Quantum Secured Communications with Integrated Photonics

Philip Sibson

Department of Electrical and Electronic Engineering

August 2016

A thesis submitted to the University of Bristol in accordance with the requirements for the degree of Doctor of Philosophy in the Faculty of Engineering, Department of Electrical and Electronic Engineering.

Word Count: $\approx 41,000$

Abstract

Quantum technologies are rapidly developing and have the potential to revolutionise the fields of computing and telecommunications. They have major implications for the security of many of our conventional cryptographic techniques which are known to be insecure against a quantum computer. Therefore, improvement in secure transmission of information is an urgent practical need for governments, corporations and individuals.

Quantum key distribution (QKD) promises security based on the laws of physics and has rapidly grown from proof-of-concept to robust demonstrations and even deployment of commercial systems. Despite these advances, QKD has not been widely adopted, and practical large-scale deployment will likely require integrated chip-based devices for improved performance, miniaturisation and enhanced functionality, fully integrated into classical communication networks.

Integrated photonics provides a stable, compact, and robust platform to implement complex photonic circuits amenable to mass-manufacture, and therefore provides a compelling technology for optical quantum information devices. The appeal of this platform has led to integrated photonic technologies increasingly being deployed in the development of practical QKD systems. Demonstrations include integrated "client" chips for Reference-Frame-Independent QKD, planar waveguide components in transmitters and receivers, and reconfigurability with discrete integrated devices.

In this thesis we demonstrate the development of integrated photonics for quantum secured communications. Ultimately, integrated photonics will allow the manufacture of single quantum communications chips with electronic and photonic processing on a monolithic device. This will enable further multiplexing and complexity of operation. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secure communications.

Acknowledgements

I would like to thank the support and supervision of Prof. Mark Thompson, Prof. John Rarity FRS, Prof. Jeremy O'Brien and (not a professor) Dr. Chris Erven. I'm extremely appreciative of the time I have spent in the research environment you have fostered.

I would further like to acknowledge the enormous contribution from the Centre for Quantum Photonics group at large — the admin and operations staff, the academics, friends and colleagues (both past and present) that are all too numerous to mention. It has been a unforgettable privilege to work with all of you. Specific mentions to Dylan Mahler, Jorge Barreto, and Chris Erven for your helpful comments and proof-reading of this thesis.

I'm indebted to my family for their love and support through the years, and finally, I'll thank my long-suffering better half for the many years of happiness we've shared, despite my countless inadequacies.

Author's Declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: .....

DATE: .....

List of Publications

Journals

P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M.G. Tanner, C.M. Natarajan, R.H. Hadfield, J.L. O'Brien, and M.G. Thompson, "Chip-based Quantum Key Distribution," *arXiv:1509.00768*, Sept. 2015 *to appear in Nature Communications*

A. Aguado, E. Hugues-Salas, P.A. Haigh, J. Marhuenda, A.B. Price, P. Sibson, J.E. Kennard, C. Erven, J.G. Rarity, M.G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources," *arXiv:1604.05861*, Apr. 2016. *to appear in Journal of Lightwave Technology*

P. Sibson, J.E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, M. G. Thompson. "Integrated Silicon Photonics for High Speed Quantum Key Distribution," *arXiv:1612.07236*, Dec 2016 *to appear in Optica*

P. Sibson, A.B. Price, C. Erven, J.L. O'Brien, M.G. Thompson. "Wavelength-Division-Multiplexed Quantum-Key-Distribution with Integrated Photonics," *in preparation*

F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J.E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M.G. Thompson, J.C.F. Matthews "An On-chip Homodyne Detector for Measuring Quantum States and Generating Random Numbers," *arXiv:1612.04676*, Dec. 2016 *submitted*

E. Hugues-Salas, P.A. Haigh, J. Marhuenda, A. Aguado, A.B. Price, J.E. Kennard, P. Sibson, C. Erven, J.G. Rarity, M.G. Thompson, R. Nejabati and D. Simeonidou. "Char-

acterisation of Quantum Key Distribution over 7-Core Multicore Fibre with Adaptive Power and Filtering" *submitted*

Patents

UK Patent Application: GB2536248 QKD device

UK Patent Application: GB1615032.8 Optical interferometer apparatus and method

Conferences

"Wavelength-Division-Multiplexed QKD with Integrated Photonics" *QCrypt 16* (Washington DC, USA) *Oral Presentation* Sept. 2016

"Integrated Silicon Photonics for Quantum Key Distribution" *QCrypt 16* (Washington DC, USA) *Oral Presentation* Sept. 2016

"Towards the Deployment of Quantum Key Distribution Systems in a Software Defined Networking Environment" *QCrypt 16* (Washington DC, USA) *Poster* Sept. 2016

"Integrated Silicon Photonics for Quantum Key Distribution" *Photon 16* (Leeds, UK) *Oral Presentation - Given by J.E. Kennard* Sept. 2016

"Integrated Photonics for Quantum Key Distribution" *CLEO EU* (Munich, Germany) *Oral Presentation* June. 2015

"Integrated Quantum Photonic Devices" *Quantum Networks and Repeaters Workshop* (California, USA) *Invited talk with J.L. O'Brien* May. 2015

"Integrated Photonic Devices for QKD" *CLEO US* (California, USA) *Oral Presentation* May. 2015

"Integrated Photonics for Quantum Key Distribution" *QCrypt 13* (Waterloo, Canada) *Poster* Aug. 2013

Contents

List of Figures

Chapter 1

Introduction

Quantum technologies are rapidly developing and have the potential to revolutionise the fields of computing and telecommunications. They have major implications for the security of many of our conventional cryptographic techniques which are known to be insecure against a quantum computer [1]. Therefore, improvement in secure transmission of information is an urgent practical need for governments, corporations and individuals.

Quantum key distribution [1,2] (QKD) promises security based on the laws of physics and has rapidly grown from proof-of-concept to robust demonstrations [3–6] and even deployment of commercial systems [7–9]. Despite these advances, QKD has not been widely adopted, and practical large-scale deployment will likely require integrated chip-based devices for improved performance, miniaturisation and enhanced functionality, fully integrated into classical communication networks.

Integrated photonics provides a stable, compact, and robust platform to implement complex photonic circuits amenable to mass-manufacture, and therefore provides a compelling technology for optical quantum information devices [10]. The appeal of this platform has led to integrated photonic technologies increasingly being deployed in the development of practical QKD systems. Demonstrations include integrated "client" chips for Reference-Frame-Independent QKD [11], planar waveguide components in transmitters and receivers [12], and reconfigurability [4] with discrete integrated devices.

In this thesis we demonstrate the development of integrated photonics for quantum secured communications. Ultimately, integrated photonics will allow the manufacture

of single quantum communications chips with electronic and photonic processing on a monolithic device. This will enable further multiplexing and complexity of operation. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secure communications.

Thesis Outline We first introduce relevant **background** material in classical and modern cryptography, introducing the historical context and currently implemented techniques. Quantum information and quantum key distribution are then introduced, illustrating the threat of quantum technologies and the security gained. Finally integrated photonics are presented focussing on the photonic technologies for quantum key distribution including photon sources, photonic manipulation and detection.

We then report low error rate, GHz clocked **chip-to-chip QKD** operation of an InP transmitter chip and a SiO_xN_y receiver chip—monolithically integrated devices that use state-of-the-art components and manufacturing processes from the telecommunications industry. We use the reconfigurability of these devices to demonstrate three important QKD protocols—BB84, Coherent One Way (COW) and Differential Phase Shift (DPS)—with performance comparable to state-of-the-art. These devices, when combined with integrated single photon detectors, satisfy the requirements at each of the levels of future QKD networks—from point-of-use through to backbones—and open the way to operation in existing and emerging classical communication networks.

We further use an efficient decoy-state BB84 scheme with biased basis preparation and measurement to increase channel capacity. We then illustrate the benefits of miniaturisation and manufacturability of integrated photonics by demonstrating a proof-of-principle **WDM-QKD** link. Two InP transmitters operated at different wavelengths are combined on to the same optical fibre, and demultiplexed and decoded on a SiO_xN_y chip to demonstrate increased rate with limited increase of error.

Integrated photonics offers great potential for quantum communication devices in terms of complexity, robustness and scalability. **Silicon photonics** in particular is a leading platform for quantum photonic technologies, with further benefits of miniaturisation, cost-effective device manufacture and compatibility with CMOS microelectronics.

However, effective techniques for high-speed modulation of quantum states in standard silicon photonic platforms have been limited. Here we overcome this limitation and demonstrate high-speed low-error QKD modulation with silicon photonic devices combining slow thermo-optic DC biases and fast (10 GHz bandwidth) carrier-depletion modulation. We illustrate this approach with the preparation of time-bin encoded BB84 QKD states, implementations of polarisation encoded BB84 QKD, and Coherent-One-Way QKD.

Finally we show the use of integrated photonics based **quantum random number generators** required for quantum key distribution systems. In particular we use weak coherent sources of light generated in InP devices and single photon detectors in a number of configurations to generate unbiased quantum random numbers. We further improve upon this rate and the versatility of the devices by demonstrating an integrated homodyne detector systems to generate 1.03 Gbps of quantum random numbers passing a number of statistical random test suites.

Chapter 2

Background

2.1 Cryptography

Throughout the history of written communication, there have been methods devised to restrict the meaning of a message until it is in possession of the intended recipients. *Steganography* approaches this problem by hiding the existence of the message [13], where as *cryptography* is the practice of obscuring the meaning of a message by rendering the contents meaningless to those without the means to decode the message [14].

The field of cryptography provides privacy, authentication, and confidentiality to its users. This allows for the secure communication between different parties, and prohibits any unauthorised party to access the content of the message [15].

In many cryptography schemes, two parties ("Alice" the sender, and "Bob" the recipient) wish to communicate, with the content of the message remaining secret, in the presence of an adversary "Eve" (as illustrated in Figure 2.1).

2.1.1 Symmetric Key Cryptography

In symmetric cryptography Alice wishes to share a message (or plain text) by altering its contents with an encryption algorithm, taking inputs of message text and key, and outputting cipher text. This cipher text is then transmitted over the communications channel, which may be untrusted. If the cipher text is intercepted or overheard by the adversary (Eve), the message should not be recoverable. Only when the message is re-

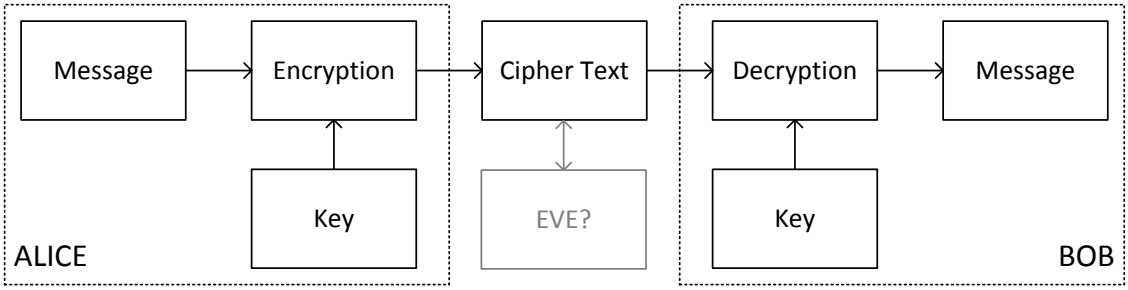

Figure 2.1: **Encryption:** The two parties, "Alice" and "Bob", communicate over a public channel but encrypt the message with a key to render the transmitted cipher text illegible to anyone other than the intended recipient.

ceived by the intended recipient (Bob), can the plain text be recovered and understood. Bob has the ability to reverse the encryption process (decrypting), using the same key that Alice had [16].

Mathematically this process can be described by representing the set of all plain text space as $\mathcal{M}$, the set of all cipher text space as $\mathcal{C}$, and a set of all key space as $\mathcal{K}$. The family of encryption functions are functions mapping plain text to cipher text:

$$\mathcal{E}_k \colon \mathcal{M} \to \mathcal{C} \quad \forall k \in \mathcal{K} \tag{2.1.1}$$

and the family of decryption functions map cipher text to plain text:

$$\mathcal{D}_k \colon \mathcal{C} \to \mathcal{M} \quad \forall k \in \mathcal{K} \tag{2.1.2}$$

such that decrypting the encrypted message reveals the initial plain text:

$$\mathcal{D}_k\left(\mathcal{E}_k\left(m\right)\right) = m \qquad \forall m \in \mathcal{M}, \quad \forall k \in \mathcal{K}\ . \tag{2.1.3}$$

With these definitions, all that is required for confidentiality is for Alice and Bob to agree on a secret key, k, over a "secure" channel. Alice then computes the cipher text, $c = \mathcal{E}_k\left(m\right)$ to send over an unsecured channel. Bob retrieves the plain-text by computing $m = \mathcal{D}_k\left(c\right)$.

Plain text message	**S**	**E**	**C**	**R**	**E**	**T**	**M**	**E**	**S**	**S**	**A**	**G**	**E**
Numerical Value	19	5	3	18	5	20	13	5	19	19	1	7	5
Add + 3	22	8	6	21	8	23	16	8	22	22	4	10	8
Cipher Text	**V**	**H**	**F**	**U**	**H**	**W**	**P**	**H**	**V**	**V**	**D**	**J**	**H**

Figure 2.2: **Caesar Cipher:** The plain text message is converted to a numerical value, and shifted by a pre-disclosed value (mod 26). This value is converted back to an alphabetical value. To decrypt the cipher text, it is shifted back by the pre-disclosed value. In this example the key is the numerical value, 3.

Caesar Cipher

An early example of such an encryption system is known as the *Caesar Cipher* [14]. The plain text is taken, one character at a time, and replaced with a letter a fixed distance away from the original in the alphabet (as illustrated in Figure 2.2). To decrypt the message, the reverse process is undertaken. The key is therefore the distance along the alphabet (or a single numerical value).

This simple scheme becomes easily breakable, once it is known that the encryption algorithm being used is the Caesar Cipher. As cryptography progressed, it has become established that the adversary could have complete knowledge of the schemes being implemented, and therefore obfuscation is not sufficient to guarantee security.

Vigenère Shift Cipher

The *Vigenère Shift Cipher* increased the level of the algorithm's complexity in comparison to the Caesar cipher by shifting each letter in the plain text along the alphabet by a distance corresponding to the value of the character in a keyword (A=1, B=2, etc.) [16]. The keyword is known by both the sender and receiver, and repeated until it is equal in length to that of the plain text (as illustrated in Figure 2.3).

If the key length is known, the problem can be broken down into a series of Caesar ciphers that can be analysed individually, reducing the complexity of decryption by an adversary.

Plain text message	**S**	**E**	**C**	**R**	**E**	**T**	**M**	**E**	**S**	**S**	**A**	**G**	**E**
Repeating Keyword	**K**	**E**	**Y**	**W**	**O**	**R**	**D**	**K**	**E**	**Y**	**W**	**O**	**R**
Numerical Value of Plain Text	19	5	3	18	5	20	13	5	19	19	1	7	5
Numerical Value of Keyword	11	5	25	23	15	18	4	11	5	25	23	15	18
Addition of Plain Text and Keyword	4	10	2	15	20	12	17	16	24	18	24	22	23
Cipher Text	**D**	**J**	**B**	**O**	**T**	**L**	**Q**	**P**	**X**	**R**	**X**	**V**	**W**

Figure 2.3: **Vigenere Shift Cipher:** The plain text message is converted to a numerical value, and shifted by a the values of a repeated keyword. This value is converted back to an alphabetical value. To decrypt the cipher text, it is shifted back by the pre-disclosed repeated keyword values.

One Time Pad

One-time pad (OTP) encryption was invented by Vernam in 1917, utilising a symmetric random secret key shared between the sender and receiver [17]. The key is the same length as the message text, resulting in a cipher text that, in principle, cannot be broken provided it is only used once (known as information theoretically secure) [14]. Shannon was later able to formulate a proof that Vernam's scheme is optimal and that no encryption method could be devised that required less key size to generate the undecipherable cipher text [18]. This scheme is equivalent to a Vigenere Shift cipher, using a completely random key with a length equal to that of the plain text.

If the message is represented in binary, the one-time pad is a string of random bits, and to encrypt the data, this is added to the message bits (modulo 2). To decrypt the data, Bob performs modulo 2 addition (known as the XOR operation) to the encrypted message with the same key string of random bits.

More formally this represents a message, cipher text, and key space existing in the same bit stream space:

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n \tag{2.1.4}$$

where n is the length of the message, and the key is selected with equal probability from the set of all possible strings:

$$k \in (\mathbb{Z}_2)^n \quad \text{with} \quad \Pr(k) = 2^{-n} \ . \tag{2.1.5}$$

With the message $m \in (\mathbb{Z}_2)^n$, the encryption and decryption can be described as

$$c = \mathcal{E}_k(m) = m \oplus k = (m_1 + k_1, \cdots, m_n + k_n) \mod 2 \tag{2.1.6}$$

$$m = \mathcal{D}_k(c) = c \oplus k = (c_1 + k_1, \cdots, c_n + k_n) \mod 2\ . \tag{2.1.7}$$

Assuming the key is generated randomly, it can be shown that Eve will gain no extra knowledge about the message, m, by intercepting the encrypted message c. The probability of the cipher text conditional on the message is

$$\begin{aligned} \Pr(c \mid m) &= \Pr(k = c \oplus m) \\ &= 2^{-n} \end{aligned} \tag{2.1.8}$$

and the probability of all cipher text messages is

$$\begin{aligned} \Pr(c) &= \sum_{m \in (\mathbb{Z}_2)^n} \Pr(m)\ \Pr(c \mid m) \\ &= 2^{-n} \sum_{m \in (\mathbb{Z}_2)^n} \Pr(m) \\ &= 2^{-n}\ . \end{aligned} \tag{2.1.9}$$

Therefore, with the use of Bayes' theorem, the probability of the message conditional on the cipher text is

$$\begin{aligned} \implies \Pr(m \mid c) &= \frac{\Pr(c \mid m)\ \Pr(m)}{\Pr(c)} \\ &= \Pr(m) \end{aligned} \tag{2.1.10}$$

showing that the probability of the message conditional on the cipher text is simply the probability of the message itself. Therefore Eve has gained no further knowledge of the message from the cipher text, unless she knows something about the key.

The issue still remains, that there must be an employable scheme to distribute secret keys to the relevant parties. The keys are required to be as long as the text to be

encrypted, and unknown to a possible adversary.

2.1.2 Asymmetric Cryptography

In comparison to symmetric cryptography, asymmetric cryptography uses pairs of keys: a public key which may be disseminated, and a private key with which it is paired and known only to the owner. Modern day cryptography is often based on mathematical principles whose security is not proven against all possible adversaries, but instead utilise problems that are currently understood to be hard to solve. The problems are expected to continue to be hard to solve for the foreseeable future under reasonable assumptions of the progression of technology. To break these schemes (e.g. determining the private key from the public) therefore requires large computational power, which is assumed to lie beyond the availability of the adversary.

Diffie-Hellman

Diffie-Hellman cryptography [19] utilises the discrete logarithm problem, which can be stated as follows. If the terms ($g^a \mod p$) and ($g^b \mod p$) are given, it is still computationally difficult to find ($g^{ab} \mod p$).

The secret, S, is generated as a symmetric key and is possessed by both Alice and Bob, but the process of establishing the key is considered asymmetric. A public-key implementation requires Alice and Bob to publicly choose values for p (a prime) and g (a primitive root mod p) [20], as well as secretly choosing a, and b separately. They then calculate and publicly declare

$$A = g^a \mod p \tag{2.1.11}$$

$$B = g^b \mod p \tag{2.1.12}$$

respectively, allowing the further computation of

$$s_a = B^a \mod p \tag{2.1.13}$$

$$s_b = A^b \mod p\ . \tag{2.1.14}$$

Since $(g^a \mod p)^b \mod p = \left(g^b \mod p\right)^a \mod p$, the values $s_a = s_b = S$. The secret S has now been shared, without the disclosure of a or b. This secret can be used as a key for any symmetric key cryptosystem or as a public key cryptosystem, based on the previously stated assumption of the hardness of the discrete logarithm problem.

For use in a public key cryptosystem, Alice will use A, g, and p, as her public key information. Bob uses this information and also chooses a random b value to send g^b mod p and a message encrypted with $g^{ab} \mod p$ to Alice, who can decrypt the message by knowing the secret value a.

RSA

Rivest, Shamir and Adleman (RSA) described the popular public-key cryptographic protocol [21], in which to generate a public and private key Alice selects two primes p and q, and calculates

$$n = pq \tag{2.1.15}$$

$$\phi(n) = (p-1)(q-1) \tag{2.1.16}$$

and chooses e, where e is coprime to $\phi(n)$, and calculates d, where:

$$d\,e \mod \phi(n) = 1\ . \tag{2.1.17}$$

Alice can now announce the public key, n and e, but withhold the private key is d. Cipher text, c, and the message, m, are related through the encryption and decryption described as

$$c = m^e \mod n \tag{2.1.18}$$

$$m = c^d \mod n \tag{2.1.19}$$

as illustrated in Figure 2.4.

The protocol utilises the property of multiplying two numbers being trivial, while decomposing a number into specific prime factors is computationally difficult. The exact relationship between cracking RSA encryption and the difficulty of prime factorisation is unknown [22], and it is possible that there are easier methods to crack RSA beyond

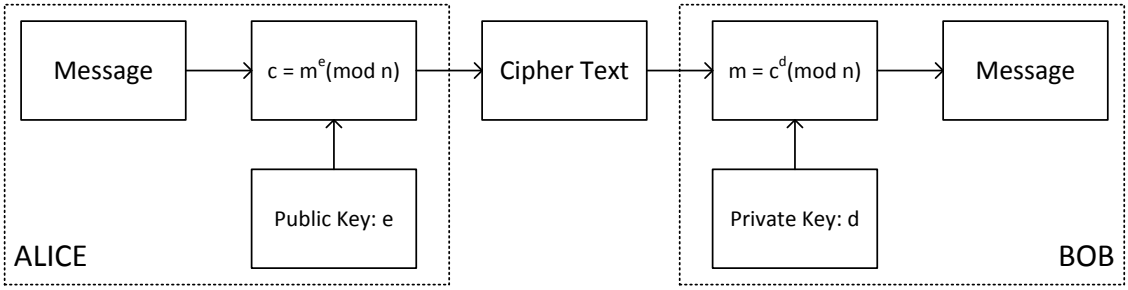

Figure 2.4: **RSA Encryption:** The two parties,"Alice" and "Bob", communicate over a public channel, and encrypt the message with a public key, to render the transmitted cipher text illegible to anyone other than the intended recipient who has kept a private key.

solving prime factorisation.

As computers become more powerful, the reliability of this technique becomes weaker and therefore we can provide an estimated lifetime to the security of the communication based on reasonable assumptions about the adversary's technology. This lifetime may be further limited by the advent of quantum technologies.

2.2 Quantum Information

2.2.1 Quantum Mechanics

Physical theories can be developed in the mathematical framework of quantum mechanics, but this framework does not specify the laws that the physical system must obey. The following postulates describe a relationship between the physical world and the mathematical formalism of quantum mechanics [23].

1. States

A quantum state is a complete description of a physical system, represented by a vector, $|\psi\rangle$, in a Hilbert space, $\mathcal{H}^d$, a finite, d-dimensional complex inner product vector space over complex-space $\mathbb{C}^d$. The class of vectors can also be multiplied by a non-zero complex scalar, so that $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are physically indistinguishable.

2. Observables

An observable is a property of a physical system that can be measured and is

described by a Hermitian operator $\hat{A} = \hat{A}^\dagger$. An operator is a linear map transforming vectors in the form

$$\begin{aligned} &\hat{A}\colon\ |\psi\rangle \to \hat{A}\,|\psi\rangle \\ &\hat{A}\colon\ \alpha\,|\psi\rangle + \beta\,|\theta\rangle \to \alpha\hat{A}\,|\psi\rangle + \beta\hat{A}\,|\theta\rangle\ . \end{aligned} \tag{2.2.1}$$

An observable $\hat{A}$ has a spectral representation, such that its eigenstates form a complete orthonormal basis in $\mathcal{H}^d$,

$$\hat{A} = \sum_n \alpha_n \hat{P}_n \tag{2.2.2}$$

where $\hat{P}_n = |\alpha_n\rangle\langle\alpha_n|$ is the orthogonal projection onto the space of the eigenstates $|\alpha_n\rangle$ with the non-degenerate eigenvalue α_n. In the case that α_n is a degenerate eigenvalue, and $\{|\alpha_{n,i}\rangle\}$ spans the eigenspace of α_n, then

$$\hat{P}_n = \sum_i |\alpha_{n,i}\rangle\langle\alpha_{n,i}|\ . \tag{2.2.3}$$

3. Measurement

The result of a measurement of an observable $\hat{A}$ is an eigenvalue α_n, with probability

$$\Pr(\alpha_n) = \langle\psi|\,\hat{P}_n\,|\psi\rangle \tag{2.2.4}$$

and the state is projected onto the corresponding eigenstate

$$|\psi\rangle \xrightarrow{\alpha_n} \frac{\hat{P}_n\,|\psi\rangle}{\sqrt{\langle\psi|\,\hat{P}_n\,|\psi\rangle}}\ . \tag{2.2.5}$$

4. Evolution

The Schrödinger equation describes the time-evolution of a closed quantum system

$$\mathrm{i}\hbar\frac{d\,|\psi\rangle}{dt} = \hat{H}\,|\psi\rangle \tag{2.2.6}$$

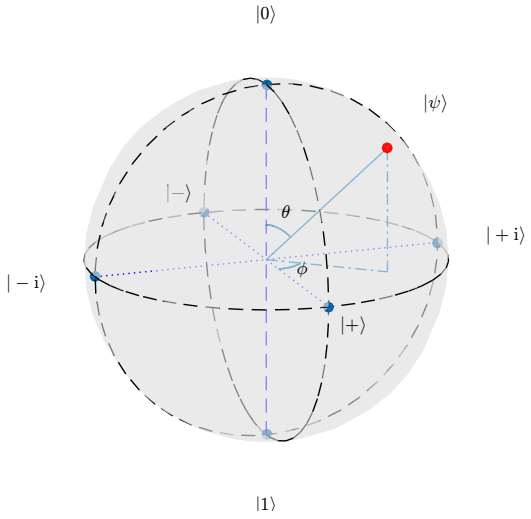

Figure 2.5: **The Bloch Sphere:** A visual representation of the *qubit*. Any pure state will lie on the boundary of the sphere, whereas mixed states lie inside the boundary. Any pure state can therefore be described by the two angles θ and ϕ.

where $\hat{H}$ is a Hermitian operator known as the Hamiltonian of the system. The evolution of the state can therefore be described by the unitary operator $\hat{U}(t) = \exp\left[-\mathrm{i}\hat{H}t/\hbar\right]$ such that

$$|\psi(t)\rangle = \hat{U}(t)\,|\psi(0)\rangle \ . \tag{2.2.7}$$

2.2.2 Qubits

In classical computation, information exists in the binary states 0 or 1, whereas in quantum computing the quantum bit (qubit) exists in the two dimensional Hilbert space $\mathcal{H}^2$, over the basis states $\{|0\rangle, |1\rangle\}$, and can exist in a linear superposition of these basis states

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.2.8}$$

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. The probability of measuring an eigenstate $|0\rangle$ is $|\alpha|^2$, and the probability of measuring the eigenstate $|1\rangle$ is $|\beta|^2$. The qubit can be also be parametrised as

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin\frac{\theta}{2}\,|1\rangle \tag{2.2.9}$$

ignoring the global phase (as discussed before in Section 2.2.1).

2.2.3 Multi-Qubits and Entanglement

In a multi-qubit system, the state-space is described by the tensor product of the individual qubit spaces. For example, if two qubits are defined as

$$|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.2.10}$$

$$|\psi_2\rangle = \gamma\,|0\rangle + \delta\,|1\rangle \tag{2.2.11}$$

then the state of the two qubits together is written as

$$\begin{aligned} |\Psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\ &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\ &= \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle\,. \end{aligned} \tag{2.2.12}$$

With two qubits, we now have a vector in $\mathcal{H}^4$ Hilbert space. Instead of starting with two separate qubits, we can also describe a two particle system as

$$|\Psi\rangle = \alpha'\,|00\rangle + \beta'\,|01\rangle + \gamma'\,|10\rangle + \delta'\,|11\rangle \tag{2.2.13}$$

where the only constraints on the complex amplitudes are normalisation

$$|\alpha'|^2 + |\beta'|^2 + |\gamma'|^2 + |\delta'|^2 = 1\ . \tag{2.2.14}$$

Therefore a valid state is

$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}\ . \tag{2.2.15}$$

If there is a measurement performed on the first particle, it collapses the superposition into either $|00\rangle$ or $|11\rangle$. This indicates that measuring the first qubit in state $|0\rangle$ guarantees the second qubit to be in state $|0\rangle$, and measuring the first qubit in state $|1\rangle$ guarantees the second qubit to be in state $|1\rangle$. This state is also known to violate Bell's inequality [24] and does not obey the assumptions of local realism (the rules that seemingly govern the macroscopic world) [25].

This property can be explained in the form of a simple game [26]. Alice and Bob each receive a quantum state and are allowed to make measurements in a basis of their choice $x \in \{0,1\}$ and $y \in \{0,1\}$, with the output results $a \in \{+1,-1\}$ and $b \in \{+1,-1\}$ respectively.

The joint probability of the measurement outcome in general is not necessarily the product of two independent probabilities. That is to say, if the particles came from the same source with pre-assigned values or a set of rules for their behaviour they may not act independently. These are known as "hidden variables" (λ) and the behaviour could be described by a probability distribution $q(\lambda)$, such that the joint probability of the measurement outcomes can be made separable:

$$\begin{aligned} p\left(a,b \mid x,y\right) &= \int_{\lambda} d\lambda\, q\left(\lambda\right)\, p\left(a \mid x,\lambda\right)\, p\left(b \mid y,\lambda\right) \\ &\not\equiv p\left(a \mid x\right)\, p\left(b \mid y\right)\ . \end{aligned} \tag{2.2.16}$$

To evaluate the outcome of the game, a value S, can now be calculated

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \tag{2.2.17}$$

where $\langle a_x b_y \rangle = \sum_{ab} ab\, p\left(a,b \mid x,y\right)$ is the expectation value of the joint measurement (x,y). If locality applies, then the joint expectation value is a product of the individual expectation values $\langle a_x b_y \rangle = \int d\lambda\, q\left(\lambda\right) \langle a_x \rangle \langle b_y \rangle$, which leads to the Clauser-Horne-Shimony-Holt (CHSH) inequality [27]

$$|S| \leq 2\ . \tag{2.2.18}$$

Alice and Bob are provided with the entangled state, $|\Psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$, and the measurement settings

$$x_0 = \hat{Z}; \quad x_1 = \hat{X}; \quad y_0 = \frac{-\hat{Z} - \hat{X}}{\sqrt{2}}; \quad y_1 = \frac{\hat{Z} - \hat{X}}{\sqrt{2}} \tag{2.2.19}$$

where

$$\hat{Z} = |0\rangle \langle 0| - |1\rangle \langle 1| \tag{2.2.20}$$

and

$$\hat{X} = |+\rangle\langle+| - |-\rangle\langle-| \tag{2.2.21}$$

where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. This yields $\langle a_0 b_0\rangle = \langle a_0 b_1\rangle = \langle a_1 b_0\rangle = \frac{1}{\sqrt{2}}$ and $\langle a_1 b_1\rangle = -\frac{1}{\sqrt{2}}$, and hence

$$S = 2\sqrt{2} > 2 \tag{2.2.22}$$

in contradiction with equation 2.2.18. This violation of the CHSH inequality has been demonstrated by experiments countless times in many laboratories and physical systems across the world, attesting that the local realism model of physical reality is seemingly misguided [26, 28–31].

2.2.4 No Cloning Theorem

When copying classical bits of information, one can measure the value of the bit or bits and prepare as many copies with same value. This is not the case with qubits, as described by the no-cloning theorem [32, 33].

As discussed in Section 2.2.1, quantum measurement is non-deterministic and collapses the wavefunction of the qubit into a random eigenvalue, with a probability described by its probability amplitudes.

It can be shown that under the linear laws of quantum mechanics that cloning of an arbitrary qubit state on to a further blank qubit is impossible, i.e. there does not exist an operator, $\hat{U}$, capable of the operation

$$\hat{U}|\psi\rangle|0\rangle \rightarrow |\psi\rangle|\psi\rangle \ . \tag{2.2.23}$$

If we have an arbitrary state written as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we require the effect of the operator on each basis state to be

$$\hat{U}|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \tag{2.2.24}$$

$$\hat{U}|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle \tag{2.2.25}$$

and the operation on the entire state will therefore be

$$\begin{aligned}\hat{U}\left|\psi\right\rangle\left|0\right\rangle &= \hat{U}\left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right)\left|0\right\rangle \\ &= \hat{U}\left(\alpha\left|0\right\rangle\left|0\right\rangle + \beta\left|1\right\rangle\left|0\right\rangle\right) \\ &= \alpha\hat{U}\left|0\right\rangle\left|0\right\rangle + \beta\hat{U}\left|1\right\rangle\left|0\right\rangle \\ &\rightarrow \alpha\left|0\right\rangle\left|0\right\rangle + \beta\left|1\right\rangle\left|1\right\rangle \end{aligned} \tag{2.2.26}$$

but equation 2.2.23 also describes the operation as

$$\hat{U}\left|\psi\right\rangle\left|0\right\rangle \rightarrow \left|\psi\right\rangle\left|\psi\right\rangle \tag{2.2.27}$$

where

$$\begin{aligned}\left|\psi\right\rangle\left|\psi\right\rangle &= \left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right)\left(\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right) \\ &= \alpha^2\left|00\right\rangle + \alpha\beta\left|01\right\rangle + \alpha\beta\left|10\right\rangle + \beta^2\left|11\right\rangle \end{aligned} \tag{2.2.28}$$

which contradicts the outcome of equation 2.2.26, showing there is no linear operator, $\hat{U}$, able to clone arbitrary quantum states.

This inability to clone arbitrary quantum states complicates techniques such as quantum error correction, but also provides quantum secured communications, as discussed in Section 2.3.

2.2.5 Quantum Computing

Quantum computing, as an idea, stems from the intuition Feynman expounded in [34], that to simulate a quantum system exactly one would need a quantum system with which to do it. This idea has matured and expanded beyond simulating other quantum systems. Developing on these ideas, Deutsch described the quantum analogue to a universal Turing machine (an abstract computer capable of performing any classical algorithm or computation). The universal quantum Turing machine is capable of performing any quantum operation and algorithm [35], providing a framework with which to understand quantum computing. He also developed the first algorithm known to have a quantum advantage in

terms of computational resources compared to its classical counterpart [36].

This purely esoteric algorithm demonstrated the power that quantum computation could have, and over the next few decades a host of further algorithms were developed. Grover's algorithm showed a polynomial speed up in computational resource to search an unsorted database for a marked element [37], Harrow, Hassidim, and Lloyd developed a quantum algorithm for solving linear systems of equations with exponential speed up over the fastest classical algorithm [38] (under certain conditions), and many proposals in the field of machine learning and data analysis have been produced over the last few years [39].

Finally, it has been shown that quantum computers have the potential to factor large integer numbers efficiently, in stark contrast to the state of the art classical algorithms. Shor's algorithm would permit a quantum computer to decrypt many of the cryptographic systems in use today in polynomial time [40]. This would have a serious impact on the current approach of public key cryptography that utilises discrete logarithm problems and factoring of integers, such as Diffie-Hellman and RSA (see Section 2.1.2), as the assumption of difficulty with respect to the adversaries computational power is no longer satisfied. These schemes are currently used to secure Web pages and encrypt emails, so that breaking them would have significant ramifications for electronic privacy and security.

2.3 Quantum Key Distribution

2.3.1 Conjugate Coding and Quantum Money

Post-quantum cryptography must therefore present schemes resistant to attacks by quantum computing, and some approaches utilise quantum mechanics for their security. One of the first steps towards this was *Conjugate Coding*, in which Wiesner first introduced a scheme for transmitting two messages where only one of the messages could be retrieved [41]. The scheme sends two messages encoded in the polarisation of photons: one encoded in the horizontal-vertical basis and one encoded in the left-right circular polarisation. The receiving equipment is configured to measure one of the two messages, as measuring in one basis will destroy the information encoded in the other basis.

Weisner developed a further scheme for "uncounterfeitable quantum money", by encoding the unique serial number of quantum money with a collection of qubits in the orthogonal states of a and b, or in α and β where

$$\alpha = \frac{1}{\sqrt{2}}(a+b)$$
$$\beta = \frac{1}{\sqrt{2}}(a-b) \ . \tag{2.3.1}$$

The scheme encodes each component of the quantum money's serial number into one of the four states, and the bank records these encodings along with a serial number. If the unit of quantum money is returned to the quantum mint, the states can be measured and compared to the initial encoding, to check its validity.

Since the bank is aware of the correct basis to measure in, there will be no disturbance to the states being introduced and there should be no error in the measurements. A counterfeiter, on the other hand, would be ignorant of the basis choice and therefore cannot copy the photon polarisation exactly. If he/she chooses the wrong basis it will cause a superposition to collapse, and remove the information encoded in the original basis.

The security of the system relies on the no-cloning theorem (see Section 2.2.4) and therefore the counterfeiter has a probability 3/4 of successfully duplicating each qubit. In the case of N-qubit quantum money, the duplication probability would be $(3/4)^N$, which becomes exponentially small.

Charles Bennett and Gilles Brassard of IBM later illustrated that encoding information in quantum systems could be used to share random secret keys between two parties along a quantum channel [42]. The secret key could be used in a one time pad cryptography scheme and relies on the transmission on photons, rather than the storage of quantum states required for quantum money. This is known as Quantum Key Distribution (QKD).

2.3.2 Protocols

Many protocols for QKD have been proposed that can be categorised broadly as

- Discrete Variable QKD

- Continuous Variable QKD
- Distributed Phase Reference QKD

Discrete Variables

BB84 Bennett and Brassard described a "prepare and measure" quantum key distribution scheme, that relies on the fact that measurement of an unknown quantum state alters that state, known as quantum indeterminacy (related to the Heisenberg uncertainty principle and the no-cloning theorem) [42]. The scheme exploits quantum mechanics to allow the detection of eavesdroppers and calculates the amount of information that has been intercepted.

In "prepare and measure" schemes, the protocol must specify which quantum state $|\Psi(\mathcal{S}_n)\rangle$ codes for the sequence of n symbols $\mathcal{S}_n = \{s_1, \ldots, s_n\}$. In most protocols, the state $|\Psi(\mathcal{S}_n)\rangle$ has the tensor product form $|\psi(s_1)\rangle \otimes \ldots \otimes |\psi(s_n)\rangle$. In BB84 the protocol requires the sender, Alice, to prepare one of four quantum states

$$\begin{aligned} |\psi_{00}\rangle = |0\rangle &= \frac{|+\rangle + |-\rangle}{\sqrt{2}} \\ |\psi_{01}\rangle = |1\rangle &= \frac{|+\rangle - |-\rangle}{\sqrt{2}} \\ |\psi_{10}\rangle = |+\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |\psi_{11}\rangle = |-\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned} \tag{2.3.2}$$

at random using two bits, the first bit to decide on a basis $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$ basis and the second to decide a value. If the qubit is encoded in polarisation, this could be related to the vertical $|\uparrow\rangle$, horizontal $|\rightarrow\rangle$, diagonal $|\nearrow\rangle$, and anti-diagonal $|\nwarrow\rangle$ states. For fibre implementations, time-bin encoding (see Section 2.4.2) is illustrated in Figure 2.6.

Note further that each state can be written as a superposition of bits from the other basis. The security of the protocol comes from the encoding of the information in non-orthogonal states, meaning that there is no one measurement that can be made to unambiguously distinguish the four possible states 100% of the time [43, 44].

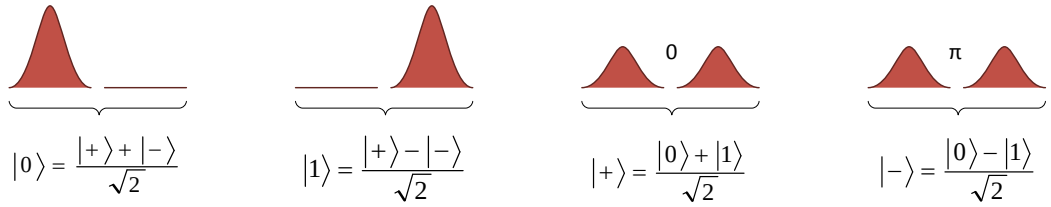

Figure 2.6: **Time-bin encoded states for BB84:** where $|0\rangle$ is a photon in the first time slot, $|1\rangle$ is a photon in the second time slot, and $|+\rangle$ and $|-\rangle$ are photons in superposition of the two time slots, with a 0 or π relative phase difference.

After Alice prepares the states, she sends the qubit to Bob over the quantum channel, who will measure the state in one of the orthonormal bases at random as he does not know which basis the state was prepared in. If the prepared state is an eigenstate of the measurement basis, Bob will determine the state exactly but will receive a random result if measured in the alternate basis. He will repeat this process for all photons he received, recording the time, the measurement basis, and the result.

After the measurement, Bob will communicate over a public classical channel to Alice, revealing the measurement basis for each received photon but not the result of the measurement. They can now discard the results of photons that were prepared in unmatched bases, which will be on average half of the states (see Figure 2.7).

In the ideal case there is now an identical set of random bits shared between Alice and Bob that can be used in a one time pad. To check for the presence of an eavesdropper, Alice and Bob disclose a subset of the remaining bit string, checking for mismatched bits as any information about the photons' state that Eve can gather will introduce errors to Bob's measurement. If more than p bits differ, they will discard the transaction and try again, where p is chosen to guarantee the security of the transmission by ensuring Eve's knowledge can be reduced to an arbitrarily small amount by privacy amplification (discussed later in this Section).

The six-state protocol [45] follows the same structure as BB84, to which it adds the third mutually unbiased basis (the $|\pm i\rangle$ basis). The interest of this protocol lies in the fact that the channel estimation becomes "tomographically complete" (the measured parameters completely characterize the channel), and its unconditional security was proved quite early [46]. As a consequence, more noise can be tolerated with respect to BB84.

ALICE RANDOM BITS	0	1	1	0	1	0	0	1
ALICE RANDOM BASIS	✢	✢	✕	✢	✕	✕	✕	✢
PHOTON POLARISATION	↕	↔	↘	↕	↘	↗	↗	↔
BOBS RANDOM BASIS MEASURE	✢	✕	✕	✕	✢	✕	✢	✢
BOBS MEASURED	↕	↗	↘	↗	↔	↗	↔	↔
PUBLIC BASIS DISCUSSION	YES		YES			YES		YES
SHARED KEY	0		1			0		1

Figure 2.7: **BB84 protocol example:** Alice uses 2 random bits to select a basis and bit to prepare one of 4 polarisations. Bob independently chooses a random basis to measure the sent photons and notes the output measurements. Public discussion allows the selection of a subset of results where Alice and Bob's basis choice match, and these results form the shared key.

However, noise is quite low in optical systems, while losses are a greater concern. In this respect, six-state performs worse, because it requires additional lossy optical components.

E91 In the "prepare and measure" scheme described above actively Alice chooses the sequence $\mathcal{S}_n$ she wants to send, prepares the state $|\Psi(\mathcal{S}_n)\rangle$ and sends it to Bob, who performs some measurement. In 1991 Ekert published a protocol [47] that instead utilises the non-local correlation properties of an entangled state of the form

$$|\Phi^n\rangle_{AB} = \frac{1}{\sqrt{d_n}} \sum_{\mathcal{S}_n} |\mathcal{S}_n\rangle_A \otimes |\Psi(\mathcal{S}_n)\rangle_B \tag{2.3.3}$$

where d_n is the number of possible $\mathcal{S}_n$ sequences and the $|\mathcal{S}_n\rangle_A$ form an orthogonal basis. By measuring in this basis, Alice learns one $\mathcal{S}_n$ and prepares the corresponding $|\Psi(\mathcal{S}_n)\rangle$ on the sub-system that is sent to Bob. An example being the Bell state $|\Phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. The scheme and its security relies on the entanglement between the two particles and the random basis measurements that Alice and Bob perform on the particle independently (either the $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$ basis).

After a stream of entangled pairs are shared between Alice and Bob and their random measurement basis is set for each successive photon, they communicate over a public channel which basis measurement they made, but keep the result of the measurement

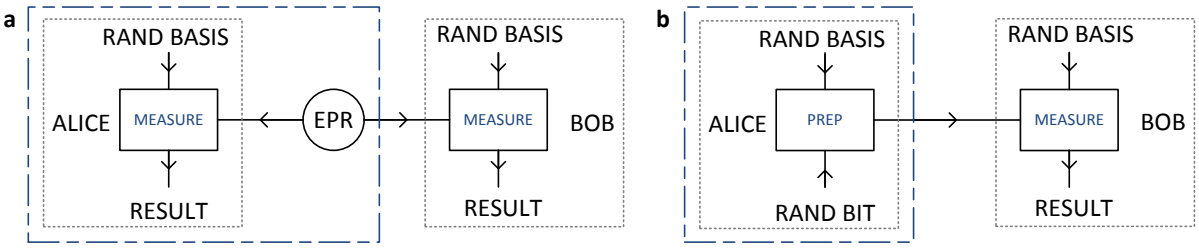

Figure 2.8: **Entanglement based and Prepare and Measure based QKD:** (a) Entanglement based protocol where an entangled pair of photons are sent to Alice and Bob. Each photon is measured in a random basis and produces a result. (b) The prepare and measure scheme has Alice inputting a random basis and bit value to prepare and send a state for Bob to measure. The box surrounding the EPR source and Alice's measurements in (a) can be considered equivalent to the box surrounding Alice's preparation and state transmission in (b).

private. In the case that they both choose the same basis to measure in, they will have perfectly correlated results with which they can generate a secure key.

To calculate the presence of an eavesdropper, they can compute a test statistic S using the correlation coefficients, similar to that in a Bell inequality (Section 2.2.3). The maximally entangled states would result in $|S| = 2\sqrt{2}$, and if this were not the case it could be understood as Eve affecting the entanglement of the system.

Some security proofs use the E91 entanglement framework for prepare and measure schemes, as they can be shown equivalent by replacing all locally chosen randomness by quantum entanglement and postponing all measurements (Figure 2.8).

Generic Protocol A generic protocol can be described by the following steps

1. State Preparation

Either an entangled pair of photons is generated and shared between Alice and Bob, or one party (usually considered to be Alice) prepares a randomly chosen single photon state to send to the other party.

2. State Estimation

Random measurements are made on the photon or photons and a subset of these can be used to estimate whether the shared state has been distributed without corruption from an eavesdropper. This is achieved by either checking some non-local statistical correlation from entanglement, or checks on quantum indeterminacy

from the non-cloning theorem. There will be some security analysis that allows the parties to agree whether or not the communication has been successful in sharing the random key. The possible information shared with Eve will be bounded, and an agreeable limit to this information set to ensure security.

3. Data Processing (Sifting)

The collected data that hasn't been used for state estimation can be used to generate the key. The data must therefore be sifted for cases that will have the correct correlations required, and Alice and Bob must agree between them which cases can be included (e.g. when Alice and Bob independently chose matching basis measurements).

4. Error Correction & Information Reconciliation

In a non-ideal system, there will be some small percentage of errors between the keys shared between Alice and Bob. These need to be corrected. This must be performed over the public channel and it is necessary to minimise the information sent about the key, as this could be read by Eve. These take many forms including cascade protocols, turbocode [48], LDPC codes [49], and polar codes [50].

5. Privacy Amplification

After the sifted data is error corrected, the problem arises that some information from this key could have been shared with Eve (along with the possible information shared within the quantum channel) and this must be minimised to an appropriate level. This process is known as privacy amplification and can take many forms, commonly an information theoretic cryptographic universal hash function is used to remove any classical correlations and extract the quantum randomness [51].

Continuous Variables

An alternative to discrete-variable QKD was developed in which photon counting is replaced with standard photodiodes (allowing for faster signal processing and more efficient measurements), and discrete values are replaced with real amplitudes. These continuous variable (CV) QKD protocols can be categorised as Gaussian or discrete modulation

protocols.

Gaussian Protocols use squeezed states of light, in which the transmitter modulates these states with a Gaussian distribution in the $\hat{x}$ or $\hat{p}$ quadrature ($\hat{x} = \frac{1}{2}(a^\dagger + a)$ and $\hat{p} = \frac{\mathrm{i}}{2}(a^\dagger + a)$ where a and $a^\dagger$ are the annihilation and creation operators of the quantum harmonic oscillator described in Section 2.4.1), and the quadratures are measured via homodyne detection by Bob. This protocol is the continuous variable counterpart to BB84, as the state sent by Alice is thermal, i.e. the average state is the same regardless of the chosen basis. This is analogous to the maximally mixed qubit state of BB84. This has been further developed to include cases where Alice generates coherent states of light. This requires a strong local oscillator for the homodyne detection, and for Bob to randomly choose whether to measure in the $\hat{x}$ or $\hat{p}$ quadrature. The results are sifted for cases in which the quadratures match between Alice and Bob [52].

Discrete-modulation protocols allow for more practical implementations as it is desirable to keep the number of possible states as low as possible and to minimise the number of parameters in the detection process. This approach combines a finite number of signals with the benefits of continuous-variable detection schemes [53].

Distributed Phase Reference Schemes

Discrete-variable and Continuous-variable quantum key distribution presented certain difficulties in practical implementations. Other schemes have been developed by experimental groups, with focus on the most practical implementations which use currently available technologies. In these schemes, the raw keys are generated from discrete variable bits and the security of the quantum channel is determined by monitoring the properties of coherent states (see Section 2.4.1), such as the phase coherence of subsequent pulses. These protocols are known as distributed-phase-reference protocols.

Differential Phase Shift (DPS) uses the relative phase between subsequent pulses of coherent light to encode bits and to test the coherence of the quantum channel for security [54, 55]. DPS has been demonstrated experimentally in [56–58].

In particular, Alice produces a sequence of coherent states of the same intensity

$$|\Psi(\mathcal{S}_n)\rangle = \cdots \left|e^{i\phi_{k-1}}\sqrt{\mu}\right\rangle \left|e^{i\phi_k}\sqrt{\mu}\right\rangle \left|e^{i\phi_{k+1}}\sqrt{\mu}\right\rangle \cdots \tag{2.3.4}$$

where each phase is prepared as either $\phi = 0$ or π. The bit is encoded in the relative difference between successive phases, i.e. $b_k = 0$ if $e^{i\phi_k} = e^{i\phi_k+1}$ and $b_k = 1$ otherwise (see Figure 2.9 (b)).

The key can be unambiguously discriminated with an unbalanced Mach-Zehnder Interferometer (see Section 2.4.3) where the difference in length is equal to the temporal offset between subsequent pulses. The security of the system comes from the measured coherence of the quantum channel, but the difficulty in analysing this protocol is inherent to the fact that the series of pulses can not be broken down into separable states, i.e. $|\Psi(\mathcal{S}_n)\rangle \neq |\psi(b_1)\rangle \otimes \cdots \otimes |\psi(b_n)\rangle$, and that the k^{th} pulse contributes to both the k^{th} bit and the $(k+1)^{\text{st}}$ bits.

Coherent One Way (COW) encodes each bit in pairs of pulses, where

$$\begin{aligned} |0\rangle_k &= |\sqrt{\mu}\rangle_{2k-1} |0\rangle_{2k} \\ |1\rangle_k &= |0\rangle_{2k-1} |\sqrt{\mu}\rangle_{2k} \\ |\text{DECOY}\rangle_k &= |\sqrt{\mu}\rangle_{2k-1} |\sqrt{\mu}\rangle_{2k} \end{aligned} \tag{2.3.5}$$

as illustrated in Figure 2.9 (a).

The first two states can be unambiguously discriminated by measuring the time of arrival of single photons. The channel security can be estimated by measuring the coherence between two successive non-empty pulses, through an asymmetric Mach-Zehnder interferometer. These non-empty pulses can be introduced on purpose by the "decoy" state, or between bits , such as a $|1\rangle_k |0\rangle_{k+1}$. This allows checks as to whether an adversary has accessed the multi-photon emissions and requires phase control between successive pulses, therefore the whole sequence must be considered as a single signal.

Both COW and DPS are prepare and measure schemes, developed to utilise readily available laser sources, instead of single photons. The derivation of a complete security

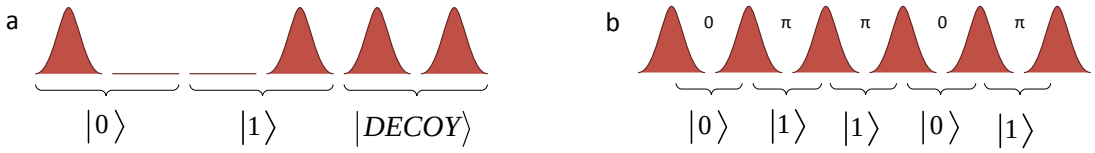

Figure 2.9: **Distributed Phase Reference Protocols:** (a) COW where weak coherent pulses encoded the $|0\rangle$ state by populating the first time bins with photons, and the $|1\rangle$ state by populating the second time bin with photons. A $|DECOY\rangle$ is included to help monitor the coherence of the quantum channel for security. (b) DPS encodes information in the relative phases between successive weak coherent pulses with 0 phase difference representing a $|0\rangle$ and π phase difference representing a $|1\rangle$ state.

analysis for distributed phase reference schemes has been an on-going priority within the QKD academic community. Developments include proof of security against a number of eavesdropping methods [59]. Existing techniques for unconditional security have only applied to $|\Psi(\mathcal{S}_n)\rangle$ if it could be decomposed into independent signals [2], and only recently have variants of this scheme been bounded with unconditional security by decomposing the signals into independent blocks [60, 61].

2.3.3 Implementation

Sources

Lasers The most practical light source to be used in QKD systems are lasers, which generate coherent light (Section 2.4.1) used in prepare and measure schemes. The output of the laser is described by a coherent state of the field

$$\left|\sqrt{\mu}e^{i\theta}\right\rangle \equiv |\alpha\rangle = e^{-\frac{|\alpha^2|}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{2.3.6}$$

where $\mu = |\alpha^2|$ is the average photon number, $|n\rangle$ is the number operator, and the phase factor $e^{i\theta}$ is measurable if there is a reference frame available. If there is no reference, the emitted state can be described by a mixed state of the form

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi} |\alpha\rangle\langle\alpha| = \sum_n e^{-\mu} \frac{\mu^n}{n!} |n\rangle\langle n| \ . \tag{2.3.7}$$

In the absence of a phase reference the laser can be said to generate Poissonian distributed mixture of number states [62].

Sub-Poissonian sources Sub-Poissonian sources are closer to ideal single-photons than an attenuated laser, as the probability of emitting two photons within the same state is smaller. The state in each mode can be described by a photon-number diagonal mixture with almost negligible contribution from multi-photon terms.

Although sub-Poissonian sources showed much promise by reducing the probability of an attacker gaining access to identically encoded multi-photon cases, the introduction of decoy states demonstrated that the same rates could be achieved with laser sources (see Section 2.3.5).

Entangled Photons Pairs of entangled photons, suitable for entanglement-based protocols such as E91, are commonly generated by spontaneous parametric down conversion (SPDC described further in Section 2.4.1), where a photon from a pump laser beam has a small probability of conversion to a pair of photons with lower energies due to non-linear optical processes in a crystal. In this process energy and momentum are conserved, and the states are entangled in time and energy, but by using other approaches the entanglement can exist in other degrees of freedom, such as time-bins for fibre optical communication, polarisation for free-space, momenta, or orbital angular momenta. These sources can be used directly in continuous-variable protocols but in the discrete-variable protocols the issue of generating multiple pairs of photons that encode identical information can lead to insecurity in the system.

Physical Channels

As Eve has full freedom of action over the physical quantum channel, the physical channel can only be characterised *a posterior*. However, it is still important to have *a priori* knowledge of the expected behaviour when designing a QKD system. Such characterisation can include parameters such as the loss, as signal to noise (due to dark counts) will ultimately limit the maximal achievable distance. There will also be other parameters, such as timing delays and the environmental effects that can lead to decoherence due to

issues such as dispersion. These parameters can not be neglected in some implementations.

Free Space The first demonstrations of QKD were in free space and this channel can be used in a number of scenarios, from short distance line-of-sight links [63, 64] to long distance ground-to-air [65] or even space-space links using astronomical telescopes [66–68]. There have been demonstrations of both entanglement-based [69] and "prepare and measure" schemes [64] that focus on the use of polarisation, as the decoherence of this degree of freedom is practically negligible.

The losses stem from both geometric and atmospheric losses. Geometric losses come from the effective apertures of the transmitting and receiving apparatus, the divergence of the beam and alignment. Atmospheric loses are due to scattering (hence using the atmospheric transmission windows of 780-850nm and 1520-1600nm seen in Figure 2.10 (b)), weather conditions, and background light sources, which can often dominate experimental noise.

Optical Fibre As with classical communication, standard fibre optics such as SMF-28 are of great interest for QKD. The losses due to random scattering processes can be described as

$$t = 10^{-\frac{\alpha l}{10}} \tag{2.3.8}$$

where l is the length of the fibre and α is the wavelength-dependent loss in dB per km. Minimal values of this loss are found at the two telecommunication windows of 1310 nm ($\alpha \simeq 0.34$ dB/km) and 1550 nm ($\alpha \simeq 0.2$ dB/km), as illustrated in Figure 2.10 (a).

Decoherence can come from two main effects: chromatic dispersion and polarisation mode dispersion. The chromatic dispersion occurs due to different wavelengths travelling at different velocities causing incoherent temporal spreading of the light pulses. Polarisation mode dispersion is due to the birefringent effect in fibres, having fast and slow orthogonal polarisation modes. This causes issues when encoding in polarisation, and one of the reason for the prevalence of time-bin or phase encoded schemes.

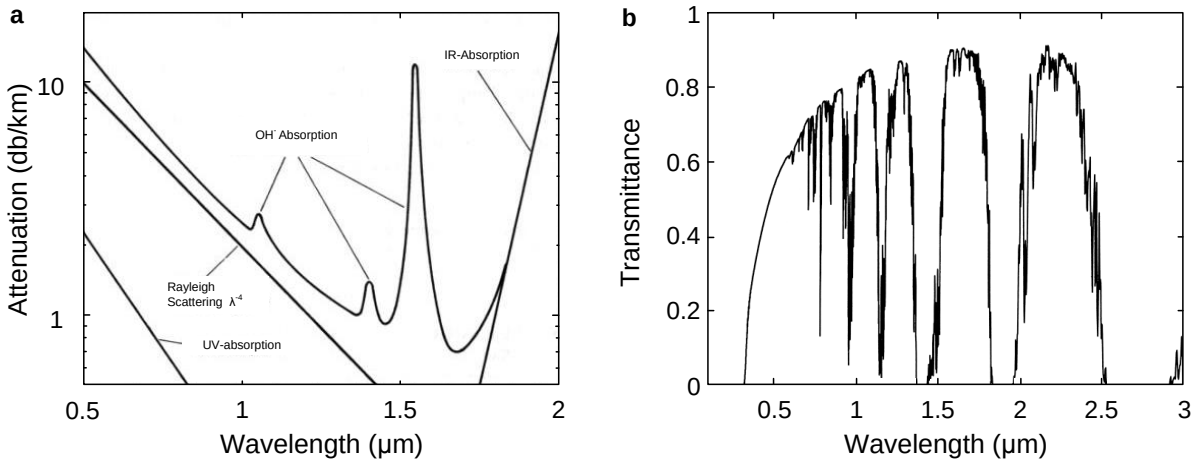

Figure 2.10: **Absorption Spectra:** (a) Optical Fibre attenuation spectrum, illustrating the effects of UV-absoprtion, IR-asorption, Rayleigh scattering, and water impurities, leading to bands of low loss transmission. (b) Free Space transmission spectrum through the atmosphere, illustrating suitable peaks of transmission for communications and troughs of transmission where absorption and scattering render lost signals [70].

Detection

Detectors for QKD can be divided into photon counting technologies, and homodyne detector systems. In discrete-variable and distributed-phase-reference protocols, photon counting is required. The important characteristics are quantum efficiency, dark counts, dead time and timing jitter (discussed further in Section 2.4.4). The common detector technologies inlcude Si APDs, InGaAs APDs (some with self-differencing [71]), visible light photon counters (VLPCs) [72], SNSPDs [73] and TES detectors [74].

Continuous-variable QKD, on the other hand, is based on measuring quadrature components of light which can be achieved with homodyne detection using photodiodes and a local oscillator (which is much stronger than the continuous variable signal and is often treated as classical). Intensity measurements are performed with *p-i-n* diodes, providing low noise, high detection efficiencies (typically $\simeq$80%), and gigahertz operation rates [75]. The benefit of the high rates is offset with the lower loss-budget compared to discrete variables. Noise from the detectors and the vacuum fluctuations, coupled with the unavoidable transmission losses in the optical channel, decrease the signal-to-noise ratio quicker than the discrete variable losses. The losses in discrete variable systems simply cause missing clicks and do not introduce further noise themselves.

Commercial Systems

A number of commercial and semi-commercial systems have been developed and actively research, such as ID Quantique [7], QuintessenceLabs [9], SeQureNet [76], and MagiQ Technologies [8]. Several companies have also established research programmes including NTT [77] and Toshiba [78].

2.3.4 Attacks and Hacking

In proving the security of a quantum key distribution protocols, one needs to model the family of attacks of which our adversary is capable. An *individual attack* is one in which Eve interacts with each transmitted state individually, and must measure any of her ancillary states before the announcement of any measurement bases and classical post-processing. A *collective attack* is one in which Eve has both the capabilities of an individual attack, but can also store the states in a quantum memory and wait until the classical post-processing announcements before choosing the best measurement strategy. Finally, *coherent attacks* are the most general family, with the capabilities of both individual and collective attacks and with the abilities to entangle and operate more freely on the states. This family is much more difficult to parameterise but the security bounds have been shown to be equivalent to those of collective attacks for BB84 and a number of other protocols.

Although BB84 can theoretically guarantee security against a general class of attacks, this assumes ideality of the source, detection, and channel, whereas in practical implementation this is not the case. Therefore, in order to achieve security, non-ideal components must be included in the analysis or mitigated through counter-measures.

Intercept-Resend

The simplest approach to infiltrate QKD protocols is the *intercept-resend attack*. In this individual attack, Eve directly measures the transmitted signal in a random basis and resends the state measured. Due to the no-cloning theorem and quantum indeterminacy, as long as Alice and Bob choose random bases, the measurement basis that Eve uses will be uncorrelated to Bob's and will therefore introduce errors on the signal Bob measures.

This can be detected through state estimation on a random subset of their results.

Man in the Middle

Further to the intercept-resend attack, Eve could also intercept the classical communication. By impersonating Bob when communicating to Alice and impersonating Alice when communicating to Bob, she can generate two keys (k_{AE} and k_{EB}). Alice will encrypt her data with k_{AE}, which Eve can decode, and encyrpt with k_{EB}, to send on to Bob. Neither party would be able to detect this presence, unless there is an authenticated channel between Alice and Bob. This can be achieved by having a small initial secret key shared between the two parties, which in reality reduces QKD to quantum key *expansion*.

Photon Number Splitting

As discussed in Section 2.3.3, ideal photons sources are often replaced with more practical techniques such as weak coherent sources and spontaneous parameteric down-conversion photons, which are probabilistic and have multi-photon terms. If there is more than one photon in a pulse they will be encoded with identical information and Eve can use the spare photons to gain information from the key without disturbing the photons sent to Bob.

With a mean photon number of μ, the probability of an attenuated laser source containing n photons is described by the Poissonian distribution

$$\Pr(n, \mu) = \frac{\mu^n \mathrm{e}^{-\mu}}{n!} \tag{2.3.9}$$

which has a finite probability that the pulse contains more than one photon. One approach to avoid this information leakage is to decrease the average intensity of a pulse to make the probability of high order terms negligible.

In QKD security, it must be assumed that Eve has all information about the devices to plan an optimal attack, as well as access to a perfectly lossless channel. In this case, Eve can stop all single photon pulses emitted from Alice, keeping at least one photon from multi-photon terms and allowing the others to reach Bob through the lossless channel. This is indistinguishable from a lossy channel, but Eve can now wait until Bob announces

his basis choice to measure the photons and gain knowledge of the key.

Side Channels

A range of vulnerabilities have been noted that can leak information from any cryptosystem [79], which in turn could compromise security. Attacks of this nature are called *side channel* attacks, and include

- Electromagnetic field radiating from devices, containing the key or plaintext information.
- Differing power consumption dependent on which parts of a system are active
- In the case of systems containing mechanical parts, the sound generated from the device could be used to extract certain information

In QKD, many other side channels exists such as photons emitted into a mode not considered in the security analysis or wavelength dependence on the states generated. Some other side-channels are described below.

Indistinguishability If there is any degree of freedom, other than the degree in which we encode information, that the photons contain (such as wavelength or polarisation) that is in some way correlated to the states being sent, then Eve can use this correlation to extract information about the key.

It is therefore necessary to characterise these extra degrees-of-freedom and mitigate the risk that these cause, such as filtering the sources in wavelength, polarisation, and time, or randomising phase.

Trojan Horse Another approach to extract the state encoding information in a deterministic way is to probe Alice's state preparation device. By sending bright light in to the transmitter apparatus via the channel and measuring the back-reflections from optical components that pass through the state encoding devices, Eve can discern Alice's encoding with a classical signal, allowing unambiguous state discrimination [80].

Detector Vulnerability A detector based attack utilises the imperfection in the detectors themselves. By using a bright laser beam, a SPAD can be saturated so that it will no longer photon-count in Geiger-mode. By decreasing the intensity, the SPAD will desaturate, causing a signal that can be mistaken for a photon count. This can allow full classical control over the receiving device, without detection of eavesdropping. This attack has been experimentally demonstrated with a number of systems and detector technologies, and countermeasures have been recommended to mitigate the risk of the attack [81].

Another approach uses the carriers in SPADs that can recombine shortly after an avalanching event [82], causing a *back flash*, which provides information as to which state Bob has measured [83]. This light is not evenly spread across the spectrum, and so the signal wavelength can be chosen such that narrow spectral filtering can remove the effect of back flash photons.

Many other attacks have been conceived and some demonstrated, such as **faked states** [84], **phase-remapping** [85], and **time-shift attacks** [86], demonstrating the caution required when claiming security.

2.3.5 Security Proofs

In deriving the security of QKD it is assumed Eve has unlimited resources, both classical and quantum. And in the ideal case of single qubit transmission, QKD can be proven unconditionally secure (no condition imposed on the eavesdropper), although there are often additional conditions required, such as:

- Eve does not have physical access to Alice's encoding device and Bob's decoding device
- The use of trusted and truly random number generators
- Unconditionally secure authentication of the classical communication channel
- One-time pad schemes are used to encrypt the classical cipher text

Infinite Bound for Single Qubit BB84

The following section describes the outline of the security analysis for infinite bound single qubit BB84 as described by Scarani *et al.* [2]. This proof assumes an entanglement-based protocol, but can be expanded into a prepare and measure scheme as discussed in Section 2.3.2. Alice prepares the entangled states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and retains the first qubit for herself, transmitting the second to Bob. This provides perfectly correlated outcomes for Z and X basis measurement ($\langle\sigma_z \otimes \sigma_z\rangle = \langle\sigma_x \otimes \sigma_x\rangle = 1$), and perfectly anti-correlated outcomes in Y ($\langle\sigma_y \otimes \sigma_y\rangle = -1$). We assume Bob flips his result when measuring in σ_y to keep perfect correlations in all three bases. It can be further assumed that the key is only established from measurements in the predominately used Z basis, where as the X and Y bases are used to estimate Eve's knowledge of the Z basis measurements.

We will take the case where there have been a large number of signals (N_t) exchanged and measured, which in the asymptotic case will tend to infinitely long keys, and provides a total raw key rate of R_t bits per second. The classical post processing required to establish a reasonably correlated key will include parameter estimation (so as to extract relevant error rates in decoding etc.), and sifting of the results (for example if Bob has not applied a suitable decoding on those items). In the infinite key length limit, the parameter estimation can be achieved with a negligible subtraction of key, and the sifting can be represented by the parameter q, which reduces the raw key rate to R_s, or N_s signals. The secret key rate, K, will then be a product of this raw key rate, and the secret fraction r (the fraction of the raw key that can be said to be secure), such that

$$K = R_\mathrm{s} r = q R_\mathrm{t} r \tag{2.3.10}$$

which is dependent on Eve's information on the raw keys.

This secret fraction is dependent on two processes. The first being error correction (or information reconciliation), a measure of which is provided by the mutual information between Alice and Bob, $I(A:B)$. The second being privacy amplification, a method to destroy Eve's knowledge of the raw key, which can be expressed by $I_E = \min\{I_{AE}, I_{BE}\}$,

where I_{XE} is Eve's information on the raw key of Alice or Bob. This provides the expression [87]

$$r = \max\{I(A:B) - I_E, 0\} \ . \tag{2.3.11}$$

We first consider the I_E term. The symmetries of the six-state protocol and BB84 imply that a security bound can be computed by considering collective attacks (attacks with the use of quantum memories and quantum gate operations) such that the state shared between Alice and Bob is diagonalised along the Bell basis set

$$\rho_{AB} = \lambda_1 \left|\Phi^+\right\rangle \left\langle\Phi^+\right| + \lambda_2 \left|\Phi^-\right\rangle \left\langle\Phi^-\right| + \lambda_3 \left|\Psi^+\right\rangle \left\langle\Psi^+\right| + \lambda_4 \left|\Psi^-\right\rangle \left\langle\Psi^-\right| \tag{2.3.12}$$

with the requirement of $\sum_i \lambda_i = 1$. The states $|\Phi^{\pm}\rangle$ gives perfect correlation in the Z basis, while $|\Psi^{\pm}\rangle$ gives anti-correlations. The quantum bit error rate (QBER), e_z, and the errors rates in the other bases (e_x and e_y) are therefore given by

$$\begin{aligned} e_z &= \lambda_3 + \lambda_4 \\ e_x &= \lambda_2 + \lambda_4 \\ e_y &= \lambda_2 + \lambda_3 \ . \end{aligned} \tag{2.3.13}$$

v For collective attacks the Holveo bound [88] can be used to express Eve's information as

$$\begin{aligned} I_E = I_{AE} &= \max_{\text{EVE}}\{\chi(A:E)\} \\ &= S(\rho_E) - \sum_a \Pr(a) S(\rho_{E|a}) \end{aligned} \tag{2.3.14}$$

where $S(\rho) = -\mathrm{tr}\left[\rho \ln \rho\right]$ is the Von-Neumann entropy, and a represents a symbol of the alphabet used with probability $\Pr(a)$. Here $\rho_{E|a}$ describes Eve's ancillary states associated with each symbol of the alphabet. Since both bit-values (0 or 1) are equiprobable this results in,

$$I_E = S(\rho_E) - \frac{1}{2} S(\rho_{E|0}) - \frac{1}{2} S(\rho_{E|1}) \ . \tag{2.3.15}$$

In this attack Eve is privy to a purification of ρ_{AB},

$$S(\rho_E) = S(\rho_{AB}) = H(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \equiv H(\boldsymbol{\lambda}) \tag{2.3.16}$$

where $H(X)$ is the Shannon entropy, defined as

$$H(X) = -\sum_i \Pr(x_i) \log \Pr(x_i) \ . \tag{2.3.17}$$

Here, purification refers to the fact that for a given mixed state there is some pure state which, when partially traced, will return the given mixed state. To compute $\rho_{E|0,1}$, we first note the explicit purification

$$|\Omega\rangle_{ABE} = \sum_i \sqrt{\lambda_i} \, |\Phi_i\rangle_{AB} \, |e_i\rangle_E \tag{2.3.18}$$

where $|\Phi_i\rangle$ is one of the four Bell states, and $\langle e_i | e_j \rangle = \delta_{ij}$. This is then traced over Bob, and Alice's qubits are projected onto $|\pm z\rangle$ for bit 0 and 1 respectively, resulting in $S(\rho_{E|0}) = S(\rho_{E|1}) = h(e_z)$, where $h(e)$ is the binary entropy function

$$h(e) = -e \log_2(e) - (1-e) \log_2(1-e) \tag{2.3.19}$$

and therefore

$$I_E(\boldsymbol{\lambda}) = H(\boldsymbol{\lambda}) - h(e_z) \ . \tag{2.3.20}$$

For the six-state protocol, both e_x and e_y are measured, and all λ_i are directly determined. Therefore

$$I_E(\boldsymbol{e}) = e_z h\left(\frac{1 + (e_x - e_y)/e_z}{2}\right) + (1 - e_z) h\left(\frac{1 - (e_x + e_y + e_z)/2}{1 - e_z}\right) \tag{2.3.21}$$

which, with the assumption of a depolarising channel, where $\epsilon = e_x = e_y = e_z$, becomes

$$I_E(\epsilon) = \epsilon + (1 - \epsilon) h\left(\frac{1 - 3\epsilon/2}{1 - \epsilon}\right) \ . \tag{2.3.22}$$

The first term in Equation 2.3.11 is the mutual information between Alice and Bob, expressed as $I(A:B) = H(A) + H(B) - H(AB)$. Each bit value has equal probability leading to $H(A) = H(B) = 1$, and the joint entropy term evaluates to $H(AB) = 1 + h(\epsilon)$. This corresponds to the secret fraction of $r = 1 - h(\epsilon) - I_E(\epsilon)$, which tends to 0 for $\epsilon \approx 12.61\%$.

For BB84 only e_y is not measured and therefore is a free parameter which must be chosen so as to maximise Eve's information. This can be calculated by formulating

$$\begin{aligned} \lambda_1 &= (1 - e_z)(1 - u) \\ \lambda_2 &= (1 - e_z)u \\ \lambda_3 &= e_z(1 - v) \\ \lambda_4 &= e_z v \end{aligned} \tag{2.3.23}$$

subject to

$$(1 - e_z)u + e_z v = e_x \tag{2.3.24}$$

where $u, v \in [0, 1]$. This leads to

$$\begin{aligned} H(\boldsymbol{\lambda}) &= h(e_z) + (1 - e_z)h(u) + e_z h(v) \\ \Rightarrow I_E(\boldsymbol{\lambda}) &= (1 - e_z)h(u) + e_z h(v) \end{aligned} \tag{2.3.25}$$

to be maximised under the constraint in equation 2.3.24. The resulting optimal choice is $u = v = e_x$ and therefore $I_E(e) = h(e_x)$. If $e_x = e_z = \epsilon$, the relationships above imply $e_y = 2\epsilon(1 - \epsilon)$. This provides the secret key rate $r = 1 - h(\epsilon) - I_E(\epsilon)$, which tends to 0 for $\epsilon \approx 11\%$.

GLLP proof

The proof of Gottesman, Lo, Lütkenhaus and Preskill (GLLP) [89] is a more general framework for security analysis than described above in Section 2.3.5. In QKD, there are more optimal strategies for an eavesdropper and she can utilise the imperfections of the devices in the system to gain information about the key. It is assumed that the quantum

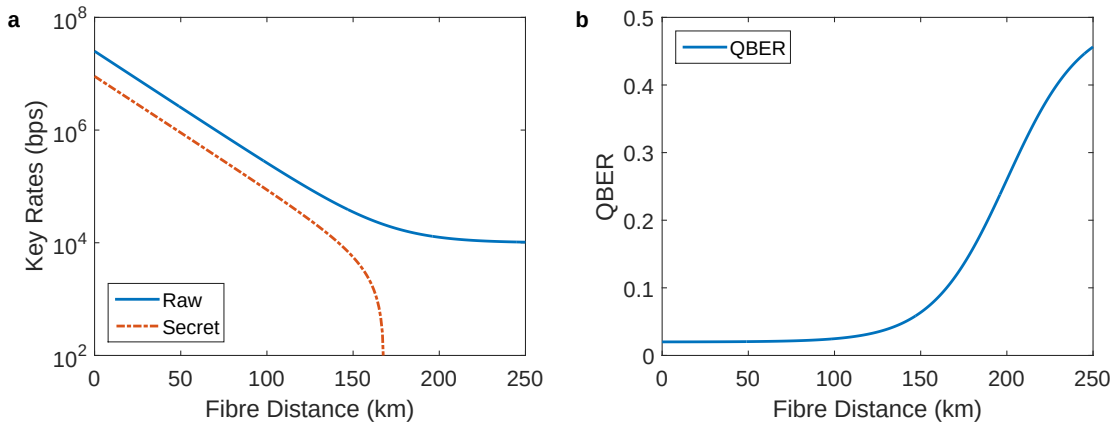

Figure 2.11: **Secret Key Rates:** Example plot of secret key rates verses distance, based on 0.2 dB/km, 6 dB receiver loss, 10% efficient detectors with 10 kHz dark counts, for a 1 GHz systems with a base error of 2% for state preparation and measurement, along with perfect error correction. Plotted are (a) the raw key rates including the fixed dark counts, the secret key rate that drops to 0 around 150 km, and (b) the quantum bit error rate which tends to 50% when there is a low signal to noise ratio.

channel is "noisy" and any of the resulting errors must be attributed to Eve as she could, in theory, replace the channel with a quieter, less lossy one and reintroduce the noise and loss when eavesdropping. Alice's source is also not an ideal photon source and all multi-photon terms emitted can be intercepted by Eve and used to gain information. Finally, if Bob's detectors are non-ideal, Eve could modify Bob's detector efficiency and attack the channel such that Bob sees no change in detector performance.

GLLP formulated an expression for the maximum key generation rate

$$K = \nu_s \max\left\{(1-\Delta) - h(\epsilon) - (1-\Delta)h\left(\frac{\epsilon}{1-\Delta}\right), 0\right\} \tag{2.3.26}$$

where ν_s is the repetition rate, Δ is the probability a qubit is *tagged* (a qubit that is to have leaked information to Eve), ϵ is the QBER, and h is the binary Shannon entropy function. The equation can be rewritten in measurable parameters so that

$$K \geq q\nu_s\Big\{-Q_\mu h\left(\epsilon_\mu\right) + Q_1\left[1 - h\left(e_1\right)\right]\Big\} \tag{2.3.27}$$

where q is the sifting factor, Q_μ is the signal gain, or fraction of detection events given Alice transmits a signal state, and ϵ_μ is the QBER of the signal states. Q_1 and e_1 represent

the gain and error rate of single photon events, where Q_1 is calculated as

$$Q_1 = Y_1 \mu \mathrm{e}^{-\mu} \ , \tag{2.3.28}$$

where Y_1 is the single photon yield, or the probability that Bob will make a single photon detection measurement given that Alice emits one photon, and μ is the average photon number of the weak coherent source. For non-decoy BB84 [90] this becomes

$$Q_1 = Q_\mu - p_\mathrm{M} \tag{2.3.29}$$

where p_M is the probability of Alice sending a multi-photon state, $p_\mathrm{M} = 1 - (1+\mu)\mathrm{e}^{-\mu}$. This gives the error rate of a single photon state

$$e_1 = \frac{Q_\mu \epsilon_\mu}{Q_1} \ . \tag{2.3.30}$$

By substituting these expressions the resulting equation for the rate is

$$K \geq q\nu_s \left\{ -Q_\mu h(\epsilon_\mu) + (Q_\mu - p_\mathrm{M}) \left[1 - h\left(\frac{Q_\mu \epsilon_\mu}{Q_\mu - p_\mathrm{M}} \right) \right] \right\} \ . \tag{2.3.31}$$

With this expression, we can find the optimal mean average photon number and secret key rate, given the characteristics of the transmitter and receiver (See Figure 2.12).

Biased Basis

Improvements to the available key rate can be achieved by biasing the basis choice that limited the inherent efficiency of the BB84 protocol to 50%. Ardehali *et al.* [91] noted that if Alice and Bob use a pre-chosen bias to one of the bases, their measurement will agree more frequently than 50%, but this bias could be exploited by Eve. To combat this issue instead of comparing the QBER for the entire transmission, Alice and Bob must compare the QBER separately for each basis.

If we consider the case where Alice and Bob choose the two bases with probability p and $1-p$, where $0 < p < \frac{1}{2}$, Eve's optimal strategy is to eavesdrop on the more likely

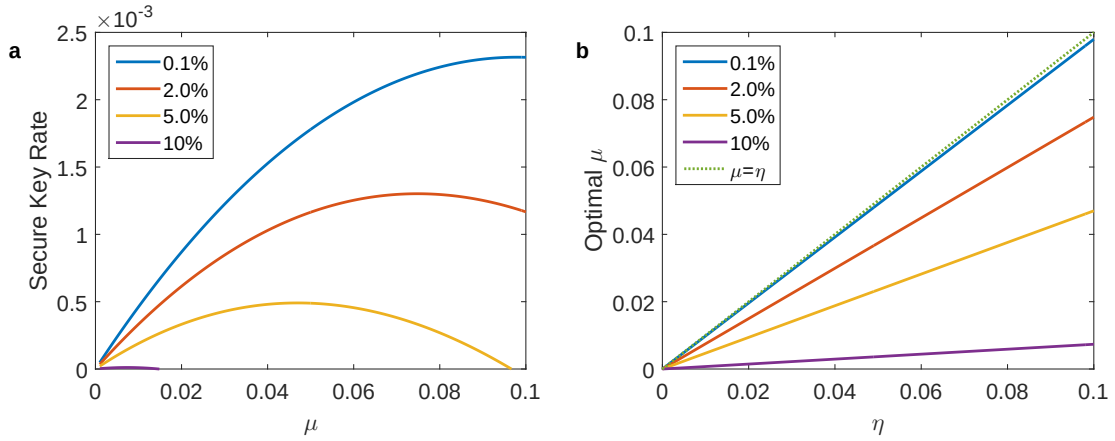

Figure 2.12: **GLLP rates and optimal μ:** (a) A graph of the rate (per transmitted bit) of BB84 for various photon numbers indicating there is an optimum value of μ dependent on the system parameters. In this example the yield is 10%. This is calculated from the GLLP proof. (b) The optimal mean photon number, μ, depends on the yield, η, and the QBER, however $\mu < \eta$.

basis. This would introduce an error of

$$\epsilon = \frac{p^2}{2[p^2 + (1-p)^2]} \tag{2.3.32}$$

under normal error checking conditions, which, in the case where p asymptotically tends to 0, would result in a negligible error contribution.

If, however, the QBER is calculated for each basis separately, the QBER in the $1-p$ probability basis will be 0, as Eve is measuring in the correct basis and can send on the correct state. In the p probability basis she will be measuring in the incorrect basis, and will therefore introduce 50% QBER, which is consequently detectable.

As p tends towards 0, the number of bits available to estimate the error on the second basis decreases and thus Eve has a better opportunity to eavesdrop undetected. It was therefore shown that the optimal p scales with key length [92]

$$p = \mathcal{O}\left(\sqrt{\frac{\log k}{N}}\right) \tag{2.3.33}$$

where k is the length of the final key and N is the number shared qubits. Therefore in the infinite key length analysis, as $N \to \infty$, the probability can tend to 0.

BB84 with Decoy State

A further approach to increase data rates and range is decoy state encoding, where the states are phase randomised and a number of intensity levels are used. These intensity levels are chosen at random by Alice, which limits the optimal attacks Eve can implement. It has been shown that using a signal intensity (μ) and two decoy levels (ν_1 and ν_2) is sufficient [62] where $\mu > \nu_1 > \nu_2$. This allows for the security rate to be calculated as

$$K_{\mathrm{BB84}} = q\nu_s\Big\{ - Q_\mu f_{\mathrm{EC}}(\epsilon_\mu)h(\epsilon_\mu) + Q_1^{\mathrm{L}}\big[1 - h(e_1^{\mathrm{U}})\big]\Big\} \tag{2.3.34}$$

where $q = \frac{1}{2}(\frac{N_\mu}{N_{\mathrm{t}}})$. Here N_μ is the number of μ intensity signals measured, and N_{t} is the total number counts. The $\frac{1}{2}$ is the sifting factor of standard BB84, and ν_s is the repetition rate. We now include $f_{\mathrm{EC}}(\epsilon_\mu) \geq 1$, the error correction efficiency, $h(x)$ is the binary Shannon entropy, and Q_μ and ϵ_μ are the transmission probability (gain) and QBER respectively of a pulse with the signal intensity μ [62, 93].

The remaining quantities Q_1^{L} and e_1^{U} are estimated in the following manner. The lower bound of the single photon transmittance, Q_1, represents the probability that a transmitted state contains just a single photon and that the receiver detects just a single photon, and is calculated to be

$$Q_1 \geq Q_1^{\mathrm{L}} = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}\left[Q_{\nu_1}\mathrm{e}^{\nu_1} - Q_{\nu_2}\mathrm{e}^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu \mathrm{e}^{\mu} - Y_0^{\mathrm{L}})\right] \tag{2.3.35}$$

where Q_i is the transmission probability of a pulse with the intensity $i \in \{\mu, \nu_1, \nu_2\}$, μ represents the signal state intensity, and (ν_1, ν_2) are the two decoy state intensities (weak and vacuum). Y_0^{L} is the lower bound for the count probability of an empty pulse, obtained from

$$Y_0 \geq Y_0^{\mathrm{L}} = \frac{\nu_1 Q_{\nu_2}\mathrm{e}^{\nu_2} - \nu_2 Q_{\nu_1}\mathrm{e}^{\nu_1}}{\nu_1 - \nu_2}\ . \tag{2.3.36}$$

Finally, the QBER for each intensity is represented as e_i and the upper bound for the single photon QBER, e_1, is given by

$$e_1 \leq e_1^{\mathrm{U}} = \frac{\mu}{\nu_1 - \nu_2}\frac{e_{\nu_1}Q_{\nu_1}\mathrm{e}^{\nu_1} - e_{\nu_2}Q_{\nu_2}\mathrm{e}^{\nu_2}}{Q_1^{\mathrm{L}}\mathrm{e}^{\mu}}\ . \tag{2.3.37}$$

The effects of error correction and privacy amplification are considered without finite key analysis and assumes the measured values are perfect, unbiased estimates taken over an infinite sample size. Finite effect have been analysed in many different settings [2,94–96].

Finite Bound

The issue that arises in the previous protocol security proofs is that they require estimates of various experimental parameters. They are assumed to be perfect unbiased estimates calculated by sampling an infinitely long key, but in practice they are estimated using a small subset of the sifted key. In the decoy state BB84 the amount of privacy amplification necessary for an unconditionally secure key will therefore need an upper bounded QBER and a lower bound on the single photon yield.

The Devetak and Winter [94] formulation of conditional entropies expresses the secure fraction as

$$r = S(A \mid E) - H(A \mid B) \tag{2.3.38}$$

where $S(x|y)$ and $H(x|y)$ are the conditional von Neumann entropy and Shannon entropy, representing the mutual information held by Alice and Eve, and Alice and Bob respectively.

In the infinite key regime N_t tends to infinity and the sifting factor, q, can tend to 1 which leads to [2]

$$\lim_{N_\mathrm{t}\to\infty} K = qR_\mathrm{t}r = R_\mathrm{t}\big\{S(A \mid E) - \mathrm{leak}_\mathrm{EC}\big\} \tag{2.3.39}$$

where

$$S(A \mid E) = Y_1\left[1 - h\left(\frac{\epsilon}{Y_1}\right)\right] \tag{2.3.40}$$

and

$$Y_1 = 1 - \left(\frac{\nu_s q}{R_\mathrm{t}}\right) p_\mathrm{M}\ . \tag{2.3.41}$$

Here $\mathrm{leak}_\mathrm{EC} = f_\mathrm{EC}(\epsilon)h(\epsilon)$ is the amount of information leaked from the process of error correction, ϵ is the total QBER, and p_M is the proportion of Alice's pulses containing more than one photon.

In the finite key regime, the issue is to express the conditional entropy between Alice

and Eve, $S(A \mid E)$, in terms of a security parameter [95] describing the precision to which it is estimated. This results in

$$K = R_{\mathrm{s}} \left\{ S_{\xi}(A \mid E) - \Delta - \mathrm{leak}_{\mathrm{EC}} \right\} \tag{2.3.42}$$

where we now include the effects of sifting, $S_{\xi}(A \mid E)$ is the estimate of Eve's information, and

$$\Delta = 7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{N_{\mathrm{s}}}} + \frac{2}{N_{\mathrm{s}} \log_2\left(\frac{1}{\varepsilon_{PA}}\right)} \tag{2.3.43}$$

where $\bar{\varepsilon}$ is the security parameter associated with the parameter estimation, ε_{PA} is the security parameter associated with privacy amplification, and N_{s} is the length of the sifted key. The leakage of information due to error correction depends on the procedure and technique used.

For BB84 without decoy states, the conditional entropy can be expressed [96]

$$S_{\xi}(A \mid E) = \tilde{Y}_1 \left[1 - h\left(\tilde{e}_1\right)\right] \tag{2.3.44}$$

where the estimate for single photon bit error rate is

$$\tilde{e}_1 = \frac{\epsilon}{\tilde{Y}_1(\mu)} \tag{2.3.45}$$

and the single photon yield is

$$\tilde{Y}_1(\mu) = \frac{1 - p_{\mathrm{M}}}{R_{\mathrm{t}}} \ . \tag{2.3.46}$$

This presents an issue, in that short finite key sizes result in a negative secure key rate (for $N_{\mathrm{s}} \lesssim 10^5$) [95] and tend to the asymptotic infinite key rate for large key sizes (for $N_{\mathrm{s}} \gtrsim 10^{10}$). Much work has focussed on improving these techniques and providing the most efficient schemes [97, 98].

In this subsection we have highlighted some of the standard approaches, problems, and solutions for proving the security of quantum key distribution. We sketched the proof for an infinite bound for single photon BB84 protocols and the GLLP proof, incorporating more realistic assumptions about the physical implementation. We discussed how to

improve these rates by biasing the basis choices and mitigate multi-photon terms from weak-coherent states by including decoy-states. Finally, we highlight the issue of finite-key analysis and understanding the limitations of estimating parameters without infinite sampling. In this thesis we will specify the security proof used to analyse the performance of our devices.

2.3.6 Other Protocols

Due to issues in security, rates, practicality, and limitation in distance a number of other protocols have been proposed, implemented and researched.

Reference Frame Independent QKD

One development in experimental feasibility of QKD in certain environments is Reference Frame Independent (RFI) QKD. The scheme tolerates an unknown and slowly varying phase between logical states. This protocol allows for the misalignment of uncalibrated reference frames of Alice and Bob and addresses a limitation of standard QKD protocols. This indicates that the real world imperfections and the impracticality of calibrating mobile devices can be overcome to allow the adoption of quantum technologies in portable systems [99].

The Z axis is assumed to be aligned, but the X and Y axes can vary in time with the expressions of

$$\begin{aligned} X_B &= \cos(\beta)\, X_A + \sin(\beta)\, Y_A \\ Y_B &= \cos(\beta)\, Y_A - \sin(\beta)\, X_A \\ Z_B &= Z_A \end{aligned} \tag{2.3.47}$$

where β can vary slowly with time.

The raw key is generated from the cases in which both Alice and Bob measure in the Z basis. The QBER is defined as

$$\epsilon = \frac{1 - \langle Z_A Z_B \rangle}{2} \,. \tag{2.3.48}$$

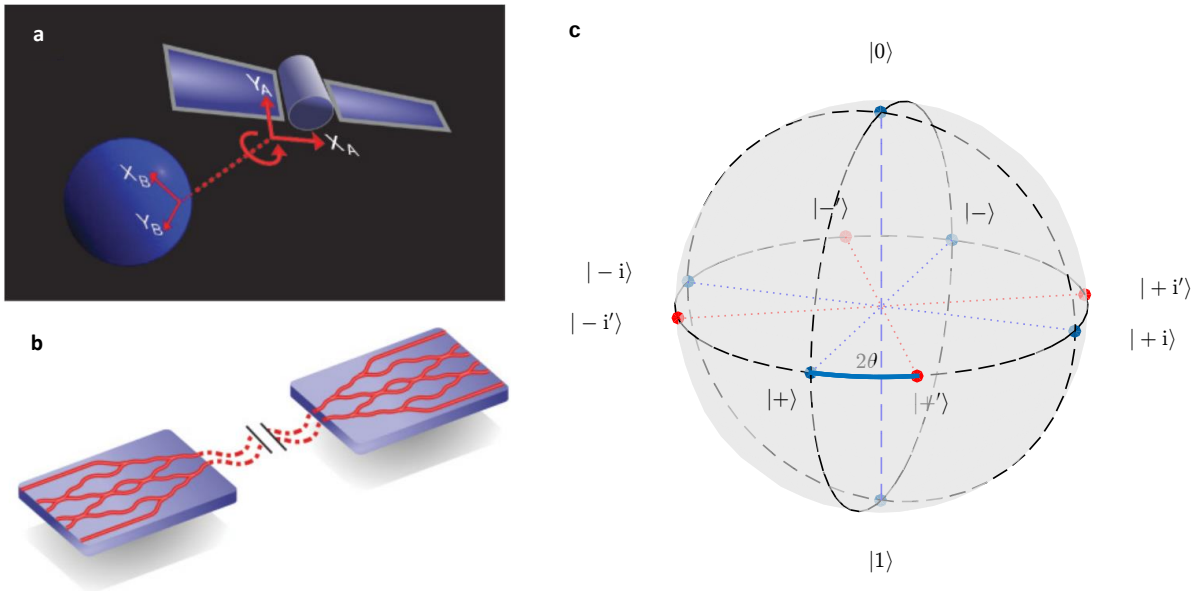

Figure 2.13: **Reference Frame Independent-QKD:** (a-b) Practical Examples in which RFI QKD can improve performance on otherwise prohibitive examples such as a geosynchronous satellite communications in which the rectilinear polarisations are not agreed upon, but the right and left circularly polarised light it agreed. And path encoded qubits in an integrated photonic device where the path length in the two connections may vary in the scale of the wavelengths. This would allow agreement on $|0\rangle$ and $|1\rangle$ states, but not superpositions of these states. (c) The Bloch Sphere diagram illustrates both Alice and Bob's axes and the misalignment of X and Y. The Z axis is assumed to remain aligned, and can represent the right and left circular polarisation between a geosynchronous satellite and a ground station.

There is then a bound on Eve's knowledge that is evaluated by calculating the value C, which is independent of the angle of rotation.

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2 \quad . \tag{2.3.49}$$

This practical solution allows secure communications in several otherwise prohibited examples, such as between the Earth and geosynchronous satellites where linear polarisation states can vary due to the rotation of the satellite, and with path encoded qubits between two integrated photonic devices with wavelength-scale changes in relative path lengths. RFI maintains a non-zero secret key fraction for all rotation angles. In comparison, BB84 and other protocol key rates can drop to 0 for certain misalignment in the reference frames of Alice and Bob [11, 100, 101].

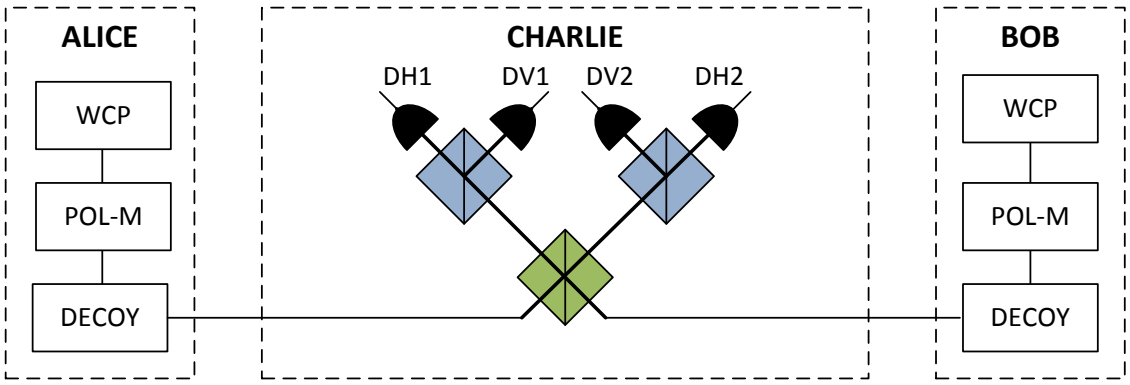

Figure 2.14: **Measurement-Device-Indepenedent (MDI) QKD:** Alice and Bob prepare phase randomised weak coherent pulses (WCP), that are then polarisation encoded in the four BB84 states at random (POL-M), with decoy states generated with an intensity modulator (DECOY). The measurement device (CHARLIE), performs a Bell-state measurement on the two states arriving, by interfering the signals on a 50:50 beam splitter before polarising beam splitters project the input photons in to the horizontal and vertical bases. The 4 single photon detectors are used to detect photons and publicly announces successful Bell state measurements, corresponding to two detector events in orthogonal polarisation being triggered. A click in DH1 and DV2, or in DV1 and DH2, indicates a projection into the Bell state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$, while a click in DH1 and DV1, or in DH2 and DV2 , reveals a projection into the Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$, but does not reveal information about the key, allowing the measurement device to become untrusted.

Measurement Device Independent QKD

To mitigate attacks on the vulnerabilities of single photon detectors discussed in section 2.3.4 there are a number of ad-hoc techniques to incorporate counter-measures and security patches to limit how the vulnerabilities can be exploited. An alternative method is to introduce new protocols that no longer depend on the detectors to act in an ideal way.

This is known as Measurement Device Independent quantum key distribution (MDI QKD) [102], where the two parties, Alice and Bob, can use untrusted measurement devices that could be operated and manufactured by Eve (as illustrated in Figure 2.14). Both Alice and Bob prepare quantum signals, transmitting them to this untrusted measurement device, or relay, known as Charlie (that could be under Eve's control). He then projects the received signals on to Bell-states (Bell-state measurements). Alice and Bob can verify

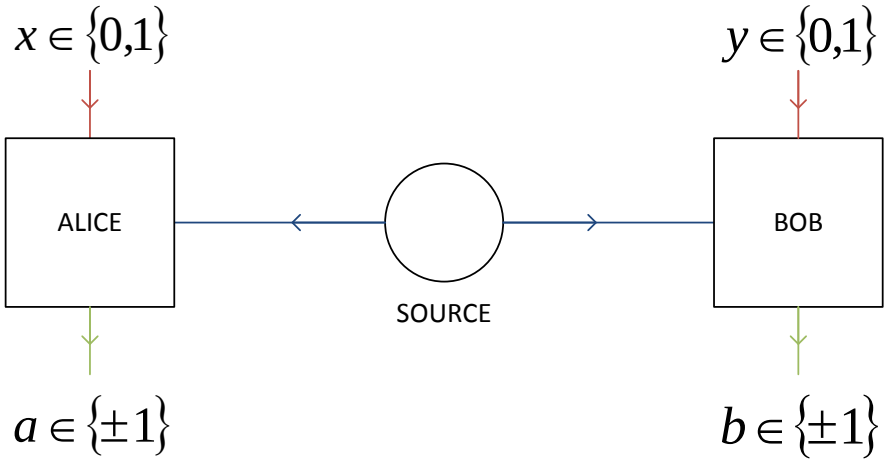

Figure 2.15: **Device-Independent QKD:** based on Bell's inequality, but requires a loophole-free implementation of the test, to remove the assumption of trust for any of the devices. A source sends entangled pairs to Alice and Bob who treat their equipment as black boxes. There is a randomly chosen basis measurement and they retrieve correlated results using loophole free Bell test to asses the presence of Eve on the quantum channel.

Charlie's honesty on a subset of the transmitted data, but he also holds no information about the key from the results of the measurements itself. It has been demonstrated experimentally [103, 104], but still requires the assumption of trust in the sources.

Device Independent QKD

The full approach to security involves removing all assumption over the source and measurement devices, known as Device-Independent (DI) QKD [105]. Here, Alice and Bob treat their devices as black boxes, so that they do not need to fully characterise the different elements. The security of DI-QKD relies on a violation of Bell's inequality, which certifies the presence of non-classical quantum correlations (see Figure 2.15). The drawback of this method is the requirement for loop-hole free Bell measurements, which has only recently become experimentally feasible (still at extraordinarily low rates for communication purposes) [106].

Issues including detection efficiency (that are required to be above 80% to overcome the detection efficiency loophole) and channel loss renders DI-QKD currently impractical. Attempts to compensate for the channel loss by including fair sampling qubit amplifiers or quantum non-demolition measurements on the number of photons in a pulse still leave the resulting secret key rates low at practical distances [107, 108].

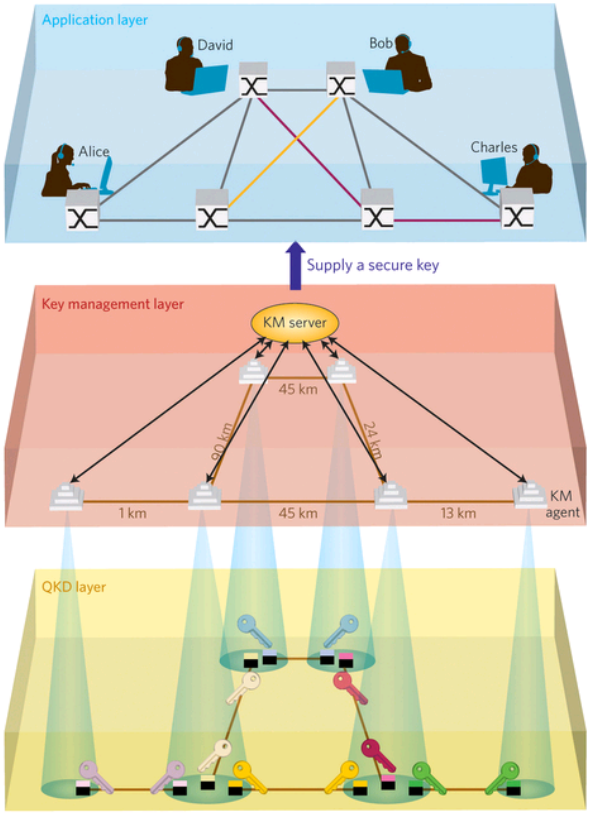

Figure 2.16: **Tokyo QKD Network:** Schematic of the Tokyo QKD network layer structure [109]. This network was based on the trusted node architecture, and implemented the hardware so that the key management layer and QKD layer could be accessed by the users' as black boxes. The encryption keys that these layers provided were used to secure video meetings and smart phone communication.

Quantum Networks

Further to this development of other protocols to extend the security, rates or practicality in point-to-point communication, there have also been a number of demonstrations of QKD in network scenarios. These include the

1. **DARPA** A 10-node DARPA quantum network running from 2004 in USA developed by BBN Technologies, Harvard University, Boston University and QinetiQ [110].

2. **SECOQC** The Secure Communication Based on Quantum Cryptography network used 200 km of standard fibre optic cable to connect six locations in Vienna in 2008. It was the first computer network secured by QKD [111].

3. **SwissQuantum** was deployed in the Geneva metropolitan area in 2009 to validate

the robustness and reliability of continuous operation QKD over a long time period in a field environment [112].

4. **Tokyo QKD Network** was developed in 2010 and involved an international collaboration of research groups and industry, securing 6 nodes using a number of different communication protocols and devices [109].

5. **Los Alamos National Laboratory** have operated a hub-and-spoke network, based on trusted node network architecture, since 2011. Each node contains a laser based transmitter but only the one common hub receives quantum messages. This also demonstrated the QKard technology, miniaturising the transmitter photonics to matchbox sizes [113].

At time of writing a long range network in China is also currently in the process of deployment [114–116] and the UK is developing metro-scale networks in Bristol and Cambridge to be connected via a quantum backbone network.

Further approaches to the network capability of QKD have been appearing, including the development of trusted node scenarios [117], Quantum Access Networks [118], Software-defined quantum networks [119, 120], and also securing network function virtualisation controllers with QKD [121].

Quantum Repeaters

With imperfect sources, channel loss, and non-ideal detectors, there is a limit to the length of an unconditionally secure quantum channel. As the channel attenuation increases, the more signal photons are lost due to random scattering and absorption, while the sources of noise (dark counts, and background radiation) remain roughly constant, thus reducing the signal to noise ratio. At some distance this ratio is too small and compromises the transmission (as all errors are considered to be the effects of eavesdropping).

To overcome this issue there have been proposals utilising the process of entanglement swapping [122], wherein Alice and Bob can each share an entangled pair with a third party, Charlie, who in turn can perform measurements on his particles. This results in Alice and Bob's particles becoming entangled (see Figure 2.17).

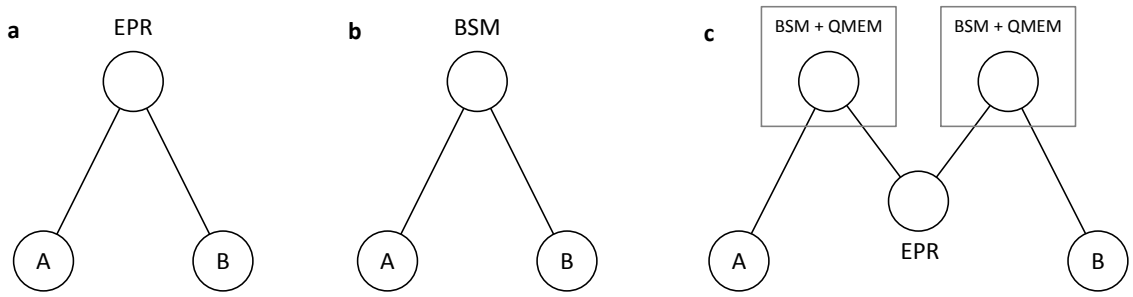

Figure 2.17: **Quantum Repeater Architectures:** (a) EPR based QKD. (b) Measurement-Device Independent QKD based on bell state measurements to project on entangled states. (c) Quantum repeater extending the distance of quantum networks, by sharing entanglement, using quantum memories to store the quantum states.

The issue of perfect sources and detectors would still remain in entanglement swapping, and therefore distance and rates limitations would still apply. However, it has been shown that weak sources of entanglement can be "distilled" into stronger entanglement at the expense of more pairs of photons, through local operations and classical communications [123].

Further expense is needed to allow arbitrarily long lengths of communication channels between two nodes, as they may not establish entanglement at the same time. This synchronisation is therefore implemented through quantum memories, until neighbouring nodes are ready to perform the necessary operations [124]. This complete procedure describes the essential steps for *quantum repeater technology* [125].

Such quantum repeating technology could be the DLCZ protocol [126], utilising atomic ensembles as quantum memories and reasonably simple photonic circuits for processing. The efficiency of this protocol scales inversely with distance, compared to the non-repeating exponential scaling.

Other approaches have been proposed such as all-photonic repeaters [127], solid state systems [128], and the inclusion of both loss tolerance and quantum error correction in to the process [129].

2.4 Integrated Photonics

So far we have reviewed the limitations of current cryptographic methods and the threat that quantum technologies pose. Quantum Key Distribution has been introduced, discussing a number of protocols and the physical implementations of sources, channels and detectors. Common methods of attacking these systems have been presented, along with the relevant techniques to assess the security of the communication and mitigate these risks. Finally, we have discussed some recent developments in the community towards greater levels of security through MDI-QKD and DI-QKD, and the progress towards implementing QKD in network scenarios and increasing the range of communication through quantum repeater architectures.

To implement the quantum communication schemes described in Section 2.3, photons are commonly used as conveyors of quantum information or qubits. We are therefore required to generate photons, encode information in some degree of freedom, understand methods of manipulating single photons, and finally detect the information.

2.4.1 Photon Sources

We first present methods of generating photons used in quantum key distribution. To understand the photons used in a quantum mechanical setting, there needs to be an appropriate description of the quantum nature of light.

Quantum Sates of Light

Single Photons and Fock States The quantised free electromagnetic field is described as a collection of harmonic oscillators, where each field has an energy corresponding to the number of photons in the given state [130]. This can be described in the Fock basis of photonic states [131], where n photons in a given mode, i, is written as $|n\rangle_i$. Each photon number state is an energy level of the quantised harmonic oscillator and therefore

creation and annihilation operators $a^\dagger$ and a can be defined as

$$\begin{aligned} a_i^\dagger \left|n\right\rangle_i &= \sqrt{n+1}\left|n+1\right\rangle_i \\ a_i \left|n\right\rangle_i &= \sqrt{n}\left|n-1\right\rangle_i \\ a_i \left|0\right\rangle_i &= 0\ . \end{aligned} \tag{2.4.1}$$

The state $\left|n\right\rangle_i$ is an eigenstate of the number operator $\hat{N}_i = a_i^\dagger a_i$, with the eigenvalue n_i corresponding to the number of photons. If multiple modes are to be considered, the total number of photons $\hat{N} = \sum_i \hat{N}_i$ is the sum of the number of photons in each mode. The creation and annihilation operators fulfil the commutation relation $\left[a_i, a_j^\dagger\right] = a_i a_j^\dagger - a_i^\dagger a_j = \delta_{ij}$.

Any Fock state can also be written as a function of the vacuum state, in the form

$$\left|n\right\rangle_i = \frac{1}{\sqrt{n!}} a_i^{\dagger n} \left|0\right\rangle \tag{2.4.2}$$

where photons can be added or removed from it using the creation and annihilation operators acting on the mode.

A more general description denotes that the vacuum is composed of orthogonal vectors spanning the spatial, polarisation, spectral and temporal configurations. It is therefore a tensor product over all the vacuum modes spanning an infinite basis space, but in practice we assume a number of discrete spatial modes where the photon's transverse spatial shape is assumed to be localised in a single mode, such as

$$\left|\Psi\right\rangle = \int dt\, \phi(t)\, a_t^\dagger\ \left|0\right\rangle \tag{2.4.3}$$

where $\phi(t)$ is the normalised temporal shape of the single photon, $a_t^\dagger$ is the creation operator at the time t, in the mode a defined by single spatial mode, and $\left|0\right\rangle$ is the vacuum (the infinite tensor product spanning all possible times in the spatial mode).

Coherent States Laser light is fundamental to photonic experiments and devices in both the quantum and classical regime. The coherent state of light $\left|\alpha\right\rangle$ is the description of

the classical optical wave in the quantised theory of light. It is defined as the eigenvector of the annihilation operator with an associated eigenvalue α corresponding to the field amplitude,

$$a\left|\alpha\right\rangle = \alpha\left|\alpha\right\rangle \ . \tag{2.4.4}$$

The coherent state is a superposition of multiple photon numbers, corresponding to a Poissonian distribution, centred around the average number of photons and is defined in the Fock basis as:

$$\left|\alpha\right\rangle = \sum_{n=0}^{\infty} b_n \left|n\right\rangle \ . \tag{2.4.5}$$

This produces

$$\sum_{n=0}^{\infty} b_{n+1}\sqrt{n+1}\left|n\right\rangle = \alpha \sum_{n=0}^{\infty} b_n \left|n\right\rangle \tag{2.4.6}$$

and so $b_{n+1} = \frac{\alpha}{\sqrt{n+1}} b_n$ for $n \geq 0$. This recursive equation leads to

$$b_n = \frac{\alpha^n}{\sqrt{n!}} b_0 \tag{2.4.7}$$

and therefore

$$\left|\alpha\right\rangle = b_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \left|n\right\rangle \ . \tag{2.4.8}$$

Imposing the normalisation condition $\langle\alpha|\alpha\rangle = 1$ gives

$$\frac{1}{\left|b_0\right|^2} = \sum_{n=0}^{\infty} \frac{\left|\alpha\right|^{2n}}{n!} = \mathrm{e}^{|\alpha|^2} \tag{2.4.9}$$

and by choosing the arbitrary global phase to be real, the coherent state is therefore given by

$$\left|\alpha\right\rangle = \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \left|n\right\rangle \ . \tag{2.4.10}$$

Single Photon Emitters

An ideal single photon source would output one — and only one — photon on demand in a pure quantum state. This requires the spectrum of the source to be identical each time it is triggered and the photon to be in a superposition of all the spectral components,

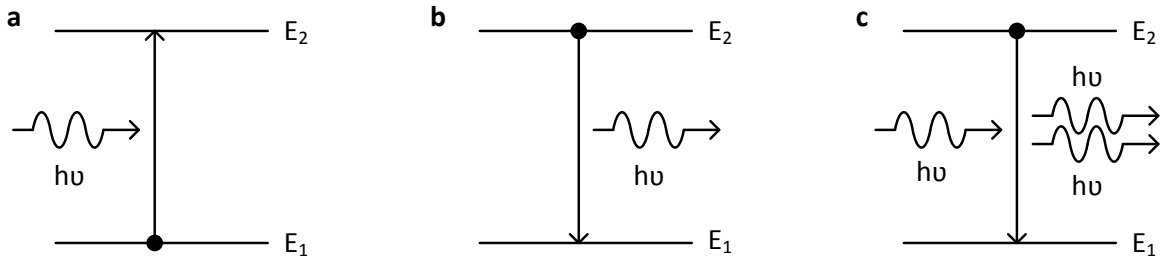

Figure 2.18: **Spontaneous and Stimulated Emission:** (a) Absorption, where a photon excites an electron in to a higher energy state. (b) Spontaneous emission, where an electron is in an excited state and spontaneous decays to a ground state releasing energy as a single photon. (c) Stimulated emission where an electron is in an excited state and is forced to decay by an incoming photon, releasing another photon in phase with the first.

rather than a statistical mixture, which is achieved when the temporal shape of the photon emitted matches the Fourier transform of its spectrum (Fourier limited).

Single photons can be generated in a number of ways, such as atomic systems emitting photons from discrete energy level transitions (see Figure 2.18 (b)), molecular based sources [132], quantum dots [133,134], and crystal colour centres [135,136]. Challenges in these systems include generating truly indistinguishable photons in pure states and with near unit light extraction efficiency [137, 138]. Solutions include engineering resonant structures, coupled to the required emitter, to force the decay of the photon in to a preferred mode [139].

These systems are in contrast to coherent states or classical fields which contain multi-photons, generated in a laser by stimulated emission (see Figure 2.18)

Photon Correlation Measurements Photon correlation measurements can provide information about the qualities of photon emission. The Hanbury, Brown, and Twiss (HBT) experiment [140] sends photons into a 50:50 beam splitter with detectors at the outputs of the two modes (see Figure 2.19 (a)). This allows photons that are closely separated in time to be detected independently. If two photons arrive at time t and $t+\tau$, this corresponds to a measurement of the second-order quantum correlation function

$$G^{(2)}(t, t+\tau) = \mathrm{tr}\left[\rho \hat{E}^{-}(t)\hat{E}^{-}(t+\tau)\hat{E}^{+}(t+\tau)\hat{E}^{+}(t)\right] \tag{2.4.11}$$

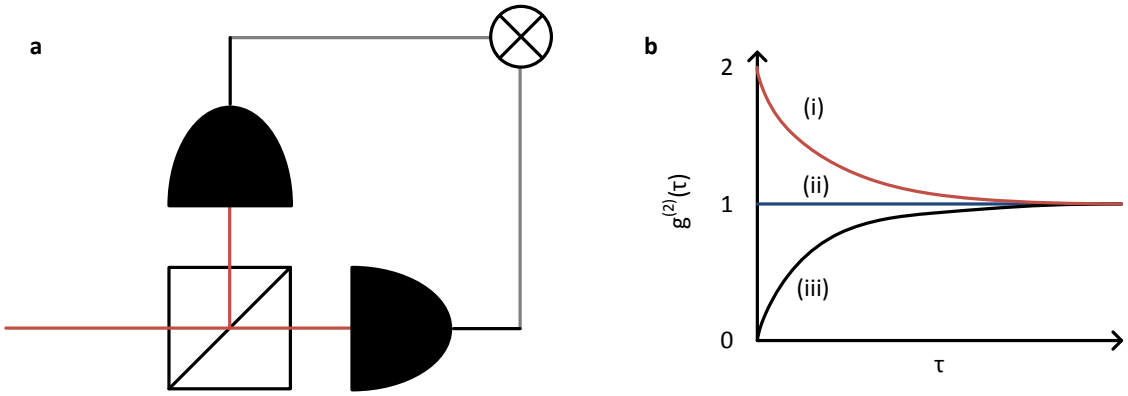

Figure 2.19: **HBT and Photon Statistics:** (a) A schematic diagram of the Hanbury, Brown, and Twiss experiment, one the photon source is placed incident on a 50:50 beam splitter, with the two output modes sent to single photon detectors. The correlation of the photon counting is recorded as a function of time. (b) The $g^{(2)}(\tau)$ function for (i) super-Poissonian statistics (ii) Poissonian statistics and (iii) sub-Poissonian statistics.

where tr [ ] is the trace function, $\hat{E}^{+} \propto a \exp[\mathrm{i}(\omega t - \mathbf{k}\cdot\mathbf{r})]$ and $\hat{E}^{-} \propto a^{\dagger} \exp[-\mathrm{i}(\omega t - \mathbf{k}\cdot\mathbf{r})]$ are the creation and annihilation field operators, and ρ is the input photon state. Ignoring initial transient effects of the light source, without loss of generality the time t can be set to 0 and one can normalise the $G^{(2)}$ measurement with respect to the first order correlation function

$$g^{(2)}(\tau) = \frac{G^{(2)}(\tau)}{|G^{(1)}(0)|^2} \tag{2.4.12}$$

where the first order correlation function is defined as $G^{(1)}(t,t') = \mathrm{tr}\left[\rho\hat{E}^{-}(t)\hat{E}^{+}(t')\right]$.

For completely uncorrelated photon arrivals, the second order correlation function is the product of two first-order correlations functions $G^{(2)}(\tau) = |G^{(1)}(\tau)|^2$ and has no temporal characteristics for τ. These uncorrelated photon detector events result in a second order correlation function of $g^{(2)}(\tau) = 1$ (see Figure 2.19 (b) ii). With each photon acting as independent particles, this leads to Poissonian statistics (such as the coherent states described in Section 2.4.1).

For a number state ($\rho = |n\rangle\langle n|$) [141], the second order correlation function is:

$$g^{(2)}(0) = 1 - \frac{1}{n} \tag{2.4.13}$$

and with a single photon source ($n = 1$), the $g^{(2)}$ value vanishes to zero; a result that

cannot be reproduced using classical wave theory. Observing this coincidence rate provides a signature of the quantum nature of the light source. A $g^{(2)}$ value below one indicates sub-Poissonian statistics, where the variance of the photon number distribution is smaller than for the Poissonian distribution of the coherent state.

The coherence of the light is not maintained for an infinite time, and the mode is repopulated, and therefore the time dependence of the $g^{(2)}$ tends to one (uncorrelated photon detector events). Since there is a tendency for photon events to be spaced in time, these are *anti-bunched photons* (see Figure 2.19 (b) iii).

For single mode thermal states

$$\rho = \sum_{n=0}^{\infty} P_n \left|n\right\rangle \left\langle n\right| \tag{2.4.14}$$

with

$$P_n = 1 - \exp(-\frac{\hbar\omega}{k_B T}) \exp(-\frac{n\hbar\omega}{k_B T}) \tag{2.4.15}$$

the $g^{(2)}(0) = 2$. This enhanced coincidence count rate is associated with super-Poissonian statistics, and indicates *photon bunching* (see Figure 2.19 (b) i).

Parametric Sources

While ideal single photon emitter sources are actively pursued in research, the backbone of quantum information experiments performed in the last two decades are intrinsically non-deterministic, but provide pairs of photons with high yield using spontaneous parametric down conversion (SPDC) [142–145] and more recently spontaneous four wave mixing (SFWM) [146, 147].

These are second and third order non-linear optical processes that occur when an electric field, $\mathbf{E}$, with a high amplitude propagates in a non-linear optical medium, such as a laser in a non-linear crystal or a silicon waveguide. The polarisation field in the medium, $\mathbf{P}$, is a function of the electric field, such that

$$\frac{\mathbf{P}}{\epsilon_0} = \chi^{(1)}\mathbf{E}(t) + \chi^{(2)}\mathbf{E}^2(t) + \chi^{(3)}\mathbf{E}^3(t) + \ldots \tag{2.4.16}$$

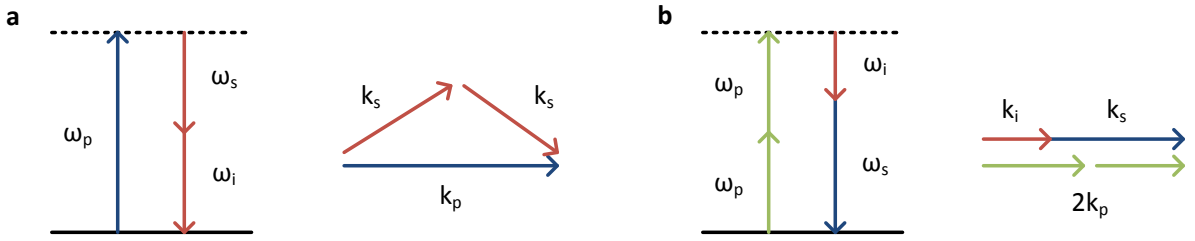

Figure 2.20: **Parametric Down Conversion and Four Wave Mixing:** (a) Spontaneous parametric down conversion, where one high energy photon is spontaneously converted to two lower energy photons of equal energy. (b) Spontaneous four wave mixing, where two photons are spontaneously converted to two other photons, where the sum of the two pump photons equal the signal and idler photon energies.

where $\chi^{(n)}$ is the n^{th} order material susceptibility. The amplitude of each component depends on the centrosymmetry of the crystal medium, where only if the material is non-centrosymmetric would a $\chi^{(2)}$ term be non-zero. If the medium is centrosymmetric, $\mathbf{P}(-\mathbf{E}) = -\mathbf{P}(\mathbf{E})$, the $\chi^{(2n)}$ terms will all be zero.

Spontaneous Parametric Down Conversion SPDC uses the $\chi^{(2)}$ non-linear coefficient to generate pairs of photons (the "signal" and "idler" photons) through the annihilation of a single "pump" photon. This requires the energy and momentum (phase matching) conditions to be conserved [142]

$$\mathbf{k}_p = \mathbf{k}_i + \mathbf{k}_s \tag{2.4.17}$$

and

$$\omega_p = \omega_i + \omega_s \ . \tag{2.4.18}$$

The state output by the crystal can be approximated with two modes of the form

$$|\Psi\rangle_{\text{PDC}} = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n \, |n,n\rangle_{AB} \tag{2.4.19}$$

where $\lambda = \tanh \xi$ with ξ proportional to the pump intensity, and the state of n photons in Alice's mode and n photons in Bob's mode is $|n,n\rangle_{AB}$ [148].

The ideal two-photon, maximally entangled state is

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} \left(|1,0\rangle_A |1,0\rangle_B + |0,1\rangle_A |0,1\rangle_B \right) \tag{2.4.20}$$

where the photons are in a superposition of two modes (such as path, time-bin encoding or polarisation). This state can be approximated by setting the mean photon-pair number per pulse $\mu = 2\lambda^2/(1-\lambda^2) \ll 1$, i.e. $\lambda \ll 1$.

In this process there are still components with multiple pairs, described approximately as

$$|\Psi\rangle = \sqrt{p(0)}\,|0\rangle + \sqrt{p(1)}\,|\Psi_2\rangle + \sqrt{p(2)}\,|\Psi_4\rangle \tag{2.4.21}$$

where $p(1) \approx \mu$ and $p(2) \approx \frac{3}{4}\mu^2$, and

$$|\Psi_4\rangle = \frac{1}{\sqrt{3}} \left(|0,2\rangle_A |0,2\rangle_B + |2,0\rangle_A |2,0\rangle_B + |1,1\rangle_A |1,1\rangle_B \right) \ . \tag{2.4.22}$$

This four-mode approximation is applicable for short pump pulses.

Spontaneous Four Wave Mixing SFWM utilises the $\chi^{(3)}$ non-linear coefficient to generate pairs of photons (the "signal" and "idler" photons) through the annihilation of two "pump" photons. This requires the energy and momentum (phase matching) conditions to be conserved [149]

$$2\mathbf{k}_p = \mathbf{k}_i + \mathbf{k}_s \tag{2.4.23}$$

and

$$2\omega_p = \omega_i + \omega_s \ . \tag{2.4.24}$$

In SPDC the conditions are satisfied when both signal and idler photons have a lower energy, and therefore longer wavelengths, where as in SFWM the signal and idler can be spaced equally on either side of the pump photons that generated the pair.

Resonant SFWM In silicon photonics, non-resonant SFWM sources based on long waveguides can be used to increase the interaction between the pump with the non-linearity of silicon. Ignoring the losses and higher order effects, the generation probability

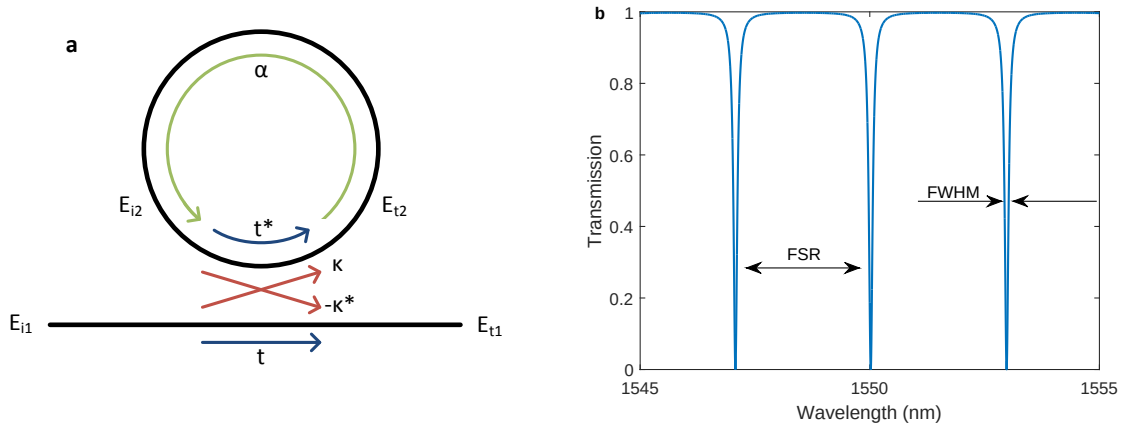

Figure 2.21: **Ring Resonator Structure:** (a) Ring resonator structure consisting of a straight waveguide evanescently coupled to a ring shaped waveguide. The ring forms a cavity, causing the constructive and destructive interference dependent on the wavelength of the signal and round trip length of the ring. (b) Spectrum of a ring resonator, illustrating that pump photons can be injected at the 1550 nm resonance, and that the signal and idler photons will be generated in resonances either side of the pump (1547 nm and 1553 nm).

will increase quadratically with the pump and length of waveguide [150]

$$\text{Prob} \propto |\xi|^2 = \gamma^2 P^2 L^2 \ . \tag{2.4.25}$$

These photons are generated in continuum of wavelengths, thus requiring spectral filtering for post selection of coincident pairs of photons.

In some experiments, a silicon ring resonator can be pumped with a pump to generate pairs of single photons through resonant SFWM. The ring resonator structure consists of a circular waveguide cavity, evanescently coupled to a straight waveguide. In this cavity, the electromagnetic field is enhanced by a factor

$$F = \frac{\mathrm{i}t}{1 - r\tau \mathrm{e}^{\frac{2\pi n_{\text{eff}} L}{\lambda}}} \tag{2.4.26}$$

where t and r are the transmission and reflectivity of the coupler, τ is the round trip loss inside the ring, L is the length of the ring, n_{eff} is the effective refractive index of the waveguide structure, and λ is the wavelength used.

This has the advantage of increased generation efficiency for those wavelengths res-

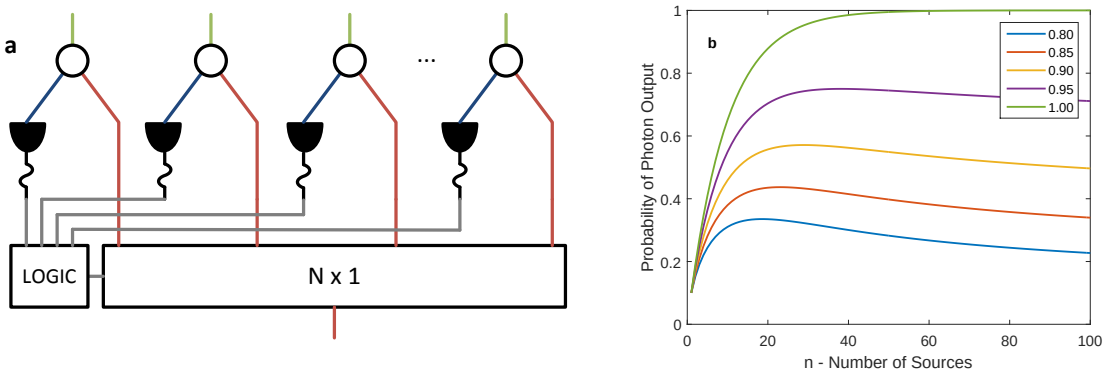

Figure 2.22: **Multiplexed Photon Sources:** (a) Multiplexed photon source schematic, from many spontaneous heralded single photon sources with single photon detectors feeding logic controlled N by 1 optical switch to route the heralded photon to the correct output. (b) The probability of single photon with n probabilistic sources of 0.1, with increasing transmission of a $\log_2(n)$ depth 2 by 2 switch tree to make an N by 1 switch assuming perfect heralding.

onant with the cavity. This also means that the ring resonator structure will generate photons within the resonance spectral function, improving the spectral separability of the generated photons [151].

Multiplexed Photon Source The spontaneous nature of these sources mean that photons are only generated some of the time. For higher photon-number experiments the probability of generating these photons at the same time drops rapidly.

One approach to tend towards on-demand single photon is a multiplexed single photon source, where many non-determinstic pair sources are used in parallel. One of the photons is used to herald the presence of the other in the pair. This signal can reconfigure an optical network to route the signal photon towards the appropriate output. Experimental demonstrations include [152–155]

2.4.2 Photon Encoding

Qubits can be encoded on single photons in a number of degrees of freedom including polarisation, path encoding, and time-bin encoding.

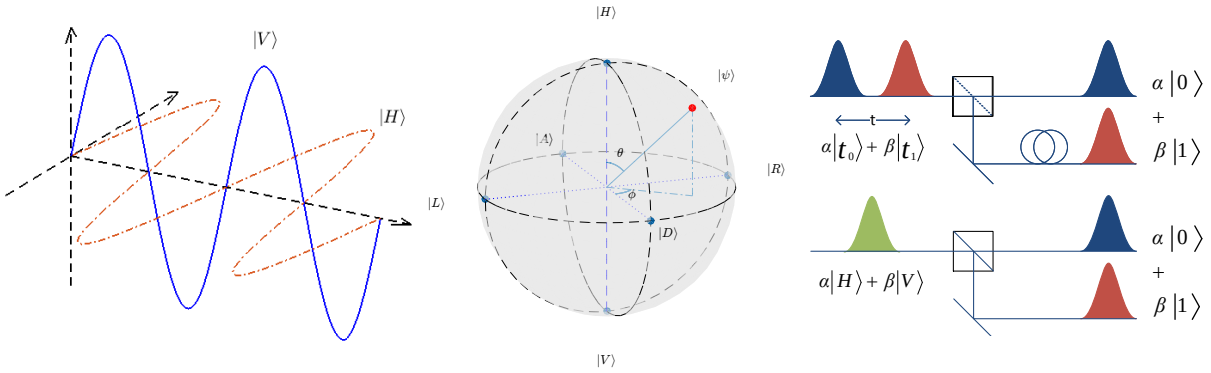

Figure 2.23: **Photon Encoding:** Polarisation encoding representing the qubit with vertically polarised photons as $|0\rangle$ and horizontally polarised photons as $|1\rangle$, whereas path encoding represents the qubit with light in the first path as $|0\rangle$ and the second path as $|1\rangle$. Polarisation or time bin encoding can be converted to path encoding, either through a time-configurable switch, or a polarisation beam splitter.

Polarisation

The polarisation of the photon allows for a qubit to be encoded. The $|0\rangle$ state can be represented by $|V\rangle$ (vertical) polarisation and the $|1\rangle$ state represented by $|H\rangle$ (horizontal) polarisation (see Figure 2.23 (a)). Any arbitrary superposition of these states can be prepared and single qubit operations can be performed with half wave plates and quarter wave plates. This encoding is particular useful for free space communication or computation, where polarisation remains coherent.

Path

When the photons are confined in waveguides (see Section 2.4.3), the path degree of freedom can be exploited. This consists of two optical waveguide modes separated in spatially (dual-rail encoded). The $|0\rangle$ state is represented by a photon in the first waveguide mode and the $|1\rangle$ state is represented by a photon in the second waveguide.

Arbitrary superpositions of photons can be prepare using beam splitters (or directional couplers and MMIs) and phase modulation (see Section 2.4.3). The polarisation and path encoded state can be converted between using a polarisation beam splitter, which converts horizontal and vertical photons in to two different spatial modes (as illustrated in Figure 2.23 (c)). This encoding is particularly useful in integrated photonics, where path lengths can be controlled with great accuracy and waveguides can be defined precisely.

Time-bin

Time-bin encoded photons use the temporal degree of freedom to encode information. The $|0\rangle$ state is represented by a photon in a first temporal slot ($|t_0\rangle$ or $a^\dagger_{t_0}|0\rangle$), and the $|1\rangle$ state is represented by a photon in the second temporal slot ($|t_1\rangle$ or $a^\dagger_{t_1}|0\rangle$).

Arbitrary superposition of photons can be prepared with the relative intensities and the relative phase between the two time-bins (see Section 2.27). This encoding is particularly useful in fibre optical communication, where polarisation rotates and path lengths differ significantly causing difficulties in maintaining alignment and coherence of the channel.

2.4.3 Linear Optical Components

To encode quantum information in a photon's degree of freedom, the propagation and characteristics of light in relevant media must be understood. The propagation of light in a medium is described by Maxwell's equations [156]

$$\begin{aligned}
\nabla \cdot \mathbf{D} &= \frac{\rho}{\epsilon_0} \\
\nabla \cdot \mathbf{B} &= 0 \\
\nabla \times \mathbf{E} &= -\frac{\partial \mathbf{B}}{\partial t} \\
\nabla \times \mathbf{B} &= \mu_0 \left(\mathbf{J} + \epsilon_0 \frac{\partial \mathbf{E}}{\partial t} \right)
\end{aligned} \tag{2.4.27}$$

where $\mathbf{E}$ and $\mathbf{B}$ are the electric field and magnetic flux respectively and the constitutive equations

$$\begin{aligned}
\mathbf{D} &= \epsilon \mathbf{E} \\
\mathbf{B} &= \mu \mathbf{H}
\end{aligned} \tag{2.4.28}$$

and Ohms law takes the form

$$\mathbf{J} = \sigma \mathbf{E} \, . \tag{2.4.29}$$

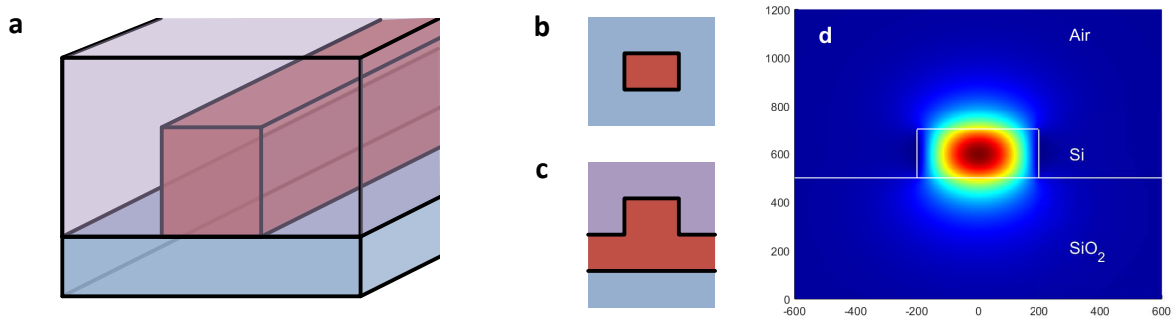

Figure 2.24: **Optical Waveguides:** (a) Square waveguide cross-section through a surrounding cladding, such as with silica waveguides. (b) Square cross-section. (c) Slab waveguide. (d) A simulated optical mode intensity profile for tranverse electric field in silicon.

Optical Waveguides

Optical waveguides underpin photonic technologies, and the guidance of light to appropriately direct communication has provided global telecommunications with optical fibres. To describe an optical waveguide, consider a perfectly dielectric ($\sigma = 0$) and inhomogeneous medium ($\mathbf{n} = n(\mathbf{r})$). Maxwell's equation can be manipulated into the following wave equations:

$$\begin{aligned} \nabla^2\mathbf{E} + \nabla\left(\frac{1}{\mathbf{n}^2}\nabla\mathbf{n}^2\mathbf{E}\right) - \epsilon_0\mu_0\mathbf{n}^2\frac{\partial^2\mathbf{E}}{\partial t^2} &= 0 \\ \nabla^2\mathbf{H} + \frac{1}{\mathbf{n}^2}\nabla\mathbf{n}^2 \times (\nabla\times\mathbf{H}) - \epsilon_0\mu_0\mathbf{n}^2\frac{\partial^2\mathbf{H}}{\partial t^2} &= 0\ . \end{aligned} \tag{2.4.30}$$

A plane travelling wave solution can then be applied to these equations in the form

$$\begin{aligned} \mathbf{E} &= \mathbf{E}(x,y)\exp\left[\mathrm{i}\left(\omega t - \beta z\right)\right] \\ \mathbf{H} &= \mathbf{H}(x,y)\exp\left[\mathrm{i}\left(\omega t - \beta z\right)\right] \end{aligned} \tag{2.4.31}$$

where $\beta = \frac{\omega}{c}n_{\text{eff}}$ is the propagation constant and n_{eff} is the effective index of the propagating mode. The phase velocity is $\nu = {}^{1}/_{\sqrt{\epsilon\mu}} = {}^{c}/_{n}$.

In a rectangular waveguide (see Figure 2.24), transverse electric (TE) and transverse magnetic (TM) modes can be defined, where the electric field is polarised in the x or y direction respectively.

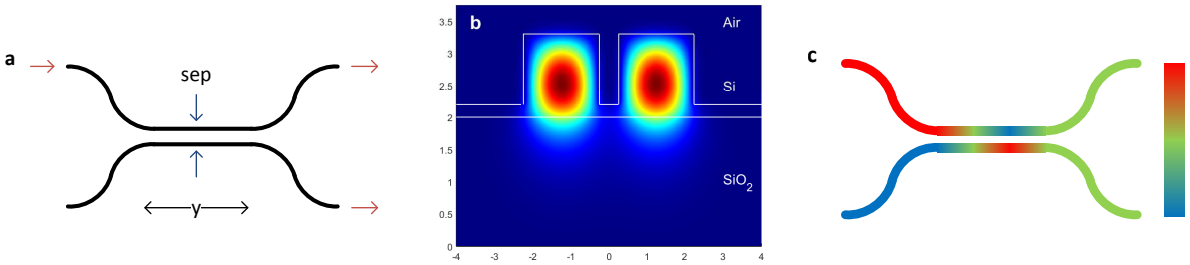

Figure 2.25: **Directional Coupler:** (a) Top view of a directional coupler with waveguide separation dictating the coupling strength between the waveguides and length controlling the reflectivity. (b) Supermodes of the two waveguides effervescently coupled. (c) Intensity of the modes as it propagates, with the length chosen to give the 50:50 splitting.

Directional Coupler

Optical waveguides allow for propagating light, but further components are required to manipulate the information encoded by this light. A directional coupler is a fundamental component in the realisation of photonic technologies and is analogous to the bulk optic beam-splitter. It is constructed by bringing two waveguides in proximity to each other so that there is evanescent coupling of the guided light modes from one waveguide to the other (see Figure 2.25).

With the two waveguide modes ($A(z)$ and $B(z)$) propagating along the z direction, with and overlap parameter κ, the coupled modal equation is

$$\begin{aligned} \frac{dA(z)}{dz} &= -\mathrm{i}\kappa B(z)\,\mathrm{e}^{-\mathrm{i}2\Delta z} \\ \frac{dB(z)}{dz} &= -\mathrm{i}\kappa A(z)\,\mathrm{e}^{+\mathrm{i}2\Delta z} \end{aligned} \tag{2.4.32}$$

where $\Delta = \beta_b - \beta_a$ is the propagation mismatch, and β_a and β_b are the propagating constants of the two waveguides. When there is no propagation mismatch ($\Delta = 0$), the solution to the system of differential equations is given in the form

$$\begin{aligned} A(z) + B(z) &= (A_0 + B_0)\,\mathrm{e}^{-\mathrm{i}\kappa z} \\ A(z) - B(z) &= (A_0 - B_0)\,\mathrm{e}^{+\mathrm{i}\kappa z} \end{aligned} \tag{2.4.33}$$

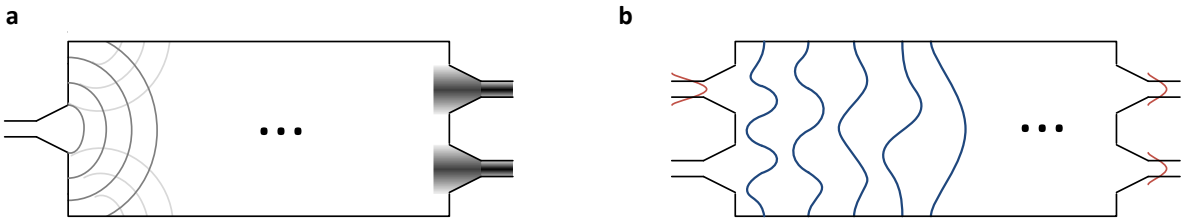

Figure 2.26: **MMI:** (a) 1x2 MMI. The abrupt expansion of the waveguide causes diffraction of the optical wave. The reflections from the interfaces cause interference patterns. The appropriate length of device can be designed to cause two spatially separated modes of equal intensity. (b) 2x2 MMI. A representation of different modes in the multi-mode section excited by the launched photons.

to give

$$\begin{aligned} \rightarrow A(z) &= A_0 \cos(\kappa z) - \mathrm{i} B_0 \sin(\kappa z) \\ B(z) &= B_0 \cos(\kappa z) - \mathrm{i} A_0 \sin(\kappa z) \end{aligned} \tag{2.4.34}$$

showing a sinusoidal variation in intensity between the two waveguides as the length z varies. This provides the transfer matrix of

$$\hat{U}_{\mathrm{DC}} = \begin{pmatrix} \cos(\kappa z) & -\mathrm{i}\sin(\kappa z) \\ -\mathrm{i}\sin(\kappa z) & \cos(\kappa z) \end{pmatrix} = \begin{pmatrix} t & r \\ r & t \end{pmatrix} \tag{2.4.35}$$

with transmittivity, t, and reflectivity r. The equivalent of a 50:50 beam splitter can be made by designing the length and separation of the directional coupler to be $\kappa z = \pi/4$ (see Figure 2.25 (c)).

A somewhat equivalent device can be constructed called a Multimode interference (MMI) device. MMI devices are based on the self-imaging principle and use the diffraction and reflection from the structure seen in Figure 2.26 to cause interference patterns throughout the structure. Any photon launched at an input port excites a superposition of supermodes, each propagating with different phase velocities. Constructive and destructive interference between these modes arise throughout the device as they propagate. The device length is designed to allow the constructive interference of two modes with equal intensities to split into the two outputs [157].

Phase Control

Thermo-optic Phase Shifter A further element to dynamically control and reconfigure photon circuits is required, by altering the relative phase between different waveguides. This can be achieved by locally heating the waveguide with a resistive heater positioned near the optical mode. The heat alters the refractive index of the waveguide

$$\Delta\phi = \frac{2\pi L}{\lambda_0}\frac{dn}{dT}\Delta T \tag{2.4.36}$$

where L is the length of the waveguide exposed to the change in temperature, λ_0 is the free-space wavelength of light, $\frac{dn}{dT}$ is the thermo-optic coefficient of the medium, and ΔT is the change in temperature applied by the resistive heater.

When a path encoded qubit is instantiated with a single photon in two possible waveguides (dual-rail encoding), the temperature in one of the waveguides relative to the other yields a phase shift given by the transfer matrix

$$\hat{U}_\phi = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{pmatrix} . \tag{2.4.37}$$

Electro-optic Phase Modulator Thermo-optic phase shifting allows reconfigurability, but suffers from slow temporal response. Fast approaches to modulation can come from the electro-optic effect, a linear change in refractive index from an electric field applied across the waveguide.

$$\Delta\phi = \frac{2\pi L}{\lambda_o}\chi^{(2)}E \tag{2.4.38}$$

where E is the electric field. Electro-optic effects are only limited by the capacitance and electrical characteristics of the modulators, and they have been exploited in material systems such as lithium niobate and gallium arsenide with bandwidths of 10's of GHz [158].

Quantum-confined Stark Effect Other methods for modulation include the quantum-confined Stark effect (QCSE), in which the absorption spectra of the material system can be tuned through application of an electric field. This change of absorption spectra is related to the real term in the exponential of the electro-magnetic field, which in turn is

related to the imaginary part of the field through a Kramers-Kronig relationship. This causes both phase and absorption dependent on voltage, and is quadratic in the low-voltage limit [159]. This phenomena is used in indium phosphide devices, where the core of the electro-optic phase modulator is a multi-quantum well strcuture, and is discussed further in Chapter 3.

Carrier Injection and Depletion Silicon photonics has many advantages, however, there is no natural $\chi^{(2)}$ non-linearity, and so alternative techniques are exploited to induce optical phases. These include carrier injection and depletion modulators.

Carrier injection modulation exploits the change in absorption and refractive index of the material by injecting carriers into the waveguide structure. This can be achieved by creating a *p-i-n* junction with the intrinsic region composed of the waveguide. The junction is then forward biased to inject carriers into the waveguide where the electric field mode exists [160].

Carrier depletion modulators exploit the change in absorption and refractive index of the material by depleting a *p-n* junction from the waveguide [161]. This can provide a phase relationship that is dependent on the length, wavelength, material, and doping profiles. For more discussion, see Chapter 5.

Mach-Zehnder Interferometer

The Mach-Zehnder Interferometer (MZI) is an important tool for photonic circuits and experiments. It consists of 2 beam splitters and two paths (see Figure 2.27 (a)). If the paths are slightly different lengths or contain an element to adjust the relative phase, the photonic source can interfere and convert a phase relationship to an intensity difference.

$$\hat{U}_{\mathrm{MZI}} = \hat{U}_{\mathrm{DC}}\hat{U}_{\phi}\hat{U}_{\mathrm{DC}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & \mathrm{i}\\ \mathrm{i} & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{\mathrm{i}\phi}\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & \mathrm{i}\\ \mathrm{i} & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1-\mathrm{e}^{\mathrm{i}\phi} & \mathrm{i}(1+\mathrm{e}^{\mathrm{i}\phi})\\ \mathrm{i}(1+\mathrm{e}^{\mathrm{i}\phi}) & -1+\mathrm{e}^{\mathrm{i}\phi}\end{pmatrix}. \tag{2.4.39}$$

If there is laser input to the top arm (E_0), the intensity of the two channels at the output are

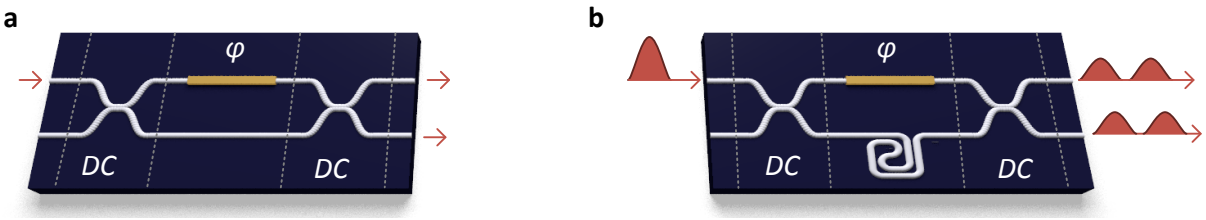

Figure 2.27: **Mach-Zehnder Interferometer:** (a) Schematic of an MZI comprising two 50:50 directional couplers, with a thermo-optic phase modulator on one arm, to change the relative intensities out of the two arms. (b) Schematic of an asymmetric MZI comprising two 50:50 directional couplers, with a thermo-optic phase modulator on one arm and a delay on the other to split a temporal pulse in to two pulses with a relative phase.

$$\rightarrow \frac{\mathrm{E}_0}{2}\begin{pmatrix} 1-\mathrm{e}^{\mathrm{i}\phi} \\ \mathrm{i}(1+\mathrm{e}^{\mathrm{i}\phi}) \end{pmatrix} \tag{2.4.40}$$

and the intensity becomes

$$\rightarrow \mathrm{I}_0\begin{pmatrix} \sin^2\frac{\phi}{2} \\ \cos^2\frac{\phi}{2} \end{pmatrix} \ . \tag{2.4.41}$$

By only considering one-photon terms and including extra phase modulators to the end of the MZI we can generate arbitrary one-qubit states in path encoding.

$$\rightarrow \sin^2\frac{\phi}{2}\left|0\right\rangle + \mathrm{e}^{\mathrm{i}\theta}\cos^2\frac{\phi}{2}\left|1\right\rangle \ . \tag{2.4.42}$$

Asymmetric Mach-Zehnder Interferometers The Asymmetric Mach-Zehnder Interferometer (AMZI) is a special case of the MZI where one arm is considerably longer than the other (see Figure 2.27 (b)). This component is useful in time-bin-encoded circuits. The effect of the circuit can be described in terms of the creation operation (Section 2.4.1), as

$$\begin{aligned} & a^\dagger_{t_0,0}\left|0\right\rangle \\ & \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}\left(a^\dagger_{t_0,0}+\mathrm{i}a^\dagger_{t_0,1}\right)\left|0\right\rangle \\ & \xrightarrow{\text{DELAY}} \frac{1}{\sqrt{2}}\left(a^\dagger_{t_0,0}+\mathrm{i}\mathrm{e}^{\mathrm{i}\phi_0}a^\dagger_{t_1,1}\right)\left|0\right\rangle \\ & \xrightarrow{\text{BS}} \frac{1}{2}\left(a^\dagger_{t_0,0}+\mathrm{i}a^\dagger_{t_0,1}+\mathrm{i}\mathrm{e}^{\mathrm{i}\phi_0}a^\dagger_{t_1,1}-\mathrm{e}^{\mathrm{i}\phi_0}a^\dagger_{t_1,0}\right)\left|0\right\rangle \ . \end{aligned} \tag{2.4.43}$$

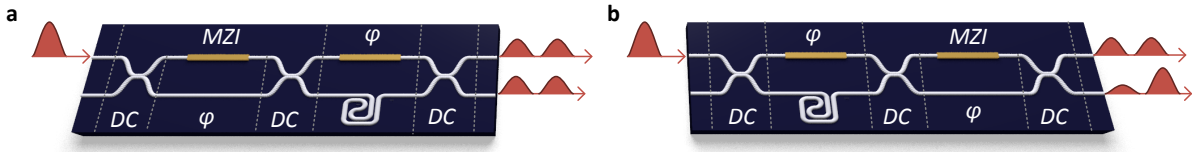

Figure 2.28: **Asymmetric Mach-Zehnder Interferometer:** (a) Schematic of an AMZI comprising an MZI instead of the front DC to change the relative intensities in the two interferometer arms, allowing for propagation loss compensation in both outputs. (b) Schematic of an AMZI comprising an MZI instead of the back DC to change the relative intensities in the two interferometer arms, allowing for propagation loss compensation in a single output.

By examining the top arm (mode 0), the state can be renormalised to

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(a^\dagger_{t_0,0} - \mathrm{e}^{\mathrm{i}\phi_0} a^\dagger_{t_1,0}\right)|0\rangle \tag{2.4.44}$$

which is equivalent to the time bin qubit state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle + \mathrm{e}^{\mathrm{i}\phi_0}|t_1\rangle\right) \ . \tag{2.4.45}$$

By including an MZI at the front or the end (Figure 2.28) one can select time bins ($|t_0\rangle$ or $|t_1\rangle$), or some arbitrary superposition of them, and compensate for the loss incurred in the longer "delay" arm.

To measure the time bin and phase information of the state, another AMZI can be implemented

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left(a^\dagger_{t_0,0} + \mathrm{e}^{\mathrm{i}\phi_0} a^\dagger_{t_1,0}\right)|0\rangle \\
&\xrightarrow{\text{BS}} \frac{1}{2}\left(a^\dagger_{t_0,0} + \mathrm{i}a^\dagger_{t_0,1} + \mathrm{e}^{\mathrm{i}\phi_0} a^\dagger_{t_1,0} + \mathrm{i}\mathrm{e}^{\mathrm{i}\phi_0} a^\dagger_{t_1,1}\right)|0\rangle \\
&\xrightarrow{\text{DELAY}} \frac{1}{2}\left(a^\dagger_{t_0,0} + \mathrm{i}\mathrm{e}^{\mathrm{i}\phi_1} a^\dagger_{t_1,1} + \mathrm{e}^{\mathrm{i}\phi_0} a^\dagger_{t_1,0} + \mathrm{i}\mathrm{e}^{\mathrm{i}\phi_0}\mathrm{e}^{\mathrm{i}\phi_1} a^\dagger_{t_2,1}\right)|0\rangle \\
&\xrightarrow{\text{BS}} \frac{1}{2\sqrt{2}}\Bigg(a^\dagger_{t_0,0} + \mathrm{i}a^\dagger_{t_0,1} + \mathrm{i}\mathrm{e}^{\mathrm{i}\phi_1}\left(a^\dagger_{t_1,1} + \mathrm{i}a^\dagger_{t_1,0}\right) \\
&\qquad + \mathrm{e}^{\mathrm{i}\phi_0}\left(a^\dagger_{t_1,0} + \mathrm{i}a^\dagger_{t_1,1}\right) + \mathrm{i}\mathrm{e}^{\mathrm{i}\phi_0}\mathrm{e}^{\mathrm{i}\phi_1}\left(a^\dagger_{t_2,1} + \mathrm{i}a^\dagger_{t_2,1}\right)\Bigg)|0\rangle
\end{aligned} \tag{2.4.46}$$

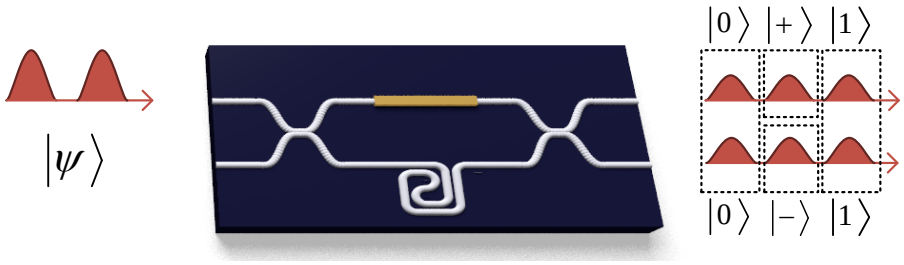

Figure 2.29: **Asymmetric Mach-Zehnder Interferometer for Time-Bin Tomography:** A schematics of am AMZI used for tomography of a time-bin encoded states where both the Z and X basis are measured in one phase setting.

which we reorder as

$$\begin{aligned} = \frac{1}{2\sqrt{2}} \Big[& a^\dagger_{t_0,0} + \mathrm{i} a^\dagger_{t_0,1} \\ & + a^\dagger_{t_1,0} \left(\mathrm{e}^{\mathrm{i}\phi_0} - \mathrm{e}^{\mathrm{i}\phi_1} \right) \\ & + \mathrm{i} a^\dagger_{t_1,1} \left(\mathrm{e}^{\mathrm{i}\phi_0} + \mathrm{e}^{\mathrm{i}\phi_1} \right) \\ & + \mathrm{e}^{\mathrm{i}\phi_0} \mathrm{e}^{\mathrm{i}\phi_1} \left(a^\dagger_{t_2,1} + \mathrm{i} a^\dagger_{t_2,0} \right) \Big] |0\rangle \end{aligned} \tag{2.4.47}$$

where the first two terms, $a^\dagger_{t_0,0}$ and $a^\dagger_{t_0,1}$, represent measuring in the Z basis with value $|0\rangle$, the last two terms, $a^\dagger_{t_2,1}$ and $a^\dagger_{t_2,0}$, represent measuring in the Z basis with value $|1\rangle$. The remaining two terms, $a^\dagger_{t_1,0}$ and $a^\dagger_{t_1,1}$, represent measuring $|+\rangle$ and $|-\rangle$ respectively, which are the X basis eigenstates (see Figure 2.29).

2.4.4 Single Photon Detection

Once single photons are generated and manipulated through photonic circuitry, the last key component in quantum photonic experiments are the electrical read out of single photon detectors. The criteria for good single photon detector technology [162] requires

- High efficiency around the wavelength range of interest, providing a high probability of output reading, given an incident photon (related to a high quantum efficiency)
- Spectral Range - The operating wavelength of interest will depend on the application or experiment. In this thesis we will be most interested in telecommunication wavelengths (around 1550 nm) that can operate with low loss through optical fibres

- Low dark count rate - which reduces the spontaneous record of a detection event, independent from the photonic input signal
- Low temporal jitter - which is the uncertainty from the time of arrival of the photon to the electronic pulse generation, signalling the detection event
- Small dead time - the minimal time interval between two consecutive detection events
- Photon number resolution - where ideally the detector can discriminate between the number of signal photons incident on the detector

Photomultiplier

PMTs were a staple of quantum photonic experiments since the 1960's until the 1980's and had efficiencies between 10 to 20% at visible wavelengths [28, 31]. They are typically constructed in a vacuum glass housing containing a photocathode, an anode, and several dynodes. An incident photon would strike the photocathode, ejecting electrons due to the photoelectric effect, which are directed by the focussing electrode towards the electron multiplier. A measurable signal is generated through the process of secondary emission which multiplies these electrons.

Avalanche Photodiode

APDs started to replace the PMT in quantum optics experiments [163], and are currently used in a wide range of experiments. For visible light, silicon APDs offer detection efficiencies of 70% at 633 nm (Perkin Elemer), with a jitter of 500 ps and deadtime of $\sim$50 ns.

For telecommunication wavelengths (1530nm to 1570 nm), silicon is transparent and other more exotic materials are needed such as InGaAs APDs, which have been recently shown to operate at 55% efficiency with a 1 GHz gated mode, through the use of self-differencing detection [164].

APDs utilise a highly reverse biased photodiode in which an incident photon causes the breakdown of the diode junction. This in turn causes an avalanche of electrons, creating

a detectable signal. This can have a downside of long recovery time (increasing the dead time) and afterpulses (false positive signals increasing the dark counts). To overcome some of these issues, the detectors are cooled as well as gated (where the reverse bias is modulated, to only allow detection when photons are expected).

Superconducting Transition Edge Sensor

Transition Edge Sensor (TES) single photon detectors have reported better than 95% efficiency, photon number resolving capability, and low dark count rates, but require mK operation temperatures [165].

The TES is a superconducting film on the brink of transitioning between superconducting and a normal resistive element, where a small change in the temperature will cause the abrupt change in state. An incident single photon will cause enough heat to transition from superconducting to resistive, which is turn generates a measurable signal.

Because these devices depend on thermal time constants, their response is typically on the order of 100 ns FWHM jitter and a slow recovery time of $\sim$1 μs, but due to their near unit efficiency and photon number resolution they have been used for quantum optics experiments to demonstrate near-loophole free Bell violations [166] and long-distance QKD [167].

Superconducting Nanowire

Superconducting nanowire single-photon detectors (SNSPDs) can be used to detect wavelengths between visible to the mid-infrared with low dark counts, short dead times, and excellent jitter [168].

The detector comprises of a thin ($\sim$100 nm wide) nanowire, patterned using a superconducting film operating around 1.5-4 K (well below the superconducting transition temperature of the material). It is then biased with a DC electrical signal, just below its critical current (the point at which the wire would become resistive). When an incident photon interacts with the material, the breaking of cooper-pair bonds causes a hot-spot of locally resistive material. This perturbs the current distribution, thus triggering an avalanche of resistivity to propagate and eventually extend across the width

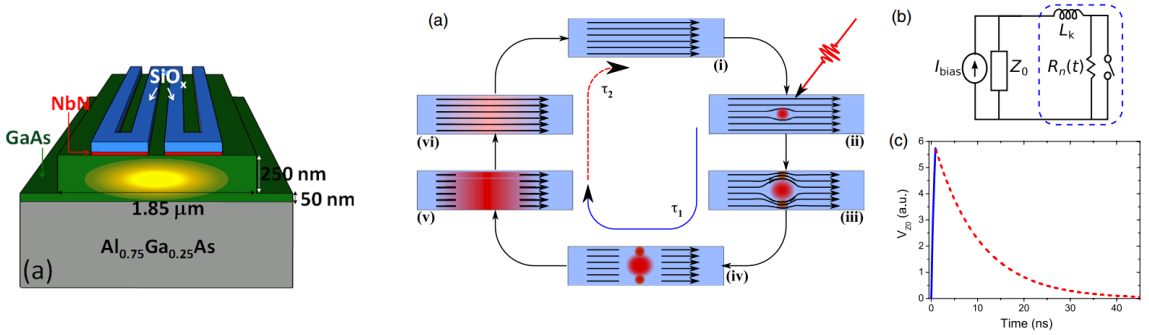

Figure 2.30: **Integrated Superconducting Nanowire Single Photon Detectors:** (a) Integrated superconducting nanowire single photon detector on top of GaAs waveguides allowing for high efficiency [169]. (b) The operation of a superconducting nanowire single photon detector, describing the generation of a hot spot through photon interaction, spreading to create a finite resistance that causes a voltage pulse. The hot section subsequently cools back down to superconducting regime [173].

of the nanowire. This triggers a fast voltage pulse, which is amplified and measured (Figure 2.30)

These detectors can either be fibre-coupled long meanders in the path of the photons, or even coplanar with an integrated waveguide. This last technique can be used to monolithically fabricate entire quantum photonic experiments on a single chip. Recent demonstrations include detectors fabricated on GaAs waveguides [169] and silicon substrates and waveguides [170–172].

2.4.5 Integrated Platforms

Many material systems can be used to generate integrated photonic circuits, each with their advantages and their disadvantages depending on the application. Here we discuss a number of standard integrated photonic platforms and some of their characteristics.

Silicon Oxide

Silicon Oxide uses a slightly higher refractive index glass in a standard silica cladding. This allows for low loss waveguide, with high fibre to chip coupling. Due to the low refractive index contrast, waveguide bends are fairly large (on the order of 5 mm) and therefore devices are limited by the size of the integrated chip. By depositing metalised layers, thermo-optic control of circuits can be utilised for reconfigurability. These devices

can be designed for a large range of waveguides from visible to infra-red and have been used to demonstrate many fundamental quantum information experiments [174].

Silicon Oxynitride

Silicon oxynitride (SiO_xN_y) is a higher refractive index contrast material than silica ($n = 1.7$), making more compact devices, but maintains a low propagation loss of ~0.1 dB/cm, and 1 dB facet loses. Thermo-optic phase modulators can reconfigure the optical circuits and devices can be designed for visible to infra-red operation [175, 176].

Gallium Arsenide & Lithium Niobate

Gallium Arsenide (GaAs) and Lithium Niobate ($LiNbO_3$) have both been used in telecommunications devices for high speed electro-optic modulation, allowing for many forms of communications up to 100 GHz [177].

Silicon-on-Insulator

Silicon-on-insulator (SoI) has a much higher refractive index contrast (~4) permitting much smaller waveguide structures on the order of 500 nm by 200 nm waveguides and bend radii on the order of 10 μm. The component density is therefore much larger, but standard single-mode waveguides are also much lossier (~3 dB/cm). The operational wavelengths are infra-red regime, as silicon is absorptive in the visible.

Thermo-optic phase modulators can be made through metallised layers or by doping areas of the waveguide to allow current to flow and heat to dissipate. Carrier injection or depletion modulators can yield fast modulation, but have non-ideal voltage, phase, and loss relationships (see Chapter 5). The non-linearity of silicon allows for generating pairs of single photons for quantum experiments by spontaneous four wave mixing [178]. Due to the indirect bandgap of the material, other elements are required to be added to generate photodiodes, or hybrid lasers [179].

Indium Phosphide

Indium Phosphide (InP) can be used to generate semiconductor optical amplifiers, lasers, electro-optic phase modulators, photodiodes. The relatively high refractive index grants high component density, and this flexibility allows for transceiver devices for the telecommunications industry [180].

In this thesis InP is utilised for transmitters in weak coherent based quantum key distribution schemes, which require the monolithic integration of lasers and high-speed modulation. SiO_xN_y is also used for receiver circuits, which benefits from low-loss and reconfigurable photonic circuits. Alternative transmitters were fabricated in SoI, benefiting from the miniaturisation and robust manufacturing processes available from silicon photon foundries.

2.5 Summary

This chapter has provided relevant background material in

- Classical and Modern Cryptography - Introducing the historical context and currently implemented encryption techniques.
- Quantum Information - Introducing the quantum phenomena relevant to quantum cryptographic technologies and the threat of quantum technologies to cryptography.
- Quantum Key Distribution - Expanding on the quantum information section to provide background in the protocols, security proofs, and physical implementations.
- Integrated Photonics - Presenting background material in the photonic technologies for quantum key distribution including photon sources, photonic manipulation, and detection, focussing on integrated photonic platforms.

Chapter 3

Chip-to-Chip Quantum Key Distribution

Statement of Work

The initial transmitter experimental concept was designed by Mark Thompson and Mark Godfrey with the initial indium phosphide transmitter mask design compiled by Mark Godfrey and fabricated by Oclaro. I designed later generation indium phosphide devices with enabling improvements and modifications, clarifying experimental concepts and permitting operation. I also developed the RF-PCB for high speed transmitter operation, as well as designing and compiling the mask design for the receiver circuit, which was fabrication by LioniX. Code development and infrastructure for experimental characterisation, operation, and data analysis was supported by Chris Erven. The detectors used for this experiment were developed Robert H. Hadfield along with Shigehito Miki, Taro Yamashita, Mikio Fujiwara, Masahide Sasaki, Hirotaka Terai, Michael G. Tanner, and Chandra M. Natarajan.

3.1 Introduction

Improvement in secure transmission of information is an urgent practical need for governments, corporations and individuals. Quantum key distribution [1,2] (QKD) promises security based on the laws of physics and has rapidly grown from proof-of-concept to robust demonstrations [3–6] and even deployment of commercial systems [7–9]. Despite these advances, QKD has not been widely adopted, and practical large-scale deployment will likely require integrated chip-based devices for improved performance, miniaturisation and enhanced functionality, fully integrated into classical communication networks. Here we report low error rate, GHz clocked QKD operation of an indium phosphide (InP) transmitter chip and a silicon oxynitride (SiO_xN_y) receiver chip — monolithically integrated devices that use state-of-the-art components and manufacturing processes from the telecom industry. We use the reconfigurability of these devices to demonstrate three prominent QKD protocols — BB84, Coherent One Way (COW) and Differential Phase Shift (DPS) — with performance comparable to state-of-the-art. These devices, when combined with integrated single photon detectors, satisfy the requirements at each of the levels of future QKD networks — from point-of-use devices through to network backbones — and open the way to operation in existing and emerging classical communication infrastructure.

Delivery of the promise of QKD will require moving to an multi-scale network, where, as with the classical communication infrastructure, each use case has particular requirements that must be met. Use of QKD in hand-held and field deployable devices, or to secure the *'Internet of Things'* for example, will require devices with a small footprint and high robustness to environmental conditions. 'QKD-to-the-home' will require moderate bandwidth, low cost devices, and co-existence with emerging fibre-to-the-home transceivers. Backbones for QKD metro and long-haul networks will require compatibility, and in some cases direct integration, with photonic and electronic semiconductor devices and systems. Also crucial will be the capability to reconfigure QKD protocols on the fly and overcome the bottlenecks currently limiting long-range, high-speed key distribution. Use of common devices will enable unification across all levels of the network. Ultimately, a QKD network must be seamlessly integrated with the classical communication network

with the distinction between classical and quantum operation ideally being defined in software not hardware.

While extreme levels of integration have been achieved in the microelectronics industry over the past decades, it is only recently that size, cost and power consumption considerations have demanded higher levels of integration in photonics. Fibre-to-the-home, data centre, and 100 Gbps metro and long-haul network applications have driven the development of the InP platform to the point of full integration of laser sources, amplifiers, modulators and detectors [180]. Integrated photonics [10] is thus poised to deliver major benefits to QKD technology and networks [109–111] by allowing the miniaturisation of components and circuits for hand-held and field deployable devices. It also provides highly robust manufacturing processes which help reduce cost for personal devices. Finally, the complexity achievable with the integrated platform enables practical implementation of mutli-protocol operation for flexibility, multiplexing for higher rates, and additional monitoring and certification circuits to protect against side-channel attacks [1] in a fibre network.

While there have been individual demonstrations of time-bin decoding [12], miniaturisation [11], and reconfigurability [4] in integrated devices; here we report QKD operation of complex devices that meet the requirements outlined above. We used the InP platform to implement a monolithically integrated transmitter (Figure 3.1 (a)), consisting of a tunable laser, optical interferometers, electro-optic phase modulators and a PIN photodiode. We implement a receiver (Figure 3.1 (b)), consisting of a photonic circuit with thermo-optic phase shifters and reconfigurable delay line in the SiO_xN_y platform, and off-chip single photon detectors. Both photonic systems were manufactured using state-of-the-art industrial fabrication processes (Oclaro and LioniX, respectively) and were designed for multi-protocol reconfigurable operation. We show performance of the photonic devices with clock rates up to 1.7 GHz, a quantum bit error rate (QBER) as low as 0.88%, and estimated secret key rates up to 568 kbps, for an emulated 20 km fibre link. These devices are manufactured using the same fabrication processes as classical communications technology and microelectronics. Together with the development of integrated single photon detectors [162], these devices point the way to seamless integration with existing and

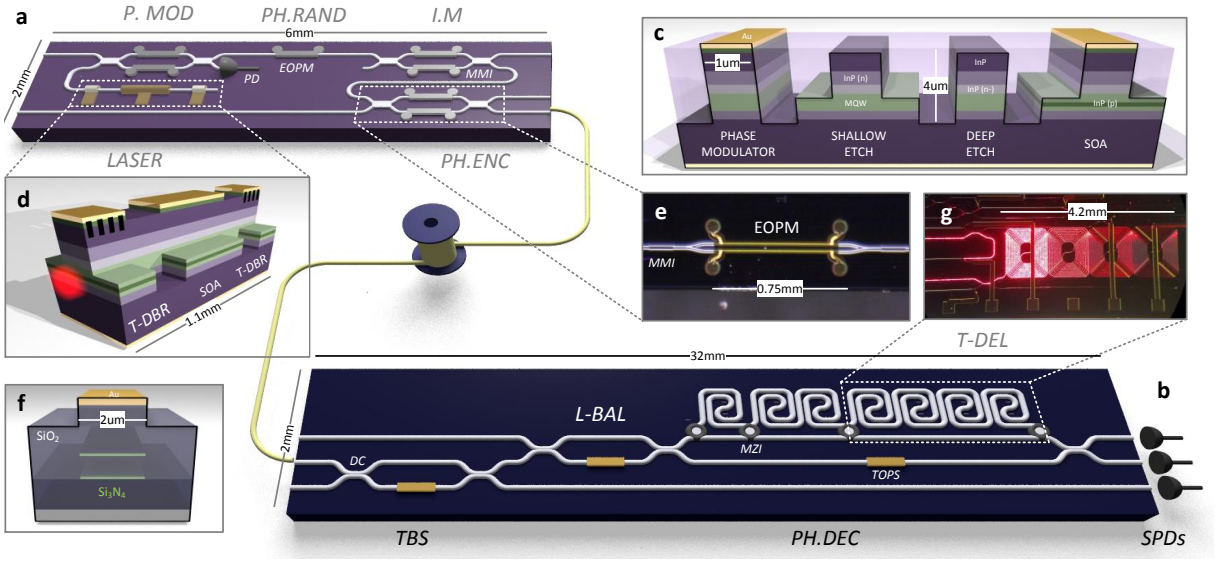

Figure 3.1: **Integrated photonic devices for quantum key distribution** consisting of: (a) A monolithically integrated Indium Phosphide (InP) transmitter for GHz clock rate, reconfigurable, multi-protocol QKD. (b) A Silicon Oxynitride (Triplex) photonic receiver circuit for reconfigurable, multi-protocol QKD that passively decodes the quantum information with off-chip single photon detectors. (c) The InP technology platform waveguide cross-section [180]. (d) Wavelength tunable continuous-wave laser, formed from two tuneable Distributed Bragg Reflectors (T-DBR) and a semiconductor optical amplifier (SOA). (e) Microscopic image of electro-optic phase modulators in Mach-Zehnder interferometer. (f) The SiO_xN_y Triplex waveguide cross-section, with metalisation for heating elements [175]. (g) Microscopic image of the receiver delay lines. [181]

emerging classical communication systems.

3.2 Integrated Transmitter Device

Figure 3.2 shows a schematic of the chip-to-chip QKD system. For the transmitter device, the InP material system was chosen to meet the requirements of fast active electro-optics (with GHz operating speeds) and monolithic integration with the laser source.

The InP-based transmitter chip was fabricated using an advanced active-passive integration technology [180], where a multistep epitaxial growth process provides large flexibility in the waveguide structure (see Figure 3.1 (c)). The on-chip tunable laser (Figure 3.1 (d)) was formed from two distributed Bragg reflectors (DBR) and a semiconductor optical amplifier (SOA). When operated in continuous wave (CW) the laser source ex-

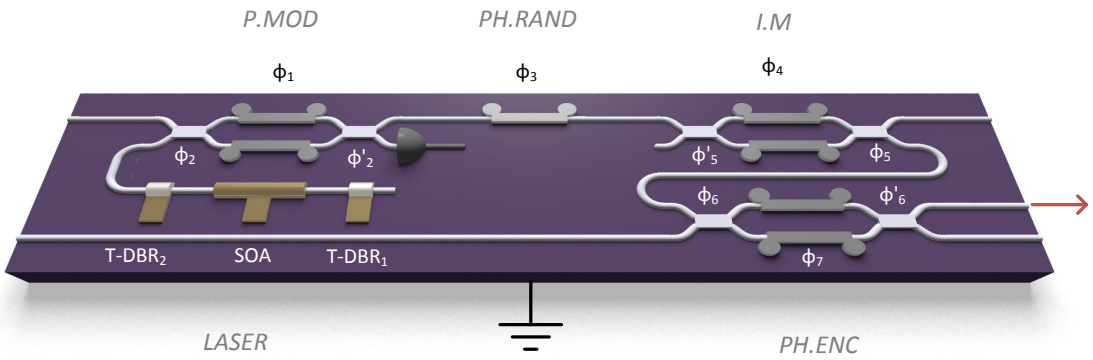

Figure 3.2: **InP TX Schematic:** The laser source consists of semiconductor optical amplifier (SOA) in a cavity formed by two tunable-distributed Bragg reflectors (T-DBR) and is operated in continuous wave mode by injecting current in the SOA. Pulse modulation (P.MOD) is achieved by controlling ϕ_2 and ϕ_2' in DC and ϕ_1 with a DC offset with an RF signal, inside an MZI. Intensity modulation (I.M), phase encoding (PH.ENC) are also achieved through the same operation of $\phi_4, \ldots, \phi_7$, while phase randomisation is achieved with a single EOPM (ϕ_3).

hibited single mode behaviour with FWHM of 34 pm, a side-mode suppression ratio of >50 dB, and an operating wavelength of 1550 nm with ∼10 nm tuning range. Short electrical pulses applied to the reverse biased electro-optic phase modulator (EOPM) in the first MZI enabled optical pulse generation with <150 ps duration and ∼30 dB extinction ratio. The exact timing between consecutive pulses could be accurately controlled by the driving electronics, and the on-chip photodiode was used to monitor the laser intensity and provide feedback to stabilise the laser current. The remaining electro-optic phase modulators and MZIs were used to drive the different QKD protocols and to attenuate the laser pulses to the single photon level. Light was coupled out of the device using a lensed optical fibre.

3.2.1 LASER

Semiconductor Optical Amplifier

The laser source is formed by a semiconductor optical amplifier (SOA) in an InP single-mode weak waveguide structure that is excited through carrier injection (Figure 3.1 (d)). The optical amplifier provides the gain medium and allows the laser device to spontaneously emit over a wide spectral band through current injection. This structure is

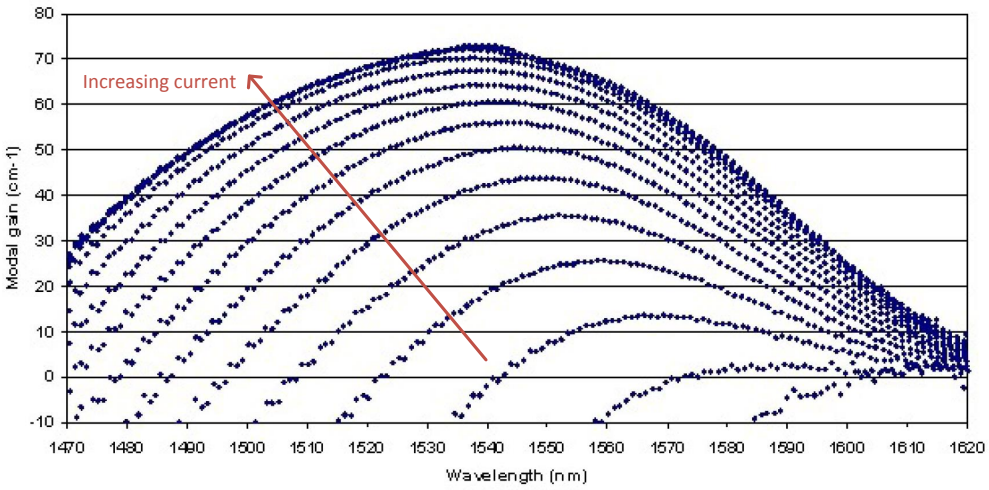

Figure 3.3: **SOA Modal Gain:** Modal gain for 325 μm F-P structure. Current from 2mA to 40mA in 2mA steps [182].

optimised to provide optical gain for TE polarization, and a typical set of modal gain curves versus wavelength and drive current are plotted in Figure 3.3 under a cold cavity model (carrier and thermal effects were therefore unaccounted). These were derived from Hakki-Paoli gain measurements on a 325 μm Fabry-Perot (F-P) test structure stepping from 2 mA to 40 mA drive in 2 mA steps [182].

Tunable Distributed Bragg Reflectors

This is combined with two tunable distributed Bragg reflectors (T-DBR) on either side of the SOA to create a Fabry-Perot cavity that resonates at specific wavelengths. The T-DBR are weakly index coupled gratings with uniform pitch, and are tunable via carrier injection.

The laser is driven by a laser diode current controller (Arroyo ComboSource 600) at ∼20 mA, and can be adjusted to provide the desired phase relationship between successive pulses (as demonstrated in Section 4.2.2). Current versus optical power of the laser, including output coupling loss, is illustrated in Figure 3.4 (a) which clearly shows a lasing threshold of ∼12 mA. The spectrum of the laser for different operating temperatures is shown in Figure 3.4 (b) from which we see it has a ∼50 dB side-band suppression. The measured full-width half-maximum (FWHM) of the laser is 34 pm, but this is likely over-estimated due to the wavelength resolution of our optical spectrum analyser (Anritsu

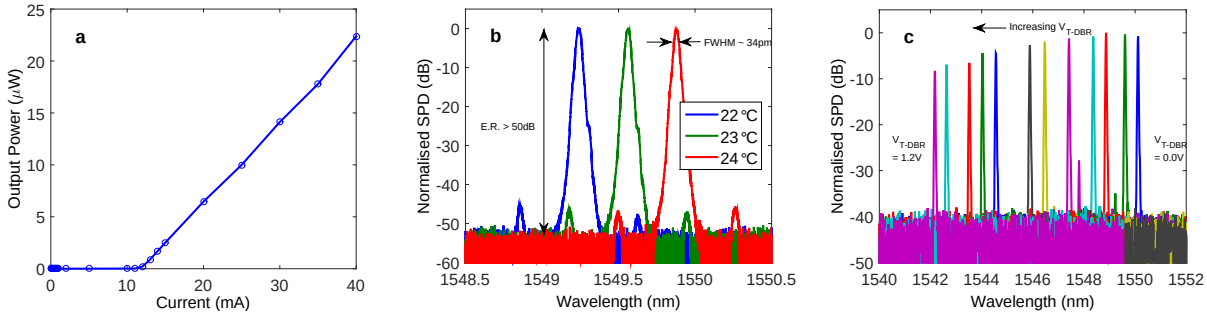

Figure 3.4: **Characterisation of the on-chip laser** showing: (a) The output power versus driving current with a lasing threshold of ∼12 mA. (b) The tunability of the laser wavelength by adjusting the temperature of the device. (c) The tunability of the laser wavelength by adjusting the voltages on the T-DBR.

MS9740A OSA - with 0.03 nm resolution). From the stable interference observed in our QKD experiments, we can instead state that our laser had a coherence time ≥1.5 ns, which would be a FWHM of ≤1.7 pm (where the coherence length $L_{coh} = \frac{c}{\pi\Delta\nu}$ where $\Delta\nu$ is the FWHM in frequency) [183]. Temperature control is required to provide stable laser operation and achieved with a peltier device and thermistor in a feedback loop. The laser wavelength can also be tuned by carrier injection into the T-DBR, as shown in Figure 3.4 (c). Using both temperature and carrier injection effects we can easily tune the wavelength of the laser over a ∼10 nm range.

3.2.2 Electro-optic Phase Modulator

Quantum Confined Stark Effect

The electro-optic phase modulators (EOPM) operate through the Quantum Confined Stark Effect (QCSE) in a waveguide in which the core is a multi-quantum well (MQW) structure [184]. By applying a reverse bias to this structure an electric field is formed, and the QCSE causes a shift in the bandgap of the material incurring a change in absorption, dependent on the applied electric field. This in turn is related to a change in refractive index and can be calculated using the Kramers-Kronig relations that relate real and

imaginary terms of a complex function of the form $\chi(\omega) = \chi_1(\omega) + i\chi_2(\omega)$ by the expression

$$\chi_1(\omega) = \frac{1}{\pi}\mathcal{P}\int_{-\infty}^{\infty} \frac{\chi_2(\omega')}{(\omega') - \omega}\, d\omega' \tag{3.2.1}$$

where $\mathcal{P}$ denotes the Cauchy principal value.

The relation between refractive index and absorption is therefore shown to be

$$n(\omega) - 1 \simeq \frac{c}{\pi}\mathcal{P}\int_{0}^{\infty} \frac{\alpha(\omega')}{(\omega')^2 - \omega^2}\, d\omega' \ . \tag{3.2.2}$$

Under the assumptions of excluding the linear electro-optic effect and that the remaining absorption changes occur in small and localised spectral regions, we can substitute $n(\omega) = n_0(\omega) + \Delta n(\omega)$ and $\alpha(\omega) = \alpha_0(\omega) + \Delta\alpha(\omega)$ into equation 3.2.2, in the energy range of $\omega_1 \leq \omega \leq \omega_2$, which results in

$$\Delta n(\omega) \simeq \frac{c}{\pi}\mathcal{P}\int_{\omega_1}^{\omega_2} \frac{\Delta\alpha(\omega')}{(\omega')^2 - \omega^2}\, d\omega' \ . \tag{3.2.3}$$

At small refractive index changes, this can be model as $\Delta n = -(1/2)n^3 s E^2$ where E is the electric field and $-(1/2)n^3 s$ will be a constant [159].

The QCSE is generally regarded as quadratic in nature, resulting in more nonlinear characteristics for phase shifters. It also has further wavelength dependence for both phase and loss, due to the proximity to the band-gap wavelength of the MQW core. This effect, when oriented parallel to the InP crystal lattice, can have an additional linear electro-optic effect which increases the effective phase for a given voltage [180]. By keeping the EOPM length less than 1 mm, the phase modulators allow up to 10 GHz in bandwidth, but this also requires careful placement on the die to minimise wirebonding lengths allowing good signal integrity to be maintained off-chip.

DC-Operation

Figure 3.5 (a) shows the intensity profiles from the DC characterisation of one of the Mach-Zehnder interferometers (MZI) on the transmitter chip, formed from two multi-

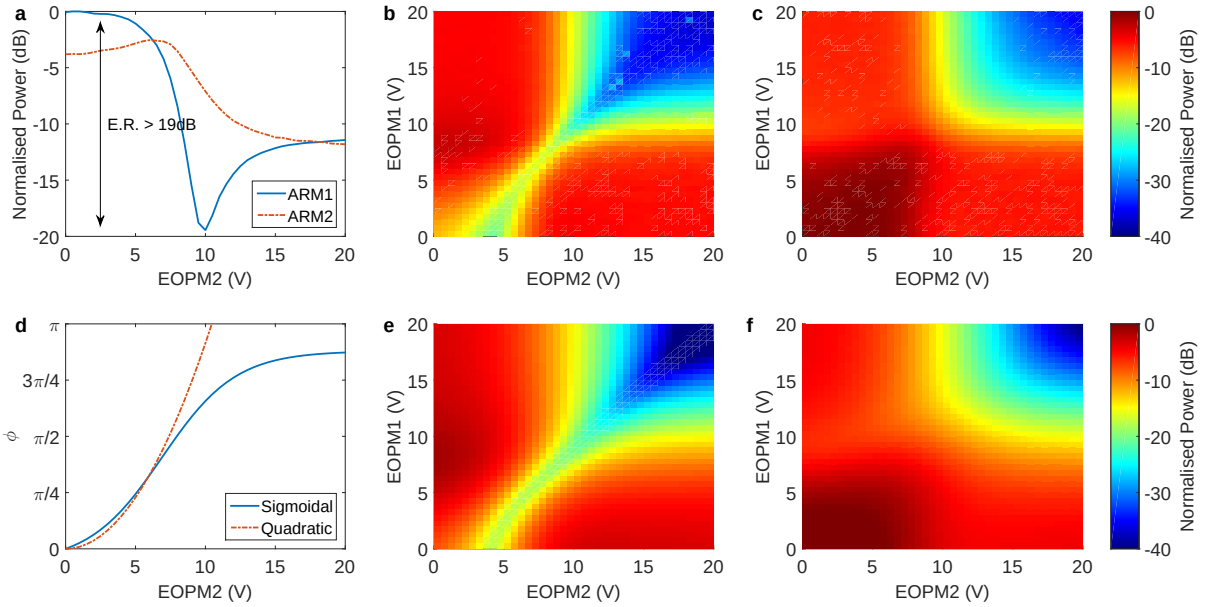

Figure 3.5: **DC EOPM MZI Characterisation:** The intensity profiles measured during the DC characterisation of one of the MZIs. (a) Optical intensity output (at EOPM1 = 10V) varied over EOPM2 voltage showing extinction ratio of over 19dB for the output of the first output arm, and the heat map of intensity at (b) the first output arm and (c) second output arm as the two EOPMs in the Mach-Zehnder have their voltages varied. (d) illustrates a fitted sigmoidal function to the data, and a quadratic function that is valid at lower electric fields (d-e) the signmoidal fitted function to the (b-c) showing good agreement between model and data.

mode interference devices (MMI) acting as 50:50 reflectivity beamsplitters and an EOPM in either arm. From this, one can see an extinction ratio of near ∼19 dB can be achieved over low voltage changes. Figure 3.5 (b) and (c) show the heat map of intensity at the two output arms for a full 2D sweep of the EOPMs. An important note is that the EOPMs suffer from saturation which can limit the range of phase that can be applied if the devices are too short.

This data can be modelled by a sigmoidal function for both phase and absorption, illustrating a near quadratic function at low voltages, followed by saturation and increased loss. The phase, $\Delta\phi$, and transmission, $\Delta\gamma$, relationships are found to be

$$\Delta\phi = \alpha\left(1+\exp\left(-\frac{V-V_0}{\beta}\right)\right)^{-1} \tag{3.2.4}$$

$$\Delta\gamma = \gamma_0\left(1+\exp\left(-\frac{V-V_0}{\beta}\right)\right)^{-1} \tag{3.2.5}$$

where α, β, V_0, and γ_0 are dependent on the length, material and wavelength. The expression for γ (equation 3.2.5) highlights the issue of phase-dependent loss as the transmission function decreases as the voltage increases. And the form of equation 3.2.4 highlights saturation of the phase effects as the voltage increases. This equation will tend to α which is dependent on length, wavelength and material properties. How quickly this occurs will also depend on these parameters and are related to V_0 and β. The loss and the saturation of the phase modulator leads to non-ideal operation that must be overcome.

In the limit of no transmission through one arm of the interferometer the output tends to that of the 50:50 beam splitters themselves, as can be seen in Figure 3.5 (a). This is also seen in Figure 3.5 (b) and (c) when one modulator is pushed to the extreme (the top left and bottom right of the images). If both modulators are forced to this regime then both arms will be extremely lossy (the top right of Figure 3.5 (b) and (c)).

Thermo-optic operation

This non-ideality of the phase modulators presents an issue when there is an absolute offset in phase in one arm of the interferometer (either caused by imperfections in the manufacturing or MMI device design). If the modulator saturates before this DC offset can be accounted for, then pulse modulation will be limited in extinction causing high QBERs. One way to account for this offset within the confines of this design and fabrication is to use the EOPM device as both electro- and thermo-optic modulators.

Thermo-optic phase modulation is slow, but almost ideal as it incurs no extra loss in the interferometer. The electro-optic phase modulator (pictured in Figure 3.1 (e)) has two gold contacts on the top surface of the chip, and a gold ground plane on the bottom. The operate in the electro-optic regime both pins should be reversed biased with the same offset compared to the ground. There is also a small resistance between these two pin contacts ($\sim$10 Ω), which allows a current to flow between them when biased with slightly different voltages. As illustrated in Figure 3.2, ϕ_2 and ϕ_2' are labelled separately to denote that they can be biased at two separate voltage levels compared to the ground on the bottom of the chip. In Figure 3.6 this thermo-optic effect is used to compensate for the original phase offset found in the MZI. By increasing the offset between the two EOPM

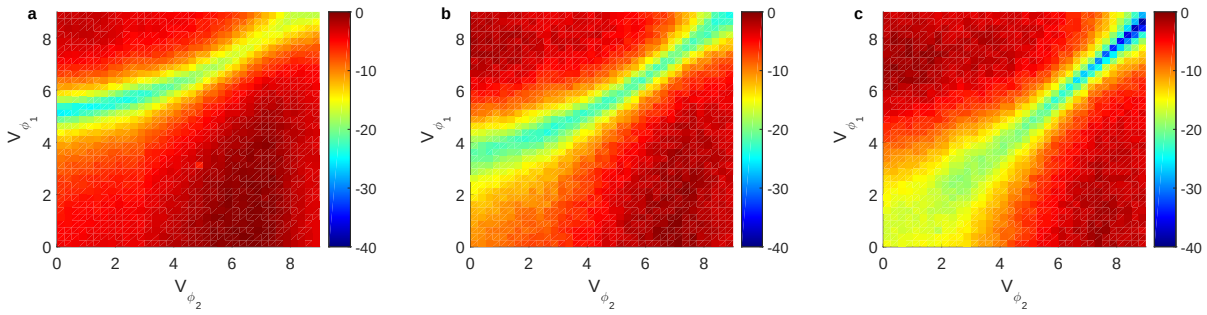

Figure 3.6: **Thermo-optic operation of EOPM:** Sweeps over V_{ϕ_1} and V_{ϕ_2} (a) $\Delta V_{\phi_2} =$ 0 mV showing the initial phase offset leading to a low intensity output at $V_{\phi_1} = 5$ V and $V_{\phi_2} = 0$ V (b) $\Delta V_{\phi_2} = 370$ mV (c) $\Delta V_{\phi_2} = 450$ mV shifts the minimum to where $V_{\phi_1} = V_{\phi_2}$ and allows very high extinction pulses for small EOPM voltage swings at $V_{\phi_1} = V_{\phi_2} \gtrsim 7$ V.

pads ($\Delta\phi = \phi_2 - \phi_2'$) to 450 mV the plot is now symmetrised and with no other EOPM DC offset the output is minimised. The effect of the two electro-optic phase modulators are now equal.

This now provides a consistent way of operating the devices. We set the DC EOPM offsets of ϕ_1 and ϕ_2 to ~7 V, and then adjust the thermo-optic phase shifter to minimise the output. The phase ϕ_2' is chosen to be always more reversed biased than ϕ_2 compared to the ground to ensure no forward biasing conditions are accidental incurred, which could damage the devices. Using the near quadratic nature of the EOPM at ~7 V DC offsets, switching ϕ_1 by less than 2 V we can now achieve a high extinction ratio (between 20-30 dB) with a small voltage swing required, minimising the power needed to drive the pulse modulator.

RF-Operation

When high speed electrical signals are to be used, transmission line physics must be considered if the length of the line is $\geq \frac{\lambda}{16}$, where λ is the wavelength of the signal. To connect to the chip electrically and operate in the GHz regime, transmission lines had to be designed to ensure good signal integrity to the chip. The lines should be made with 50 Ω characteristic impedance to maximise signal transmission, and limit reflections and distortions of the signal [185].

Design, simulations and test were implemented with Rogers 6006ns substrate which has a high dielectric ($\epsilon_r = 6.15$), and would allow for the etching of coplanar transmission

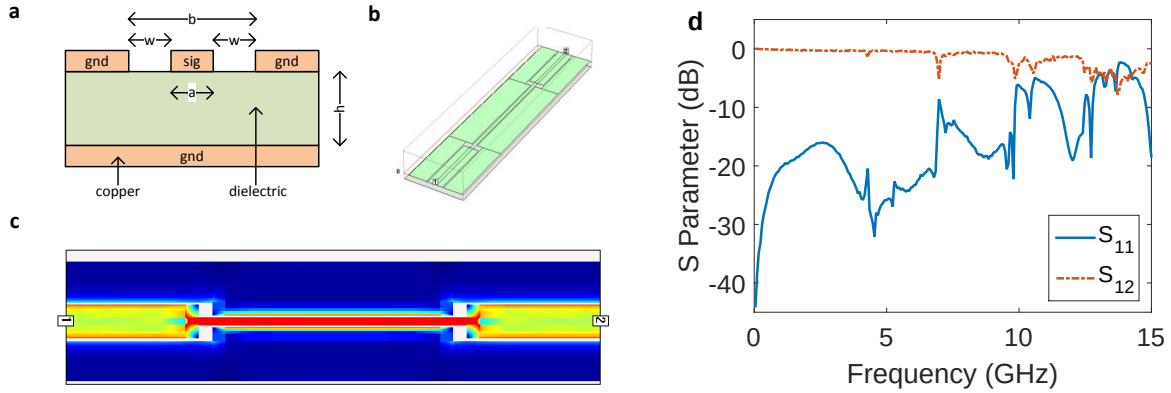

Figure 3.7: **RF Transmission Lines:** (a) Schematic of the coplanar with ground transmission line, consisting of a dielectric material with copper on the top and the bottom. (b) An example model of the coplanar waveguide with transitions from the standard SMA connector size and the calculated 50 Ω characteristic impedance waveguide. (c) Simulated results from the model in (b), illustrating confinement of high field intensities in the waveguide, but also areas of reflections and interference in the sharp corners. (d) An example frequency sweep of the transmission (S_{12}) and reflection (S_{11}) measurements made on a few cms transmission lines.

lines (laser etched with feature sizes ∼100 μm). These circuits consist of a signal line, with ground planes surrounding them on the top of the printed circuit board (PCB), and a large ground plane on the bottom of the PCB separated by dielectric (see Figure 3.7 (a)). The high dielectric and coplanar design would allow for thinner waveguides to limit dispersion, which becomes important when sending pulsed data.

The approximate characteristic impedance of the transmission line can be calculated by [186]

$$Z_0 = \frac{60\pi}{\sqrt{\epsilon_{\text{eff}}}} \frac{1}{\frac{K(k)}{K(k')} + \frac{K(k_l)}{K(k_l')}} \tag{3.2.6}$$

where

$$\begin{aligned} k &= \frac{a}{b} \\ k' &= \sqrt{1-k^2} \\ k_l &= \frac{\tanh(\frac{\pi a}{4h})}{\tanh(\frac{\pi b}{4h})} \\ k_l' &= \sqrt{1-k_l^2} \end{aligned} \tag{3.2.7}$$

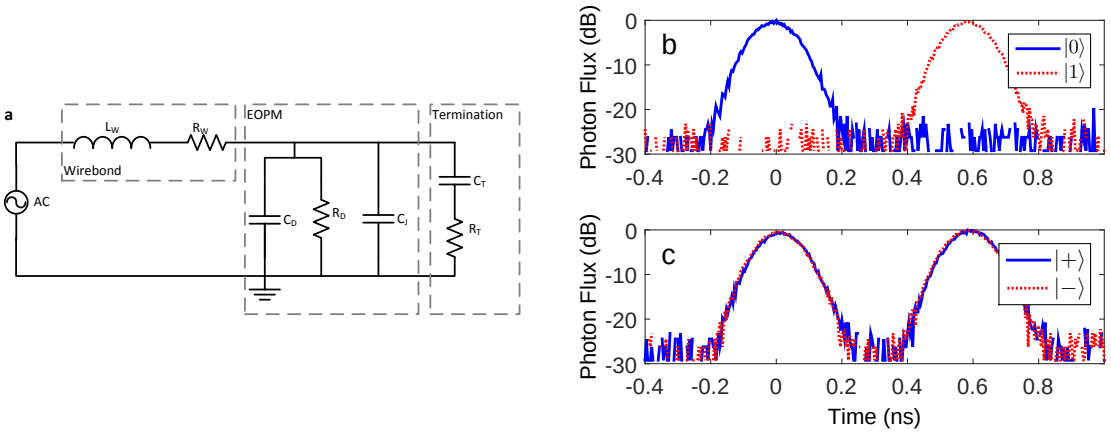

Figure 3.8: **RF EOPM Characterisation:** (a) A simple model for the termination circuit for each EOPM, including the resistance and inductance effects from the wire bond, the capacitance and resistance effects from the small signal model of a reversed biased diode, and the capacitor and resistor series combination to allow 50Ω impedance matching. (b-c) The resulting pulse shape showing an extinction ratio of ∼29 dB, FWHM of 134 ps, and separation of 580 ps between pulses.

where a is the width of the waveguide, b is the width of the waveguide plus the gaps between the waveguide and the ground ($b = a + 2w$), and the effective dielectric constant is defined as

$$\epsilon_{\text{eff}} = \frac{1 + \epsilon_r \frac{K(k')K(k_l)}{K(k)K(k_l')}}{1 + \frac{K(k')K(k_l)}{K(k)K(k_l')}} \tag{3.2.8}$$

where $K(k)$ is the elliptical integral of the first kind. With the dielectric thickness (h) of 250 μm this leads to 260 μm wide waveguides with a 100 μm gap between signal and ground planes for 50 Ω characteristic impedance. To avoid microstrip line modes its also recommended that $h \gg b$, and that the component side ground extends away from the track on each side much more than b. Although the limited thickness of this PCB substrate may lead to some microstrip line modes, the designs were verified with finite element simulations (Sonnet Lite), also incorporated the transitions between standard SMA side edge coupled electrical connections (Figure 3.7 (b) and (c)). Manufactured test circuits allowed for characterisation with a Vector Network Analyser (VNA - Keysight N5225A PNA Microwave Network Analyzer), that showed limited attenuation (S_{12} parameter) and ≤10 dB reflection (S_{11} parameter) within the 10 GHz regime (Figure 3.7 (d)).

The EOPM is terminated with a parallel combination of a DC-blocking capacitor and AC-terminating 50 Ω resistor in series, allowing for high-speed RF operation with limited

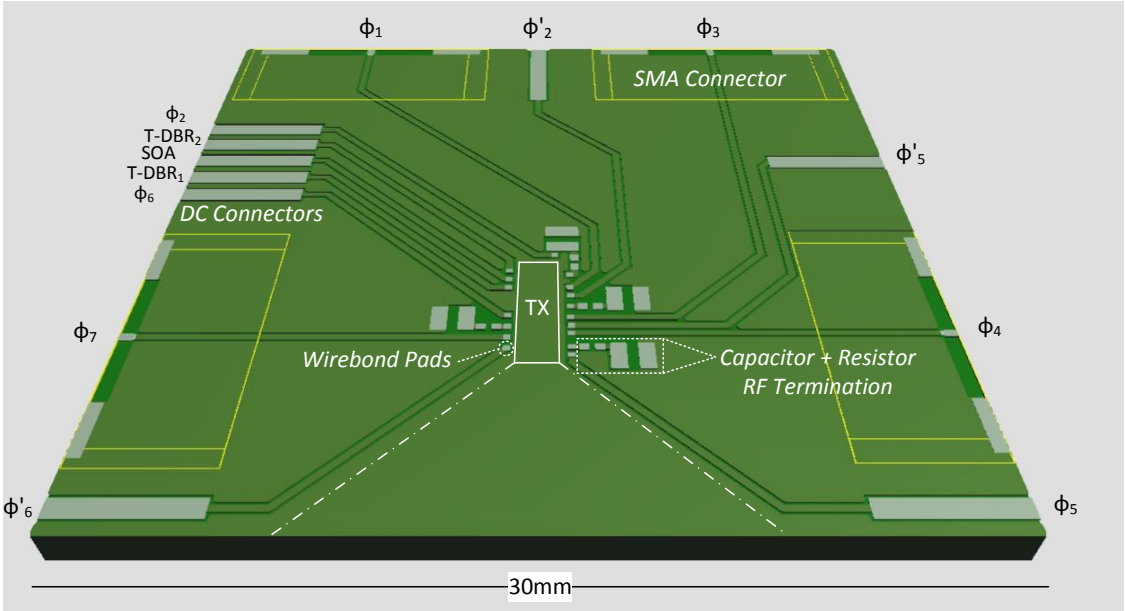

Figure 3.9: **RF PCB:** Rendering of the PCB design that allows connections to the relevant photonic components on the transmitter chip.

reflections (Figure 3.8). By concatenating two MZIs in series, one for timing intensity modulation (I.M) and one for phase encoding (PH.ENC), time bin encoded states can be prepared with an extinction ratio of ∼29 dB, FWHM of 134 ps, and pulse separation of 580 ps. This illustrates the high speed operation of our device and is given without compensating for detector jitter, time interval analysis, or trigger jitter.

A full PCB design is included in Figure 3.9 illustrating an example package, where the front section is removed to allow fibre coupling. The design is 3 by 3 cm^2 housing the 6 by 2 mm^2 photonic device, as well as four RF terminating capacitor and resistor combination, four SMA connectors (which constrained the design size), and 9 DC connections. Wirebonding pads were electrolytically gold plated to match the gold wirebond pads on the chip, and a section of the PCB was cut out to allow the side edged fibre optic coupling (the front two dashed lines).

3.2.3 Photodiode

The photodiode is a 1 GHz bandwidth, blocking (full absorption) waveguide-pin structure. This PIN photodiode structure can be used to monitor the output from the laser signal to ensure stable laser intensity, by providing feedback for current input to the SOA. It can also be used in characterisation, by maximising the power on the photodiode while sweeping the thermo-optic phase shifter, the alternative output will be minimised as described in Section 3.2.2.

3.2.4 Characterisation and Operation

Phase Encoding

To create $|+\rangle$ qubits, photon pulses are generated in the two temporal time bins with no phase change; however, the $|-\rangle$ state requires a π phase difference between the two pulses. Because of complications associated with driving the EOPM's to V_π, we instead can encode the π phase shift by applying $\{0, \phi\}$ and $\{\phi, 0\}$ to the top and bottom EOPMs in the MZI (PH.ENC - ϕ_6 and ϕ_7) during the first and second time bin respectively. The amplitude of the output of a balanced MZI is

$$E_{\text{out}} = E_{\text{in}}[\exp(\text{i}\phi_6) - \exp(\text{i}\phi_7)] \tag{3.2.9}$$

where ϕ_i is the phase modulator on either side of the interferometer. The amplitude of the first set of states is therefore

$$\begin{aligned} E_{\text{out}} &= E_{\text{in}}[\exp(\text{i}0) - \exp(\text{i}\phi)] \\ &= E_{\text{in}}[1 - \exp(\text{i}\phi)] \end{aligned} \tag{3.2.10}$$

and the amplitude of the second set of states is.

$$\begin{aligned} E_{\text{out}} &= E_{\text{in}}[\exp(\text{i}\phi) - \exp(\text{i}0)] \\ &= E_{\text{in}}[\exp(\text{i}\phi) - 1] \ . \end{aligned} \tag{3.2.11}$$

This gives the ratio of these two states as

$$\frac{1 - \exp \mathrm{i}\phi)}{\exp(\mathrm{i}\phi) - 1} = -1 = \exp(\mathrm{i}\pi) \tag{3.2.12}$$

which is equivalent to a π phase shift. We used this process to encode the π phase shift because we otherwise could not reach the required voltages without incurring too much loss or saturation in the EOPMs. Taking the phase induced loss into consideration, the ratio becomes

$$\frac{1 - \gamma(\phi)\exp(\mathrm{i}\phi)}{\gamma(\phi)\exp(\mathrm{i}\phi) - 1} = -1 = \exp(\mathrm{i}\pi) \tag{3.2.13}$$

ehich still allows for a good phase relationship no matter the intensity.

Reversing the combination of EOPM states also provides a π phase shift, but with a different global phase. This process was used to guide a calibration of the phase relationship and does not require the EOPMs to reach a full π range without loss, which is difficult to achieve with the QCSE driven EOPMs.

Bulk Optical Receiver To demonstrate this phase relationship and the ability to encode the BB84 quantum states, a bulk optical receiver was constructed to decode the signals. Illustrated in Figure 3.10 (a), the receiver contained a fibre-based polarisation controller before outputting to free space. Once in free space the path was incident on a polarisation beam splitter (PBS) that transmits horizontal and reflects vertical polarisation states. The combination of the polarisation controller and PBS allows a portion of the signals to be directed into a collection stage and towards a single photon detector (SPD) and the other portion in to an AMZI. The AMZI contains two 50:50 beam splitters (BS), and extra delay arm made from two mirrors. The mirrors were mounted on top of a translation stage for coarse temporal alignment of the delay which also had piezo control for fine control of the phase relationship between the two arms. To alter the phase by 2π would be 1.55 μm in free space, which was $\sim$4 V on the piezo driver. The two outputs of the AMZI were incident on fibre collection stages connected to the inputs of single photon detectors.

The entire system was enclosed in a polystyrene box for temperature stability, and placed on an air-lifted optical bench to reduce vibrations. This still lead to drift in the

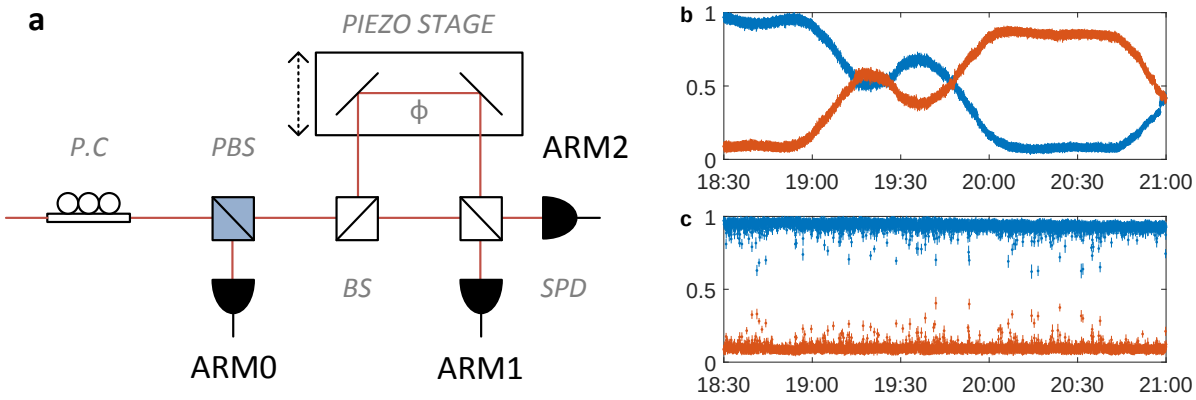

Figure 3.10: **Bulk Optical Receiver Stability:** (a) Schematic of the bulk optical receiver circuit. The polarisation controller (P.C) and the polarisation beam splitter (PBS) allow a portion of the signal to be sent straight to a detector (SPD). The remaining portion enter an AMZI made from two 50:50 beam splitters (BS), and two mirrors mounted on a piezo controlled translation stage allowing for coarse temporal adjustments and fine phase control. (b) The normalised power of the two outputs of the AMZI with thermal insulation and vibration damping. (c) The normalised power of the two outputs of the AMZI with thermal insulation, vibration damping and PID feedback loop to provide a consistent phase relationship.

system as if evident in Figure 3.10 (b) where the red and blue signals are the normalised measured power of the two outputs of the AMZI, and drift relative to each other over the time of a few hours. To compensate for this drift, a feedback loop was implemented that measured and optimised the visibility ($\frac{I_0-I_1}{I_0+I_1}$) periodically using a PID (proportional integral differential) feedback scheme [187]. This led to for a more consistent phase relationship (Figure 3.10 (c)).

With this stabilised system, measurements on the phase relationships could be demonstrated as illustrated in Figure 3.11. The four BB84 states were sent through the bulk optical receiver device and decoded through the passive basis choice as displayed in Figure 3.11 (a) where the first time bin of both output arms represent a $|0\rangle$ state measurement, the last time bin of both output arms represent a $|1\rangle$, the middle time bin of ARM1 represents a $|+\rangle$ and the middle time bin of ARM2 represents a $|-\rangle$. The probability of measurement for the ideal case is represented in Figure 3.11 (b), where the left axis is the transmitted state, and the right axis in the measured state normalised for a unit probability. For example if the $|0\rangle$ state is sent then half the time it is measured in the $\{|0\rangle, |1\rangle\}$ basis and always measured as $|0\rangle$, half the time it is measured in the $\{|+\rangle, |-\rangle\}$

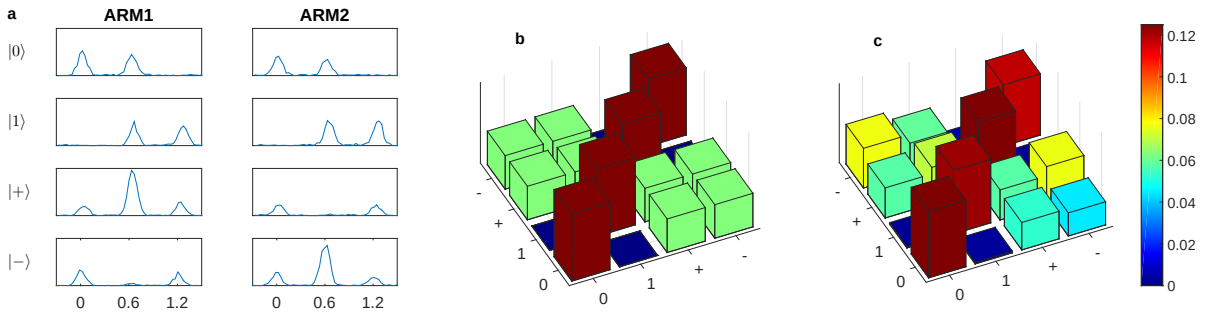

Figure 3.11: **Bulk Optical Receiver with BB84 States:** (a) Histograms of single photon detector events for the four BB84 states sent in time bin encoded and measured through the bulk optical receiver circuit. Measurements in the first timing window of both ARM1 and ARM2 represent the measurement of a $|0\rangle$ and measurement in the third timing window represent the measurement of a $|1\rangle$ state. Measurement in the second timing window of ARM1 represents a $|+\rangle$ state and measuring in the second timing window of ARM2 represents a $|-\rangle$. (b) The ideal probability of each measurement outcome (right axis) given the input state (left axis) normalised to probability 1. (c) Experimental measurements from the integrated transmitter and bulk optical receiver circuits.

basis with equal probability of each outcome. The experimental results are shown in Figure 3.11 (c), and are in good agreement with the ideal case, demonstrating the capability of time and phase encoding required for BB84.

Phase Randomisation

Phase randomisation is required to match the security analysis in decoy state protocols [62, 93]. This is achieved by the single electro-optic phase modulator (PH.RAND - ϕ_3 is Figure 3.2). The phase for each qubit sent is randomly chosen from a set of 10 discrete phases between 0 and 2π which are themselves randomly chosen. This is sufficient to approach the asymptotic limit of perfect phase randomisation [188, 189].

The issue described before of phase dependent loss also comes into relevance in this section. To limit the effects of phase dependent loss it should be first noted that in Section 3.2.4 it was highlighted that there were two ways of encoding a $|+\rangle$ state and two ways of encoding $|-\rangle$ state, and that the global phase difference between them would be π. This can be used to provide a random π phase shift and limits the amount of phase that ϕ_3 in Figure 3.2 needs to cover.

Other methods of phase randomisation could be explored, including switching the laser

below threshold between each states. By injecting sufficient current when initially below the lasing threshold the stimulated emission event is based on a random spontaneous emission event and therefore allows a random global phase based on a quantum process. This has been demonstrated in [190], but may also still contain some correlations between neighbouring pulses if the laser does not become completely depleted. This technique is also used to generate amplified spontaneous emission quantum random numbers, but often with the help of classical cryptographic post-processing to ensure the random numbers do not contain these correlations [191].

Quantum Random Number Generation

The quantum random numbers for selecting bit and basis values were generated offline, prior to key exchange, using the transmitter chip as a quantum random number generator (QRNG). The temporally modulated weak coherent source and an on-chip MZI acting as a beamsplitter were used to randomly split photons to one of two off-chip fibre-coupled superconducting nanowire single photon detectors [192], producing a random stream of 0's and 1's. To achieve a fair or appropriately biased coin, the values were fed through a Bernoulli factory [193] to provide coins with the required probability statistics. For example, an even output coin 0 followed by 1 is output as 0, and 1 followed by 0 is output as 1, and other pairs are discarded. These two outcomes have the same probability no matter the input bias of $\{p, (1-p)\}$ for choosing $\{0, 1\}$ and is most efficient when $p \sim 0.5$. Once generated, these quantum random numbers were used to set the basis, bit, decoy intensities, and phase randomisation for each qubit sent. Further methods for quantum random number generation and post-processing techniques are discussed in Chapter 6.

3.3 Integrated Receiver Circuit

The integrated receiver circuit, shown in Figure 3.12, is a monolithically fabricated SiO_xN_y device comprised of passive waveguides and thermo-optic phase shifters combined into interferometers to route signals and decode timing and phase information for multiple-protocol quantum key distribution. The photonic signals are detected by off-chip superconducting nanowire single photon detectors [173] to convert single photons into classical

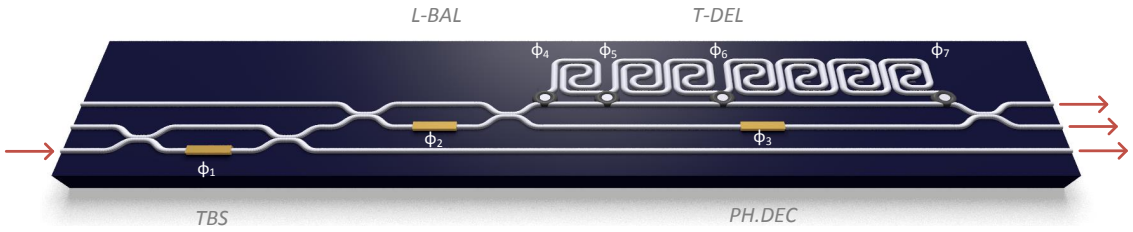

Figure 3.12: **Integrated Receiver Circuit Schematic:** Illustration of the integrated SiO_xN_y receiver circuit with thermo optic phase shifters ϕ_1 to ϕ_7. Each controls the phase relationship in either a balanced MZI (ϕ_1, ϕ_2 and ϕ_4 to ϕ_7) or AMZI (ϕ_3). The circuit consists of a MZI to control the portion of the signal straight to a detector (TBS) and the rest in the phase decoding AMZI. This AMZI contains a reconfigurable discrete time delay and a loss balancing MZI (L-BAL) to compensate for the propagation loss in the longer arm.

electronic signals.

For the integrated receiver device, the SiO_xN_y material system was chosen to minimise photon loss from fibre-to-chip coupling and waveguide propagation loss, whilst maintaining a compact footprint. This device, along with fibre coupled single photon detectors, represent the full photonic QKD receiver.

The SiO_xN_y receiver chip was fabricated using the TripleX technology platform [175], where alternating layers of Si_3N_4 and SiO_2 were deposited and etched to create a "double stripe" structure to guide light in a high index-contrast but low loss waveguides ($\sim$0.5 dB/cm), and with low coupling loss between chip and fibre ($\lesssim$2 dB), yielding a total loss $\sim$ 9dB for BB84 configuration, excluding the detector system. Metal layers on top of the structure created thermo-optic phase shifters for circuit reconfigurability.

As illustrated in Figure 3.12, the first MZI acts as a tunable beamsplitter (TBS) and taps off a portion of the incoming signal, which was routed to a single photon detector and used primarily for the COW protocol (see Section 3.4). The second MZI (L-BAL) acts to balance the losses in the asymmetric MZI (AMZI), which incorporates a digitally reconfigurable delay line, tunable from 0 to 2.1 ns in steps of 300 ps. The thermo-optic phase shifter (TOPS) within the AMZI was used calibrate the phase relationship between the two arms of the interferometer. Light was coupled out of the device and into external fibre-coupled superconducting nanowire single-photon detectors mounted in a closed cycle refrigerator [173] which had an system detection efficiency of $\sim$45% from the fibre input,

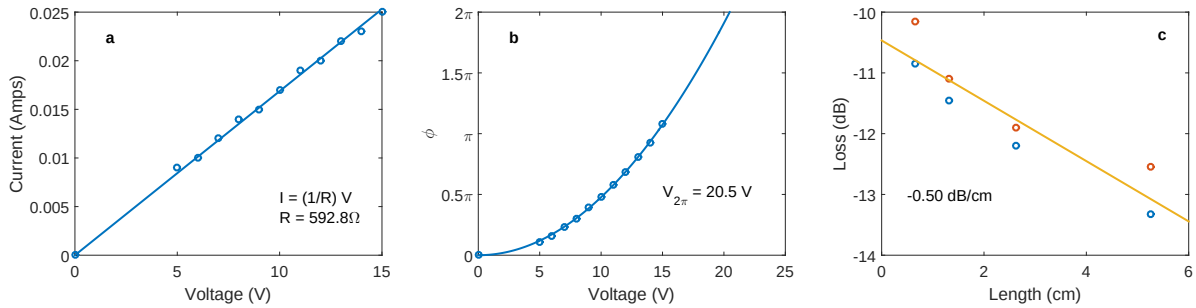

Figure 3.13: **Receiver Circuit Characterisation:** (a) Current versus Voltage plot for a 1.5 mm thermo-optic phase shifters showing a resistance of ∼590 Ω. (b) Phase (in units of π) versus voltage, showing a quadratic relationship and a 2π phase shift at ∼20 V. (c) Loss versus length measurements from 2 separate copies of the device, leading an estimate of 0.5 dB/cm.

a temporal jitter of ∼50 ps, and a dead-time of ∼10 ns.

The entire chip is temperature controlled with a Peltier controller and thermistor feedback loop to maintain a constant phase relationship in the asymmetric interferometer structures used to decode phase information.

3.3.1 Thermo-Optic Phase Shifters

The thermo-optic phase shifters (TOPS) are a chronium-gold metal layer on top of the passive triplex waveguide structure creating a resistance. With a length of 1.5 mm the phase shifters have a resistance of ∼590 Ω and reach a 2π phase shift at ∼20 V (Figure 3.13 (a) and (b)). The thermo-optic coefficient is linear with power and therefore quadratic with voltage. The TOPS were characterised inside MZIs formed from two directional couplers acting as 50:50 reflectivity beamsplitters.

3.3.2 Loss

Propagation loss was measured to be around 0.5 dB/cm, or 8.0 dB/ns when considering the group refractive index of 1.7 [175]. This was measured using 4 different lengths of waveguide that allow a linear fitting to remove the effects of coupling loss (Figure 3.13 (c)). The fibre to chip facet loss was between 1.7 - 5 dB loss depending on alignment and index matching gel with polarisation maintaining single mode fibre arrays.

This insertion loss and the detector efficiency was the main factor that limits the

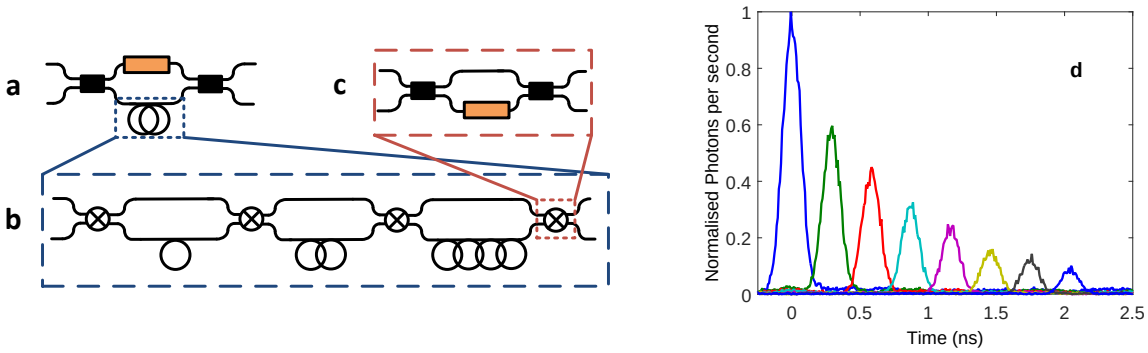

Figure 3.14: **Receiver Circuit and Discrete Time-bins:** Schematic diagram of the (a) asymmetric Mach-Zehnder interferometer (AMZI), (b) digital delay lines, (c) MZI used to switch the signal into the different discrete delay line choices, and (d) the loss incurred for each of the possible digital delays.

achievable rates. Improvements in performance could be achieved with lower insertion losses, such as demonstrations of 0.7 dB loss in fibre-to-chip coupling in silicon [194] and 1.2 dB/m propagation loss in Si_3N_4 [195].

3.3.3 Discrete Time Bins

The asymmetric MZI is used to decode the phase encoded information and allows for discrete time bins to be chosen as illustrated in Figure 3.14 (a)-(b). Combinations of 1 bin, 2 bins, and 4 bins can be included in the delay by tuning MZI switches (Figure 3.14 (c)), allowing for any delay between 0 and 2.1 ns in steps of ∼300 ps. Increasing the delay does bring with it increasing loss, as shown in Figure 3.14 (d). For further calibration techniques see Section 4.3.2.

This design allows for a single receiver design to facilitate communication between a range of devices using different protocols and clock rates, which could be necessary in a network setting.

3.3.4 Calibration and Timing

To balance the loss inside the longer arm of the asymmetric MZI, there is a MZI (L-BAL) which routes a larger percentage of signal into the longer arm than the shorter arm. This percentage should allow for equal intensities in both arms at the recombination

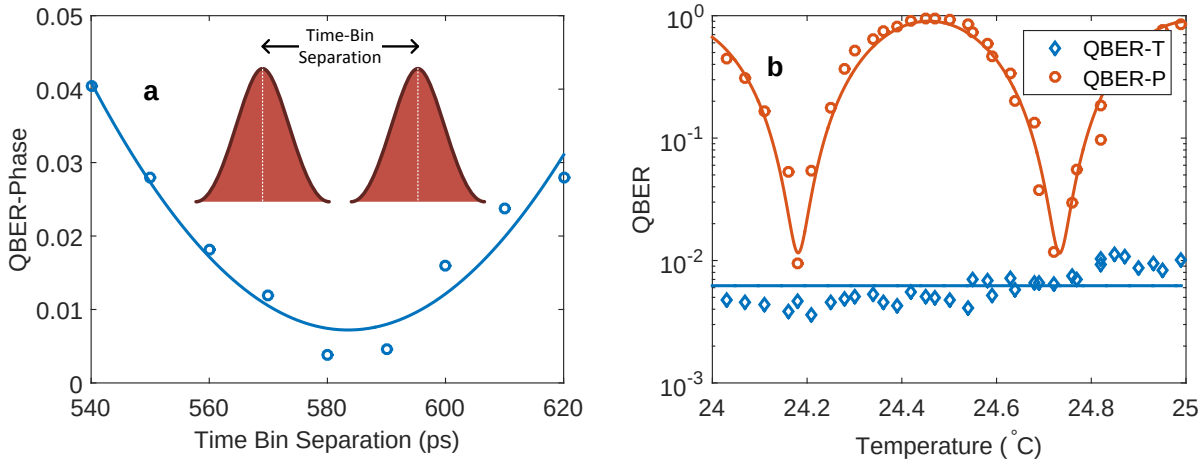

Figure 3.15: **Timing and Phase Calibration:** (a) Calibration of the optimum temporal delay, representing the time-bin separation, on Alice's transmitter which produces the lowest QBER when measuring qubits sent through Bob's receiver, and (b) the drift in the QBER due to the timing information (QBER-T) and phase information (QBER-P) as a function of the temperature of the receiver chip.

beamsplitter. To calibrate this tuning, the phase is swept and visibility is maximised.

To minimise the QBER due to the timing and phase errors, the temporal delay between the electronically defined time-bins on the transmitter chip was adjusted to match one of the fixed digital delays on the receiver chip. The optimum was found to be ∼580 ps, as shown in Figure 3.15 (a). Figure 3.15 (b) shows that sweeping the temperature of the chip does not affect the temporal information (QBER-T); however, the phase relationship between the two arms does change (QBER-P). The temperature corresponding to the minimum QBER-P was chosen. Further techniques for phase calibration are discussed in Section 4.2.2.

3.3.5 Stability

To test the ability to encode the BB84 quantum states from the integrated transmitter device, a ($60\times60\times60$ cm^3) bulk optical receiver was constructed to allow for the decoding of the signals. Illustrated in Figure 3.16 (a), the receiver contained a fibre-based polarisation controller before outputting to free space. Once in free space the path was incident on a polarisation beam splitter (PBS) that transmits horizontal and reflects vertical polarisation states. The combination of the polarisation controller and PBS allows a portion

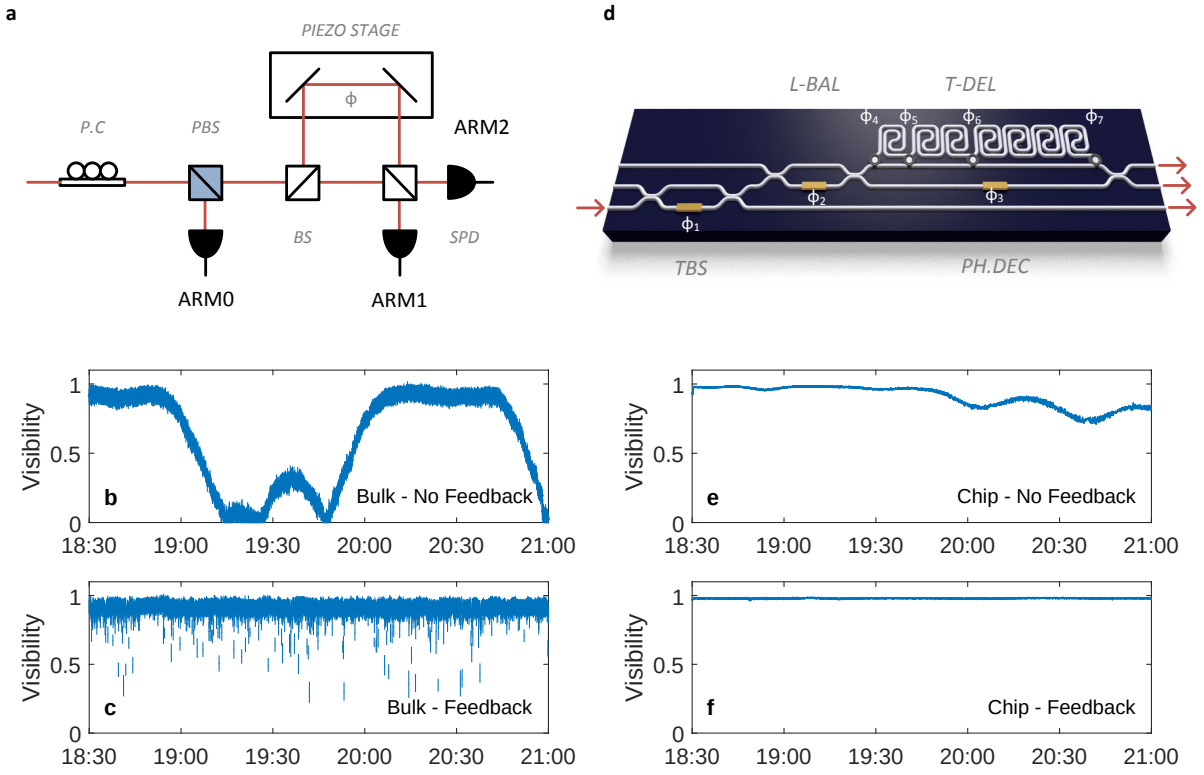

Figure 3.16: **Interferometer Stability:** (a) Schematic of bulk optic interferometer. (b) Visibility measure without feedback illustrating noise and drift over time, and (c) with gradient descent feedback on the piezo-stage, reducing the drift but still suffering from noise. (d) Schematic of the integrated device interferometer. (e) Visibility without feedback illustrating a slower level of drift, and (f) with feedback, showing a reduction in drift and noise.

of the signals to be directed into a collection stage and towards a single photon detector (SPD) and the other portion in to an AMZI. The AMZI contains two 50:50 beam splitters (BS), and extra delay arm made from two mirrors. The mirrors were mounted on top of a translation stage for coarse temporal alignment of the delay which also had piezo control for fine control of the phase relationship between the two arms. To alter the phase by 2π would be 1.55 μm in free space, which was $\sim$4 V on the piezo driver. The two outputs of the AMZI were incident on fibre collection stages connected to the inputs of single photon detectors.

The entire system was enclosed in an insulating polystyrene box for temperature stability, and placed on an air-lifted optical bench to reduce vibrations. This still lead to noise and drift in the system as is evident in Figure 3.16 (b) where we illustrate the visibility ($\frac{I_0-I_1}{I_0+I_1}$) over time. To compensate for this drift, a feedback loop was implemented

that measured and optimised the visibility periodically using a gradient descent feedback scheme, using the piezo controller for fine phase control. This led to for a more consistent phase relationship (Figure 3.16 (c)).

We further compare these results to the (2×32 mm^2) integrated receiver device illustrated in Figure 3.16 (d). The chip was temperature controlled with a PID loop measuring a thermistor resistance and with a Peltier device to sink the heat generated from the thermo-optic phase modulators. Without any other feedback (Figure 3.16 (e)) we see a less noisy visibility measurement and longer stability period. Figure 3.16 (f) shows further improvement, by implementing a gradient descent feedback scheme with the thermo-optic phase shifter (ϕ_3) a stable visibility measurement was achievable, without the same level of fluctuations and noise seen in the bulk interferometer.

3.3.6 Superconducting Single Photon Detectors

This experiment utilised external fibre coupled superconducting nanowire single-photon detectors (SNSPD) [173] mounted in a closed cycle refrigerator which had a system detection efficiency of ∼45%, an average dark count rate of ∼500 Hz, and dead times on the order of 10 ns. The operating voltage bias was chosen to optimise the signal to noise of the detectors, by limiting the dark counts compared to the single photon counts per second when signals are sent. The detector signals were discriminated with a Hydraharp 400 from PicoQuant, which provides up to 8 channels with up to 1 ps timing bin resolution and an internal jitter of ∼12 ps rms. The overall timing jitter was estimated to be around 50-60 ps when using a coaxial cable to provide the synchronisation of the system.

The detector results were binned in time and gated by a top-hat window function after the measurements were taken, only including measurements arriving inside the window in the raw and secret key counts. This window was centred around the mean value of the histogram measurements and the width chosen to be the FWHM of a fitted Gaussian. Further optimisation can be taken to improve the rates by scanning this window size to compare the absolute raw count rate and the error rate as illustrated in Figure 3.17. The QBER increases roughly linearly compared to the gating window due to the increase collection of dark counts and the inclusion of lower extinction sections of the pulse. The

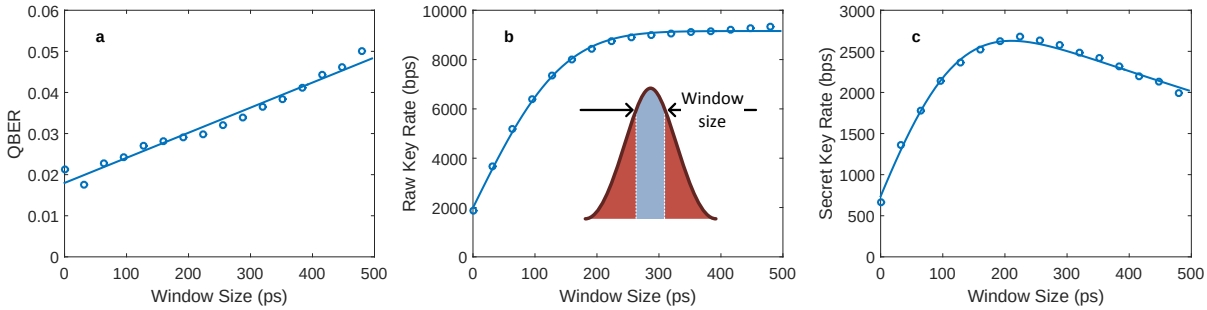

Figure 3.17: **Secret Key Rate against Detector Window:** (a) The QBER against the detector gating window. (b) An example raw key rate against the detector gating window. (c) The combination of the increasing error rates (which decreases the secret key) and increasing raw count rates (that increases the secret key rate) leads to an optimum choice for the window size.

raw counts will also further increase as the gating window increases, but saturates soon after the FWHM. The combination of raw count rates and error can produce an estimate for the secret key rate that can be maximised by choosing an appropriate window size ∼200 ps given a pulse with a FWHM of 150 ps.

This post processed gating scheme was suitable to use with the SNSPD system as the dead time is sufficiently short, the jitter sufficiently small and the rates sufficiently low to not miss many results from counts outside the gating window. In other systems such as InGaAs detectors, timing jitter, dark counts and after pulsing probabilities require the use of gating schemes, which can not be achieved in post processing [196].

3.4 Protocols

These devices are sufficiently flexible to encode and decode quantum information for a number of different QKD protocols. This provides an opportunity in a network setting of using single generic devices that can operate with many different standards, clock rates, and protocols.

3.4.1 BB84

The BB84 quantum key distribution protocol [42] transmits 4 states, consisting of 2 orthogonal states in 2 non-orthogonal bases. In a time-bin encoding this can be achieved

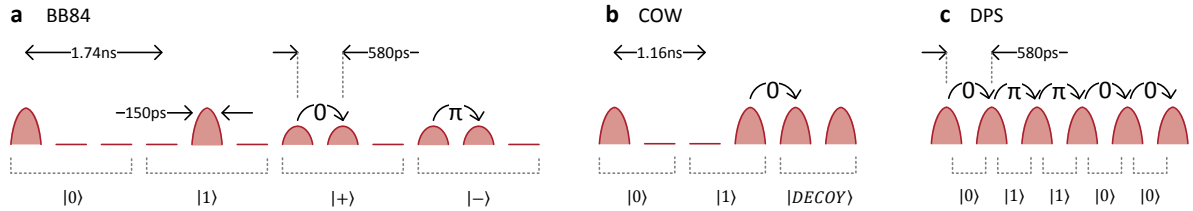

Figure 3.18: **Protocol State Timing Diagrams:** (a) The four states for the BB84 protocol, where $|0\rangle$ and $|1\rangle$ are encoded by photons in the first or second time-bin respectively, and $|+\rangle$ and $|-\rangle$ are encoded with a photon in a superposition of being in the first and second time-bin with a 0 and π phase shift respectively. (b) The three states for the COW protocol, where $|0\rangle$ and $|1\rangle$ are again encoded by photons in the first or second time-bin respectively and security is monitored by measuring the coherence across a pair of pulses from any combination of the $|\text{DECOY}\rangle$, $|0\rangle$, and $|1\rangle$ states. (c) The pulse-train used for the DPS protocol, where 0 and 1 are encoded as a phase of 0 or π respectively between pulses and security is monitored by measuring the coherence between pulses which shows up as errors in the measured bit values.

through $|0\rangle$ encoded by a photon in the first time-bin $|0\rangle_t |\alpha\rangle_{t-\tau}$, $|1\rangle$ encoded by a photon in the second time-bin $|\alpha\rangle_t |0\rangle_{t-\tau}$, $|+\rangle$ encoded by a photon in a superposition of being in the first and second time-bin with no relative phase change $\left|\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$ or $\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|-\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$, and $|-\rangle$ encoded by a photon in a superposition of being in the first and second time-bin with a π relative phase change $\left|\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|-\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$ or $\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$. The four states are illustrated in Figure 3.18 (a).

The integrated transmitter modulates the continuous wave laser source, selecting the time-bin choice. The light is then phase randomised, attenuated and intensity modulated. Additionally, we attenuate the average photon number per pulse of the $\{|+\rangle, |-\rangle\}$ basis to half the intensity of the $\{|0\rangle, |1\rangle\}$ basis to maintain the same average photon number for each state. The final MZI encodes the relative phase between successive time-bins to implement a $|-\rangle$ state.

The four possible BB84 states enter the AMZI, which overlaps successive time-bins to allow phase information to interfere, creating three possible time-bins within which to detect photons. Measurement of a photon in the first or third time-bin in either detector constitutes a measurement in the $\{|0\rangle, |1\rangle\}$ basis with the first time-bin indicating a $|0\rangle$ and the third time-bin indicating a $|1\rangle$; whereas, measurement in the second time bin constitutes a measurement in the $\{|+\rangle, |-\rangle\}$ basis with the top detector indicating a $|+\rangle$

and the bottom detector indicating a $|-\rangle$. This design allows the receiver to use a passive optical detection circuit, once the appropriate phases are set on the TOPS, removing the need for high-speed quantum random numbers and an active basis selection in the receiver. While this has been a common detection scheme in many different experiments, it can potentially open a security loophole, which can be mitigated with active basis selection [197].

To increase data rates and range, the states are phase randomised and decoy intensity levels are used. This allows for the security rate to be calculated following the security proof of Ma *et al.* [62]

$$K_{\mathrm{BB84}} = q\nu_s \left\{ -Q_\mu f_{\mathrm{EC}}(\epsilon_\mu) h(\epsilon_\mu) + Q_1^{\mathrm{L}} \left[1 - h(e_1^{\mathrm{U}}) \right] \right\} \tag{3.4.1}$$

where $q = \frac{1}{2}(\frac{N_\mu}{N_{\mathrm{t}}})$. Here N_μ is the number of μ intensity signals measured, and N_{t} is the total number counts. The $\frac{1}{2}$ is the sifting factor of standard BB84, and ν_s is the repetition rate. $f_{\mathrm{EC}}(\epsilon_\mu)$ is the error correction efficiency (which we set to $f_{\mathrm{EC}}(\epsilon_\mu) = 1.2$ based on literature estimates), $h(e) = -e\log_2(e) - (1-e)\log_2(1-e)$ is the binary Shannon entropy, and Q_μ and ϵ_μ are the transmission probability and QBER respectively of a pulse with the signal intensity μ.

The remaining quantities Q_1^{L} and e_1^{U} are estimated using the following formulas. The lower bound for the single photon transmittance, Q_1, which represents the probability that the signal state contains 1 photon and that the receiver detects just 1 photon, is calculated to be

$$Q_1 \geq Q_1^{\mathrm{L}} = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \left[Q_{\nu_1}\mathrm{e}^{\nu_1} - Q_{\nu_2}\mathrm{e}^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu \mathrm{e}^{\mu} - Y_0^{\mathrm{L}}) \right] \tag{3.4.2}$$

where Q_i is the transmission probability of a pulse with the intensity $i \in \{\mu, \nu_1, \nu_2\}$, μ represents the signal state intensity, and (ν_1, ν_2) are the two decoy state intensities (weak and vacuum). Y_0^{L} is the lower bound for the count probability of an empty pulse, obtained from

$$Y_0 \geq Y_0^{\mathrm{L}} = \frac{\nu_1 Q_{\nu_2}\mathrm{e}^{\nu_2} - \nu_2 Q_{\nu_1}\mathrm{e}^{\nu_1}}{\nu_1 - \nu_2} \,. \tag{3.4.3}$$

Finally, the QBER for each intensity is represented as e_i, and the upper bound for the

single photon QBER, e_1, is given by

$$e_1 \leq e_1^{\mathrm{U}} = \frac{\mu}{\nu_1 - \nu_2} \frac{e_{\nu_1} Q_{\nu_1} \mathrm{e}^{\nu_1} - e_{\nu_2} Q_{\nu_2} \mathrm{e}^{\nu_2}}{Q_1^{\mathrm{L}} \mathrm{e}^{\mu}} \ . \tag{3.4.4}$$

The effects of error correction and privacy amplification are considered without finite key analysis since the focus of this work is on the devices. The effects of finite key analysis heavily depend on a number of system-specific factors, including the amounts of key sent in a particular transmission.

3.4.2 COW

Distributed phase reference protocols require similar operations to BB84, including temporally defining states and implementing relative phases. In Coherent-One-Way (COW) QKD [2], the key information is encoded in the timing of the pulses while the security of the channel is monitored through the coherence of successive pulses. To implement COW, we transmit a train of light pulses, with an average photon number $\mu < 1$ in each pulse. At time t, for each pair of time-bins there are three possible states: $|0\rangle$ has a photon in the first time bin, represented as $|0\rangle_t |\alpha\rangle_{t-\tau}$; $|1\rangle$ has a photon in the second time bin, represented as $|\alpha\rangle_t |0\rangle_{t-\tau}$; and $|\mathrm{DECOY}\rangle$ consists of photons in both time bins $|\alpha\rangle_t |\alpha\rangle_{t-\tau}$. The three states are illustrated in Figure 3.18 (b). In this representation τ is the repetition rate of the train of pulses.

To decode the information sent over the quantum channel a portion of the signal is detected directly by an SNSPD while the rest of the signal is sent through an asymmetric MZI. The directly detected signals allow Bob to learn Alice's bit value through its time-of-arrival thus generating the key. The security of the channel is monitored through the coherence of successive photon pulses. This is done by setting the delay in the AMZI equal to the temporal period, τ, separating each pulse in the train of pulses so that successive pulses of light are overlapped and interfered, the visibility of which is monitored. In this protocol, the phase between the pulses in the state $|\mathrm{DECOY}\rangle$ is not changed and therefore these should always constructively interfere and be output from the first arm when successive pulses of photons are sent. Further, Bob's device also measures the

coherence across half a decoy pulse and either of the $|0\rangle$ or $|1\rangle$ states or even across the $|0\rangle$ and $|1\rangle$ states. This added benefit of having the coherence distributed both within and across signal separations means that Eve cannot count the number of photons in any finite number of pulses without introducing errors, thus prohibiting any photon number splitting (PNS) attacks [2, 59].

While the key was generated unambiguously from the time of arrival of the single photon in a pair, security of the channel was determined by measuring the visibility from interfering successive photon pulses. A decoy state, with photon pulses in each time-bin ($|0\rangle$ and $|1\rangle$), was included to increase the probability of occupied successive pulses, allowing a more accurate measurement of interference. Using the first MZI, the receiver routes a larger proportion of the input signal to single photon detectors for key generation, and a smaller proportion to the AMZI for visibility measurement.

The derivation of a complete security analysis for COW is an on-going priority within the QKD academic community, including a proof of security against the photon number splitting attack and some collective attacks [2]. For this work, we use the upper bound security analysis of Branciard *et al.* [59] and chose the mean photon number per pulse of 0.28 when intending to send a photon. We estimated the secure key rate using

$$K_{\mathrm{COW}} = R\left\{1 - I_E^{\mathrm{COW}}(\mu) - f_{\mathrm{EC}}(\epsilon)h(\epsilon)\right\} \tag{3.4.5}$$

where R is the receiver raw key rate, $f_{\mathrm{EC}}(\epsilon)$ is the error correction efficiency (which we set to $f_{\mathrm{EC}}(\epsilon) = 1.2$ based on literature estimates), and $h(\epsilon)$ is the binary Shannon entropy. We calculate the remaining quantities as

$$I_E^{\mathrm{COW}}(\mu) = \epsilon + (1-\epsilon)h\left(\frac{1+F_V(\mu)}{2}\right) \tag{3.4.6}$$

where ϵ is the QBER, and $F_V(\mu)$ is given by

$$F_V(\mu) = (2V-1)\mathrm{e}^{-\mu} - \xi\sqrt{1-\mathrm{e}^{-2\mu}}\ . \tag{3.4.7}$$

This yields a positive key rate when $\mathrm{e}^{-\mu} > \xi \equiv 2\sqrt{V(1-V)}$, where V is the measured

visibility.

Further variants of the COW protocol have led to more general security proofs that could be the focus of future work [60]

3.4.3 DPS

The Differential Phase Shift (DPS) QKD protocol [54,55] encodes the key information in the relative phases between successive pulses in a pulse train, where 0 phase difference encodes a $|0\rangle$, and a π phase difference encodes a $|1\rangle$, each with an average photon number of less than 1. The qubits are thus delocalised across more than one pulse, removing the PNS attack since splitting off a photon from a pulse does not reveal any key information to an eavesdropper. Alice creates a steady train of photon pulses (similar to repeating the $|+\rangle$ and$|-\rangle$ states from BB84) with her first MZI (P.MOD), attenuates the source through the intensity modulator (I.M), and, using quantum random numbers, randomly encodes either a 0 or π phase between each pulse representing the key bits 0 and 1 respectively, as shown in Figure 3.18 (c).

The stream of data is sent directly to Bob where he uses his first MZI to direct all of the light to the top AMZI where successive pulses are overlapped to interfere constructively or destructively depending on the relative phase of successive photons. Referring to Figure 3.19, his top detector fires when a 0 phase is measured, while his middle detector fires when a π phase is measured. Any attempt by an eavesdropper to listen in to the communication will necessarily disturb the coherence of these states and produce errors in the measurement results.

An optimal average photon number of 0.28 was chosen for each pulse [59], and the secure key rate was estimated by

$$K_{\mathrm{DPS}} = R\left\{1 - I_E^{\mathrm{DPS}}(\mu) - f_{\mathrm{EC}}(\epsilon)h(\epsilon)\right\} \tag{3.4.8}$$

where I_E^{DPS} is calculated analogously to the COW protocol, but now the visibility and QBER are related by $\epsilon = \frac{1-V}{2}$. Unlike the COW protocol this result is not analytic, but the numerical calculations of Branciard *et al.* [59] show that its robustness under the same

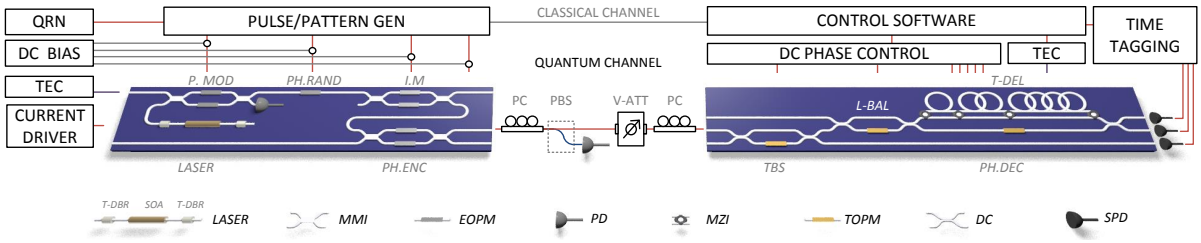

Figure 3.19: **Experimental Schematic:** Schematic of the reconfigurable integrated InP transmitter "Alice" chip (left) which encodes quantum information on weak coherent laser light to be sent over optical fibre to a SiO_xN_y receiver "Bob" chip (right). A temperature controller (TEC) and current driver stabilise the laser and control its intensity using feedback from an on-chip photodiode (PD). Electro-optic phase modulators (used to perform pulse modulation (P.MOD), phase randomisation (PH.RAND), intensity modulation (I.M), and finally phase encoding (PH.ENC)) are controlled through a combination of DC reverse biases (DC BIAS) and quantum random number (QRN) signals sent from a pattern generator through RF amplifiers. The polarisation of the optical output of the transmitter chip is filtered by a polarisation controller (PC) and polarisation beam splitter (PBS), and the quantum channel is emulated by a variable optical attenuator (V.ATT) .The receiver also requires a temperature controller (TEC) for phase stability and voltage sources (DC PHASE CONTROL) to control the thermo-optic phase modulators which determine the (passive) operation of the device. Off-chip superconducting nanowire single-photon detectors (SPD) detect the photons with time-tagging (TIME TAGGING) hardware, and control software synchronizes the experiment and post-processes the data.

family of attacks is very similar to COW and is used as an estimate of the performance of distributed-phase-reference protocols in the presence of errors [2].

Further variants of the DPS protocol with block phase randomisation have led to more general security proofs that could be the focus of future work [61].

3.5 Results

Our experimental configuration is shown in Figure 3.19, with Alice on the left and Bob on the right. Alice is a fully integrated Indium Phosphide (InP) [180] QKD transmitter capable of being modulated at GHz rates at standard telecommunications wavelengths, while Bob is an integrated Silicon Oxynitride (SiO_xN_y, Triplex [175]) QKD receiver capable of passively measuring Alice's signals. The control hardware and software used to operate the integrated devices is also shown.

On the transmitter side, a temperature controller (TEC) stabilises the laser wave-

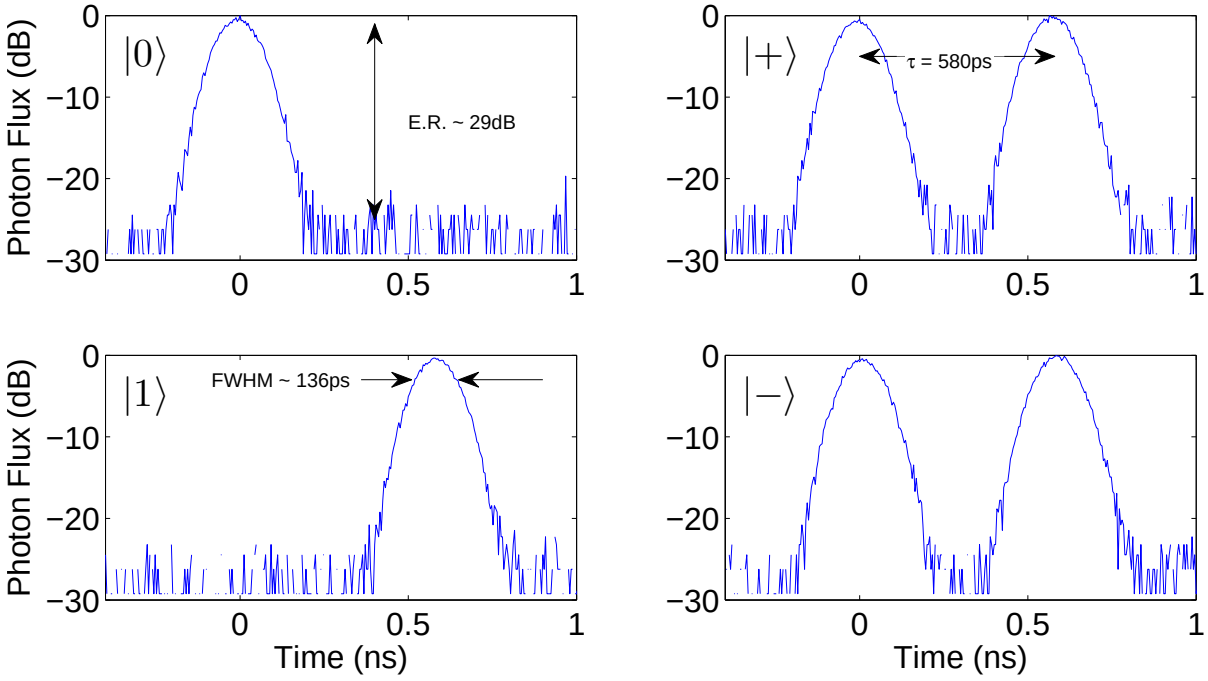

Figure 3.20: **BB84 States from Transmitter:** Transmitter output for the four BB84 states, demonstrating the 136 ps FWHM pulses with near 30 dB extinction, and temporal separation of 580 ps [181]. The measurements were made by directly detecting single photons straight from the transmitter using the SNSPDs and building up a histogram of time-tagged single photons.

length, while a current driver (CURRENT DRIVER) is used to control the intensity of the continuous wave laser using feedback from the photodiode (PD) via a transimpedance amplifier (TIA) when needed. Alice's electro-optic phase modulators (EOPM) are controlled through a combination of DC reverse biases (DC BIAS) and RF voltage levels from a pattern generator in order to perform pulse modulation (P.MOD), phase randomisation (PH.RAND), intensity modulation (I.M), and phase encoding (PH.ENC). For each qubit sent, the basis, bit, decoy intensities and phase randomisation are chosen using quantum random numbers (QRN) generated using Alice's chip prior to the key exchange.

The receiver also requires temperature control (TEC) for phase stability in the asymmetric Mach-Zender interferometer (AMZI) and voltage sources (DC PHASE CONTROL) to control the thermo-optic phase shifters (TOPS) determining the operation of the device. Off-chip super-conducting nanowire single-photon detectors (SNSPD) [173] are fibre coupled to the integrated devices and signals are time-tagged (TIME TAGGING) relative to a synchronisation signal sent from Alice over coaxial cable. Control software is

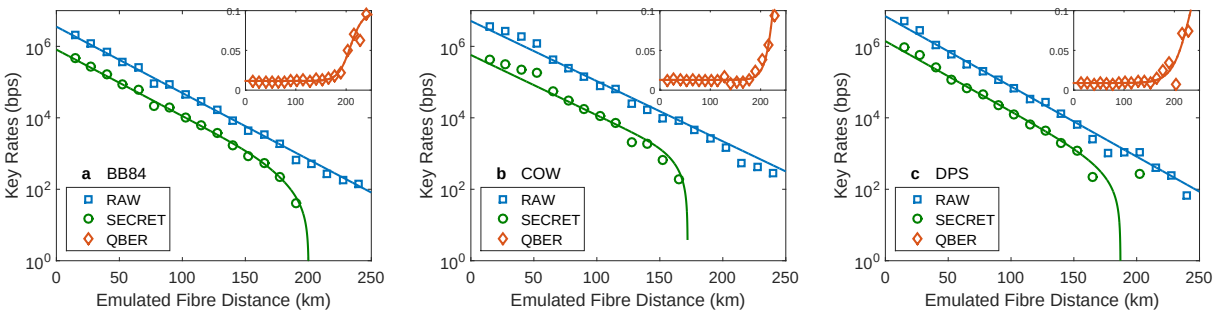

Figure 3.21: **Experimental Secure Key Rates:** Experimental results for (a) BB84, (b) COW, and (c) DPS showing the raw detection rate, estimated asymptotic secret key rate, and relevant QBER. For BB84 the QBER is derived from the timing and phase errors, while for COW the QBER is derived from the timing error and security of the channel is estimated from phase coherence between successive pulses, and finally for DPS the QBER is estimated based on the error from the phase encoded information. State (or clock) rates of 575 MHz, 860 MHz, and 1.72 GHz were used for BB84, COW, and DPS respectively [181].

used to synchronise the system and compare the generated and measured signals allowing the extraction of the successfully distributed raw key, measurement of the QBER, and estimation of the secret key rate.

The highly reconfigurable nature of the transmitter and receiver devices allowed the implementation of a number of different QKD protocols. Here, we specifically investigated the three protocols of BB84, COW and DPS as described in Section 3.4.

The CW laser source was modulated (P.MOD) to select the time bin choice, which were then phase randomised with a single electro-optic modulator (PH.RAND) before being attenuated and intensity modulated (I.M). The intensity of the $\{|+\rangle, |-\rangle\}$ states was reduced by half, compared to the $\{|0\rangle, |1\rangle\}$ states in order to maintain the same average photon number per state. The intensity modulator was also used to encode the decoy photon levels required to mitigate multi-photon contamination for security [62]. The final MZI encoded the relative phase between successive time bins to implement the $|-\rangle$ state.

Within the receiver chip, the digitally tunable delay line was reconfigured to match the 600 ps time interval between time-bins from the transmitter device. The first MZI (TBS) is used to directly measure the time of arrival information primarily for COW, and the AMZI can measure both phase and timing information through passive basis selection

Protocol	μ (per pulse)	State Rate (GHz)	QBER Time (%)	QBER Phase (%)	Secret Rate (kbps)	Attack Security	Key Analysis
BB84	0.45	0.58	1.17±0.18	0.92±0.11	345±15	General	Asymptotic
COW	0.28	0.86	1.37±0.15	1.36±0.16	311±50	Collective	Asymptotic
DPS	0.28	1.72	N/A	0.88±0.10	565±89	Collective	Asymptotic
BB84 [97]	0.42	∼1	$Q_{X,Z} \sim \{3.6, 4.3\}$		4390	Collective	Finite
COW [198]	0.06	0.63	2.4	0.85	248	Collective	Finite
DPS [199]	0.19	2.0	N/A	1.89	733	Individual	Asymptotic

Table 3.1: **Summary of Results:** Comparison of parameters and measured rates for the three QKD protocols over an emulated fibre link of 20 km, assuming 0.2 dB/km, using a digital variable attenuator. Further example parameters for 20 km (4 dB) links for biased-basis BB84 (1.09 Mbps at 50 km) [97], COW (12.7 kbps at 16.9 dB) [198], and DPS (1.16 Mbps at 10 km) [199] included for comparison. These values were either provided directly in the references or estimated/interpolated from the accessible data, and $Q_{X,Z}$ refers to the two basis QBERs, which were not directly comparable to the time and phase QBERs demonstrated in this work.

for BB84, and the coherence of the channel for DPS and COW. In this experiment the receiver chip was mounted on a metal core PCB and optically coupled with a v-groove array which in turn was mounted on a multi-axis alignment stage. This lack of fixed coupling led to slight variation in the rates in Figure 3.21.

Each of the above three protocols was implemented on the chip-to-chip system, where the length of optical fibre link was emulated using a variable optical attenuator to induce channel loss, where a loss of 0.2 dB/km was assumed (standard within telecommunications fibres at 1550 nm), although rates could be improved through use of low loss fibres [198], and the distance extending by optimising the SNSPDs for ultra low dark counts [200]. The effects of dispersion were considered negligible for the broad ∼150 ps pulses used here, although future field trials will verify this claim. The performance of our integrated devices for all three protocols is shown in Figure 3.21, where the raw key rate, estimated secret key rate, and QBER observed are plotted. For BB84, using an attenuation equal to 20 km of fibre we obtained an estimated secret key rate of 345 kbps using a clock rate of 575 MHz; using average single photon numbers of 0.45, 0.1, and 5.0×10^{-4} for the signal and two decoy states chosen with probabilities of 0.8, 0.15, and 0.05 respectively; and observed an average QBER of 1.05%. The secret key rate for BB84 was calculated using the raw and sifted key rates, and the measured QBER, using the security proof of Ma *et*

al. [62].

For COW, again using an attenuation equal to 20 km of fibre we obtained an estimated secret key rate of 311 kbps using a clock rate of 0.86 GHz with a QBER of 1.37% due to timing information and a QBER of 1.36% due to the interferometer and security of the channel. The secret key rate of COW was calculated using the sifted key rate and measured visibilities according to the security proof by Branciard *et al.* [59] shown to be a secure upper bound for some collective attacks.

For DPS at the same attenuation we obtained an estimated secret key rate of 565 kbps using a clock rate of 1.72 GHz and measuring a QBER of 0.88%. The secret key rate of DPS was calculated by measuring the key errors and visibilities according to the security proof by Branciard *et al.* [59] and is limited to some collective attacks.

3.5.1 Comparisons with other Results

Table 3.1 includes comparisons between this work and a sample of recent publications. We have included the result of Lucamarini *et al.* [97], which demonstrates an efficient implementation of BB84 through biased basis selection. The experimental finite key analysis illustrates security against collective attacks producing results of 1.09 Mbps at 50 km of standard (0.2 dB/km) fibre. We estimate the QBERs from Figure 3, and extrapolate the results back to 20 km distances (4 dB), and assumed a constant error rate over this range of distances. Later work has extended this analysis to prove security against more general attacks [98], and simulates that the percentage of secure key rate would not reduce dramatically, for example at 30 km the estimated key rate for collective attacks is 3.41 Mbps, and for general attacks this reduces to 3.12 Mbps (91.5%).

We further give examples of COW and DPS. The COW demonstration from Korzh *et al.* [198] implemented finite key analysis against collective attacks for long range QKD over ultra-low loss fibres (∼0.16 dB/km). The data provided was 12.7 kbps secure rate at 16.9 dB (or 104 km), and extrapolated back to 20 km distances (4 dB). Providing the higher data rates this would likely reduce the uncertainty of measurement and increase the proportion of secure rate in the finite case, and therefore the estimate provided of 248 kbps may be a slight under-estimate.

The DPS example from Wang *et al.* [199] provides asymptotic secure key rates under individual attack security. The data points provided include 1.16 Mbps at 10 km and 185 kbps at 50 km, from which we interpolate a result of 733 kbps for 20 km.

3.6 Summary

A summary of these results are presented in Table 3.1, where in all cases we show a performance comparable to the state-of-the-art in current fibre and bulk optical systems [1]. This work demonstrates the feasibility of using fully integrated devices within QKD systems, implementing three important protocols by utilising the reconfigurability of the devices. The integrated photonic platform allowed us to demonstrate miniaturised devices exploiting robust, low-cost manufacturing processes, that allow flexibility in fibre network settings.

These devices could be readily adapted to implement more protocols, such as the reference-frame independent and measurement-device independent QKD protocols [99, 102]. Also the tunablity of the laser source enables flexibility in the wavelength of operation, this combined with the complexity achievable with the platform will be key to enabling high capacity wavelength division multiplexing schemes of the quantum channel in a practical implementation. The increased complexity allowed by integrated photonics will facilitate the implementation of further monitoring and certification circuits, protecting against security flaws and side channel attacks [1] with minimal change in footprint and cost.

Compatibility with current integrated photonic telecommunication hardware will ultimately allow seamless operation alongside classical communications transceivers, enabling hybrid classical and quantum communications devices. Moreover, the ability to scale up these integrated circuits to 100's or even 1000's of components [180] opens the way to new and advanced integrated quantum communications technologies.

3.7 Futher Developments - Improvements

3.7.1 WDM-QKD

One of the issues of quantum key distribution is the limited rates achievable. The use of one-time-pad is very expensive in terms of resource, as it requires as many bits in the key as in the message. The limitations of rates comes from the less than single photon probability of transmission, the absorption and scattering in the fibre, the limitation in detector efficiency, the limited number of raw keys that can be sifted to create correlated key, and the errors and possible shared information that accrues that must be eliminated through error correction and privacy amplification.

One way to overcome this limitation is to use the key that is generated to seed another cryptographic system with random bits. Examples include the Advanced Encryption Standard (AES), which in itself if not information theoretically secure, but relies on assumptions over the abilities of Eve's computational power. By refreshing the random input seed periodically with the keys generated from QKD systems the capabilities of Eve's computational power becomes increasingly larger to break the encryption before the seed is refreshed [201].

Other implementations include higher dimensional alphabets for the communications to increase the number of bits per measurement [202], and a further approach is to increase the rates of the secret keys generated by multiplexing the systems in some degree of freedom, including time, spatial, mode or wavelength [203]. Integrated photonics is particularly suited to this approach, as many copies of the same or similar circuit can be reproduced in a manufacturable, miniaturised and robust manner. This approach is explored and demonstrated in Chapter 4.

3.7.2 MDI-QKD

Another criticism of QKD implementations is that physical equipment does not necessarily match the assumption a security proof makes. Such an example is the vulnerability many detector systems face. APDs can be distorted by the use of very bright classical light taking it out of its single photon detector regime and can therefore be controlled by

an adversary [81]. Many approaches to mitigate this risk can be implemented, such as the inclusion of further monitoring circuitry, or random adjustment of detector efficiency following decoy state methodology [204].

A further approach is to provide the adversary with the control of the measurement device equipment and remove the correlation between the results of the detectors and the key information. This is known as measurement-device-independent (MDI) QKD [102] and has been experimentally demonstrated in a number of cases [103, 104, 205, 206]. The devices demonstrated in this chapter could be operated as the transmitters of MDI-QKD, where they are required to send decoy-state BB84 states, but also required the indistinguishability of the photons sent (to allow interference and bell state projection at the measurement device). This requires the other degrees of freedom to be overlapped and equivalent, including spectrum, polarisation and temporal [207]. The devices described in this chapter allow tunable wavelength, control of the temporal relationship of the states, and show a good level of side-band-suppression of the laser spectrum that could, in principle, allow MDI-QKD operation.

3.7.3 Device Packaging

To improve the robustness of the devices, the integrated chips must be packaged appropriately. Designs and initial prototype are under way to develop this packaging, which includes the RF PCB manufacture, mounting and termination described earlier in this chapter, as well as the aligning and fixing of the output lensed fibre coupling. This will be encased in a metal box allowing for temperature control, DC control and RF input signals (as illustrated in Figure 3.22).

The receiver only requires DC voltage signals, and temperature control. The larger power dissipation from thermo-optic phase modulators requires a larger temperature control peltier device, and heat sink to ensure consistent operation. Furthermore, the receiver has multiple optical inputs and outputs which can be accessed by standard v-groove arrays with 127 μm pitch spacing, and again aligned, mounted and fixed with UV-cured epoxy. This is housed in a larger metal chassis as pictures in Figure 3.23.

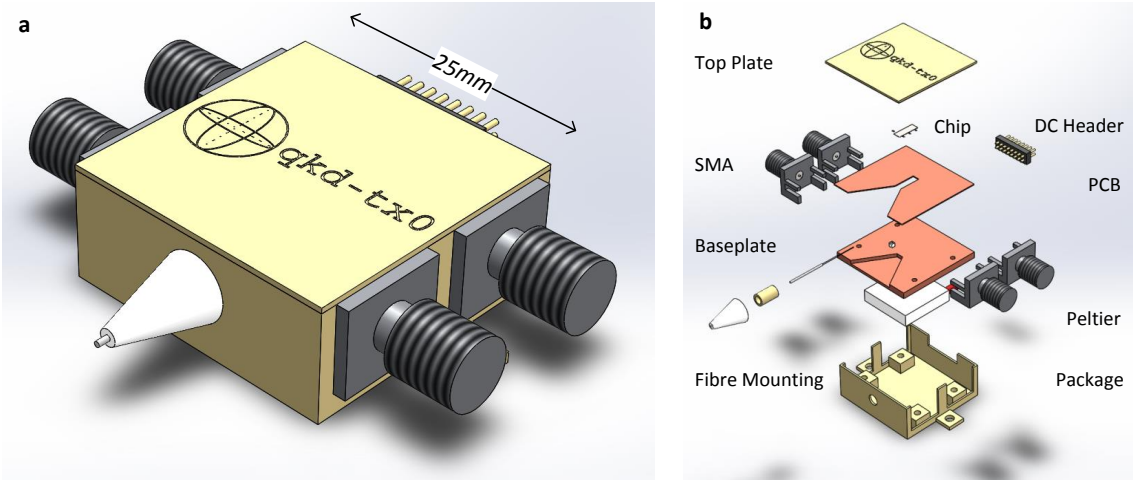

Figure 3.22: **Transmitter Packaging:** (a) Fully assembled package for the integrated transmitter chips. (b) Exploded diagram of the component parts involved, which includes mounting the chip and PCB on a copper base plates for thermal and electrical conductivity. DC and RF connection are supplied with standard SMA and header connector. The base plate sits on top of a peltier for temperature control and is housed an a metal package to allow heater dissipation. The single output fibre is aligned and glued to the package and hermetically sealed to the outputs of the package to limit environmental exposure of the devices.

3.7.4 QKD Systems and Electronics

Further to the electrical and optical packaging of the devices, the current operation of the QKD experiment is not yet deployable as it relies on large pieces of generic equipment such as pulse/pattern generators (PPG) for signal generation and TCSPC for time tagging of the photon detection events. Development of bespoke equipment will allow deployment of the devices in the near-term future.

This development is illustrated in the schematic system diagrams in Figure 3.24, which highlights the functional components required to form a operational QKD system. On the transmitter side, quantum random numbers (QRNG) are processed in to the data required to be sent (DATA GEN), which in turn is buffered in memory (BUFFER), and generates transmitter electrical signals (SERIALISER & PPG). The transmitter chip has to be controlled for temperature and DC voltages, as well as appropriately monitored before sending over the quantum channel. This is controlled by a larger processing control unit which ensures the correct configuration of these component blocks, and may be

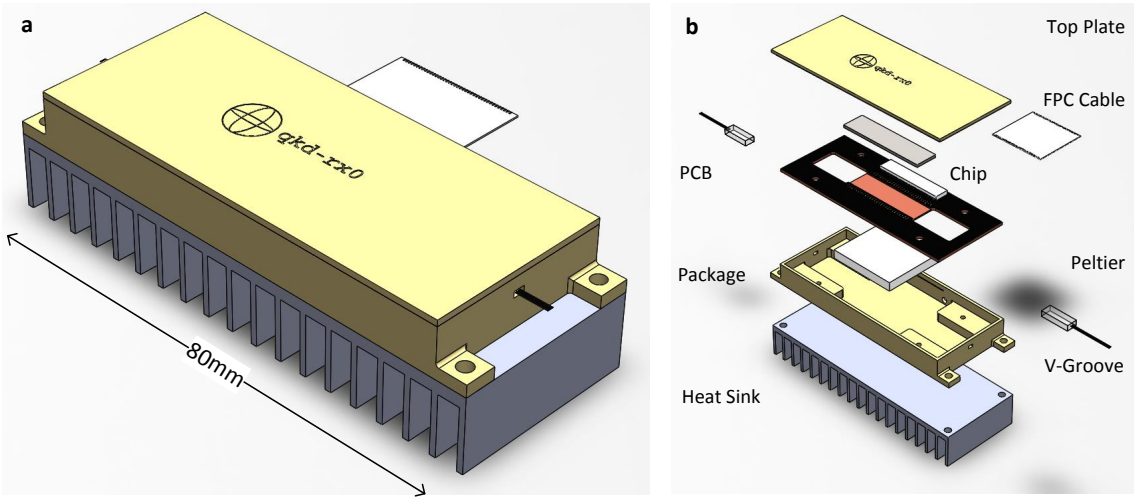

Figure 3.23: **Receiver Packaging:** (a) Fully assembled package for the integrated receiver chips (b) Exploded diagram of the component parts involved, which includes mounting the chip on to a metal-core PCB with thermal epoxy for good thermal conductivity. The PCB has a FPC electrical connector that allows a high density of electrical connections for the thermo-optic phase shifters. The PCB is mounted on top of a peltier cooler which dissipates heat to the bottom of the metal package which is connected to a heat sink allowing for the thermal stability required in the AMZI. The multiple optical I/O are accessed via standard v-groove assemblies which are connected with UV-cured epoxy for a robust connection, and all hermetically sealed to limit environmental exposure.

implemented in software or embedded on hardware.

Classical communication is required between the transmitter and receiver for clock synchronisation and post processing. On the receiver side, the same voltage and temperature control is required and may be dynamically reconfigured by the processing control unit. High speed time-to-digital conversion of the detector results is required to recover the transmitted quantum states, and buffered in memory to allow the sifting, error correction and privacy amplification to occur in real time, before the keys are established.

The major areas of development have focused on the data generation, serialiser and PPG, that require high clock rates and short pulse windows (1.7 GHz clocks and 100 ps pulses). Initial prototyping has occurred with the Xilinx Virtex UltraScale FPGA VCU1287 Characterization Kit with built in transceiver modules capable of operation at 16 and 30 Gbps and ∼100 ps pulses have been generated as illustrated in Figure 3.25. This system will be used to develop the first bespoke system for QKD transmission with integrated

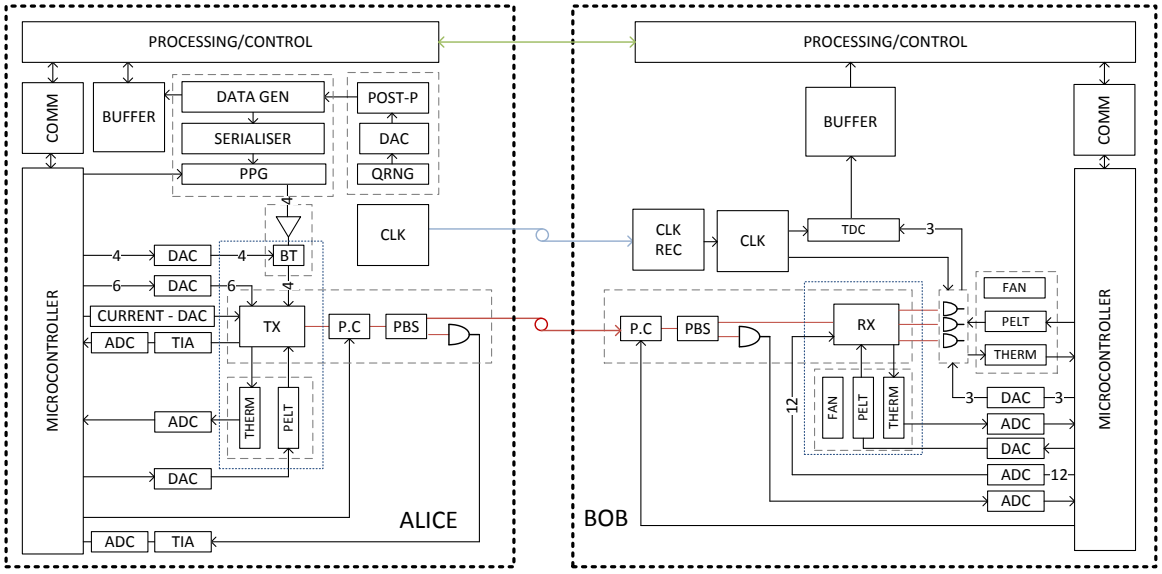

Figure 3.24: **QKD System Diagram:** Illustrating the functional components required to form a functional QKD system. The transmitter side the processing control unit controls the configuration of the functional blocks of the system, which include the quantum random numbers generated (QRNG), the processing on these number to store data in a buffer and to serialise the data to create electronic signals to the transmitter chip (TX). The temperature and operating conditions of the chip are set and monitored with appropriate feedback, and sent over the quantum channel to the receiver. The receiver also has a proessing control unit to communicate with the transmitter, and to configure the receiver system to appropriately decode the transmission. A classical clock (CLK) is sent from the transmitter to synchronise the time-to-digital (TDC) required to decode the quantum information from the detectors. The results are stored in buffer memory ready to be sifted, error corrected and privacy amplified.

photonics.

Along with the bespoke hardware development, there is also work with software to prepare a framework in which the operation, processing and prototyping of QKD devices and systems can be developed. This includes abstract classes that can be flexibly tailored dependent on the physical hardware, experiment or protocol available. An example of this work is illustrated in Figure 3.26 which contains a Unified Modelling Language (UML) diagram of inter-node communication, allowing the transmitter and receiver to communicate, establishing the parameters and protocols of the communication depending on the capabilities of the device and the network setting.

Figure 3.25: **FPGA Pulse Output:** An example signal generated from the Xilinx Virtex UltraScale FPGA VCU1287 Characterization Kit with ∼112 ps pulse output from the device. This output would be amplified and then given a DC offset through a bias-tee to control the photonic transmitter chip.

3.7.5 Single Photon Detectors

Further to the work demonstrated here, future systems will require the integration or the packaging of detectors to be included in the receiver system. Within superconducting detector technology there has been a number of examples of monolithically fabricated detector and photonic chips [162, 173, 208], with recent demonstrations in GaAs [169], and silicon substrates and waveguides [170–172]. This raises certain issues when trying to combine phase control and cryogenic temperatures. This could be overcome when moving to a MDI-QKD approach, where the detector circuit for time bin encoded systems is a 50:50 beams splitter and single photon detectors [103, 104].

Future quantum network scenarios may move towards centralised resources, such as the quantum access network [118] or "client-server" models [11]. This in turn may allow more resource expensive cryogenic cooling systems to be shared between many users, in a similar vain to the use of expensive ATMs and cheap credit cards.

More near term practical single photon detector for large scale deployment may use

other detector technologies, such as avalanche hhotodiodes (APDs). This can have a downside of long recovery time (increasing the dead time), and afterpulses (false positive signals increasing the dark counts). To overcome some of these issues, the detectors are cooled, as well as gated (where the reverse bias is modulated, to only allow detection when photons are expected). For telecommunication wavelength (1530nm to 1570 nm) more exotic materials are needed, such as InGaAs APDs, which have been recently shown to operate at 55% efficiency, with a 1 GHz gating, through the use of self-differencing detection [164]. These systems could introduce more noise (in terms of dark counts and afterpulses), more errors (in terms of timing jitter), and lower count rates (in terms of larger dead time) which in turn would limit the achievable distances and secure key rates demonstrated in this work. This may in principle be integrable in to InP integrated technologies, or in the short term, patterned in arrays and fixed to the outputs of the integrated receiver devices. Silicon photonics may also become appealing with the possibility of Silicon-Germanium (SiGe) based single photon detectors that could be directly integrated in a monolithic device [209, 210].

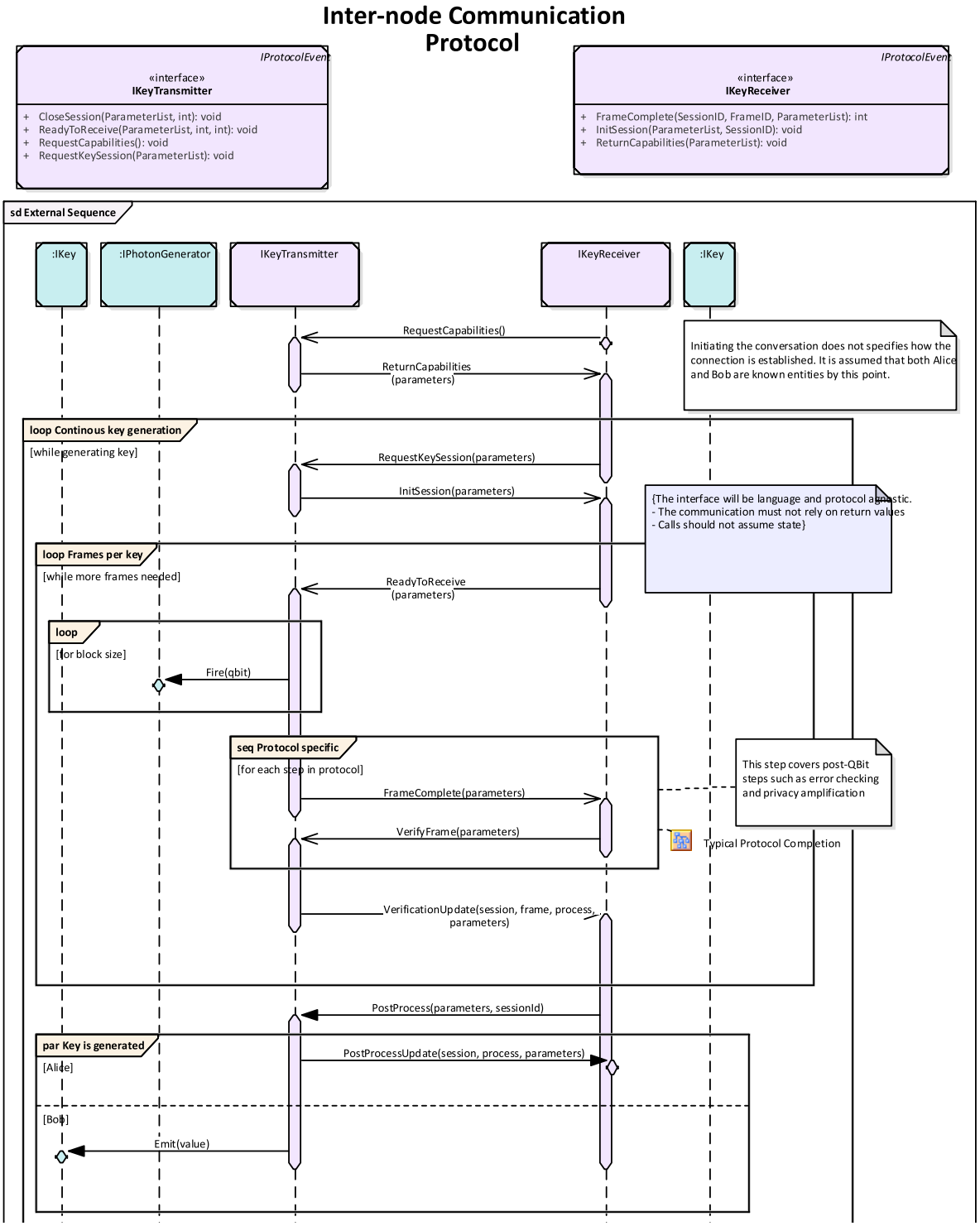

Figure 3.26: **UML for QKD Framework:** An example UML diagram illustrating inter-node communication protocol that first establishes the capabilities fo the hardware to ensure quantum communication can be accomplished. It then continuously loops a key generating session in which raw transmission can start and blocks of key are periodically combined to complete protocol specific error correction and privacy amplification. The abstract framework allows many specific instances of hardware to be facilitated.

Chapter 4

Wavelength Division Multiplexed QKD

Statement of Work

I developed the experimental concept for this initial proof-of-principle work. Along with utilising the previously design InP devices (fabricated by Oclaro), I designed the receiver circuit and compiled the photonic fabrication mask (fabricated by LioniX). Initial characterisation was conducted in collaboration with Alasdair Price. I designed and compiled the mask for future generation integrated WDM transmitters and receivers with support from Chris Erven and Alasdair Price in receiver mask compilation.

4.1 Introduction

Global telecommunications is an extraordinarily enabling and now common technology, but with it comes risks and the need for robust security. Quantum Key Distribution (QKD) can provide secure channels by establishing random keys between two parties, which can then be used to cryptographically secure messages [2]. To encrypt these messages, without assuming an adversary has limited resources, the most secure method is the One-Time-Pad (OTP - see Section 2.1.1) which requires keys that are the same length as the message [14].

One of the major limitations for current QKD implementations is the achievable rates, which are limited by detector efficiency, fast and reliable single photon sources, channel loss, and the inefficiency of error reconciliation and privacy amplification [1]. Even with these limitations, QKD has been demonstrated to achieve substantial rates of 1 Mbps over 50 km, and continues to improve over time [98].

A number of approaches have been suggested to overcome the current bandwidth limits including Continuous-Variable QKD (see Section 2.3.2), which utilises homodyne detection schemes and multi-GHz bandwidth standard photodiodes to discretise continuous variables and produce many bits per measurement to increase the achievable rates. Other methods use the reasonably slow key rates provided by QKD to seed other cryptographic protocols, such as the Advanced Encryption Standard (AES) [211]. This loses the information-theoretically secure claim that OTP provides, but can substantially increase the throughput of the encyrption.

A final approach to increase the rates of QKD is to multiplex many independent transmitters and receivers on the same channel. This can be achieved with polarisation, temporal, spatial, and wavelength division multiplexing, and has been vital to the increase of channel capacity in classical communication networks [212]. Wavelength-division-multiplexing (WDM - see Figure 4.1), in which many signals are combined into one signal over the same optical channel but separated by wavelengths, is especially common as optical fibres can support a band of wavelengths. The signals can also be combined (multiplexed) or separated (de-multiplexed) with passive optical components. This techniques allows multiple independent channels to operate over the same optical

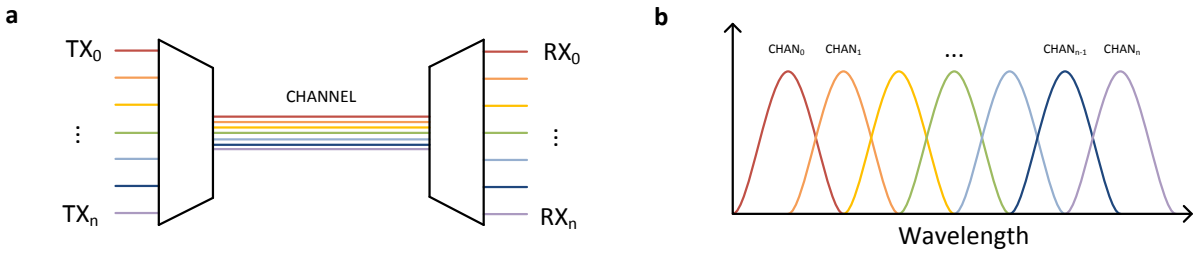

Figure 4.1: **Wavelength-Division-Multiplexing:** (a) Schematic of WDM techniques to increase overall rates of transmission in communication where multiple pairs of transmitters working at different wavelengths are combined (multiplexed) into a single signal on a shared channel and separated (de-multiplexed) to the intended receiver. (b) Spectra of multiple channels, illustrating the separation of different wavelengths, and the overlap (crosstalk) that may occur between neighbouring channels.

fibre, and higher rates can be achieved, compared to a single sender. This approach has previously been demonstrated in QKD with a number of experimental implementations [12, 203, 211, 213–217].

Current bulk and fibre implementations of QKD schemes render the multiplexing approach infeasible on large scales, as many copies of the systems have to be made independently and with large devices. This approach greatly limits the practicality of deploying these devices in telecommunication networks, where space is limited and costly. Integrated photonics provide a suitable platform in which to implement such a scheme, as many copies of the same structures can be fabricated on a monolithic device without a significant increase in overhead [10]. The miniaturised devices have high component density to achieve higher circuit complexity, are amenable to manufacture, with a small footprint, and high robustness to environmental conditions. In the previous chapter, integrated photonic transmitter and receiver devices for QKD were demonstrated with ∼500 kbps estimated secure key rates over an emulated channel of 20 km.

In this experiment, we demonstrate a proof-of-principle experiment for WDM-QKD with integrated photonics where two InP transmitters operated at different wavelengths are combined into the same optical fibre, and demultiplexed and decoded on a SiO_xN_y chip to demonstrate increased rates with limited increase of error. We further use an efficient decoy-state BB84 scheme with biased basis preparation and measurement to further increase channel capacity [218]. We demonstrate an estimated secure key rate of 1.11 Mbps over an emulated 20 km fibre using two independent transmitter and receiver

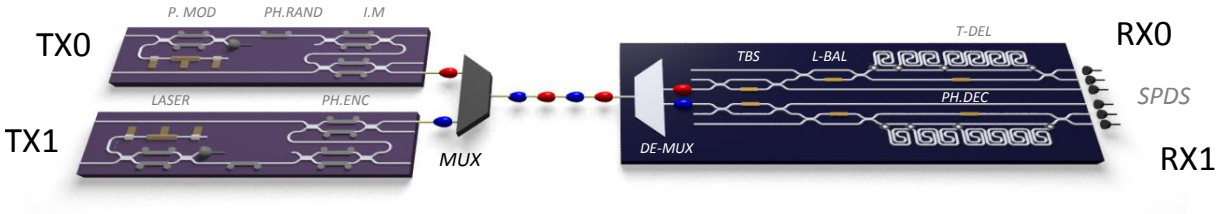

Figure 4.2: **Schematic of WDM QKD experiment:** with two integrated InP transmitter chips, multiplexed on a single fibre, then demultiplexed and decoded on a monolithic SiO_xN_y receiver chip and off-chip SNSPDs. The two different wavelengths of light are represented as red and blue photons and are also interleaved in time to limit crosstalk between the channels without reducing the individual channel clock rates (see Section 4.4.1).

links, utilising both wavelength and temporal filtering to reduce channel crosstalk and noise.

This demonstrates the feasibility of WDM-QKD with integrated photonics, and could easily be extended to ∼20 Mbps of secure key over 20 km distance using 16 DWDM channels, which has led to the design of next generation devices. These devices described in Section 4.7 contain 4 channels, with the possibility of extending further with a daisy-chained architecture (see Section 4.7.3). Together with the development of integrated single photon detectors [162], these devices will lead to high-rate QKD for quantum secured communications.

4.2 Integrated Transmitter Devices

Figure 4.3 shows a schematic of a single transmitter in the chip-to-chip WDM-QKD system. For the transmitter device, the InP material system [180] was chosen to meet the requirements of fast active electro-optics (with GHz operating speeds) and monolithic integration with a laser source as described in Section 3.2.

We operate each individual transmitter as described before in Section 3.5, where the CW laser source was modulated (P.MOD) to create weak coherent pulses of light, which were then phase randomised with a single electro-optic modulator (PH.RAND) before being attenuated and intensity modulated (I.M). The BB84 [42] QKD protocol was implemented using time-bin encoding, where $|0\rangle$ was encoded by a photon in the first time-bin and $|1\rangle$ was encoded by a photon in the second time-bin, while $|+\rangle$ was encoded by a

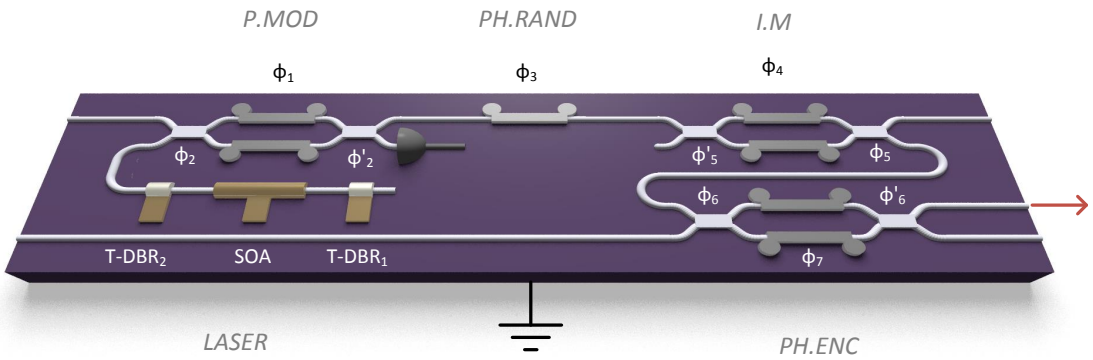

Figure 4.3: **WDM-QKD TX Schematic:** The laser source consists of semiconductor optical amplifier (SOA) in a cavity formed by two tunable-distributed Bragg reflectors (T-DBR) and is operated in continuous wave mode by injecting current in the SOA. Pulse modulation (P.MOD), intensity modulation (I.M), phase encoding (PH.ENC), and phase randomisation (PH.RAND) are achieved as described in Section 3.2.

photon in a superposition of the first and second time-bin with zero relative phase, and $|-\rangle$ was encoded by a photon in a superposition of being in the first and second time-bin with a π relative phase (PH. ENC). The intensity of each pulse in the $\{|+\rangle, |-\rangle\}$ states was reduced by half, compared to the $\{|0\rangle, |1\rangle\}$ states in order to maintain the same average photon number per state. This same intensity modulator (I.M) was also used to encode the decoy photon levels required to mitigate multi-photon contamination for security [62]. The final MZI (PH.ENC) encoded the relative phase between successive time-bins to implement the $|-\rangle$ state. Each laser operating wavelength was tuned with T-DBR$_1$ and T-DBR$_2$ as described below.

4.2.1 Laser

The integrated laser is based on two tunable distributed Bragg reflectors (T-DBR) forming a Fabry-Perot cavity around a semiconductor optical amplifier (SOA). The wavelength of the laser can be shifted by altering the refractive index of the medium, either by temperature or by carrier injection into the T-DBR. The latter technique allows different operating wavelengths of multiple transmitters on a monolithic device.

The coherence time of the laser is at least greater than 1.5 ns, and can be tuned around ∼7 nm in a 1.2 V range (as illustrated in Figure 4.4). This change in wavelength is approximately linear with the current, and therefore exponential with the voltage (as

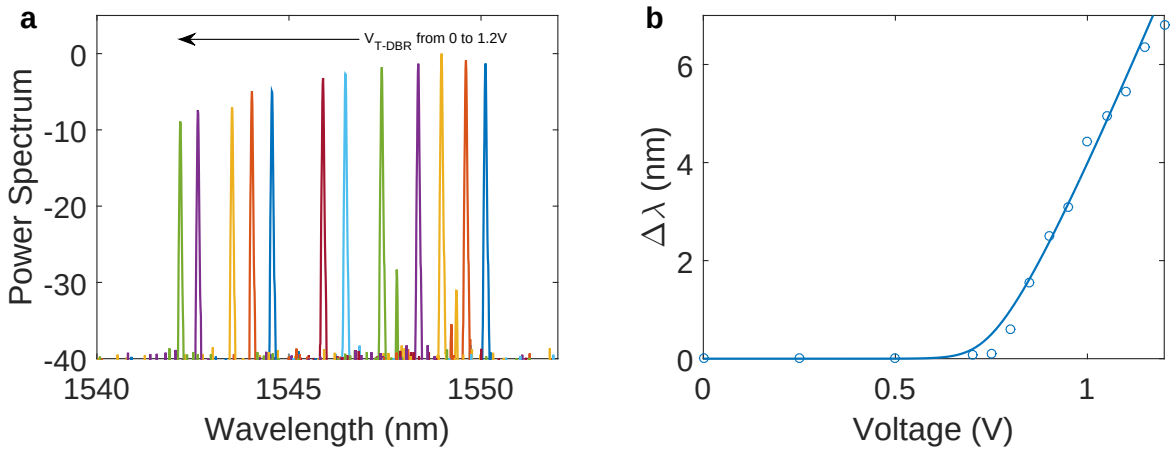

Figure 4.4: **Laser Spectrum Control with T-DBR:** (a) Laser spectrum tunability demonstrated over 7 nm with 1.2 V, with increasing voltage decreasing the wavelength. (b) A fitted plot of the shift in wavelength based on the voltage applied, where there is an exponential increase in $\Delta\lambda$ with a $\sim$0.7 V threshold.

it is a diode-like device). As the wavelength decreases, there is an increase of loss through the device, due to the absorption profile of the waveguides, as the light gets closer to the bandgap of the InP material.

4.2.2 Phase Control

Although we have described how to generate a π phase difference for the $\{|+\rangle, |-\rangle\}$ states with the PH.ENC MZI of Figure 4.3 (See Section 3.2.4), we haven't described how to ensure the $|+\rangle$ state is prepared and measured as $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, rather than any other state of the form $\frac{|0\rangle+\exp(i\phi)|1\rangle}{\sqrt{2}}$.

As described in Section 2.4.3, an AMZI has a wavelength dependent interference pattern due to the difference in optical path lengths causing relative phase between the two paths. With CW light and a specific wavelength this interference can be altered by applying another relative phase in the form of thermo-optic phase shifts in one of the arms of the interferometer, or changing the temperature of the entire interferometer (as the temperature dependent refractive index will cause a change in the relative optical path lengths). The interference pattern can also be altered by changing the wavelength of the source of light.

The time-bins described in this chapter are just intensity envelopes over the underlying

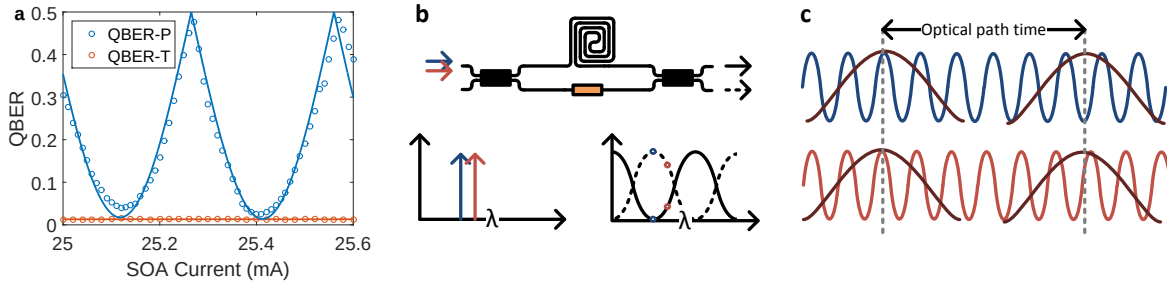

Figure 4.5: **Phase Control with SOA Current:** (a) QBER measurements from timing information (QBER-T) and phase information (QBER-P) showing the phase tunability from laser wavelength (the QBER is always less than 0.5, because the results are flipped if they are wrong more than half the time). (b) An AMZI with blue or red laser light and the interference it causes. (c) The two wavelengths represented as sinusoidal functions, showing their phase offsets for a given optical path time (the representation of the unbalance optical path length of the AMZI). The time-bins are generated as intensity envelopes over the top of the continuous wave laser and do not explicitly define the phase relationship between the two time-bins (although it will effect the visibility of the interference as illustrated in Section 3.3.3).

CW laser signals, and it is the combination of the laser wavelength, and the phase in the AMZI from optical path length differences that defines the interference between these two time-bins. Therefore, the relative phase between the two time-bins is defined by the precise wavelength of the laser, and the interference signals this generates at the output of the receiver's AMZI. Fine control of this phase can be achieved by increasing or decreasing the wavelength of the laser, through the overall temperature of the receiver AMZI, or the thermo-optic control of the phase shifter inside the receiver AMZI. In this way we can define and measure a $|+\rangle$ state.

A change in current in the SOA of the laser causes small alterations to the characteristics of the gain medium in the laser cavity and shifts the wavelength of the central peak very slightly, while also changing the intensity an almost negligible amount. This slight change in wavelength causes the different interference through the temperature controlled AMZI on the receiver circuit, and can be calibrated to provide the best error rate (as illustrated in Figure 4.5). The change in intensity can be compensated by the intensity modulator DC offset, included in the calibration stage.

4.2.3 WDM MUX

There are a number of techniques available for wavelength division multiplexing and demultiplexing using passive optical components. On the transmitter side we could have used an AWG, as a passive optical component that has roughly fixed loss, somewhat independent of the number of channels created [219]. Due to the weak coherent light nature of the prepare and send QKD protocols we employ a simpler approach; to use a 50:50 beam splitter to combine the two signals.

This approach loses 50% of the light and therefore the transmitter must be calibrated to ensure the proper photon number appears on the quantum channel. If the 50:50 beam splitter is colourless, this approach permits any wavelength of light from the two transmitters to be combined and to match whichever receiver WDM is employed. This would allow dynamic reconfiguration of the spectra that each transmitter is allocated for flexible network operation.

This WDM approach was implemented externally to the integrated photonics for this proof-of-principle demonstration, but can be included in future monolithic designs (see Section 4.7.1).

4.3 Integrated Receiver Circuit

The integrated receiver circuit, shown in Figure 4.6, is a monolithically fabricated SiO_xN_y device comprised of passive waveguides and thermo-optic phase shifters combined into interferometers to demultiplex two WDM channels, route signals, and decode timing and phase information for multi-protocol WDM-QKD. The photonic signals are detected by superconducting nanowire single photon detectors [173] to convert single photons into classical electronic signals.

For the integrated receiver device, the SiO_xN_y material system was chosen to minimise photon loss from fibre-to-chip coupling and waveguide propagation loss, whilst maintaining a compact footprint [175]. This device, along with fibre coupled single photon detectors, represent the full photonic WDM-QKD receiver.

As illustrated in Figure 4.6, the first AMZI acts as a wavelength filter, routing the two

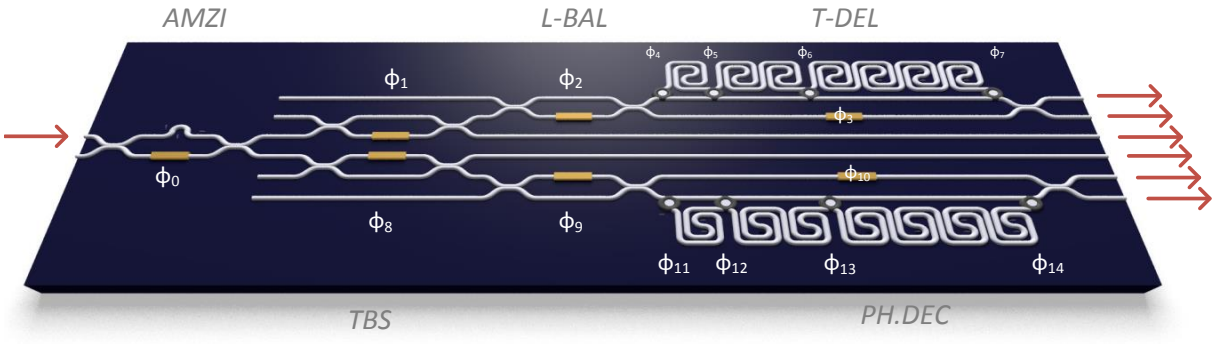

Figure 4.6: **WDM-QKD Receiver Circuit:** Illustration of the integrated SiO_xN_y receiver circuit with thermo optic phase shifters ϕ_1 to ϕ_{14}. Each controls the phase relationship in either a wavelength filter AMZI (ϕ_0), balanced MZI ($\phi_{\{1,2,4-9,11-14\}}$) or phase-decoding AMZI ($\phi_{\{3,10\}}$). The circuit consists of a wavelength filtering AMZI to demultiplex the channel followed by two copies of the receiver circuit. The receiver combines an MZI to control the portion of the signal straight to a detector (TBS) and the rest in the phase decoding AMZI. This AMZI contains a reconfigurable discrete time delay and a loss balancing MZI (L-BAL) to compensate for the propagation loss in the longer arm.

different transmitter wavelengths into independent copies of the receiver circuit described in Section 3.3. The next MZI acts as a tunable beamsplitter (TBS) and taps off a portion of the incoming signal, which was routed to a single photon detector and used to bias the basis measurement (see Section 4.4.2). The second MZI (L-BAL) acts to balance the losses in the asymmetric MZI (AMZI), which incorporates a digitally reconfigurable delay line, tunable from 0 to 2.1 ns in steps of 300 ps. Light was coupled out of the device and into external fibre coupled superconducting nanowire single-photon detectors mounted in a closed cycle refrigerator [173] which had a system detection efficiency of ∼45% from the fibre input, a temporal jitter of ∼50 ps, and a dead-time of ∼10 ns.

4.3.1 WDM deMUX

There are a number of passive optical components that are available when designing the demultiplexing of WDM channels, including Array-Waveguide-Gratings (AWG - Figure 4.7 (a)) [219], ring resonators [220], and AMZI filters [12]. For this proof-of-principle demonstration, 2-channel WDM-QKD was chosen to be demulitplexed by an AMZI filter with a small difference in path lengths, as illustrated in Figure 4.7 (b). This small offset provides wavelength dependent phase and therefore changes the relative intensity

of the two output arms dependent on the input wavelength. The phase is related to the difference in optical path length by

$$\begin{aligned}\phi(\lambda) &= \mathbf{k} \cdot \delta L \\ &= \frac{2\pi n \delta L}{\lambda} \ .\end{aligned} \tag{4.3.1}$$

We are primarily interested in the free spectral range (FSR) of the AMZI which defines the channel spacing, and is characterised as the difference in wavelengths between two maxima (or the difference in phase being 2π), therefore:

$$\begin{aligned}\Delta\phi &= \phi(\lambda_1) - \phi(\lambda_2) \\ &= \frac{2\pi n \delta L}{\lambda_1} - \frac{2\pi n \delta L}{\lambda_2} \\ &= 2\pi\end{aligned} \tag{4.3.2}$$

where we have assumed the refractive index is fairly constant between the two wavelengths. This can be manipulated to produce

$$\begin{aligned}\mathrm{FSR} &= \lambda_1 - \lambda_2 \\ &\approx \frac{\lambda_0^2}{nL}\end{aligned} \tag{4.3.3}$$

which for a 200 GHz channel spacing at 1550 nm gives a path difference of $\sim$442 μm with a refractive index of 1.71. The two channel wavelengths are required to be separated into two separate waveguides, and therefore the FSR of the filter is double the channel spacing. The frequency bandwidth ($\Delta\nu = 200$ GHz) can be related to wavelength bandwidth ($\Delta\lambda$) as

$$\Delta\nu = \frac{c}{\lambda^2}\Delta\lambda \tag{4.3.4}$$

around a centre wavelength of $\lambda = 1550$ nm, providing a channel spacing of 1.6 nm and therefore an FSR of 3.2 nm.

The results shown in Figure 4.7 (d) show an unequal extinction ratio between the two outputs, due to non-idealities of the 50:50 directional couplers. The output of the MZI

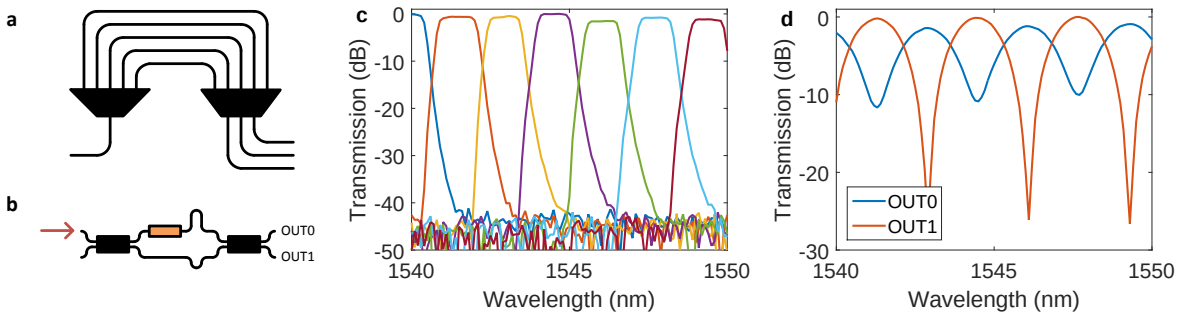

Figure 4.7: **WDM de-Multiplexing:** (a) AWG schematic comprising a multimode splitter followed by many paths of slightly different lengths causing different phase relationships for the different colours of light. As these are combined in a further multimode interference device the different colours interfere constructively into different output waveguides. (b) AMZI filter schematic comprising of two beam splitters with unequal path lengths inside the interferometer causing a wavelength dependent phase. (c) AWG spectrum, showing multiple channels with a 1 nm bandpass, and then roll-off with an extinction ratio of 50 dB. There is also crossover between the separate channels. (d) AMZI channel spectra for WDM QKD receiver for two channels. The unequal and finite extinction ratios will cause crosstalk and associated errors. The AMZI also doesn't have a flat bandpass as the AWG does, which therefore requires more consistent control of the transmitter wavelengths to limit crosstalk.

with reflectivity beam splitters of η_1 and η_2 given input light in one mode is

$$\begin{aligned} I_0 &= \eta_1\eta_2 + (1-\eta_1)(1-\eta_2) - 2\sqrt{\eta_1\eta_2(1-\eta_1)(1-\eta_2)}\cos(\phi) \\ I_1 &= \eta_1(1-\eta_2) + (1-\eta_1)\eta_2 + 2\sqrt{\eta_1\eta_2(1-\eta_1)(1-\eta_2)}\cos(\phi) \end{aligned} \tag{4.3.5}$$

where I_0 and I_1 are the normalised optical intensities of the first and second output respectively. If we assume that $\eta_1 = \eta_2 = \eta$, then this reduces to

$$\begin{aligned} I_0 &= \eta^2 + (1-\eta)^2 - 2\eta(1-\eta)\cos(\phi) \\ I_1 &= 2\eta(1-\eta) + 2\eta(1-\eta)\cos(\phi) \end{aligned} \tag{4.3.6}$$

which returns the extinction ratio ($I_{\max}/I_{\min}$) values of

$$\begin{aligned} \mathrm{ER}_0 &= \frac{\eta^2 + (1-\eta)^2 + 2\eta(1-\eta)}{\eta^2 + (1-\eta_1)^2 - 2\eta(1-\eta)} \\ \mathrm{ER}_1 &= \frac{2\eta(1-\eta) + 2\eta(1-\eta)}{2\eta(1-\eta) - 2\eta(1-\eta)} \end{aligned} \tag{4.3.7}$$

which tends to ∞ for output 1 no matter the splitting ratio, but moves away from ∞ for the output 0 as the reflectivity moves away from 50:50. There is also a difference in the maximum transmission between one arm and the other, with a ratio of

$$\frac{I_{0,\max}}{I_{1,\max}} = \frac{\eta^2 + (1-\eta_1)^2 + 2\eta(1-\eta)}{2\eta(1-\eta) + 2\eta(1-\eta)} \tag{4.3.8}$$

which tends to 1 as the reflectivity becomes the ideal 50:50. The experimental results were estimated to be closer to 35:65 in their splitting ratio than 50:50 due to fabrication tolerances and manufacturing imperfections. This led to ∼10 dB extinction for one of the output arms as illustrated in Figure 4.7 (d), in comparison to the ∼25 dB extinction ratio for the other output arm, and the >40 dB extinction seen in the AWG of Figure 4.7 (c).

4.3.2 Time-Bin Calibration

The tunable delay lines in either receiver circuit required characterisation and calibration. Figure 4.8 illustrates that for each possible delay length, there is a configuration of the three delays it needs to pass through, which in turn provides a set of MZI switching states. The MZI is either "off" where the two inputs of the MZI are routed to the same outputs (represented as 0), or "on" where the two inputs of the MZI are touted to the opposite outputs (represented as 1).

For the calibration, it can be assumed that there are a set of random phases on each of the MZI switches, which make it act as a beam splitter with random reflectivity, and not the fully transmissive or full reflective states required for correct configuration. By sending a pulse of light with a FWHM much less than the smallest delay line, we can generate a combination of times bin at the output of the final MZI that does not enter the rest of the receiver AMZI.

Figure 4.9 (a-d) contains an intensity heat map with a temporal x axis and the phase voltage y axis. This illustrates the 8 possible time-bins (0 to 2.1 ns in steps of 300 ps) that vary in intensity as the phase in one of the MZIs changes the effective reflectivity. Using the information from Figure 4.8 we can interpret the results of sweeping the first switches phase by summing the intensities of 0, 2, 4, and 6 (time-bins that require 0 for

Time Bin	Delays	Switch state
0	0 0 0	0 0 0 0
1	1 0 0	1 1 0 0
2	0 1 0	0 1 1 0
3	1 1 0	1 0 1 0
4	0 0 1	0 0 1 1
5	1 0 1	1 1 1 1
6	0 1 1	0 1 0 1
7	1 1 1	1 0 0 1

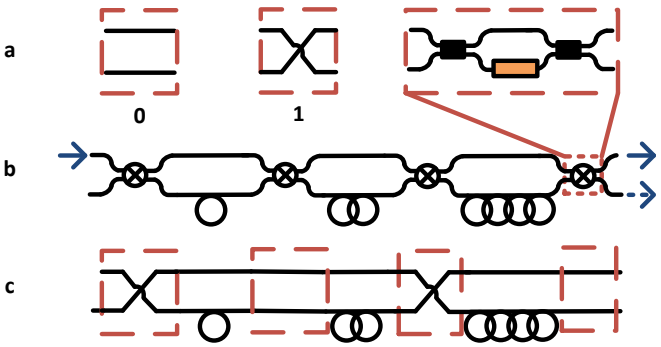

Figure 4.8: **Time-bin configurations:** Illustrating how to configure the tunable delay. For example the table shows time-bin 3 (900 ps) is made from the first delay line (300 ps) and the second delay line (600 ps) represented by 110. (a) The MZI can either be off (0) where the two inputs go to the same outputs, or on (1) where the two inputs are routed to the opposite outputs. (c) The switch configuration for time-bin 3 therefore needs to route the light in to the first time-bin (on), route it through the second delay (off), back out to miss the third delay (on) and straight in to the AMZI (off), represented as 1010.

the first switch) and comparing the output of 1, 3, 5, and 7 (time-bins that require 1 for the first switch). This provides a maximum and minimum setting, that could be either the switch state as 0 or 1, but is independent of the other random phase settings. The same approach applies to each of the switches, and provides a set of two phases for each of the four switches. A test set of these max/min voltages can be set, and used to characterise which voltages correspond to which switching states.

This approach specifies a way of calibrating the voltages without having to search over the full 4 dimensional parameters, which would become resource expensive activity if more delay lines were included.

4.4 Protocols and Operation

Our experimental configuration is shown in Figure 4.10, with the two transmitters on the left and the receiver circuits on the right. The transmitter is a fully integrated Indium Phosphide (InP) [180] QKD transmitter capable of being modulated at GHz rates at standard telecommunications wavelengths, combined through an external 50:50 beamsplitter onto a single channel. The receiver is an integrated Silicon Oxynitride (SiO_xN_y, Triplex [175]) QKD receiver capable of demultiplexing the two transmitter channels and

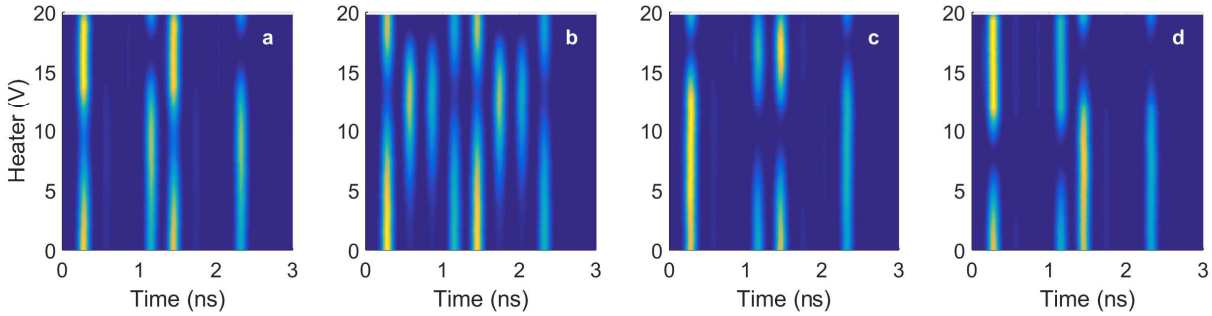

Figure 4.9: **Calibration of RX Delay line:** (a-d) Histogram measurements of the outputs of the tunable delay while sweeping over the voltages of each MZI switch. By summing the intensities of the time-bins related to the 0 or 1 state of each switch as defined by the combinations in Figure 4.8, we can calibrate the 0 and 1 voltage of each switch.

passively measuring Alice's signals. The control hardware and software used to operate the integrated devices is also shown.

On the transmitter side, a temperature controller (TEC) stabilises the laser wavelengths, while a current driver (CURRENT DRIVER) is used to control the intensities of the continuous wave laser and the relative phase between the two time-bins. Alice's electro-optic phase modulators (EOPM) are controlled through a combination of DC reverse biases (DC BIAS) and RF voltage levels from a pattern generator in order to perform pulse modulation (P.MOD), phase randomisation (PH.RAND), intensity modulation (I.M), and phase encoding (PH.ENC). For each qubit sent, the basis, bit, decoy intensities and phase randomisation are chosen using quantum random numbers (QRN) generated using Alice's chip prior to the key exchange. The outputs of the transmitters are polarisation controlled (PC) and passed through a polarisation beam splitter (PBS) to ensure the channels are sent through the fibre over the same polarisation. This is to mitigate the polarisation dependency of the receiver circuit. The channel is then emulated with a variable optical attenuator (VOA), assuming standard SMF optical fibre attenuation of 0.2 dB/km.

The receiver also requires temperature control (TEC) for phase stability in the asymmetric Mach-Zender interferometer (AMZI) and voltage sources (DC PHASE CONTROL) to control the thermo-optic phase shifters (TOPS) determining the operation of the device. Off-chip super-conducting nanowire single-photon detectors (SNSPD) [173] are fibre

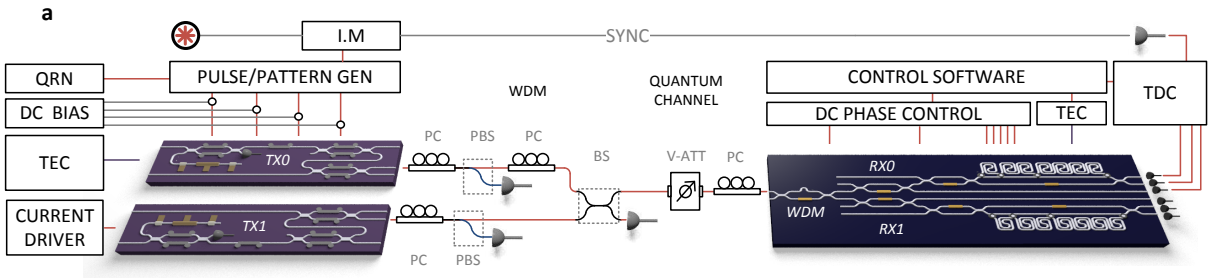

Figure 4.10: **WDM-QKD Experimental Set Up:** Schematic of WDM experimental set up illustrating the two InP integrated photonic devices for QKD transmission (TX0 and TX1), combined onto a single optical channel through passive optical components (polarisation controllers (PC), polarisation beam splitters (PBS) and a 50:50 beam splitter (BS). The optical channel loss is emulated with a variable optical attenuator (VOA), before entering the receiver chip. The receiver chip demultiplexes the signal with an AMZI wavelength filter (WDM), before the two signals go through respective receiver circuits (RX0 and RX1) and are detected by external SNSPDs. The surrounding hardware infrastructure is similar to that of Chapter 3, except for an optical synchronisation link instead of coaxial cable.

coupled to the integrated devices and signals are time-tagged (TIME TAGGING) relative to a synchronisation signal sent from Alice over a separate optical channel using a 40 GHz intensity modulator, CW laser and 25 GHz photodiode. Control software is used to synchronise the system and compare the generated and measured signals allowing the extraction of the successfully distributed raw key, measurement of the QBER, and estimation of the secret key rate.

4.4.1 Temporal Filtering

Along with the wavelength division multiplexing, another technique that can be employed is a form of temporal filtering. As illustrated in Figure 4.7 (a) neighbouring channels in AWGs often have more crosstalk between them than channels that are separated further. To reduce the effect of this crosstalk, neighbouring channel signals can be also temporally offset by half a period, meaning that any gating on the detectors can further remove the effect of crosstalk from the finite extinction between multiplexed channels, as illustrated in Figure 4.11.

In this first experimental demonstration, using an AMZI as a demultiplexing filter, there was an asymmetry to the extinction ratio of the filter as illustrated in Figure 4.7 (b).

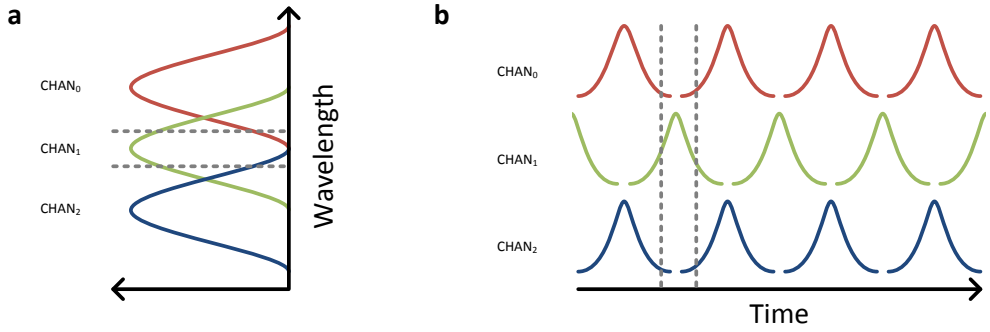

Figure 4.11: **WDM with Temporal Filtering:** Scheme for temporal and spectral filtering of WDM QKD signals to minimise crosstalk induced errors. The channels are separated in wavelength, but will still contain some crosstalk, especially with neighbouring channels. A filter will try and remove the effects of this crosstalk by bandpass filtering a window of spectra. To reduce the noise further a temporal filter will gate a window in time for the results, and have neighbouring channels offset by half a period to minimise the amount of signal that could enter this detection window.

If the two channels produce time-bin signals that temporally overlap, the only mechanism to limit the crosstalk induced errors would be the wavelength filtering. Assuming fully independent channels, any crosstalk measurement will incur 50% error, and therefore the measured extinction of ∼10 dB would induce an extra 5% QBER, potentially limiting the security of the channel. By offsetting the signals by half a period and gating the detection results, we increase this filtering by an additional ∼20 dB with only minor reduction in raw key rates. The QBER can therefore reduced to an almost negligible amount and the secret key rate can be maintained and optimised by varying the gating window.

4.4.2 Biased Basis BB84

To further improve the secure key rates, we have employed a biased basis BB84 protocol [91]. By sending and measuring in a higher proportion of one basis, this can ensure a greater amount of the raw key can remain after sifting. This can be shown to be secure, following the security proof of Lo *et al.* [92].

To implement the bias basis selection on the transmitter, the unbiased random numbers to pick the basis were grouped into larger strings, e.g. a string of 2, where 00 means one basis is chosen (and the three other combinations the other basis) provides a 75:25 split. On the receiver circuit the AMZI provides an unbiased method of measuring each

basis, as described in Section 3.4. To bias the basis choice, the first MZI (TBS) can split a portion of the signal from the incoming stream, and detect the time of arrival directly. This provides $\{|0\rangle, |1\rangle\}$ basis selection at a greater rate, to appropriately match the bias of the transmitter and thus increase the rate of sifted to raw key.

The scheme implemented is based on the proposal from Wei *et al.* in which decoy-state quantum key distribution with biased bases is described [218]. Alice prepares all of the signal (μ) states in the Z basis, $\{|0\rangle, |1\rangle\}$, from which the secure key will be extracted, and prepares weak decoy pulses ν_1, with the X basis, $\{|+\rangle, |-\rangle\}$, and Z basis, with certain probabilities. The choice of vacuum state does not require the setting of basis and bit value as this intensity should be sufficiently low. Bob receives the transmitted weak coherent pulses and measures in the X and Z basis with probabilities p_x and p_z respectively. This approach can reduce the amount of random numbers required to prepare each state, and improves on the performance of standard BB84 with decoy states.

Following the GLLP security analysis [89], the secure key generation rate is given by

$$\begin{aligned} K &\geq q\nu_s \left\{-I_{\mathrm{EC}} + Q_1^z \left[1 - h(e_1^{pz})\right] + Q_0\right\} \\ q &= \frac{N_\mu p_z}{N_{\mathrm{t}}} \\ I_{\mathrm{EC}} &= Q_\mu \, f_{\mathrm{EC}}(\epsilon_\mu) \, h(\epsilon_\mu) \end{aligned} \tag{4.4.1}$$

where q is the raw data sift factor, I_{EC} is the cost of the error correction and the other terms refer to the privacy amplification required. The raw data sift factor is calculated from the proportion of signal states sent $\frac{N_\mu}{N_{\mathrm{t}}}$, and the probability of Z basis measurements. The error correction term is calculated through $f_{\mathrm{EC}}(\epsilon_\mu)$, the inefficiency of the error correction estimated to be 1.1, Q_μ is the transmission probability of the signal intensity states, ϵ_μ is the quantum bit error rate of the signal states, and $h(\epsilon)$ is the binary Shannon entropy function. Both Q_μ and ϵ_μ can be measured directly. Q_1^z is the transmission probability of the single photon components, e_1^{pz} is the single photon phase error rate, and Q_0 is the background gain; parameters that need to be estimated for privacy amplification. To lower bound the key rate, there must be a lower bound for Q_1^z and Q_0, and upper bound for e_1^{pz}.

As described in Section 3.4.1, the lower bound for the transmittance of single photon states can be described as

$$Q_1 \geq Q_1^{\mathrm{L}} = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \left[Q_{\nu_1} \mathrm{e}^{\nu_1} - Q_{\nu_2} \mathrm{e}^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_\mu \mathrm{e}^{\mu} - Y_0^{\mathrm{L}}) \right] \tag{4.4.2}$$

with a lower bound of the yield of vacuum components provided by

$$Y_0 \geq Y_0^{\mathrm{L}} = \frac{\nu_1 Q_{\nu_2} \mathrm{e}^{\nu_2} - \nu_2 Q_{\nu_1} \mathrm{e}^{\nu_1}}{\nu_1 - \nu_2} \tag{4.4.3}$$

which allows the calculation of the gain of the background as

$$Q_0 = Y_0 \mathrm{e}^{-\mu} Q_\mu \ . \tag{4.4.4}$$

These can then allow the upper bounding of the single photon error rate as

$$e_1 \leq e_1^{\mathrm{U}} = \frac{\mu}{\nu_1 - \nu_2} \frac{\epsilon_{\nu_1} Q_{\nu_1} \mathrm{e}^{\nu_1} - \epsilon_{\nu_2} Q_{\nu_2} \mathrm{e}^{\nu_2}}{Q_1^{\mathrm{L}} \mathrm{e}^{\mu}} \ . \tag{4.4.5}$$

4.5 Results

The experimental results can be seen in Figure 4.12, where each of the two channels is displayed independently with and without the effects of the neighbouring channel noise. At the equivalent of 20 km distance the two channels operate at 489 kbps and 730 kbps, with 1.18% and 0.96% signal intensity QBER respectively without the effects of the neighbouring channel noise. When the neighbouring channel is introduced it will incur random errors (as the two signals are independent and uncorrelated), which are reduced through the wavelength and temporal filtering approaches described above. This produces estimated secure key rates of 457 kbps and 662 kbps with 1.51% and 1.48% signal intensity QBER respectively when including the effects of the neighbouring channels and can be summed to produce an estimated secure key rate of ∼1.11 Mbps over 20 km emulated fibre link.

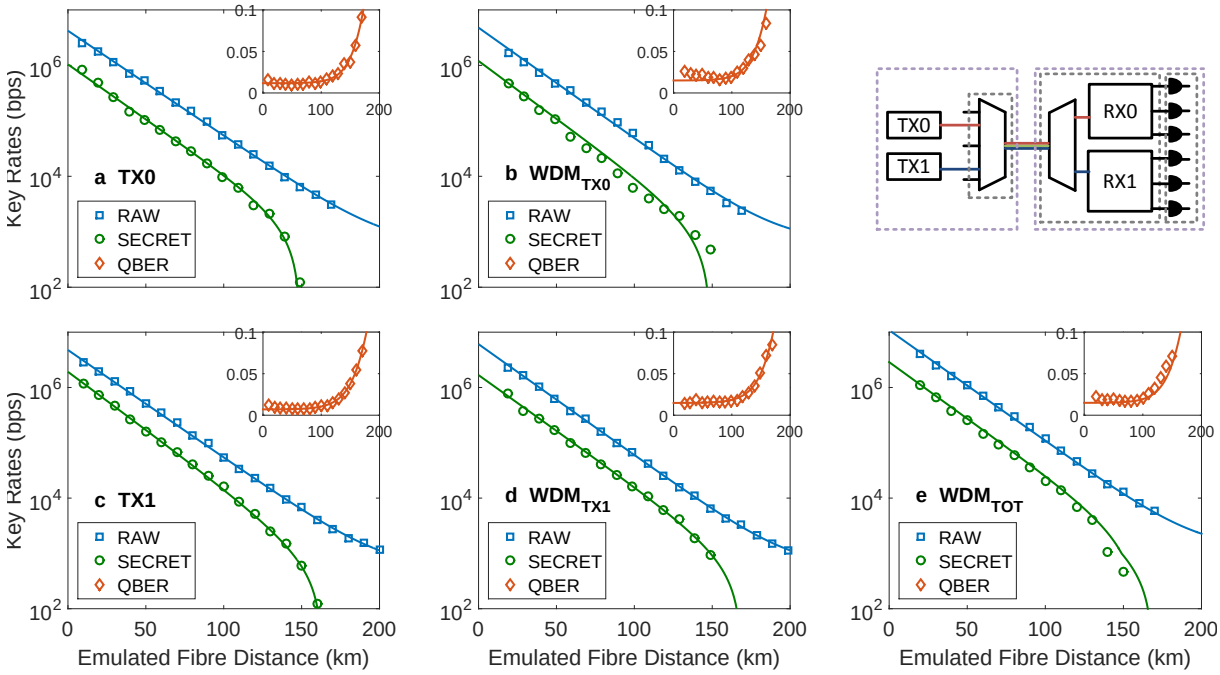

Figure 4.12: **WDM-QKD Secret Key Rates:** (a) Channel 0 rates without operating channel 1. (b) Channel 0 rates while operating channel 1. (c) Channel 1 rates without operating channel 0. (d) Channel 1 rates while operating channel 0. (e) Total rate of the WDM-QKD link

4.6 Summary

This work demonstrates the feasibility of using fully integrated devices within QKD systems, and specifically an approach to increase the rates of QKD by demonstrating WDM-QKD. We used two integrated transmitters and a receiver circuit that included both demultiplexing and decoding to generate a total estimated secret key rate of 1.1 Mbps at an emulated 20 km fibre attenuation (4 dB). The integrated photonic platform allowed us to demonstrate miniaturised devices exploiting robust, low-cost manufacturing processes, that allow flexibility in fibre network settings.

By adopting an integrated photonics platform, we were able to produce highly complex and reconfigurable photonic circuitry capable of performing high-speed, multi-protocol, and multiplexed QKD. We have demonstrated the utility of exploiting this platform and the benefits it can bring the current QKD and quantum communication technologies. By increasing the rates of QKD with practical and miniaturised devices, this approach will ultimately allow for the operation of high-speed ultra-secure encryption across telecom-

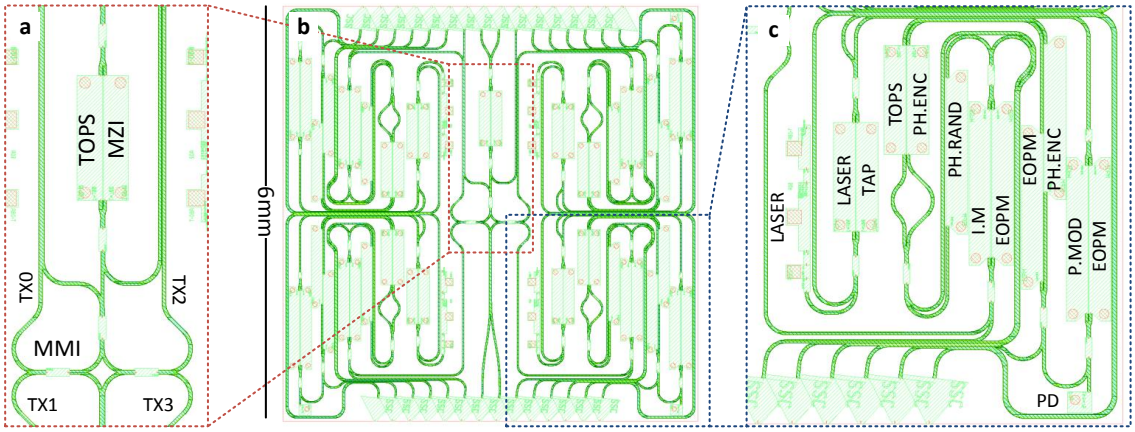

Figure 4.13: **Daisy-chained WDM-QKD TX mask:** (a) WDM mask containing the 3 MMI splitters to combine the 4 channels together, followed by an MZI acting as tunable beam splitter to add additional channels from other chips. (b) 4-WDM channel TX mask containing 4 copies of the transmitter circuitry and the WDM combiner (c) TX mask containing a tunable laser, electro-optic and thermo-optic modulators inside interferometers to operate as multi-protocol transmitters.

munication networks. Moreover, the ability to scale up these integrated circuits to 1000's of components [180] opens the way to even more new and advanced integrated quantum communications technologies.

4.7 Further Developments - Improvements

Future demonstrations of this work will include increasing the number of transmitters and receivers in one link, making monolithic devices to reduce the need for the extra fibre-optical components required for this demonstrations, and optimising the operation of these devices to ensure the highest rate of secured key can be extracted. Here we describe next generation designs and design considerations for WDM-QKD receivers and transmitters, as well as modelling techniques for WDM-QKD links that will allow for parameter optimisation.

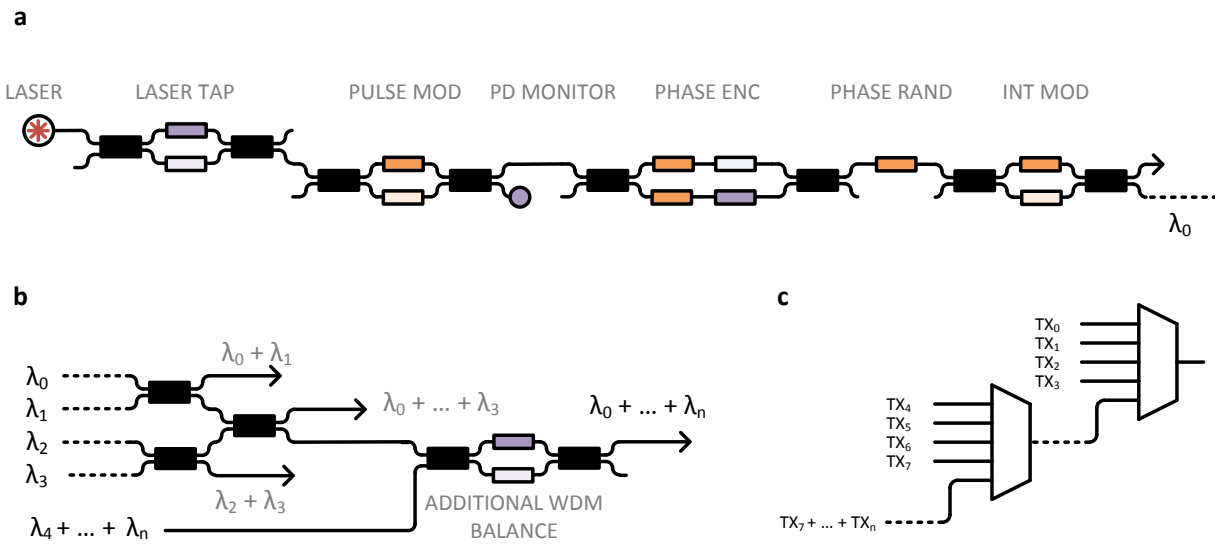

Figure 4.14: **Daisy-chained WDM-QKD TX schematic:** (a) TX schematic as described in Chapter 3 and above. The EOPMs are represented as orange blocks, with the lighter colour representing use for DC offsets and the purple blocks represent TOPS. (b) WDM through 50:50 beamsplitter combining λ_0 to λ_3, but followed by an optional tunable beam splitter, that allows further channels to be combined on to the same channel in a daisy-chained configuration (c) The daisy-chained configuration schematic allowing $4n$ channel MUX.

4.7.1 Daisy Chain TX Design

To increase the secure key rates of the WDM-QKD link we can further increase the number of transmitters, for which I have designed and compiled a mask for an Indium Phosphide device with 4 transmitters to be fabricated by Oclaro (see Figure 4.13). Some of the design considerations include keeping the fast RF EOPM connections near the edge of the chip, and keeping slower EOPM and TOPS on the inside of the device. This will reduce wire bonding lengths for the high-speed modulators which could increase the parasitic inductances and resistances, ultimately limiting the achievable modulation speeds.

A TOPS-MZI (LASER TAP) has been included to easily calibrate the laser wavelength externally before going through the attenuation of the circuit, as well as TOPMs to provide the correct DC offsets inside the phase encoding MZI (as described in Section 3.2.4) with better accuracy.

The transmitter WDM-MUX was implemented using passive 50:50 combiners as de-

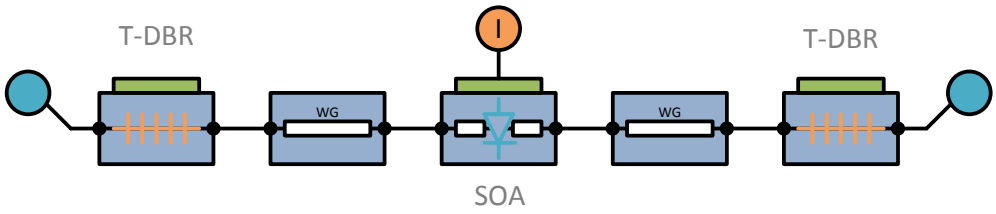

Figure 4.15: **WDM-QKD TX Laser design:** Functional component design of the laser including two T-DBRs, and SOA material, and separating passive waveguide sections.

scribed above. This will allow flexible wavelength channel spacings on the transmitter side to match any WDM de-MUX receiver circuit designed in the future, or for dynamic reconfiguration of the channel spectra during operation.

A further addition to the WDM-MUX design was a final TOPS-MZI, that could allow the weighted inclusion of another 4 channels from a second chip. This in principle could allow $4n$ transmitters by daisy-chaining the devices (as illustrated in Figure 4.14 (c)), until the power of the lasers are insufficient to provide the correct photon numbers per pulse (which heavily depends on the coupling and component loss of the devices).

4.7.2 LASER modifications

The operation of this multi-chip daisy-chained architecture intrinsically causes a lot of loss (at least $(\frac{1}{2})^{\log_2(N)}$ transmitivity, where N is the number of transmitters, and excluding device and chip facet losses) and therefore requires lasers with sufficient output power to overcome this attenuation and still be calibrated to have a $\sim$0.5 photon number per pulse. The laser has therefore been modified from previous designs to provide a higher output power at a possible cost of spectral linewidth and therefore coherence.

The design of the laser focusses on a Fabry-Perot laser diode, comprising two T-DBRs surrounding SOA gain media (Figure 4.15).

T-DBR

A distributed Bragg reflector (DBR) is a periodic structure formed from alternating dielectric layers that can be used to achieve nearly total reflection within a range of frequencies (stop-band). A common example is known as a quarter-wave mirror, where each optical layer has a thickness corresponding to a quarter of the design wavelength [221]. Each

interface between the two materials causes a Fresnel reflection (where the behaviour of light transitioning between media with differing refractive indices causes reflections). For the wavelength under consideration, the optical path length difference between reflections from subsequent interfaces is half the wavelength, with an additional amplitude reflection coefficient alternating in sign. These reflected components from the interfaces therefore interfere constructively and cause strong wavelength dependent reflection (see Figure 4.16 (a)).

The same effect can be generated from Bragg-gratings, where the different layers are created by alternating the effective refractive index of the mode. The DBR's reflectivity (R) for intensity is approximately given by [222]

$$R = \left[\frac{n_0(n_2)^{2N} - n_s(n_1)^{2N}}{n_0(n_2)^{2N} + n_s(n_1)^{2N}}\right]^2 \tag{4.7.1}$$

where n_i is the refractive indices of the originating medium, n_0, the two alternating materials, n_1 and n_2, and the terminating medium, n_s, and where N is the number of repeated pairs of alternative refractive index material.

The frequency bandwidth Δf of the photonic stop-band can also be calculated by

$$\frac{\Delta f}{f_0} = \frac{4}{\pi}\arcsin\left(\frac{n_2 - n_1}{n_2 + n1}\right) \tag{4.7.2}$$

where f_0 is the central frequency of the band.

This can also be shown to lead to a narrow range of wavelengths in which the "Bragg condition" is satisfied

$$\begin{aligned} \frac{2\pi}{\Lambda} &= \frac{4\pi n_{\text{eff}}}{\lambda_{\text{B}}} \\ \Rightarrow \lambda_{\text{B}} &= 2n_{\text{eff}}\Lambda \end{aligned} \tag{4.7.3}$$

where Λ is the grating period, λ_{B} is the free space wavelength, and n_{eff} is the effective refractive index of the light in the waveguide. For 1550 nm light, in a material with effective refractive index ~3, then this would require a grating period of 258 nm. The bandwidth ($\Delta\lambda$) is defined as the wavelength spacing between the first minima, and in

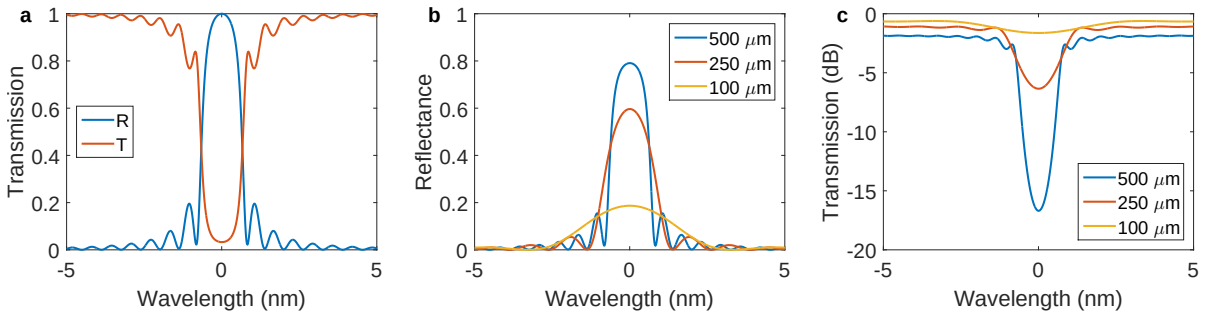

Figure 4.16: **DBR Reflection and Transmission:** PICWave simulations of (a) transmission and reflection of an idealised Distributed Bragg Reflector showing a band of wavelengths that are reflected. (b) Reflection at different lengths of Bragg Reflector, showing that as the reflector length increases so does the strength of the reflection and the bandwidth decreases. (c) The transmission represented in dB to also demonstrate the increased extinction ratio as the length increases, but also a relationship between the length and the loss that it incurs in the pass-bands of the mirror.

the strong grating limit is

$$\Delta\lambda = \left[\frac{2\delta n_0 \eta}{\pi}\right] \lambda_{\mathrm{B}} \tag{4.7.4}$$

where δn_0 is the variation in the refractive index, η is the fraction of the power in the core of the waveguide. This is an approximation that does not apply when the grating length, L_g, is not large compared to $\lambda_{\mathrm{B}}/\delta n_0$.

By increasing the number of pairs in the DBR, we can see an increase in the mirror reflectivity and decrease in transmission (see Figure 4.16 (b) and (c)), and by increasing the refractive index contrast (or grating coupling strength), we can increase both the reflectivity and the bandwidth as illustrated in Figure 4.17 (b).

To fully understand and design the operating conditions of the T-DBR, there must be a specific length chosen, as well as the pitch (Figure 4.17 (a)), and index contrast. Further manipulation of the mirror can be achieved by current injection (as illustrated in Figure 4.17 (c)), where injecting current causes a change in the refractive index of the material and therefore a change in the location of the central wavelength of the stop-band. In this simulation it can also be seen that this current injection causes an increase in loss in the pass-band of the material, which will eventually limit the laser operability.

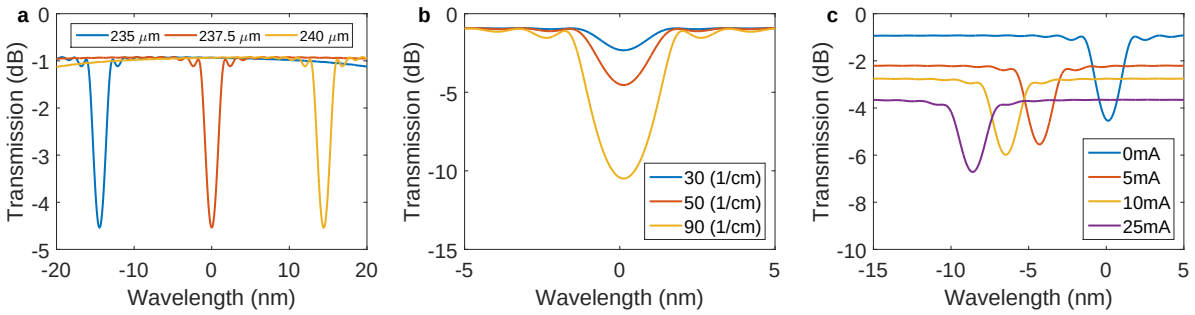

Figure 4.17: **DBR Parameter Variations:** (a) Variation in the pitch of the grating, illustrating the change in central wavelength by altering the pitch. (b) The grating coupling strength, κ, is defined by the grating etch depth of the process, with Oclaro offering 30, 50 and 90 cm^{-1} as preferred values, with increasing κ causing a greater extinction ratio for the stop-band. (c) Current injection can alter the central wavelength of the stop-band, by changing the refractive index of the structure, but also increases the loss in the device.

SOA

The semiconductor optical amplifier (SOA) is an optical amplifier based on a semiconductor gain medium. The SOA available in InP allows gain of optical modes over a large spectrum given current injection into the medium (as illustrated in Figure 3.3 in Section 3.2.1). When combined with the DBR in a laser diode structure the spontaneous emission will cause interference in the cavity and lead to stimulated emission in a dominant mode.

DBR Laser Diodes

A distributed Bragg reflector laser comprises two DBRs in a Fabry-Perot laser resonator, with active gain medium inside the cavity [223, 224]. The corrugated waveguide structure of the DBR grating section provides wavelength-dependent feedback to define the emission wavelength. The amplifying medium (SOA) combined with the two DBR sections cause a single-frequency laser with diffraction-limited output. The tunability can therefore be controlled by a separate phase section inside the cavity (such as electrical heating), or by varying the temperature of the gain region via the drive current. Typically the line-width of a DBR diode is a few MHz. Higher powers can be generated by an additional amplifier section after the initial laser structure, but will cause emission that may no longer be in

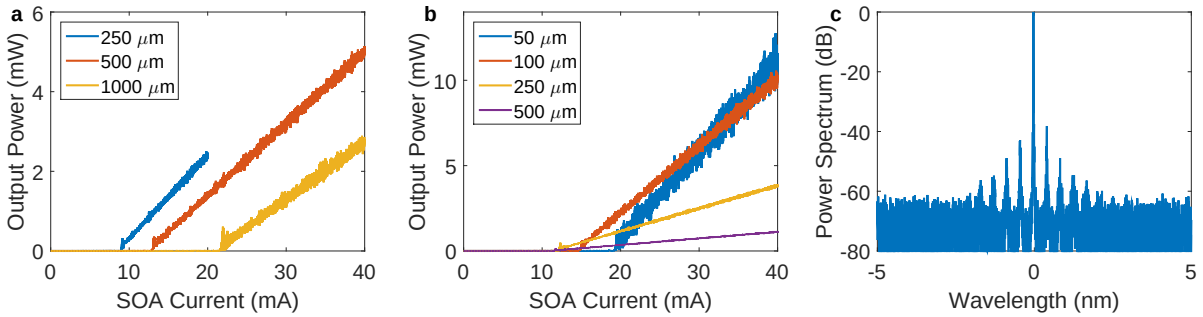

Figure 4.18: **WDM-QKD TX Laser design:** (a) Power vs Current for different SOA sizes illustrating that smaller SOA gives smaller current thresholds, and higher efficiency. Smaller SOA sections also have higher current densities at which points the simulations may not sufficiently represent how the SOA will respond, as seen in the 250 μm simulation. (b) Power vs current different front T-DBR given a fixed length of 250 μm, showing that increasing lengths provide lower current thresholds, but also lower gradients for power vs current. As the front T-DBR is decreased there is also opportunity for increased noise output. (c) An example spectrum from the simulations illustrates a ∼40 dB side band suppression, and -60dB spontaneous emission spectra. The FWHM is expected to be ∼200 fm although may again be limited by the resolution of the simulation.

a signal mode. It will include additional spontaneous emission and noise, but still with a relatively small bandwidth.

Figure 4.18 illustrates some of the simulations used to design this next generation laser, including varying the length of the SOA section, and the length of the front and back T-DBRs. The previous design consisted of a 200 μm length T-DBR on both sides, with a pitch of 237.8 nm and standard κ of 50 cm^{-1}. The centre SOA was chosen to be 500 μm, with two waveguides of length 100 μm inside the cavity, separating the SOA from the T-DBR.

With the design requirements of higher output power with similar coherence, the laser parameters were chosen to therefore maximise the power output without significantly increasing the noise sources. This was achieved by decreasing the length of the front T-DBR and increasing the length of the back T-DBR. The front T-DBR being smaller causes more spontaneous emission and sidebands to leak through to the mode, therefore increasing the noise. The back T-DBR being longer than the front will also mean that more signal will come out the front into the circuit compared to the back where it is not used. The new design therefore consists of a 300 μm length T-DBR on the back and 100 μm on the front side, with a pitch of 237.8 nm and standard κ of 50 cm^{-1}. The centre

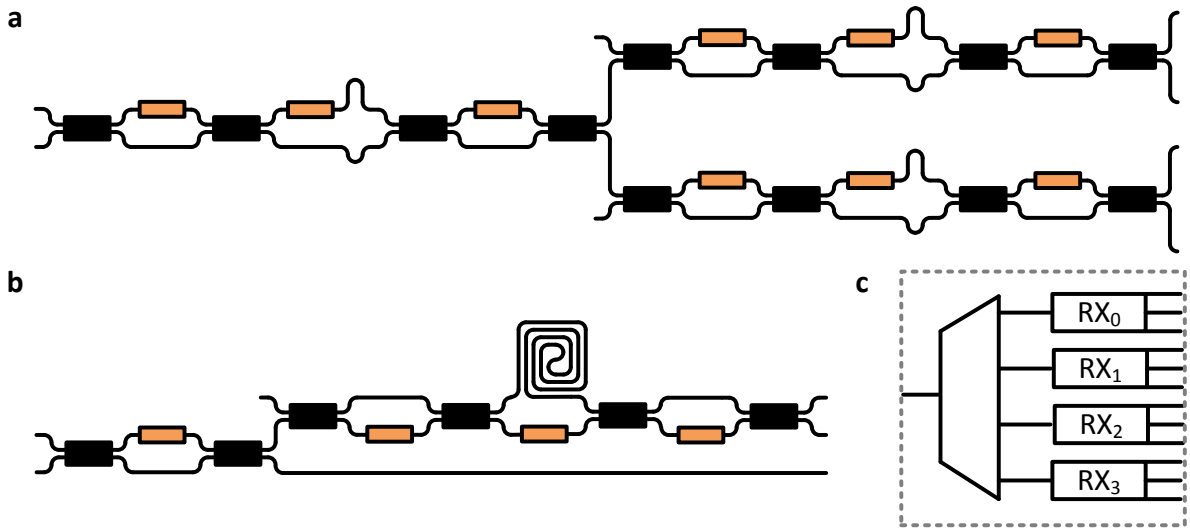

Figure 4.19: **WDM-QKD RX Schematic:** (a) WDM de-MUX circuitry with concatenated AMZI filters, where each filter contains two MZIs to provide tunable beam splitters and set them to be 50:50 for increased and balanced extinction ratios. (b) RX circuitry as described in Chapter 3, but without the reconfigurable delay line. An MZI is used at the final beam splitter to ensure good visibility can be achieved. (c) Schematic of 4-RX WDM circuit combination.

SOA was again chosen to be 500 μm, and with two waveguides of length 100 μm inside the cavity, separating the SOA from the T-DBR.

This design will require a slightly higher current threshold around 20 mA compared to the previous 12 mA, as it takes more current to cause population inversion and lasing.

4.7.3 WDM deMUX

The next generation receiver circuit has been designed and mask compiled for fabrication in SiO_xN_y by LioniX. The design is based on the previous RX circuit (see Figure 4.19 (b)), but has limited the time-bin selection to 600 ps, and increased the number of receiver circuits to 4 (see Figure 4.19 (c)).

Based on the previous results achieved in Section 4.3.1, there was variability in the directional couplers due to manufacturing tolerances, which led to the 35:65 splitting observed. This reduces the achievable interference of the $\{|+\rangle, |-\rangle\}$ measurements. To reduce this effect, an MZI is now implemented at the end of the AMZI instead of a directional coupler so that a TOPS can be used to provide the appropriate 50:50 splitting, thus reducing the QBER achievable.

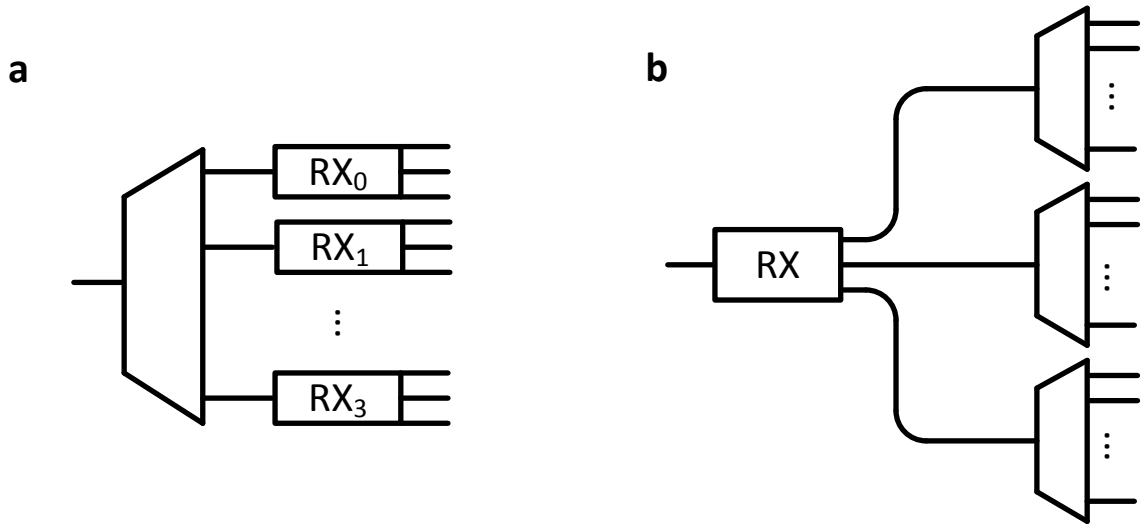

Figure 4.20: **De-Multiplexing Architectures:** (a) De-MUX followed by n receivers. (b) One receiver with three de-MUX blocks. Each de-MUX has n outputs as well, but could reduce space requirements if the de-MUX are more compact that the receiver circuit.

To de-MUX the four QKD channels, AMZI filters have been used (see Figure 4.19 (a)). The first MZI with a FSR of 3.2 nm splitting channel 1 and 3 in to the top arm, and channels 2 and 4 in to the bottom arm (where the channel spacing was chosen to be the standard 200 GHz DWDM). The second AMZI filters are used to split channel 1 and 3 into two separate outputs, and to separate channel 2 and 4. These last two therefore require an FSR double the previous. To ensure good extinction on both arms, the directional couplers have been replaced with MZIs to allow for 50:50 splitting with good reliability.

The outputs of these lead to 4 copies of a reconfigurable RX circuit to allow for multi-protocol QKD operation (Figure 4.21 (a)). Test structures of ring resonators have been included to asses the feasibility of ring-filters, as they can provide a sharper FWHM to FSR ratio compared to the AMZI, which could allow for a better signal-to-noise ratio in the signal (as illustrated in Figure 4.21 in the bottom right of the mask).

This approach may prove infeasibly large when multiplexing many more signals, and another technique has been included in this design to evaluate the different approaches. This has the input of the circuit being a single copy of the receiver circuit, that each channels passes through followed by WDM de-MUX on each outputs (Figure 4.20). This approach allows decoding on the independent TX channels, but cannot implement fully independent protocol reconfiguration. Though this could limit flexibility of operation, it

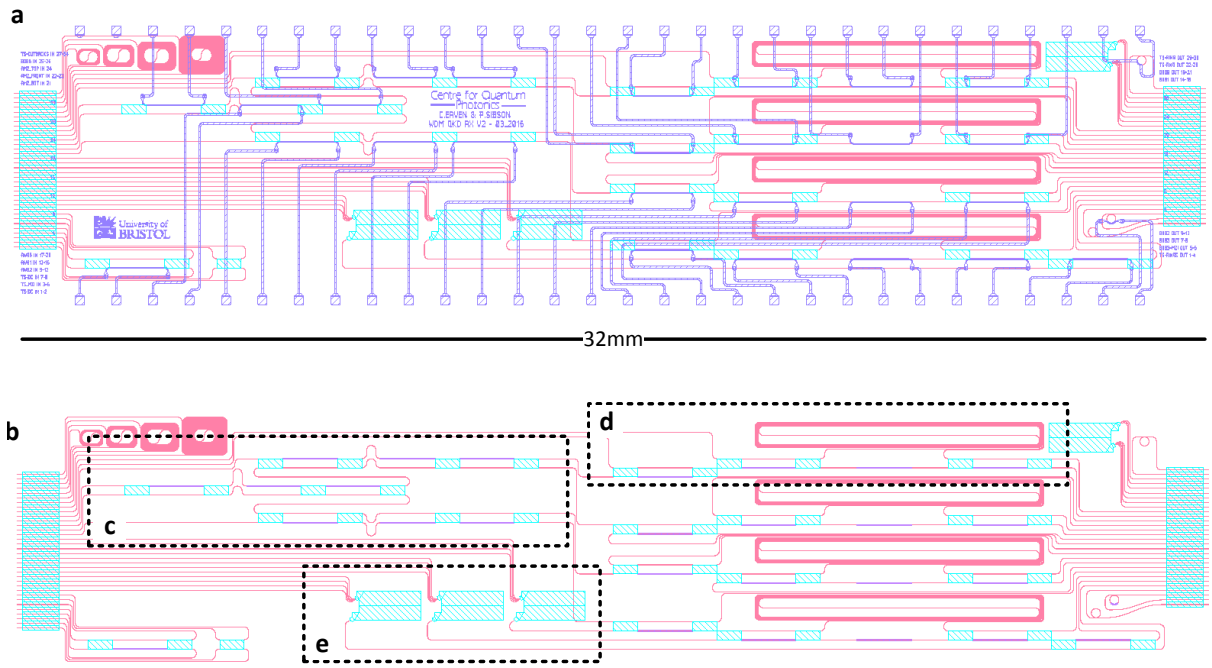

Figure 4.21: **WDM-QKD RX Mask:** (a) Full photonic mask for next generation WDM-QKD RX. (b) Mask without metal routing for clarity with highlights around (c) WDM AMZI circuitry, (d) one copy of the reconfigurable multi-protocol receiver circuit, and (e) AWG circuits that could replace the WDM AMZI circuitry, or provide a different architecture as illustrated in Figure 4.20.

does not compromised the security and may provide for more compact devices when using small footprint de-MUX e.g. AWGs compared to the fairly large receiver circuits. AWGs also allow a relatively fixed loss, independent of the number of channels, and therefore are a suitable approach for large numbers of channels, whereas systems such as AMZIs and ring resonators will have around $O(\log(n))$ loss, where n is the number of channels. The two approaches are both included in the single device as illustrated Figure 4.21 (b).

4.7.4 Modelling and Optimisation

The effects of extra noise from the crosstalk between channels need to be included in the security models or mitigated against to ensure the appropriate measure are taken to guarantee the security of the system. Firstly the channels need to be operated independently, including separate quantum random numbers with no correlation to drive the different transmitters, and to reduce crosstalk as much as is reasonably possible through

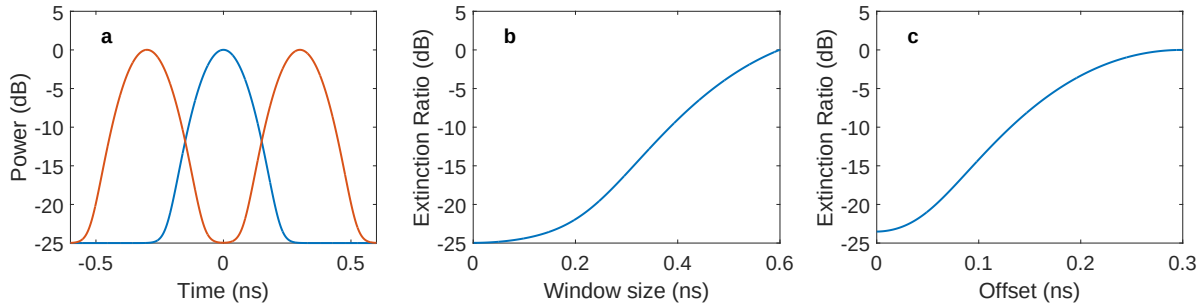

Figure 4.22: **Modelling Errors from Temporal Filtering** (a) Two signals, the blue signal channel and the red channels offset by half a period without any wavelength filtering. (b) The effective extinction ratio of the temporal filtering for a given window size. (c) The effective extinction ratio of the temporal filtering given a 150 ps window function but varying the precise offset between the two channels away from half a period.

wavelength and temporal filtering as described above. Following this, the extra effects of crosstalk should be modelled to optimise the appropriate decoy state levels and error bounds.

Temporal and Wavelength Filtering

As described in Section 4.4.1 there is not only wavelength filtering of the WDM channel, but also neighbouring channels have an offset of half a period and a window gating the detector events. For an assumed Gaussian shaped pulse modulation with FWHM of 150 ps separated by 600 ps but with a finite extinction of 25 dB (Figure 4.22 (a)), we can work out the effectiveness of temporal filtering as a function of the window size (Figure 4.22 (b)). The smaller the window the closer to the -25 dB extinction we can achieve, but as the window gets bigger there is less effect for this filtering. There will be a trade off against the amount of channel signals we can get collect in the window and the crosstalk errors it incurs.

We can also see in Figure 4.22 (c) that for a given window size of 150 ps, the more the neighbouring channel is offset from the half period timing difference, the less effective the temporal filtering is.

Errors

The errors can be modelled to include the effects of dark counts, general state preparation and measurement issues, and the crosstalk from neighbouring WDM channels. The state preparation and measurement errors should be consistent and approximately independent of the channel attenuation. They stem from the visibility of the receiver AMZI, the extinction of the pulse modulation and detector jitter in the measurements. The effects of dark counts become more problematic as the channel loss increases, whereas the crosstalk should also be consistent.

Incorporating these factors into a model accurately can be difficult. Taking a phenomenological modelling approach we can combine all of these effects into a simple model. For the signal QBER, we can define a base error rates, ϵ_{b}, and given attenuation length define the expected error as

$$\epsilon_{\mu} = \epsilon_{\mathrm{b}} + \frac{0.5 - \epsilon_{\mathrm{b}}}{1 + \exp\left[-\alpha(L - \beta)\right]} \tag{4.7.5}$$

where α and β can be extracted from experimental data (with our model using $\alpha = 0.1$ and $\beta = 200$). As illustrated in Figure 4.23 (b) this function tends to 0.5 QBER as the signal-to-noise increases when the attenuation of the signal is more than the dark counts expected on the detector. It also has an approximately flat error rate when the effects of dark count signals are limited, and the effects of state preparation and measurement are dominant.

For a decoy state the intensity is less than that of the signal state, and therefore the signal-to-noise ratio will be less. This is somewhat equivalent to the length, L, increased proportionately to the ratio of the signal and decoy state

$$L_{\nu_1} = L - \frac{10\log_{10}(\frac{\nu_1}{\mu})}{0.2} \tag{4.7.6}$$

where the value 0.2 is used as the standard attenuation of fibre optics in dB/km, and μ and ν_1 are the signal and decoy state intensities respectively.

A second step in estimating the error in the decoy intensity states is including an alteration to the base QBER (ϵ_{b}), to incorporate some of the non-ideal and non-linear

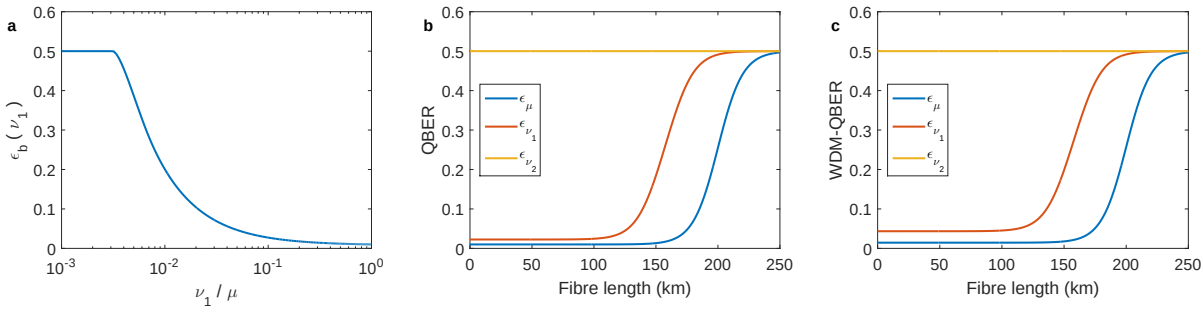

Figure 4.23: **Modelling Errors from Attenuation:** (a) The decoy QBER rate can start with a higher base line QBER from the finite extinction in the modulators. The plot shows that as the intensity compared to the signal intensity gets smaller, the baseline QBER also tends to 0.5, as the non-ideal operations of the concatenated MZIs are not perfectly linear. (b) Example model for errors over fibre distance. As the distance increases the dark counts start to become non-negligible and eventually dominate, causing the error to tend toward 50%. There is a non-zero offset (1% for μ and 2.5% for ν_1) to begin with that is due to the finite precision of state preparation and measurement. The first decoy state tends to 50% QBER more quickly as it is less intense and therefore succumbs to dark counts earlier. (c) Cross-talk effects on the error causing the μ error to a baseline level 1.4% and ν_1 to 4.6% for -20 dB noise.

effects of the concatenated intensity and pulse modulators. This results in a slightly lower extinction ratio between the occupied and unoccupied pulses and therefore more errors. The form of this adjusted baseline error rates, $\epsilon_{\mathrm{b}}(\nu_1)$ is illustrated in Figure 4.23 (a).

This now provides an error rate of

$$\epsilon_{\nu_1} = \epsilon_{\mathrm{b}}(\nu_1) + \frac{0.5 - \epsilon_{\mathrm{b}}(\nu_1)}{1 + \exp\left[-\alpha\left(L_{\nu_1} - \beta\right)\right]} \,. \tag{4.7.7}$$

This illustrates that the decoy intensity state starts with a slightly higher base QBER, as well as a shorter span before the effects of the dark counts start to dominate. The vaccuum state is assumed to not to send any real data and therefore always has an error rate of 0.5, as illustrated in Figure 4.23 (a).

When considering the effect the WDM channels have on the errors, we use the extinction of the wavelength filter (ER_λ) and the extinction from the temporal filter (ER_t) in dB to produce a term for the amount of crosstalk by first calculating the average photon

intensity apparent from the neighbouring channel, $\hat{\mu}$,

$$\begin{aligned}\hat{\mu} &= 10^{-\left(\frac{\mathrm{ER}_\lambda + \mathrm{ER}_t}{10}\right)}\mu_{\mathrm{avg}} \\ \mu_{\mathrm{avg}} &= \left(\mu p_{za} + \nu_1(1-p_{za})p_{\nu_1} + \nu_2(1-p_{za})(1-p_{\nu_1})\right)\end{aligned} \tag{4.7.8}$$

where p_{za} is the probability that Alice transmits a signal intensity state, and p_{ν_1} is the probability of sending a ν_1 state compared to a ν_2 state. This average photon number provides a weighting for the amount of errors it introduces compared to the original channel. Due to the independence of the two channels it should always provide 50% error on average. The errors therefore become

$$\begin{aligned}\hat{\epsilon}_\mu &= \frac{\epsilon_\mu \mu + 0.5\hat{\mu}}{\mu + \hat{\mu}} \\ \hat{\epsilon}_{\nu_1} &= \frac{\epsilon_{\nu_1}\nu_1 + 0.5\hat{\mu}}{\nu_1 + \hat{\mu}} \\ \hat{\epsilon}_{\nu_2} &= 0.5\ .\end{aligned} \tag{4.7.9}$$

This will effect the error associated with the first vacuum state more than the signal state. This can be seen in Figure 4.23 (c), where it increases the decoy base level error from 2.5% to 4.6%, whereas the signal state error only increases from 1% up to 1.4%. This was simulated with a crosstalk level of -20 dB (which was an underestimate of the crosstalk filtering achievable in this experiment).

Gain

To model the gain, it was assumed that the dominant effects were channel attenuation, receiver detector efficiency, dark counts, and crosstalk from the channels. The detectors were assumed to be non-number resolving, and therefore two photons incident on the detector would register as a single click. Assuming Poissonian statistics, this can be modelled as a unit efficiency detector with the loss before reducing the average photon number to

$$\mu' = \eta_{\mathrm{DET}}\eta_{\mathrm{BOB}} 10^{-\frac{\alpha L}{10}}\mu \tag{4.7.10}$$

where η_{DET} and η_{BOB} are the efficiency of the detector and the transmission of the receiver circuit respectively, and L is the fibre distance, with α being approximated as 0.2 dB/km for standard telecommunication fibres. The probability of a detection signal is the probability of there being at least one photon, $(\bar{p_0})$, or equivalently not the probability of no photons.

$$\begin{aligned}\bar{p_0} &= \sum_{i=1}^{\infty} p_i \\ &= 1 - p_0 \\ &= 1 - \exp(-\mu') \end{aligned} \tag{4.7.11}$$

and therefore the gain can be estimated to be

$$Q_\mu = \eta_{\mathrm{T.W}}(\bar{p_0} + p_{\mathrm{d}}) \tag{4.7.12}$$

where p_{d} is the probability of intrinsic dark counts in the detectors, and $\eta_{\mathrm{T.W}}$ is the percentage of signals appearing in the gating window of the detector. This model does not take into account some other effects, such as dead-time of the detectors causing counts to be missed. This effect should be fairly negligible at the photon flux levels measured in this experiment. This provides a method to simulate Q_μ, Q_{ν_1}, and Q_{ν_2}, required in the security proof of the decoy protocol, by replacing the relevant intensities in equation 4.7.10.

To include the effects of the neighbouring WDM channel we can average the gains for each intensity level and add this to the gain of the single channel

$$\hat{Q}_\mu = Q_\mu + Q_{\mathrm{avg}} 10^{-\left(\frac{\mathrm{ER}_\lambda + \mathrm{ER}_t}{10}\right)} \tag{4.7.13}$$

where

$$Q_{\mathrm{avg}} = \left(Q_\mu p_{za} + Q_{\nu_1}(1 - p_{za})p_{\nu_1} + Q_{\nu_2}(1 - p_{za})(1 - p_{\nu_1})\right) . \tag{4.7.14}$$

This can therefore give an lower bound for the single photon gain [62]

$$Q_1 \geq Q_1^{\mathrm{L}} = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2}[Q_{\nu_1}\mathrm{e}^{\nu_1} - Q_{\nu_2}\mathrm{e}^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}(Q_\mu \mathrm{e}^{\mu} - Y_0^{\mathrm{L}})] \tag{4.7.15}$$

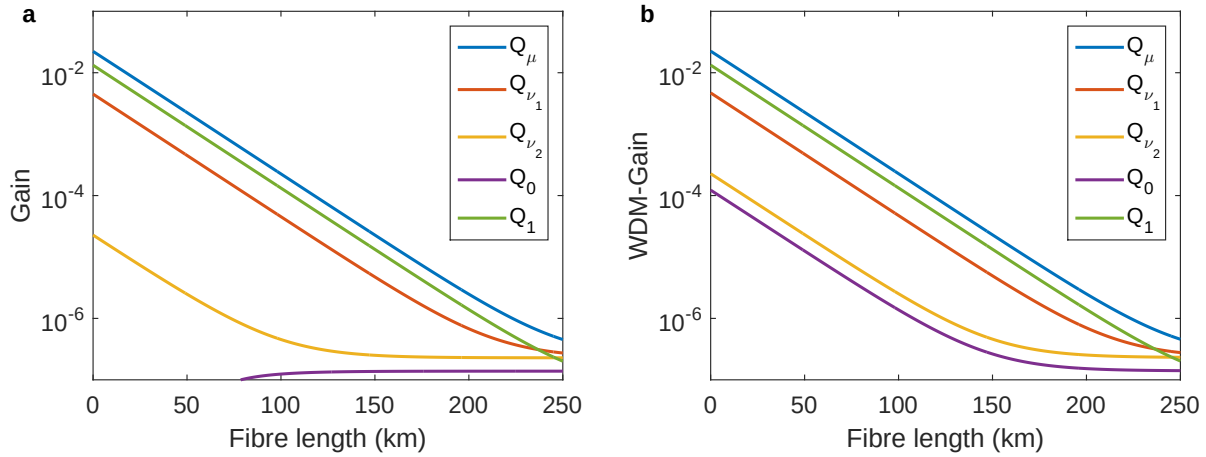

Figure 4.24: **Modelling Gain in WDM-QKD:** For a fixed value of $\mu = 0.5$, $\nu_1 = 0.1$ and $\nu_2 = 5 \times 10^{-4}$ (a) Example model for gain for the three intensities, and the bounded single photon and background gains given 10 dB loss in the receiver circuit, and 45% detector efficiency with a dark count probability of 2.28×10^{-7}. (b) The effects of WDM-QKD on these bounds. Although the single photon gain is fairly robust, the background gain has increased dramatically, especially at lower attenuations.

with a lower bound of the yield of vacuum components provided by

$$Y_0 \geq Y_0^{\mathrm{L}} = \frac{\nu_1 Q_{\nu_2} \mathrm{e}^{\nu_2} - \nu_2 Q_{\nu_1} \mathrm{e}^{\nu_1}}{\nu_1 - \nu_2}, \tag{4.7.16}$$

which allows the calculation of the gain of the background as

$$Q_0 = Y_0 e^{-\mu} \tag{4.7.17}$$

as illustrated in Figure 4.24.

Decoy State Rates

This model can then provide a method for estimating the upper bounding of the single photon error rate as [218]

$$e_1 \leq e_1^{\mathrm{U}} = \frac{\mu}{\nu_1 - \nu_2} \frac{\epsilon_{\nu_1} Q_{\nu_1} \mathrm{e}^{\nu_1} - \epsilon_{\nu_2} Q_{\nu_2} \mathrm{e}^{\nu_2}}{Q_1^{\mathrm{L}} \mathrm{e}^{\mu}} \ . \tag{4.7.18}$$

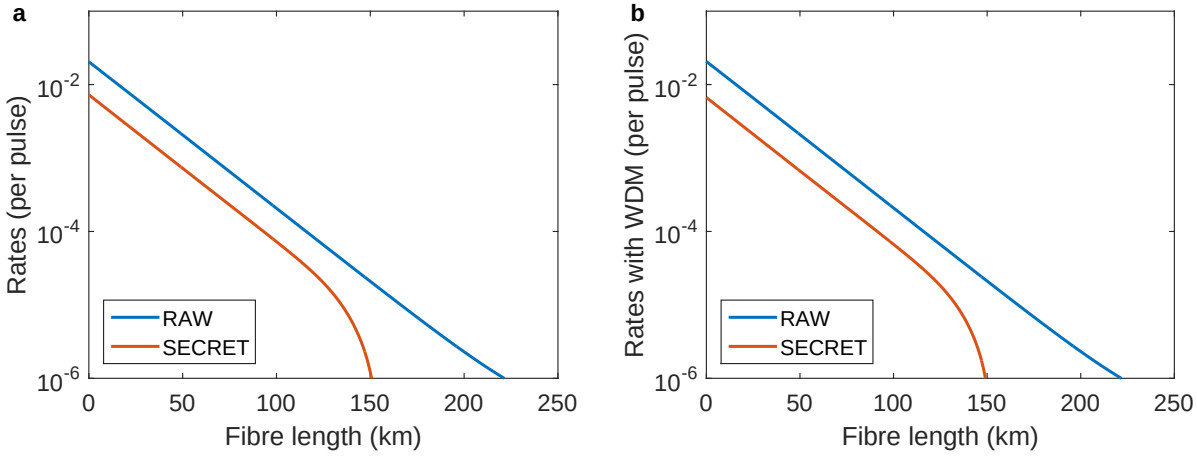

Figure 4.25: **Modelling Rates in WDM-QKD:** For a fixed value of $\mu = 0.5$, $\nu_1 = 0.1$ and $\nu_2 = 5 \times 10^{-4}$ (a) Example calculation of the secret key rate given 10 dB loss in the receiver circuit, and 45% detector efficiency with a dark count probability of 2.28×10^{-7}. The probability of sending a particularly decoy state is 0.9, 0.09, and 0.01 for $\{\mu, \nu_1, \nu_2\}$ respectively. The probability of measuring in the Z basis was set to 0.9. (b) The effects of WDM-QKD on these estimates. The effects of WDM with wavelength and temporal filtering of to -20 dB was fairly insignificant, with the rates reduced by $\lesssim$8% at $\lesssim$100 km attenuation, and dropping off slightly earlier, at the 150 km mark.

And therefore a secure key rates of

$$\begin{aligned} K &\geq q\nu_s \left\{-I_{\mathrm{EC}} + Q_1^z \left[1 - h(e_1^{pz})\right] + Q_0\right\} \\ q &= \frac{N_\mu p_z}{N_{\mathrm{t}}} \\ I_{\mathrm{EC}} &= Q_\mu \, f_{\mathrm{EC}}(\epsilon_\mu) \, h(\epsilon_\mu) \end{aligned} \tag{4.7.19}$$

where q is the raw data sift factor, I_{EC} is the cost of the error correction and the other terms referring to the privacy amplification required. The raw data sift factor is calculated from the proportion of signal states sent $\frac{N_\mu}{N_{\mathrm{t}}}$, and p_z the probability of Z basis measurements. The error correction term which is calculated through $f_{\mathrm{EC}}(\epsilon_\mu)$, the inefficiency of the error correction estimated to be 1.1, Q_μ is the transmission probability of the signal intensity states, ϵ_μ is the quantum bit error rate of the signal states, and $h(\epsilon)$ is the binary Shannon entropy function. This is illustrated in Figure 4.25

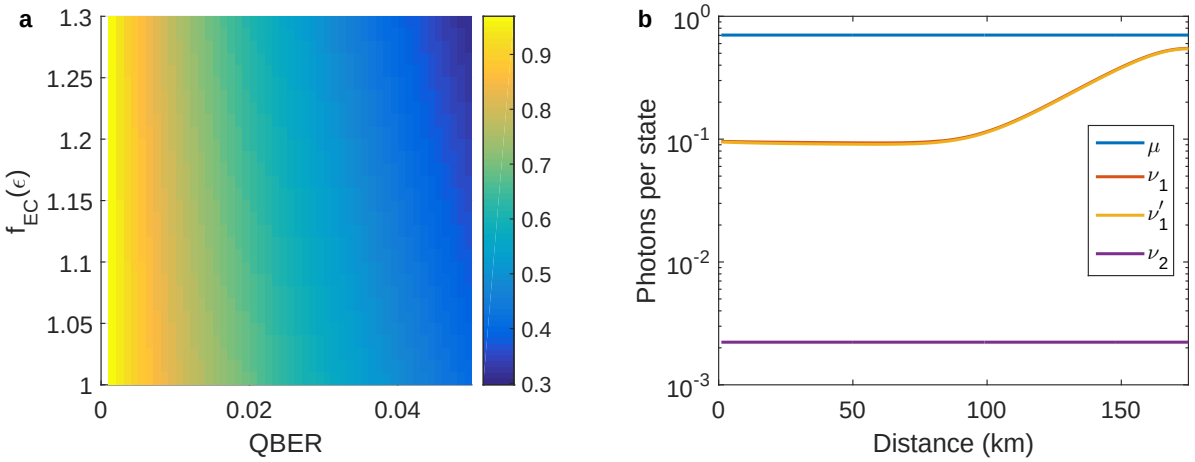

Figure 4.26: **Optimising μ Rates in WDM-QKD:** (a) For the decoy state method, optimise the value μ based on the QBER and f_{EC} achievable. (b) The optimised values of ν_1 and ν_1'; the decoy state intensity for single channel and WDM-QKD cases respectively are shown but closely overlap due to the limited effects of crosstalk.

Optimisation

This model can then be used to optimise free parameters of the system to extract the maximum available key rates. This includes the intensities, $\{\mu, \nu_1, \nu_2\}$, the probabilities of sending the states $\{p_\mu, p_{\nu_1}, p_{\nu_2}\}$, the probability of measuring in the Z basis, p_z, under the constraints of extinction ratio limitations and unit probabilities.

To simplify the optimisation μ can be chosen independently of other free parameters, only dependent on the base error rate and error correction inefficiency as [62]

$$K \approx -\eta\mu f_{\text{EC}}(\epsilon_b)h(\epsilon_b) + \eta\mu \mathrm{e}^{-\mu}[1 - h(\epsilon_b)] \ . \tag{4.7.20}$$

To optimise this rate with respect to μ, we choose $\mu = \mu_{opt}$ which fulfils

$$(1-\mu)\mathrm{e}^{-\mu} = \frac{f_{\text{EC}}(\epsilon_b)h(\epsilon_b)}{1 - h(\epsilon_b)} \tag{4.7.21}$$

which produces $\mu \approx 0.48$ for $f_{\text{EC}} = 1.22$ and $\epsilon_b = 3.3\%$ (see Figure 4.26)

We can then use a standard optimisation tool to find the optimal values for the rest of the free parameters. The cost function of which should include the real part of a secure key rate, excluding results that involve any negative or imaginary key rates. Other

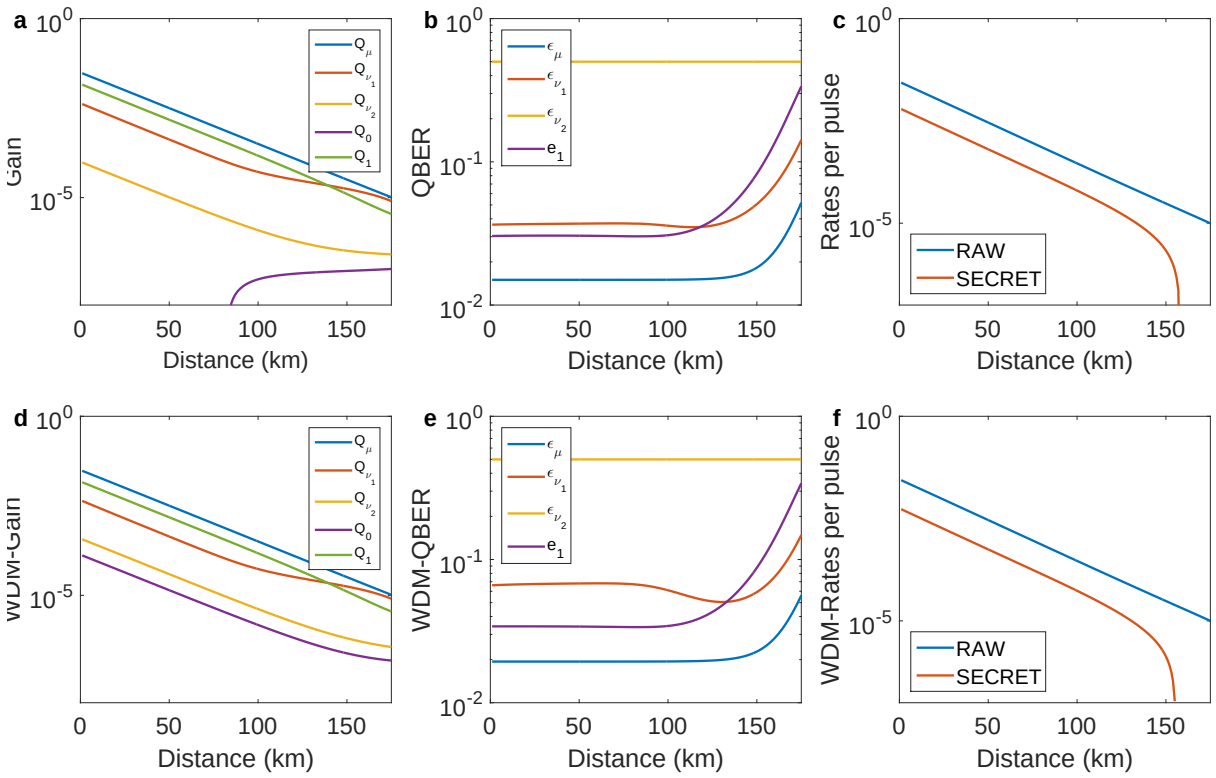

Figure 4.27: **Optimising Rates in WDM-QKD:** (a)&(d) provide the modelled gain for the optimised parameters, (b)&(e) are the modelled errors for the optimised parameters, and (c)&(f) the modelled raw and secret key rates for the optimised parameters. Both given for the single channel, and WDM-QKD results respectively, showing extreme similarity between the respective key rates with -20 dB filtering.

regulatory parameters are included to ensure reasonable results such as a term from the bounded single error rate. The effects of the weightings between these terms will affect the performance results achievable. An example of this approach, varying the ν_1 intensity is illustrated with Figure 4.27, where both the WDM and the non-WDM channel follow very similar patterns, and fail to achieve a real result at lengths $\gtrsim$150 km.

Future models should also include the effects of finite key sizes, and errors in statistical measurements to capture and optimise the probabilities used, and how these can be optimised to provide the best key rates [98, 218]. It could also include cases of non-symmetric channel crosstalk, and the effects this could have on independently selecting different intensity values for the decoy states.

4.8 Conclusion

This work demonstrated two independently operated WDM-QKD transmitter and receivers with 1.1 Mbps of secure key rates. Future designs and design considerations have been including for a system of four independent WDM-QKD channels on monolithic devices, with improved transmitter and receiver performances to at least double the secure key rate. The modelling then described will allow the development of optimised performance rates under security proof assumptions to increase rates further, providing high key rates for practical applications of quantum secured communications.

Chapter 5

Silicon Photonic QKD Transmitters

Statement of Work

For this set of technology demonstrations, I designed the experiments and encoding scheme and translated the circuits to a silicon-on-insulator process with fabrication by OpSIS and IMEC. Initial characterisation was taken in collaboration with Stasja Stansinic and later experimental results were performed in collaboration with Jake Kennard.

5.1 Introduction

Integrated photonics offers great potential for quantum communication devices in terms of complexity, robustness and scalability. Silicon photonics in particular is a leading platform for quantum photonic technologies, with further benefits of miniaturisation, cost-effective device manufacture and compatibility with CMOS microelectronics. However, effective techniques for high-speed modulation of quantum states in standard silicon photonic platforms have been limited. Here we overcome this limitation and demonstrate high-speed low-error QKD modulation with silicon photonic devices combining slow thermo-optic DC biases and fast (10 GHz bandwidth) carrier-depletion modulation. We illustrate this approach with the preparation of time-bin encoded BB84 QKD states with 2.1% QBER. We further demonstrate this technology with implementations of polarisation encoded BB84 QKD (1 GHz clock rate, 1.1% QBER, 329 kbps secret key rate) and Coherent-One-Way QKD (1.72 GHz clock rate, 1.01% QBER, 916 kbps secret key rate) over a 20 km fibre link.

Quantum technologies are rapidly developing and have the potential to revolutionise the fields of computing and telecommunications. They have major implications for the security of many of our conventional cryptographic techniques which are known to be insecure against a quantum computer [1]. Fortunately, quantum key distribution (QKD) provides a highly secure approach to sharing random encryption keys by transmitting single photons [2]. Although QKD has advanced from simple proof-of-principle experiments towards robust long-term demonstrations [3–6], it has still not obtained wide-scale adoption.

Integrated photonics provides a stable, compact, and robust platform to implement complex photonic circuits amenable to mass-manufacture, and therefore provides a compelling technology for optical quantum information devices [10]. Silicon photonics, in particular, is a leading platform for quantum photonic technologies with the promise of high density integration, mature fabrication processing, and compatibility with microelectronics [225]. Silicon has been used to demonstrate sources of quantum light, manipulation and transmission of quantum information, and integration with single photon detectors [226–228]. It has also been used in classical computing and communications

for modulation, transceivers [229], and a recent demonstration of optical interconnects alongside electronic microprocessor technology [230].

The appeal of this platform has led to integrated photonic technologies increasingly being deployed in the development of practical QKD systems. Demonstrations include integrated "client" chips for Reference-Frame-Independent QKD [11], planar waveguide components in transmitters and receivers [12], and chip-to-chip QKD using GHz clocked indium phosphide transmitters and silicon oxynitride receivers [181].

However, high-speed modulation of quantum states in standard silicon photonic fabrication has been limited. With no natural electro-optic non-linearity, many silicon quantum photonic experiments instead utilise slow thermo-optic phase modulators (TOPM) for high-fidelity state preparation. Carrier injection or carrier depletion modulators (CDM) offer high-speed operation, but incur phase dependent loss and saturation [231], which are detrimental in quantum applications where state preparation has stringent requirements.

Here we show an approach to overcome the limitations of saturation and phase dependent loss of high-speed carrier-depletion modulators in standard silicon photonic fabrication. First we describe a combination of slow, but ideal, thermo-optic phase modulators alongside fast, but non-ideal, carrier depletion modulators utilised for QKD state preparation at GHz speeds. We then use this technique to demonstrate three implementations of high-speed low-error QKD (Figure 5.1): chip-to-chip Coherent One Way (COW) QKD, polarisation encoded BB84, and time-bin encoded BB84 [42] state preparation. We achieve estimated asymptotic secret key rates of up to 916 kbps and quantum bit error rates (QBER) as low as 1.01% over 20 km of fibre, experimentally demonstrating the feasibility of high-speed QKD integrated circuits based on standard silicon photonic fabrication.

5.2 Phase Modulation

Optical communication systems rely on some method of encoding information on a degree of freedom of light. As discussed in Section 2.4.3, this can be achieved with a number of different phenomena (thermo-optic, electro-optic etc.), and with a number of degrees of freedom (polarisation, time-bin, path etc.).

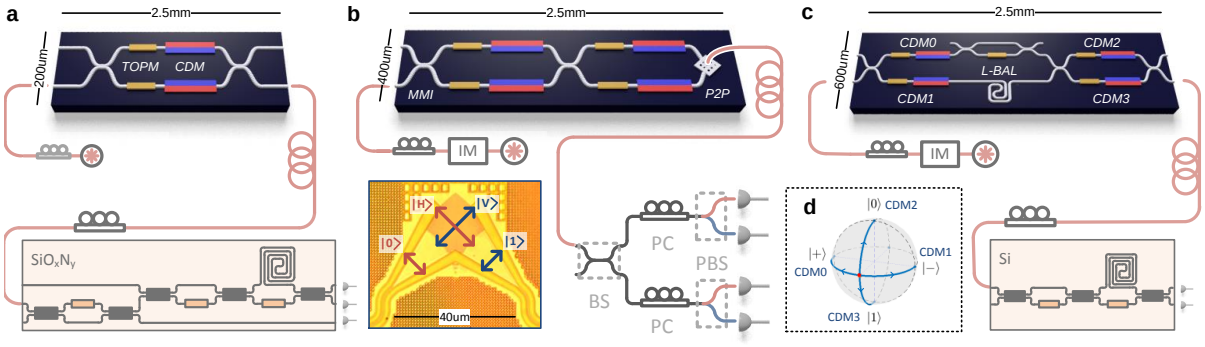

Figure 5.1: **Integrated Silicon Photonic Devices for QKD:** (a) A balanced Mach-Zehnder interferometer (MZI) comprising two multi-mode interference (MMI) devices acting as a beam splitter, with phase modulation from thermo-optic phase modulators (TOPM) and carrier-depletion modulators (CDM) allows for the encoding of quantum information in path, or pulse modulation. (b) Polarisation encoded transmitter: Combining the two paths of the MZI with a two-dimensional grating coupler allows for the conversion between path encoded information to polarisation encoded information (P2P), suitable for communication in free space. (c) Time-bin encoded transmitter: An unbalanced asymmetric MZI (AMZI) allows for encoding in time by temporally separating weak coherent pulses in to two time intervals using an on-chip delay of 1.5 ns. The extra loss this incurs is balanced by an MZI used as a tunable beam splitter on the opposing arm. The last beam splitter in the AMZI is replaced with another MZI that allows for the selection of time bin $|0\rangle$ and $|1\rangle$ states. DC offsets are provided by TOPM and fast modulation by four CDMs. (d) An illustrated Bloch sphere highlighting the DC offset at $|+\mathrm{i}\rangle$, set by the thermo-optic phase modulators. Each CDM is only required to modulate up to $\pi/2$ to permit the encoding of each BB84 state.

In QKD, polarisation is popular for free space communication and forms of time-bin encoding are commonly used for optical fibre communication [1]. In integrated photonics, path encoding is used as a stable degree of freedom with which to encode, and this can be converted to both polarisation and time-bin encoding (see Section 2.4.2).

To encode arbitrary states in path-based systems, we can implement an MZI with the ability to reconfigure the relative phase between the two path. This can be achieved through modulation of the refractive index of the material or optical path length. In silicon photonics, DC offsets can be implemented through slow an ideal thermo-optic phase modulators, but it becomes more complex for high-speed encoding. Silicon has no natural $\chi^{(2)}$ non-linearity and therefore a standard electro-optic effect can not be used.

Although methods exist to induce this non-linearity in silicon [232], use all optical switching [233], or hybridise materials [234], in current silicon photonic platforms a pop-

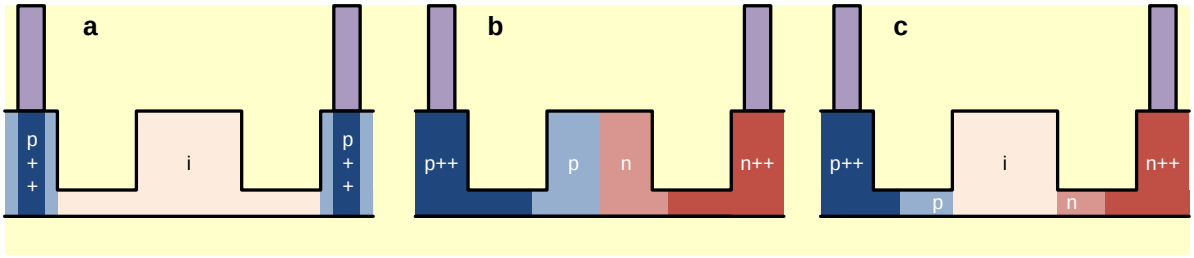

Figure 5.2: **Silicon Photonic Phase Modulation:** (a) Thermo-optic phase shifter cross-section: The intrinsic silicon (i) is used in a rib-waveguide structure, with p++ doping in channels either side. This permits a resistive element near the waveguide where heat dissipation causes a thermo-optic phase shift in the waveguide. (b) Carrier depletion modulator cross-section: The waveguide is doped with p and n to form a diode structure across the waveguide, with p++ and n++ doping to form good electrical contacts with the metal above. This diode structure contains carriers which can be swept out through reverse biasing inducing phase modulation. (c) Carrier injection modulator cross-section: The waveguide is doped in a p-i-n pattern to form a large intrinsic region diode. Carriers can be injected in to the waveguide causing phase modulation.

ular approach is to use doped waveguide sections (see Figure 5.2) and employ carrier injection or carrier depletion techniques to induce phase relationships [235]. These unfortunately cause non-ideal loss characteristics, and this must be taken in to account when designing circuits, especially for quantum applications where the requirements are often more stringent than many classical applications.

5.2.1 Thermo-optic

The thermo-optic shifters (TOPS) in this chapter were designed in silicon-on-insulator with the intention of minimising loss while using doped resistive heating in the waveguide slab, as illustrated in Figure 5.2 (a). This design provides an ohmic electrical characteristic, and a phase relationship proportional to the square of the voltage (see Figure 5.3).

These thermo-optic phase shifters have a 2π voltage of $\sim$24 V with $\sim$6.14 kΩ for 150 μm and 4.1 kΩ for 100 μm. By reducing the length of the heater the overall power required to reach 2π phase difference remains the same, but the voltage reduces. The resistance is linear with the length

$$R = \frac{\rho L}{A} \propto L \tag{5.2.1}$$

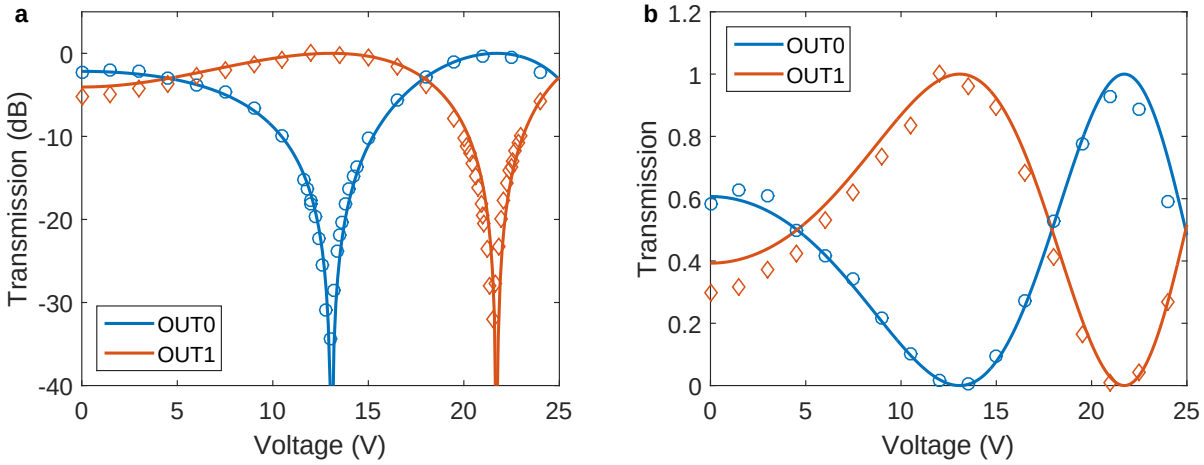

Figure 5.3: **Thermo-optic phase shifter:** The output of an MZI structure (a) in dB showing over 30dB extinction, and (b) the normalised optical power, showing good agreement with a lossless quadratic phase-voltage fit. The 2π voltage is $\sim$24 V.

and the phase is proportional to the power, where the power is described as

$$P = IV = \frac{V^2}{R} \propto \frac{V^2}{L} \ . \tag{5.2.2}$$

This will remain true until the non-ohmic behaviour becomes non-negligible. For a given power, reducing the length will therefore reduce the 2π voltage.

The efficiency of the heater could be improved by decreasing the distance between the resistive element (p++ in Figure 5.2 (a)) and the optical mode (i-region in Figure 5.2 (a)). This has the disadvantage of also increasing the loss of the device as the carriers present in the p++ region induce absorption of the optical mode.

5.2.2 Carrier Injection

Carrier injection modulation (CIM) induces a phase by injection of carrier into the intrinsic mode of the optical waveguide. This is achieved by forward biasing a p-i-n junction formed through doping p and n regions in the slab of the silicon waveguide (Figure 5.2 (c)). The injection of carriers in to the optical waveguide increase the absorption of the waveguide and therefore induce a phase relationship as illustrated in Figure 5.4. The current is exponential with the voltage as is the phase relationship.

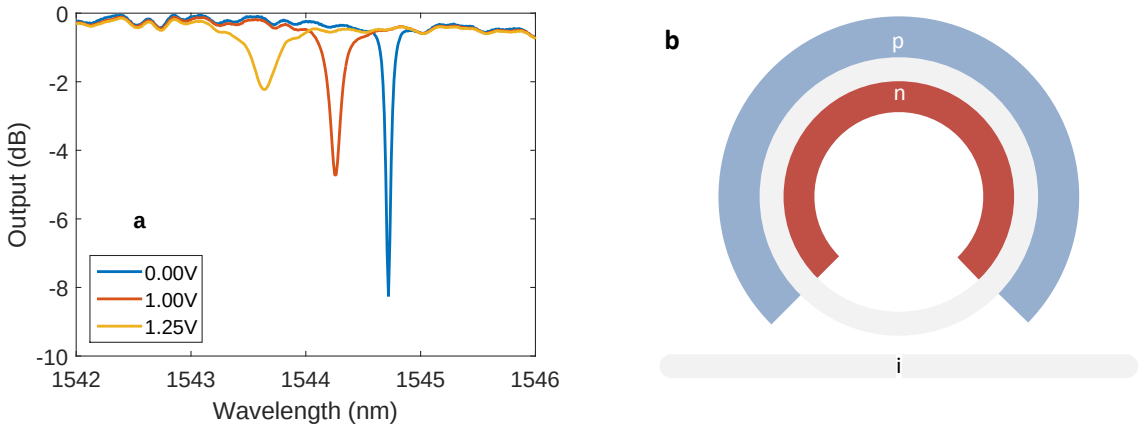

Figure 5.4: **Carrier-Injection Modulation:** (a) Spectrum of an optical ring resonator for different forward bias voltages showing a shift in the phase causing an offset in the resonance, and also a decreasing of the extinction ratio indicative of an increase in loss of the ring. (b) A schematic of the ring resonator structure with *p*-*i*-*n* cross section in the ring.

5.2.3 Carrier Depletion

DC

Carrier depletion modulation (CDM) induces a phase by reducing the carriers occupying the region overlapping the optical mode. This is achieved by reverse biasing a *p*-*n* junction formed by doping *p* and *n* regions in the core of the silicon waveguide (Figure 5.2 (b)).

The depletion of carrier in the optical waveguide decreases the absorption of the waveguide and therefore induces a phase relationship [179].

$$\Delta n = -\left[8.8 \times 10^{-22} \times \Delta N_e + 8.5 \times 10^{-18} \times (\Delta N_h)^{0.8}\right] \tag{5.2.3}$$

$$\Delta \alpha = -\left[8.5 \times 10^{-15} \times \Delta N_e + 6.0 \times 10^{-18} \times \Delta N_h\right] \tag{5.2.4}$$

where ΔN_e and ΔN_h are the carrier densities of the electrons and holes respectively.

The current remains low as it would with reverse bias of a diode, and the response can be modelled as

$$\phi(\mathrm{V}) = \alpha\left[1 - \exp\left(-\beta \mathrm{V}\right)\right] \tag{5.2.5}$$

where α and β are device dependent parameters that will vary due to doping profiles and

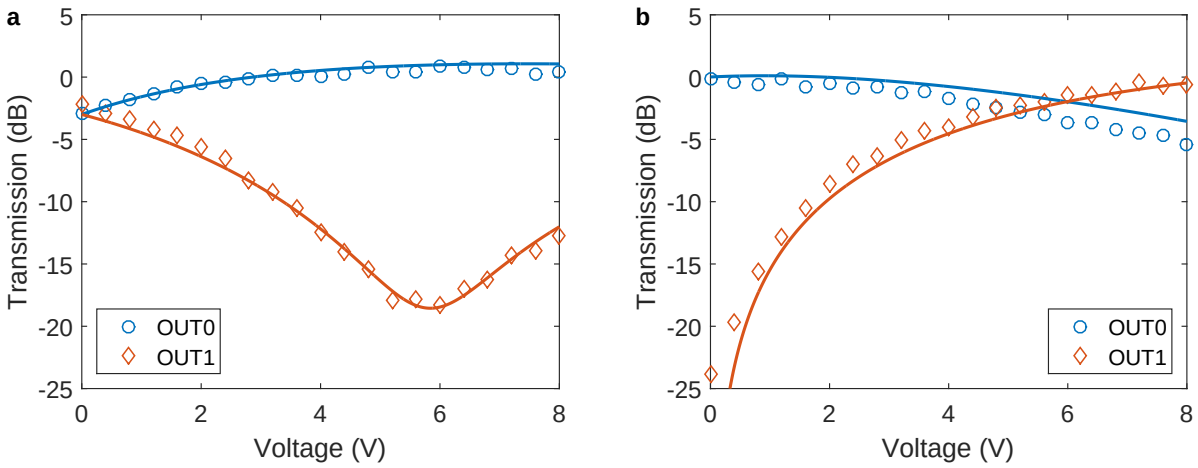

Figure 5.5: **Carrier-Depletion Phase Modulation:** (a) Normalised transmission in dB showing ∼20 dB extinction with initial biasing of $\pi/2$ phase set by the thermo-optic phase modulator. (b) Normalised transmission in dB showing ∼25 dB extinction with initial biasing of 0 phase set by the thermo-optic phase modulator.

device geometry. There is also a phase dependent loss limiting the operating conditions achievable. The change in transmission $\Delta\gamma$ can be described as

$$\Delta\gamma(\mathrm{V}) = \gamma_0 \left[1 - \exp\left(-\beta \mathrm{V}\right)\right] + 1 \tag{5.2.6}$$

where γ_0 will also depend on the doping profiles and device geometry.

These relationships illustrate that the achievable phase will tend towards α as V increases at a rate determined by β. For a given doping profile and waveguide geometry this saturation value will vary dependent on the length of the device, with longer lengths inducing a greater phase. The disadvantage to increasing the length is the increase in overall loss it will incur, and the decrease in the modulation speeds achievable.

Figure 5.5 illustrates data taken from the two outputs of an MZI biased with an ideal thermo-optic phase shifter to $\pi/2$ (Figure 5.5 (a)) and 0 (Figure 5.5 (b)). The model fit taken from Figure 5.5 (a) is applied to Figure 5.5 (b) showing good agreement under different biasing conditions

As displayed in Figure 5.6, for a 1.5 mm device length α=1.1686π, therefore limiting the achievable phase, and β=0.0933 illustrating that $\pi/2$ would be reached at ∼5 V. The change in transmission provides a fit for γ_0=0.5567, limiting the change in amplitude from

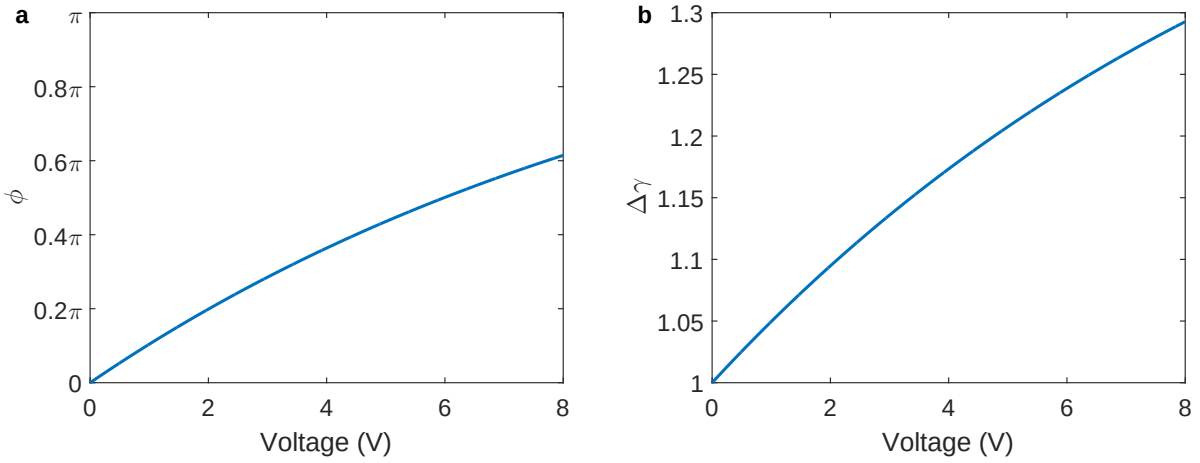

Figure 5.6: **Carrier-Depletion Phase Modulation Fit:** The fitted parameters from Figure 5.5 (a) The fitted phase relationship showing $\pi/2$ achievable with ∼5 V. (b) The change in transmission against voltage, showing a change in amplitude from 1 to ∼1.2 by 5 V.

1 to ∼1.2 by 5 V. The absolute loss was expected to be ∼5 dB for the 1.5 mm structure, or ∼30 dB/cm.

RF

The devices inside an MZI can further be tested at high-speeds. The estimate -3 dB bandwidth of the devices changes with biasing conditions, but was quoted as ∼10-15 GHz. Figure 5.7 (a) illustrates the use of these carrier depletion for pulse modulation over a range of pulse width. This demonstrates the diminishing extinction achievable for shorter pulse. Figure 5.7 (b) also illustrates less periodic data transmission with consistent pulse shape showing the suitability of this modulator to produce the random data patterns seen in QKD.

Pulse Modulation

Figure 5.1 (a) includes both TOPMs and CDMS inside an Mach-Zehnder interferometer (MZI) used for the pulse modulation of coherent light in QKD. The TOPMs provide a DC offset to minimise one of the MZI output intensities. Small changes in one of the CDMs phases will cause a large change in intensity of this output arm with a high extinction ratio without requiring a full π phase change.

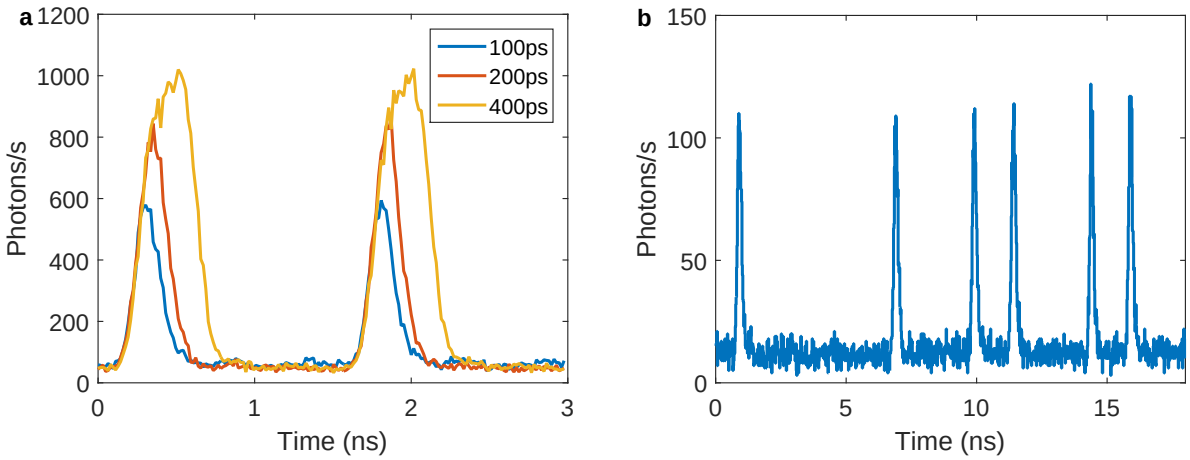

Figure 5.7: **Pulse Modulation with Carrier Depletion Modulators:** (a) Pulses generated at a period of 1.5 ns, with differing pulse widths. Illustrating the decreasing extinction achievable when the pulses shorten. (b) Periodic data generation showing the suitability of the modulator to generate the random data signals required for QKD.

5.3 Path Encoding State Preparation

As discussed in Section 5.2, taking the phase dependent transmission and saturation effects in to account is required when modulating using carrier depletion modulation. One approach to mitigate effects of phase dependent loss and phase saturation was described before in Section 3.2.4 where the π phase shift was induced by opposite but equal phases applied to either side of an MZI.

Another approach is to use the ideal but slow phase modulators to apply a DC offset, and use the non-ideal but fast modulators to apply a small AC value. As illustrated in Figure 5.1 (a), using an MZI with thermo-optic phase shifters on the inside and outside of the interferometer, we can prepare a $|+\mathrm{i}\rangle$ state with almost unit fidelity. Having non-ideal phase modulators on each of the four positions, and shifting by $\pi/2$ would prepare any of the BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. This $\pi/2$ shift therefore limits the requirement of any fast modulation, and would also reduce any of the phase dependent loss, allowing a reasonable preparation of the four BB84 states with non-ideal phase modulators.

Given the model for carrier-depletion modulators described before, the outputs of an

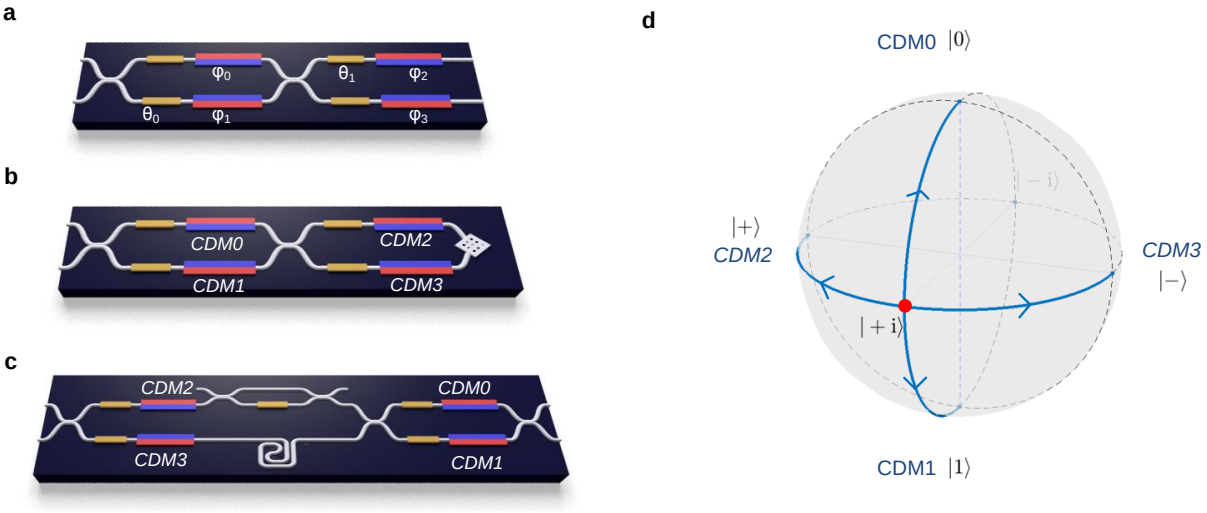

Figure 5.8: **Silicon Photonic State Preparation:** (a) Path Encoded qubit state preparation with an MZI. (b) Polarisation Encoded qubit state preparation with an MZI and 2D grating coupler. (c) Time bin encoded qubit state preparation in an asymmetric MZI. (d) Bloch-sphere representation, illustrating the DC bias condition (red), and the effect of each CDM to prepare the four BB84 states.

MZI is

$$|\psi\rangle = \alpha\Bigg[\gamma_2 \exp\left(\mathrm{i}\left(\phi_2+\theta_1\right)\right)\Big(\gamma_0\exp(\mathrm{i}\phi_0)-\gamma_1\exp\left(\mathrm{i}(\phi_1+\theta_0)\right)\Big)|0\rangle \\ +\mathrm{i}\gamma_3\exp(\mathrm{i}\phi_3)\Big(\gamma_0\exp(\mathrm{i}\phi_0)+\gamma_1\exp\left(\mathrm{i}(\phi_1+\theta_0)\right)\Big)|1\rangle\Bigg] \tag{5.3.1}$$

where ϕ_i and γ_i and the carrier depletion voltage dependent phase and transmission terms, θ_i are the thermo-optic phase shifts, and α is the normalisation term

$$\alpha = \sqrt{\begin{array}{r}\gamma_2^2\left(\gamma_0^2+\gamma_1^2-2\gamma_0\gamma_1\cos(\phi_0-\phi_1-\theta_0)\right) \\ +\gamma_3^2\left(\gamma_0^2+\gamma_1^2+2\gamma_0\gamma_1\cos(\phi_0-\phi_1-\theta_0)\right)\end{array}}^{-1}. \tag{5.3.2}$$

This is set to the DC state

$$|\psi\rangle_{\mathrm{DC}} = |+\mathrm{i}\rangle = \frac{|0\rangle+\mathrm{i}\,|1\rangle}{\sqrt{2}}\,. \tag{5.3.3}$$

Each carrier depletion modulator is then individually driven to provide the four BB84 states (CDM0 provides a $|0\rangle$, CDM1 produces $|1\rangle$, CDM2 produces $|+\rangle$ and CDM3 pro-

duces $|-\rangle$).

To measure the accuracy of the state preparation we can use the fidelity measurement. For two density matrices ρ and σ the fidelity is defined as

$$F(\rho,\sigma) = \mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right] \ . \tag{5.3.4}$$

If one of the states is pure ($\rho = |\phi\rangle\langle\phi|$, $\sqrt{\rho} = |\phi\rangle\langle\phi|$, and $\mathrm{Tr}\left[|\phi\rangle\langle\phi|\right]) = 1$)

$$\begin{aligned} F(\rho,\sigma) &= \mathrm{Tr}\left[\sqrt{|\phi\rangle\langle\phi|\,\sigma\,|\phi\rangle\langle\phi|}\right] \\ &= \sqrt{\langle\phi|\,\sigma\,|\phi\rangle}\mathrm{Tr}\left[\sqrt{|\phi\rangle\langle\phi|}\right] \\ &= \sqrt{\langle\phi|\,\sigma\,|\phi\rangle} \ . \end{aligned} \tag{5.3.5}$$

If the second state is also pure, $\sigma = |\psi\rangle\langle\psi|$, the fidelity is then defined as

$$\begin{aligned} F(\rho,\sigma) &= \sqrt{\langle\phi|\psi\rangle\langle\psi|\phi\rangle} \\ &= |\langle\phi|\psi\rangle| \ . \end{aligned} \tag{5.3.6}$$

Given this model and the parameters fitted to the data, we can extract an expected fidelity of 99.5% for all four states, which would provide a QBER of $\leq$1.1%. This is equivalent to a -19.5 dB extinction ratio between measuring the state $|\psi\rangle_i$ and its orthogonal counterpart $|\bar{\psi}\rangle_i$ e.g. measuring $|1\rangle$ when preparing $|0\rangle$ or measuring $|-\rangle$ when preparing $|1\rangle$.

5.4 Path-to-Polarisation

The MZI can be used to prepare the four BB84 states with a reasonable fidelity, but path encoding has limited applications in communications. Small changes in path length over large distances cause fast varying phase information and decoherence of the states, but if this path encoded state can be converted to polarisation it could be used for free-space communications.

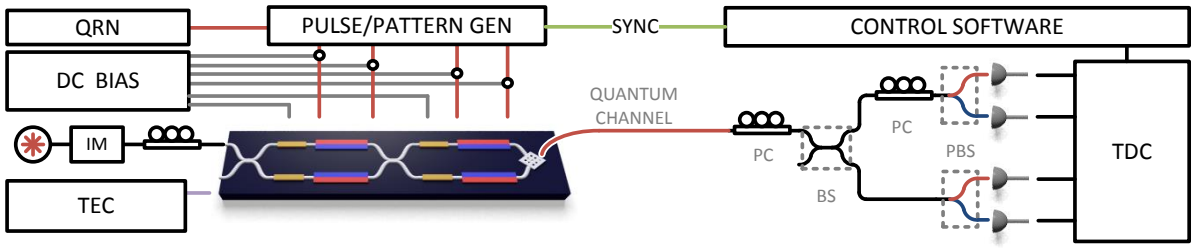

Figure 5.9: **Path-to-Polarisation Circuit:** Path-to-Polarisation QKD transmitter in silicon on insulator photonic device. The chip contains thermo-optic and carrier-depletion modulators to encode path information which is converted to polarisation. This is connected to a fibre based receiver circuit containing polarisaton controller (PC) and polarisation beam splitters (PBS) to set the measurement bases.

5.4.1 TX

Figure 5.9 illustrates such a transmitter, with an pulse modulated (IM) input laser coupled in to silicon photonic chip. The chip contains an MZI for state preparation in path encoding using both ideal, but slow, phase shifters, and non-ideal, but fast, carrier depletion modulators. Quantum random numbers (QRN) are pre-loaded to a pulse/pattern generator to modulate the carrier depletion modulators. DC biases are applied to the thermo-optic phase shifters and to the carrier depletion modulators through bias tees. Finally this path encoded state is combined on a 2D grating coupler that acts as a path to polarisation converter.

2D-grating coupler

The grating coupler is a device use to transmit light from the waveguide to and optical mode outside the chip (either free space, or for fibre coupling). It uses a periodic ridge grating in the waveguide to cause the mode to propagate out of the chip upwards (see Figure 5.10 (a)). By designing the grating in a particular shape a Gaussian shaped single-mode can be produced and coupled efficiently in to an optical fibre [236].

These devices can maintain polarisation of the mode, and therefore, if the mode is TE in the waveguide it can be converted to horizontal out of the waveguide. Since the waveguides in the silicon are polarisation maintaining, if the input light is TE polarised then the two output modes of the MZI described in Section 5.3 will also be TE.

If two waveguides turn to each other with a 90° angle, the output grating coupler

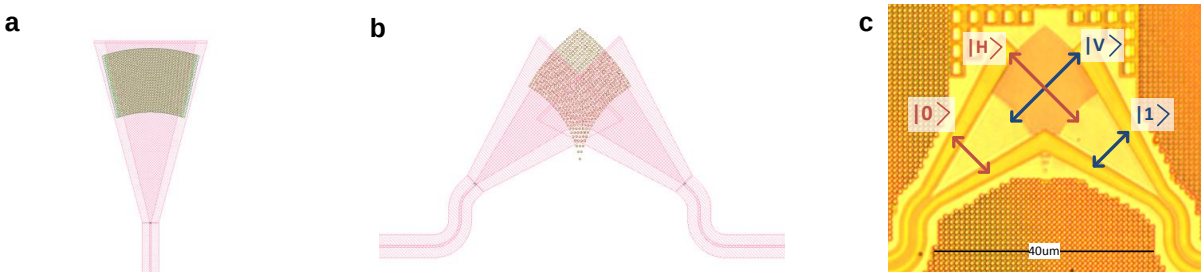

Figure 5.10: **Grating couplers:** (a) A 1-D grating coupler where the waveguide (dark pink waveguide core and light pink waveguide slab) tapers out and the light is allowed to interfere on the periodic grating (brown) causing the mode to be guided upwards out of the chip. (b) A 2-D grating coupler with two waveguides arranged at 90° to each other coming into contact as the waveguides taper out. The periodic grating covers both tapers in order to produce a single free-space mode when converting the path encoded information into polarisation states. (c) A micrograph of our fabricated 2-D grating coupler.

would now be polarised in horizontal and vertical respectively. If the grating couplers overlap spatially, then there is only one spatial mode with a polarisation encoded state equivalent to the path encoded state where $|0\rangle$ converts to $|H\rangle$, $|1\rangle$ converts to $|V\rangle$, and any arbitrary superposition (see Figure 5.10 (b)).

This component has also been demonstrated to distribute entangled states between chips with 98.8% fidelity [237]. It does suffer from a higher loss in comparison to the 1-D grating coupler (∼7 dB in comparison to ∼4.5 dB), but can be used as part of the attenuation required to calibrate the ≤1 average photon per pulse.

5.4.2 Fibre RX

To verify the state preparation a fibre-based receiver, shown in Figure 5.9, was constructed to decode and measure the output polarisation states. It consists of a 50:50 beam splitter (BS) to passively choose the measurement basis, with one arm going to a polarisation beam-splitter (PBS) to measure $|H\rangle$ and $|V\rangle$, and one arm going to a polarisation beam-splitter to measure $|D\rangle$ and $|A\rangle$. A polarisation controller (PC) is used to undo the polarisation rotation of the fibre, and then a PC in each arm is used to set the measurement basis. The outputs are coupled to single photon detectors and a time-to-digital converter is used to collect the data.

We initially calibrated the device by using the inner TOPMs to bias the MZI such that

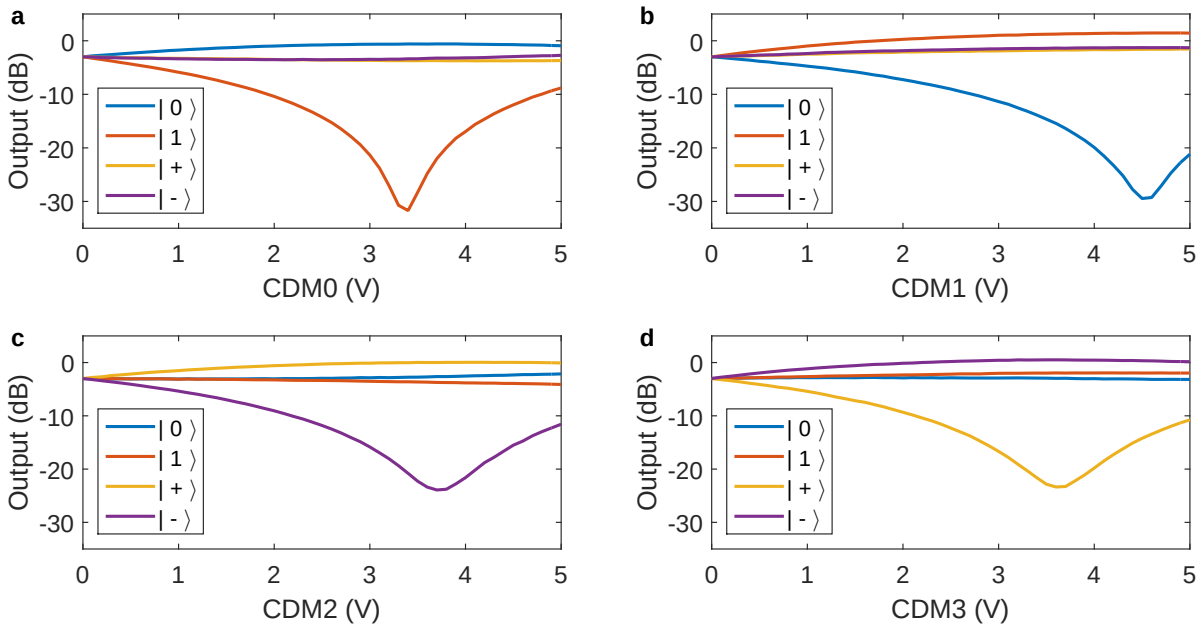

Figure 5.11: **DC parameter sweep for the four polarisation BB84 states:** Preparing the (a) $|0\rangle$ state with CDM0 at 3.3 V, (b) $|1\rangle$ state with CDM1 at 4.5 V, (c) $|+\rangle$ state with CDM2 at 3.9 V, and (d) $|-\rangle$ state with CDM3 at 3.8 V, all for optimal QBER.

equal intensities were observed in each arm through measuring the outputs via taps (not shown) added to the integrated circuit. The inside CDMs of the MZI were then swept with DC voltages to find the voltages required to produce the states $|0\rangle$ and $|1\rangle$. These states were then sent through the receiver circuit to align the first basis $\{|0\rangle, |1\rangle\}$. The second basis was then aligned by first using the polarisation controller to ensure an equal probability of counts in either arm for these two states. This was followed by returning to the DC offset and tuning the TOPMs outside the MZI until the results were also equal over the first and second basis, thus producing the DC state of $|+i\rangle$. Following this step, DC sweeps were taken for the final two CDMs outside the MZI to find the voltage offsets required to produce the states $|+\rangle$ and $|-\rangle$. Figure 5.11 shows the final DC sweeps taken to verify the correct state preparation and the final modulation parameters required.

In order to verify that we are able to produce realistic data with our device, we took data by generating a random sequence of states. Figure 5.12 (a) shows the ideal probabilities of preparation and measurement one would expect, and Figure 5.12 (b) shows data taken from the experiment using the TOPMs to apply the DC offset and the CDMs for state encoding. As one can see, the data shows good agreement with ideal

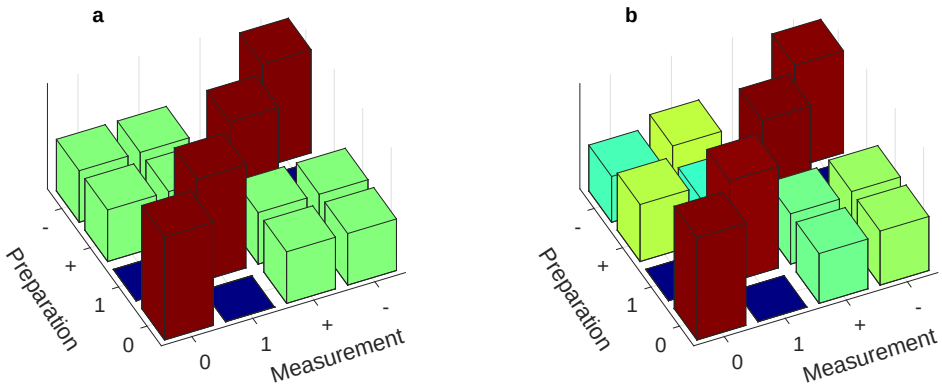

Figure 5.12: **Polarisation state preparation:** (a) Theoretical measurement probabilities for each of the four BB84 states, where the prepared state is indicated by the left axis and probability of a measured state is indicated on the right axes. (b) Measured probability data from the system showing good agreement with the ideal model.

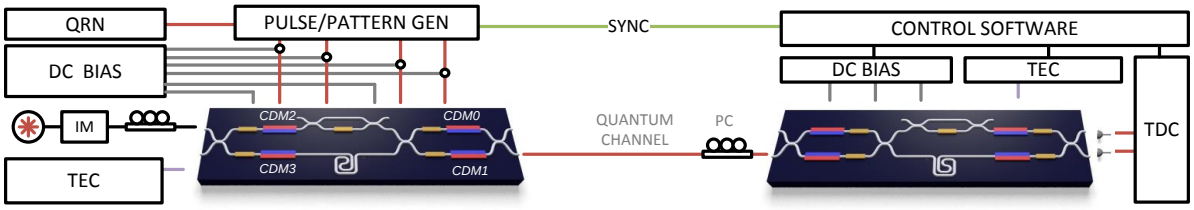

Figure 5.13: **Time-bin Circuit:** Time-bin encoded QKD transmitter in silicon on IMEC chip. The chip contains thermo-optic and carrier-depletion modulators to encode time bin information with an AMZI. This is connected to a second AMZI receiver circuit to passively set the measurement bases. The temperature controlled for phase stability.

theoretical probabilities and produces an average QBER of 1.1%. This demonstrates the suitability of the techniques and components described above for QKD, as it is well below the QBER threshold calculated from the security proofs discussed below.

5.5 Time-bin Encoding

Polarisation encoded systems are commonly used in free-space links, but in fibre-based communications polarisation will often rotate out of alignment. Time-bin encoding is a much more suitable degree of freedom to encode with, and the same approach for state preparation can be applied to this encoding scheme.

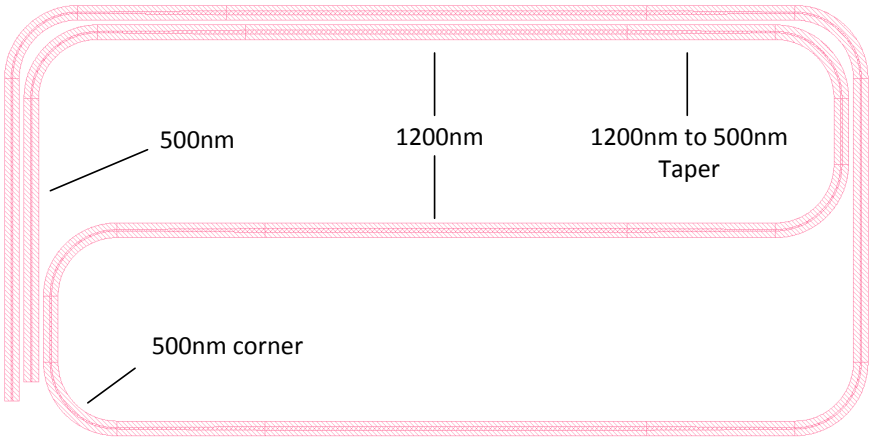

Figure 5.14: **Low Loss Delay Line:** fabricated using 1200 nm waveguide for low loss straight sections, adiabatically tapering to single mode 500 nm waveguides to turn the corners.

5.5.1 TX

A schematic of the experimental setup including the integrated Si time-bin transmitter and an identical copy of the Si chip used as a receiver is shown in Figure 5.13. It begins with an input laser first intensity modulated (IM) to produce pulses before being coupled into the silicon photonic transmitter chip. The chip contains an AMZI for state preparation in time-bin encoding using both ideal, but slow, phase shifters, and non-ideal, but fast, carrier depletion modulators.

The circuit consists of an AMZI with a 1.5 ns delay line, which includes a MZI with TOPMs in the opposite arm to apply a DC loss balancing condition to balance the extra loss experienced in the delay line. The inside of the AMZI includes CDM2 and CDM3 and TOPMs to control the relative phase between the two separate pulses. The final beam splitter of the AMZI is replaced with a further MZI which allows us to select the first or second time-bin to output to a single output fibre. Quantum random numbers (QRN) are again pre-loaded into a pattern generator to modulate the CDMs. DC biases are applied to the TOPMs and the CDMs through bias tees.

Delay Line

The propagation loss inside the delay lines can be prohibiting for time bin operation with integrated photonics. In silicon-on-insulator photonics a standard single-photon waveguide can incur a propagation loss of 2.5 dB/cm, with a group index of 4.18. Since we are interested in the temporal delay we can measure the loss as 17.93 dB/ns . To decrease this loss we can use wider waveguides, changing the width from 500 nm to 1.2 μm, which in turn changes the loss to 0.5 dB/cm and a group index of 3.79. This is a loss of 3.95 dB/ns, which can dramatically reduce the overall propagation loss of the device.

The wider waveguides are no longer single mode and have the ability to support higher order modes. To ensure these modes are not excited there must be an adiabatic taper between the single mode and wider waveguides, and that the wider waveguides are only used in straight sections. To conserve costly real-estate space on the photonic designs, spiral sections are used for longer delays, but to introduce lower-loss and straight wide-waveguide sections we must taper in and out to thinner single-mode waveguides to turn the corner where higher-order modes cannot be excited.

A design can be optimised given the delay required and the usable space by minimising the number of turns used and maximising the number of a straight low loss sections to be incorporated.

5.5.2 RX

The receiver circuit consists of a matched AMZI with which we can passively select the measurement basis. As illustrated in Figure 5.13, this was achieved using a second copy of the transmitter chip. This is lossier than using a dedicated receiver design, for example one that does not include the CDMs which have a certain inherent loss, but was sufficient to verify the state preparation and measurement operation. The CDMs were left at a bias of 0 V while the TOPM in the MZI was biased so as to balance the loss of the delay line while measuring the output with super-conducting nanowire single photon detectors (SNSPD).

A further issue arises in the temperature control of the two chips. The phase informa-

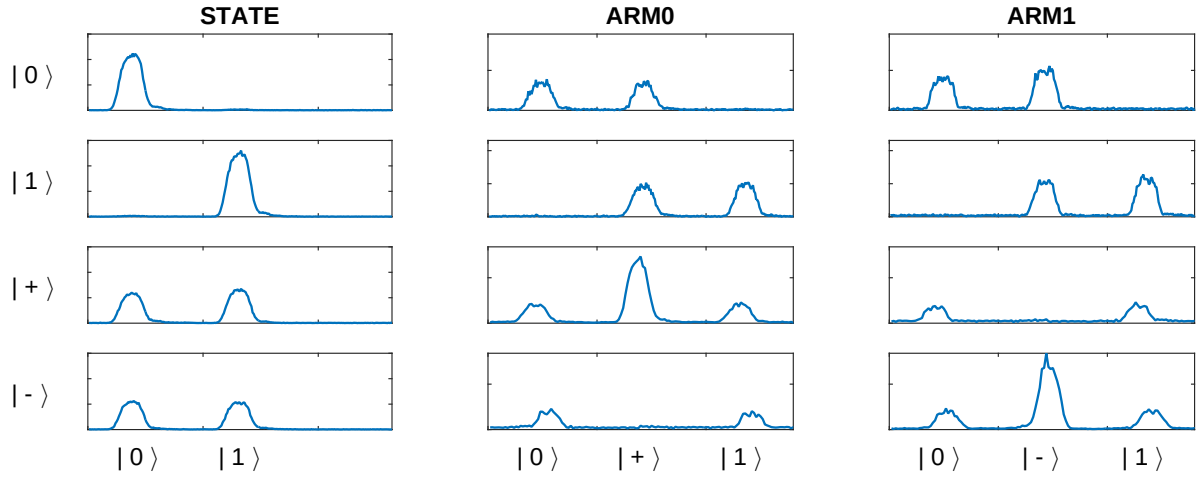

Figure 5.15: **BB84 Time Bin States:** The direct measurements of the four BB84 states, and the measurement outputs of the two arms of the receiver AMZI. Measurement in the first time window of either output represents a $|0\rangle$, a measurement in the final window is $|1\rangle$ and measurements in the second window interferes the phase between the first and second time bin and represents a $|+\rangle$ measurement in ARM0 and $|-\rangle$ measurement in ARM1.

tion between time-bins is sensitive to the difference in optical path lengths between the short and long arm of the AMZI. This is turn is dependent on the temperature dependent refractive index of the silicon which quickly adds up in the 1.5 ns delay introduced in this design. In comparison to the silicon oxynitride (SiO_xN_y) receiver of Chapter 3, where a temperature difference of $\sim 0.6°$ was required for a 2π phase shift in the 600 ps AMZI, our silicon receiver with a 1.5 ns delay can cause 2π fluctuations in $\leq 0.1°$. This meant that a temperature stability of $0.01°$ was required for both independent chips and ultimately was one of the limiting factors of the QBER achievable in this experimental implementation.

Figure 5.15 illustrates a histogram of the state generation before the receiver circuit (left column) and the measurement outcomes when using the receiver and SNSPDs (right columns, ARM0 and ARM1). We use the TOPMs for DC modulation and the CDMs for RF modulation to prepare a preloaded set of data. The results yielded an average QBER of 2.1%.

The major issue limiting the results was the temperature stability of the systems, which could be improved with better insulation. Future versions of this system have already been designed with smaller delays in the AMZI which will decrease the temperature dependence significantly so that a better error rate can be achieved.

5.6 Protocols

5.6.1 Non-Decoy BB84

The BB84 QKD protocol [42] transmits one of four quantum states, consisting of two orthogonal states in two non-orthogonal bases. In a time-bin encoding this can be achieved through $|0\rangle$ encoded by a photon in the first time-bin $|0\rangle_t |\alpha\rangle_{t-\tau}$, $|1\rangle$ encoded by a photon in the second time-bin $|\alpha\rangle_t |0\rangle_{t-\tau}$, $|+\rangle$ encoded by a photon in a superposition of being in the first and second time-bin with no relative phase change $\left|\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$ or $\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|-\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$, and $|-\rangle$ encoded by a photon in a superposition of being in the first and second time-bin with a π relative phase change $\left|\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|-\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$ or $\left|-\frac{\alpha}{\sqrt{2}}\right\rangle_t \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{t-\tau}$. The four states are illustrated in Figure 5.15.

When detecting the photons (using the receiver chip shown in Figure 5.13) the four possible BB84 states enter the AMZI, which overlaps successive time-bins to allow phase information to interfere, creating three possible time-bins within which to detect photons. Measurement of a photon in the first or third time-bin in either detector constitutes a measurement in the $\{|0\rangle, |1\rangle\}$ basis with the first time-bin indicating a $|0\rangle$ and the third time-bin indicating a $|1\rangle$; whereas, measurement in the second time bin constitutes a measurement in the $\{|+\rangle, |-\rangle\}$ basis with the top detector indicating a $|+\rangle$ and the bottom detector indicating a $|-\rangle$. This design allows Bob to use a passive optical detection circuit, once the appropriate phases are set on the TOPM's, removing the need for high-speed quantum random numbers and an active basis selection in the receiver.

The successive states are not currently phase randomised and our circuit did not include another intensity modulator that is be required for the use of decoy states [62]. We therefore use a security proof [93] providing security against general attacks in the case of non-phase-random, non-decoy state BB84, with the key rate given by

$$K_{\mathrm{BB84}} = R_{\mathrm{s}} \left\{1 - f_{\mathrm{EC}}(\epsilon) h(\epsilon) - h(\epsilon_{\mathrm{ph}})\right\} \tag{5.6.1}$$

where $R_{\mathrm{s}} = qR_{\mathrm{t}}$ is the sifted raw key rate, which in the standard BB84 protocol has a sifting factor $q = \frac{1}{2}$ compared to the total counts per second (R_{t}). Here ϵ is the observed

quantum bit error rate, $f_{\mathrm{EC}}(\epsilon) \geq 1$ is the error correction inefficiency used to perform key reconciliation, and $h(\epsilon) = -\epsilon \log_2(\epsilon) - (1-\epsilon)\log_2(1-\epsilon)$ is the binary Shannon entropy. The term ϵ_{ph} is a function of ϵ given by

$$\epsilon_{\mathrm{ph}} = \epsilon + 4\Delta'(1-\Delta')(1-2\epsilon) + 4(1-2\Delta')\sqrt{\Delta'(1-\Delta')\epsilon(1-\epsilon)} \tag{5.6.2}$$

where

$$\Delta' = \frac{\Delta}{Q} = \frac{1}{2Q}\left\{1 - \mathrm{e}^{-\frac{\mu}{2}}\left[\cos\left(\frac{\mu}{2}\right) + \sin\left(\frac{\mu}{2}\right)\right]\right\} \tag{5.6.3}$$

Q is the gain, and μ is the mean photon number for the pulses.

To improve upon these rates and distances achievable, we could further implement decoy intensity levels using an extra intensity modulator and phase randomise the source. This would allow us to follow security proofs such as Ref. [62]. Also, we could bias the basis choice to increase the successful sifting rate according to Ref. [92].

5.6.2 COW

As in Section 5.9 we estimated the secure key rate using

$$K_{\mathrm{COW}} = R\left\{1 - I_E^{\mathrm{COW}}(\mu) - f_{\mathrm{EC}}(\epsilon)h(\epsilon)\right\} \tag{5.6.4}$$

where R is the receiver raw key rate per second, and again $f_{\mathrm{EC}}(\epsilon)$ is the error correction efficiency (which we set to $f_{\mathrm{EC}}(\epsilon) = 1.2$ based on literature estimates), $h(\epsilon)$ is the binary Shannon entropy. We calculate the remaining quantities as

$$I_E^{\mathrm{COW}}(\mu) = \epsilon + (1-\epsilon)h\left(\frac{1 + F_V(\mu)}{2}\right) \tag{5.6.5}$$

where ϵ is the QBER, and $F_V(\mu)$ is given by

$$F_V(\mu) = (2V-1)\mathrm{e}^{-\mu} - \xi\sqrt{1 - \mathrm{e}^{-2\mu}}\ . \tag{5.6.6}$$

This yields a positive key rate when $\mathrm{e}^{-\mu} > \xi \equiv 2\sqrt{V(1-V)}$, where V is the measured visibility.

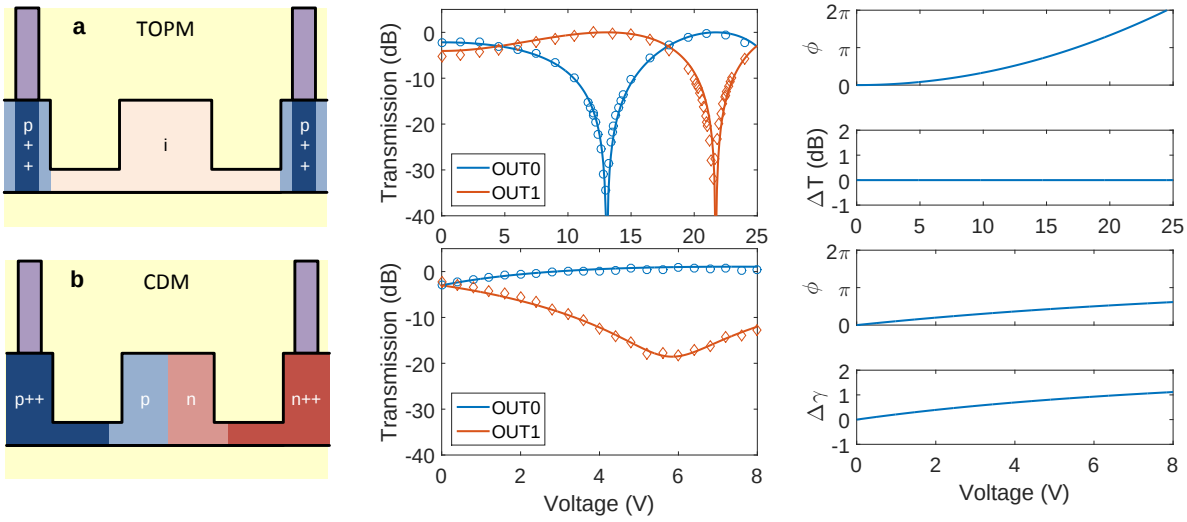

Figure 5.16: **Thermo-optic and Carrier-depletion Phase Modulation in Silicon Photonics:** fabricated with standard doping processes [238]. (a) Cross-section of the thermo-optic phase modulation waveguide with p++ doping in the waveguide slab and intrinsic (i) silicon waveguide core, followed by the power measured at the two outputs of an MZI, the fitted quadratic phase (ϕ) relationship, and the change in transmission (ΔT) as a function of the applied voltage (V). (b) Cross-section of the carrier depletion phase modulator with p and n doping in the waveguide core, followed by the power measured at the two outputs of an MZI (with an additional TOPM providing a $\pi/2$ offset or initially equal intensity outputs), the fitted phase (ϕ) relationship illustrating saturation, and the change in transmission (ΔT) as a function of the applied voltage (V).

5.7 Results

Figure 5.17 illustrates the results from our three implementations of high-speed low-error QKD with integrated silicon photonics. Figure 5.17 (a) shows the raw and secret key rates, and the QBER from the system performing the COW QKD protocol. Here, pulse modulation provides 175 ps FWHM pulses with a high ~25 dB extinction ratio between bright and empty pulses. The system operates with a 1.72 GHz clock-rate with a QBER of 1.01% and estimated asymptotic secure key rate of 916 kbps over a 20 km fibre, following the upper-bound security proof against collective attacks of Branciard *et al.* [59].

For the polarisation and time-bin BB84 QKD protocols, we model and fit the data from our TOPMs and CDMs in Figure 5.16 (a) and (b), resulting in an expected state preparation fidelity of 99.5%, which yields an expected QBER of $\leq$1.1%. This is equivalent to a 19.5 dB extinction ratio between measuring the state $|\psi\rangle_i$ and its orthogonal counterpart $|\bar{\psi}\rangle_i$ (e.g. measuring $|1\rangle$ when preparing $|0\rangle$ or measuring $|-\rangle$ when preparing

$|+\rangle$).

Figure 5.17 (b) shows the measured raw and secret key rates as well as the QBER from operating the transmitter for polarisation encoding and using the passive fibre-based receiver detection scheme described. We measure a low QBER of 1.1% while the transmitter is operated with a 1 GHz clock-rate which yields an estimated asymptotic secure key rate of 329 kbps over a 20 km fibre using a non-phase randomised weak coherent BB84 security proof without decoy states against general attacks [93]. The rate and maximum secure distance could be increased drastically with the addition of an extra integrated intensity modulator to produce decoy states [62].

Finally, measurements of the time-bin encoded states, using a second identical chip as the receiver circuit as described above, are shown in Figure 5.17 (c). Analysing these measurements, we observe a low QBER of ∼2.1% for this proof-of-principle demonstration of time-bin encoded BB84 state preparation. Future systems will benefit from a dedicated low-loss silicon receiver circuit by minimising the fibre-to-chip coupling loss (currently ∼-4.5 dB), removing the *p*-*n* carrier depletion modulators (∼-5 dB each) as well as reducing the loss incurred in the on-chip delay, e.g. reducing the 1.5 ns delay used here to the 600 ps used in COW would increase transmission by >3 dB.

5.8 Summary

In conclusion, this work experimentally demonstrates the feasibility of high-speed QKD transmitters in CMOS-based silicon photonic integrated circuits. In particular, we show an approach to overcome the problems of high-fidelity state preparation when using non-ideal fast modulation in standard silicon photonic fabrication. Using a combination of slow, but ideal TOPMs alongside high-bandwidth (∼10 GHz), but non-ideal CDMs we demonstrate QKD state preparation and pulse modulation. We show three successful implementations: time-bin encoded BB84 state preparation and measurement, polarisation encoded BB84 (1 GHz clock-rate, 1.1% QBER, 329 kbps estimated asymptotic secret key rate), and pulse modulation for COW QKD (1.72 GHz clock-rate, 1.01% QBER, 916 kbps estimated asymptotic secure key rate) over a 20 km fibre link.

Future generations of silicon based chips will benefit from the recent developments of

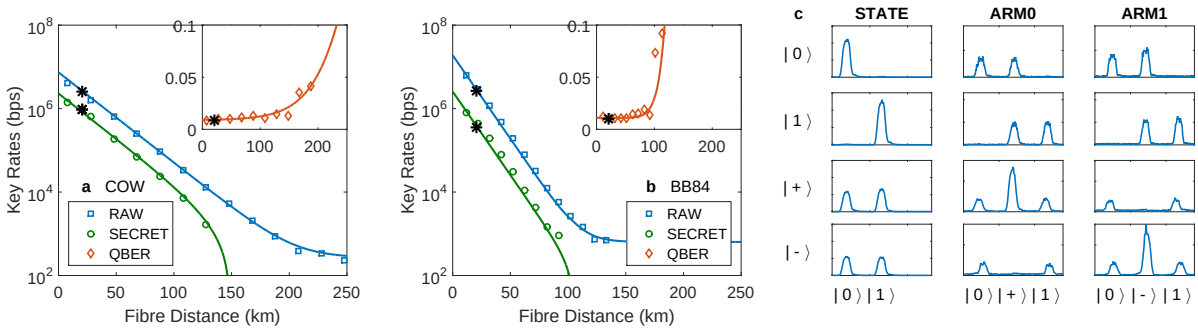

Figure 5.17: **Estimated Secret Key Rates:** The main data sets (squares, circles, and diamonds) were collected by emulating a quantum channel with the use of a variable optical attenuator and assuming standard fibre losses; however, the data shown with asterisks was collected using a 20 km fibre spool as the quantum channel. (a) Raw and secure key rates using the chip to implement the COW QKD protocol, as illustrated in Figure 5.1 (a). The system operates with a 1.72 GHz clock-rate with a QBER of 1.01% and estimated secure key rate of 916 kbps over a 20 km fibre. (b) Raw and secure key rates using the chip to produce polarisation encoded BB84 states, as illustrated in Figure 5.1 (b). We measure a low QBER of 1.1% while the transmitter is operated with a 1 GHz clock-rate which yields an estimated secure key rate of 329 kbps over a 20 km. **(c)** Histogram measurements of the time-bin encoded BB84 state preparation and measurement, as illustrated in Figure 5.1 (c).

low-loss couplers [194], low-loss delay lines [239], integrated laser sources [240], and integrated single photon detectors [171], allowing high-performing monolithically integrated transmitter and receiver devices. Performance could be further improved by introducing additional functionality, such as integrated pulse modulation, intensity modulators for decoy-state [62], and attenuation calibration, and by increasing the rates beyond the 10 GHz bandwidth demonstrated here [231].

Ultimately, integrated silicon photonics will allow the manufacture of quantum communication chips with electronic and photonic processing on a single monolithic device and will enable further multiplexing, complexity and operation with single photon detection. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secured communications.

5.9 Further Developments - Improvements

5.9.1 Future Designs

Future designs have been compiled and sent to fabrication. This includes polarisation and time-bin circuits that contain pulse modulation (as illustrated in Figure 5.18), to limit the need for the external intensity modulation that used in this experiment. This will allow the implementation of BB84 with decoy states to extend the range of the systems. Receiver circuits in silicon have also been designed with the use of lower loss grating couplers (∼2 dB), and thermo-optic phase shifters to allow decoding. Both the transmitters and receiver contain a reduced delay length (∼600 ps) to match the silicon oxynitride receiver circuits and to reduce the temperature stability required for high-speed low-QBER QKD.

Further work would benefit from the integration of single photon detection [228]. There has been many demonstrations of superconducting single photon detector integration with photonic platforms including high efficiency results in silicon [227]. Si-Ge single photon avalanche photodiodes are also a promising technology with the possibility of integration, without the need for cryogenic temperature [210].

5.9.2 1310 nm Operation alongside Classical Data

Integration with classical communication systems is a requirement for QKD, and occupation in fibres alongside classical data transmission has been demonstrated in a number of systems [241, 242]. One common method is through wavelength-division-multiplexing, but requires high levels of filtering to remove the bright data signals, and the background noise this creates from processes such as Raman scattering

Silicon devices could offer this high wavelength filtering through concatenated ring resonator structures or other filtering devices [243]. Further to this operation in the 1310 nm telecommunications band would also remove the quantum signal from some of the background noise sources. Silicon photonics is also capable of operating in this band with many experimental demonstrations of their use [235].

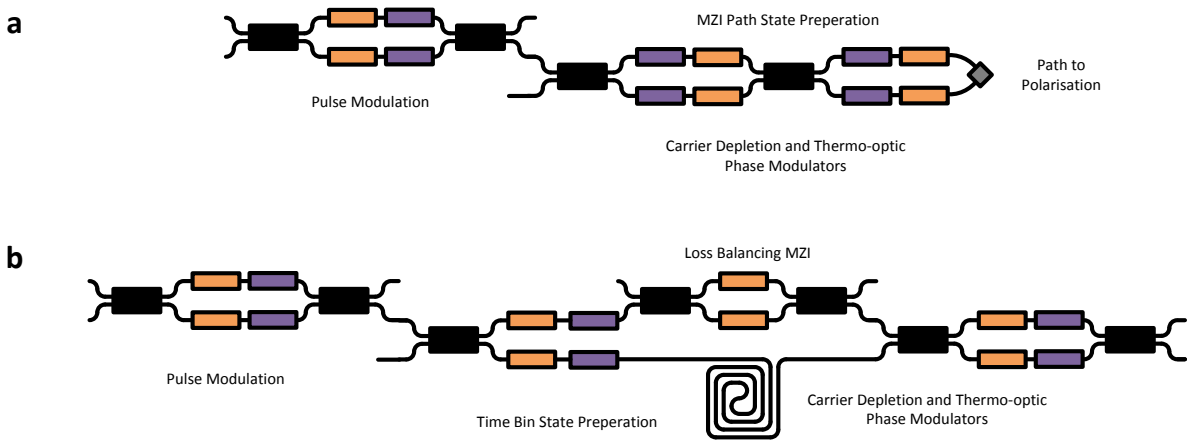

Figure 5.18: **Future Silicon QKD Transmitters:** (a) Polarisation encoded transmitter with pulse modulation (b) Time bin encoded transmitter with pulse modulation.

5.9.3 CV QKD

Silicon could also be used not only in discrete variable systems, as has been demonstrated in the Chapter, but also in CV-QKD schemes (see Section 2.3.2). The demonstration of high speed and efficient silicon germanium photodiodes has been well documented and is now common within silicon photonic platforms [225]. These can be utilised in homodyne detection schemes, alongside the modulators demonstrated in this chapter for transmitters and receivers.

5.9.4 Photon Sources

Finally, this work would benefit from the integration of single photon sources. Lasers have also been demonstrated in a range of integrated platform (such as the InP devices in Chapter 3 and 4), but also hybrid laser structures could provide a suitable technology and have been demonstrated with a number of material systems and designs [244]. Foregoing the development of integrated laser systems, flip-chip boding of laser diodes could also provide a suitable method of manufacturing these technologies, and could also be explored.

Other methods could include light emitting diode structures to generate weak pulses of light, or even the use of silicon's $\chi^{(3)}$ non-linearity for spontaneous parametric four wave mixing which has been demonstrated to create entangled pairs or heralded single photons in the telecommunications band suitable for quantum technologies [226].

Chapter 6

Integrated Quantum Random Number Generation

Statement of Work

This set of experiments were developed along with Dylan Mahler, with the photonic designs translated to fabrication along with Damien Bonneau. The devices were fabricated in a CMOS-based silicon-on-insulator process by IMEC. The devices and electronics were developed by Giacomo Ferranti and Francesco Raffaelli. The data was taken and processed in collaboration with Francesco Raffaelli.

6.1 Introduction

Quantum Key Distribution (QKD) provides a provably secure approach to share keys used to encrypt secret information by transmitting single photons [1]. Integrated photonics provides a stable, compact, miniaturized, and robust platform to implement complex photonic circuits amenable to manufacture and therefore provide a compelling technology to implement future quantum communication systems [10]. In previous chapters we have demonstrated a number of examples of quantum communications with integrated photonic implementations, including chip-to-chip QKD with InP and SiO_xN_y [181], and high-speed silicon transmitters for time-bin and polarisation encoded BB84 . In each implementation we required the use of unbiased random numbers, and in network communication systems these would be required to be high-bandwidth and real-time.

Random numbers are essential in many fields including cryptography [18], fundamental tests of physics [24], coordination in computer networks [245], and scientific simulations [246]. These applications rely on the unpredictability of random numbers, which cannot be guaranteed when using classical techniques. In comparison, quantum mechanical systems can be prepared in a superposition of states, and the outcome of a measurement of this state can be intrinsically random. Therefore, the inherently random nature of quantum measurements can be exploited to generate truly random numbers [247].

QKD and the devices developed in the previous chapters require quantum random numbers to control the bit values, basis values, random phases and decoy intensity levels. For the system described in Chapter 4 we require ∼7 Gbps of unbiased random numbers to properly provide the required biases for decoy state choice and basis selection.

Here we show the use of integrated photonics based quantum random number generators (QRNG). In particular we use weak coherent sources of light generated in InP devices and single photon detectors in a number of configurations to generate 10.5 Mbps and 145 Mbps of unbiased quantum random numbers. We further improve upon this rate and the versatility of the devices by demonstrating an integrated homodyne detector system to generate 1.03 Gbps of quantum random numbers passing a number of statistical random test suites.

We discuss further approaches to increase these rates up to the required amount, and

the possibility of integrating these devices with transmitters to allow single quantum photonics chips to be manufactured. Ultimately, integrated photonics will allow the manufacture of single quantum communications chips with electronic and photonic processing on a monolithic device. This will enable further multiplexing and complexity of operation. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secure communications.

6.2 Quantum Random Number Generator

6.2.1 Random numbers

Random numbers are exploited in many technological fields [248], in applications that rely on the unpredictability of random numbers. Random number generators are often based on pseudo-random number generation algorithms that expand on an initial seed in a deterministic manner [249], suffering from problems of periodicity and long-term correlations that can undermine the security.

The certification on random numbers also poses a problem, with statistical tests used to examine and quantify the outputs of random number generators [250–253]. These methods are still susceptible to false positive results coming from predetermined strings that can pass all the statistical analysis, and therefore true randomness can only be obtained with inherently random processes. In comparison to pseudorandom algorithms, quantum mechanical systems can be prepared in a superposition of states, and the measurement of this state can be intrinsically random. Therefore, the inherently random nature of quantum measurements can be exploited to generate truly random numbers [247].

6.2.2 Single photons

As illustrated in Figure 6.1, a practical quantum random number generator can be made by preparing single photons incident on a beam splitter to create the superposition of $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Single photon detectors can then measure this state to randomly select the 0 or 1 bit values [192, 254].

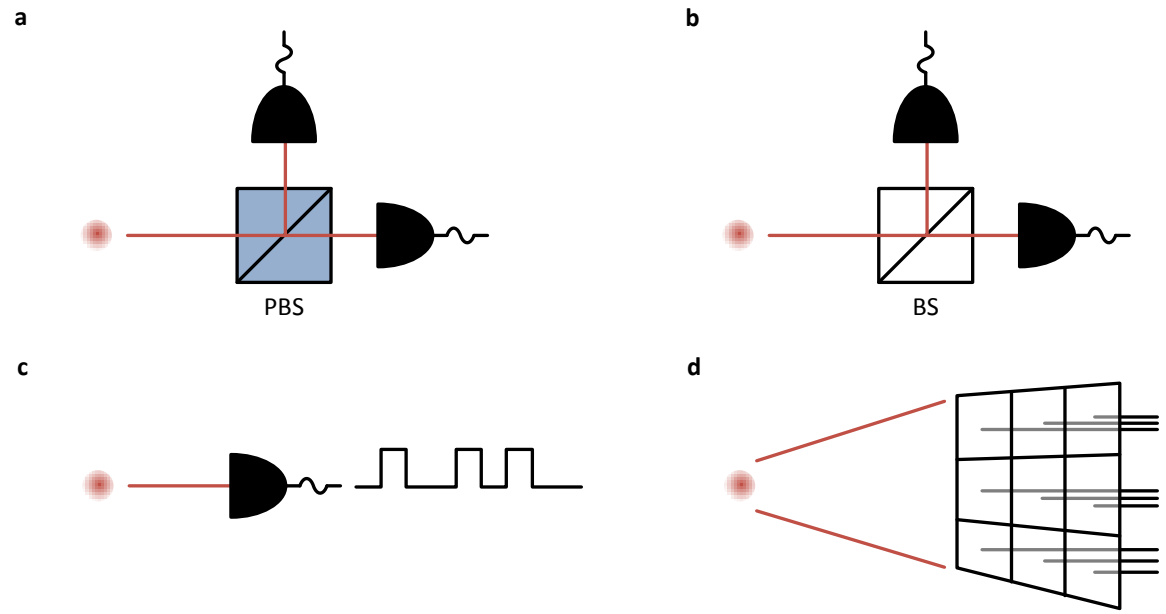

Figure 6.1: **Practical QRNGs based on single photon measurement:** (a) A photon is originally prepared in a superposition of horizontal (H) and vertical (V) polarizations, described by $\frac{|H\rangle+|V\rangle}{\sqrt{2}}$. A polarising beam splitter (PBS) transmits the horizontal and reflects the vertical polarisation. For random bit generation, the photon is measured by two single photon detectors (SPDs). (b) After passing through a symmetric beam splitter (BS), a photon exists in a superposition of transmitted (T) and reflected (R) paths, $\frac{|R\rangle+|T\rangle}{\sqrt{2}}$. A random bit can be generated by measuring the path information of the photon. (c) QRNG based on measurement of photon arrival time. Random bits can be generated, for example, by measuring the time interval, Δt, between two detection events. (d) QRNG based on measurements of photon spatial mode. The generated random number depends on spatial position of the detected photon, which can be read out by an SPD array.

Generally, these QRNGs can generate numbers with reasonably high speed, but in real experiments the quantum effects are mixed with classical noise, which in principle could be known to an adversary. The quantum randomness must therefore be extracted out of the system by modelling the underlying noise sources and appropriate post processing to provide unbiased quantum random numbers (see Section 6.5.2).

The source and measurement equipment used to generate the random numbers must be trusted, but can be generated using any readily manipulated degree of freedom such as spatial [192, 254, 255], temporal [256–259] or photon number [260–262].

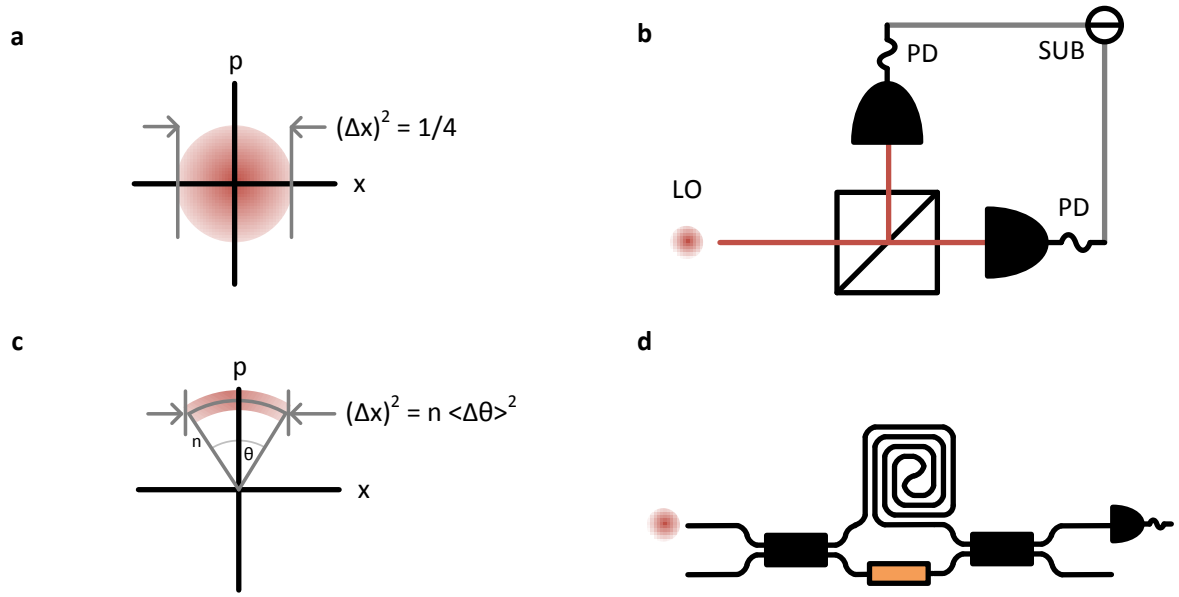

Figure 6.2: **QRNGs using macroscopic photodetectors:** (a) Phase-space representation of the vacuum state. The variance of the X-quadrature is 1/4. (b) QRNG based on vacuum noise measurements. The system comprises a strong local oscillator (LO), a symmetric beam splitter (BS), a pair of photon detector (PD), and an electrical subtracter (SUB). (c) Phase-space representation of a partially phase-randomised coherent state. The variance of the X-quadrature is in the order of $n\,\langle\Delta\theta^2\rangle$, where n is the average photon number and $\langle\Delta\theta^2\rangle$ is the phase noise variance. (d) QRNGs based on measurements of laser phase noise. The first coupler splits the partially phase-randomised laser beam into two beams, which propagate through two optical fibres of different lengths, thereafter interfering at the second coupler. This converts relative phase into intensity measurements and is recorded by a photon detector. The extra length ΔL in one fibre introduces a time delay T_d between the two paths, which in turn determines the variance of the output signal.

6.2.3 Continuous Variables

The limitation of single photon random numbers comes from the cost of single photon detectors and ultimate rates at which the detectors can be operated. To improve upon these rates and cost of implementation, a number of different proposals have surfaced, including amplified vacuum noise with homodyne detectors [263–265] and measuring phase [191,266–270] or intensity noise [271,272] from amplified spontaneous emission, which is quantum mechanical by nature. These techniques have the benefit of using standard telecommunications and classical photonic technologies, and also (ideally) allowing a continuum of random numbers, which can be discretised so that one measurement can

produce a string of random numbers.

6.3 Single Photon QRNG with Integrated Photonics

6.3.1 Beam Splitter based QRNG

The transmitter chip described in Chapter 3 can be used as part of a QRNG. The temporally modulated weak coherent source and an on-chip MZI acting as a beamsplitter were used to randomly split photons to one of two off-chip fibre-coupled superconducting nanowire single photon detectors [192], producing a random stream of zeros and ones (Figure 6.3 (a)). To achieve a fair or appropriately biased coin, the values were fed through a Bernoulli factory [193] to provide coins with the required probability statistics. For example, in the event of a 0 followed by 1 the output of the Bernoulli factory is 0, and if the measurement is 1 followed by 0 the output is 1, and other pairs are discarded. These two outcomes have the same probability, $p(1-p)$, no matter the input bias probability of $\Pr(0) = p$ and $\Pr(1) = 1 - p$ and is most efficient when $p \sim 0.5$.

The average photon number, μ, was set to 0.1 per pulse to limit the probability of multi-photon terms. The detector efficiency was ∼40% with 500 dark counts per second (cps) in each arm. The dead-time of the detectors and the counting logic limited the achievable rates. With the maximum count-rate of around 12 Mcps on each channel, we were able to generate ∼21 Mcps from the of time-tagged data from the two channels (compared to the 45 Mcps achievable at 1 GHz repetition rate if there was no dead-time). With the measured bias of 49.1:50.9, the extraction of unbiased numbers was 49.98% leading to and average count of ∼10.5 Mbps of quantum random numbers.

6.3.2 Time-based QRNG

A second method for generating random numbers with this architecture is to use the timing information of single photons arriving [245, 257]. For example, the preparation of a time-bin superposition qubit $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ with weak coherent light can allow the measurement of one bit per detection. Another example is a Gaussian shaped single photon envelope encoding a continuous quantum variable that can be discretised into equal probability

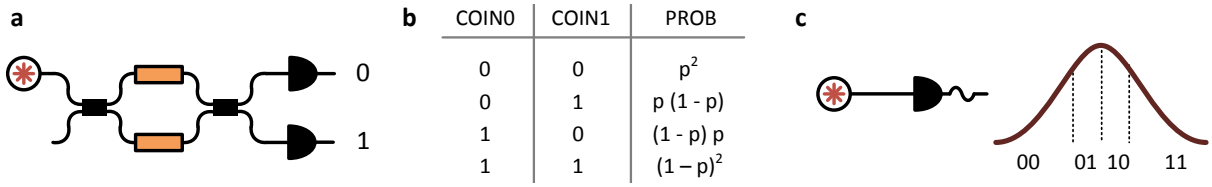

Figure 6.3: **Quantum Random Number Generation:** (a) Schematic of the QRNG comprising the on chip laser and MZI set as a 50:50 beamsplitter incident on two single photon detectors. The output of one detector represents a 0, and the output of the other represents a 1. (b) This random string is put through a Bernoulli factory to ensure equal probability of 0 and 1s. If the string 01 or 10 occurs they will have the same probability no matter the bias. 00 and 11 are discarded. (c) Another approach would be to use the Gaussian shape of an attenuated coherent pulse and the time of arrival of single photon events. This can be discretised in to more bins to get more random numbers per measurement with a single detector.

timing intervals 6.3 (c). The discrete bins allow for more random numbers to be generated per measurement and reduces the number of single photon detectors required.

A similar approach described in [259] generates quantum random numbers based on photon arrival time relative to an external timing reference. With a highly attenuated continuous wave signal from the on-chip laser diode, the time interval between successive detection events can in principle generate n bits, where n is dependent on the time resolution of the measurement. However, the drawback of this scheme is that the Poissonian statistics governing this Δt between detector events follows an exponential-family distribution, which is highly biased and therefore the random bits extracted from the raw data is inefficient.

By applying an external reference, the distribution of temporal difference between a single photon event and the periodic timing signal is approximately uniform. The randomness of this system is derived from the photon arrival time in a given period $(t,t+T)$. With the mean photon number of λT, where λ describes the laser intensity, the photon number (k) follows a Poisson distribution,

$$\Pr(k) = \frac{e^{-\lambda T}(\lambda T)^k}{k!} \ . \tag{6.3.1}$$

The external reference is set to T, and each period $(t,t+T)$ into N smaller bins $\{\tau_1, \tau_2, \ldots, \tau_N\}$, where $\tau_i = (t + \frac{i-1}{N}T, t + \frac{i}{N}T)$. Detecting a photon in a time period $(t,t+T)$, it can be

shown that the photon appears in each smaller time bin τ_i with the same probability of $1/N$. The randomness extraction will be affected by device imperfections, such as multi-photon emission, dark counts, and detector dead time.

To model the system one must include the detector efficiency η, the dead time τ_d, and multi-photon emission events (which will not be distinguished). An upper bound on the highest probability detection event is $p_1 = \Pr(n = 1|k)$ provided by the equation

$$p_1 \leq \frac{\lambda T \eta}{N(1 - e^{-\lambda T \eta})} \ . \tag{6.3.2}$$

This provides a lower bound for the min-entropy (widely used to quantify the randomness of the system discussed further in Section 6.5.1) of the scheme

$$\begin{aligned} H_\infty &= -\log_2(\max_i p_i) \\ &= -\log_2(p_1) \\ &\geq \log_2 N + \log_2(1 - e^{-\lambda T \eta}) - \log_2(\lambda T \eta) \ . \end{aligned} \tag{6.3.3}$$

The laser intensity is chosen to ensure less than one photon detection will happen in each external reference period on average. With a count rate of 12.5 Mcps and time period of 16.4 ns period (61 MHz), this provides a value of $\lambda T \eta$ of 0.2. The 16.4 ns can be split into 4 ps resolution which is 12 bits per period ($N = 2^{12}$), or 150 Mbps of raw data. Overall we calculate a min-entropy of 0.98 random bits per bit of raw data. By applying appropriate randomness extraction techniques (see Section 6.5.2) we can therefore generate ∼145 Mbps of quantum random numbers.

6.4 Integrated Homodyne detectors

6.4.1 Homodyne Detectors

The quantum optical vacuum state can be described by a pair of non-commuting amplitude and phase quadrature operators ($\hat{x}$ and $\hat{p}$ with $[\hat{x}, \hat{p}] = \frac{\mathrm{i}}{2}$), which cannot be measured to arbitrarily high precision simultaneously [273]. This can be explicitly stated

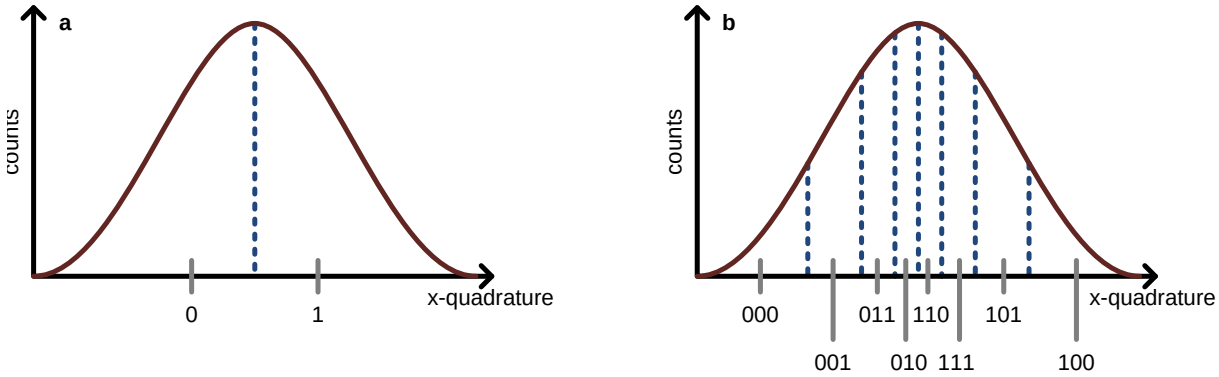

Figure 6.4: **Homodyne Quantum Random Number Generation:** (a) The probability distribution of the vacuum state is discretised into two bins, providing one random bit of equal probability for each measurement outcome. (b) The same probability distribution is binned into 2^n equally probable bins. The random bits are generated by assigning bit combinations of length n to each bin. The example of $n = 3$ is illustrated above.

as $\langle(\Delta\hat{x})^2\rangle \langle(\Delta\hat{p})^2\rangle \geq \frac{1}{16}$ where $\Delta\hat{x} = \hat{x} - \langle\hat{x}\rangle$, with $\langle\hat{x}\rangle$ being the expectation value of $\hat{x}$. This is illustrated in Figure 6.4 (a), where the vacuum state is represented by a two-dimensional Gaussian distribution centred at the origin with uncertainty of $\frac{1}{4}$ (the shot-noise variance). The random numbers can be generated by measuring this Gaussian distribution, and can be physically measured by sending a strong laser (local oscillator) through a symmetric beam splitter and detecting the differential signal of two outputs with balanced photo-receivers [274] (Figure 6.4 (b)).

The vacuum state can be written in the quadrature representation as

$$|0\rangle = \int_{-\infty}^{\infty} \psi(x) \, |x\rangle \, dx \tag{6.4.1}$$

where $\psi(x)$ is a Gaussian function, with mean $x = 0$, describing the ground-state wavefunction. Here $|x\rangle$ are the eigenstates of the amplitude quadrature, such that

$$\langle x|x'\rangle = \delta(x - x') \; . \tag{6.4.2}$$

A measurement of this state will cause the unpredictable collapse of the wavefunction in to one of the quadrature eigenstates, the outcome of which is weighted by the Gaussian probability distribution ($|\psi(x)|^2$). The measurements are discretised such that the

probability of each discrete outcomes are equal, i.e.

$$\int_{-\infty}^{x_1} |\psi(x)|^2 \, dx = \int_{x_1}^{x_2} |\psi(x)|^2 \, dx = \cdots = \int_{x_l}^{\infty} |\psi(x)|^2 \, dx \ . \tag{6.4.3}$$

This quadrature measurement is performed by interfering the vacuum state with a strong local oscillator on a beam splitter, where the two outputs are measured in intensity by photodiodes which must be well balanced. The subtracted difference between the two detector signals is proportional to the quadrature amplitudes of the vacuum state [274].

This approach uses the quantum random resource of the vacuum state, which can be prepared with high fidelity, and loss can be compensated by increasing the LO power. Finally the field quadrature is a continuous variable, and in principle more than one random bit can be generated from one sample.

In a physical system, there will be additional noise that could be potentially observed or controlled by an adversary. To efficiently extract quantum randomness, the detectors system should be operated in the shot-noise limited region, and the dominant noise should by generated from the vacuum. Shot-noise limited homodyne detectors have been demonstrated, but are often limited to a few hundred MHz, which could limit the operating speed [275–277].

6.4.2 Characterisation

The homodyne detector was designed for a silicon-on-insulator technology platform that can fabricate waveguides and MMI devices to create the symmetric beam splitter required. Light is coupled in to the device through broadband grating couplers with an estimated 4.5 dB of loss, and the detectors are fabricated by depositing germanium elements in the silicon waveguides to allow absorption of telecommunications frequency light.

The results are taken using a tunable telecommunications laser (Yenista TUNICS T100) as a stable local oscillator, with the outputs of the detectors going through an electronic circuit, amplifying the differential current of the balanced detectors (Figure 6.5). The voltage output is measured through an oscilloscope (Keysight DSOV134A) where the sample rate and range can be controlled.

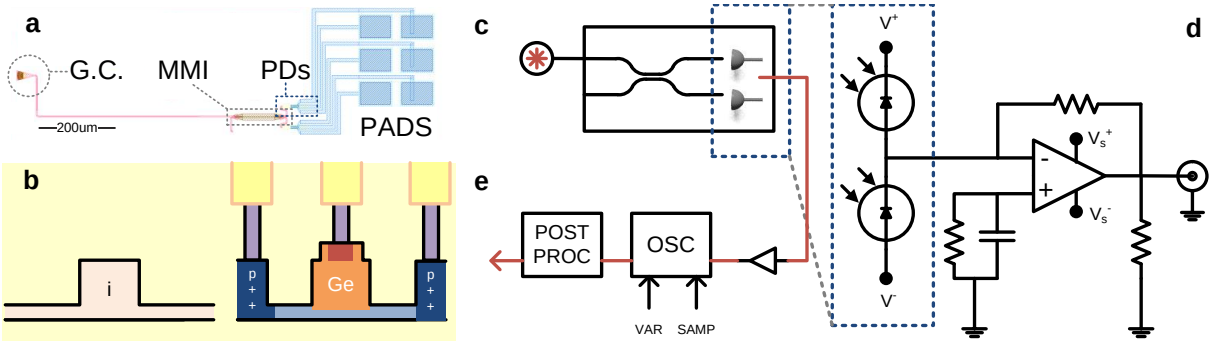

Figure 6.5: **Experimental Homodyne QRNG:** (a) Device mask illustrating the grating coupler (GC) for external laser coupling, the MMI acting as a 50:50 beamsplitter and two photodiodes (PDs). (b) Schematic cross section of silicon germanium photodiode compared to intrinsic waveguide. (c) Experimental set-up illustrating the chip, external laser source, (d) subtracting photo-current circuitry, and (e) oscilloscope measurements before offline post processing is performed.

The responsivity, dark current, and bandwidth of the detector is crucial to ensure a good signal to noise level. The integrated silicon-germanium detectors are rated to 0.95 A/W with ≤15 nA dark current, based at 1550 nm. The bandwidth is defined by the -3dB frequency of the opto-electric $|S_{12}|^2$ parameter representing the frequency dependent transfer function between the optical input and electrical output in $10\log_{10}$ dB scale and estimated to be ≥10 GHz [238].

As illustrated in Figure 6.5 (e), the difference in photocurrent was amplified with a single stage op-amp (OPA847 Op-Amp 3900 MHz SOT-23). Capacitors, voltage regulators, diodes and resistors were used to appropriately bias and power the photodiodes and amplifier stage, minimising the noise sources.

The 10 bit vertical resolution of the oscilloscope was then used and set to $\sim 3\sigma$ of the measurement, to get a good spread of signal measurements, and high resolution in 99.7% of the possible measurements (Figure 6.6 (a) and (b)). These 10 bit samples can be subsequently binned in to windows of equal probability as described in Section 6.4.1.

As illustrated in Figure 6.6 (c), the -3 dB bandwidth of the homodyne detector estimated at ∼150 MHz, with ∼10 dB between the classical and total noise. The sample rate on the oscilloscope was subsequently set to 125 MHz, and at least 500,000 samples were taken each sweep to get a reasonable statistical measurement of the randomness extracted.

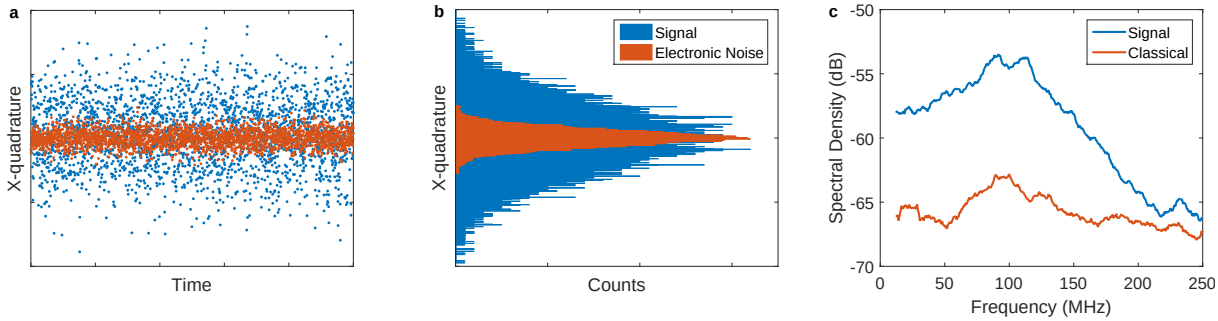

Figure 6.6: **Quantum and Classical Noise measurements:** (a) The measurements of the signal (blue), electronic noise (red) over the quasi-continuous voltage. (b) Resulting histograms of the signal and electronic noise. (c) Bandwidth measurements of the signal and electronic noise.

6.5 Experimental Quantum Random Numbers and Validation

6.5.1 Entropy Measures and Sampling

Entropy provides a measure of the randomness of a system. The total entropy $H(X)_t$ of a bit sequence contains the effects of both quantum ($H(X)_q$) and classical ($H(X)_c$), the classical noise being generated from electronic noise and local oscillator noise due to imperfect MMI splitting ratio and unbalanced detector efficiency. The entropy of the quantum mechanical randomness can be calculated as

$$H(X)_q = H(X)_t - H(X)_c \tag{6.5.1}$$

where

$$H(X)_t = -\sum_{i=1}^{l+1} p_i \log_2 p_i \tag{6.5.2}$$

and p_i is the probability of measuring an outcome in the i^{th} bin of the vacuum state probability distribution.

The classical entropy can be measured as $H(X)_t$ when the local oscillator is switched off. This can provide an entropy estimation, allowing the calculation of the effective number of bits generated from the quantum entropy. For example in Figure 6.7, by varying the number of bins per sample we can demonstrate a convergence to the maximum

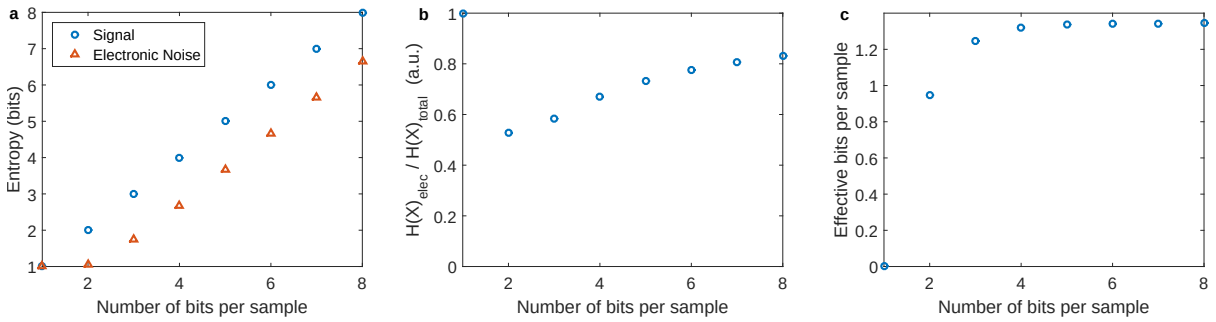

Figure 6.7: **Entropy and Effective Random Bits:** (a) The measured entropy from signal and electronic noise for different number of bits per sample. (b) The ratio of entropy from total and electronic noise. (c) The effective numbers of quantum random bits achieved for different number of bits per sample.

information capacity. The entropy increases linearly for the larger numbers of bits per sample, but by increasing the number of bits per sample the classical noise also increases after a threshold of 2 bits. The ratio of the two sources of noises is minimised for 2 bits, but by calculating the effective numbers of random bits per sample, the value converges towards 1.4 random bits per sample, where the least number of bits per sample is chosen to minimise the requirements of the post-processing hardware.

Min-Entropy

Although the Shannon entropy provides a measure of the channel capacity or the signal to noise of the quantum versus the classical noise, it has been shown that randomness cannot be well quantified by this measure, and that the randomness from non-universal hashing functions relies on computational assumptions [278]. In particular, because the operation of a quantum random number generator is not to recover a specific quantum signal from the background of classical noise, it is sufficient to generate random bits with no correlation to the classical noise [268].

A more suitable approach to evaluate randomness is therefore the min-entropy of a probability distribution X on $\{0,1\}^n$, defined as

$$H_\infty(X) = -\log_2 \left[\max_{\upsilon \in \{0,1\}^n} \Pr(X = \upsilon) \right] . \tag{6.5.3}$$

To model the quantum random number generator we assume the total signal is a mixture

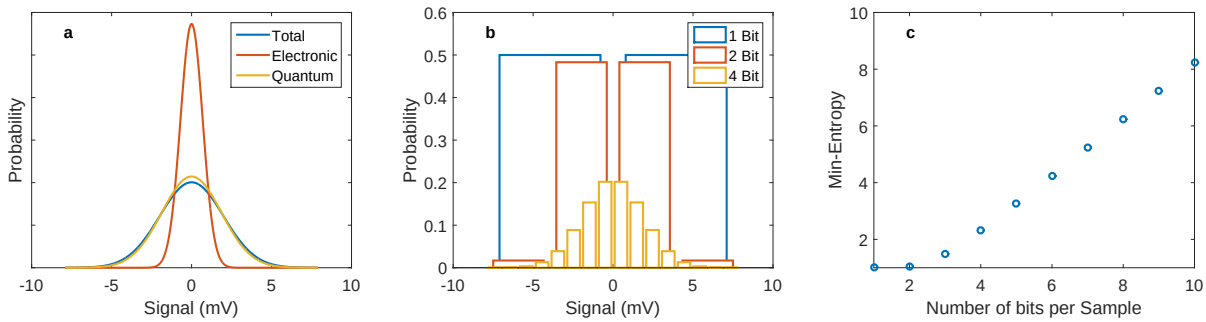

Figure 6.8: **Min-Entropy and Effective Random Bits:** (a) Probability distributions of the total, electronic and quantum signals. (b) probability of Gaussian-shaped quantum signal with equal bin sizes. (c) Min-Entropy of the quantum data against bits per sample.

of independent quantum signal and classical noise. We further note that the quantum signal follows an analogue Gaussian distribution, which is digitised via an analogue-to-digital converter. We can define a ratio between the variances of the quantum and classical signals (γ), and the total signal variance can be estimated and measured (σ_t^2). This last assumption is satisfied when the sequence of raw data is independent and identically distributed, and without the need to assume that the classical noise follows a Gaussian distribution.

The variance of the quantum signal can be described as

$$\sigma_q^2 = \frac{\gamma \sigma_t^2}{1+\gamma} \ . \tag{6.5.4}$$

The analogue signal is sampled by the 10-bit ADC oscilloscope to generate digital bits with a variance $\sigma_t^2 = 3.947$ mV^2 from 20 mW of optical laser power external to the integrated device (as illustrated in Figure 6.6 (a) and (b)). The electronic noise is measured with the laser off with $\sigma_c^2 = 0.4849$ mV^2. These two measurements provide a quantum variance of $\sigma_q^2 = 3.4621$ mV^2, or a $\gamma = 7.1397$, at a sampling rate of 125 MHz. This gives a min-entropy measurement of 8.24 bits per sample at with a 10 bit ADC with equal voltage spacing (Figure 6.8). This therefore generates 1.03 Gbps of quantum random numbers when using appropriate post processing techniques.

6.5.2 Post-processing

To remove the effects of classical noise from the randomness generated (assumed to be known to the adversary) the entropy is smoothed by cryptographic hashing. The amount of quantum mechanical entropy contained in the raw data is known, and therefore there can be an appropriate one-way function to project the raw data on to a shorter set of truly random numbers determined by the measure of entropy. This can be achieved by hashing with well known and optimised implementations such as SHA512, Whirlpool, RipeMD and Trevisan's extractor [15, 278].

We previously estimated a lower bound of the quantum min-entropy of 8.24 bits per sample, which means we should be able to generate 8.24 information-theoretically random bits from each of the 10 bit samples. This must be extracted from the raw data, to both remove the classical noise correlation and generate a uniform distribution from the Gaussian distribution measured. This randomness extraction will be a function of the form

$$\{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m \tag{6.5.5}$$

where a non-perfect input sequence X (a binary string of n bits) with min-entropy $H_\infty(X) \geq m$, and a small input seed of d bits, will allow the extraction of an output sequence Y (a binary string of m bits) of near perfect-randomness and uniform probability.

The Toeplitz hashing extractor is such an information theoretically secure extractor with the ability to take finite-size effects into account [279]. A Toeplitz matrix is a matrix in which each diagonal from left to right is constant, for example the $n \times n$ matrix of the form

$$\begin{bmatrix} a_0 & a_{-1} & a_{-2} & \dots & \dots & a_{-(n-1)} \\ a_1 & a_0 & a_{-1} & \ddots & & \vdots \\ a_2 & a_1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{-1} & a_{-2} \\ \vdots & & \ddots & a_1 & a_0 & a_{-1} \\ a_{n-1} & \dots & \ddots & a_2 & a_1 & a_0 \end{bmatrix} \tag{6.5.6}$$

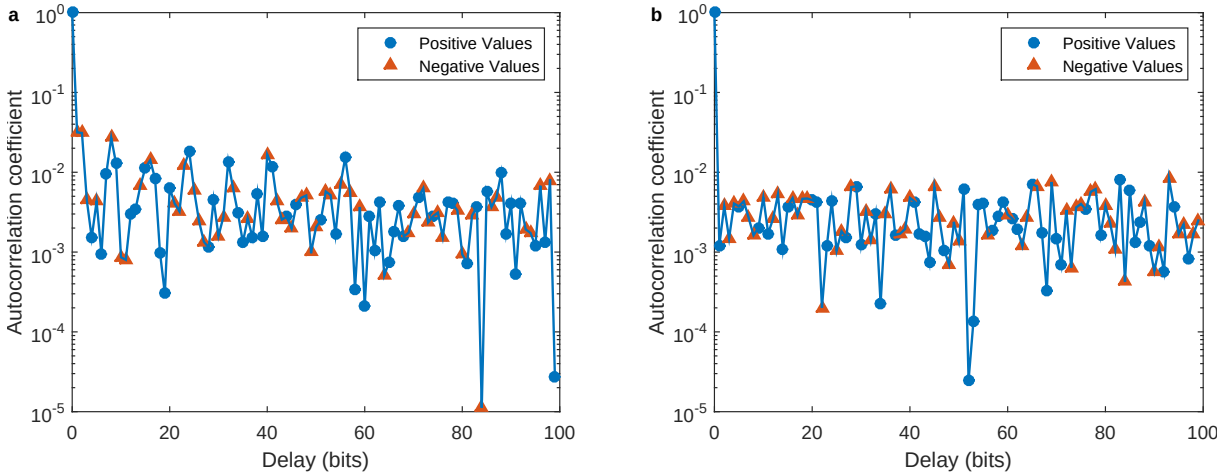

Figure 6.9: **Autocorrelation Evaluation:** (a) Autocorrelation coefficients of the raw data with an average of 1.5×10^{-3}. (b) Autocorrelation coefficients of the post-processed data with an average of -8.21×10^{-4}. This was calculated from 10,000 pieces of data.

or a matrix described as

$$\mathbf{A}_{i,j} = \mathbf{A}_{i+1,j+1} = a_{i-j} \ . \tag{6.5.7}$$

The random seed takes the form of a Toeplitz matrix (n-by-m matrix) which is multiplied with the n-bit raw data to extract the m-bit random output. This requires a $d = n + m - 1$ seed length of random bits to form the matrix.

This extractor was implemented in software, and would not be sufficient for real-time processing of data. Further implementations would require optimised software or hardware implementations, such as those demonstrated in [259, 280].

6.5.3 Testing and validation

These data can be tested and validated based with standard test suites used to test the statistical randomness of bit sequences. We present the autocorrelation of the function to illustrate the comparison of raw and post-processed data (see Figure 6.9). The raw data shows considerable correlation in the first autocorrelation coefficients in comparison to the post-processed data, with a mean of 1.5×10^{-3} for the raw data compared to -8.21×10^{-4} over the first 100 autocorrelations, evaluated with for 10,000 bits of random data.

NIST test suites [281, 282], TestU01 [283] and DIEHARD [251] tests place further stringent requirements on the data, and are used to validate the post-processed results.

	Raw Data		Hashed-Data		
Statistical Test	Proportion	Result	p-value	Proportion	Result
Frequency	0/15	failure	0.001	15/15	pass
Block-Frequency	15/15	pass	0.276	15/15	pass
Cumulative sums	0/15	failure	0.091	15/15	pass
Runs	0/15	failure	0.637	15/15	pass
Longest run	0/15	failure	0.437	15/15	pass
Rank	0/15	failure	0.049	15/15	pass
FFT	15/15	pass	0.006	15/15	pass
Nonoverlapping template	11/15	failure	0.163	14/15	pass
Overlapping template	0/15	failure	0.003	15/15	pass
Universal	0/15	failure	0.000	15/15	pass
Approximate Entropy	0/15	failure	0.025	13/15	pass
Serial	13/15	pass	0.163	15/15	pass
Linear Complexity	15/15	pass	0.000	15/15	pass

Table 6.1: **Statistical Tests** using the NIST test suites [282] illustrating the failure of the raw data compared to the success of the post-processed output.

The raw data, which still contains electronic noise, fails 9 of the tests illustrated in Table 6.1, compared to the hashed data that passes all 13 of the listed tests. This assures that the random sequences generated from our quantum random number generator display excellent statistical randomness in comparison to pseudo-random equivalents. The improvement in performance between the raw and hashed data set illustrates the need to properly account for the influence of knowable classical electronic noise.

6.6 Summary

Random numbers are essential in many fields including cryptography, fundamental tests of physics and scientific simulations. These applications rely on the unpredictability of random numbers, which cannot be guaranteed when using classical techniques. Random number generators are often based on pseudo-random number generation algorithms that expand on an initial seed in a deterministic manner, suffering from problems of periodicity and long-term correlations that can undermine the security. In comparison, quantum mechanical systems can be prepared in a superposition of states, and the measurement of this state can be intrinsically random. Therefore, the inherently random nature of

quantum measurements can be exploited to generate truly random numbers.

Here we showed the use of integrated photonics for generating quantum random numbers. In particular we use weak coherent sources of light generated in InP devices and single photon detectors in a number of configurations to generate 10.5 Mbps and 145 Mbps of unbiased quantum random numbers. We further improve upon this rate and the versatility of the devices by demonstrating the use of integrated homodyne detector systems to generate 1.03 Gbps of unbiased quantum random numbers.

Ultimately, integrated photonics will allow the manufacture of single quantum communications chips with electronic and photonic processing on a monolithic device. This will enable further multiplexing and complexity of operation. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secure communications.

6.7 Further Developments - Improvements

Future designs and development of this work has included a fully integrated homodyne detection methods with integrated laser source in InP devices to be fabricated by Oclaro (see Figure 6.10 (b)).

The design also incorporates a second laser in the vacuum arm, that in principle could be used to generate another coherent state that could interfere with the first. This could be operated in a number of ways; firstly, by switching above and below threshold, a random global phase is generated, which can interfere with the steady CW arm. The interference will convert an amplified spontaneous phase into a relative intensity measured directly by the photodetector (analogous to the scheme described in [267]).

Secondly, the second laser could be operated around the threshold value, allowing phase random amplified spontaneous emission, that can again interfere with the steady CW laser from the other arm (analogous to the scheme described in [266, 268, 270]). This technique requires the attenuation of the steady CW laser to ensure maximum visibility of the interfered spontaneous signals. These techniques mitigate the need for long and lossy delay lines used in self-heterodyne schemes, but will have more stringent requirements

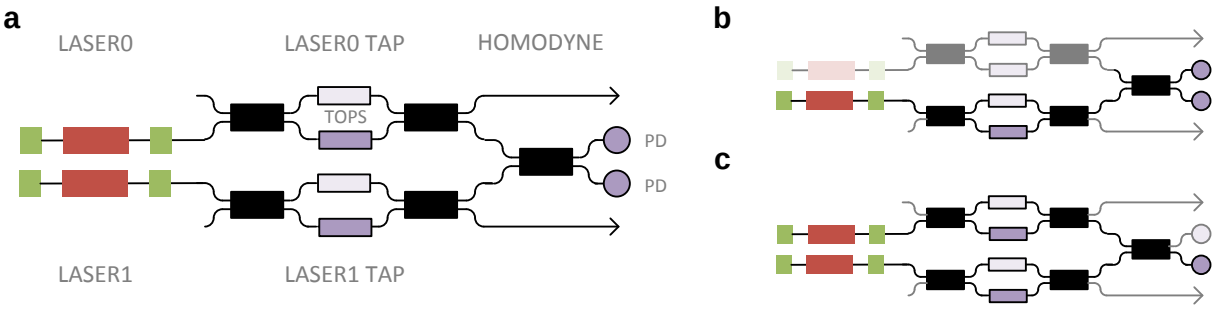

Figure 6.10: **Future QRNG designs:** (a) Full schematic of future generation integrated quantum random number generators with laser sources, reconfigurable output monitoring for calibration. (b) Configured as a homodyne detector with a single laser source, with the laser taps routing as much light towards the detectors. (c) Configured to measure phase noise from amplified spontaneous emission, either by pulsing the second laser above and below threshold or holding near threshold level compared to a steady CW laser. This requires the use of a single output detector.

to overlap two separate lasers, the control of which can be achieved through the carrier injection on the T-DBR as described in Section 4.2.1.

Other devices have been designed for fabrication by IMEC in silicon-on-insulator, which will use a single off-chip laser source for amplified spontaneous emission schemes using an AMZI to convert relative phases in to amplitude outputs as illustrated in Figure 6.2 (d). This self-heterodyne detection scheme [266, 268, 270] reduces the need to overlap separate laser sources and in principle allow multi-GHz operation, as the photodiodes have ∼15 GHz bandwidths.

Chapter 7

Conclusion

7.1 Summary

In this thesis we demonstrate the development of integrated photonics for quantum secured communications. We first reported low error rate, GHz clocked **chip-to-chip QKD** operation of an InP transmitter chip and a SiO_xN_y receiver chip—monolithically integrated devices that use state-of-the-art components and manufacturing processes from the telecom industry. We used the reconfigurability of these devices to demonstrate three important QKD protocols—BB84, Coherent One Way (COW) and Differential Phase Shift (DPS)—with performance comparable to state-of-the-art. We demonstrated clock rates up to 1.72 GHz, a quantum bit error rate (QBER) as low as 0.88%, and estimated secret key rates up to 575 kbps, for an emulated 20 km fibre link. These devices, when combined with integrated single photon detectors, satisfy the requirements at each of the levels of future QKD networks—from point-of-use through to backbones—and open the way to operation in existing and emerging classical communication networks.

We further used an efficient decoy-state BB84 scheme with biased basis preparation and measurement to increase channel capacity. We then illustrated the benefits of miniaturisation and manufacturability of integrated photonics by demonstrating a proof-of-principle **WDM-QKD** link. Two InP transmitters operated at different wavelengths are combined on to the same optical fibre, and demultiplexed and decoded on a SiO_xN_y chip to demonstrate increased rate with limited increase of error. We demonstrated an

estimated secure key rates of 1.11 Mbps over emulated 20 km fibre, with two independent transmitter and receiver links, using both wavelength and temporal filtering to reduce channel cross-talk noise.

Integrated photonics offers great potential for quantum communication devices in terms of complexity, robustness and scalability. **Silicon photonics** in particular is a leading platform for quantum photonic technologies, with further benefits of miniaturisation, cost-effective device manufacture and compatibility with CMOS microelectronics. However, effective techniques for high-speed modulation of quantum states in standard silicon photonic platforms have been limited. Here we overcame this limitation and demonstrated high-speed low-error QKD modulation with silicon photonic devices combining slow thermo-optic DC biases and fast (10 GHz bandwidth) carrier-depletion modulation. We illustrated this approach with the preparation of time-bin encoded BB84 QKD states with 2.1% QBER. We further demonstrated this technology with implementations of polarisation encoded BB84 QKD (1 GHz clock rate, 1.1% QBER, 329 kbps secret key rate) and Coherent-One-Way QKD (1.72 GHz clock rate, 1.01% QBER, 916 kbps secret key rate) over a 20 km fibre link.

Finally we showed the use of integrated photonics based **quantum random number generators** required for quantum key distribution systems. In particular we used weak coherent sources of light generated in InP devices and single photon detectors in a number of configurations to generate 10.5 Mbps and 145 Mbps of unbiased quantum random numbers. We further improve upon this rate and the versatility of the devices by demonstrating an integrated homodyne detector systems to generate 1.03 Gbps of quantum random numbers passing a number of statistical random test suites.

7.2 Outlook

In this thesis we demonstrated the development of integrated photonics for quantum secured communications. Quantum technologies are rapidly developing and have the potential to revolutionise the fields of computing and telecommunications. They have major implications for the security of many of our conventional cryptographic techniques which are known to be insecure against a quantum computer [1]. Therefore, improvement in se-

cure transmission of information is an urgent practical need for governments, corporations and individuals.

Quantum key distribution [1,2] (QKD) promises security based on the laws of physics and has rapidly grown from proof-of-concept to robust demonstrations [3–6] and even deployment of commercial systems [7–9]. Despite these advances, QKD has not been widely adopted, and practical large-scale deployment will likely require integrated chip-based devices for improved performance, miniaturisation and enhanced functionality, fully integrated into classical communication networks.

Ultimately, integrated photonics will allow the manufacture of single quantum communications chips with electronic and photonic processing on a monolithic device. This will enable further multiplexing and complexity of operation. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secure communications.

Bibliography

[1] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

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

[3] K.-i. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," *Opt. Exp.*, vol. 21, no. 23, pp. 31395–31401, 2013.

[4] B. Korzh, N. Walenta, R. Houlmann, and H. Zbinden, "A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator," *Opt. Exp.*, vol. 21, no. 17, pp. 19579–19592, 2013.

[5] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "High speed prototype quantum key distribution system and long term field trial," *Opt. Exp.*, vol. 23, no. 6, pp. 7583–7592, 2015.

[6] M. Sasaki, M. Fujiwara, R.-B. Jin, M. Takeoka, H. Endo, K.-I. Yoshino, T. Ochi, S. Asami, A. Tajima, *et al.*, "Quantum Photonic Network: Concept, Basic Tools, and Future Issues," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, no. 3, pp. 1–13, 2015.

[7] idQuantique. http://www.idquantique.com/, 2015.

[8] MagiQ. http://www.magiqtech.com/, 2012.

[9] Quintessence Labs. http://www.quintessencelabs.com, 2015.

[10] M. G. Thompson, A. Politi, J. C. Matthews, and J. L. O'Brien, "Integrated waveguide circuits for optical quantum computing," *IET circuits, devices & systems*, vol. 5, no. 2, pp. 94–102, 2011.

[11] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, "Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client," *Phys. Rev. Lett.*, vol. 112, no. 13, p. 130501, 2014.

[12] A. Tanaka, M. Fujiwara, K.-i. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-speed quantum key distribution system for 1-Mbps real-time key generation," *Quantum Electronics, IEEE Journal of*, vol. 48, no. 4, pp. 542–550, 2012.

[13] P. Wayner, *Disappearing Cryptography: Information Hiding: Steganography & Watermarking*. Morgan Kaufmann, 2009.

[14] J. Katz and Y. Lindell, *Introduction to modern cryptography: principles and protocols. Cryptography and network security*. Chapman & Hall/CRC, Boca Raton, 2008.

[15] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[16] N. Biggs, *Codes: An Introduction to Information Communication and Cryptography*. Springer London, 2008.

[17] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *AIEE, Journal of the*, vol. 45, no. 2, pp. 109–115, 1926.

[18] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[19] D. R. Stinson, *Cryptography: theory and practice*. CRC press, 2005.

[20] P. Ribenboim, *The book of prime numbers records*. New York, Springer-Verlag, 1989.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[22] D. Boneh and R. Venkatesan, "Breaking RSA may not be equivalent to factoring," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 59–71, Springer, 1998.

[23] J. Preskill, "Lecture notes for physics 229: Quantum information and computation," *California Institute of Technology*, vol. 12, p. 14, 1998.

[24] J. S. Bell, "On the Einstein Podolsky Rosen Paradox," 1964.

[25] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical review*, vol. 47, no. 10, p. 777, 1935.

[26] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of Modern Physics*, vol. 86, no. 2, p. 419, 2014.

[27] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical review letters*, vol. 23, no. 15, p. 880, 1969.

[28] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 28, no. 14, p. 938, 1972.

[29] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via bell's theorem," *Physical review letters*, vol. 47, no. 7, p. 460, 1981.

[30] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities," *Physical review letters*, vol. 49, no. 2, p. 91, 1982.

[31] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers," *Physical review letters*, vol. 49, no. 25, p. 1804, 1982.

[32] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[33] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[34] R. P. Feynman, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6, pp. 467–488, 1982.

[35] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 400, pp. 97–117, The Royal Society, 1985.

[36] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 439, pp. 553–558, The Royal Society, 1992.

[37] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, ACM, 1996.

[38] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," *Physical review letters*, vol. 103, no. 15, p. 150502, 2009.

[39] M. Schuld, I. Sinayskiy, and F. Petruccione, "An introduction to quantum machine learning," *Contemporary Physics*, vol. 56, pp. 172–185, Apr. 2015.

[40] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pp. 124–134, IEEE, 1994.

[41] S. Wiesner, "Conjugate Coding," *SIGACT News*, vol. 15, pp. 78–88, Jan. 1983.

[42] C. Bennett and G. Brassard in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, (New York), p. 175, 1984.

[43] M. Dušek, M. Jahma, and N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Physical Review A*, vol. 62, no. 2, p. 022306, 2000.

[44] R. B. Clarke, A. Chefles, S. M. Barnett, and E. Riis, "Experimental demonstration of optimal unambiguous state discrimination," *Physical Review A*, vol. 63, no. 4, p. 040305, 2001.

[45] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Physical Review A*, vol. 59, no. 6, p. 4238, 1999.

[46] H.-K. Lo, "Proof of unconditional security of six-state quatum key distribution scheme," *Quantum Information & Computation*, vol. 1, no. 2, pp. 81–94, 2001.

[47] A. K. Ekert, "Quantum cryptography based on Bells theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[48] K.-C. Nguyen, G. Van Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," *arXiv eprint arXiv:cs/0406001*, 2004.

[49] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information reconciliation for quantum key distribution," *arXiv preprint arXiv:1007.1616*, 2010.

[50] P. Jouguet and S. Kunz-Jacques, "High performance error correction for quantum key distribution using polar codes," *Quantum Information & Computation*, vol. 14, no. 3-4, pp. 329–338, 2014.

[51] R. Renner and R. König, "Universally composable privacy amplification against quantum adversaries," in *Theory of Cryptography*, pp. 407–425, Springer, 2005.

[52] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A*, vol. 63, no. 5, p. 052311, 2001.

[53] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 db loss limit," *Physical Review Letters*, vol. 89, no. 16, p. 167901, 2002.

[54] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase-shift quantum key distribution," in *Photonics Asia 2002*, pp. 32–39, International Society for Optics and Photonics, 2002.

[55] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Physical Review A*, vol. 68, no. 2, p. 022317, 2003.

[56] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105 km fibre," *New Journal of Physics*, vol. 7, no. 1, p. 232, 2005.

[57] E. Diamanti, H. Takesue, C. Langrock, M. Fejer, and Y. Yamamoto, "100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors," *Optics Express*, vol. 14, no. 26, pp. 13073–13082, 2006.

[58] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors," *Nature Photonics*, vol. 1, no. 6, pp. 343–348, 2007.

[59] C. Branciard, N. Gisin, and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," *New J. Phys.*, vol. 10, no. 1, p. 013031, 2008.

[60] T. Moroder, M. Curty, C. C. W. Lim, L. P. Thinh, H. Zbinden, and N. Gisin, "Security of Distributed-Phase-Reference Quantum Key Distribution," *Physical Review Letters*, vol. 109, p. 260501, Dec. 2012.

[61] K. Tamaki, M. Koashi, and G. Kato, "Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization," *arXiv preprint arXiv:1208.1995*, 2012.

[62] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[63] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[64] T. Schmitt-Manderbach *et al.*, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, p. 010504, Jan 2007.

[65] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, no. 5, pp. 382–386, 2013.

[66] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, pp. 387–393, May 2013.

[67] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, p. 023006, Feb. 2013.

[68] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Physical Review Letters*, vol. 115, no. 4, p. 040502, 2015.

[69] Y. Cao, H. Liang, J. Yin, H.-L. Yong, F. Zhou, Y.-P. Wu, J.-G. Ren, Y.-H. Li, G.-S. Pan, T. Yang, X. Xa, C.-Z. Peng, and J.-W. Pan, "Entanglement-based quantum key distribution with biased basis choice via free space," *Optics Express*, vol. 21, no. 22, pp. 27260–27268, 2013.

[70] A. Berk, L. Bernstein, G. Anderson, P. Acharya, D. Robertson, J. Chetwynd, and S. Adler-Golden, "MODTRAN cloud and multiple scattering upgrades with application to AVIRIS," *Remote Sensing of Environment*, vol. 65, no. 3, pp. 367–375, 1998.

[71] Z. Yuan, A. Sharpe, and A. Shields, "Unconditionally secure one-way quantum key distribution using decoy pulses," *arXiv preprint quant-ph/0610015*, 2006.

[72] J. Kim, S. Takeuchi, Y. Yamamoto, and H. H. Hogue, "Multiphoton detection using visible light photon counter," *Applied Physics Letters*, vol. 74, no. 7, pp. 902–904, 1999.

[73] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. Goltsman, and A. Semenov, "Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range," *Applied Physics Letters*, vol. 80, no. 25, pp. 4687–4689, 2002.

[74] A. J. Miller, S. W. Nam, J. M. Martinis, and A. V. Sergienko, "Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination," *Applied Physics Letters*, vol. 83, no. 4, pp. 791–793, 2003.

[75] S. Camatel and V. Ferrero, "Homodyne coherent detection of ASK and PSK signals performed by a subcarrier optical phase-locked loop," *Photonics Technology Letters, IEEE*, vol. 18, no. 1, pp. 142–144, 2006.

[76] SeQureNet. http://www.sequrenet.com/, 2015.

[77] N. Telegraph and T. Corporation. http://www.ntt.co.jp, 2015.

[78] Toshiba Research Europe Ltd. http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution, 2015.

[79] J. Friedman, "TEMPEST: A signal problem," *NSA Cryptologic Spectrum*, p. 4, 1972.

[80] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics*, vol. 48, no. 13, pp. 2023–2038, 2001.

[81] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[82] A. L. Lacaita, F. Zappa, S. Bigliardi, and M. Manfredi, "On the bremsstrahlung origin of hot-carrier-induced photons in silicon devices," *Electron Devices, IEEE Transactions on*, vol. 40, no. 3, pp. 577–582, 1993.

[83] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?," *Journal of Modern Optics*, vol. 48, no. 13, pp. 2039–2047, 2001.

[84] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.

[85] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Physical Review A*, vol. 75, no. 3, p. 032314, 2007.

[86] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *arXiv preprint quant-ph/0512080*, 2005.

[87] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[88] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 3–11, 1973.

[89] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, p. 136, IEEE, 2004.

[90] X. Ma, "Unconditional security at a low cost," *Physical Review A*, vol. 74, no. 5, p. 052325, 2006.

[91] M. Ardehali, H. Chau, and H.-K. Lo, "Efficient quantum key distribution," *arXiv preprint quant-ph/9803007*, 1998.

[92] H.-K. Lo, H.-F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[93] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with non-random phases," *Quantum Information and Computation*, vol. 7, no. 5&6, pp. 431–458, 2007.

[94] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, pp. 207–235, The Royal Society, 2005.

[95] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Physical review letters*, vol. 100, no. 20, p. 200501, 2008.

[96] R. Y. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.

[97] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Optics express*, vol. 21, no. 21, pp. 24550–24565, 2013.

[98] M. Lucamarini, J. F. Dynes, B. Frohlich, Z. Yuan, and A. J. Shields, "Security bounds for efficient decoy-state quantum key distribution," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, no. 3, pp. 197–204, 2015.

[99] A. Laing, V. Scarani, J. G. Rarity, and J. L. OBrien, "Reference-frame-independent quantum key distribution," *Physical Review A*, vol. 82, no. 1, p. 012304, 2010.

[100] J. Wabnig, D. Bitauld, H. Li, A. Laing, J. O'Brien, and A. Niskanen, "Demonstration of free-space reference frame independent quantum key distribution," *New Journal of Physics*, vol. 15, no. 7, p. 073001, 2013.

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

[102] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 108, p. 130503, Mar. 2012.

[103] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep 2013.

[104] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, p. 130501, Sep 2013.

[105] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, p. 230501, 2007.

[106] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, pp. 682–686, 2015.

[107] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," *Physical Review Letters*, vol. 105, no. 7, p. 070501, 2010.

[108] M. Curty and T. Moroder, "Heralded-qubit amplifiers for practical device-independent quantum key distribution," *Physical Review A*, vol. 84, no. 1, p. 010304, 2011.

[109] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[110] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in *Defense and Security*, pp. 138–149, International Society for Optics and Photonics, 2005.

[111] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[112] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[113] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," *arXiv preprint arXiv:1305.0305*, 2013.

[114] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, *et al.*, "Field test of wavelength-saving quantum key distribution network," *Optics letters*, vol. 35, no. 14, pp. 2454–2456, 2010.

[115] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[116] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, *et al.*, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Optics Express*, vol. 17, no. 8, pp. 6540–6549, 2009.

[117] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, "Security of quantum key distribution using a simplified trusted relay," *Phys. Rev. A*, vol. 91, p. 012338, Jan 2015.

[118] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, no. 7465, pp. 69–72, 2013.

[119] T. S. Humble and R. J. Sadlier, "Software-defined quantum communication systems," *Optical Engineering*, vol. 53, p. 086103, Aug. 2014.

[120] V. R. Dasari, R. J. Sadlier, R. Prout, B. P. Williams, and T. S. Humble, "Programmable Multi-Node Quantum Network Design and Simulation," *ArXiv e-prints*, Apr. 2016.

[121] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson, A. Lord, R. Nejabati, and D. Simeonidou, "First Experimental Demonstration of Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources," *ArXiv e-prints*, Apr. 2016.

[122] M. Żukowski, A. Zeilinger, M. Horne, and A. Ekert, ""Event-ready-detectors" Bell experiment via entanglement swapping," *Physical Review Letters*, vol. 71, no. 26, p. 4287, 1993.

[123] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical review letters*, vol. 76, no. 5, p. 722, 1996.

[124] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[125] D. Collins, N. Gisin, and H. De Riedmatten, "Quantum relays for long distance quantum cryptography," *Journal of Modern Optics*, vol. 52, no. 5, pp. 735–753, 2005.

[126] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, 2001.

[127] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, p. 6787, Apr. 2015.

[128] P. L. McMahon and K. De Greve, "Towards Quantum Repeaters with Solid-State Qubits: Spin-Photon Entanglement Generation using Self-Assembled Quantum Dots," *ArXiv e-prints*, Jan. 2015.

[129] L. Childress, J. Taylor, A. S. Sørensen, and M. D. Lukin, "Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters," *Physical Review A*, vol. 72, no. 5, p. 052330, 2005.

[130] C. Cohen-Tannoudji, J. Dupont-Roc, and G. Grynberg, "Photons and atoms: introduction to quantum electrodynamics," 2001.

[131] P. A. M. Dirac, *The principles of quantum mechanics*. No. 27, Oxford university press, 1981.

[132] B. Lounis and W. Moerner, "Single photons on demand from a single molecule at room temperature," *Nature*, vol. 407, no. 6803, pp. 491–493, 2000.

[133] P. Michler, A. Kiraz, C. Becher, W. Schoenfeld, P. Petroff, L. Zhang, E. Hu, and A. Imamoglu, "A quantum dot single-photon turnstile device," *Science*, vol. 290, no. 5500, pp. 2282–2285, 2000.

[134] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "Triggered single photons from a quantum dot," *Physical Review Letters*, vol. 86, no. 8, p. 1502, 2001.

[135] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, "Stable solid-state source of single photons," *Physical review letters*, vol. 85, no. 2, p. 290, 2000.

[136] B. Johnson, S. Castelletto, T. Ohshima, and T. Umeda, "Fabrication of single photon centres in silicon carbide," in *COMMAD 2012*, pp. 217–218, IEEE, 2012.

[137] J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gérard, "A highly efficient single-photon source based on a quantum dot in a photonic nanowire," *Nature Photonics*, vol. 4, no. 3, pp. 174–177, 2010.

[138] M. E. Reimer, G. Bulgarini, N. Akopian, M. Hocevar, M. B. Bavinck, M. A. Verheijen, E. P. Bakkers, L. P. Kouwenhoven, and V. Zwiller, "Bright single-photon sources in bottom-up tailored nanowires," *Nature communications*, vol. 3, p. 737, 2012.

[139] M. Fox, *Quantum Optics: An Introduction*. OUP Oxford, 2006.

[140] R. H. Brown and R. Twiss, "A test of a new type of stellar interferometer on Sirius," *Nature*, vol. 178, no. 4541, pp. 1046–1048, 1956.

[141] P. Kok and B. W. Lovett, *Introduction to optical quantum information processing*. Cambridge University Press, 2010.

[142] D. C. Burnham and D. L. Weinberg, "Observation of simultaneity in parametric production of optical photon pairs," *Physical Review Letters*, vol. 25, no. 2, p. 84, 1970.

[143] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letters*, vol. 75, no. 24, p. 4337, 1995.

[144] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultra-bright source of polarization-entangled photons," *Physical Review A*, vol. 60, no. 2, p. R773, 1999.

[145] G. Bonfrate, V. Pruneri, P. Kazansky, P. Tapster, and J. Rarity, "Parametric fluorescence in periodically poled silica fibers," *Applied physics letters*, vol. 75, no. 16, pp. 2356–2358, 1999.

[146] M. Fiorentino, P. L. Voss, J. E. Sharping, and P. Kumar, "All-fiber photon-pair source for quantum communications," *Photonics Technology Letters, IEEE*, vol. 14, no. 7, pp. 983–985, 2002.

[147] J. E. Sharping, K. F. Lee, M. A. Foster, A. C. Turner, B. S. Schmidt, M. Lipson, A. L. Gaeta, and P. Kumar, "Generation of correlated photons in nanoscale silicon waveguides," *Optics Express*, vol. 14, no. 25, pp. 12388–12393, 2006.

[148] R. Loudon, *The quantum theory of light*. OUP Oxford, 2000.

[149] R. W. Boyd, "Chapter 1 - the nonlinear optical susceptibility," in *Nonlinear Optics (Third Edition)* (R. W. Boyd, ed.), pp. 1 – 67, Burlington: Academic Press, third edition ed., 2008.

[150] M. Reid and D. Walls, "Quantum theory of nondegenerate four-wave mixing," *Physical Review A*, vol. 34, no. 6, p. 4929, 1986.

[151] S. Clemmen, K. P. Huy, W. Bogaerts, R. G. Baets, P. Emplit, and S. Massar, "Continuous wave photon pair generation in silicon-on-insulator waveguides and ring resonators," *Optics express*, vol. 17, no. 19, pp. 16558–16570, 2009.

[152] X.-s. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, "Experimental generation of single photons via active multiplexing," *Physical Review A*, vol. 83, no. 4, p. 043814, 2011.

[153] T. Meany, L. A. Ngah, M. J. Collins, A. S. Clark, R. J. Williams, B. J. Eggleton, M. Steel, M. J. Withford, O. Alibart, and S. Tanzilli, "Hybrid photonic circuit for multiplexed heralded single photons," *Laser & Photonics Reviews*, vol. 8, no. 3, pp. L42–L46, 2014.

[154] C. Xiong, X. Zhang, Z. Liu, M. Collins, A. Mahendra, L. Helt, M. Steel, D.-Y. Choi, C. Chae, P. Leong, *et al.*, "Active temporal multiplexing of indistinguishable heralded single photons," *arXiv preprint arXiv:1508.03429*, 2015.

[155] G. J. Mendoza, R. Santagati, J. Munns, E. Hemsley, M. Piekarek, E. Martín-López, G. D. Marshall, D. Bonneau, M. G. Thompson, and J. L. O'Brien, "Active temporal and spatial multiplexing of photons," *Optica*, vol. 3, no. 2, pp. 127–132, 2016.

[156] G. Lifante, "Review of the electromagnetic theory of light," *Integrated Photonics: Fundamentals*, pp. 24–51.

[157] L. B. Soldano and E. Pennings, "Optical multi-mode interference devices based on self-imaging: principles and applications," *Lightwave Technology, Journal of*, vol. 13, no. 4, pp. 615–627, 1995.

[158] R. W. Boyd, "Chapter 11 - The Electrooptic and Photorefractive Effects," in *Nonlinear Optics (Third Edition)* (R. W. Boyd, ed.), pp. 511 – 541, Burlington: Academic Press, third edition ed., 2008.

[159] J. S. Weiner, D. A. Miller, and D. S. Chemla, "Quadratic electro-optic effect due to the quantum-confined Stark effect in quantum wells," *Applied physics letters*, vol. 50, no. 13, pp. 842–844, 1987.

[160] Q. Xu, S. Manipatruni, B. Schmidt, J. Shakya, and M. Lipson, "12.5 Gbit/s carrier-injection-based silicon micro-ring silicon modulators," *Optics express*, vol. 15, no. 2, pp. 430–436, 2007.

[161] F. Y. Gardes, A. Brimont, P. Sanchis, G. Rasigade, D. Marris-Morini, L. O'Faolain, F. Dong, J. M. Fedeli, P. Dumon, L. Vivien, T. F. Krauss, G. T. Reed, and J. Martí, "High-speed modulation of a compact silicon ring resonator based on a reverse-biased pn diode," *Optics express*, vol. 17, no. 24, pp. 21986–21991, 2009.

[162] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature photonics*, vol. 3, no. 12, pp. 696–705, 2009.

[163] J. G. Rarity, K. D. Ridley, and P. Tapster, "Absolute measurement of detector quantum efficiency using parametric downconversion," *Applied optics*, vol. 26, no. 21, pp. 4616–4619, 1987.

[164] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. Yuan, R. V. Penty, and A. J. Shields, "Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm," *Journal of Applied Physics*, vol. 117, no. 8, p. 083109, 2015.

[165] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," *Optics express*, vol. 16, no. 5, pp. 3032–3040, 2008.

[166] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, "Bell violation using entangled photons without the fair-sampling assumption," *Nature*, vol. 497, no. 7448, pp. 227–230, 2013.

[167] D. Rosenberg, S. W. Nam, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita, and A. J. Miller, "Quantum key distribution at telecom wavelengths with noise-free detectors," *Applied physics letters*, vol. 88, no. 2, p. 021108, 2006.

[168] G. GolTsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," *Applied Physics Letters*, vol. 79, no. 6, pp. 705–707, 2001.

[169] J. Sprengers, A. Gaggero, D. Sahin, S. Jahanmirinejad, G. Frucci, F. Mattioli, R. Leoni, J. Beetz, M. Lermer, M. Kamp, S. Höfling, R. Sanjines, and A. Fiore, "Waveguide superconducting single-photon detectors for integrated quantum photonic circuits," *Applied Physics Letters*, vol. 99, no. 18, p. 181110, 2011.

[170] S. Dorenbos, E. Reiger, U. Perinetti, V. Zwiller, T. Zijlstra, and T. Klapwijk, "Low noise superconducting single photon detectors on silicon," *Applied Physics Letters*, vol. 93, no. 13, p. 131101, 2008.

[171] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics*, vol. 7, no. 3, pp. 210–214, 2013.

[172] C. Schuck, W. H. Pernice, O. Minaeva, M. Li, G. Gol'tsman, A. V. Sergienko, and H. X. Tang, "Matrix of integrated superconducting single-photon detectors with high timing resolution," *Applied Superconductivity, IEEE Transactions on*, vol. 23, no. 3, pp. 2201007–2201007, 2013.

[173] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," *Superconductor science and technology*, vol. 25, no. 6, p. 063001, 2012.

[174] A. Politi, J. C. Matthews, M. G. Thompson, and J. L. O'Brien, "Integrated quantum photonics," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 15, no. 6, pp. 1673–1684, 2009.

[175] A. Leinse, R. Heideman, E. Klein, R. Dekker, C. Roeloffzen, and D. Marpaung, "TriPleX; platform technology for photonic integration: Applications from UV through NIR to IR," in *Information Photonics (IP), 2011 ICO International Conference on*, pp. 1–2, May 2011.

[176] F. Morichetti, A. Melloni, M. Martinelli, R. Heideman, A. Leinse, D. Geuzebroek, and A. Borreman, "Box-Shaped Dielectric Waveguides: A New Concept in Integrated Optics?," *Lightwave Technology, Journal of*, vol. 25, pp. 2579–2589, Sept 2007.

[177] L. A. Eldada, "Advances in telecom and datacom optical components," *Optical Engineering*, vol. 40, pp. 1165–1178, 2001.

[178] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G. Thompson, "On-chip quantum interference between silicon photon-pair sources," *Nature Photonics*, vol. 8, no. 2, pp. 104–108, 2014.

[179] G. T. Reed and A. P. Knights, *Silicon photonics*. Wiley Online Library, 2008.

[180] M. Smit *et al.*, "An introduction to InP-based generic integration technology," *Semiconductor Science and Technology*, vol. 29, no. 8, p. 083001, 2014.

[181] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, *et al.*, "Chip-based Quantum Key Distribution," *arXiv preprint arXiv:1509.00768*, 2015.

[182] Oclaro Inc., "Design Manual for Oclaro PIC process (n+ InP substrate)," 2015.

[183] E. Hecht, *Optics, 4th*, vol. 3. Addison-Wesley, San Francisco, 2002.

[184] D. Miller, D. Chemla, T. Damen, A. Gossard, W. Wiegmann, T. Wood, and C. Burrus, "Band-edge electroabsorption in quantum well structures: the quantum-confined Stark effect," *Physical Review Letters*, vol. 53, no. 22, p. 2173, 1984.

[185] M. M. Radmanesh, *RF & Microwave Design Essentials: Engineering Design and Analysis from DC to Microwaves*. AuthorHouse, 2007.

[186] B. C. Wadell, *Transmission line design handbook*. Artech House Publishers, 1991.

[187] K. Ogata, *Modern control engineering*. Prentice Hall PTR, 2001.

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

[189] Y. Zhao, B. Qi, and H.-K. Lo, "Experimental quantum key distribution with active phase randomization," *Applied physics letters*, vol. 90, no. 4, p. 044106, 2007.

[190] T. Kobayashi, A. Tomita, and A. Okamoto, "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser," *Physical Review A*, vol. 90, no. 3, p. 032320, 2014.

[191] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Applied Physics Letters*, vol. 104, no. 26, p. 261112, 2014.

[192] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, pp. 1675–1680, Apr. 2000.

[193] A. A. Abbott and C. S. Calude, "Von Neumann normalisation of a quantum random number generator," *Computability*, vol. 1, no. 1, pp. 59–83, 2012.

[194] J. Cardenas, C. B. Poitras, K. Luke, L.-W. Luo, P. A. Morton, and M. Lipson, "High coupling efficiency etched facet tapers in silicon waveguides," *IEEE Photonics Technol. Lett*, vol. 26, no. 23, pp. 2380–2382, 2014.

[195] J. F. Bauters, M. L. Davenport, M. J. Heck, J. Doylend, A. Chen, A. W. Fang, and J. E. Bowers, "Silicon on ultra-low-loss waveguide photonic integration platform," *Optics express*, vol. 21, no. 1, pp. 544–555, 2013.

[196] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Optics express*, vol. 16, no. 23, pp. 18790–18797, 2008.

[197] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources," *Phys. Rev. A*, vol. 84, p. 062308, Dec 2011.

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

[199] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Optics letters*, vol. 37, no. 6, pp. 1008–1010, 2012.

[200] H. Shibata, T. Honjo, and K. Shimizu, "Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors," *Optics Letters*, vol. 39, p. 5078, Sept. 2014.

[201] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, A. Lord, and A. Shield, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Optics express*, vol. 22, no. 19, pp. 23121–23128, 2014.

[202] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," *Physical Review A*, vol. 87, no. 6, p. 062322, 2013.

[203] K.-i. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, *et al.*, "High-speed wavelength-division multiplexing quantum key distribution system," *Optics letters*, vol. 37, no. 2, pp. 223–225, 2012.

[204] C. C. W. Lim, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, no. 3, pp. 192–196, 2015.

[205] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Physical review letters*, vol. 112, no. 19, p. 190503, 2014.

[206] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, 2016.

[207] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Practical aspects of measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 15, no. 11, p. 113007, 2013.

[208] A. Gaggero, S. J. Nejad, F. Marsili, F. Mattioli, R. Leoni, D. Bitauld, D. Sahin, G. Hamhuis, R. Nötzel, R. Sanjines, and A. Fiore, "Nanowire superconducting single-photon detectors on GaAs for integrated quantum photonic applications," *Applied Physics Letters*, vol. 97, no. 15, p. 151108, 2010.

[209] M. Aminian, A. Sammak, L. Qi, L. K. Nanver, and E. Charbon, "A Ge-on-Si single-photon avalanche diode operating in Geiger mode at infrared wavelengths," in *SPIE Defense, Security, and Sensing*, pp. 83750Q–83750Q, International Society for Optics and Photonics, 2012.

[210] R. E. Warburton, G. Intermite, M. Myronov, P. Allred, D. R. Leadley, K. Gallacher, D. J. Paul, N. J. Pilgrim, L. J. Lever, Z. Ikonic, R. W. Kelsall, E. Huante-Cerón, A. P. Knights, and G. S. Buller, "Ge-on-Si single-photon avalanche diode detectors: design, modeling, fabrication, and characterization at wavelengths 1310 and 1550 nm," *Electron Devices, IEEE Transactions on*, vol. 60, no. 11, pp. 3807–3813, 2013.

[211] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[212] R. Ramaswami, K. Sivarajan, and G. Sasaki, *Optical networks: a practical perspective*. Morgan Kaufmann, 2009.

[213] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, "Stable quantum key distribution with active polarization control based on time-division multiplexing," *New Journal of Physics*, vol. 11, no. 6, p. 065004, 2009.

[214] A. Tanaka, A. Tomita, A. Tomita, and A. Tajima, "Colourless interferometric technique for large capacity quantum key distribution systems by use of wavelength division multiplexing," *ECOC 2009*, 2009.

[215] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," *Optics express*, vol. 18, no. 9, pp. 9600–9612, 2010.

[216] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, p. 051123, 2014.

[217] J. Mower, F. Wong, J. H. Shapiro, and D. Englund, "Dense wavelength division multiplexed quantum key distribution using entangled photons," *arXiv preprint arXiv:1110.4867*, 2011.

[218] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, "Decoy-state quantum key distribution with biased basis choice," *Scientific reports*, vol. 3, 2013.

[219] X. J. Leijtens, B. Kuhlow, and M. K. Smit, "Arrayed waveguide gratings," in *Wavelength Filters in Fibre Optics*, pp. 125–187, Springer, 2006.

[220] D. G. Rabus, *Integrated ring resonators*. Springer, 2007.

[221] A. Othonos and K. Kalli, *Fiber Bragg gratings: fundamentals and applications in telecommunications and sensing*. Artech House, 1999.

[222] C. J. R. Sheppard, "Approximate calculation of the reflection coefficient from a stratified medium," *Pure and Applied Optics: Journal of the European Optical Society Part A*, vol. 4, no. 5, p. 665, 1995.

[223] T. Numai, "Fabry–perot laser diodes," *Laser Diodes and their Applications to Communications and Information Processing*, pp. 123–190.

[224] T. L. Koch, U. Koren, R. P. Gnall, C. A. Burrus, and B. I. Miller, "Continuously tunable 1.5 μm multiple-quantum-well GaInAs/GaInAsP distributed-Bragg-reflector lasers," *Electronics Letters*, vol. 24, no. 23, pp. 1431–1433, 1988.

[225] A. E.-J. Lim, J. Song, Q. Fang, C. Li, X. Tu, N. Duan, K. K. Chen, R. P.-C. Tern, and T.-Y. Liow, "Review of silicon photonics foundry efforts," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 20, no. 4, pp. 405–416, 2014.

[226] J. Silverstone, D. Bonneau, J. O. Brien, and M. Thompson, "Silicon quantum photonics," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. PP, no. 99, pp. 1–1, 2016.

[227] W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, and H. X. Tang, "High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits," *Nature Communications*, vol. 3, p. 1325, Dec. 2012.

[228] F. Najafi, J. Mower, N. C. Harris, F. Bellei, A. Dane, C. Lee, X. Hu, P. Kharel, F. Marsili, S. Assefa, K. K. Berggren, and D. Englund, "On-chip detection of non-classical light by scalable integration of single-photon detectors," *Nature communications*, vol. 6, 2015.

[229] C. Doerr, "Silicon photonic integration in telecommunications," *Frontiers in Physics*, vol. 3, p. 37, 2015.

[230] C. Sun, M. T. Wade, Y. Lee, J. S. Orcutt, L. Alloatti, M. S. Georgas, A. S. Waterman, J. M. Shainline, R. R. Avizienis, S. Lin, *et al.*, "Single-chip microprocessor that communicates directly using light," *Nature*, vol. 528, no. 7583, pp. 534–538, 2015.

[231] G. T. Reed, G. Mashanovich, F. Gardes, and D. Thomson, "Silicon optical modulators," *Nature photonics*, vol. 4, no. 8, pp. 518–526, 2010.

[232] R. S. Jacobsen, K. N. Andersen, P. I. Borel, J. Fage-Pedersen, L. H. Frandsen, O. Hansen, M. Kristensen, A. V. Lavrinenko, G. Moulin, H. Ou, C. Peucheret, B. Zsigri, and A. Bjarklev, "Strained silicon as a new electro-optic material," *Nature*, vol. 441, no. 7090, pp. 199–202, 2006.

[233] V. R. Almeida, C. A. Barrios, R. R. Panepucci, and M. Lipson, "All-optical control of light on a silicon chip," *Nature*, vol. 431, no. 7012, pp. 1081–1084, 2004.

[234] J. H. Wülbern, S. Prorok, J. Hampe, A. Petrov, M. Eich, J. Luo, A. K.-Y. Jen, M. Jenett, and A. Jacob, "40 GHz electro-optic modulation in hybrid silicon–organic slotted photonic crystal waveguides," *Optics letters*, vol. 35, no. 16, pp. 2753–2755, 2010.

[235] Z. Fang and C. Z. Zhao, "Recent progress in silicon photonics: a review," *ISRN Optics*, vol. 2012, 2012.

[236] D. Taillaert, P. Bienstman, and R. Baets, "Compact efficient broadband grating coupler for silicon-on-insulator waveguides," *Optics letters*, vol. 29, no. 23, pp. 2749–2751, 2004.

[237] J. Wang, D. Bonneau, M. Villa, J. W. Silverstone, R. Santagati, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-to-chip quantum photonic interconnect by path-polarization interconversion," *Optica*, vol. 3, no. 4, pp. 407–413, 2016.

[238] P. P. Absil, P. De Heyn, H. Chen, P. Verheyen, G. Lepage, M. Pantouvaki, J. De Coster, A. Khanna, Y. Drissi, D. Van Thourhout, and J. Van Campenhout, "Imec iSiPP25G silicon photonics: a robust CMOS-based photonics technology platform," in *SPIE OPTO*, pp. 93670V–93670V, International Society for Optics and Photonics, 2015.

[239] J. Cardenas, C. B. Poitras, J. T. Robinson, K. Preston, L. Chen, and M. Lipson, "Low loss etchless silicon photonic waveguides," *Optics express*, vol. 17, no. 6, pp. 4752–4757, 2009.

[240] D. Liang and J. E. Bowers, "Recent progress in lasers on silicon," *Nature Photonics*, vol. 4, no. 8, pp. 511–517, 2010.

[241] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. G. Muñoz, and J. Capmany, "Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON," *Optics Express*, vol. 20, no. 15, pp. 16358–16365, 2012.

[242] L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimental multiplexing of quantum key distribution with classical optical communication," *Applied Physics Letters*, vol. 106, no. 8, p. 081108, 2015.

[243] M. Piekarek, D. Bonneau, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. Tanner, C. M. Natarajan, R. H. Hadfield, J. O'Brien, and M. Thompson, "Passive High-Extinction Integrated Photonic Filters for Silicon Quantum Photonics," in *Conference on Lasers and Electro-Optics*, p. FM1N.6, Optical Society of America, 2016.

[244] M. Heck, J. F. Bauters, M. L. Davenport, J. K. Doylend, S. Jain, G. Kurczveil, S. Srinivasan, Y. Tang, and J. E. Bowers, "Hybrid silicon photonic integrated circuit technology," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 19, no. 4, 2013.

[245] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *arXiv preprint arXiv:1604.03304*, 2016.

[246] N. Metropolis and S. Ulam, "The monte carlo method," *Journal of the American statistical association*, vol. 44, no. 247, pp. 335–341, 1949.

[247] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *arXiv preprint arXiv:1510.08957*, 2015.

[248] B. Hayes, "Randomness as a resource," *American Scientist*, vol. 89, no. 4, pp. 300–304, 2001.

[249] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms. II.* Addision Wesley, 1998.

[250] A. N. Kolmogorov, "On tables of random numbers," *Theoretical Computer Science*, vol. 207, no. 2, pp. 387–395, 1998.

[251] G. Marsaglia, "DIEHARD: a battery of tests of randomness." http://stat.fsu.edu/~geo/diehard.html, 1996.

[252] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., DTIC Document, 2001.

[253] S.-J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST statistical test suite for randomness," *arXiv preprint nlin/0401040*, 2004.

[254] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, vol. 47, no. 4, pp. 595–598, 2000.

[255] Q. Yan, B. Zhao, Q. Liao, and N. Zhou, "Multi-bit quantum random number generation by measuring positions of arrival photons," *Review of Scientific Instruments*, vol. 85, no. 10, p. 103116, 2014.

[256] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Applied Physics Letters*, vol. 93, no. 3, p. 031109, 2008.

[257] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *Journal of Modern Optics*, vol. 56, no. 4, pp. 516–522, 2009.

[258] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Applied Physics Letters*, vol. 98, no. 17, p. 171105, 2011.

[259] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Applied Physics Letters*, vol. 104, no. 5, p. 051110, 2014.

[260] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Optics express*, vol. 18, no. 12, pp. 13029–13037, 2010.

[261] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Physical Review A*, vol. 83, no. 2, p. 023820, 2011.

[262] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, and A. J. Shields, "Efficient and robust quantum random number generation by photon number detection," *Applied Physics Letters*, vol. 107, no. 7, p. 071106, 2015.

[263] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics*, vol. 4, no. 10, pp. 711–715, 2010.

[264] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," *Physical Review A*, vol. 81, no. 6, p. 063814, 2010.

[265] T. Symul, S. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," *Applied Physics Letters*, vol. 98, no. 23, p. 231103, 2011.

[266] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Optics letters*, vol. 35, no. 3, pp. 312–314, 2010.

[267] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," *Optics express*, vol. 19, no. 21, pp. 20665–20672, 2011.

[268] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Optics express*, vol. 20, no. 11, pp. 12366–12377, 2012.

[269] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Optics express*, vol. 22, no. 2, pp. 1645–1654, 2014.

[270] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Review of Scientific Instruments*, vol. 86, no. 6, p. 063105, 2015.

[271] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Optics Express*, vol. 18, no. 23, pp. 23584–23597, 2010.

[272] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," *Optics letters*, vol. 36, no. 6, pp. 1020–1022, 2011.

[273] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Reviews of Modern Physics*, vol. 77, no. 2, p. 513, 2005.

[274] M. Collett, R. Loudon, and C. Gardiner, "Quantum theory of optical homodyne and heterodyne detection," *Journal of Modern Optics*, vol. 34, no. 6-7, pp. 881–902, 1987.

[275] R. Okubo, M. Hirano, Y. Zhang, and T. Hirano, "Pulse-resolved measurement of quadrature phase amplitudes of squeezed pulse trains at a repetition rate of 76 MHz," *Optics letters*, vol. 33, no. 13, pp. 1458–1460, 2008.

[276] Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. Lvovsky, and L. Tian, "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution," *New Journal of Physics*, vol. 13, no. 1, p. 013003, 2011.

[277] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. Huntington, and A. Lvovsky, "Versatile wideband balanced detector for quantum optical homodyne tomography," *Optics Communications*, vol. 285, no. 24, pp. 5259–5267, 2012.

[278] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," *Physical Review A*, vol. 87, no. 6, p. 062327, 2013.

[279] Y. Mansour, N. Nisan, and P. Tiwari, "The computational complexity of universal hashing," in *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, pp. 235–243, ACM, 1990.

[280] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, "Maximization of extractable randomness in a quantum random-number generator," *Physical Review Applied*, vol. 3, no. 5, p. 054004, 2015.

[281] F. Pareschi, R. Rovatti, and G. Setti, "Second-level NIST randomness tests for improving test reliability," in *2007 IEEE International Symposium on Circuits and Systems*, pp. 1437–1440, IEEE, 2007.

[282] "NIST.gov - Computer Security Division - Computer Security Resource Center." http://csrc.nist.gov/groups/ST/toolkit/rng/. Accessed: 2016-06-29.

[283] P. L'Ecuyer and R. Simard, "TestU01: AC library for empirical testing of random number generators," *ACM Transactions on Mathematical Software (TOMS)*, vol. 33, no. 4, p. 22, 2007.