation

The experimental setup is the same as in Chapter 6, with an added RF track for the EAM. An AWG and SMUs drive the components on the chip, including the EAM. The first experiment

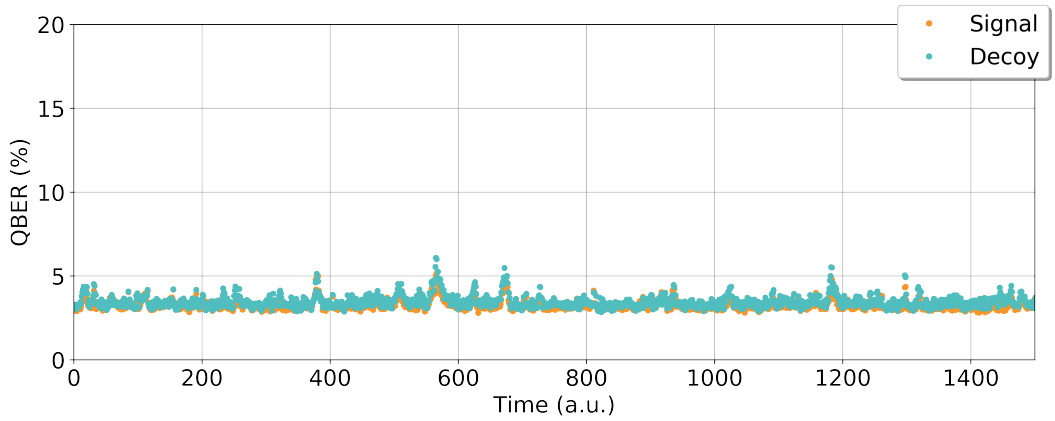

Figure 7.5: QBER over time for a QKD experiment with decoy states generated on chip.

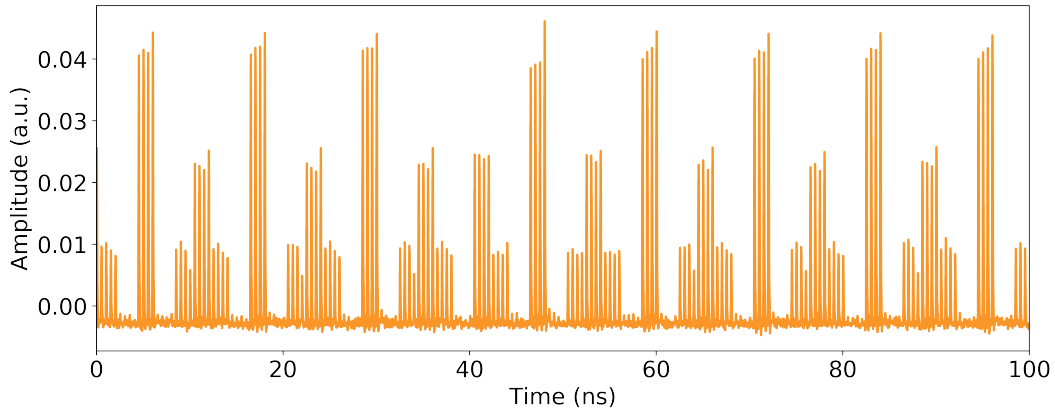

Figure 7.6: EAM attenuation of decoy states at four different levels.

measures the capabilities of the EAM to attenuate pulses. The AWG drives the EAM to attenuate (or not) groups of four pulses. This is done at four different levels, as shown in Figure 7.6.

The next step requires to calculate the visibility of interfering pulses. This is important in order to check whether the introduction of decoy states adds noise to the system. This is not the case: Figure 7.7 shows that the visibility is above 98%, which proves that there is still a good coherence transfer and the EAM does not introduce any noticeable noise.

7.4.2 QKD with decoy states

Finally, a QKD experiment is performed with decoy states generated on chip. The experiment is akin to the one described in Chapter 6, using the same photon fluxes for the decoy-state BB84 protocol and the same probabilities of sending a decoy or vacuum state. Using SNSPDs, the SKR at 10 dB is estimated to be around 1 Mbit/s when the QBER is around 5%.

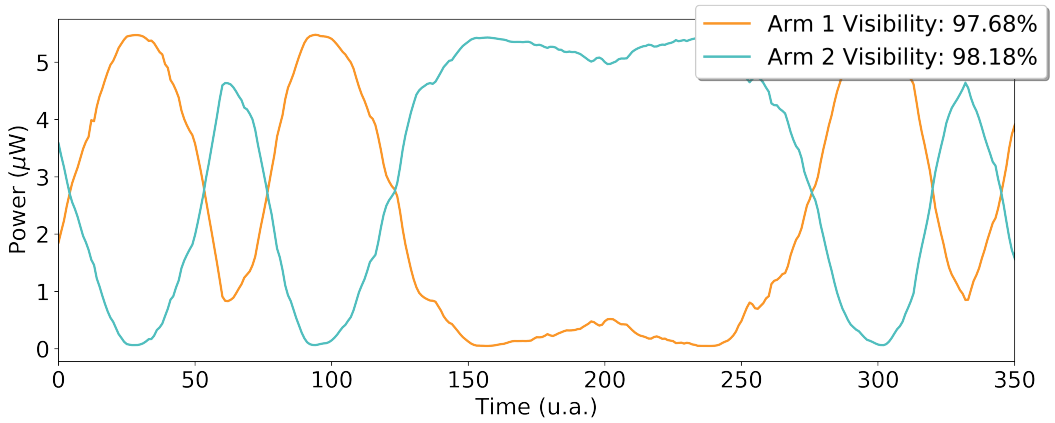

Figure 7.7: Visibility of interfering pulses. Both signal and decoy states are interfering.

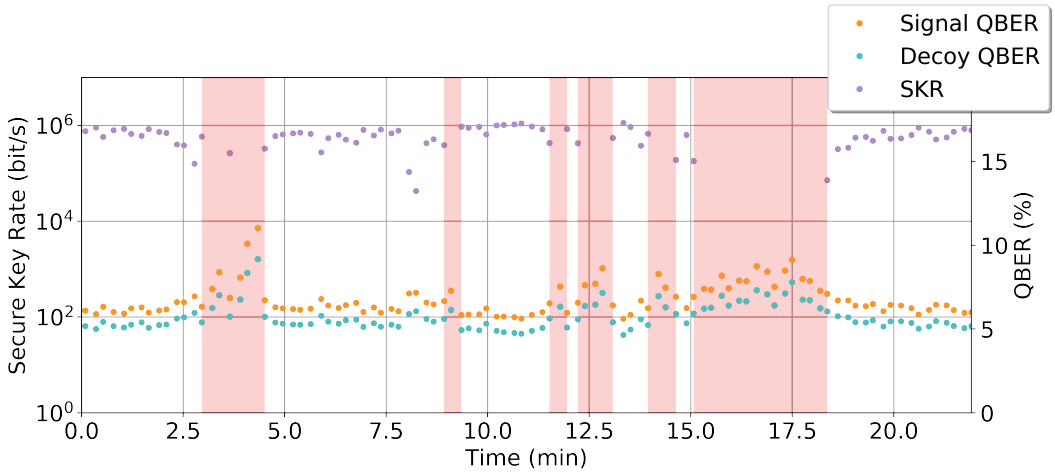

Figure 7.8: 1 Mbit/s secure key rate achieved using decoy-state BB84. The red sections are times when a positive SKR is not achievable due to high QBER.

Compared to the other experiment reported in the previous chapter, this system performs significantly worse. The QBER values are higher (and consequently the SKR lower), and the output is less stable over time. However, this is not due to the presence of an EAM in the circuit: the main reason for this decrease in results comes from issues in the fabrication process, affecting the performance of the chips. This has been verified by running tests on chips from the same fabrication batch, which do not have an EAM but still perform worse than their counterparts from previous batches.

7.5 Conclusions and discussion

Generating decoy states efficiently is one of the major challenges for QKD. The PNS attack is a big security flaw for the BB84 protocol, as it would allow Eve to obtain information about the key by exploiting multi-photon pulses [61]. Lowering the mean photon number to minimise multi-photon events would reduce drastically the count rates and the maximum distance achievable. Decoy states overcome this issue, as using different intensities give a way for Alice and Bob to detect eavesdropping by measuring detection statistics.

Decoy state generation has been performed using on-chip MZI modulators, however these require high driving powers. A more power-efficient approach using EAM has proven to be very effective at generating decoy states while still using extremely low power. The I-V curve shown in Figure 7.3 prove that even at a bias of $-4\,\mathrm{V}$ the current stays low, around $15\,\mu\mathrm{A}$, which results in a power consumption of $\sim 60\,\mu\mathrm{W}$ when operating in high-extinction regimes.

The performance of the integrated EAM has been tested. Generating decoy states does not affect the coherence transfer, and key rates of $>1\,\mathrm{Mbit/s}$ at $10\,\mathrm{dB}$ loss are achievable with better stabilisation of the system. This is possible by mitigating the temperature drifts affecting the chip: in turn, that would also make it easier to find good driving parameters for the QTx. This would mean a decrease of the QBER which will increase dramatically the SKR. Improving the fabrication process, which was the main contributing factor to the high QBER values, will also contribute to the stability of the chip.

This page intentionally left blank.

Chapter 8

Real-time generation of quantum random numbers

This chapter will describe a chip-based approach to QRNG [198], similar to already developed systems [199]. The novelty of this QRNG is given by its real-time generation capabilities and the ability to generate data at high rates, thanks to compact electronics.

The author was responsible for data acquisition. Results show random number generation rates higher than similarly-designed QRNGs

8.1 Random Number Generation

The security of QKD discussed in this thesis holds if and only if the initial string sent from Alice to Bob is chosen completely randomly and unpredictably [106]. Generating random numbers has been a challenge to researchers for decades, and random number generators (RNGs) are used in a wide range of applications: lotteries, scientific simulations, cryptography are some of the most prominent users of random numbers.

For practical purposes, sometimes pseudo-random number generators (PRNGs) are used, which output random numbers with a certain degree of predictability. These number generators are based on algorithms [200]: the next number in the sequence can be generated by

$$x_{n+1} = f(x_n, s), \tag{8.1}$$

where s is the *seed*, a small number needed to initialise the algorithm, x_n is the previous number in the sequence, and f should be complex enough that it is hard to compute the next number in a sequence by only looking at the sequence itself. Such approach is useful in applications where security is not a concern and repeatability is desirable, such as scientific simulations. However, it is important to make sure that the chosen algorithm successfully outputs uniformly distributed numbers, as non uniformity can lead to issues [201].

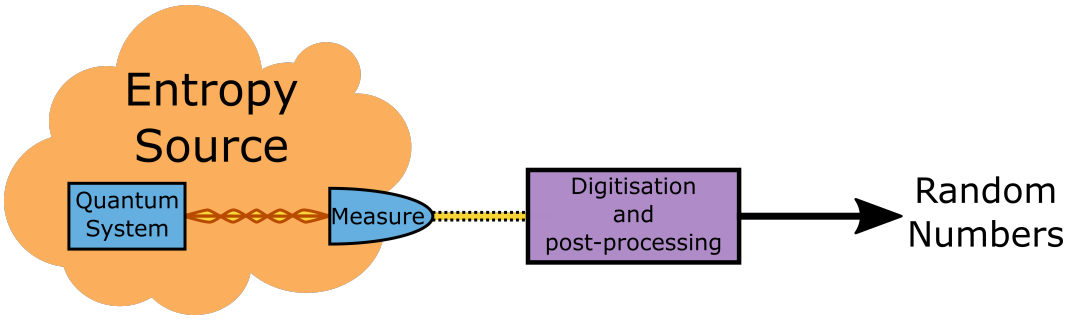

Figure 8.1: Schematic representation of a QRNG.

If reproducibility of the results is a security issue [202, 203], true random number generators (TRNGs) might be used instead. TRNGs are more complex systems than PRNGs: this is due to the difficulty in finding a truly random source [204], but also to the difficulty of certifying the randomness of the generated numbers. TRNGs rely on physical processes, such as thermal or atmospheric noise, to generate random numbers. Their chaotic behaviour (i.e. their dependence on sensitive changes of initial conditions) ensures that the result is unpredictable as it is impossible to know the position and momentum of every single particle in the system.

Despite their unpredictability, however, they are still deterministic devices in principle, as the laws governing their behaviours are chaotic but classical. This means that, despite being random, they can still be obtained by an all-powerful attacker. A guarantee of security only comes from quantum phenomena, which is the basis for QRNGs. Because of the inherent randomness and unpredictability of quantum phenomena, such generators are often seen as the best candidates for generating random numbers.

A simple example of a QRNG is a single photon travelling through a beam splitter with one detector at each output arm [205, 206]. If the beam splitter has an exact 50:50 splitting ratio, the photon will randomly travel to one detector or the other, without any chance to predict which outcome will occur.

A more general description of a QRNG includes an entropy source, a digitisation system and a post-processing element (Figure 8.1). The entropy source is represented by the measurement of a quantum system (not the quantum system itself): the randomness comes from the quantum process and the measurement collapses the wave function at each clock cycle and outputs an analog signal that is recorded by the digitising system. The digitisation process is needed for post-processing: the measurement results (e.g. the photocurrent readout from a photodiode) are converted into a stream of bits that can be easily manipulated by common electronics. Finally, the post-processing is used to remove any classical noise and ensure that the unpredictability of the generated string only comes from quantum events. The digitisation and post-processing steps are usually implemented on the same electronic equipment.

8.2 Phase noise in DFB lasers

For QKD, the usual light source is an attenuated pulsed laser. This makes it convenient to use lasers to generate random numbers as well [207–209]. In particular, DFB lasers are the most widespread choice, as they are easily fabricated and require relatively low driving powers, as well as allowing high-speed modulation.

When a laser is kept below its lasing threshold, coherent emission is suppressed while spontaneous emission is the dominant phenomenon. Spontaneously emitted photons have a phase determined by vacuum fluctuations, which are inherently random [181, 182, 210]. The driving current is then increased above the lasing threshold: this guarantees emission of light at a deterministic amplitude but a phase determined by the spontaneously emitted photons.

In terms of the rate equations, the behaviour can be expressed with the same equations discussed in Section 5.2 without the injection-related terms:

$$\frac{\mathrm{d}N(t)}{\mathrm{d}t} = J(t) - R(N) - \Gamma a[N(t) - N_{tr}]S(t) + F_N(t) \tag{8.2}$$

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t} = \{\Gamma a[N(t) - N_{tr}] - \gamma_p\}S(t) + \beta BN^2(t) + F_S(t) \tag{8.3}$$

$$\frac{\mathrm{d}\phi(t)}{\mathrm{d}t} = \frac{\alpha}{2}\Gamma a[N(t) - N_{tr}] + F_\theta(t). \tag{8.4}$$

The noise terms $F_N(t), F_S(t), F_\theta(t)$ cannot be neglected in this case, and will contribute to the random phase diffusion in the cavity. Pulsing the laser periodically above and below threshold (making sure that the OFF time is enough to suppress any leftover coherence and for enough noise to enter the cavity), consecutive pulses will have random phase differences (Figure 8.2). Such a difference can then be recorded and used as a source for random numbers.

Gain-switching a laser to generate short pulses, however, does not provide good quality interference: this is due to the chirping and jitter effects happening at the beginning of the pulses (as discussed in Section 5.4), caused by fast changes in the carrier density. This can be overcome by increasing the electrical pulse's duty cycle, as well as increasing the laser's DC bias. After the initial overshoot, light will stabilise to a steady state, where the optical properties of the pulse are stable and interference will have negligible noise from those phenomena. That steady-state section of the pulse interference will be sampled from the pulse train and processed by the capturing electronics.

Calculating true randomness It is important to notice that, in real devices, other noise factors will have a contribution to the recorded data. In particular, as mentioned in Section 2.1, classical contributions to the data coming from thermal noise or timing jitter will have a gaussian distribution which distorts the histogram's U-shape. In the most conservative scenario, similar to what happens with QKD, it is assumed that all classical noise is controlled by Eve. It is then necessary to evaluate how much knowledge Eve has

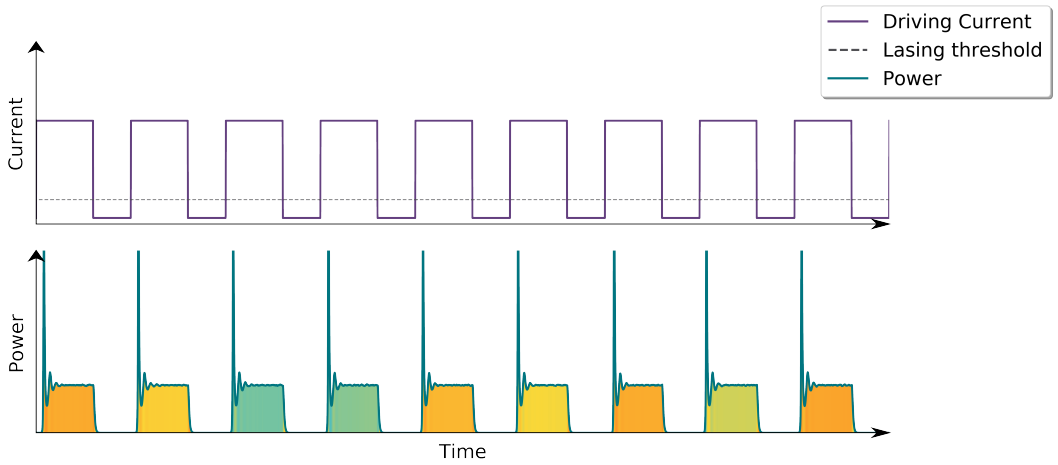

Figure 8.2: Sequence of gain-switched pulses from a DFB laser. The phase is represented by the coloured filling in the bottom plot.

about the string, in order to extract only the quantum randomness from the generated raw numbers.

The model considered here [211] assumes that the signal M recorded by the photodiode can be described as a sum of the quantum and classical contributions, respectively Q, N:

$$M = Q + N.$$

The probability density function (PDF) of this signal, $f_M(m)$ is given by the convolution of the two individual PDFs, $f_Q(q), f_N(n)$. The next step is calculating the conditional probability distribution function of M, given the classical noise N, which can be proven to be equal to the PDF of the quantum noise:

$$f_{M|N}(m \mid n) = f_Q(m - n).$$

After discretising the PDF (which accounts for the action of the analog-to-digital converter (ADC)), the min-entropy of the quantum randomness, i.e. the quantity that measures how much randomness can be extracted from the system, can be obtained by calculating the entropy of the maximum probability value:

$$H_{min}(M_{dis} \mid N) = -\log_2 \left[\max_{\substack{n \in [n_{min}, n_{max}] \\ m_i \in M_{dis}}} P_{M_{dis}|N}(m_i \mid n) \right],$$

where $[n_min, n_max]$ are the noise bounds and M_{dis} is the discretised signal.

8.3 Experimental setup

Figure 8.3 shows a schematic of the device. The photonic chip contains the interfering DFB lasers and is driven by an electronic board providing both DC and RF signals. The

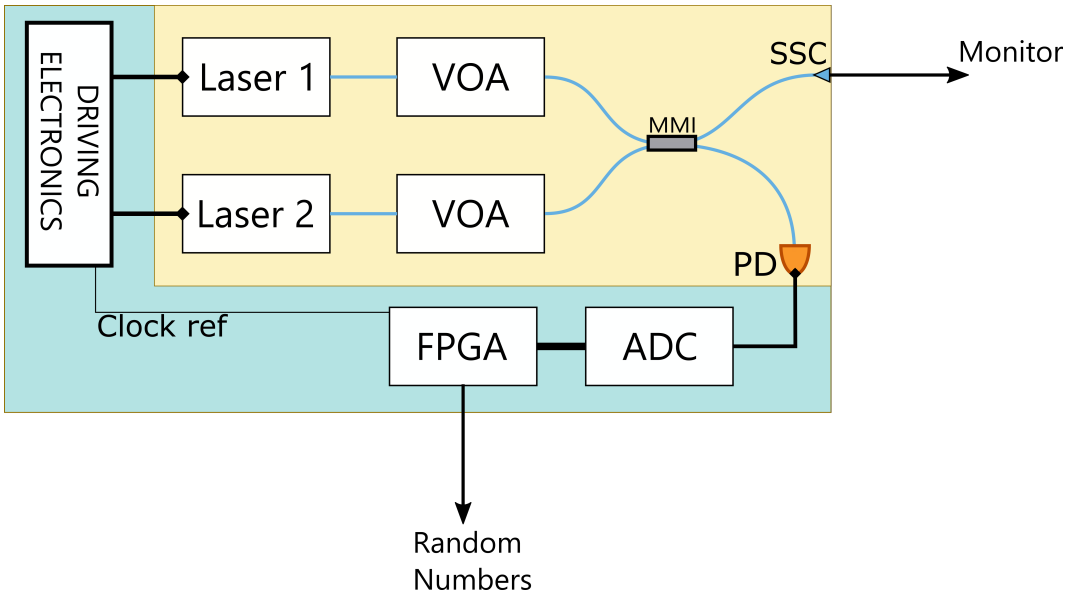

Figure 8.3: Experimental setup. The yellow section is the photonic circuit, the teal section includes the electronics. The lasers output powers are calibrated using the VOAs. The ADC and FPGA digitise and analyse data to generate random numbers.

on-chip photodiode records the interference, and the signal is transmitted to an ADC and post-processed by a FPGA board.

Integrated transmitter

The InP chip presents a minimal circuit design: Two DFB lasers are driven by the built-in electronics. VOAs calibrate the emitted powers to match at the MMI where the pulses interfere. Half of the interfering light is collected by a P-I-N photodiode connected to the data capturing electronics, while the other half is sent to a SSC and coupled out of the chip for monitoring purposes: light can be sent to an oscilloscope to check the shape of the pulses, or to an OSA to check the emission spectrum.

Real-time number generation capabilities

Electronic boards provide both the driving signals and the post-processing hardware. A two-channel phase-locked loop oscillator, clocked by the processing FPGA, provides the RF waveforms that, after amplification, drive the two lasers. The lasers are gain-switched at a repetition rate of 1 GHz. The electrical signals are skewed so that the optical pulses are generated at the same time.

After the interfering light is detected by the photodiode, its electrical signal is amplified and sent to an ADC. The resulting string of raw numbers is then processed by an FPGA

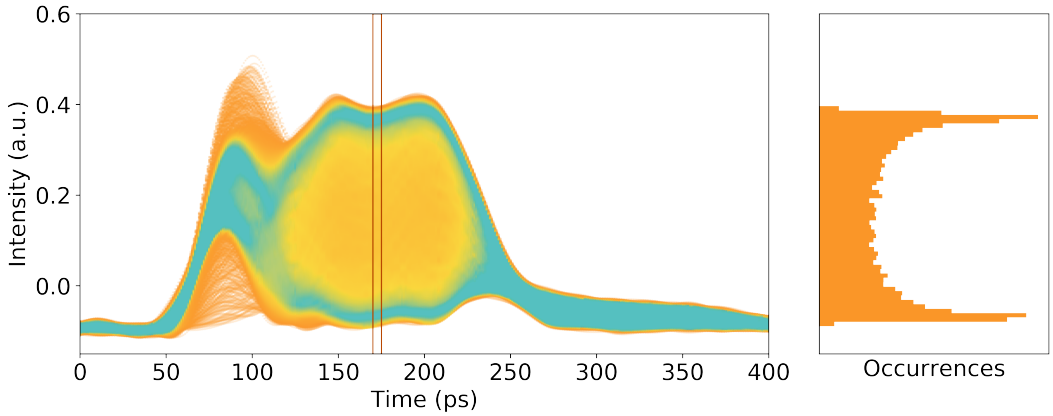

Figure 8.4: 1000 interference events, recorded by an oscilloscope, are overlapped and plotted on the left hand side. On the right is the distribution of $\sim$ 800000 interference intensities, measured in the interval highlighted by the rectangle.

board. Such a setup allows for real-time processing of the data: the ADC and FPGA are fast enough to process optical data streams at 1 GHz.

8.4 Characterisation

Temporal and spectral alignment are important to obtain good quality interference. Temporal alignment can be obtained by delaying one of the pulses' electrical signals. Spectral alignment is achieved by using the DFB lasers' heaters: these are resistive elements that heat up when a voltage is applied to them. Each laser has its own heater on the chip, independently driven by a DC voltage source. the temperature change shifts the cavity's refractive index, which in turn changes the emission wavelength.

The monitoring output is used for a first characterisation. Light is sent to an OSA to calibrate wavelength matching, and to a fast-sampling oscilloscope to match the temporal characteristics. Once the pulses are aligned, the oscilloscope can be used to tweak the interference of the two lasers. Figure 8.4 shows how the interference looks like and exhibits the characteristic U-shaped histogram, signature of randomness coming from phase noise.

This first step was crucial: characterising the system is useful not only for estimating the performance of the QRNG, but especially to find the right driving parameters and ensure that the generated numbers have a truly random source. The histogram in Figure 8.4 agrees with the predicted behaviour discussed in Section 8.1, hence is a strong indicator that true quantum noise is present in the system and can be extracted by post-processing. Note that this is a qualitative measurement, aimed mainly at finding the correct operating parameters of the two lasers. Data acquisition and analysis is discussed in the next section.

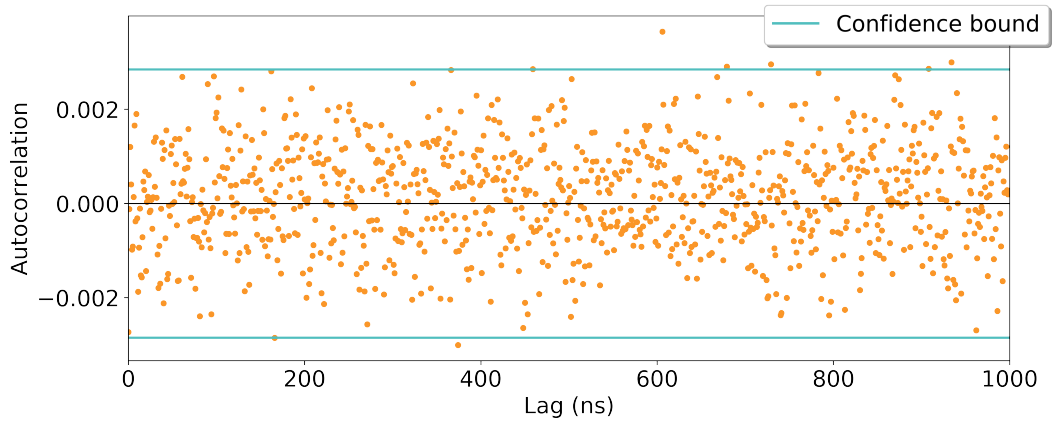

Figure 8.5: Autocorrelation of consecutive pulses obtained by using the plug-and-play QRNG system. Confidence interval is 99 %

8.5 Results

The next step is to generate random numbers using the capture electronics. The ADC has a 10-bit range, which is downsized to 8 bits by the FPGA. A measurement of the pulses autocorrelation (Figure 8.5) shows that pulses are not correlated (within statistical confidence intervals). This is a good sign, as it means that an eavesdropper could not retrieve the whole string if they have access to a subset of it.

The raw numbers read by the board are biased, as shown in the histogram of Figure 8.6, and differ significantly from the expected distribution: an attacker would know that the amplitudes corresponding to the peaks of the histogram appear more frequently. The raw string does not span the whole 8-bit range $[0, 255]$, due to the fact that the maximum power that the board is able to record is higher than the powers used for the experiment: this reduces the randomness of the string even further, as the attacker could discard a large region of the range for their guesses. Another feature worth noticing is that the U-shape of the histogram is not symmetric. This is mainly due to the electronic noise floor of the capture board. Classical noise is also responsible for the peaks of the U-shape being significantly broader and, consequently, lower than the expected distribution.

In order for the numbers to be uniformly distributed across the whole 8-bit range, several approaches can be used. A simple method to uniformly distribute the numbers is to apply a finite impulse response (FIR) filter (Figure 8.7) [212]. This is a polynomial function applied to the raw data that allows to scramble the string in order for it to uniformly span the 8-bit range:

$$y(n) = \sum_{i=0}^{N} b_i x(n-i), \tag{8.5}$$

where $x(n)$ is the input signal, $y(n)$ is the output signal, N is the filter order and b_i are the filter coefficients. Since such an extractor simply scrambles the raw number distribution,

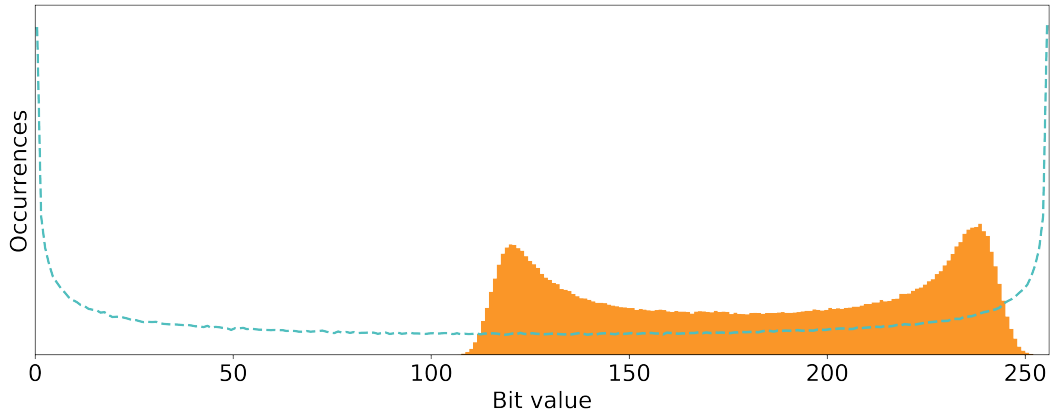

Figure 8.6: Histogram obtained by recording data using the plug-and-play QRNG system. The dashed, teal line represents the expected distribution in the ideal scenario of no classical noise and spanning the whole ADC 8-bit range. In a real system, classical noise makes the peaks of the U-shape histogram broader and lower, and the ADC range is higher than the pulses amplitude, which makes the histogram not span the whole 8 bits.

the output rate of random numbers is simply given by multiplying the optical pulse rate (1 GHz) by the number of raw bits recorded per pulse (8 bit from the ADC). This results in a generation rate of 8 Gbit/s.

However, the FIR filter does not extract randomness from the raw string: classical noise is still present and affects the security of the random numbers guaranteed by quantum mechanics. Nevertheless, this filter is still useful if the numbers are used in applications where security is not a concern, such as in scientific simulations.

Data obtained from a QRNG is generated from both quantum and classical noise. The latter is usually introduced by imperfections in the components, such as the limited band-

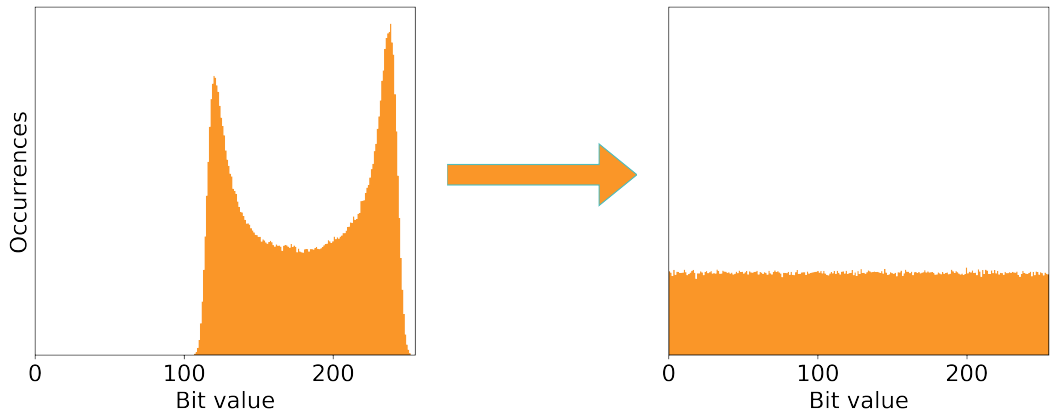

Figure 8.7: An FIR filter flattens and spreads the distribution across the 8-bit range.

width of the detection apparatus or the electronic noise in the driving signals. Classical noise is an issue because it comes from a deterministic source, hence can give an attacker information about the raw string. If security of the generated numbers is required, the FPGA can be programmed to implement randomness extractors (i.e. post-processing algorithms that remove classical noise from the raw data) such as the Toeplitz [213] extractor. This is proven to be secure against quantum adversaries; moreover, the random hashing matrices needed for the algorithm can reuse the same seed multiple times without loss of security, which makes it more efficient. For this QRNG, the amount of quantum randomness extractable was estimated by calculating the min-entropy of the data, as shown at the beginning of this chapter [211]. A min-entropy of 4.09 bits per 8-bit sample was calculated, which would translate in a secure generation rate of $\sim$4 Gbit/s.

8.6 Conclusions and discussion

This chapter has successfully demonstrated the real-time generation capabilities of a QRNG system based on integrated photonics. Such a system is stable and does not require external control once it is running. This QRNG does not require any additional equipment. The whole system is contained in a 2U rack box and is ready to use, which makes this a very practical device for QKD.

In order to assess how good the generated random numbers are, samples of the generated string are passed to the NIST test suite [214]. This is a battery of tests that analyse the distribution of a set of data by looking for patterns. The data generated with this QRNG is able to pass all tests of randomness (Table 8.1). This is a good sign that the numbers are distributed uniformly.

Since this is a proof of principle experiment, aimed at showing the plug-and-play capabilities of the system, only one battery of tests was run. There are more comprehensive testing suites, performing more tests, which can be used. It is worth noticing that the suites test strings of already post-processed data. This is because what these tests do is checking that the output of the QRNG is uniformly distributed. The reason post-processing of the raw data is needed in the first place is because the raw string of numbers is biased by the arcsin distribution of intensities. A string of pre-processed numbers, hence, would not (and is not required to) pass these randomness tests: post-processing is an integral part of a QRNG system.

It is important to consider the security of the device. The generated random numbers can be considered secure as long as the device can be trusted. Assumptions on trust have to be carefully considered: while device-independent approaches guarantee security without having to trust the system, they are still at a very early development stage, and require constant control over the system in order for it to work. In a realistic scenario, however, it is not unfair to assume that it is possible to check a system and rule out tampering from

Statistical test	P **value**	**Proportion**	**Result**
Frequency	0.9061	0.989	Success
Block Frequency	0.0835	0.992	Success
Cumulative Sums	0.8817	0.986	Success
Cumulative Sums	0.3838	0.989	Success
Runs	0.8580	0.986	Success
Longest Run	0.2968	0.992	Success
Rank	0.6371	0.986	Success
FFT	0.2812	0.993	Success
Non Overlapping Template	0.5045	0.990	Success
Overlapping Template	0.8343	0.983	Success
Universal	0.1238	0.987	Success
Approximate Entropy	0.3330	0.990	Success
Random Excursions	0.4151	0.989	Success
Random Excursions Variant	0.4882	0.992	Success
Serial	0.2012	0.990	Success
Serial	0.4101	0.995	Success
Linear Complexity	0.3361	0.992	Success

Table 8.1: Results of the NIST test battery applied on 10^3 strings, each having a length of 10^6 bits.

external attackers. At that point, the main limitation comes from the sensitivity of the system to certain parameters, e.g. temperature. If a system is well characterised, and the parameters are kept under control, then trusting the device is a fair assumption and the QRNG can be used to generate secure numbers.

This page intentionally left blank.

Part III

Final remarks

This page intentionally left blank.

Chapter 9

Conclusions

With the advent of quantum computers, it is becoming more and more important to secure existing data transit using technologies that are able to resist attacks from a computationally all-powerful attacker. Current public-key protocols such as RSA are based on problems that a quantum computer can solve easily, making the security of data in transit a big concern. Quantum mechanics is a threat for security, but it can also become beneficial if exploited to counter such attacks, "fighting fire with fire". Indeed, quantum communications have been quickly developing over the last two to three decades, demonstrating that it is possible to communicate securely, using quantum mechanics to detect and eliminate eavesdropping. QKD is the most promising technology to enable secure communications: the laws of quantum physics guarantee a key distribution between Alice and Bob which is safe from any eavesdropping. The security of the key is independent from any attacker's computational power, as it is not generated from an algorithm. After the key distribution, classical symmetric key protocols such as the one-time pad or AES can be used to encrypt the message and send it through the communication channel.

This thesis has demonstrated how photonic integrated circuits have the capabilities to dramatically change the field of quantum communications. QKD in particular has benefitted from the new technology, as the number of needed components currently make systems expensive and space-consuming. Chip-based implementations have been shown to perform in line with bulk optics systems, while occupying a fraction of the space and costing a fraction of the price of a commercial QKD system.

The novel light source based on direct phase modulation and optical injection locking guarantees a good quality encoding while removing the need for power hungry components such as phase modulators, simplifying the experimental requirements as well as reducing the cost of the system. Moreover, its major advantage is interoperability, which was demonstrated in this work: in Chapter 5 we showed that such a transmitter is able to encode information in different protocols and clock rates, which is desirable when users have a wide range of choice in buying a new system. The experiment demonstrated the flexibility of such a transmitter,

which is able to communicate with different receiver hardware with settling times of less than 5 seconds.

Integrating this technology on chip proved that the laser seeding technique is efficient and can out-perform existing chip-based QKD systems. In this work, we tested the capabilities of our integrated QTx by performing QKD experiments over simulated and real fibre channels. Both BB84 and DPS protocols were implemented on a simulated quantum link, achieving record results for an integrated QTx. At 20 dB, which is equivalent to 100 km of standard optical fibre, the transmitter was able to obtain SKRs of 270 kbit/s for the BB84 protocol, and 400 kbit/s for the DPS protocol, using SNSPDs. Key rates of 618 kbit/s were obtained with the BB84 protocol in a 75 km real fibre link. Using SDAPDs instead of superconducting detectors has the advantage of working at room temperature, instead of the cryogenic temperatures required for SNSPDs. These detectors do not perform as well, as they have higher dark count rates and lower efficiencies, but at the same time they are more practical and suitable for real-life implementations. Using SDAPDs, the QKD link loss was limited to less than 20 dB; SKRs for both protocols are estimated at 10 dB to be 814 kbit/s and 125 kbit/s for the BB84 and DPS protocols, respectively.

For the BB84 protocol, the PNS attack poses a major threat, as weak coherent pulses have a nonzero probability of having more than one photon. While reducing the mean photon number per pulse decreases the probability of multi-photon events, it also decreases the obtainable key rates. Decoy states offer a practical solution to this: sending pulses at different intensities, they will be blocked with different probabilities by Eve. Measuring the photon statistics for signal and decoy pulses gives a way to detect eavesdropping. In this thesis we show that decoy states can be efficiently generated on chip by using an EAM, which is able to modulate the intensity of the pulses at high speeds while using low driving voltages thanks to the QCSE. This was demonstrated in another experiment with a different transmitter. The QTx used in this experiment has lasers emitting at ∼1570 nm, due to the high losses the EAM would add at lower wavelengths. Nevertheless, decoy states could be generated efficiently at different intensity levels, while the QBER of the system remains unaffected. Key rates of 1 Mbit/s were achieved by implementing the decoy-state BB84 protocol with real-time generated decoy states. Such a result can be further improved by reducing the QBER. The relatively high values of QBER in this experiment could be attributed to defects in fabrication, as different chips from the same batch all presented the same issues.

Finally, a requirement for all QKD protocols is that the choice of the state preparations and measurements has to be random. Failing to meet this requirement would open a vulnerability in the system, as an attacker could infer information directly from the raw string, without the need for eavesdropping. To this end, a QRNG based on integrated photonics was also demonstrated in this thesis. The electronic post-processing based on an FPGA is able to output random numbers in real time at high rates, while still maintaining

a small form factor. The device is able to generate random numbers at the record rate of 8 Gbit/s using an FIR filter, or ∼4 Gbit/s using a strong randomness extractor for secure random number generation.

This page intentionally left blank.

Chapter 10

Future work

The field of integrated photonic quantum communications has a lot to offer in the near future. QKD has benefitted from the development of PICs and is expected to move towards integrated technologies in the future, in order to enable large scale deployment of secure quantum networks.

The development of QKD is still at an early stage, however: much has to be done before it can become a widespread technology. First of all, it is important to notice how the key rates obtainable from QKD are orders of magnitude lower than the Tbit/s rates currently exchanged worldwide in classical fibre links. This is mostly limited by the need to use single photons and the amount of information they can encode. There are theoretical bounds on how much information can be transmitted using point-to-point links [41]. While new protocols can surpass this bound and reach distances of hundreds of kilometres, the actual key rates are too low to be efficiently integrated into classical communications. Moreover, these protocols are often very hard to stabilise and require a large number of components, making them impractical for real-life applications. Research should be aimed at finding new solutions to this problem.

Detectors have already been the target for several attacks to QKD protocols, and despite the proposal of countermeasures to these attacks they still remain a vulnerable element in a QKD system. Protocols like MDI-QKD and TF-QKD allow to relax some of the assumptions on the measurement devices, but they remain constrained by large experimental setups which hinder their deployability. Attacks on detectors and other QKD components must be addressed, as the goal is to eventually bound Eve's information from every possible information leakage source to a minimum.

In the field of integrated photonics, the lack of optical isolation is surely a hindrance in developing QKD chips based on laser seeding. While this could be worked around by carefully adjusting the attenuation between the two lasers, an InP-based optical isolator or circulator would surely improve the performances of QKD experiments. It is also important to notice how back-reflections could potentially open side channels for attackers. While not

investigated in this thesis, it might be of interest to further analyse how this affects the obtainable key rates. The development of low-loss EAMs in the 1550 nm region is another challenge that would increase the compatibility of integrated QTxs with existing technology. On the receiver side, it will be important to minimise the coupling and propagation losses, to ensure higher detection (hence secure key) rates.

Currently, single photon detection is mainly performed off-chip: development of chip-based detectors is currently researched, and there have been interesting ideas and realisations of integrated SPDs [215–217]. However, monolithic integration of these components is still far from reality. This is arguably the most important challenge in the future for QKD, as currently used detectors constitute a bottleneck in the miniaturisation of systems. SNSPDs or fast-gated APDs [192] can be used to detect single photons. The latter are especially convenient if practical solutions are preferred over performance in single photon detection, which is better in SNSPDs. SDAPDs have lower efficiencies at telecom wavelengths, around 20 % and higher dark count rates, which results in a lower SKR when performing QKD experiments. However, they have the convenient advantage of working at room temperature, instead of the cryogenic temperatures needed for SNSPDs. SNSPDs, on the other hand, are especially useful for applications where high efficiencies and very low dark count rates are necessary.

The next step of QKD development is network applications. Point-to-point links are effective and suitable for small-scale use cases, but a widespread QKD technology will require the development of networks for secure communications. Such a development is already in progress: several countries have performed or are performing field trials of QKD systems in network configurations, with or without classical data alongside quantum keys. Integrated photonic devices will surely pave the way for a more capillary diffusion of secure communications worldwide.

Bibliography

[1] L. Tan et al. 'Future internet: The Internet of Things'. In: *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*. 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE 2010) (Chengdu, China, 2010). IEEE, 2010, pp. V5-376-V5–380.

[2] Suetonius. *Vita Divi Iulii*. Vol. 1. De vita Caesarum. Rome, 56.

[3] S. Singh. *The code book: The science of secrecy from ancient Egypt to quantum cryptography*. 1st Anchor books ed. New York: Anchor Books, 2000.

[4] F. H. Hinsley et al. *Codebreakers: The Inside Story of Bletchley Park*. Oxford University Press, 2001.

[5] W. Stallings. *Cryptography and network security: Principles and practice*. Prentice Hall, 1999.

[6] C. Adams et al. *Understanding Public-key Infrastructure: Concepts, Standards, and Deployment Considerations*. Macmillan Technical, 1999.

[7] S. Garfinkel et al. *PGP: Pretty Good Privacy*. O'Reilly Media, Incorporated, 1995.

[8] O. Goldreich. *Foundations of cryptography*. Cambridge: Cambridge University Press, 2004.

[9] W. Diffie et al. 'New directions in cryptography'. *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[10] R. C. Merkle. 'Secure communications over insecure channels'. *Communications of the ACM* 21.4 (1978), pp. 294–299.

[11] R. L. Rivest et al. 'A method for obtaining digital signatures and public-key cryptosystems'. *Communications of the ACM* 21.2 (1978), pp. 120–126.

[12] P. W. Shor. 'Algorithms for quantum computation: discrete logarithms and factoring'. In: *Foundations of computer science. 35th Annual symposium : Papers*. 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, USA). Ed. by S. Goldwasser. Institute of Electrical and Electronics Engineers. Piscataway: IEEE Press, 1994, pp. 124–134.

[13] F. Arute et al. 'Quantum supremacy using a programmable superconducting processor'. eng. *Nature* 574.7779 (2019), pp. 505–510. eprint: 31645734.

[14] A. Bogdanov et al. 'Biclique Cryptanalysis of the Full AES'. In: *Advances in cryptology - ASIACRYPT 2011. 17th International Conference on the Theory and Application of Cryptology and Information Security* (Seoul (South Korea), 2011). Ed. by D. H. Lee et al. Lecture notes in computer science 7073. Springer, 2011, pp. 344–371.

[15] L. K. Grover. 'A fast quantum mechanical algorithm for database search'. In: *Proceedings of the twenty-eighth annual ACM symposium on the theory of computing* (Philadelphia, PA (United States), 1996). Ed. by G. L. Miller. ACM. Special Interest Group for Algorithms and Computation Theory. New York, New York, USA: ACM Press, 1996, pp. 212–219.

[16] C. E. Shannon. 'Communication Theory of Secrecy Systems*'. *Bell System Technical Journal* 28.4 (1949), pp. 656–715.

[17] F. Miller. *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. C. M. Cornwell, 1882.

[18] S. Skorobogatov. 'Data Remanence in Flash Memory Devices'. In: *Cryptographic Hardware and Embedded Systems CHES 2005 00. 7th International Workshop* (Edinburgh (United Kingdom), 2005). Ed. by J. R. Rao et al. Lecture notes in computer science 3659. Berlin and Heidelberg: Springer-Verlag Berlin Heidelberg, 2005, pp. 339–353.

[19] C. H. Bennett et al. 'Quantum cryptography: Public key distribution and coin tossing'. In: *International Conference on Computer System and Signal Processing, IEEE, 1984*. 1984, pp. 175–179.

[20] G. C. Ghirardi et al. 'Quantum mechanics and faster-than-light communication: Methodological considerations'. en. *Il Nuovo Cimento B (1971-1996)* 78.1 (1983), pp. 9–20.

[21] W. K. Wootters et al. 'A single quantum cannot be cloned'. *Nature* 299.5886 (1982), pp. 802–803.

[22] W. Heisenberg. 'ber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik'. *Zeitschrift fr Physik* 43.3-4 (1927), pp. 172–198.

[23] C. Doescher et al. *An introduction to quantum coin-tossing*. LaTeX2e, 13 pages, 1 figure. 2002.

[24] A. Kent. 'Unconditionally Secure Bit Commitment'. *Phys. Rev. Lett.* 83.7 (1999), pp. 1447–1450.

[25] D. Mayers. 'Unconditionally Secure Quantum Bit Commitment is Impossible'. *Physical Review Letters* 78.17 (1997), pp. 3414–3417.

[26] H.-K. Lo et al. 'Why quantum bit commitment and ideal quantum coin tossing are impossible'. *Physica D: Nonlinear Phenomena* 120.1-2 (1998), pp. 177–187.

[27] A. Tajima et al. 'Quantum key distribution network for multiple applications'. en. *Quantum Science and Technology* 2.3 (2017), p. 034003.

[28] K. Inoue et al. 'Differential Phase Shift Quantum Key Distribution'. en. *Physical Review Letters* 89.3 (2002), p. 037902.

[29] C. H. Bennett. 'Quantum cryptography using any two nonorthogonal states'. *Physical Review Letters* 68.21 (1992), p. 3121.

[30] B. Huttner et al. 'Quantum cryptography with coherent states'. *Physical Review A* 51.3 (1995), p. 1863.

[31] H.-K. Lo et al. 'Decoy State Quantum Key Distribution'. en. *Physical Review Letters* 94.23 (2005), p. 230504.

[32] M. Lucamarini et al. 'Efficient decoy-state quantum key distribution with quantified security'. en. *Optics Express* 21.21 (2013), p. 24550.

[33] A. K. Ekert. 'Quantum cryptography based on Bell's theorem'. *Physical Review Letters* 67.6 (1991), p. 661.

[34] M. Lucamarini et al. 'Overcoming the rate–distance limit of quantum key distribution without quantum repeaters'. En. *Nature* 557.7705 (2018), p. 400.

[35] Z. L. Yuan et al. 'Avoiding the blinding attack in QKD'. En. *Nature photonics* 4.12 (2010), p. 800.

[36] N. Jain et al. 'Attacks on practical quantum key distribution systems and how to prevent them'. *arXiv preprint arXiv:1512.07990* (2015).

[37] A. Koehler-Sidki et al. 'Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution'. en. *Physical Review Applied* 9.4 (2018).

[38] H.-K. Lo et al. 'Measurement-Device-Independent Quantum Key Distribution'. en. *Physical Review Letters* 108.13 (2012).

[39] V. R. R. Valivarthi et al. 'Measurement Device Independent Quantum Key Distribution with id210 Detectors' (2014).

[40] Y.-H. Zhou et al. 'Making the decoy-state measurement-device-independent quantum key distribution practically useful'. en. *Physical Review A* 93.4 (2016).

[41] S. Pirandola et al. 'Fundamental limits of repeaterless quantum communications'. eng. *Nature Communications* 8 (2017), p. 15043. eprint: 28443624.

[42] X. Ma et al. 'Phase-matching quantum key distribution'. *arXiv:1805.05538 [quant-ph]* (2018).

[43] Z.-W. Yu et al. 'Sending-or-not-sending twin-field quantum key distribution in practice'. eng. *Scientific Reports* 9.1 (2019), p. 3080. eprint: 30816159.

[44] M. Curty et al. 'Simple security proof of twin-field type quantum key distribution protocol'. *npj Quantum Information* 5.1 (2019), p. 1023.

[45] M. Minder et al. 'Experimental quantum key distribution beyond the repeaterless secret key capacity'. en. *Nature Photonics* 13.5 (2019), pp. 334–338.

[46] J.-P. Chen et al. *Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km*. 17 pages, 10 figures and 8 tables. 2019.

[47] K. Inoue et al. 'Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack'. *Physical Review A* 71.4 (2005), p. 042305.

[48] J. Wabnig et al. 'Demonstration of free-space reference frame independent quantum key distribution'. *New Journal of Physics* 15.7 (2017), p. 073001.

[49] R. J. Hughes et al. 'Practical free-space quantum key distribution over 10 km in daylight and at night'. *New Journal of Physics* 4.1 (2002), p. 43.

[50] C. Liorni et al. 'Satellite-based links for quantum key distribution: beam effects and weather dependence'. en. *New Journal of Physics* 21.9 (2019), p. 093055.

[51] K. A. Patel et al. 'Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks'. *Applied Physics Letters* 104.5 (2014), p. 051123.

[52] L.-J. Wang et al. 'Long-distance copropagation of quantum key distribution and terabit classical optical data channels'. *Phys. Rev. A* 95.1 (2017), p. 413.

[53] A. J. Shields. 'Semiconductor quantum light sources'. *Nature photonics* 1.4 (2007), pp. 215–223.

[54] F. Hargart et al. 'Electrically driven quantum dot single-photon source at 2 GHz excitation repetition rate with ultra-low emission time jitter'. *Applied Physics Letters* 102.1 (2013), p. 011126.

[55] T. M. Babinec et al. 'A diamond nanowire single-photon source'. eng. *Nature nanotechnology* 5.3 (2010), pp. 195–199. eprint: 20154687.

[56] J. Volz et al. 'Observation of entanglement of a single photon with a trapped atom'. eng. *Physical Review Letters* 96.3 (2006), p. 030404. eprint: 16486671.

[57] X. He et al. 'Carbon nanotubes as emerging quantum-light sources'. eng. *Nature materials* 17.8 (2018), pp. 663–670. eprint: 29915427.

[58] N. Lütkenhaus et al. 'Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack'. *New Journal of Physics* 4 (2002), p. 44.

[59] D. Gottesman et al. 'Security of Quantum Key Distribution with Imperfect Devices'. *Quantum Info. Comput.* 4.5 (2004), pp. 325–360.

[60] N. Lütkenhaus. 'Security against individual attacks for realistic quantum key distribution'. *Physical Review A* 61.5 (2000), p. 052304.

[61] G. Brassard et al. 'Limitations on Practical Quantum Cryptography'. *Physical Review Letters* 85.6 (2000), pp. 1330–1333.

[62] L. Lydersen et al. 'Hacking commercial quantum cryptography systems by tailored bright illumination'. *Nature Photonics* 4.10 (2010), pp. 686–689.

[63] C. Wiechers et al. 'After-gate attack on a quantum cryptosystem'. *Quantum Info. Comput.* 13.1 (2011), p. 013043.

[64] A. Koehler-Sidki et al. 'Intrinsic mitigation of the after-gate attack in quantum key distribution through fast-gated delayed detection'. *Physical Review Applied* 12.2 (2019).

[65] C. H. Bennett et al. 'Experimental quantum cryptography'. *Journal of Cryptology* 5.1 (1992), pp. 3–28.

[66] S.-K. Liao et al. 'Long-distance free-space quantum key distribution in daylight towards inter-satellite communication'. *Nat Photon* 11.8 (2017), pp. 509–513.

[67] Z.-F. Han et al. 'Stability of phase-modulated quantum key distribution systems'. en. *Applied Physics Letters* 86.22 (2005), p. 221103.

[68] R. S. Tucker. 'High-speed modulation of semiconductor lasers'. *IEEE Transactions on Electron Devices* 32.12 (1985), pp. 2572–2584.

[69] A. E. Amari et al. 'Statistical Prediction and Experimental Verification of Concatenations of Fiber Optic Components with Polarization Dependent Loss'. EN. *Journal of Lightwave Technology* 16.3 (1998), p. 332.

[70] E. L. Wooten et al. 'A review of lithium niobate modulators for fiber-optic communications systems'. *IEEE Journal of Selected Topics in Quantum Electronics* 6.1 (2000), pp. 69–82.

[71] R. S. Weis et al. 'Lithium niobate: summary of physical properties and crystal structure'. *Applied Physics A* 37.4 (1985), pp. 191–203.

[72] G. Brassard et al. 'Secret-Key Reconciliation by Public Discussion'. In: *Advances in Cryptology – EUROCRYPT '93. Workshop on the Theory and Application of Cryptographic Techniques* (Lofthus (Norway), 1993). Ed. by T. Helleseth. Lecture notes in computer science 765. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 1994, pp. 410–423.

[73] J. Martinez-Mateo et al. 'Key Reconciliation for High Performance Quantum Key Distribution'. en. *Scientific Reports* 3.1 (2013), pp. 1–6.

[74] P. Jouguet et al. 'High performance error correction for quantum key distribution using polar codes'. *Quantum Information & Computation* 14.3-4 (2014).

[75] C. H. Bennett et al. 'Privacy Amplification by Public Discussion'. *SIAM Journal on Computing* 17.2 (1988), pp. 210–229.

[76] C. H. Bennett et al. 'Generalized privacy amplification'. *IEEE Transactions on Information Theory* 41.6 (1995), pp. 1915–1923.

[77] N. Gisin et al. 'Quantum cryptography'. *Rev. Mod. Phys.* 74.1 (2002), pp. 145–195.

[78] V. Scarani et al. 'Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing'. en. *Physical Review Letters* 100.20 (2008).

[79] R. Y. Q. Cai et al. 'Finite-key analysis for practical implementations of quantum key distribution'. *New Journal of Physics* 11.4 (2009), p. 045024.

[80] M. Tomamichel et al. 'Tight finite-key analysis for quantum cryptography'. *Nature Communications* 3 (2012), p. 634.

[81] Z. Yuan et al. '10-Mb/s Quantum Key Distribution'. EN. *Journal of Lightwave Technology* 36.16 (2018), pp. 3427–3433.

[82] A. Boaron et al. 'Secure quantum key distribution over 421 km of optical fiber'. *arXiv:1807.03222 [quant-ph]* (2018).

[83] B. Korzh et al. 'Provably secure and practical quantum key distribution over 307 km of optical fibre'. *Nature photonics* 9.3 (2015), pp. 163–168.

[84] J.-P. Chen et al. 'Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km'. *Physical Review Letters* 124.7 (2020), p. 070501.

[85] R. Bedington et al. 'Progress in satellite quantum key distribution'. en. *npj Quantum Information* 3.1 (2017).

[86] S.-K. Liao et al. 'Satellite-to-ground quantum key distribution'. *Nature* 549.7670 (2017), pp. 43–47.

[87] S.-K. Liao et al. 'Satellite-Relayed Intercontinental Quantum Network'. eng. *Physical Review Letters* 120.3 (2018), p. 030501. eprint: 29400544.

[88] Y.-C. Zhang et al. *Long-distance continuous-variable quantum key distribution over 202.81 km fiber*. 7 pages, 3 figures. 2020.

[89] C. Elliott et al. 'Current status of the DARPA Quantum Network'. *arXiv:quant-ph/0503058* (2005).

[90] M. Peev et al. 'The SECOQC quantum key distribution network in Vienna'. *New Journal of Physics* 11.7 (2009), p. 075001.

[91] A. Mirza et al. 'Realizing long-term quantum cryptography'. EN. *JOSA B* 27.6 (2010), A185–A188.

[92] D. Stucki et al. 'Performance of the SwissQuantum network over 21 months'. In: *International Society for Optics and Photonics*. Vol. 8189. oct,

[93] M. Sasaki et al. 'Field test of quantum key distribution in the Tokyo QKD Network'. en. *Optics Express* 19.11 (2011), p. 10387.

[94] S. Wang et al. 'Field and long-term demonstration of a wide area quantum key distribution network'. EN. *Optics Express* 22.18 (2014), pp. 21739–21756.

[95] A. Wonfor et al. 'Field trial of a QKD and high-speed classical data hybrid metropolitan network (Conference Presentation)'. In: *SPIE, Broadband Access Communication Technologies XII*. Ed. by B. B. Dingel et al. mar, San Francisco: SPIE, 2018, p. 1055907.

[96] P. Sibson et al. 'Chip-based quantum key distribution'. *Nature Communications* 8 (2017), p. 13984.

[97] P. Sibson et al. 'Integrated silicon photonics for high-speed quantum key distribution'. *Optica* 4.2 (2017), pp. 172–177.

[98] D. Bunandar et al. 'Metropolitan quantum key distribution with silicon photonics'. *Physical Review X* 8.2 (2018), p. 021009.

[99] T. K. Paraïso et al. 'A modulator-free quantum key distribution transmitter chip'. *npj Quantum Information* 5.1 (2019), p. 42.

[100] J. L. Duligall et al. 'Low cost and compact quantum key distribution'. *New Journal of Physics* 8.10 (2006), p. 249.

[101] H. Chun et al. 'Handheld free space quantum key distribution with dynamic motion compensation'. EN. *Optics Express* 25.6 (2017), pp. 6784–6795.

[102] G. Mélen et al. 'Handheld Quantum Key Distribution'. EN. In: *Quantum Information and Measurement (QIM) 2017, QT6A.57*. apr, Optical Society of America, 2017.

[103] H. Bechmann-Pasquinucci et al. 'Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography'. *Phys. Rev. A* 59.6 (1999), pp. 4238–4248.

[104] Y. Zhao et al. 'Experimental quantum key distribution with active phase randomization'. *Applied Physics Letters* 90.4 (2007), pp. 656–661.

[105] H.-K. Lo et al. 'Phase randomization improves the security of quantum key distribution'. *arXiv preprint quant-ph/0504209* (2005).

[106] H.-K. Lo et al. 'Security of quantum key distribution using weak coherent states with nonrandom phases'. *Quantum Information & Computation* 8 (2007), pp. 431–458.

[107] W.-Y. Hwang. 'Quantum Key Distribution with High Loss: Toward Global Secure Communication'. en. *Physical Review Letters* 91.5 (2003), p. 057901.

[108] C. C. W. Lim et al. 'Concise security bounds for practical decoy-state quantum key distribution'. en. *Physical Review A* 89.2 (2014), p. 022307.

[109] Y. Zhao et al. 'Experimental Quantum Key Distribution with Decoy States'. en. *Physical Review Letters* 96.7 (2006).

[110] X.-B. Wang. 'Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography'. en. *Physical Review Letters* 94.23 (2005), p. 230503.

[111] X. Ma et al. 'Practical decoy state for quantum key distribution'. *Physical Review A* 72.1 (2005), p. 012326.

[112] D. Rusca et al. 'Finite-key analysis on the 1-decoy state QKD protocol'. *Applied Physics Letters* 112.17 (2018), p. 171104.

[113] K. Inoue et al. 'Differential-phase-shift quantum key distribution using coherent light'. en. *Physical Review A* 68.2 (2003), p. 022317.

[114] A. Mizutani et al. 'Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity'. *arXiv:1705.00171* (2017).

[115] A. Mizutani et al. 'Quantum key distribution with simply characterized light sources'. en. *npj Quantum Information* 5.1 (2019), pp. 1–7.

[116] T. Moroder et al. 'Security of Distributed-Phase-Reference Quantum Key Distribution'. en. *Physical Review Letters* 109.26 (2012).

[117] K. Inoue. 'Differential Phase-Shift Quantum Key Distribution Systems'. *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 109–115.

[118] D. Stucki et al. 'Fast and simple one-way quantum key distribution'. *Applied Physics Letters* 87.19 (2005), p. 194108.

[119] J. González-Payo et al. *Upper security bounds for coherent-one-way quantum key distribution*. 2020.

[120] R. Going et al. 'InP-based Coherent PICs for 100 Gbaud Operation'. In: *OSA Advanced Photonics Congress (AP) 2019*. Signal Processing in Photonic Communications (Burlingame, CA (United States)). Washington, D.C.: OSA, 2019.

[121] T. Barwicz et al. 'Silicon photonics for compact, energy-efficient interconnects [Invited]'. *Journal of Optical Networking* 6.1 (2007), p. 63.

[122] A. M. Streltsov et al. 'Study of femtosecond-laser-written waveguides in glasses'. EN. *JOSA B* 19.10 (2002), pp. 2496–2504.

[123] G. Della Valle et al. 'Micromachining of photonic devices by femtosecond laser pulses'. en. *Journal of Optics A: Pure and Applied Optics* 11.1 (2008), p. 013001.

[124] K. Sugioka et al. 'Femtosecond laser three-dimensional micro- and nanofabrication'. *Applied Physics Reviews* 1.4 (2014), p. 041303.

[125] W. Bogaerts et al. 'Basic structures for photonic integrated circuits in Silicon-on-insulator'. eng. *Optics Express* 12.8 (2004), pp. 1583–1591. eprint: 19474984.

[126] A. Politi et al. 'Integrated Quantum Photonics'. *IEEE Journal of Selected Topics in Quantum Electronics* 15.6 (2009), pp. 1673–1684.

[127] J. Soole et al. 'Polarisation-independent InP arrayed waveguide filter using square cross-section waveguides'. *Electronics Letters* 32.4 (1996), p. 323.

[128] R. C. Alferness. 'Efficient waveguide electro–optic TE-TM mode converter/wavelength filter'. *Applied Physics Letters* 36.7 (1980), p. 513.

[129] R. A. Soref et al. 'Single-crystal silicon: a new material for 1.3 and 1.6 µm integrated-optical components'. *Electronics Letters* 21.21 (1985), p. 953.

[130] B. Schüppert et al. 'Optical channel waveguides in silicon diffused from GeSi alloy'. *Electronics Letters* 25.22 (1989), p. 1500.

[131] L. Liao et al. 'High speed silicon Mach-Zehnder modulator'. *Optics Express* 13.8 (2005), p. 3129.

[132] D. Marris-Morini et al. 'Low loss 40 Gbit/s silicon modulator based on interleaved junctions and fabricated on 300 mm SOI wafers'. eng. *Optics Express* 21.19 (2013), pp. 22471–22475. eprint: 24104136.

[133] D. Liang et al. 'Hybrid Integrated Platforms for Silicon Photonics'. *Materials* 3.3 (2010), pp. 1782–1802.

[134] H. Rong et al. 'A continuous-wave Raman silicon laser'. eng. *Nature* 433.7027 (2005), pp. 725–728. eprint: 15716948.

[135] H. Rong et al. 'Low-threshold continuous-wave Raman silicon laser'. *Nat Photon* 1.4 (2007), pp. 232–237.

[136] H. Rong et al. 'A cascaded silicon Raman laser'. *Nat Photon* 2.3 (2008), pp. 170–174.

[137] G. K. Celler et al. 'Frontiers of silicon-on-insulator'. *Journal of Applied Physics* 93.9 (2003), pp. 4955–4978.

[138] J. Klamkin et al. 'Indium Phosphide Photonic Integrated Circuits: Technology and Applications'. In: *2018 IEEE BiCMOS and Compound 2018*, pp. 8–13.

[139] Y. Kawamura et al. 'Monolithic integration of InGaAs/InP DFB lasers and InGaAs/InAlAs MQW optical modulators'. *Electronics Letters* 22.5 (1986), p. 242.

[140] F. Kish et al. 'System-on-Chip Photonic Integrated Circuits'. *IEEE Journal of Selected Topics in Quantum Electronics* 24.1 (2018), pp. 1–20.

[141] R. Nagarajan et al. 'Large-scale photonic integrated circuits'. *IEEE Journal of Selected Topics in Quantum Electronics* 11.1 (2005), pp. 50–65.

[142] J. Summers et al. '40 Channels × 57 Gb/s monolithically integrated InP-based coherent photonic transmitter'. In: *The European Conference on Optical Communication (ECOC)* (Cannes (France)). [Palaiseau, France]: [Systematic], 2014, pp. 1–3.

[143] C. Cremer et al. 'Bragg gratings on InGaAsP/InP waveguides as polarization independent optical filters'. *Journal of Lightwave Technology* 7.11 (1989), pp. 1641–1645.

[144] C. Bornholdt et al. 'Waveguide-integrated pin photodiode on InP'. *Electronics Letters* 23.1 (1987), pp. 2–4.

[145] P. Albrecht et al. 'TE/TM mode splitters on InGaAsP/InP'. *IEEE Photonics Technology Letters* 2.2 (1990), pp. 114–115.

[146] M. Smit et al. 'An introduction to InP-based generic integration technology'. *Semiconductor Science and Technology* 29.8 (2014), p. 083001.

[147] G. Serafino et al. 'Photonic approach for on-board and ground radars in automotive applications'. *IET Radar, Sonar & Navigation* 12.10 (2018), pp. 1179–1186.

[148] V. M. N. Passaro et al. 'Recent advances in integrated photonic sensors'. eng. *Sensors (Basel, Switzerland)* 12.11 (2012), pp. 15558–15598. eprint: 23202223.

[149] T. Mappes et al. 'Integrated photonic lab-on-chip systems for biomedical applications'. In: *Micro-Optics 2010*. SPIE Photonics Europe (Brussels, Belgium). Ed. by H. Thienpont et al. SPIE Proceedings. SPIE, 2010, 77160R.

[150] S. Germer et al. 'Si-based light emitter in an integrated photonic circuit for smart biosensor applications'. In: *Integrated Photonics: Materials, Devices, and Applications II*. SPIE Microtechnologies (Grenoble, France, 2013). Ed. by J.-M. Fédéli et al. SPIE Proceedings. SPIE, 2013, p. 876710.

[151] T. Vo-Dinh. *Biomedical Photonics Handbook: Biomedical Diagnostics*. CRC Press, 2014.

[152] N. Pleros et al. 'Optical Static RAM Cell'. *IEEE Photonics Technology Letters* 21.2 (2009), pp. 73–75.

[153] L. Chen et al. 'Integrated GHz silicon photonic interconnect with micrometer-scale modulators and detectors'. eng. *Optics Express* 17.17 (2009), pp. 15248–15256. eprint: 19688003.

[154] J. Sun et al. 'Large-scale nanophotonic phased array'. en. *Nature* 493.7431 (2013), pp. 195–199.

[155] G. E. Moore. 'Cramming more components onto integrated circuits'. *Electronics* 38.8 (1965), p. 114.

[156] J. Wang et al. 'Integrated photonic quantum technologies'. en. *Nature Photonics* (2019), pp. 1–12.

[157] A. Politi et al. 'Shor's quantum factoring algorithm on a photonic chip'. eng. *Science (New York, N.Y.)* 325.5945 (2009), p. 1221. eprint: 19729649.

[158] A. Peruzzo et al. 'Quantum walks of correlated photons'. eng. *Science (New York, N.Y.)* 329.5998 (2010), pp. 1500–1503. eprint: 20847264.

[159] A. Crespi et al. 'Integrated multimode interferometers with arbitrary designs for photonic boson sampling'. *Nat Photon* 7.7 (2013), pp. 545–549.

[160] A. Crespi et al. 'Anderson localization of entangled photons in an integrated quantum walk'. *Nat Photon* 7.4 (2013), pp. 322–328.

[161] L. Sansoni et al. 'Two-Particle Bosonic-Fermionic Quantum Walk via Integrated Photonics'. *Physical Review Letters* 108.1 (2012), p. 010502.

[162] F. Caruso et al. 'Fast escape of a quantum walker from an integrated photonic maze'. eng. *Nature Communications* 7 (2016), p. 11682. eprint: 27248707.

[163] S. Paesani et al. 'Experimental Bayesian Quantum Phase Estimation on a Silicon Photonic Chip'. *Physical Review Letters* 118.10 (2017), p. 100503.

[164] J. B. Spring et al. 'Chip-based array of near-identical, pure, heralded single-photon sources'. *Optica* 4.1 (2017), p. 90.

[165] S. Paesani et al. 'Generation and sampling of quantum states of light in a silicon chip'. *Nature Physics* 15.9 (2019), pp. 925–929.

[166] W. H. P. Pernice et al. 'High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits'. eng. *Nature Communications* 3 (2012), p. 1325. eprint: 23271658.

[167] R. A. Taylor et al. 'Comprehensive system-level optimization of thermoelectric devices for electronic cooling applications'. *IEEE Transactions on Components and Packaging Technologies* 31.1 (2008), pp. 23–31.

[168] J. C. A. Peltier. 'Nouvelles expériences sur la caloricité des courans électriques'. *Annales de Chimie et de Physique (in French)* 56 (1834), pp. 371–386.

[169] M. P. Gallaher et al. *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry*. 2004.

[170] B. Korzh et al. 'A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator'. en. *Optics Express* 21.17 (2013), p. 19579.

[171] ETSI, ed. *Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment*. Version 1.1.4. 28th Feb. 2019.

[172] P. J. Winzer et al. 'Advanced Optical Modulation Formats'. *Proceedings of the IEEE* 94.5 (2006), pp. 952–985.

[173] I. Lucio-Martinez et al. 'Proof-of-concept of real-world quantum key distribution with quantum frames'. en. *New Journal of Physics* 11.9 (2009), p. 095001.

[174] M. M. Howerton et al. 'Fully packaged, broad-band LiNbO 3 modulator with low drive voltage'. *IEEE Photonics Technology Letters* 12.7 (2000), pp. 792–794.

[175] R. Ding et al. 'Sub-Volt Silicon-Organic Electro-optic Modulator With 500 MHz Bandwidth'. *Journal of Lightwave Technology* 29.8 (2011), pp. 1112–1117.

[176] M. Shirasaki et al. 'Fibre transmission properties of optical pulses produced through direct phase modulation of DFB laser diode'. *Electronics Letters* 24.8 (1988), p. 486.

[177] V. Scarani et al. 'The black paper of quantum cryptography: Real implementation problems'. *Theoretical Computer Science* 560 (2014), pp. 27–32.

[178] Z. L. Yuan et al. 'Directly Phase-Modulated Light Source'. en. *Physical Review X* 6.3 (2016), p. 031044.

[179] C. J. Buczek et al. 'Laser injection locking'. *Proceedings of the IEEE* 61.10 (1973), pp. 1411–1431.

[180] J. K. Alexander et al. 'On-Chip Investigation of Phase Noise in Monolithically Integrated Gain-Switched Lasers'. *IEEE Photonics Technology Letters* 29.9 (2017), pp. 731–734.

[181] I. Fatadin et al. 'Numerical Simulation of Intensity and Phase Noise From Extracted Parameters for CW DFB Lasers'. *IEEE Journal of Quantum Electronics* 42.9 (2006), pp. 934–941.

[182] K. Y. Lau. 'Gain switching of semiconductor injection lasers'. *Applied Physics Letters* 52.4 (1988), pp. 257–259.

[183] G. L. Roberts et al. 'Modulator-Free Coherent-One-Way Quantum Key Distribution'. en. *Laser & Photonics Reviews* 11.4 (2017), p. 1700067.

[184] G. L. Roberts et al. 'Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution'. en. *Applied Physics Letters* 111.26 (2017), p. 261106.

[185] G. L. Roberts et al. 'Experimental measurement-device-independent quantum digital signatures'. en. *Nature Communications* 8.1 (2017), p. 1098.

[186] G. L. Roberts et al. 'Patterning-effect-free intensity modulator for secure decoy-state quantum key distribution'. *arXiv:1807.07414 [quant-ph]* (2018).

[187] C. M. Natarajan et al. 'Superconducting nanowire single-photon detectors: physics and applications'. *Superconductor Science and Technology* 25.6 (2012), p. 063001.

[188] F. M. Soares et al. 'InP-Based Foundry PICs for Optical Interconnects'. *Applied Sciences* 9.8 (2019), p. 1588.

[189] K. Cooney et al. 'Analysis of multimode interferometers'. eng. *Optics Express* 24.20 (2016), pp. 22481–22515. eprint: 27828321.

[190] L. B. Soldano et al. 'Optical multi-mode interference devices based on self-imaging: principles and applications'. *Journal of Lightwave Technology* 13.4 (1995), pp. 615–627.

[191] L. A. Coldren et al. *Diode lasers and photonic integrated circuits*. Vol. 218. John Wiley & Sons, 2012.

[192] Z. L. Yuan et al. 'High speed single photon detection in the near infrared'. *Applied Physics Letters* 91.4 (2007), p. 041114.

[193] L. C. Comandar et al. 'Room temperature single-photon detectors for high bit rate quantum key distribution'. *Applied Physics Letters* 104.2 (2014), p. 021101.

[194] D. A. B. Miller et al. 'Band-Edge Electroabsorption in Quantum Well Structures: The Quantum-Confined Stark Effect'. *Physical Review Letters* 53.22 (1984), p. 2173.

[195] S. G. Carter et al. 'Quantum Coherence in an Optical Modulator'. *Science* 310.5748 (2005), pp. 651–653.

[196] I. B. Akca et al. 'Electro-optic and electro-absorption characterization of InAs quantum dot waveguides'. EN. *Optics Express* 16.5 (2008), pp. 3439–3444.

[197] N. Le Thomas et al. 'Widely tunable light-emitting diodes by Stark effect in forward bias'. *Applied Physics Letters* 81.9 (2002), pp. 1582–1584.

[198] T. Roger et al. 'Real-time interferometric quantum random number generation on chip'. *Journal of the Optical Society of America B* 36.3 (2019), B137.

[199] C. Abellan et al. 'Quantum entropy source on an InP photonic integrated circuit for random number generation'. *Optica* 3.9 (2016), p. 989.

[200] F. James. 'A review of pseudorandom number generators'. *Computer Physics Communications* 60.3 (1990), pp. 329–344.

[201] Ferrenberg et al. 'Monte Carlo simulations: Hidden errors from "good" random number generators'. eng. *Physical Review Letters* 69.23 (1992), pp. 3382–3384. eprint: 10046804.

[202] J. Kelsey et al. 'Cryptanalytic attacks on pseudorandom number generators'. In: *Fast Software Encryption*. Springer, 1998, pp. 168–188.

[203] M. Matsumoto et al. 'Pseudorandom Number Generation: Impossibility and Compromise'. *J. UCS* 12.6 (2006), pp. 672–690.

[204] P. Hellekalek. 'Good random number generators are (not so) easy to find'. *Mathematics and Computers in Simulation* 46.5-6 (1998), pp. 485–505.

[205] T. Jennewein et al. 'A fast and compact quantum random number generator'. *Review of Scientific Instruments* 71.4 (2000), pp. 1675–1680.

[206] A. Stefanov et al. 'Optical quantum random number generator'. *Journal of Modern Optics* 47.4 (2000), pp. 595–598.

[207] M. Jofre et al. 'True random numbers from amplified quantum vacuum'. eng. *Optics Express* 19.21 (2011), pp. 20665–20672. eprint: 21997077.

[208] Z. L. Yuan et al. 'Robust random number generation using steady-state emission of gain-switched laser diodes'. *Applied Physics Letters* 104.26 (2014), p. 261112.

[209] C. Abellán et al. 'Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode'. eng. *Optics Express* 22.2 (2014), pp. 1645–1654. eprint: 24515170.

[210] P. Vasil'ev. *Ultrafast diode lasers : fundamentals and applications*. Boston: Artech House, 1995.

[211] S.-H. Sun et al. 'Experimental study of a quantum random-number generator based on two independent lasers'. *Physical Review A* 96.6 (2017).

[212] A. Oppenheim. *Signals and systems*. Englewood Cliffs N.J: Prentice-Hall, 1983.

[213] Y. Mansour et al. 'The computational complexity of universal hashing'. *Theoretical Computer Science* 107.1 (1993), pp. 121–133.

[214] A. Rukhin et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Booz-Allen and Hamilton Inc Mclean Va, 2001.

[215] O. Kahl et al. 'Waveguide integrated superconducting single-photon detectors with high internal quantum efficiency at telecom wavelengths'. *Scientific Reports* 5 (2015), p. 10941.

[216] V. B. Verma et al. 'High-efficiency superconducting nanowire single-photon detectors fabricated from MoSi thin-films'. en. *Optics Express* 23.26 (2015), p. 33792.

[217] A. D. Semenov et al. 'Quantum detection by current carrying superconducting film'. *Physica C: Superconductivity* 351.4 (2001), pp. 349–356.