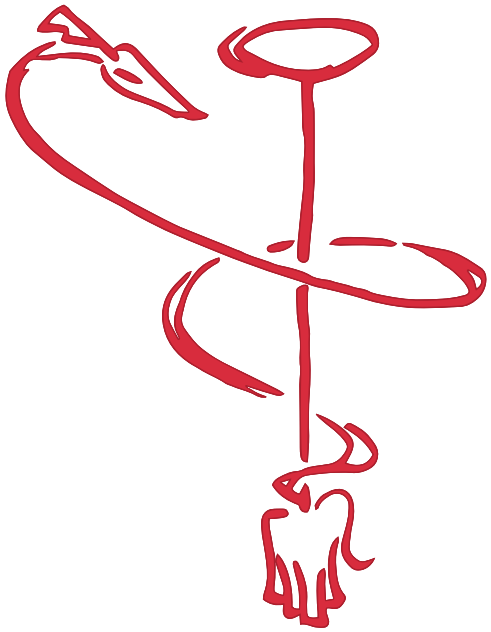
Author:
Semenenko, Henry

Title:
Advances in Chip-Based Quantum Key Distribution

Advances in Chip-Based Quantum Key Distribution

Henry Semenenko



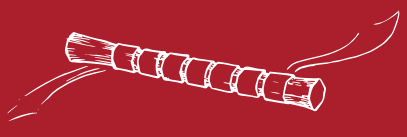
Do not be afraid of making mistakes; the only way to avoid them is to do nothing.

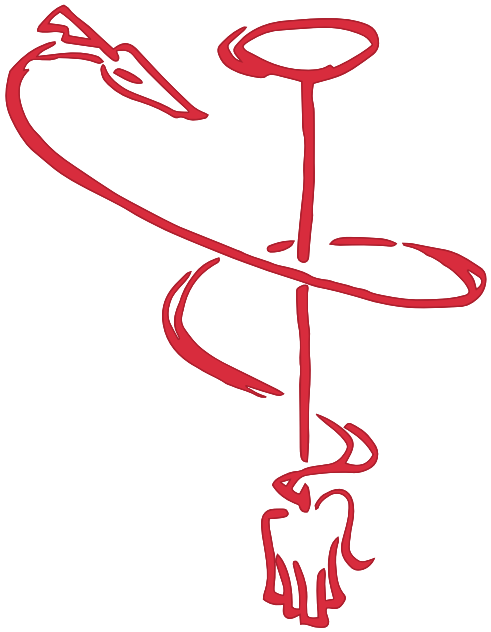
Prof. Jake MacMillan FRS

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Doctor of Philosophy in the Faculty of Science.

Word count: 44662

April 2020





Abstract

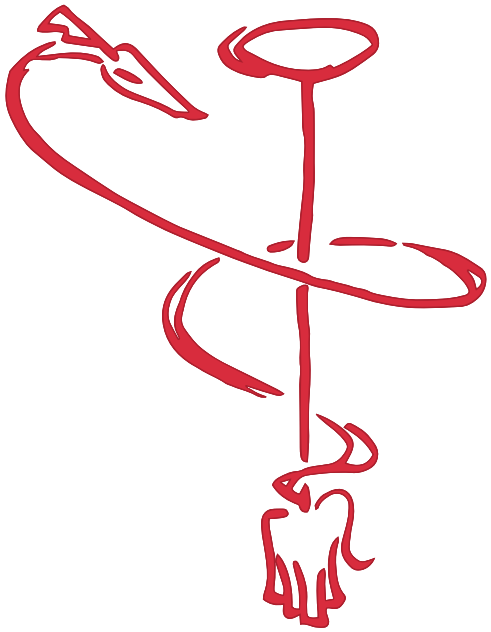
Technology founded in quantum phenomena is set to revolutionise computation, sensing and communication. With an entirely different method of manipulating information, quantum computers in particular are able to offer significant advances when compared to their classical counterparts. Unrelenting research throughout the world implies that such machines are set to be the demise of public-key cryptography that is critical to modern society.

Quantum key distribution (QKD) offers a method to securely distribute randomness between distant parties using the fundamental nature of the universe. Protocols do not depend on assumed hard problems and so the security of the key does not decrease as computing power increases. However, QKD systems have been susceptible to information leakage or hacks which compromises their security at the time of key exchange. As research demonstrations evolve into commercial systems, the security of a physical implementations must be addressed.

Device-independent protocols have since been introduced to relieve the possibility of secret information falling into the hands of an adversary. Using correlations between random events, the physical system does not contain any information about the key. Therefore, it is not susceptible to attacks or able to reveal the secret key. This simplifies the task of characterising a system to guarantee a secure key exchange.

Before QKD can be widely adopted, a cost-effective and scalable platform must be developed. In the last decade, photonic integration has been refined to facilitate circuit complexity simply not possible with bulk alternatives. The inherent robustness and phase-stability make it an excellent candidate for future quantum-secured networks.

This thesis will explore how integrated photonics can be deployed in device-independent QKD protocols to both ensure practical security and enhance network accessibility. We will show how integrated components can be used to generate quantum states with high fidelity and demonstrate quantum interference. The complexity of photonic integration will be explored to demonstrate new circuits for QKD that will eventually form the backbone of quantum-secured networks.



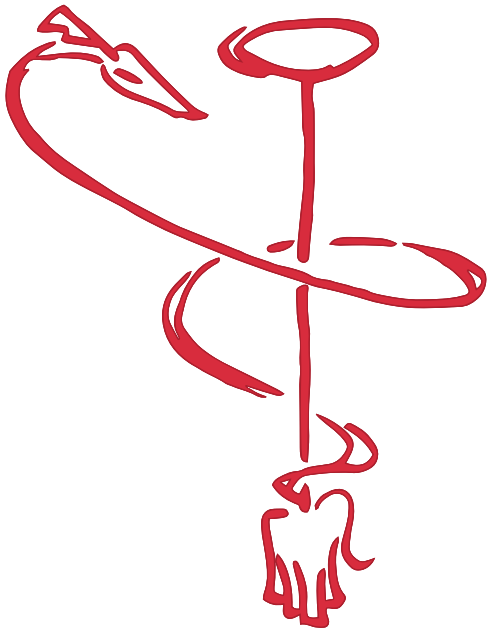
Acknowledgements

I would firstly like to thank Dr Chris Erven for his supervision and encouragement throughout my PhD and I am ever grateful to Dr Philip Sibson for his patience and Wikipedia-like knowledge. Thank you to Dr David Lowndes and Dr Alasdair Price for their (often not misguided) advice and Prof. John Rarity FRS for his endless inspiring tales. Thank you to Dr Djeylan Aktas, Dr Jorge Barreto, Friederike Jöhlinger, Dr Alasdair Price and Lawrence Rosenfeld for taking the time to proofread this thesis.

I am indebted to each and every member of QETLabs of which there are, unfortunately, far to many to name here. I am incredibly appreciative of the support from the ops team, past and present, without whom I would have never been able to achieved half of the things I was able to. In particular to Lorraine, Holly, Emma, Helen, Andrea, Lin and Rebecca.

Thank you to the whole of cohort 2, Alex, Dan, Geraint, Jason, Joe, Lawrence, Lucio, Martin and Sam, who have made this journey so memorable; to Dr. Milica Prokic and Neil Simmons for providing the artwork that has been used to decorate this thesis; to Dr Graham Marshall for your help despite my continual harassment; and to Andy Murray for his unrivalled technical knowledge.

Finally, I want to thank my family for their support, inspiration and for getting me here in one piece. Thank you to my friends for trying their best to make it more than one piece.



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: .....

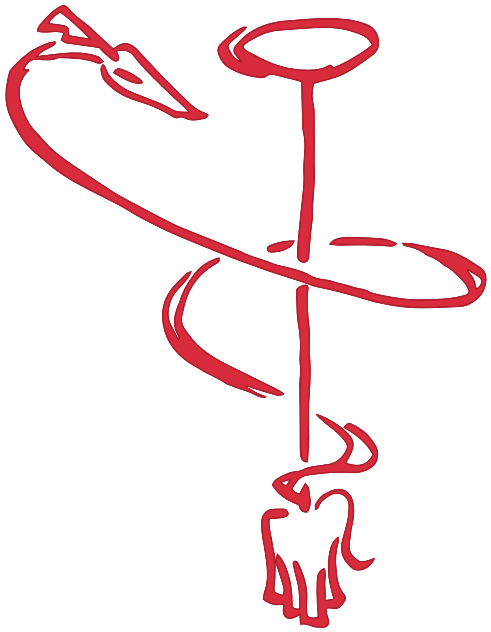
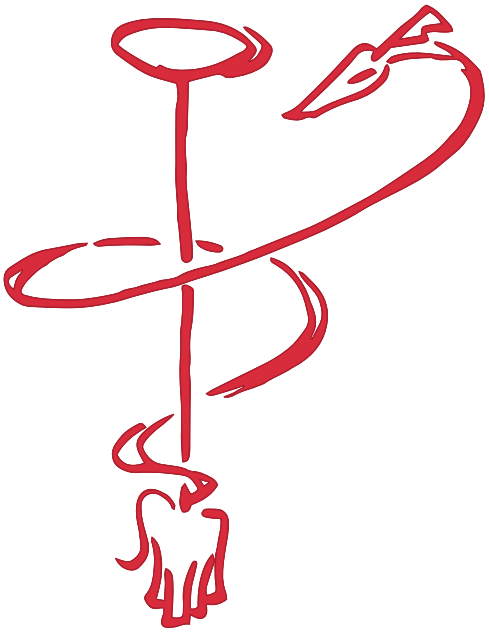
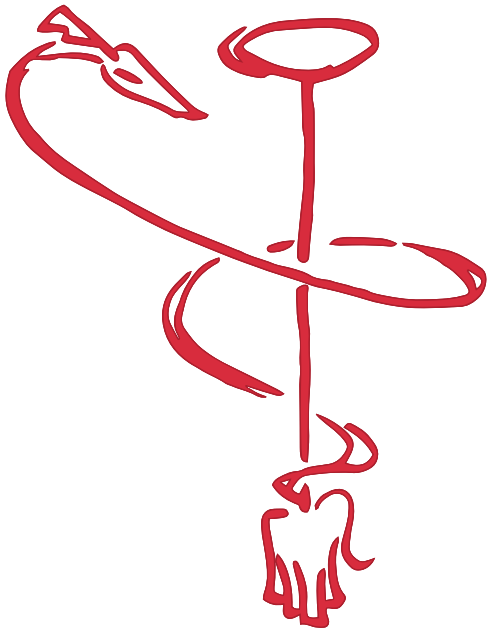


Table of Contents





List of Publications

Journals

H. Semenenko, P. Sibson, M. G. Thompson and C. Erven, "Interference between independent photonic integrated devices for quantum key distribution," *Opt. Lett. 44, 275-278*, Jan. 2019

H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity and C. Erven, "Chip-based measurement-device-independent quantum key distribution," *Optica*, vol. 7, Mar. 2020

Conferences

H. Semenenko, P. Sibson, A. Hart, M. G. Thompson and C. Erven, “Chip-based measurement-device-independent quantum key distribution,” *oral presentation*, QCrypt, Aug. 2019

H. Semenenko, P. Sibson, M. G. Thompson and C. Erven, “Integrated devices for measurement-device-independent quantum key distribution,” *oral presentation*, CLEO, Apr. 2019

P. Sibson, D. Lowndes, S. Frick, A. Price, H. Semenenko, F. Raffaelli, D. Llewellyn, J. Kennard, Y. Ou, F. Ntavou, E. Hugues Salas, A. Hart, R. Collins, A. Laing, C. Erven, R. Nejabati, D. Simeonidou, M. G. Thompson and J. G. Rarity, “Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol’s Activities in the UK Quantum Communications Hub,” *oral presentation given by P. Sibson*, QCrypt, Sep. 2017

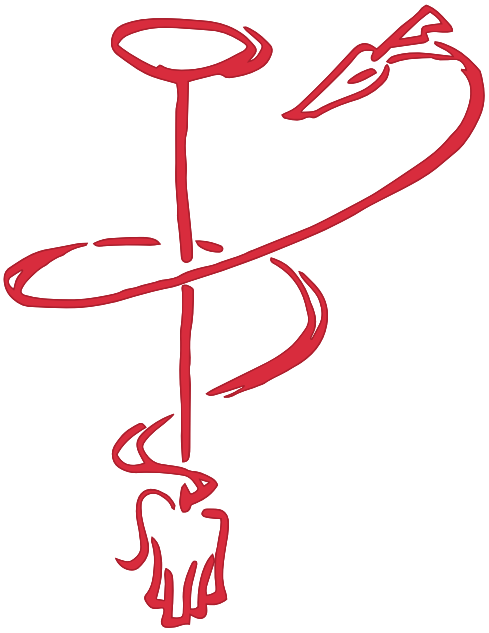
H. Semenenko, P. Sibson, J. Barreto and C. Erven, “Towards Accessible Metropolitan Quantum Secure Communication,” *oral presentation*, Young Quantum Information Scientist, Sep. 2017

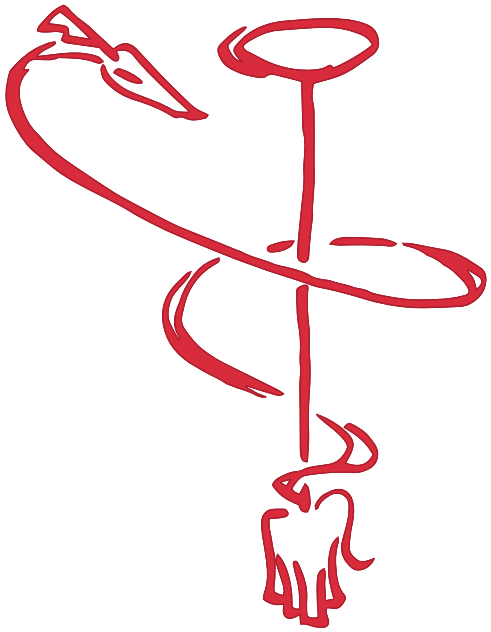
A. Vaquero-Stainer, R. A. Kirkwood, V. Burenkov, C. J. Chunnilall, A. G Sinclair, A. Hart, H. Semenenko, P. Sibson, C. Erven and M. G. Thompson, “Measurements towards providing security assurance for a chip-scale QKD system,” *oral presentation given by A. Vaquero-Stainer*, Proc. SPIE 10674, Quantum Technologies, May 2018

H. Semenenko, P. Sibson, M. G. Thompson and C. Erven, "Integrated Photonic Devices for Measurement-Device-Independent Quantum Key Distribution," *poster*, QCrypt, Aug. 2018

A. Hart, H. Semenenko, S. Frick, C. Erven, D. Lowndes, P. Sibson, M. Thompson and J. G. Rarity, "Small Form Factor, Low Cost Electronics for Chip Scale and Handheld Quantum Key Distribution Systems," *poster*, QCrypt, Aug. 2018

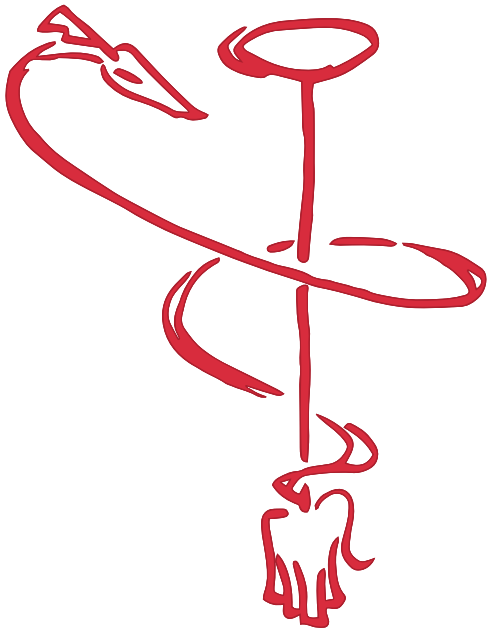
D. V. Aktas, P. Sibson, D. Lowndes, S. Frick, A. Price, H. Semenenko, F. Raffaelli, D. Llewellyn, J. Kennard, Y. Ou, F. Ntavou, E. Hugues Salas, A. Hart, R. Collins, A. Laing, C. Erven, R. Nejabati, D. Simeonidou, M. G. Thompson and J. G. Rarity, "A Metropolitan Quantum Network with Hand-Held and Integrated Devices," *poster presentation given by D. V. Aktas*, GDR IQFA, Nov. 2018





List of Tables

List of Figures

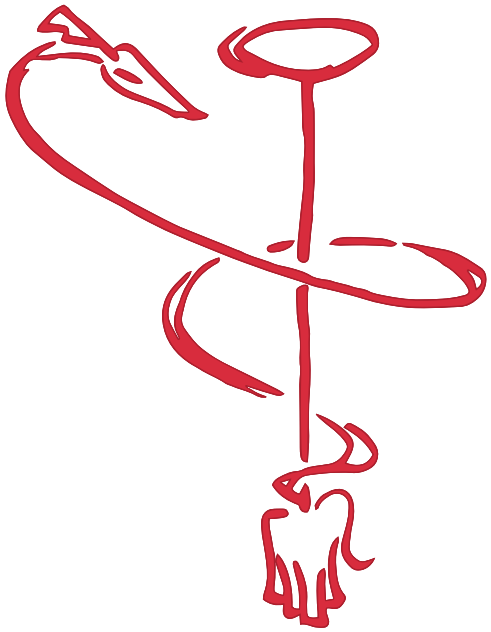


List of Abbreviations and Acronyms

3DES	Triple data encryption standard
AES	Advanced encryption standard
aMZI	Asymmetric Mach-Zehnder interferometer
APD	Avalanche photodiode
ASIC	Application-specific integrated circuit
AWG	Arbitrary waveform generator
BB84	Bennett-Brassard 1984
BS	Beam splitter
CB-CPW	Conductor-backed coplanar waveguide
CI-PM	Current-injection phase modulator
CMOS	Complementary metal-oxide-semiconductor
COW	Coherent-one-way
CPW	Coplanar waveguide
CV-QKD	Continuous-variable QKD
CW	Continuous wave
DBR	Distributed Bragg reflector
DC	Direct current
DES	Data encryption standard
DFB	Distributed feedback
DI-QKD	Device-independent QKD
DPR-QKD	Distributed-phase-reference QKD
DPS	Differential-phase-shift
DV-QKD	Discrete-variable QKD
DWDM	Dense wavelength-division multiplexing
E91	Ekert 1991

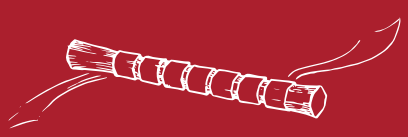
ENIG	Electroless nickel immersion gold
EOPM	Electro-optic phase modulator
ETSI	European Telecommunication Standards Institute
FFC	Flexible flat cable
FPGA	Field-programmable gate array
FWHM	Full width at half maximum
GCHQ	The Government Communications Headquarters
GCPW	Grounded coplanar waveguide
HHI	Heinrich Hertz Institute
HOM	Hong-Ou-Mandel
IMOS	Indium phosphide membrane on silicon
InP	Indium phosphide
ISI	Inter-symbol interference
MDI-QKD	Measurement-device-independent QKD
MitM	Man-in-the-middle
MMI	Multi-mode interferometer
MQW	Multi quantum well
MZI	Mach-Zehnder interferometer
NbTiN	Niobium-titanium-nitride
NIST	The National Institute of Standards and Technology
NPL	The National Physical Laboratories
NSA	National Security Agency
OSA	Optical spectrum analyser
OTP	One-time pad
PBS	Polarising beam splitter
PC	Polarisation controller
PCB	Printed circuit board
PD	Photodiode
PIC	Photonic integrated circuit
PLS	Pulsed laser seeding
PNS	Photon number splitting
PPG	Pulse pattern generator

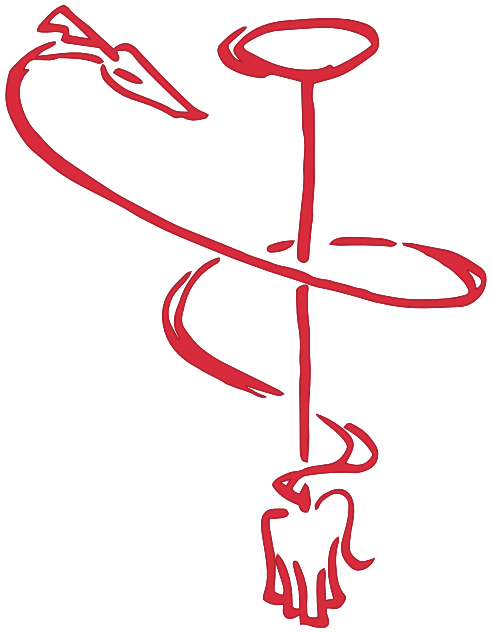
PRNG	Pseudo-random number generator
PVM	Projection valued measure
QCSE	Quantum-confined stark effect
QKD	Quantum key distribution
QRNG	Quantum random number generator
RF	Radio frequency
RSA	Rivest-Shamir-Adleman
SFWM	Spontaneous four-wave mixing
SNSPD	Superconducting nanowire single-photon detector
SOA	Semiconductor optical amplifier
SOI	Silicon-on-insulator
SPAD	Single-photon avalanche diode
SPD	Single-photon detector
SPDC	Spontaneous parametric down conversion
SSC	Spot-size converter
TE	Transverse electric
TM	Transverse magnetic
TOPM	Thermo-optic phase modulator
VGA	V-groove array
VOA	Variable optical attenuator
WCP	Weak coherent pulse
WCS	Weak coherent state
WDM	Wavelength-division multiplexing



1

Introduction





1.1 Foreword

The second quantum revolution is steadily progressing with no immediate sense of slowing. The prospect of a large scale quantum computing a no longer a pipe dream with small quantum computers available publicly online. The current scale of research focused on the field suggests that the question should not be *if* but rather *when*.

The promised benefits of quantum computing seem immeasurable, partly because the benefits have not been fully explored beyond a few applications. However, one well-known example threatens the future of modern secure communication [1]. With large scale quantum computing forthcoming [2], we must explore new methods of secure communication before such quantum algorithms become a reality.

Quantum key distribution (QKD) is one such attempt to securely distribute randomness which exploits quantum phenomena to create a secure key exchange based on nature [3, 4]. There are no assumptions of mathematically-hard problems meaning the security of the key doesn't decrease after the exchange. While there has been rapid progress from initial demonstrations into commercial systems, QKD has not been widely adopted. Cost aside, there are two factors that limit the progression of ubiquitous QKD systems: practical security and mass-manufacturability.

Recently, the claims of QKD security have come under pressure from the quantum hacking community. While the security is not based off mathematical assumptions, it is important that the physical system matches the performance that is predicted by the theory. It has been demonstrated that physical systems do not necessarily meet this requirement [5].

In an effort to reduce the characterisation required for the security of a key exchange, device-independent protocols were developed [6]. This has since inspired new protocols which are more practical with current technology. For example, measurement-device-independent QKD (MDI-QKD) removes all possible attacks against the detections system [7].

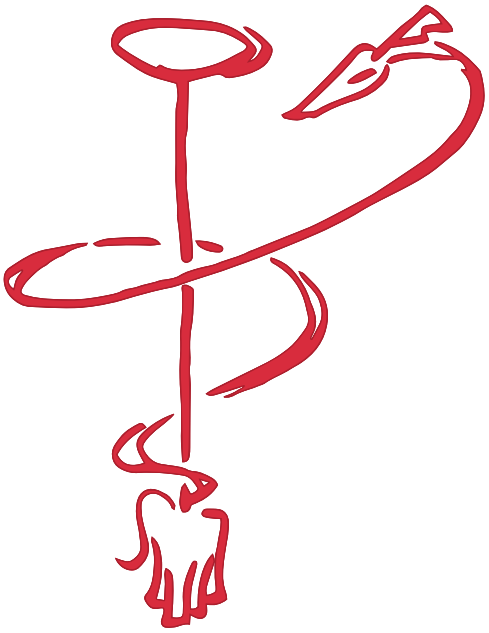
Following many successful demonstrations of quantum phenomena in laboratories, interest turned from fundamental science to quantum engineering. Robust platforms were required to scale the potential technologies for application outside the lab. Pioneering work in photonic integration has allowed a drastic increase in the level of complexity in quantum photonic experiments [8]. These platforms allow for entire QKD systems to be created from monolithic devices [9].

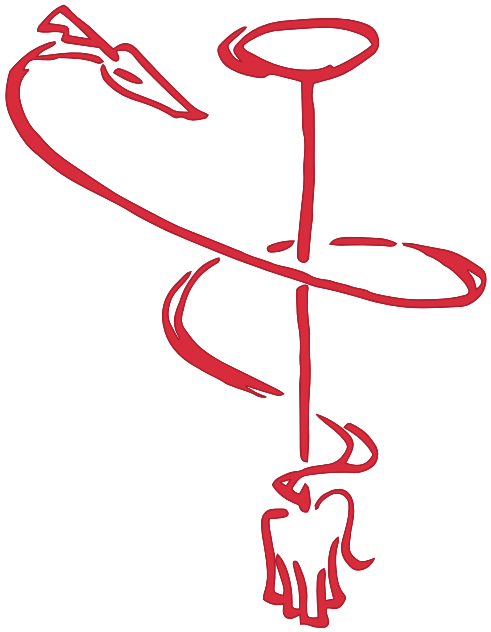
This thesis will explore the extension of the integrated photonic platform into new protocols which will simultaneously increase security and facilitate wide-scale quantum-secured networks. We will show how fine precision of integrated light sources allows for high-fidelity quantum interference. Potential security flaws in previous QKD demonstrations will be addressed and next-generation devices presented.

1.2 Outline

The outline of the remainder of this thesis is as follows:

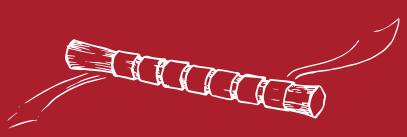
- Chapter 2 will introduce the general concepts required for the rest of the thesis. Cryptography will be put in context with advances that have been made over the last 4000 years which will end with the current state of modern protocols. Quantum information will be introduced starting with the foundations of quantum mechanics. The notion of quantum bits is discussed as well as key aspects that will be relevant for secure key exchange. Several different QKD protocols will be presented and the practical security of them discussed. Finally, the field of integrated photonics will be introduced and the essential building blocks will be described. Information encoding through quantum photonics will be reviewed and the different platforms for photonics integration will be compared.
- Chapter 3 presents the fundamental Hong-Ou-Mandel (HOM) interference effect and how it can be performed with integrated devices. The photonic chips will be introduced and their operation discussed. We will show how interference between independent devices can be achieved at 431 MHz. Finally, we will show how active-phase randomisation is achieved, which will be crucial for QKD devices.
- Chapter 4 builds on the HOM interference by demonstrating MDI-QKD which removes all potentially information leaks from the detection system. We will see how entirely integrated components can generate 250 MHz-clocked quantum states and distribute 1 kbps of key at 100 km. The security of the transmitters will be reviewed as well as the security trade-off for cost-effective electronics. Finally, we will see how developments in silicon photonics could enable a fully-integrated QKD system to further reduce cost and enable multi-user, metropolitan, quantum-secured networks.
- Chapter 5 explores new photonic integrated circuits (PICs) for QKD by using the ever-advancing integrated photonics platform. New methods of generating quantum states will be discussed. We will also introduce new integrated circuits that will simplify the electronics required for operation. We will show how photonic chips become devices through optical and electrical connections, as well as discussing the challenges.
- Chapter 6 concludes this thesis with a summary of the presented work. The importance of HOM interference and its place in QKD will be discussed. The importance of ensuring security in any key exchange system will be reviewed and how closing loopholes will be vital to the success of QKD. The integrated photonics platform, and the new devices presented in chapter 5, will be discussed in the larger context of future quantum networks.

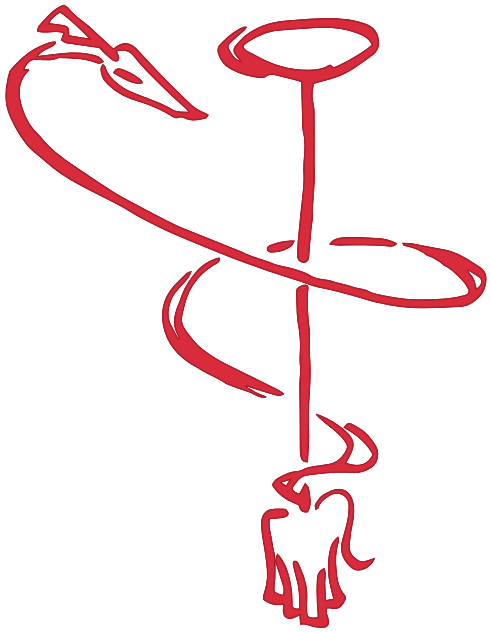




2

Background





2.1 Cast of Characters

Before we begin, we will need to introduce the cast of characters that will each have parts to play throughout this thesis. While the exact reasons behind each persons' role is unclear, we can be sure that they will follow their roles without question.

Alice, for reasons that we will not discuss here, would like to send a message to Bob. The particular message is unknown publicly and she would like it to remain as such. While she has never met Bob, she wants to make sure that the message is actually being sent to Bob. Often she will require to know that the message has reached Bob but will rarely seek any further response.

Bob wants to receive and also read the message from Alice, whom he has never met, whilst also being sure that the message is, in fact, from Alice. He also wants to ensure that the message he received is a faithful representation of the one Alice sent and has not been modified along the way. Bob is not very talkative and doesn't often respond to messages from Alice.

Charlie is a mutual acquaintance of Alice and Bob (despite having never met either of them) who volunteers to act as a mediator for their communication. His specific role will depend on exactly how Alice and Bob are communicating and he is often not required beyond moral support. While he is not actively trying to sabotage Alice and Bob's communication, neither is he actively protecting them.

Eve is a very nosey individual who listens to all public communication between Alice and Bob. She is intent on reading the message sent by Alice but while very persistent, she is not very inventive so will not put very much effort into deciphering the message. Eve is often mistaken as Mallory, as they have similar intents.

Mallory would also like to know what Alice has sent to Bob, but will go to more extreme measures to discover their secrets. She is particularly fortunate in having unlimited resources available (confined only by the laws of physics) and will use all possible methods within her power to expose the hidden message. Her motivations are unknown.

The reader is encouraged to picture their own cast of characters in their mind's eye to bring this thesis to life. Any likeness of characters to any persons, real or imaginary, is purely coincidental.

2.2 Cryptography

Elements of cryptography date back almost 4000 years to Ancient Egyptian times where unusual hieroglyphs were found to have been added to potential shroud mystery over the meaning [10]. While generally not considered a serious attempt at hiding any secret message (and therefore considered steganography) such concepts of concealment are fundamental in modern cryptography.

It has been argued that cryptography was known to the Ancient Greeks. To incite a revolt against the Persians around 440 BC, Histiæus was said to shave the head of his most trusted slaves so that a tattooed message would be hidden by his regrown hair [11]. References were also made centuries later to a long stick called a scytale around the 3rd century BC [12]. Parchment was wound around the scytale and, in effect, created a transposition of the message which was then used in the Spartan military. While these were revolutionary for their time, they are not considered cryptographic as the message is merely hidden rather than encrypted.

To better define whether a system can be classified a cryptography, and truly distinguishable from steganography, we must fast-forward to the 19th century. Systems designed at hiding messages, but not necessarily encrypting them, were commonplace. Auguste Kerckhoffs presented a set of six principles that any cryptographic system should satisfy [13]. While technological advances have superseded some of the list, Kerckhoffs' principle remains. It is succinctly summarised as

"The enemy knows the system" - Claude Shannon [14]

Any cryptographic system should remain secure without requiring secrecy of the underlying protocol. Alice and Bob should assume that Eve and Mallory have a copy of their system when considering its security. Only the *key* will remain secret to Alice and Bob. Of course, we will see that the definition of "secure" will change depending on the context to mean *practically* or *mathematically* indecipherable.

This section will introduce some of the important advances in cryptographic history. We will discuss how the modest origins of classical cryptography will become a crucial part of society and how cryptography may have even altered the course of history.

2.2.1 Symmetric-Key Cryptography

The first algorithms used for cryptography were so called symmetric-key algorithms. Alice and Bob initially decide on a shared key. Historically, these keys would have been shared in person, although technological advances have allowed these keys to be shared from a distance. The shared key can be used by Alice and Bob to both encrypt and decrypt the message, but the exact transformation for encryption or decryption may differ.

2.2.1.1 Monoalphabetic Ciphers

The most basic ciphers are those that are simple permutations of the alphabet. These are known as monoalphabetic ciphers. The symmetric key in these ciphers is the permutation used, that can be as simple as a single number. Here, we will introduce a couple of simple examples of monoalphabetic ciphers.

Caesar Cipher

One well-known example of cryptography in history was used by the Romans and is now referred to as the Caesar cipher. According to Seutonius, Julius Caesar used this simple cipher to communicate important messages to his generals [15].

Each letter of the alphabet is assigned a numeric value i.e. 'a' = 0, 'b' = 1, etc. and Alice and Bob agree a key $k \in \mathbb{Z}_{26}$ which they keep secret. When Alice wants to send a message, she converts her message into a number and systematically 'adds' the secret key, k, to each of the letters, modulo 26. Caesar was reported to use $k = 3$, which would give the encoding

Plain:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

where the Alice finds the letter of her plain text in the top row and substitutes it with the cipher text in the bottom row. Eve and Mallory would not be able to make out the works without the secret key.

Once Bob receives the message from Alice, he can decipher the message by 'subtracting' k from the message i.e. moving from the bottom row of the table above to the top row. This allows him to read the message.

In an era where most people would have been illiterate, the cipher was likely to be secure. However, with only 25 possible combinations to try, guessing each permutation is rather trivial. Once a single word has been uncovered the entire message would be forfeit.

Affine Cipher

A slightly more complex monoalphabetic permutation comes from the affine cipher, although it seems to be confined more for academic interest than real world use. The cipher is still a simple permutation of the alphabet but Alice and Bob now share two numbers. They agree on two integers $k, \lambda \in \mathbb{Z}_{26}$ such that λ is coprime to k i.e. they have no common factors greater than 1. For each letter, x, we can encrypt using the mapping

$$x \to \lambda \cdot x + k \pmod{26} \tag{2.1}$$

where the decryption requires the inverse of λ. For example, using $k = 3$ and $\lambda = 7$, we get the mapping

Plain:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher:	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W

which seems more 'random' than the Caesar cipher. However, the cipher still only relies on two numbers to encrypt and decrypt. Eve or Mallory may just guess two of the mappings which

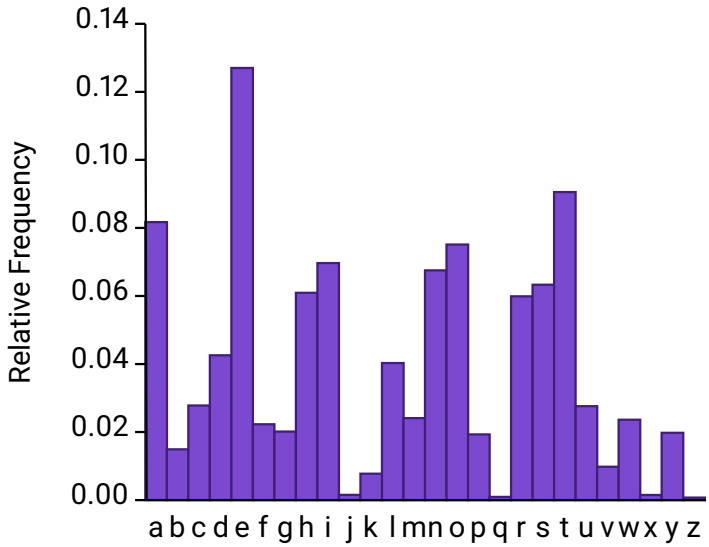


Figure 2.1: A histogram of the relative letter frequency in the English language which can be used to break monoalphabetic ciphers.

allows them to decipher the entire message. Alternatively, as the cipher contains only $12 \cdot 26$ possible combinations, Mallory could easily perform a brute force attack.

Frequency Analysis

With ciphers being commonly used, interest turned to analysing cipher text. In the case of a monoalphabetic cipher, Mallory can consider the relative frequency of the letters. Figure 2.1 shows a histogram of the letters used in the English language. One finds that the letter ‘e‘ is the most common, while letter such as ‘j’, ‘q’, ‘x’ and ‘z‘ are rarely used.

If Mallory knows that the cipher being used is a monoalphabetic one (which we will assume from Kerckhoffs’ principle) then they can calculate the letter frequency of the message. By matching the most used letters in the cipher text to the letter frequency, they may be able to decode the message.

In more complex analysis, one can even consider the frequency of letters at the beginning or ends of words, and also the frequency of two or three letter fragments. Once parts of the cipher text have been decrypted, it will usually be sufficient to recover the rest.

2.2.1.2 Polyalphabetic Ciphers

Since the invention of the Caesar cipher in Roman times, there were not many advances in encryption until the 15th century. Up until this point, encryption methods generally used simple substitutions or permutations. The next evolution was to develop polyalphabetic ciphers where each letter was encrypted (and decrypted) using a different permutation of the alphabet. Essentially, they were a collection of monoalphabetic ciphers used in a particular order.

Vigenère Cipher

This cipher was originally developed by Giovan Battista Bellaso in 1553 [16] but is attributed to Blaise de Vigenère [17]. The cipher was believed for a long time to be unbreakable as it was not initially clear how frequency analysis techniques could be adjusted for the multiple permutations.

The cipher introduces a word or phrase shared by Alice and Bob which is used as the key. The keyword is repeated to match the length of the message and each letter represents its own Caesar cipher. For example, Alice and Bob may choose to share the keyword 'photon' in which case they would encrypt as

Plain:	`wewillbuildaquantumcomputerbytheendofthisdecade`
Keyword:	`photonphotonphotonphotonphotonphotonphotonphoto`
Cipher:	`LLKBZYQBWERNFBOGHHBJCFDHILFUMGWLSGRBUAVBGQTJOWS`

where decryption is the reverse and each letter is 'subtracted' from the message.

If the message is long enough, then the problem can be reduced to analysing k individual Caesar ciphers, where k is the length of the keyword. However, this requires Eve or Mallory to know the length of the keyword. Therefore, they need a method of calculating k.

A method introduced by William F. Friedman considered the comparing the cipher text with a shifted version of itself. To understand how this might work, consider compare two passages of text with one shifted relative to the other. How often would we expect the letters between the two to match? For example,

```
        l       u                              de
wewillbuildaquantumcomputerbytheendofthisdecadeusingtodaystools
    wewillbuildaquantumcomputerbytheendofthisdecadeusingtodaystools
```

where the second message has been shifted by four letters. The letters that match between the two texts are highlighted above in red. In this example, we found 4 out of 63 letters match (6.3 %). How often should we expect this to happen?

Considering the frequencies of each letters, as shown in figure 2.1, we can calculate the probability as

$$P(\mathrm{id}) = p_{\mathsf{a}}^2 + p_{\mathsf{b}}^2 + \cdots + p_{\mathsf{z}}^2 \approx 0.0655 \tag{2.2}$$

where the 'id' refers to the fact that the messages were both written with the same alphabet.

Suppose we were to instead compare two messages which had a different encoding, for example the plain text message with a monoalphabetic cipher text. Let us denote a monoalphabetic encoding of the alphabet as $\pi(i)$ which is acts on the ith letter. We then like to calculate

$$P(\pi) = \sum_{\text{'a'}}^{\text{'z'}} p_i \cdot p_{\pi(i)} \tag{2.3}$$

In general, the probability of coincidence will *always* be less when comparing two different encodings. For any non-trivial permutation π,

$$P(\mathrm{id}) - P(\pi) = \sum p_i^2 - \sum p_i \cdot p_{\pi(i)} \tag{2.4}$$

$$= \frac{1}{2}\left(\sum p_i^2 + \sum p_{\pi(i)}^2\right) - \sum p_i \cdot p_{\pi(i)} \tag{2.5}$$

$$= \frac{1}{2}\sum (p_i - p_{\pi(i)})^2 > 0 \tag{2.6}$$

On average, we would expect a match probability of around 1⁄26 ≈3.85 %. To apply this to the Vigenère cipher, one simply needs to compare the cipher text with a shifted version of itself. The probability of coincidence will be maximised when the text is shifted by a multiple of the keyword length. Once the length of the keyword has been discovered, the problem reduces to analysing multiple Caesar ciphers. Frequency analysis can be applied to break each individually and recover the plain text from the cipher text.

One-Time Pad

The one-time pad (OTP) is a polyalphabetic cipher where the key is made as long as the message and every message is encrypted with a unique and random key. It was initial described in 1882 by Frank Miller [18] but it wasn't widely recognised until 1919 when a Gilbert Vernam patented a method to combine the message and key on punched-tape [19]. In the patent, the tape that stored the key was reused after a full cycle. It was later realised that if the key was completely random and not reused then "the messages are rendered entirely secret" [20].

Typically, the OTP is concerned with bit level operations where encrypting and decrypting are both performed with addition modulo 2. Consider that the message, m, can be represented as a bit string $m_1 m_2 \dots m_k$, and similarly for the key and cipher text, then encrypting the message is simply

$$c_i = m_i + k_i \pmod 2 \tag{2.7}$$

where k_i are the bits that represent the key which is of the same length as the message and c_i is the cipher text bit. Equivalently, decryption is

$$m_i = c_i + k_i \pmod 2 \tag{2.8}$$

Since each letter is encrypted with a random monoalphabetic cipher, there is no way to perform frequency analysis. Likewise, the general cryptanalysis used for the Vigenère cipher will provide no information as there is no repetition in the key.

Providing that the key is chosen randomly and not reused, the OTP can be proven to be information-theoretic secure [14]. That is to say that even Mallory, with her unlimited power, would not be able to comprise the message without the secret key. Intuitively, as the key is completely random, each decryption is equally likely so there is no way to reveal the true message.

While the protocol itself provides a 'perfect' method of encryption, this doesn't exclude physical vulnerabilities in the system. Information may be leaked through side-channels in specific system implementations. Alice and Bob also have to overcome the problem of securely distributing the keys.

2.2.1.3 Block Ciphers

Despite the inherent security provided by the OTP, it is rarely used in practice. Challenges with key exchange render it impractical as Alice and Bob must have keys that are as long as the message itself. Methods to exchange these keys remain slow meaning that, typically, the theoretical security of a system is relaxed in favour of practicality.

The most used encryption methods in modern communication are block ciphers that were introduced by Horst Feistel [21]. Instead of considering the message as individual letters (or binary bits), a block cipher will consider the message in blocks of a certain length. These blocks are the passed through a deterministic algorithm that encrypts the message with a short key. The exact length of the block will depend on the cipher being used, but is always shorter than the message meaning the security is weakened when compared with the OTP. However, as the data is encoded in vectors encryption and decryption can be performed by matrix multiplication which is computationally efficient.

The message block is split into two equal parts v and w which are encoded in the first round using

$$v' = w \quad \text{and} \quad w' = v + F(w, k) \tag{2.9}$$

where F is a vector-valued function and k is the key. The key is then modified to generate a subkey in which the process above is repeated with v, w and k replaced by v', w' and k'. The

function F and the method of generating the subkeys is depending on the block cipher being used. This process is easily reverse by

$$w = v' \quad \text{and} \quad v = w' + F(v', k) \tag{2.10}$$

The first widely used block cipher was data encryption standard (DES) introduced in 1977 [22] and was based mostly on Feistel's idea. The algorithm uses a key length of 56 bits and separates the data into 64 bit blocks which are divided into two vectors, v and w, each of length 32 bits. The vector-valued function for DES is described in algorithm 2.1 which is repeated for 16 rounds.

Algorithm 2.1: Data Encryption Standard

1. w is expanded from 32 bits to 48 bits by repeating certain bits.
2. The key, k, is divided into two separate 28-bit keys.
3. In each successive round, the two keys are shifted by one or two bits depending on the round.
4. 24 bits from each key are selected to create a 48-bit subkey which is added to the expanded vector, w.
5. Each block is separated into eight six-bit sections which are substituted with four-bit outputs from a lookup table. This transformation is non-linear.
6. Finally, the 32 outputs are permuted by a fixed mapping.

Immediately following the release of DES, there was scrutiny concerning the involvement of the National Security Agency (NSA) and the short length of the key. It was suggested that a machine could be built at the cost of only $20 million which could break DES in a day [23]. Despite these concerns, DES remained a standard until 2001. At which point, a number of brute-force attacks had been demonstrated, notably by the Electronic Frontier Foundation.

DES was replaced by advanced encryption standard (AES) in 2001 [24] which was based on the same block cipher structure. The message is now split into 128 bit messages and secret keys of length 128, 192, or 256 bits available to prevent brute-force attacks. Block ciphers are not information-theoretic secure, as each bit of key is expanded and used to encrypted more than one bit of the message. It is believed that AES remains computationally secure. That is to say that it is not feasible to build a computer that can break an AES cipher in a reasonable amount of time.

2.2.2 Public-Key Cryptography

We have alluded to the challenges of distributing keys between Alice and Bob for use in a symmetric key algorithm. The obvious solution is for Alice and Bob to meet in person prior to their secret communication. However, it might not always be possible for them to meet and it certainly is not practical.

In order to exchange secret messages over insecure communication channels, public-key cryptography algorithms were developed. Alice and Bob act asymmetrically basing security from number theory problems are assumed hard. There has yet to be an algorithm that can claim with certainty to be even computationally secure.

Such problems employ trapdoors: functions that are easy to compute one way, but challenging to invert without secret information. Alice will use the function to encrypt, but only Bob has the secret information to decrypt the message. As the name suggests, Bob will publicly announce certain information which Alice (or anyone else for that matter) can use to encrypt a message. However, he keeps a private key which will allow him to decrypt the messages.

This section will introduce two public-key algorithms that are widely used. While the algorithms can be used as a method to send messages, the computational intensity of encryption and decryption means that they are typically used to distribute keys. These keys are then used in a symmetric key algorithm such as AES.

Diffie-Hellman Algorithm

The first public-key cryptography algorithm was proposed by Whitfield Diffie and Martin Hellman in 1976 [25]. It was later revealed that researchers at the Government Communications Headquarters (GCHQ) had previously demonstrated that such a protocol was possible [26,27].

The security of the protocol is based on the hardness of the discrete logarithm problem. The problem is to find $k = \log_a(b)$ given a prime number, p, and integers $1 < a < p$ and b, such that

$$a^k = b \pmod{p} \tag{2.11}$$

There is no publicly known classical algorithm that can efficiently compute the discrete logarithm. However, an algorithm was presented by Peter Shor in 1994 that uses a quantum algorithm to solve the discrete logarithm in polynomial time [1].

The Diffie-Hellman algorithm is not used to send a message between Alice and Bob, but instead is used to establish a key between them. This key can then be used in a symmetric key algorithm. The protocol is presented in algorithm 2.2.

Algorithm 2.2: Diffie-Hellman Key Exchange

1. Alice and Bob agree on a large prime number, p, and a primitive root, a. These numbers can be publicly available.
2. They both also secretly choose integers d_A and $d_B \in \mathbb{N}$.
3. Alice sends her public key, $q_A = a^{d_A}$, to Bob, and Bob send his public key, $q_B = a^{d_B}$ to Alice.
4. On receiving a public key, Alice and Bob compute $k = q_B^{d_A} = a^{d_A \times d_B}$ and $k = q_A^{d_B} = a^{d_A \times d_B}$, respectively.
5. Alice and Bob now share the secret key k.

The information that is available to Eve or Mallory are the numbers p, a, q_A and q_B. However, without being able to solve the discrete logarithm, they are unable to compute d_A or d_B. Hence, they cannot efficiently compute the secret key k.

Now that Alice and Bob share a secret key k, they can choose a symmetric key algorithm, such as AES, to send encrypted messages.

RSA Algorithm

Two years later, the Rivest-Shamir-Adleman (RSA) algorithm would be released publicly, named after its inventors [28]. As with the Diffie-Hellman algorithm, it was later discovered that the RSA method had been known by Clifford Cocks during his time at GCHQ [29].

Unlike the Diffie-Hellman algorithm, the RSA algorithm allows Alice to send a predetermined message to Bob. Its security relies on the hardness of factoring semi-primes: a number that is the product of two prime numbers. The RSA algorithm is given below.

Algorithm 2.3: Rivest-Shamir-Adleman Key Exchange

1. Bob needs to first choose a secret key. He selects two large prime numbers, p and q, and calculates $n = p \times q$.
2. He then chooses some $d < (p-1)(q-1)$ which is coprime to $(p-1)(q-1)$.
3. Finally, Bob calculates the inverse, e, of d modulo $(p-1)(q-1)$ and publishes the public key N and e whilst keeping p, q and d private.
4. Alice breaks her message into integers $m < N$ and encrypts as $c =$

$m^d \pmod N$. The ciphertext c can now be sent to Bob.

5. To decrypt Alice's message, Bob computes c^d and the communication is complete.

To prove that the decoded message is equivalent to the original message, we note that

$$b \equiv c^d \equiv m^{d \cdot e} \pmod N \tag{2.12}$$

and as e is the inverse of d modulo $(p-1)(q-1)$, we have

$$d \cdot e = t \cdot (p-1)(q-1) + 1 \tag{2.13}$$

for $t \in \mathbb{Z}$. If m and p are coprime, then Fermat's little theorem states that

$$m^{p-1} \equiv 1 \pmod p \tag{2.14}$$

from which, we find

$$b \equiv m^{t \cdot (p-1)(q-1)+1} \equiv m \cdot (m^{p-1})^{t \cdot (q-1)} \equiv m \pmod p \tag{2.15}$$

If p is not coprime to m, then p divides m and also b. Therefore, $b \equiv m \pmod p$ which can be equivalently reasoned for q. Since b and m were taken modulo N, we must have that $b \equiv m \pmod N$.

Generating keys for the RSA algorithm uses computationally efficient algorithm to check for primality and fast modular exponentiation. However, there is no method at the present to break the cipher without factoring N.

Interestingly, while this outlines the underlying concepts, the algorithm as it stands is not secure. As the algorithm is deterministic, Mallory can produce the cipher text of any plain text message. They can compare these to the cipher text of the message being sent from Alice to Bob. To protect against this attack, Alice introduces some random bits into the message, m, through a method called padding [30].

2.2.3 Authentication

We have described how Alice can send a message to Bob without having ever met to share a secret key by using public-key cryptography. How can she be sure that the public key that she is using to encrypt her message was actually *Bob's* public key? Without being sure, they can fall foul to a man-in-the-middle (MitM) attack.

As Mallory is aware of the protocol that Alice and Bob are using (again referring to Kerckhoffs' principle) she can appear to Bob to Alice and, likewise, appear as Alice to Bob. By

providing a public key to Alice and using Bob's public key to establish a secure communication, Mallory can take full control of the protocol.

Alice will encrypt a message, that is intended for Bob, with Mallory's public key who is able to decrypt the message into plain text. Mallory can then re-encrypt the message using Bob's public key and send it to him. Without authentication neither Alice or Bob will know that their message was compromised.

For Bob to verify that the message came from Alice, they will use an authentication protocol. This is typically achieved using a pre-shared key between Alice and Bob from which then can create an authentication tag to send alongside their message. Specific authentication protocols are beyond the scope of this thesis. However, we will note that their importance in modern communication is paramount and remains a prevalent discussion for the future of cryptography.

2.2.4 Post-Quantum Cryptography

In light of recent advances in quantum computing architectures [2], it is becoming more realistic that current public-key cryptography will become vulnerable to Shor's algorithm [1] in the near future. To counter these advances, post-quantum algorithms have been suggested as alternatives that will remain secure even against quantum computers. These algorithms use the same classical computers and networks, but are based on different problems. These algorithms are part of quantum-safe cryptography.

Since November 2017, The National Institute of Standards and Technology (NIST) has been developing a new public standard for post-quantum algorithms. The process invited protocols to be submitted for assessment. In total 82 candidates were submitted, of which 69 were accepted as the first round candidates [31]. Finalists are expected to be selected in 2020.

Proving the security of an algorithm remains challenging, particularly against quantum computers. A recent algorithm, *Soliloquy*, was a lattice-based algorithm created by researchers at GCHQ. After a brief development between 2010 and 2013, a quantum algorithm was discovered that would efficiently break the cipher. The story was published as a cautionary tale for future algorithms. A paper from Peter Shor that claimed to efficiently break lattice-based cryptography was quickly withdrawn following a mistake [32]. Such developments demonstrate the rapidly changing landscape of cryptography.

2.2.5 Cryptanalysis

Cryptanalysis aims to test the integrity of a cryptographic system and find weaknesses. This may be to analyse the mathematical problems which form the basis of the security of an algorithm or it may be testing the physical implementation. Successful cryptanalysis has been

performed throughout history, mainly motivated through war, and may have even changed the course of history.

A notable example of cryptanalysis was during WWI in the form of the Zimmermann telegram [33]. The message, intended to form an alliance between Germany and Mexico, was intercepted and deciphered by British intelligence. The United States, who were neutral at the time, joined the war three months later.

The most well known example of cryptanalysis was in Bletchley Park during the second world war. Hut 8 was specifically designated to analysis the enigma machine that was being used by the Axis powers [34]. The team used *cribs*, plain text that was suspected to be in a cipher text, with great success to break enigma codes. Such messages included "nothing to report" and physical intervention was even used to force the German Navy to send cribs [34]. This work eventually led to Turning developing the first computer from the Polish Bombes.

2.3 Quantum Information

From a thorough understanding of quantum mechanics came the new field of quantum information. Using fundamental particles, it was suggested that information could be encoded in a completely new way [35, 36]. This section will give a brief introduction to quantum mechanics theory and how it can be used to encode information. Some fundamental aspects will be discussed including a brief digression into quantum computing.

2.3.1 Quantum Mechanics

The postulates of quantum mechanics are not quite axiomatic, but rather guidelines for developing a more comprehensive framework for a particular system. The postulates are what connects the mathematical framework of quantum mechanics to physical systems.

Postulate 1: The State Space

The first postulate concerns the state of the system. Any closed quantum system exists in a Hilbert space, $\mathcal{H}$, which is known as the state space of the system. The system is described by a vector of unit length within $\mathcal{H}$. Any vectors that differ by a global factor represent the same state.

Of course, the postulate doesn't tell us which Hilbert space to choose for our particular quantum system. Nor does it give the vector associated with our quantum state. To answer such questions, one must consult theories such as quantum electrodynamics. The simplest spaces and states are those found in quantum information which is restricted to two-level systems. These states are called qubits and take the general form

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.16}$$

where $|0\rangle$ and $|1\rangle$ form an orthonormal basis with the Hilbert space and are called the computational basis. α and β are complex numbers which satisfy $|\alpha|^2 + |\beta|^2 = 1$ so that the state has unit length.

Postulate 2: Quantum State Evolution

Evolution of a closed quantum system is described by the second postulate. It states that quantum states evolve through unitary transformations. The state at some time t_2 is related to the state at an earlier time t_1 by a unitary operator i.e.

$$|\psi_{t_2}\rangle = \hat{U}\,|\psi_{t_1}\rangle \tag{2.17}$$

When one is concerned with the time evolution of a quantum system, it is described by the Shrödinger equation,

$$i\hbar\frac{\mathrm{d}\,|\psi\rangle}{\mathrm{d}t} = \hat{H}\,|\psi\rangle \tag{2.18}$$

where $\hbar$ is Plank's reduced constant and $\hat{H}$ is the Hamiltonian of the system. If the Hamiltonian of a system is known, then we can completely describe its dynamics. The Hamiltonian is a Hermitian operator meaning that the unitary transformation is given by

$$\hat{U} = \mathrm{e}^{-i(t_2-t_1)\hat{H}/\hbar} \tag{2.19}$$

Postulate 3: Measurement of the State

Contrary to classical systems, where the state can be measured with arbitrary accuracy, quantum mechanics places inherent restrictions on the accuracy of measurements. Before describing the measurement process, we will introduce observables. Physical quantities in a quantum system are given by the observables which are a self-adjoint operators on $\mathcal{H}$. The spectral theorem gives a decomposition of a d-dimensional observable $\hat{A}$ as

$$\hat{A} = \sum_{i=1}^{d} \lambda_i\,|e_i\rangle\,\langle e_i| = \sum_{i=1}^{d} \lambda_i \hat{P}_{\lambda_i} \tag{2.20}$$

where the eigenvectors are the set $\{|e_1\rangle, \ldots, |e_d\rangle\}$ associated with the eigenvalues $\{\lambda_1, \ldots, \lambda_d\}$. $\hat{P}_{\lambda_i}$ is the eigenprojector associated to the eigenvalue λ_i.

To describe measurements of a quantum state, we will introduce a projection valued measure (PVM) over a set $\{\lambda_1, \ldots, \lambda_n\}$. The PVM is given by a collection of projections $\{\hat{P}_{\lambda_1}, \ldots, \hat{P}_{\lambda_n}\}$ over the subsets of the Hilbert space $\mathcal{H}$ such that

1. The projections are orthogonal i.e. $\hat{P}_{\lambda_i}\hat{P}_{\lambda_j} = \delta_{ij}\hat{P}_{\lambda_i}$
2. The projections are complete i.e. $\sum_{i=1}^{n}\hat{P}_{\lambda_i} = \hat{\mathbb{I}}$

Measurements on a quantum system, $|\psi\rangle$ have outcomes $\{\lambda_1, \ldots, \lambda_N\}$ which are described by a PVM on the Hilbert space $\mathcal{H}$. The outcome of the projection is random with a probability distribution

$$P(\lambda_k) = |\hat{P}_{\lambda_k}|\psi\rangle|^2 = \langle\psi|\hat{P}_{\lambda_k}|\psi\rangle \tag{2.21}$$

Given that the outcome of the measurement was λ_k, the resulting state after normalisation will be

$$|\psi'\rangle = \frac{\hat{P}_{\lambda_k}|\psi\rangle}{|\hat{P}_{\lambda_k}|\psi\rangle|} \tag{2.22}$$

This postulate describes the inherent randomness in quantum mechanics. The amount of information that we can gain by measuring a quantum state or system is limited regardless of the precision of the measurement device. It also raises the question of how the state is disturbed during measurement. The measurement process gives rise to different interpretations of quantum mechanics which are beyond the scope of this thesis.

Postulate 4: Composite Systems

The final postulate allows us to describe systems that are made from more than one state. Any composite quantum states exist in a Hilbert space that is the tensor product of the Hilbert spaces of the individual states. If each of N states is prepared individually, the combined state is simply

$$|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_N\rangle \tag{2.23}$$

This postulate also applies to states that are not simply the product of individual states i.e. not *product* states. Such systems are called entangled states.

2.3.2 Quantum Bits and Entanglement

Similar to how information is represented as bits in classical computers, we can introduce the concept of a quantum bit, which we will call qubits. As mentioned above, qubits are two-level systems that exist in $\mathcal{H}_2$ where we introduce the orthonormal basis $|0\rangle$ and $|1\rangle$, called the computational basis. It is more usual to consider qubits in a Bloch representation,

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle \tag{2.24}$$

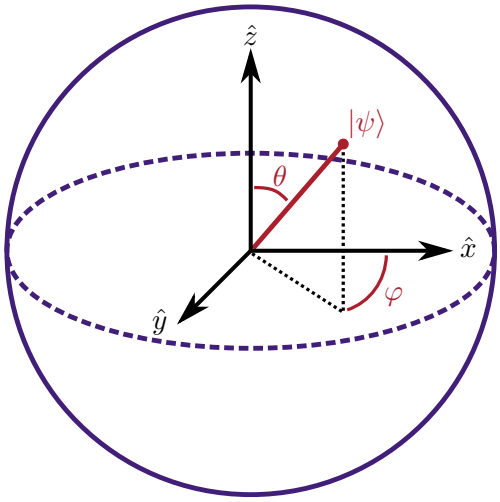


Figure 2.2: Bloch ball representation of the qubit state $|\psi\rangle$. We introduce the real variables $0 \leq \theta \leq \pi$ and $0 \leq \varphi < 2\pi$ where an unphysical global phase has been omitted.

where $0 \leq \theta \leq \pi$ and $0 \leq \varphi < 2\pi$ as shown in figure 2.2. Mathematically speaking, this representation is a closed ball, rather than a sphere which describes only the surface. The space bounded by a sphere gives a ball. Pure states exist on the surface on the ball, while mixed states exist within.

We introduce the Pauli matrices

$$\hat{x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.25}$$

which form the observables of qubits and are given in the computational basis.

As per postulate 4, we can form composite systems through the tensor product of individual qubits for form more complex systems. Given two qubits,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad \text{and} \quad |\phi\rangle = \delta\,|0\rangle + \gamma\,|1\rangle \tag{2.26}$$

that were prepared individually, the composite system is

$$|\psi\rangle\,|\phi\rangle = \alpha\delta\,|00\rangle + \alpha\gamma\,|01\rangle + \beta\delta\,|10\rangle + \beta\gamma\,|11\rangle \tag{2.27}$$

which exists in the Hilbert space $\mathcal{H}_4$. Equally, we could consider a state that was prepared in $\mathcal{H}_4$ that is not a product state. Then general form of such a state is

$$|\Psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \tag{2.28}$$

where we are only constrained by normalisation conditions that $|a|^2+|b|^2+|c|^2+|d|^2=1$. This allows us to introduce the states

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.29}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.30}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{2.31}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{2.32}$$

which are entangled and form the Bell basis. If we consider measuring the Bell states, perhaps in the computational basis, we will find the outcomes will be random but always exactly correlated. In fact, we would find that the outcomes would be correlated for any basis choice.

These states were first introduced in the seminal paper by Einstein, Podolsky and Rosen in 1935 [37], but it was Schrödinger who coined the term

> *"I would not call [entanglement] one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."*
>
> - Erwin Schrödinger [38]

It wasn't until 1964 that a method to test whether entanglement was non-classical was proposed by John Bell who placed a bound on correlations between systems [39]. From the theory proposed by Bell, Clauser, Horne, Shimony and Holt (CHSH) proposed an experiment in 1969 that would verify the theorem [40]. The CHSH inequality is given by

$$|S| \leq 2 \tag{2.33}$$

for

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b') \tag{2.34}$$

where E is the expectation value for $\{a, a'\}$ measurements on the first state and $\{b, b'\}$ on the second. This bound has been violated numerous times experimentally, most notably in 2015 when three separate experiments closed all loopholes [41–43].

2.3.2.1 Encoding

How $|0\rangle$ and $|1\rangle$ are encoded will depend on the physical system being used. Some notable examples of encoding are electron spins; nuclear spins; photon path, polarisation or timing;

and superconducting flux. Each has their own benefits and drawbacks and will be suited for different tasks in quantum information processing.

Of course, for quantum communication we will be interested in sending quantum information between distant parties, Alice and Bob. Light is already fundamental in modern communications networks. By considering single-photons, we can encode qubits that are compatible with much of the existing network architecture. These encodings will be discussed further in section 2.5.2.

2.3.3 No-Cloning Theorem

A fundamental theorem in quantum mechanics is the no-cloning theorem which will also underpin the security of quantum key distribution (QKD). The general principle of the theorem states that there is no physical process that copies, or clones, an arbitrary quantum state. We can state this more formally:

Theorem 2.1: No-Cloning Theorem

The no-cloning theorem states that there is no unitary transformation such that

$$\hat{U} |\psi\rangle |a\rangle = |\psi\rangle |\psi\rangle \tag{2.35}$$

for an arbitrary quantum state $|\psi\rangle$ and an ancillary quantum state $|a\rangle$.

Consider two arbitrary quantum states $|\psi\rangle$ and $|\phi\rangle$. Let us assume that there is a unitary that allows us to copy a quantum state

$$\hat{U} |\psi\rangle |a\rangle = |\psi\rangle |\psi\rangle \tag{2.36}$$

$$\hat{U} |\phi\rangle |a\rangle = |\phi\rangle |\phi\rangle \tag{2.37}$$

If we compare the overlap of the states on the left and right of the equation we find

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \tag{2.38}$$

which has two solutions. Either $\langle\psi|\phi\rangle = 0$ and the states are orthogonal or $\langle\psi|\phi\rangle = 1$ and the states are identical. Therefore, we cannot clone an *arbitrary* quantum state.

2.3.4 Quantum Computing

To motivate the introduction of quantum-safe communication, we will introduce some quantum computing algorithms. While the progression in quantum computing has played a large

part in the motivation of quantum-safe cryptography, it is not the only factor. However, an algorithm that will break modern cryptography provides a very tangible reason to replace public-key algorithms.

Shor's algorithm efficiently factors composite numbers into their prime factors [1] meaning that both RSA and Diffie-Hellman are vulnerable to attacks from a quantum computer. The estimated number of physical qubits needed to factor RSA-2048 has reduced drastically in recent years from one billion [44,45] to twenty million [46]. A state-of-the-art quantum processor was recently demonstrated with fifty qubits [2]. Another important metric is the circuit depth possible during a calculation. The quantum processor managed a circuit depth of 20 which is far below the estimated 10^9 required [47]. While this quantum computer is very far away from the estimates, it is a necessary first step towards ubiquitous quantum computers.

Grover's algorithm could also be used to search through keys in a block cipher protocol [48]. However, the speed-up is only $\sqrt{n}$ which has been proven as the lower bound for an unordered search [49]. Therefore, the same security in a post-quantum world can be achieved by doubling the key length i.e. moving from 128 bit to 256 bit AES.

2.4 Quantum Key Distribution

Quantum key distribution (QKD) is a fundamentally new method of key exchange by exploiting quantum mechanics to ensure security that is guaranteed by the laws of physics. It falls under the umbrella of quantum safe cryptography and, together with post-quantum cryptography, is likely to form a crucial part of future global networks.

Unlike the public-key protocols introduced in section 2.2, QKD does not rely on assumed computationally hard trapdoor functions. Instead, the security is based on the no-cloning theorem and, with minimal assumptions, can provide information-theoretic secure key exchange.

The concept for QKD was derived idea developed in the 1960's by Stephen Wiesner. However, this wouldn't be published until 1983 [50]. Through *conjugate coding* Wiesner developed two schemes. The first allowed Alice to send two messages to Bob, but Bob could only choose to read one message depending on his basis. Upon measurement, the other message would be destroyed.

The second idea allow uncounterfeitable money to be created based simply on the superposition principle. By introducing two sets of orthogonal states, $\{a, b\}$ and $\{\alpha, \beta\}$ where

$$\alpha = \frac{a+b}{\sqrt{2}} \quad \text{and} \quad \beta = \frac{a-b}{\sqrt{2}} \tag{2.39}$$

banks could print a serial number on each note made from the four states. The basis choice associated with each qubit would be stored in the bank records. Upon return of a note, the

bank would be able to measure each qubit in the correct basis to verify that it was the original. Any attempt to counterfeit a note would result in errors during the verification.

In a QKD protocol, we will introduce a new resource that is available to Alice and Bob: a quantum channel. This channel allows Alice to send quantum states to Bob. We will, of course, assume that the channel is prone to errors but we need not assume that the channel is private. Both Eve and Mallory will have full access. Uniquely, QKD offers the ability to detect an eavesdropper as measurements of quantum states causes them to collapse.

As with public-key cryptography, we will require an *authenticated* classical channel between Alice and Bob to avoid MitM attacks. This classical channel, as with the quantum channel, can be completely public. The authentication of the classical channel is something that is not solved with QKD and will need to utilise post-quantum algorithms. As Alice and Bob will require some initial bit of shared secret to authenticate their messages, QKD is sometimes referred to as quantum key *expansion*.

As the security of QKD systems stems from the laws of physics it has often been claimed to be *perfectly* secure. However, we will see later that side-channels or imperfections in different physical implementation will decrease the security. It is perhaps more accurate to say that, provided that the key is securely stored following a protocol, the security of that key does not decrease with advances in computing.

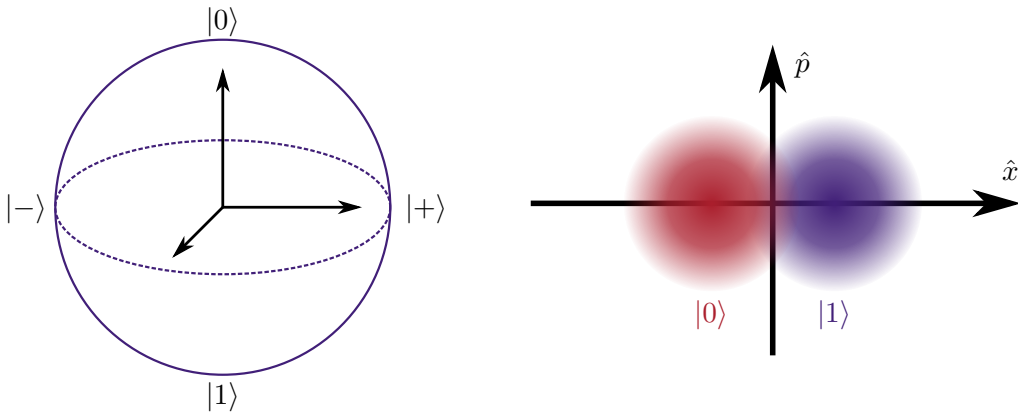
2.4.1 Protocols

QKD protocols are generally separated into three distinct categories: discrete-variable QKD (DV-QKD), continuous-variable QKD (CV-QKD) and distributed-phase-reference QKD (DPR-QKD). Here, we will introduce each with discussion of how qubits are encoded and the practicalities of each.

2.4.1.1 Discrete-Variable

The first ways that it was conceived that information could be encoded on photons was using orthogonal states to represent 0 or 1. For example, one could use the vertical and horizontal polarisations of a photon where diagonal and anti-diagonal could be used to encode super-positions.

A more practical method of encoding information when intending to use fibre optics to transmit the photons is a time-bin encoding. Now the timing and relative phase information between two pulses gives us a complete encoding of all quantum states. Provided that the two time-bins are closely spaced they won't be as affected by fluctuations in the fibre.



Discrete-variable QKD Continuous-variable QKD

Figure 2.3: States used to encode information for DV-QKD and CV-QKD.

BB84

The first QKD protocol to be developed Bennett-Brassard 1984 (BB84), named after its inventors [3] which was demonstrated in a proof-of-principle experiment a few years later [51]. Since then, there have been numerous demonstrations of BB84 either demonstrating new platforms or realising backbone quantum networks [52]. BB84 remains a favourite choice for systems despite alternative protocols being available [53–56].

We will introduce the four states

$$|0\rangle\,, \quad |1\rangle\,, \quad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \text{and} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.40}$$

that we will refer to as the BB84 states.

BB84 is a prepared-and-measure protocol where Alice and Bob play complementary roles. Alice prepares a quantum state which she sends to Bob who measures the state in a predefined way.

Algorithm 2.4: Bennett-Brassard 1984

1. Alice generates two uniform and random bit strings, b_a and n. The first bit string will determines the basis, Z = {$|0\rangle$,$|1\rangle$} if 0 or X = {$|+\rangle$,$|-\rangle$} if 1. The second bit string n determines whether the first or second state in each basis is chosen.

2. Each state is sent sequentially to Bob via the quantum channel.

3. Similarly, Bob generates a bit string, b_b uniformly and random. This de-

termines either the X or Z basis in which to measure. These are equivalent to the Pauli $\hat{x}$ and $\hat{z}$ observables introduced earlier.

4. Bob measures each of the bits in turn using the randomly selected bases and records the outcomes.

5. Alice and Bob announce their basis bit strings, $b_{\{a,b\}}$, over the authenticated classical channel. They discard all events where the bases didn't match.

6. Using some of the remaining events, they compare their values to check for eavesdropping. If an unacceptable amount do not match, they abort the protocol.

7. Finally, privacy amplification can be applied where Alice and Bob sacrifice some of their key to reduce the amount of knowledge Eve could have gained to satisfy security requirements.

Upon successfully finishing a BB84 protocol, Alice and Bob share a symmetric key. If they wished, they could use a OTP cipher to ensure information-theoretic secure communication. However, as one bit of key is needed to encrypt each bit of message, more pragmatic systems will implement a block cipher.

BB84 with Decoy States

As single-photon sources remain technically challenging to engineer, QKD system have preferred using weakly attenuated laser pulses to generate weak coherent states (WCSs). However, as WCS have a distribution of photon numbers, it opens the system up to a photon number splitting (PNS) attack.

In such an attack, we assume that Mallory has access to a device that can make a non-demolition of the photon number of the state. She will block each state which contains zero or one photons, and for each multi-photon state will keep one photon in a quantum memory until Alice and Bob announce the chosen bases.

One can consider the security of using WCS in the BB84 protocol describe above. However, this will offer a far reduced secret key rate due to the information leakage [57, 58]. Instead, decoy state protocols have been developed allowing Alice and Bob to bound the knowledge that could have been accessed by Eve [59].

During the first step of the protocol, Alice will randomly modulate the intensity of her WCS. Typically, Alice and Bob will agree on two decoy states that will be chosen to optimise the key rate depending on the error rate. As Mallory has no way to tell which decoy state Alice has sent,

she is more likely to block the decoy states than the signal states. During the basis discussion stage, Alice and Bob can bound the number of true single-photon events and use that to inform how much privacy amplification is required, or to abandon the protocol altogether.

Ideally, Alice and Bob would like to have perfect, unbiased estimators of the single-photon events in their key exchange. However, in a realistic exchange, they will necessarily have a finite number of events in which to estimate the parameters. Therefore, they must instead consider the finite key effects and calculate bounds on the single-photon statistics [60].

E91

Independently of the development of BB84, another protocol was developed by Artur Ekert in 1991 [4]. The Ekert 1991 (E91) protocol takes advantage of the correlations of entangled states and realised that by distributing two entangled photons between Alice and Bob meant that their measurements would be correlated. Further, using Bell's test and CHSH measurements they could verify that an eavesdropper hadn't interfered with the states [39, 40].

Algorithm 2.5: Ekert 1991

1. Alice generates an entangled state, for example one of the Bell states in equations 2.29 to 2.32.
2. She sends one qubit from the state to Bob and keeps one for herself.
3. Alice and Bob independently and randomly choose one of the CHSH angles [40] in which to measure their qubit.
4. After a sufficient number of states, they each announce their basis choices while keeping the results secret.
5. They use a random set of the measurement results to calculate the S and verify that the state was entangled.
6. If they can successfully violate a Bell inequality, the remainder of the events should be correlated.
7. Finally, they apply error reconciliation and privacy amplification as required.

As Alice and Bob are able to verify that the state is entangled, we don't need to assume that one of them is generating the entangled state. The protocol could be equally secure if Charlie, Eve or Mallory were generating the state. Any tampering with the state would only result in a reduction of key rate.

Entanglement-based protocols are often used as a method to prove the security of other prepare-and-measure protocols. For example, the chosen randomness used in a BB84 protocol is mathematically equivalent to a postponed measurement on an entangled state.

2.4.1.2 Continuous-Variable

More recently there has been an interest in continuous-variable QKD (CV-QKD) due to the compatibility with current telecommunication equipment [61]. Instead of single-photon detectors (SPDs), Bob can use photodiodes to perform measurements on the states through homodyne (or heterodyne) detection.

CV-QKD uses states that are described in Hilbert spaces of infinite dimension. Protocols have been proposed that encode information in Gaussian states [62] and squeezed states [63]. Both are considered prepare-and-measure schemes and the outline of the protocols remains the same.

Algorithm 2.6: Continuous-Variable Quantum Key Distribution

1. Alice encodes a random variable in a quantum state. In the case of Gaussian modulation, Alice encodes the information from a set of overlapping Gaussian states. In the case of squeezed state encoding, she randomly chooses between squeezing in the $\hat{x}$ and $\hat{p}$ quadratures.
2. The states are sent to Bob through the quantum channel which is typically assumed to be a thermal-loss channel.
3. Bob performs a homodyne (or heterodyne) measurement, switching between the $\hat{x}$ and $\hat{p}$ quadratures.
4. Alice and Bob use the classical channel to compare the quadratures they chose.
5. Using some of the matching bases, they perform parameter estimations to bound the knowledge that could have been gained by Eve or Mallory.
6. Finally, they perform privacy amplification as required.

For homodyne detection to be meaningful, Alice and Bob need to make sure they share a local oscillator. This provides a phase reference so that the prepared states can be reconciled with the measured states. Often, the local oscillator is multiplexed with the encoded state to avoid any mismatch in the phase fluctuations from the quantum channel [64].

For a long time, there were questions about the security of the CV-QKD systems. There

has since been a composable proof against general attacks [65] which was later extended to better consider finite key effects [66]. The post-processing requirements for CV-QKD are also computationally challenging. Unlike in discrete-variable QKD (DV-QKD), where only photons that reach Bob require analysis, CV-QKD requires each potentially event to be analysed which leads to large overheads.

2.4.1.3 Distributed-Phase-Reference

Distributed-phase-reference QKD (DPR-QKD) protocols were developed in order to solve practical issues with the security of QKD systems when using realistic equipment [67]. As single-photon sources are not widely available, system typically use coherent states that are prone to PNS attacks. In DPR-QKD protocols, the qubits are encoded in timing or relative phases of signals where a joint measurement of subsequent signals is required. Protocols include coherent-one-way (COW) [55] and differential-phase-shift (DPS) [54].

2.4.2 Security and Hacking

Generally, security proofs for QKD protocols fall into three categories. Individual attacks allow an adversary to interact with each state individually as it is sent. A collective attack allows them to process the states and store state indefinitely in a quantum memory. Finally, a coherent attack allows Mallory to generate arbitrary ancilla states which can interact with the states and be measured jointly. Coherent attacks only limit Mallory to the laws of physics and nothing more.

A proof of a protocol gives a security guarantee against an adversary but only under certain assumptions. It is often claimed that QKD is information-theoretic secure when used with a OTP. However, verifying the assumptions required for security is challenging in a practical setting and has been scrutinised by the quantum hacking community.

As the systems exist in the real world, the security of a key exchange is only as good as the model used to describe it. Any part of the system that is not fully characterised may leak information through side-channels allowing Eve to gain knowledge of the secret key. Such channels may include polarisation, after-pulses or wavelength. The concept of side-channels is not something unique to QKD and has been previously exploited to break RSA-4096 keys using a smartphone microphone [68]. In fact, side-channels were present even in the first demonstrations by Bennett and Brassard:

> *"...power supplies make noise, and not the same noise for the different voltages needed for different polarizations... Thus, our prototype was unconditionally secure against any eavesdropper who happened to be deaf!"* - Gilles Brassard [69]

Attack	Target	References
Photon-number splitting	Photon source	[57, 58]
Inter-symbol interference	State modulation	[70]
Trojan horse	Phase modulation	[71–73]
Time-shift	Single-photon detectors	[74, 75]
Detector Blinding	Single-photon detectors	[76, 77]
Laser damage	Any	[78, 79]

Table 2.1: Attacks demonstrated against QKD systems. Further details about the attacks, including countermeasures and bounds, can be found in refs. [5, 52].

Since then, there have been a number of attacks proposed on QKD systems exploiting uncharacterised channels [5]. Many have been demonstrated against both research and commercial systems. A brief list is compiled in table 2.1, although this list is far from exhaustive.

One of the most vulnerable parts of a QKD system seems to be the SPDs. Due to their complexity, they have been exposed to many attacks which have allowed Mallory to be in complete control of a key exchange [76, 77, 80–85].

Counter measures have been proposed to alleviate specific attacks against certain systems [86, 87]. There have also been bounds set for the amount of information that can be gained against particular attacks such as the trojan horse attack [88]. However, continually testing and patching systems with physical changes will be impractical for any ubiquitous network. A new vulnerability could render an entire system insecure requiring the hardware to be modified or replaced.

2.4.3 Device-Independence

Realising that the arms race between cryptographers and hackers would lead to an unending cycle, interest turned to reducing the assumptions required for security of a system [6, 89, 90]. In particular, how the assumptions about specific equipment can be removed. Device-independent QKD (DI-QKD) provides a method for Alice and Bob to verify the operation of the equipment *during* a protocol through a Bell test. Alice and Bob then only need to ensure that there are no communication channels out of their lab and that the laws of physics are correct.

Implementing a DI-QKD scheme remains incredibly challenging with modern technology as it requires near unity single-photon detection [91]. It also requires a loophole-free Bell test to be performed which, while such experiments have recently been realised [41–43], had rates that were far slower than needed for communication protocols.

In order to create more practical systems with improved security, protocols were developed which relaxed the device-independence. Measurement-device-independent QKD (MDI-QKD) removes the need to characterise the detection system, which remains challenging due to their

complexity [7]. It does, however, still required characterisation of the transmitters. MDI-QKD will be discussed further in chapter 4.

2.5 Integrated Photonic Circuits

On the route to an accessible technology, we will need to find a platform which allows for many devices to be made without an exponential increase in resources. Photonic integration is by no means a new idea having been considered for more than half a century [92]. However, the techniques have recently been adopted by the quantum photonic community for information processing.

In this section, we will cover the basic concepts in quantum photonics before discussing integrated photonics circuits. Some fundamental components that are used to create circuits will be presented and, finally, some of the more common platforms for photonic integration will be introduced.

2.5.1 Quantum Photonics

We will begin with the description of a quantised electromagnetic field as a harmonic oscillator with associated annihilation and creation operators, $\hat{x}$ and $\hat{p}$. For a more complete description or derivation of these operators, we refer the reader to any number of quantum optics textbooks [93–95]. The energy in the field corresponds to discretised packets of energy known as photons. The number of excitations in the field is described in the Fock basis and written as $|n\rangle$ for $n \in \mathbb{Z}_{\geq 0}$. The annihilation and creation operators change the photon number accordingly,

$$\hat{a}\,|n\rangle \;= \sqrt{n}\,|n-1\rangle \tag{2.41}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{2.42}$$

$$\hat{a}\,|0\rangle \;= 0 \tag{2.43}$$

where the final equation imposes that the energy of the field must be positive. The number operator, $\hat{n} = \hat{a}^\dagger\hat{a}$, is an eigenvector of Fock states such that

$$\hat{n}\,|n\rangle = n\,|n\rangle \tag{2.44}$$

An interesting state in the quantised electromagnetic field is the coherent state, which exist at the boundary of quantum and classical. Coherent states satisfy

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{2.45}$$

for $\alpha \in \mathbb{C}$. As the Fock states form a complete set, we must be able to write

$$|\alpha\rangle = \sum_{n=0}^{\infty} c_n |n\rangle \tag{2.46}$$

which of course must then satisfy

$$\hat{a} |\alpha\rangle = \sum_{n=1}^{\infty} c_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} c_n |n\rangle \tag{2.47}$$

Each c_n is uniquely determined in terms of α and c_0. By imposing normalisation conditions on the state, we arrive at

$$|\alpha\rangle = \mathrm{e}^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n}} |n\rangle \tag{2.48}$$

The generation of coherent states from vacuum is described through the displacement operator, $\hat{\mathcal{D}}(\alpha)$, and defined as

$$\hat{\mathcal{D}}(\alpha) = \mathrm{e}^{\alpha \hat{a}^\dagger - \alpha^* \hat{a}} \tag{2.49}$$

which acts on the vacuum state, $|0\rangle$, to generate a coherent state with average photon number $|\alpha|^2$:

$$|\alpha\rangle = \hat{\mathcal{D}}(\alpha) |0\rangle \tag{2.50}$$

The study of coherent states stemmed from an interest in the boundary of quantum and classical mechanics and the concept is almost as old as quantum mechanics itself [96]. More practically speaking, coherent states are readily produced from lasers which makes them far more practical for QKD than probabilistic single-photon sources.

2.5.2 Photon Encoding

We have discussed how single-mode photons can be represented but have yet to mention exactly what mode is used to encode information. This section will discuss the degrees of freedom available in photonics in which to encoding information, which are shown in figure 2.4.

Polarisation

The orientation of the electric field can be used to encode information in the polarisation. We can describe the computational basis by encoding $|0\rangle$ as a horizontal photon, $|1\rangle_H$, and $|1\rangle$ as vertical, $|1\rangle_V$. Relative phases and amplitudes between these states allow the entire Bloch

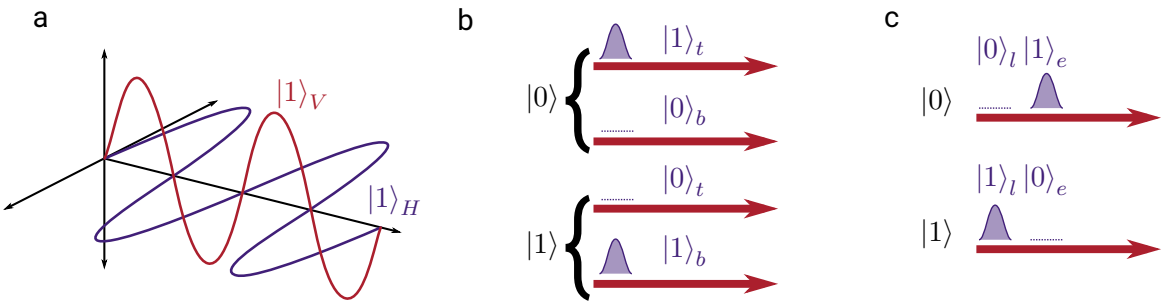


Figure 2.4: Information can be encoding in photons in different ways where superposition of each basis give access to the full Bloch sphere. Subscripts refer to the mode than the Fock state is in. **a** Orthogonal polarisations of light can be used as a basis, typically horizontal, H, and vertical, V are chosen. **b** The position, or path encoding can be used as a spatial encoding. Basis states are given by a photon either in the top path, t, or the bottom path, b. **c** The early or late arrival time of a photon, e and l, can be used to encode the computational basis.

sphere to be access. The manipulation of the states is performed through sequences of half and quarter wave plates. Polarisation is typically used in free-space quantum optics where there is minimal rotation of the fields. More recently, there have been developments in integrated optics that have allows waveguide polarisation rotation [97] meaning it could be a useful encoding scheme in the future.

Path

The spatial mode of photons can be use to encode qubits in which path they are following. The phase stability of integrated circuits means that paths are the typically encoding of choice. Two separate waveguides provide different paths which we will call the top, t, and bottom, b, paths. These can, with relative phases and intensities between the paths, encode arbitrary qubits in a computational basis. Beam splitters and phase modulators are used to manipulate the states and linear optic components can convert from path encoding to polarisation easily.

Time-bin

Finally, the time of arrival can be used to form a basis in distinct bins. Early and late photons, e and l modes, can be used to represent $|0\rangle$ and $|1\rangle$. Again, the relative phases of the time-bins can be controlled using phase modulation. Delay lines can be used to allow the early and late photons to interact. Time-binning is used in fibre optics where a polarisation or path encoding would be unstable from environmental drifts.

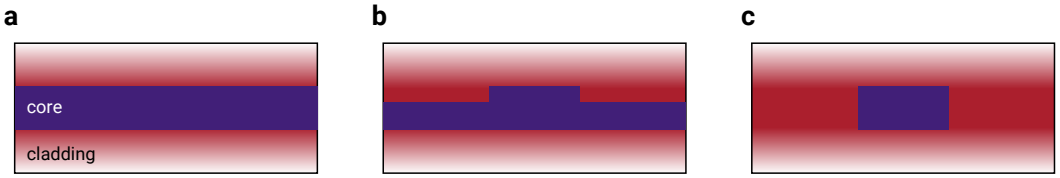


Figure 2.5: There are three main types of waveguide structures: **a** Slab; **b** Rib; **c** Strip. The core is shown in purple while the cladding is shown in red.

2.5.3 Components

Integrated photonics utilises fundamental components that will be used to guide, control, manipulate and detect photons. Here we will describe some fundamental components that will facilitate quantum information processing through linear optics.

Waveguides

To manipulate the path of lights, waveguide structures are created in a photonic integrated circuit (PIC) which guide light through total internal reflection. It is well established that the theory of light is is governed by Maxwell's equations which provide a set of relationships between the electric field, $\mathcal{E}$, and the magnetic field, $\mathcal{H}$ [98]. For light propagating in an insulating material, where there are no free electric charges or currents, the set of equations become

$$\nabla \cdot \mathcal{E} = 0 \tag{2.51}$$

$$\nabla \cdot \mathcal{H} = 0 \tag{2.52}$$

$$\nabla \times \mathcal{E} = -\mu_0 \frac{\partial \mathcal{H}}{\partial t} \tag{2.53}$$

$$\nabla \times \mathcal{H} = \epsilon \frac{\partial \mathcal{E}}{\partial t} \tag{2.54}$$

where μ_0 is the magnetic permeability of free space and ϵ is the dielectric permittivity of the material. These equations describe the electromagnetic field in a semiconductor material where the energy of the photon is less than the band gap. By combining the above equations, we can derive the wave equations

$$\nabla^2 \mathcal{E} + \nabla \left(\frac{1}{n^2} \nabla n^2 \mathcal{E} \right) - \epsilon_0 \mu_0 n^2 \frac{\partial^2 \mathcal{E}}{\partial t^2} = 0 \tag{2.55}$$

$$\nabla^2 \mathcal{H} + \frac{1}{n^2} \nabla n^2 \times (\nabla \times \mathcal{H}) - \epsilon_0 \mu_0 n^2 \frac{\partial^2 \mathcal{H}}{\partial t^2} = 0 \tag{2.56}$$

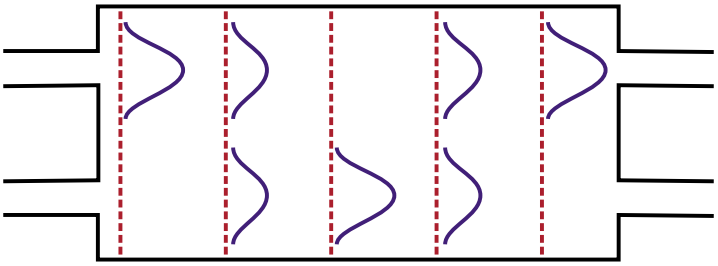


Figure 2.6: Illustration of MMI operation. The input light excites a superposition of modes with different propagation velocities. Depending on the length, the modes will either constructively or destructively interfere. This figure shows the simplest case for a 2 x 2 MMI but in principle can be designed to be n x m.

where the refractive index, $n(\mathbf{r})$, is dependent on the spatial coordinates. These equations yield a plane wave solution which are of the form

$$\mathcal{E}(\mathbf{r},t) = E(x,y)e^{i(\omega t-\beta z)} \tag{2.57}$$

$$\mathcal{H}(\mathbf{r},t) = H(x,y)e^{i(\omega t-\beta z)} \tag{2.58}$$

introducing the complex amplitudes, E and H, of the electric and magnetic fields. The angular frequency of the wave is ω and $\beta = {}^{\omega N}/_{c}$ is the propagation constant for some effective refractive index N.

Multi-Mode Interferometer

Different spatial modes in photonics experiments are typically interfered using a beam splitter. The traditional half-silvered mirror isn't something that is easily fabricated as a linear optical components, so another method is required.

Directional couplers allow waveguides to interfere as they are brought in close proximity. Evanescent coupling allows the mode to shift from one to the other. The splitting ratio of a directional coupler is dependent on the length of interaction. This makes fabricating accurate couplers challenging as small variations in length can cause a large change in splitting ratio.

Alternatively, waveguide modes can be interfered with multi-mode interferometers (MMIs) that are based on the self-imaging principle [99]. A schematic is shown in figure 2.6. Light in the input mode excites a superposition of modes within the MMI. As these modes propagate, they constructively and destructively interfere. The length is chosen to allow the light to be split equally when there is constructive interference into two output modes. The same structure can equally be designed to create n x m splitters. In general, the transfer matrix is

$$\hat{U}_{\mathrm{MMI}} = \begin{pmatrix} r & t \\ t & r \end{pmatrix} \tag{2.59}$$

where r and t are complex numbers that correspond to the reflectivity and transmission, respectively, and will be constrained such that the matrix is unitary. A balanced MMI will have the transformation matrix

$$\hat{U}_{\mathrm{MMI}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \tag{2.60}$$

Phase modulation

There are a few different methods that we can use to control the phase of photons. Of course, it only makes sense to talk about a relative phase, such as when a photon is in superposition. The transfer matrix of a phase modulator over two modes is given by

$$\hat{U}_{\mathrm{PM}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{2.61}$$

where a phase modulation is applied to the second mode, relative to the first which is left untouched.

Thermo-optic effects can be used to change the phase of a waveguide by changing the refractive index and is ubiquitous in integrated photonics. The change of phase, $\Delta\theta$, is given by

$$\Delta\theta = \frac{2\pi \cdot L \cdot (\Delta T)}{\lambda} \frac{\mathrm{d}n}{\mathrm{d}T} \tag{2.62}$$

where L is the length of the modulator, ΔT is the change in temperature, λ is the wavelength of light and $\mathrm{d}n/\mathrm{d}T$ is the thermo-optic coefficient of the material. Thermo-optic phase modulators (TOPMs) can achieve very good precision and stability with very low loss but have a slow response time.

To achieve faster modulation, which will be required for communication protocols, electro-optic effects have been explored. The effects exploit non-linear properties of a material where a change of phase is given by

$$\Delta\theta = \frac{2\pi \cdot L \cdot \chi^{(2)} \cdot E}{\lambda} \tag{2.63}$$

where E is the applied electric field and $\chi^{(2)}$ is the second-order non-linear optical susceptibility. Therefore, only materials that exhibit a second-order component can exhibit this type of

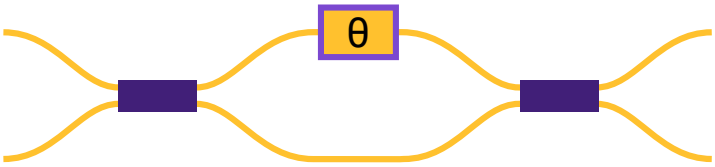


Figure 2.7: Illustration of MZI made from two 50:50 beam splitters and a phase modulator.

electro-optic modulation. Due to the centro-symmetry in silicon, other methods are required. However, lithium niobate modulators are commercially available with bandwidths up to 40 GHz while 100 GHz has been demonstrated in laboratories [100, 101].

Carrier effects can be used in semiconductor materials to change the absorption in p-i-n or p-n junctions which in turn generates a phase relationship through a Kramer-Kronig relation. These modulations are used where high-bandwidths are required in materials that don't have intrinsic electro-optic effects, such as silicon. These modulators have been shown to operate at 10 GHz bandwidths [102].

A final effect that we will mention is the quantum-confined stark effect (QCSE). The effect presents itself in materials where the absorption can be varied through an electric field applied over a multi-quantum well structures. Again, the change in absorption provides a phase relationship through the Kramers-Kronig relation and can provide modulation bandwidths above 10 GHz [9, 97, 103–105]. The QCSE will be discussed in more detail in chapter 3.

Mach-Zehnder Interferometer

Combining phase modulators and MMIs, we can create on-chip Mach-Zehnder interferometers (MZIs) which can be used for very fast routing, intensity modulation and phase encoding. A schematic is shown in figure 2.7 where a phase modulation is applied to one arm of the MZI. We can calculate the transfer matrix by simply combing the matrices for phase modulation and 50:50 MMI to get

$$\hat{U}_{\mathrm{MZI}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1-e^{i\theta} & i(1+e^{i\theta}) \\ i(1+e^{i\theta}) & -1+e^{i\theta} \end{pmatrix} \tag{2.64}$$

When the phase modulator in the circuit has a high bandwidth, MZIs can be used for fast intensity modulation of the states, as we will see in chapter 3, but also more stable phase modulation, which is discussed further in chapter 4. In the ideal case, the phases accumulated in each arm of the MZI will be equivalent. However, due to fabrication tolerances this is challenging to achieve. Therefore, MZIs combine slow phase modulation to correct for an offset with a fast phase modulator for high speed operation. This combination maximises the performance.

Single-photon Detection

An important part of any quantum photonic information processing is detection of single-photon states. A number of different technologies are available for single-photon detection [106]. Some metrics used to compare SPDs are

- **Efficiency:** the probability that the detector will fire given a photon was present.
- **Timing Jitter:** the uncertainty in the time of arrival of a photon.
- **Dead Time:** the time in which a detector cannot detect photons after firing.
- **Dark Counts:** the number of events when no photons are present.

Avalanche photodiodes (APDs) have been widely used for quantum optics experiments with efficiency in the visible spectrum exceeding 60 % [106]. Dark counts for APDs can be relatively high with kHz rates which can be reduced with cooling. Jitter is typically O(100 ps). The detection efficiency for longer wavelengths, such as light used in telecommunications, is typically lower. More recently, there has been a demonstrated of a 1 GHz gated APD for QKD with an efficiency of 55 % [107]. There have been demonstrations of integrated Ge-on-Si APDs with efficiency up to 35 % at 125 K [108,109]. While the efficiency here is lower, there are obvious advantages in terms of scalability and reduced coupling losses.

Advances in cryogenic cooling technology have allowed superconducting nanowire single-photon detectors (SNSPDs) to become more widely available. Their uptake in quantum photonics experiments has been rapid due to their unmatched efficiency which can easily exceed 90 % with timing jitter of O(10 ps) [106]. Short recovery times can allow for high count rates and dark counts lower than 1 per hour [110]. Waveguide integrated detectors have been demonstrated [111] which benefit from enhanced interaction between the confined light and the detector. Photonic cavities have been explored to further increase the detection efficiency and reduce the jitter [112–114].

2.5.4 Platforms

Different materials will exhibit different properties that provide benefits and weaknesses when making PICs. Some different platforms will be introduced here with some of their favourable properties discussed.

Silicon-on-Insulator

One of the more mature PIC platform is silicon-on-insulator (SOI) which has leveraged fabrication from the ubiquitous silicon microelectronics industry. Complementary metal-oxide-semiconductor (CMOS) compatibility has enabled large, complex devices to be fabricated [8].

A high index contrast between the waveguide and the substrate allows tight confinement of the light meaning small bend radii are possible.

As silicon is centro-symmetric, it has no natural $\chi^{(2)}$ which means that there is no electro-optic effect to use for phase modulation. Instead, modulation is achieved through thermo-optic effects, which are slow, or carrier injection/depletion modulators, which suffer from phase dependent losses. There have been attempts to break this centro-symmetry to achieve high bandwidth modulation [115,116].

A strong $\chi^{(3)}$ non-linearity allows single-photon generation through spontaneous four-wave mixing (SFWM) [117]. However, as silicon doesn't have a direct band gap lasers there is no immediate route to integrating lasers. Instead, hybrid platforms have emerged to utilise III-V lasers [118,119]. Doped silicon has allowed fast photodiodes to be waveguide integrated with high bandwidths [120].

Light can be edge-coupled but grating structures are more common as they are not restricted to the edge of the device. Periodic structures in the silicon projects the waveguide mode verically into single-mode fibres. Losses have been shown to be as low as 0.36 dB [121], although the loss is typically higher. Silicon suffers from high non-linear losses which are suppressed at longer wavelengths [122].

Silicon Nitride

Silicon nitride (Si_3N_4) offers a wider band gap than silicon meaning that it has a much wider transparency. This has added benefits at mid-infra-red wavelengths as the non-linear losses, such as two-photon absorption [123], are reduced which is crucial for quantum photonic technologies [124]. Reconfigurable circuits can be achieved through themo-optic phase modulation and MMIs. Like silicon, there is no natural electro-optic effect so any fast modulation is achieved through carrier effects.

Indium Phosphide

Indium phosphide (InP) offers benefits over other platforms, especially with its direct band gap which allows easily integrable lasers. Semiconductor optical amplifiers (SOAs) and distributed Bragg reflectors (DBRs) structures allow Fabry-Pérot lasers to be created and directly coupled to waveguides. Alternatively, high-bandwidth distributed feedback (DFB) components are also available [97,125]. Multi-quantum well structures allow fast phase modulation up to 40 GHz through the QCSE with similar bandwidth photodiodes also available [97]. Thermo-optic effects are also available for stable modulation and tuning.

As there is no insulator, like in SOI, there is a very low index contrast to create grating couplers as the light from similar structures would launch into the substrate. Therefore, edge couplers are required to access the optical circuits. Spot-size converters (SSCs) are tapered

waveguides that convert the waveguide to single-mode fibre. This low contrast also means that the bend radius is larger meaning that the component density is lower than silicon.

More recently, there has been work to replicate SOI with InP membrane on silicon (IMOS) [126,127]. This increases the index contrast in the waveguides meaning that bend radii can be smaller [128]. In this first demonstration of SFWM in InP it was noted that the non-linearity is actually stronger than silicon. However, the non-linear losses through two-photon absorption is far larger. This could be solved by either increasing the band gap of the material, much like silicon nitride compared with silicon. Alternatively, longer wavelength photons would be unable to cause two-photon absorption [122].

Lithium Niobate

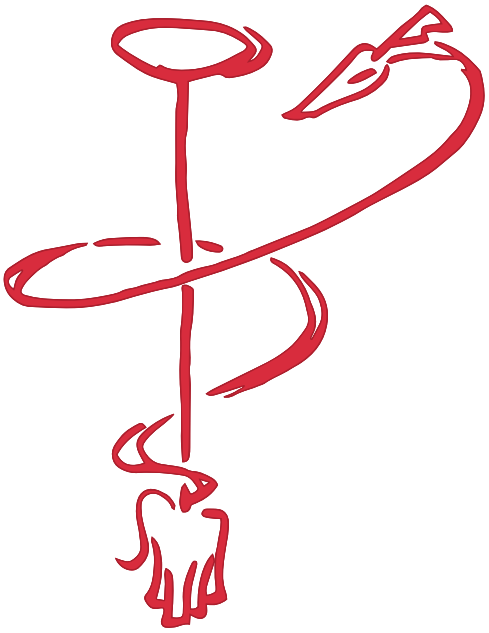
Lithium niobate is a favourite choice for phase and intensity modulation offering very high bandwidth modulation [100,101]. Single-photon generation is also available through spontaneous parametric down conversion (SPDC) in periodically poled structures [129]. Reconfigurable circuits have been demonstrated making it a potential candidate for future networks [130].

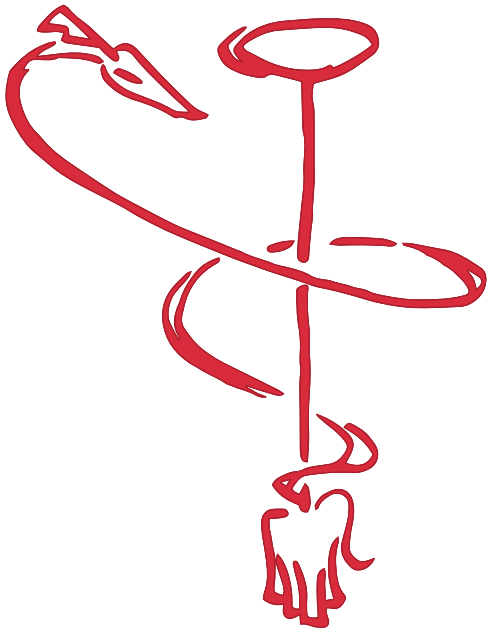
2.6 Summary

In this background chapter, we have introduced important cryptographic techniques, quantum theory and integrated photonics that will form the foundation for the remainder of this thesis. The humble beginning of cryptography have been incredibly influential throughout history and remains a vital endeavour. With a better understand of cryptoanalysis techniques the field will need to keep evolving.

Advances in the understanding of quantum mechanics has allowed a more complete view of the world. It has also facilitated a new range of quantum technologies to complement their classical counterparts. Through quantum key distribution, we can develop entirely new ways to securely communicate. At the same time, thorough analysis will be crucial to their claims of security.

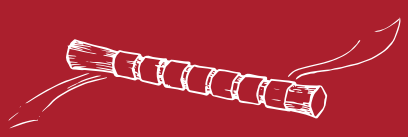
As with any technology, the mass-manufacturability of quantum photonic circuits will be key to its success. Developments in integrated platforms have allowed quantum photonics to progress from modest proof of principle experiments into the commercial world. Quantum communication systems are set to utilise these techniques to become part of future quantum networks. The rest of this thesis concerns developing the integrated platform for quantum key distribution.

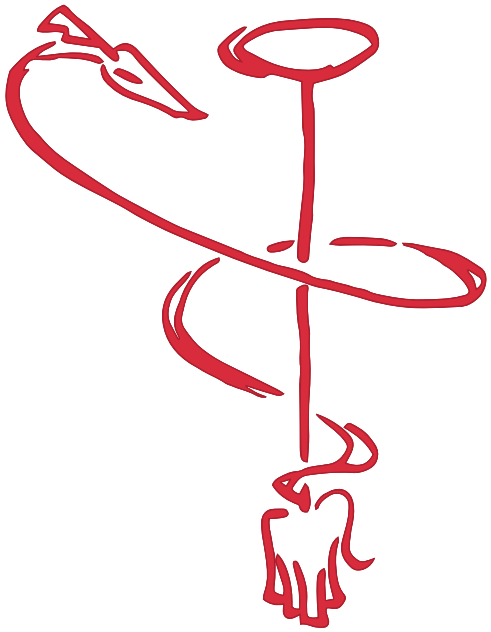




3

Hong-Ou-Mandel Interference Between Integrated Devices





Statement of Work

The photonic chips were initially conceived by Mark Thompson and Mark Godfrey. The chip mask was designed by Mark Godfrey and fabricated by Oclaro. The experiment was initially designed by Chris Erven and Philip Sibson and initial characterisation of the chips performed by Philip Sibson. I modified the initial experimental design and packaged the devices for electrical and optical testing. I performed the experiment and analysed the data with support from Philip Sibson. This chapter will expand on the work previously published in reference [105]. Where appropriate, text and figures have been reused that had been written or created by me.

3.1 Introduction

Secure communication protocols have been the focus of much academic research since the promise of quantum computing attacks against modern cryptography [1]. Quantum key distribution (QKD) aims to provide long-term security without assuming the computational power of an adversary [3, 4]. However, inconsistencies between theory and experiment have raised questions in terms of real-world security, while large and power-hungry commercial systems have slowed wide-scale adoption.

QKD has been under scrutiny from the emerging 'quantum hacking' community who have demonstrated that real-world implementations do not always meet the assumptions of the theoretical models [7]. This can lead to malicious attacks that allow Mallory to gain information about the secret key. These include side channels [131], where vulnerable information is leaked through uncharacterised channels, or responses to external manipulation of devices through classical means [71]. In particular, many attacks have been directed at the single-photon detectors (SPDs) due to their complexity and inconsistencies between theory and experiment [75, 80, 81].

Measurement-device-independent QKD (MDI-QKD) is a recent protocol that tackles some of the more prevalent attacks on systems by removing all detector side channels [7]. It does so by introducing a third party (Charlie) who acts as a relay to mediate detection events by announcing quantum correlations between states sent by Alice and Bob. The detection events alone do not contain any information about the secret key, so an eavesdropper cannot gain information by targeting the detectors.

At the heart of the MDI-QKD protocol is Hong-Ou-Mandel (HOM) interference [132], a quantum phenomenon where indistinguishable single-photons incident on a beam splitter interfere. HOM interference is a fundamental phenomenon in quantum optics which describes an important interaction between photons. However, interference between independent sources remains challenging due to the requirement of the photons being indistinguishable in all degrees of freedom [133]. It is possible to perform HOM-like interference using weak coherent

states, albeit with a reduced visibility in coincidences [134].

One of the more challenging degrees of freedom to ensure indistinguishability is the wavelength of the sources. Heterodyne detection is typically used to measure the frequency difference between two independent lasers where interference of optical fields on a beam splitter will produce a beat note when measured by a photodiode. However, photodiodes require much higher optical powers than those typically used for QKD protocols in order to register measurements. Without drastically increasing the complexity of a system, we can instead use HOM interference to characterise the wavelength overlap between independent sources.

Integrated quantum photonics has facilitated a drastic increase in complexity of experiments simply not possible with alternatives. The inherent phase stability is a vital resource for quantum experiments meaning integrated devices are poised to create an accessible platform. QKD systems have historically been bulky and expensive which has limited their practicality and has slowed their commercial adoption.

Recent developments on indium phosphide (InP) photonic integrated devices have established them as a promising platform for telecommunications [97]. The platform fulfils all of the requirements to perform QKD at state-of-the-art rates [9]. The monolithic inclusion of laser sources provides a method of producing weak coherent states that can be used in a decoy-state QKD protocol [59]. Efficient and fast phase modulation can be performed through the quantum-confined stark effect (QCSE) with a bandwidth up to 40 GHz [97]. The possibility of mass production means that InP devices are an excellent candidate to reduce the access cost of a QKD network and allow wide adoption [125].

In this chapter, we experimentally demonstrate that InP devices fulfil all the requirements for state-of-the-art HOM interference while also being a practical platform for future quantum networks. Using on-chip lasers and pulse modulation, we generated weak coherent pulses (WCPs) and measured a visibility of 46.5 ± 0.8 % between independent devices clocked at 431 MHz. Using gain-switching as an alternative means to accomplish phase randomisation between pulses, we show that the same interference is possible at 250 MHz without a reduction in state fidelity. This visibility is comparable to other demonstrations [135–137] with the benefit of being performed with integrated devices. Crucially, this level of interference demonstrates InP fulfills the required control for future MDI-QKD networks.

3.2 Hong-Ou-Mandel Interference

HOM interference is a quantum phenomenon where two indistinguishable single-photons incident on a balanced beam splitter will interfere and bunch. It was first seen by Hong, Ou and Mandel in 1987 [132] and is fundamental to many quantum information technologies from computation to communication and sensing.

Conceptually, the experiment is simple. We first consider two single-photons that are dis-

tinguishable only in their spatial modes. Mathematically, this can be represented as

$$\hat{a}^\dagger \hat{b}^\dagger \left|0,0\right\rangle_{a,b} = \left|1,1\right\rangle_{a,b} \tag{3.1}$$

where a, b are the two spatial modes.

In general, we can consider an ideal beam splitter to have some relationship between the input and output modes by reflection and transmission components. The transformation matrix is given generally as

$$\hat{U}_{bs} = \begin{pmatrix} t_{ac} & r_{bc} \\ r_{ad} & t_{bd} \end{pmatrix} \tag{3.2}$$

such that

$$|t_{ac}|^2 + |r_{bc}|^2 = |r_{ad}|^2 + |t_{bd}|^2 = 1 \quad \text{and} \quad t_{ac}^* r_{bd} + t_{bd} r_{bc}^* = t_{ac} r_{bd}^* + t_{bd}^* r_{bc} = 0 \tag{3.3}$$

where $t_{ij}, r_{ij} \in \mathbb{C}$ are the transmission and reflection, respectively, along the input mode i to the output mode j. The restrictions on r_{ij} and t_{ij} come from the unitarity of quantum transformations.

For a balanced beam splitter, we can use the transformation matrix

$$\mathsf{BS}_{50:50} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.4}$$

where the −1 is physically represented as a relative π phase being applied between the two reflected paths. This representation is not unique and will depend on the physical system being used. However, all representations are equivalent up to a phase transformation in the output modes. In an operator formalism, the creation operators will transform as

$$\hat{a}^\dagger \to \frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}} \quad \text{and} \quad \hat{b}^\dagger \to \frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}} \tag{3.5}$$

where $\hat{a}$ and $\hat{b}$ are the two input modes and $\hat{c}$ and $\hat{d}$ the two output modes. Then two photons incident on a 50:50 beam splitter become

$$\hat{a}^\dagger \hat{b}^\dagger \left|0,0\right\rangle_{a,b} \to \left(\frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}}\right)\left(\frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}}\right)\left|0,0\right\rangle_{c,d} = \frac{1}{2}\left((\hat{c}^\dagger)^2 - (\hat{d}^\dagger)^2\right)\left|0,0\right\rangle_{c,d} \tag{3.6}$$

We find that after the photons have interfered there is zero probability that exactly one photon ends up in each of the output modes of the beam splitter. This is referred to as the photons bunching, creating the superposition state

$$\frac{1}{2}\left(|2,0\rangle_{c,d} - |0,2\rangle_{c,d}\right) \tag{3.7}$$

If we were to look at the detection events after the beam splitter, we would not see any coincidences in the output modes. This is a useful measure of how indistinguishable the input photons are. By deliberately introducing some distinguishability between the two photons (for example a time delay), a measure of visibility can be introduced as the ratio of coincidences with and without HOM interference. Explicitly, this is

$$\text{Visibility} = 1 - \frac{\mathsf{P}_{\mathsf{HOM}}}{\mathsf{P}_{\mathsf{ind}}} \tag{3.8}$$

where $\mathsf{P}_{\mathsf{HOM}}$ is the probability of coincidence with maximal interference and $\mathsf{P}_{\mathsf{ind}}$ is the probability of coincidence without interference.

3.2.1 Coherent States on a Beam Splitter

While HOM interference is typically considered when single-photons interfere on a beam splitter, the same phenomenon can be seen with coherent states. However, the extent of the interference will be reduced due to multi-photon terms [134]. Here, we will consider how the effect presents itself with WCPs and how the intensity of the light is important. We will distinguish this interference from classical wave interference by introducing phase randomisation between the states which will be discussed further in section 3.2.3.

Consider two coherent states, $|\alpha\rangle$ and $|\beta\rangle$, incident on a beam splitter. Before the beam splitter, the states can be written as

$$|\alpha\rangle_a = \hat{\mathcal{D}}_a(\alpha)\,|0,0\rangle_{a,b} = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\,|0,0\rangle_{a,b} = e^{-\frac{|\alpha|^2}{2}} e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger}\,|0,0\rangle_{a,b} \tag{3.9}$$

$$|\beta\rangle_b = \hat{\mathcal{D}}_b(\beta)\,|0,0\rangle_{a,b} = e^{\beta\hat{b}^\dagger - \beta^*\hat{b}}\,|0,0\rangle_{a,b} = e^{-\frac{|\beta|^2}{2}} e^{-\beta^*\hat{b}} e^{\beta\hat{b}^\dagger}\,|0,0\rangle_{a,b} \tag{3.10}$$

which, before the beam splitter, can be written jointly as

$$\hat{\mathcal{D}}_a(\alpha) \otimes \hat{\mathcal{D}}_b(\beta)\,|0,0\rangle_{a,b} \tag{3.11}$$

From the beam splitter transformation above, the creation operator transformations are

$$\hat{a}^\dagger \to r\hat{c}^\dagger + t\hat{d}^\dagger \quad \text{and} \quad \hat{b}^\dagger \to t\hat{c}^\dagger - r\hat{d}^\dagger \tag{3.12}$$

and similarly for the annihilation operators. We will consider a beam splitter with variable reflectivity so that we can see how fabrication tolerances within the beam splitter would affect

the potential visibility. Applying these relations to incident coherent states, we find after the beam splitter the state becomes

$$\hat{\mathcal{D}}_a(\alpha) \otimes \hat{\mathcal{D}}_b(\beta) \left|0\right\rangle = e^{\alpha\hat{a}^\dagger - \alpha^* \hat{a}} e^{\beta\hat{b}^\dagger - \beta^* \hat{b}} \left|0,0\right\rangle_{a,b} \tag{3.13}$$

$$\longrightarrow e^{\alpha(r\hat{c}^\dagger + t\hat{d}^\dagger) - \alpha^*(r^*\hat{c} + t^*\hat{d})} e^{\beta(t\hat{c}^\dagger - r\hat{d}^\dagger) - \beta^*(t^*\hat{c} - r^*\hat{d})} \left|0,0\right\rangle_{c,d} \tag{3.14}$$

$$= e^{(\alpha r + \beta t)\hat{c}^\dagger - (\alpha^* r^* + \beta^* t^*)\hat{c}} e^{(\alpha t - \beta r)\hat{d}^\dagger - (\alpha^* t^* - \beta^* r^*)\hat{d}} \left|0,0\right\rangle_{c,d} \tag{3.15}$$

$$= \hat{\mathcal{D}}_c(\alpha r + \beta t) \otimes \hat{\mathcal{D}}_d(\alpha t - \beta r) \left|0,0\right\rangle_{c,d} \tag{3.16}$$

For a 50:50 beam splitter, the output would become

$$\hat{\mathcal{D}}_c\left(\frac{1}{\sqrt{2}}(\alpha + \beta)\right) \otimes \hat{\mathcal{D}}_d\left(\frac{1}{\sqrt{2}}(\alpha - \beta)\right) \left|0,0\right\rangle_{c,d} \tag{3.17}$$

We will model the SPDs as threshold detectors meaning that single-photon events are not distinguishable from multi-photon events. Therefore, we will need to consider how the efficiency of detection changes with multi-photon events. Consider an SPD with efficiency of detection η, then the probability that the detector clicks, given n photons were present, is

$$1 - \mathsf{P}\left(\text{no photons detected}\right) = 1 - (1 - \eta)^n \tag{3.18}$$

Then assuming that that the two detectors, Det_c and Det_d, at the output of the beam splitter have efficiencies η_c and η_d, respectively, the probability of a click is

$$\mathsf{P}(\mathsf{Det}_c \text{ click}) = \sum_{n=0}^{\infty} \frac{\left|\alpha r + \beta t\right|^{2n} e^{-\left|\alpha r + \beta t\right|^2}}{n!} (1 - (1 - \eta_c)^n) \tag{3.19}$$

$$= 1 - e^{-\left|\alpha r + \beta t\right|^2 \eta_c} \tag{3.20}$$

and equivalently,

$$\mathsf{P}(\mathsf{Det}_d \text{ click}) = 1 - e^{-\left|\alpha t - \beta r\right|^2 \eta_d} \tag{3.21}$$

Therefore, the probability of a coincidence click, with both coherent states overlapped on a beam splitter, is

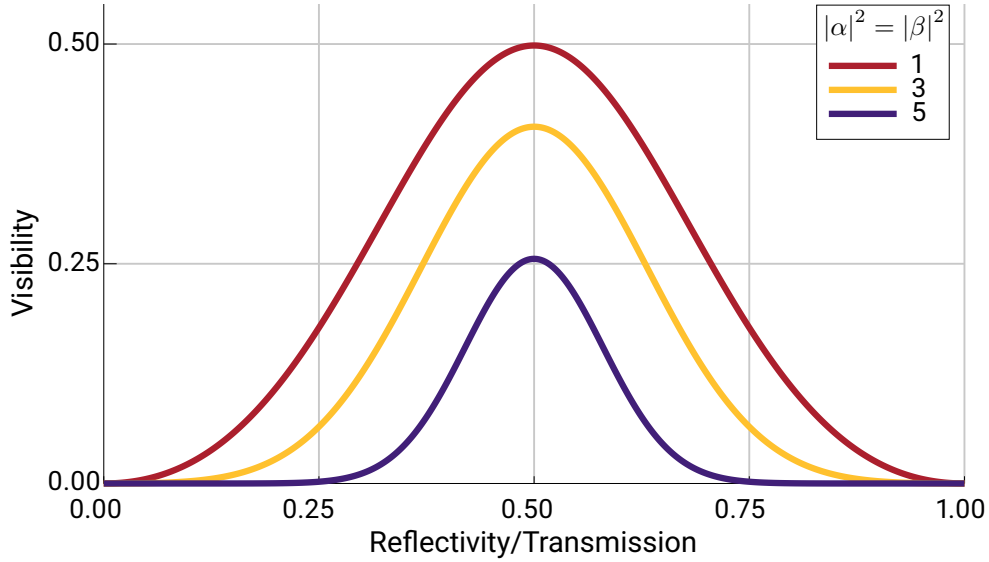


Figure 3.1: Graph plotting the effect of an unbalanced beam splitter on the visibility of a HOM dip. Maximal visibility is found when the beam splitter is 50:50. Photon number also has an effect on visibility due to the increased probability of multi-photon terms. Here, we plot average photon numbers ranging from 1 to 5. Both incoming states are assumed to have equal average photon number. As the average photon number tends to zero, the visibility on a 50:50 beam splitter will tend towards 50 %. We assume unity detection efficiency i.e. $\eta_{\{}c, d\} = 1$.

$$\mathrm{P_{HOM}}(\text{coincidence}) = \mathrm{P}(\mathrm{Det}_c \text{ click}) \times \mathrm{P}(\mathrm{Det}_d \text{ click}) \tag{3.22}$$

$$= \left(1 - e^{-|\alpha r + \beta t|^2 \eta_c}\right)\left(1 - e^{-|\alpha t - \beta r|^2 \eta_d}\right) \tag{3.23}$$

To get a visibility for the HOM dip, we need to consider two coherent states not interfering on a beam splitter e.g. two states with orthogonal polarisation. Then the distributions after a beam splitter are the sum of the reflected and transmitted states. Therefore, the probability of coincidence is given by

$$\mathrm{P_{ind}}(\text{coincidence}) = \left(1 - e^{-\eta_c(|\alpha r|^2 + |\beta t|^2)}\right)\left(1 - e^{-\eta_d(|\alpha t|^2 + |\beta r|^2)}\right) \tag{3.24}$$

We will see later that we want to consider pulses that are phase randomised relative to each other. For this, we can introduce a phase into the pulse incident from channel a. Mathematically speaking, we substitute $\alpha \to e^{i\theta}\alpha$ for $0 \leq \theta < 2\pi$. The coincidence probabilities then become

$$\mathsf{P}_{\mathsf{HOM}}(\text{coincidence}) = \frac{1}{2\pi}\int_0^{2\pi}\left(1-e^{-|e^{i\theta}\alpha r+\beta t|^2\eta_c}\right)\left(1-e^{-|e^{i\theta}\alpha t-\beta r|^2\eta_d}\right)\mathrm{d}\theta \tag{3.25}$$

$$\mathsf{P}_{\mathsf{ind}}(\text{coincidence}) = \left(1-e^{-\eta_c(|\alpha r|^2+|\beta t|^2)}\right)\left(1-e^{-\eta_d(|\alpha t|^2+|\beta r|^2)}\right) \tag{3.26}$$

where the visibility of the HOM dip can be calculated from the ratio of the interfering and non-interfering cases, as introduced in equation (3.8).

Using this equation, we can estimate the visibility of a HOM dip given a variable reflectivity beam splitter and average photon number, as shown in figure 3.1. The average photon number is assumed to be the same for both incoming states. As the beam splitter becomes more reflective (or transmissive), the visibility reduces to zero as the incoming states will no longer be interfering. However, we do see that small deviations from a 50:50 beam splitter do not cause the visibility to drastically decrease. We also see that an increase in the average photon number of the states will reduce the visibility. This is due to an increase in the multi-photon terms in the coherent states.

3.2.2 Wavelength Dependence

As previously mentioned, we will be using the HOM interference as a measure of wavelength overlap of independent sources. Therefore, it will be useful to understand what this interaction will look like. The experiment will see a continuous wave (CW) laser intensity modulated into pulses with a Gaussian shape in time. We will assume that the linewidth is much smaller than the frequency broadening due to pulse modulation so that the electric field can be modelled as a single frequency. This is to say that the pulses will be Fourier-transform limited. We will also assume that effects from chirp are negligible. Therefore, we can model the normalised electric field of each pulse as

$$\mathcal{E}_j(t,t_p,\omega_j,\phi_j) = \sqrt{\frac{2\sqrt{2\ln(2)}}{t_p\sqrt{\pi}}}\exp\left(-\frac{4\ln(2)t^2}{t_p^2}\right)\exp\left(i(\omega_j t+\phi_j)\right) \tag{3.27}$$

where $j = a, b$ are the beam splitter inputs, t_p is the full width at half maximum (FWHM) of the pulse in time (assumed the same for both inputs), $\ln(x)$ is the natural logarithm, ω_j are the frequencies and ϕ_j are the phases.

To calculate the interaction, we can use the beam splitter relations for electric fields,

$$\mathcal{E}_c = \frac{1}{\sqrt{2}}\left(\mathcal{E}_a+\mathcal{E}_b\right) \tag{3.28}$$

$$\mathcal{E}_d = \frac{1}{\sqrt{2}}\left(\mathcal{E}_a-\mathcal{E}_b\right) \tag{3.29}$$

By substituting the Gaussian pulses from above into the beam splitter relationships we can find the electric fields after interference. After integrating over the pulses in time, we can calculate the intensities of the output electric fields as

$$\mathcal{I}_c = 1 + \exp\left(-\frac{t_p^2(\Delta\omega)^2}{32\ln(2)}\right)\cos(\Delta\phi) \tag{3.30}$$

$$\mathcal{I}_d = 1 - \exp\left(-\frac{t_p^2(\Delta\omega)^2}{32\ln(2)}\right)\cos(\Delta\phi) \tag{3.31}$$

where we introduce $\Delta\omega = \omega_a - \omega_b$ to represent the relative frequencies between the two input fields and $\Delta\phi = \phi_a - \phi_b$ for the relative phases.

When the intensities of the fields are low the probability of coincidence is proportional to the product of the intensities averaged over the relative phase [134]. Explicitly, we want to find

$$P(\text{1 photon in } c, \text{1 photon in } d) \approx \langle \mathcal{I}_c \mathcal{I}_d \rangle_{\Delta\phi} \tag{3.32}$$

Multiplying the intensities calculated above and averaging $\Delta\phi$ over 2π, we find

$$\langle \mathcal{I}_c \mathcal{I}_d \rangle_{\Delta\phi} = \frac{1}{2\pi}\int_0^{2\pi}\left(1 - \exp\left(-\frac{t_p^2\Delta\omega^2}{16\ln(2)}\right)\cos^2(\Delta\phi)\right)d(\Delta\phi) \tag{3.33}$$

which gives the shape of the interference in terms of the relative frequencies of the two incoming pulses as

$$P(1,1) = 1 - \frac{1}{2}\exp\left(-\frac{t_p^2(\Delta\omega)^2}{16\ln(2)}\right) \tag{3.34}$$

This is the upper bound for the visibility of the interference. Any distinguishability between the pulses in degrees of freedom other than frequency would cause a reduction in the visibility of the HOM dip.

3.2.3 Quantum Over Classical

A natural question to ask when considering a quantum effect with electric fields is how the interference is different from classical wave interference. If we considered two coherent electric fields on a beam splitter we would see an interference in the fields and a change in the number of coincidences at the output. It could be argued that the limitation of 50 % visibility is due to a misconfiguration of the experimental set up allowing a distinguishability in an unconsidered degree of freedom.

We can distinguish the quantum interference from a classical fringe by considering the intensities of the individual outputs of the beam splitter. In a classical fringe, we would expect the intensity of the individual beam splitter outputs to vary as the electric fields interfere. Therefore, to verify that the interference is due to HOM effects, we need to show that the individual intensities are not changing with the change in coincidences. When we average over the relative phases and look at the intensity of each beam splitter output we find

$$\langle \mathcal{I}_c \rangle_{\Delta\phi} = \langle \mathcal{I}_d \rangle_{\Delta\phi} = 1 \tag{3.35}$$

So changing the relative wavelengths of the input pulses does not change the intensities of the individual outputs from the beam splitter. However, as calculated before, the change in wavelength will cause a decrease in coincidence probability. This difference is due to the phase randomised nature of the incoming light and distinguishes the interference from classical interference where the light fields would have a fixed relative phase.

3.3 Sources and Requirements

In this section, we will discuss the main experimental challenges in performing HOM interference and describe some of the photon sources that can be used to fulfil the stringent requirements of high-visibility interference. To show good interference between light fields, they need to be indistinguishable. Put more explicitly, for maximal interference, the two pulses need to have the same wavelength, arrive at the same time, have equal intensities, be in the same polarisation and have the same pulse shape.

3.3.1 Single-Photons

Historically, Hong-Ou-Mandel interference experiments have been performed with single photons. The first demonstrations used spontaneous parametric down conversion (SPDC) to generate pairs of single photons that were distinguishable only in spatial mode [132,138]. By delaying one of the photons before interfering on a beam splitter, HOM interference could be demonstrated. Subsequent experiments have demonstrated interference between different single-photon sources including spontaneous four-wave mixing (SFWM) [139], atomic systems [140], quantum dots [141] and NV centres [142].

While there have been many advances in single-photon sources through increased rates and coherence, they remain probabilistic. State-of-the-art rates are currently limited to tens of MHz [143] meaning they are impractical for modern communication protocols. Therefore, it is hard to claim that in their current form they will make good candidates for scalable quantum technologies without requiring multiplexing and feed-forward techniques, each of which introduces their own set of practical challenges.

It is worth noting that as quantum networks evolve from simple key exchange networks it will be necessary to develop single-photon sources [144]. As such developments occur, they will impact the field of QKD which would benefit from on-demand, single-photon sources provided that they fulfil the rate and loss requirements of modern communication networks.

3.3.2 Weak Coherent States

In the absence of true single-photon sources, another source of light needs to be considered for scalable quantum key exchange protocols. Coherent states represent a close approximation to single photons when strongly attenuated. They are also readily produced from lasers and easily manipulated through phase modulation.

As previously mentioned, the requirements for high-fidelity HOM, and therefore MDI-QKD, are stringent. Here we discuss some of the requirements for WCP sources to be useful in a QKD system.

Extinction Ratio

While not necessarily required for HOM interference, for use in a QKD protocol the quantum states will need to exhibit low encoding errors. The extinction ratio will be the ratio of the optical powers between the logical $|0\rangle$ and $|1\rangle$ states. In a time-bin encoding scheme, this means that there should be a high extinction ratio between the *on* and *off* states of the photon source allowing early and late time-bins to be well defined. A 20 dB extinction ratio between time-bins will result in a 1 % error rate in the timing information.

Timing Jitter

In order to keep up with high data rates of modern networks, we will need to have clock speeds that are comparable to those of classical devices. Therefore, it is important that we have a small uncertainty, or jitter, of the timing of the states to ensure the quantum states can be encoded in short time bins. As we move towards GHz clock speeds, timing jitter on the order of picoseconds will be required.

Coherence

In a time bins encoding scheme, we will need to make sure that the laser pulses in the early and late time-bins maintain coherence. This will allow us to faithfully encode phase between the time bins giving a complete encoding scheme. Physically, this means that the coherence of the laser should be much longer than the separation of the time bins. For a 1 GHz clocked system, we would need coherence longer than 2 ns meaning a linewidth of less than 150 MHz.

Phase Randomisation

A vital part of the HOM interference is for the WCPs to be phase randomised. This means that each quantum state should have a phase reference that is uncorrelated to the previous state. Phase randomisation is also an important part of QKD security, that will be discussed further in chapter 4.

Linearly Polarised

As mentioned before, the states will need overlap in each degree of freedom. The polarisation should be linear for maximal interference. While a polarising beam splitter (PBS) can be used to ensure polarisation overlap for interference, this adds complexity and loss to the system. Orthogonal polarisations can also introduce side channels into a QKD system to allow Eve to extract knowledge of the secret key during the exchange.

Wavelength Tunable

Modern telecommunications networks heavily rely on wavelength-division multiplexing (WDM) to maintain the data rates required. To ensure quantum compatibility with the same networks, it is likely that the wavelength of a QKD system will need to be tunable in order to switch between the standardised frequency bands. This may also restrict the use of wavelength filters, unless they are easily tunable. Moreover, unfiltered wavelengths can introduce side channels which could be exploited by Eve or Mallory.

3.3.3 Previous Methods

Several methods have been used to generate WCPs for QKD systems. Here we briefly discuss the benefits and drawbacks of each.

Gain-switched lasers

While gain-switched lasers offer simplicity and easily satisfy the phase randomisation constraint, they can suffer from bad timing jitter from the spontaneous emission and have broad spectra which require filtering [119].

Laser seeding

Laser seeding uses two separately controlled lasers, a master and a slave, to generate pulses [145]. The control is through multi-level RF electronics which can increase the cost of a system and, again, wavelength filtering is required. This method will be discussed further in chapter 5.

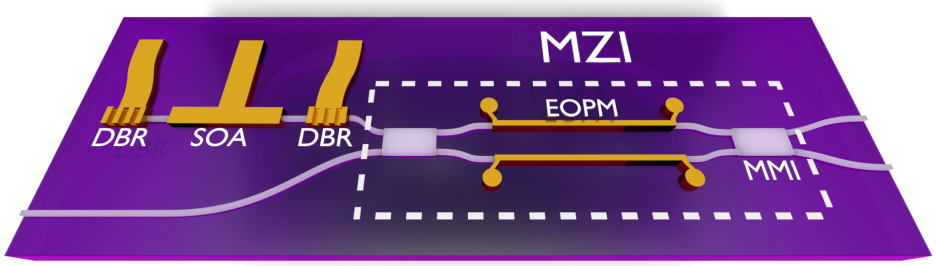


Figure 3.2: Schematic for the InP transmitters for weak coherent state generation. The integrated CW Fabry-Pérot laser is made from two distributed Bragg reflectors (DBRs) which forms a cavity around a semiconductor optical amplifier (SOA). Light is intensity modulated using multi-mode interferometers (MMIs) and electro-optic phase modulators (EOPMs) which make a Mach-Zehnder interferometer (MZI). States are coupled into fibre through spot-size converters at the edge of the device.

Intensity modulation

Starting from a CW laser, the light can be intensity modulated into distinct time bins. There is no inherent phase randomisation involved, although, this method doesn't broaden the spectrum beyond the Fourier-transform limit meaning wavelength filtering is not required [9].

3.4 Integrated Weak Coherent Source

In this section, we will describe the integrated transmitters that we will use for generating weak coherent states. Each transmitter is an InP device, measuring $6 \times 2\,\text{mm}^2$, that was fabricated by the commercial foundry service Oclaro. A schematic is shown in figure 3.2 showing the on-chip laser source and Mach-Zehnder interferometer (MZI).

3.4.1 Laser Source

As described in chapter 2, a huge benefit for III-V materials, such as InP, over silicon is the ability to monolithically integrate lasers into devices. This makes the platform particularly suited for telecommunications and generating weak coherent states for QKD.

Each device contains a Fabry-Pérot CW laser which is shown in figure 3.3. The 1 mm long cavity is made from two distributed Bragg reflector (DBR) gratings which are tunable through current injection and allow a wavelength tuning of around 10 nm. The DBR gratings themselves are periodic structures of differing refractive index. The peak reflected wavelength (λ_{DBR}) is dependent on the grating pitch (Λ) and effective refractive index (n_{eff}) of the waveguide and is given by

$$\lambda_{\text{DBR}} = 2\Lambda n_{\text{eff}} \tag{3.36}$$

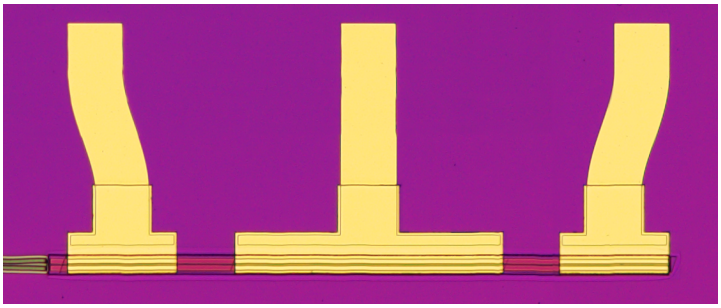


Figure 3.3: Microscope image of the Waveguide integrated Fabry-Pérot laser. Two tunable DBRs, which forms the optical cavity, and an SOA for optical gain. Gold pads allow wirebonding for electrical control through current injection. Each DBR is 200 µm long while the SOA is 500 µm for a total length of 1 mm including isolation sections.

From this, we find that changes in the refractive index will linearly change the reflection peak. The grating pitch is chosen to be 237.7 nm giving a peak reflected wavelength around 1550 nm, where $n_{\text{eff}} = 3.26$.

From the picture in figure 3.3, we can see that the DBRs are both the same length. Typically, the rear DBR would be longer to increase the reflectivity back into the cavity which increases the laser power. While the applications here only require weak coherent states, continuous-variable QKD (CV-QKD) [62] requires a bright local oscillator which needs to be considered during chip design. Subsequent chip designs should consider this design change to include a longer rear DBR to increase the laser power for CV-QKD applications.

The semiconductor optical amplifier (SOA) is a single-mode, ridge waveguide structure that is optimised for transverse electric (TE) polarisation. An electrical current is used to pump the carriers for a population inversion. Figure 3.4 shows the characteristics of the laser with a threshold current of 14 mA and a diode voltage around 0.7 V. The optical power is shown to be linear with applied laser current after the threshold and the diodes were tested up to 80 mA. Operating the laser at higher currents (more than around 60 mA) can have detrimental effects on the lasing stability as heating within the cavity can cause the laser to mode hop. Operating the laser at currents below 60 mA resolves this issue.

Typical spectra of the two transmitter lasers are shown in figure 3.5 which demonstrate $<$30 pm FWHM and $>$50 dB sideband suppression. The linewidth here is stated as $<$30 pm FWHM as this is limited to the precision of the optical spectrum analyser (OSA) used (Anritsu MS9740A). The two lasers were deliberately offset in wavelength to show each spectrum. The spectra demonstrate the reproducibility offered by integrated optics. Typically, we would expect the spectrum of a Fabry-Pérot laser to be Lorentzian [146] but the limited precision of the OSA is unable to measure this level of detail.

While the spectrum is limited by the precision of the OSA, we can put bounds on the linewidth from coherent measurements. The coherence length of the laser can be calculated

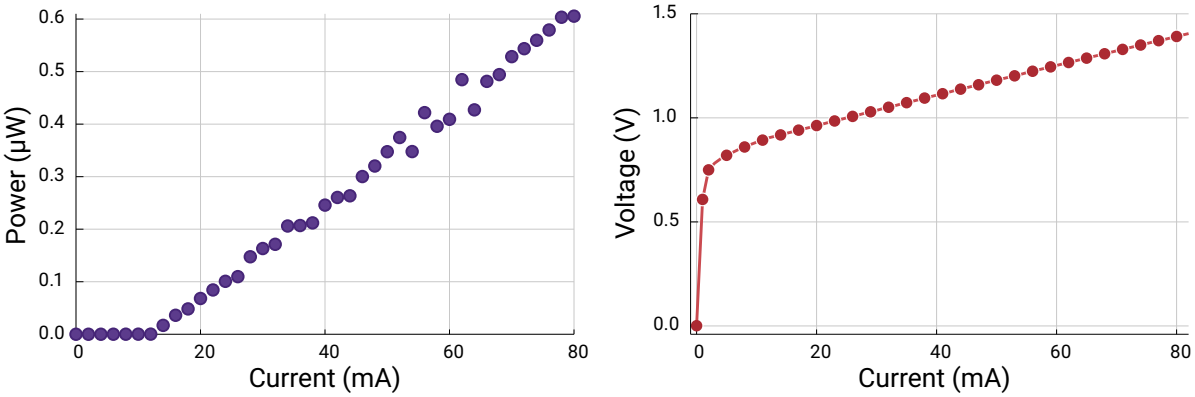


Figure 3.4: Characteristics of the on-chip laser. We find a lasing current threshold of around 14 mA and diode voltage of 0.7 V. The power given includes losses from optical components and fibre coupling so the on-chip power would be higher.

from the linewidth by

$$L_{\text{coh}} = \frac{c}{\pi \Delta v} \tag{3.37}$$

where Δv is the FWHM of the laser in frequency. The integrated lasers from Oclaro have previously demonstrated a coherence length of 45 cm which corresponds to a FWHM of 212 MHz (1.7 pm at 1550 nm) [9]. We will see later that partial coherence can be seen at 1.2 m which provides a lower bound on the FWHM of around 87 MHz (or 0.7 pm). In order to measure the linewidth more accurately than the previous OSA measurement, a self-heterodyne measurement technique [147] can be used but has not been performed in this thesis.

In figure 3.6, we show laser tuning through current injection of the DBRs which will change the reflection peak through heating effects. By varying the voltage from 0 V to 1 V, the wavelength can be tuned by about 10 nm within the telecommunications C-band. Both the front and rear DBRs need to have similar voltages applied to maintain a good cavity mode for lasing. Alternatively, the wavelength can be tuned by changing the temperature of the whole device, which causes the cavity to expand or contract.

The wavelength of the lasers can also be finely tuned through current injection of the SOA itself. This is shown in figure 3.7 where changing the driving current from 20 to 28 mA sees an increase in wavelength of around 100 pm. This wavelength shift is primarily due to heating effects in the cavity but carrier effects in the SOA will also be present. As the wavelength changes, so will the intensity of the laser. As we saw in figure 3.1, the photon number is an important aspect to control during a HOM interference. Therefore, when using SOA current injection to sweep the wavelength some attenuation will also be required.

We note here that the narrow linewidth of the laser means that during no experiment with the InP chips do we need to use a wavelength filter to clean up the light or optical pulses. This

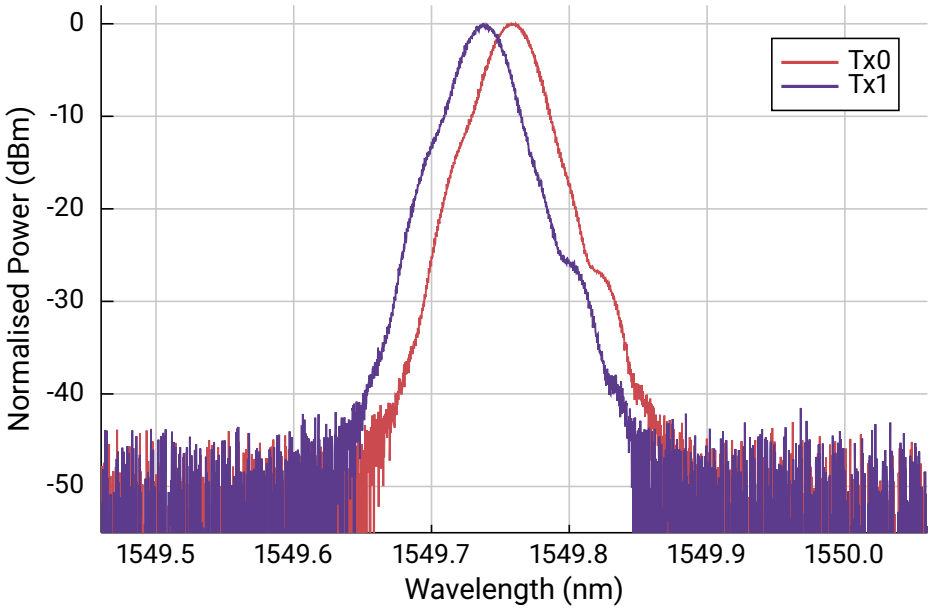


Figure 3.5: Typical spectra of the two independent on-chip lasers. Each demonstrates a FWHM of 30 pm (limited to the precision of the OSA) and a sideband suppression of 50 dB. The two lasers were deliberately detuned in wavelength so both spectra could be seen.

is important as it removed a component that would add cost to any system but also restrict the wavelength operation of the devices. Without the need for a filter, the lasers are free to operate in a wavelength that spans more than 10 nm. This will be crucial as it is likely that QKD systems will needed to be WDM compatible to meet the demands of high-speed networks for increased rates or quantum-classical multiplexing.

3.4.2 Phase Modulation

To create weak coherent states, we will use two different types of phase modulation for good extinction WCPs at high speed.

3.4.2.1 Electro-Optic Phase Modulation

The main modulation effect that we will use is the QCSE which has operating speeds of more than 40 GHz [97, 148]. The waveguide contains a multi quantum well (MQW) structure which has a variable absorption that is dependent on the electric field applied over the waveguide. The refractive index change due to this absorption can be calculated through the Kramers-Kronig relation between the real and imaginary parts. Given a complex function of the form $\chi(\omega) = \chi_1(\omega) + i\chi_2(\omega)$ we have that

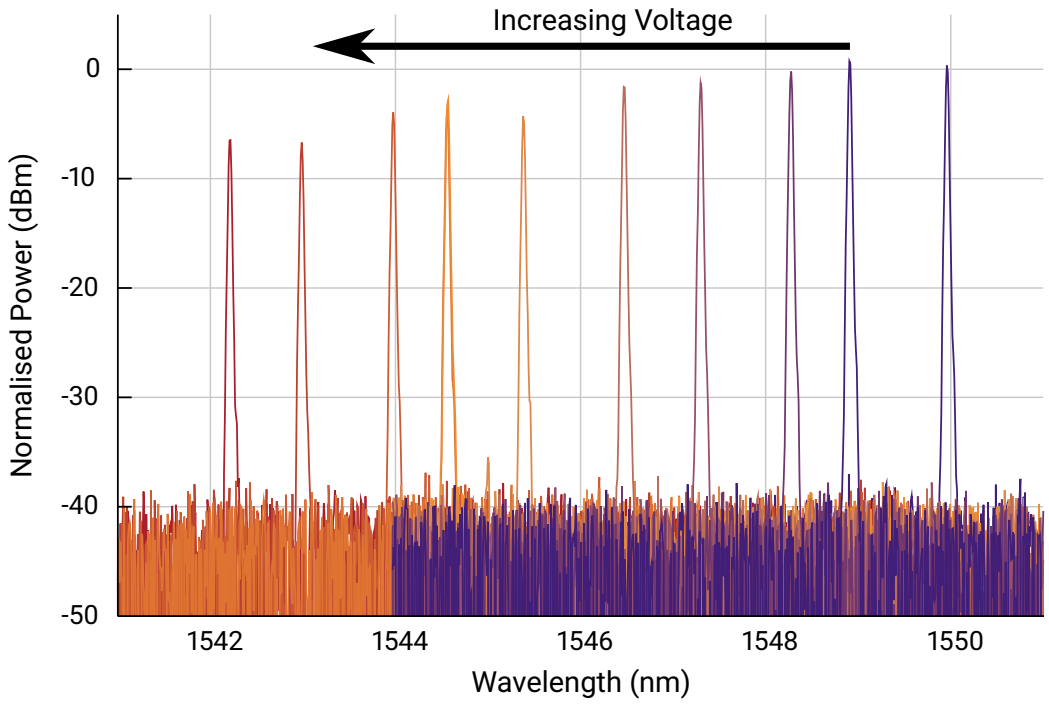


Figure 3.6: Through current injection of the DBRs we can change the wavelength of the laser due to heating effects. By sweeping the front and back DBRs, we can tune the laser around 10 nm within the telecomms C-band.

$$\chi_1(\omega) = \frac{1}{\pi}\mathcal{P}\int_{-\infty}^{\infty}\frac{\chi_2(\omega')}{\omega'-\omega}d\omega' \tag{3.38}$$

where Cauchy principal value is denoted by $\mathcal{P}$. From this, the refractive index, n, is related to the absorption coefficient, α, by [149]

$$n(\omega) - 1 \approx \frac{c}{\pi}\mathcal{P}\int_{0}^{\infty}\frac{\alpha(\omega')}{(\omega')^2-\omega^2}d\omega' \tag{3.39}$$

As we are only interested here in the refractive index change due to the QCSE, we will neglect all other electro-optic effects. We will also assume that the changes in the absorption are localised within a small region [150]. Therefore, we can rewrite the refractive index as $n(\omega) = n_0(\omega) + \Delta n(\omega)$ and similarly for the absorption coefficient. Within the frequency range $\omega_1 < \omega < \omega_2$ and assuming that $\Delta\alpha \neq 0$, we find the change in refractive index to be

$$\Delta n(\omega) \approx \frac{c}{\pi}\mathcal{P}\int_{\omega_1}^{\omega_2}\frac{\alpha(\omega')}{(\omega')^2-\omega^2}d\omega' \tag{3.40}$$

By comparing the absorption of the material with and without the electric field, $\alpha(\omega)$ can be estimated. Numerical integration can then be used to calculate the refractive index change

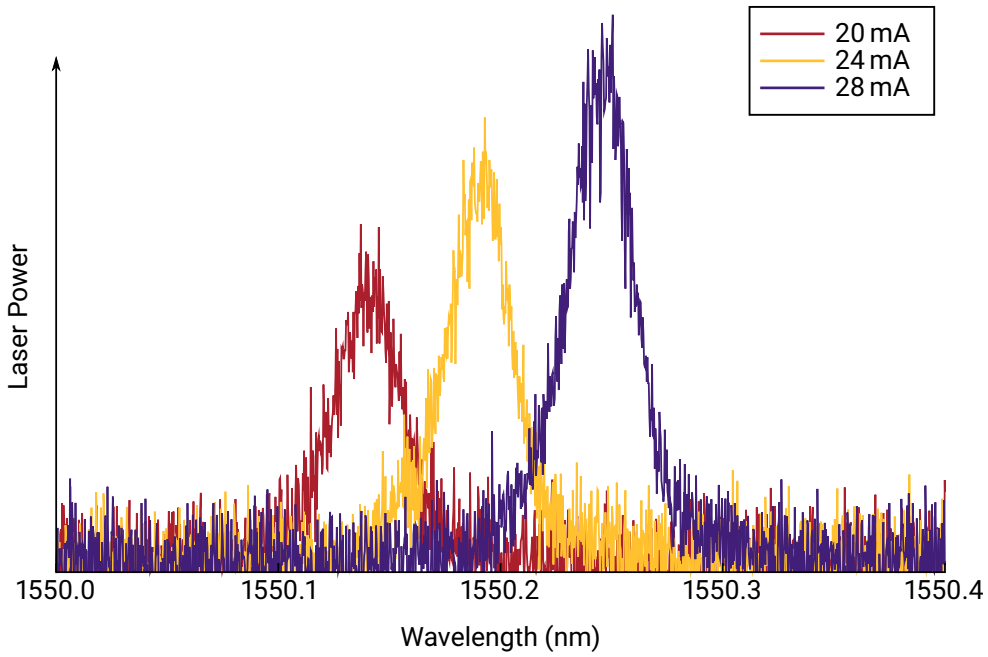


Figure 3.7: By changing the driving current of the on-chip laser, we can change the wavelength through heating and carrier effects. This will also vary the power output of the laser. The precision of the wavelength tuning is only limited by the control of the current source.

due to an applied electric field. For small refractive index changes

$$\Delta n \propto E^2 \tag{3.41}$$

where E is the applied electric field [148]. As the electric field increases, the effect saturates meaning that the quadratic nature is only valid for small changes in the refractive index. Exactly how the electric field and the refractive index are proportional is related to the exciton peak which is dependent on the specific material.

The exact relationship between phase and applied voltage has not been calculated for the devices presented here. This is due to the complexity of the circuit meaning it was not possible to isolate the effects of a single modulator.

The modulators are oriented parallel to the major flat axis of the substrate so that linear electro-optic effects add to the QCSE, whereas they would subtract if placed orthogonally. While the effect from the QCSE can reach speeds in excess of 40 GHz, design of the modulator and device packaging are important to maximise performance. For speeds above 10 GHz, the modulator should be less than 1 mm [97]. To ensure the faithful transfer of RF signals to the chip, wirebond length should be minimised and effective termination employed to stop reflections.

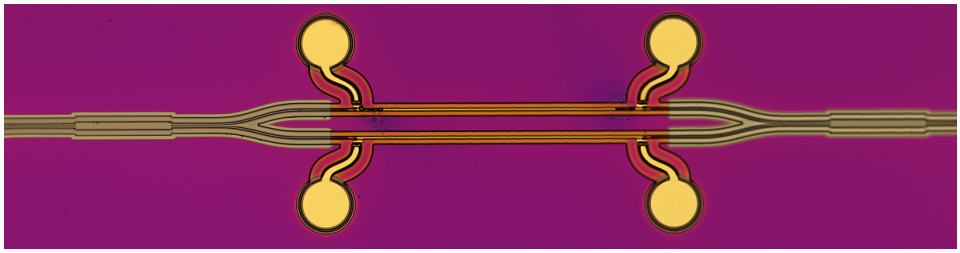


Figure 3.8: Microscope image of an integrated Mach-Zehnder interferometer made from two MMIs and two EOPMs which can be used for intensity modulation of light into WCPs. The MZI measures approximately 1 mm in length and around 350 µm in width. Electrical connections to the EOPMs can be made via the bond pads.

3.4.2.2 Mach-Zehnder Interferometer

As we will be operating the chip laser in CW mode, we need to modulate the intensity of the light to create well-defined time bins for our WCPs. Using electro-optic phase modulators (EOPMs) as described above, together with multi-mode interferometers (MMIs), we can create an MZI with modulation speeds in excess of 10 GHz. A microscope image of the integrated MZI is shown in figure 3.8.

The structure is 1 mm in length, while the modulators themselves are approximately 500 µm to ensure modulation speeds of more than 10 GHz. MMIs are used as integrated 50:50 beam splitters to split the light between the two EOPMs. Unlike directional couplers which exhibit a drastic wavelength-dependent splitting ratio, MMIs are used to ensure a good splitting for a wide range of wavelengths. Bond pads are used for electrical connections to the modulators and provide bias voltages and currents.

3.4.2.3 Thermo-Optic Phase Modulation

Imperfections in the MZIs due to the fabrication of the devices mean that the phases accumulated on the top and bottom path are not the same. While not designed for thermo-optic modulation, the EOPMs have a resistance of around 10 Ω which can also be used to vary the phase. By passing a small current over one arm of the MZI, we can correct for the phase mismatch to recover the desired performance.

To operate the MZI using the thermo-optic effect on one modulator and electro-optic modulation on the other, a negative DC voltage offset is first applied to both modulators. This is to balance the phase-dependent losses in both arms of the MZI and to access the quadratic effects of the QCSE. A current is then used to apply thermo-optic phases to balance any phase mismatch between the two arms. This current will also cause a small phase change due to electro-optic effect but these changes will be small so can be compensated for using the DC offset. RF signals can then be applied to the electro-optic modulator to create high-extinction ratio states.

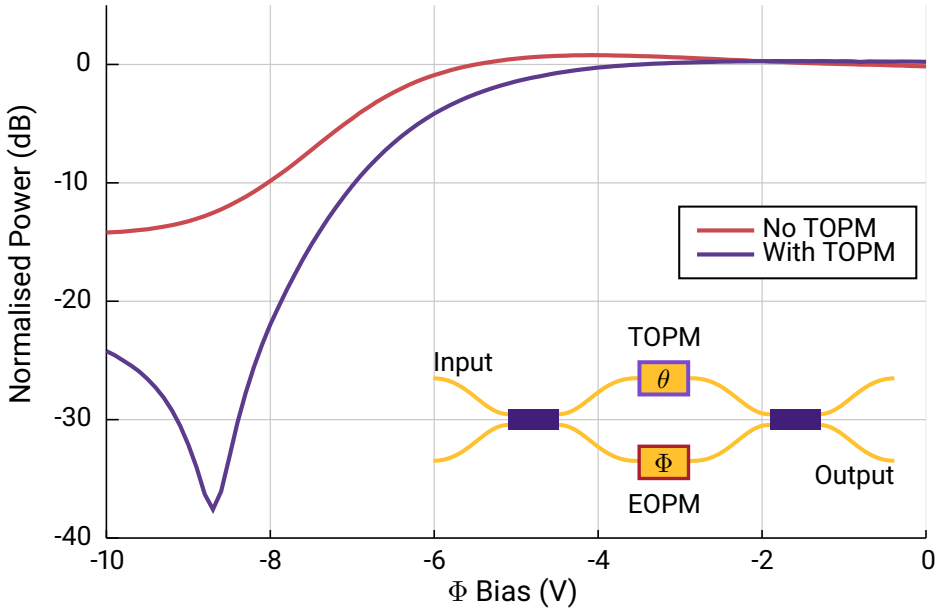


Figure 3.9: Effect of applying thermo-optic phase modulation (TOPM) and electro-optic phase modulation (EOPM) within an MZI. Without heating, we can only get an extinction of 15 dB by using the QCSE. By correcting for phase differences through thermo-optic effects, we can increase the extinction to more than 35 dB.

Figure 3.9 demonstrates how heating effects can change the characteristics of an MZI. By changing the voltage bias for the QCSE over one arm of the modulator (Φ) whilst the other arm is kept constant (θ) we can characterise the performance. Φ is swept over the range 0 to −10 V and the power at the arm output of the MZI is measured. We can then compare the difference in DC modulation with and without heating.

Without heating, the absorption effects mean that the extinction ratio possible is limited to only around 15 dB. However, by correcting for the phase difference in the two arms, the extinction ratio can be increased to 30 dB with voltage swing of 3 V_{pp}.

Using this heating technique, we can apply RF modulation to the MZI to create WCPs, as shown in figure 3.10. Without correcting for detector and electronic timing uncertainty, the FWHM is 175 ps. We also find an extinction ratio of more than 20 dB for a 2 V_{pp} electrical pulse.

3.4.3 Fibre Coupling

To efficiently couple the light from the waveguide mode (1.5 µm) to a fibre mode (10 µm), a spot-size converter (SSC) on the chip is used to expand the light mode to 3 µm. The SSC also changes the mode to be more circular from the elliptical waveguide mode. A lensed fibre was then used to convert this mode to a standard 10 µm fibre mode. The fibre was held in a Elliot

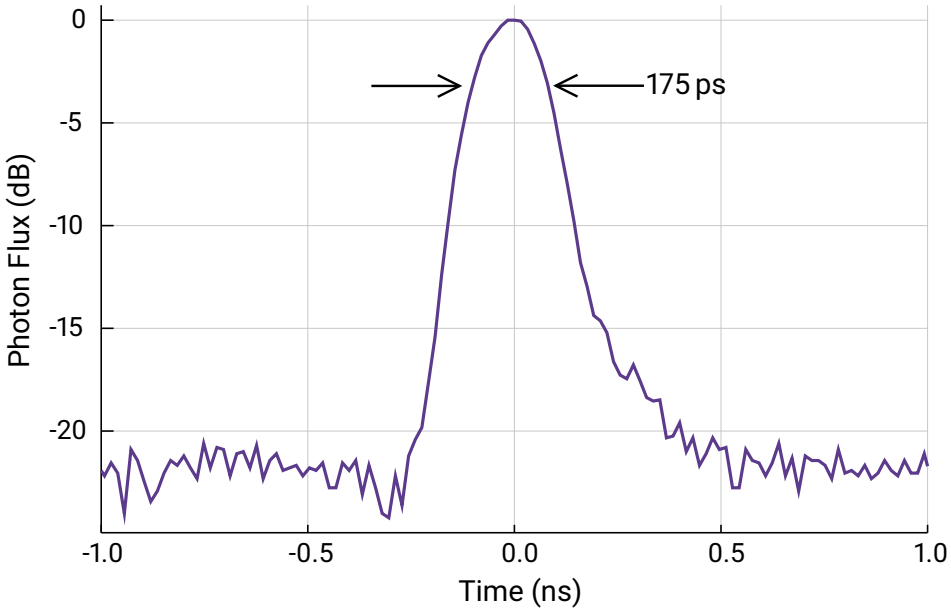


Figure 3.10: Histogram of single-photon events after intensity modulation with an MZI. We find an extinction ratio of just over 20 dB and a FWHM of 175 ps. The histogram is not corrected for detector or time-tagging jitter so the FWHM includes these uncertainties. The slope after the pulse is attributed to the initial signal shape from the signal generator, the impedance matching on the PCB and reflections from the RF termination.

Gold fibre launch stage with piezo-electric actuators that gave a precision of 10 nm in the X, Y and Z axes over a range of 25 µm.

To reduce reflections back into the waveguide, the facet of the SSC is at an angle relative to the edge of the chip. On these devices, the waveguides are at 7° to the edge which minimises back scattering from the high refractive index contrast. When coupling from the chip through air into a fibre, we need to consider refraction to minimise loss. From Snell's law, we can calculate that the fibre should be at 23° to the edge of the chip, given that the waveguide refractive index is 3.26.

It was not possible to directly measure the coupling losses on these devices as there were no test structures to isolate the waveguides and spot-size converters. From foundry tests, the coupling loss from an SSC to a standard single-mode fibre was estimated to be 1.5 dB. It is expected that these devices will have similar losses.

3.4.4 Packaging

To access the electrical components of the integrated devices, we need to create a package to transfer the signals from the driving electronics to the chip. A PCB was designed to electrically connect the modulators and laser to SMA connectors for high-speed operation and DC pins for

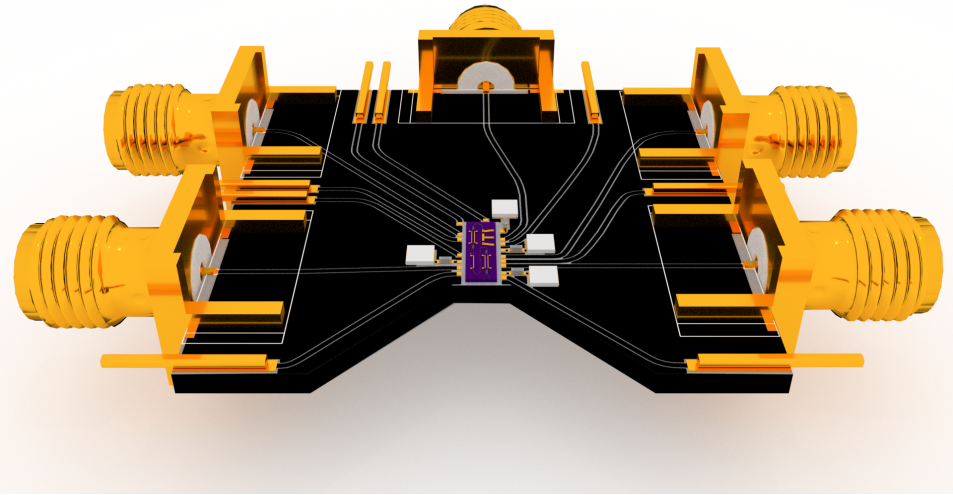


Figure 3.11: Chip packaging to breakout the electrical connections on the chip. SMA connectors were used for the high-speed connections to offer a response of more than 10 GHz. Capacitors and resistors were also used for termination of RF modulation signals. DC pins were used for low-speed connections for thermo-optic modulation and distributed Bragg reflector tuning. The bottom of the PCB is cut out to allow optical access to the side of the chip.

biasing. A render is shown in figure 3.11. The bottom of the chip is ground which connects to a copper block that is also connected to the ground of the PCB. Silver epoxy was used to glue the chip to the mount to ensure a good electrical connection. It also provided a good thermal connection for temperature stabilisation. The PCB is designed with a cut-out for optical access to the chip from one side.

In order to maintain a good signal integrity, the impedance of the tracks needs to match the electronics. As the devices require a number of RF connections to a small area, using standard FR-4 material would not be sufficient. Instead, Rogers 6006ns material was chosen for its high dielectric constant of 6.15 meaning that narrow conductor-backed coplanar waveguides (CB-CPWs) could maintain a 50 Ω impedance. A schematic of the waveguides is shown in figure 3.12. The characteristic impedance of a CB-CPW can be approximated by [151]

$$Z_0 = \frac{60\pi}{\sqrt{E_{\text{eff}}}} \frac{1}{\frac{K(k)}{K(k')} + \frac{K(k_l)}{K(k_l')}} \tag{3.42}$$

where, for a track of width a, waveguide of width b and substrate of height h we have

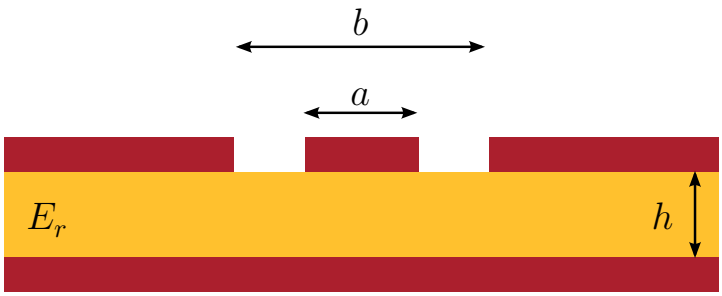


Figure 3.12: CB-CPW schematic for RF signal transmission. a is the width of the waveguide while b is the width of the waveguide plus the space between ground. h is the thickness of the substrate and E_r is the dielectric constant.

$$k = \frac{a}{b} \qquad k' = \sqrt{1 - k^2} \tag{3.43}$$

$$k_l = \frac{\tanh\left(\frac{\pi a}{4h}\right)}{\tanh\left(\frac{\pi b}{4h}\right)} \qquad k_l' = \sqrt{1 - k_l^2} \tag{3.44}$$

$$E_{\text{eff}} = \frac{1 + E_r \frac{K(k')}{K(k)} \frac{K(k_l)}{K(k_l')}}{1 + \frac{K(k')}{K(k)} \frac{K(k_l)}{K(k_l')}} \tag{3.45}$$

where $K(k)$ is the elliptic integral of the first kind.

The thickness of the substrate used was 250 µm so a track of width 260 µm with a spacing of 100 µm (giving a total waveguide width of 460 µm) has a characteristic impedance of 50 Ω. Ideally, to avoid microstrip line modes the design should have $h \gg b$ and the ground plane should extend away from the waveguide more than b [152]. In this design, these restrictions will be relaxed due to space constraints. However, through operation we will see that the waveguide can support a modulation bandwidth up to 10 GHz.

The tracks were designed and then laser etched into the copper on the substrate. The PCB was given a gold coating using electroplating to avoid oxidation of the copper and to help with gold wirebonding. In future iterations, a nickel layer should be applied before the gold to avoid gold diffusing into the copper. SMA, DC pins, capacitors and resistors were then soldered onto the PCB using a low-temperature solder paste.

The pads on the chip were wirebonded to the PCB with a 25 µm ball bond and then a wedgebond onto the PCB. Silver epoxy was then applied over the wedgebond to ensure a good electrical contact with the PCB and to increase durability. The PCB was designed such that the length of the RF wirebonds was minimised so that capacitance and resistance of the gold wire were reduced. Such effects can be detrimental for high-speed operation.

An RF signal could be applied to one side of an EOPM while the other side provided termination to minimise electrical reflections. A capacitor blocked the DC component of the signal while a 50 Ω resistor terminates the AC signal.

3.5 Fibre-Optic Transmitter

For initial demonstrations of the on-chip laser and pulse generation, it will be useful to have a well characterised source of WCPs. Here, we describe the commercial fibre components that can be used to replicate the chip components.

3.5.1 State Preparation

A CW fibre laser (Yenista T100s-hp) with a wide tuning around the C-band in steps of 1 pm was used as the source. This meant that the laser could be swept very precisely compared with the integrated laser, which would remain fixed.

The lithium niobate fibre modulator (ThorLabs LN27S-FC) was used to intensity modulate the light. It required a 5 V_{pp} pulse meaning that amplification of the signal from the pulse pattern generator (PPG) was needed. The amplifier used was an SHF 810 with 29 dB gain and up to 40 GHz operation.

The time-bandwidth product of a Gaussian pulse is

$$\Delta\omega = \frac{4\ln(2)}{\tau_p} \tag{3.46}$$

where τ_p is the FWHM of the pulse in time and $\Delta\omega$ is the angular frequency FWHM. For a pulse width of $\tau_p = 100\,\text{ps}$ the minimum spectral width of a Gaussian pulse is 4 GHz. The typical linewidth of the fibre laser was $<$400 kHz so it is a good approximation to assume that any WCPs will be Fourier-transform limited as the contribution from pulsing is much larger than the linewidth.

3.6 Measurement

As the pulses were coupled into fibre, we could make use of commercial fibre components for control, interference and measurement. This section will describe the required control off chip, as well as the detection and correlation of photons.

3.6.1 Polarisation and Projection

Fibre polarisation controllers are used to rotate the polarisation of the pulses and a PBS gives a known polarisation in a polarisation maintaining fibre. A polarisation-maintaining 50:50 beam

splitter is used for the interference to ensure that both transmitters are overlapped in polarisation.

3.6.2 Photon Number Feedback

As we will be using the current of the on-chip laser to vary the wavelength this will also change the power. To ensure maximal interference, both transmitters should have an equal photon number. Using the sum total counts of the detectors, a feedback loop was used to ensure that both transmitters (fibre or chip-based) remained constant in photon number. Each transmitter used a digital variable optical attenuator (VOA) (Oz Optics DA100) to vary the power with 0.01 dB precision.

3.6.3 Detection

The detectors used in the experiment were fibre-coupled superconducting nanowire single-photon detectors (SNSPDs) from Photonspot which were chosen over other single-photon detectors for their high efficiency ($>$80 %), small timing jitter (30 ps) and short recovery time (100 ns). The detectors were housed in a closed-cycle helium refrigerator that was kept at 0.7 K. A successful event was indicated by an RF signal of around 10 mV which was amplified with a low-noise amplifier to around 200 mV which could then be time-tagged.

3.6.4 Time-tagging

Detection events were time-tagged using a PicoQuant Hydraharp 400 and saved to a computer for later analysis. An optical link was used to provide a synchronisation signal from the transmitters to the time-tagger. The precision of timing events could be set by the user and could be as low as 1 ps with an electronic jitter of $<$12 ps. The dead time of the tagging electronics is $<$80 ns, which is comparable to the detector dead time so should not impact the experiment. In this experiment, 16 ps bins were used. As the exact series of events could be reconstructed from the time tags, the number of coincidences could be calculated from the saved tags provided the timing information between transmitters had been calibrated.

The coincidence window could be varied in the analysis after to ensure that the coincidences come from when the pulse is a Gaussian shape. As we see from figure 3.10, there is a 'tail' on the later edge of the pulses that could cause chirp in the pulse. This would have two effects on the HOM interference. Firstly, if the two pulse shapes are different, this would cause a reduced interference as the photons would have different wavelengths. Secondly, this would change the shape of the HOM dip from the Gaussian shape that was derived in section 3.2.2.

3.6.5 Synchronisation

As the HOM interference is dependent on the time of arrival of the two pulses, we need to ensure that the pulses arrive at the beam splitter at the same time. It is also crucial that we can reconstruct the events using the timing electronics, meaning that we require to fully calibrate the optical and electrical delays. This meant that the pulses that seemed to match in the time-tagging electronics were actually those that interfered at the beam splitter.

We will make the assumption that the total delay (optical and electronic) between the two arms of the measurement system after the beam splitter was less than 50 ns. This was reasonable as 50 ns in fibre equates to about 12 m, and is similar in the coaxial RF cables. Then the pulse generation could be slowed to send a pulse at less than 10 MHz so that the pulse separation was more than 100 ns and the pulses could be matched to the nearest coincident event. The delay between the arms of the measurement in this experiment were found to be less than 10 ns which was verified through the HOM interference.

To keep the transmitter electronics synchronised with the detection electronics, an optical signal was sent over a separate fibre which acted as a reference clock.

3.7 Control Electronics

A multi-channel DC voltage source was used to create a voltage potential over the EOPMs for the QCSE. Each modulator could be controlled separately up to a maximum bias of 10 V. The DC biases were mixed with the RF signals using bias tees (Mini-Circuits ZX85-12G-S+) with a bandwidth of up to 12 GHz.

To generate the RF signals, a PPG (Keysight 81134A) was used which had a maximum output voltage swing of 2 V_{pp}. A PPG was used over a more general arbitrary waveform generator as only two levels were required for operation of the device for this test. The minimum pulse width that could be set was 100 ps which when measured on an oscilloscope (Keysight DSA91304A) was around 120 ps FWHM. The maximum speed of the PPG was 3.35 GHz which could be varied and frequency dividers could also be used to vary the pulse repetition rate.

A separate voltage source was used to pass a small current over one side of the MZI to achieve thermo-optic phase modulation. The voltage could be set with a precision of 1 mV with typically 200 to 700 mV being required for modulation. These values depended heavily on the fabrication of the device as well as different resistances from packaging.

A 10 kΩ thermistor placed in the copper mount was used to give feedback to a PID loop controlled by an Arroyo 6601 and a Peltier under the chip mount stabilised the temperature. The temperature is maintained around 25 °C with an instability of less than 0.01 °C.

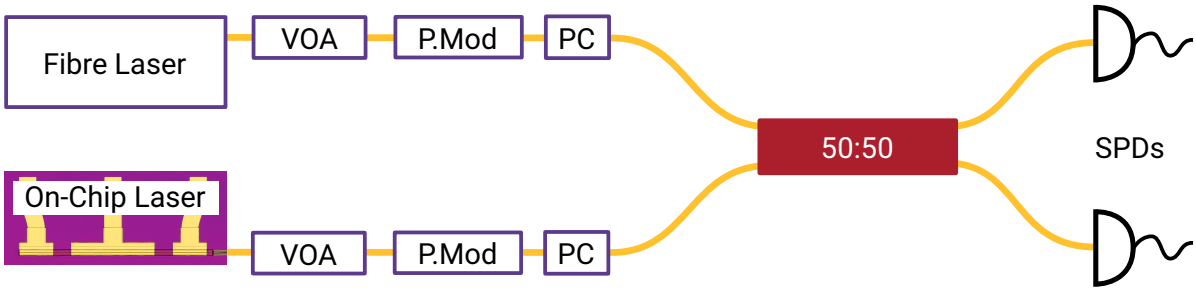


Figure 3.13: Experimental schematic for HOM interference between a fibre laser and on-chip laser with external pulse modulation. Both the on-chip and fibre CW lasers are modulated into WCPs with digital VOAs and lithium niobate intensity modulators (P. Mod). Polarisation control (PC) contains both a polarisation rotator and a PBS to ensure overlap. The pulses interfere at a 50:50 beam splitter and the outputs are measured by SPDs.

3.8 Fibre Optic Hong-Ou-Mandel Demonstration

To simplify the first tests of the integrated devices, a transmitter was set up using a fibre laser and lithium niobate intensity modulators so that HOM interference could be demonstrated with a tested source. The on-chip laser was also intensity modulated using a separate fibre modulator. A schematic of the experiment is shown in figure 3.13. This setup would let us isolate the chip laser to characterise the interference using commercial components.

3.8.1 Fibre Laser Wavelength Sweep

The initial tests of the system used the wavelength tunability of the fibre laser as the variable degree of freedom while the on-chip laser remained fixed in wavelength and power. This first demonstration would show that the integrated laser source would have a long enough coherence over the 100 ps pulse to interfere. This would also provide information about the precision required from tunability of the on-chip laser.

The wavelengths of the individual lasers were first coarsely overlapped on an OSA. Then the fibre laser could be finely tuned relative to the integrated laser and coincidence counts measured. The timing of the pulses was controlled with electrical delays in the PPGs and a histogram used to overlap them with picosecond resolution. For this experiment the system clock was set to 1.72 GHz. A pulse was sent every 4 clock cycles for a state repetition rate of 431 MHz. Polarisation controllers and PBSs ensured both transmitters were in the same polarisation mode before interference.

In figure 3.14, we show the single and coincidence events as the fibre laser is swept in 1 pm steps over a 150 pm range. As the two transmitters become more indistinguishable in wavelength, the number of coincidences reduces close to the theoretical maximum visibility of 50 %. From the current injection of the on-chip laser in figure 3.7, we can see that this level

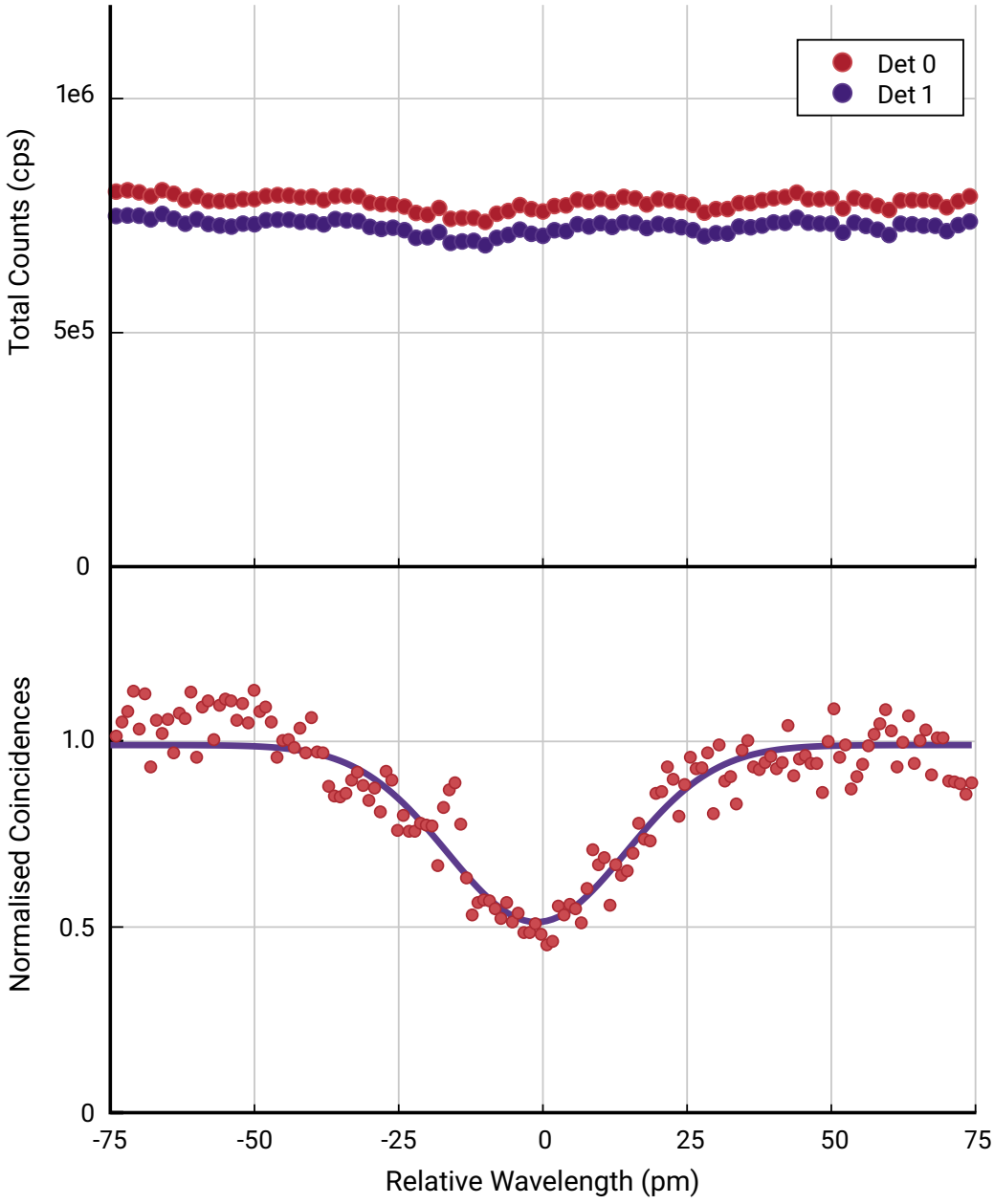


Figure 3.14: The fibre laser wavelength was tuned over a 150 pm range relative to the fixed on-chip laser. The pulses were interfered on a beam splitter to show good interference of 48.4 ± 1.8 % which is close to the theoretical limit. The total counts remain constant through the sweep showing that the coincidence dip is not explained through classical interference.

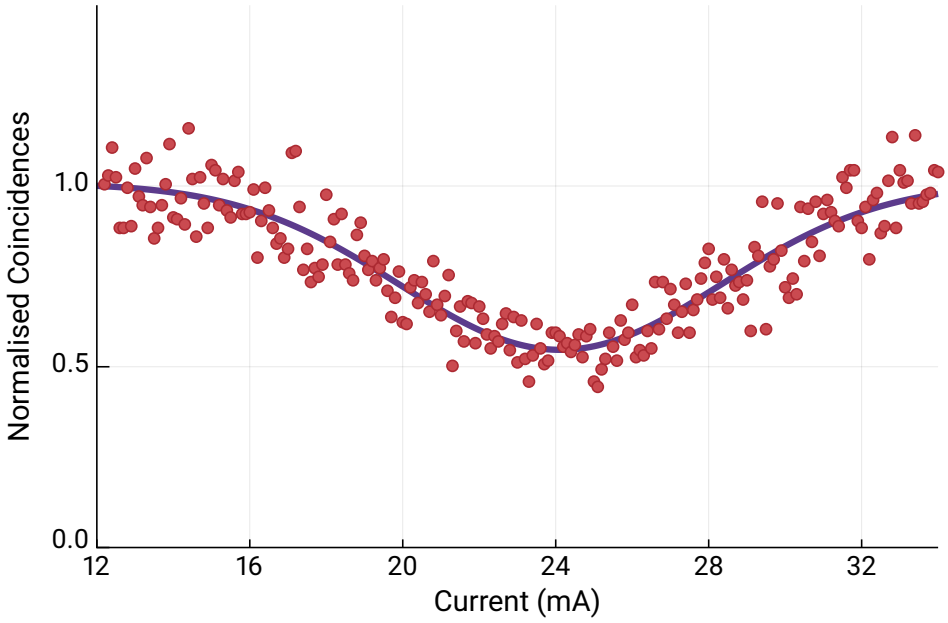


Figure 3.15: By increasing the current of the on-chip laser, whilst keeping the fibre laser fixed, we can change the relative wavelength through heating effects. We find HOM interference as the lasers become indistinguishable in wavelength. The total number of counts on each detector was used to vary the attenuation to account for the increasing laser power. From the fit, we find a visibility of 45.7 ± 2.0 %.

of precision is well within the capability of the chip.

By looking at the total number of counts in each detector, we can see that they do not vary with the change in coincidences. This demonstrates that the reduction in coincidences cannot be attributed to classical interference. The difference between the detector counts is due to a slight difference in efficiency between detectors.

3.8.2 On-Chip Laser Current Sweep

As we have demonstrated that the on-chip laser can show HOM interference, we now need to show that the wavelength of the laser can be controlled with the precision required.

Using the same experimental setup as in figure 3.13, we can fix the wavelength of the fibre laser and use the current injection of the integrated laser to tune the wavelength. As the current injection will also vary the photon number per pulse, we used a digital VOA with feedback from the sum total number of events from both SPDs.

In figure 3.15, we change the wavelength of the chip laser by sweeping the driving current from 12 to 34 mA. As before, we see a reduction in coincidence counts close to the maximum visibility of 50 % [134]. The number of counts in each detector remained constant through the experiment verifying that this is not coherent interference between lasers.

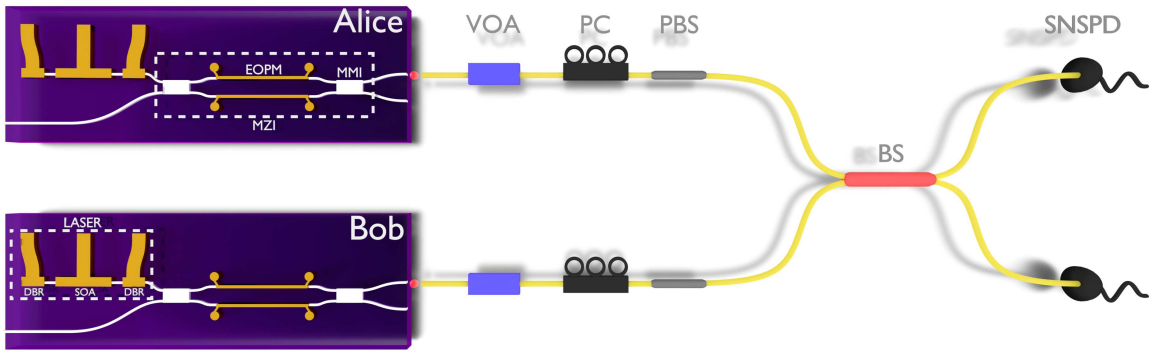


Figure 3.16: Experimental setup of of the HOM interference experiment. Two identical InP chips prepare quantum states of light to be interfered on a 50:50 beam splitter. On-chip CW lasers are intensity modulated into time bins with MZIs. The pulses are coupled into a fibre where variable optical attenuators (VOAs) ensure matched intensities and polarisation controllers (PCs) and polarising beam splitters (PBSs) overlap the polarisation. Pulses are interfered on a beam splitter (BS) and detected by superconducting nanowire single-photon detectors (SNSPDs). An optical channel (not shown) synchronises the transmitters and detectors.

3.9 Hong-Ou-Mandel Interference Between Independent Integrated Devices

Having demonstrated that the linewidth and control of the chip laser was sufficient to demonstrate interference, the next step is to demonstrate that two independently controlled devices could show the same interference.

The experiment uses two InP devices which we will call Alice and Bob and a schematic is shown in figure 3.16. Each chip measures only $6 \times 2\,\mathrm{mm}^2$ and contains all the photonic components to generate the required states to perform HOM interference between independent devices. One only need compare the sizes of these optical components to fibre based optics to justify the benefits of integrated devices.

3.9.1 HOM Interference

Hong-Ou-Mandel interference was demonstrated between two independent photonic integrated circuits (PICs) by varying the relative wavelengths of the lasers, where weak coherent states (WCSs) were modulated from CW lasers at 431 MHz using MZIs. The relative wavelength of the lasers was chosen as the distinguishing degree of freedom as all others could be overlapped manually. However, a sweep in timing or polarisation would have seen similar interference provided a good wavelength overlap.

The two transmitters were initially overlapped in time, polarisation and photon number. Using ps resolution electronic delays in the pulse generation, a histogram from the SPDs allowed a timing overlap between the pulses at the beam splitter. Care was taken to ensure that the

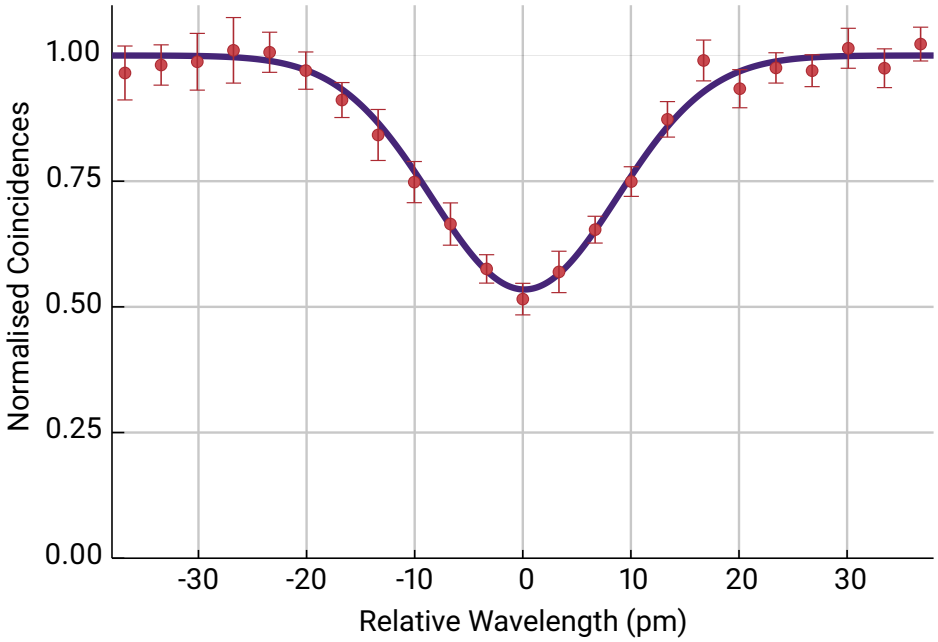


Figure 3.17: HOM dip between independently generated WCPs by two integrated devices. By changing the relative wavelength between the two devices, we demonstrate a reduction in coincidences due to HOM interference. From the fit (shown in purple) we find a visibility of 46.5 ± 0.8 % which is limited to 50 % for coherent states due to multi-photon terms.

pulses that were overlapped on the histogram matched with the pulses that could have interfered on the beam splitter and not a repetition rate or sync window apart. This required calibration of the relative optical and electronic delays after the beam splitter.

Similarly, the photon number of each pulse was calibrated using a histogram of the pulses relative to one another. This allowed the photon number to be calibrated regardless of the detector efficiency and fibre losses, provided that the beam splitter was balanced. By looking at each transmitter independently an average photon number per pulse was calculated to be 10^{-3}. The value was chosen to minimise effects from multi-photon terms in the coherent state and to be far away from saturation of the detectors, both of which would have reduced the visibility.

As previously mentioned, current injection into the SOA can be used to vary the wavelength with a precision of 80 fm. However, this will also change the power of the laser and increase the number of photons per pulse. Therefore, a digital VOA was used to vary the attenuation during the sweep based on the sum total of detection events. The assumption was made that the losses (coupling or otherwise) did not vary during the experiment.

The polarisation of the transmitters was rotated using fibre polarisation controllers and the pulses were immediately sent through a PBS after which was kept in polarisation maintaining fibre. The beam splitter used polarisation maintaining fibre to ensure that the polarisation did

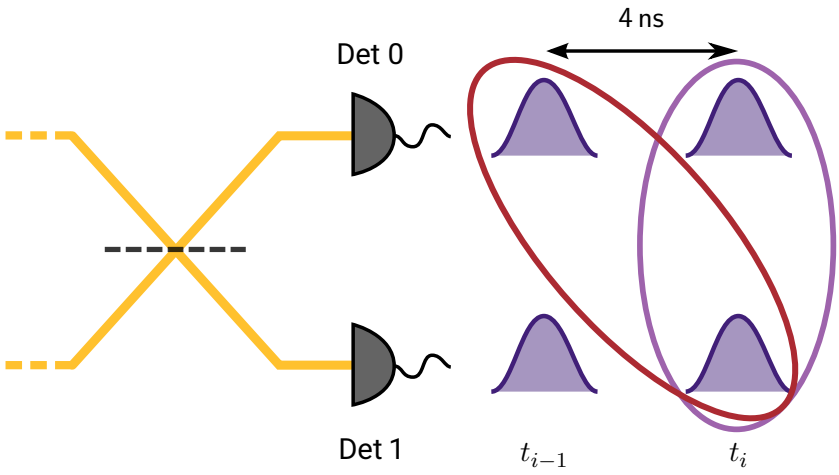


Figure 3.18: Schematic for how coherence of the lasers can be checked through coincidences of events between the two detectors in different time bins, t_i. The colours are the same as those used in figure 3.20. We can check between states that interfered on the beam splitter (purple) and those that did not interfere (red).

not change after the beam splitter. After the interference, the polarisation maintaining fibre was no longer required as only the time of arrival of photons was important at the detectors.

In figure 3.17, we demonstrate Hong-Ou-Mandel interference between the two devices by sweeping the relative wavelengths of the lasers. From a Gaussian fit we find a visibility of 46.5 ± 0.8 %. It is pertinent to note that during the experiment there was no active feedback to control the polarisation, pulse carving or timing which demonstrates the stability possible with an integrated platform.

3.10 HOM Interference with Actively Phase Randomised Pulses

We have previously discussed that, to demonstrate quantum interference instead of classical interference, the laser pulses should be phase randomised relative to one another. In the previous experiment, as the lasers were not phase locked, we could average over the phases by taking data for long enough for the phases between the two lasers to drift. However, for QKD purposes this would not meet criteria for security. This means that we need to be able to actively create pulses with randomised phases between states. This section will describe how we can utilise gain-switching to create phase randomised windows and intensity modulation to create well-defined pulses.

To verify that the WCPs are phase randomised, we can use coincidence counts between neighbouring pulses while both lasers are active. By this, we mean that we will look at events that occurred in the two detectors, but were separated by a time bin. This is shown in figure 3.18 where we introduce the time bins t_i and t_{i-1}. Events that happened in the same time bin

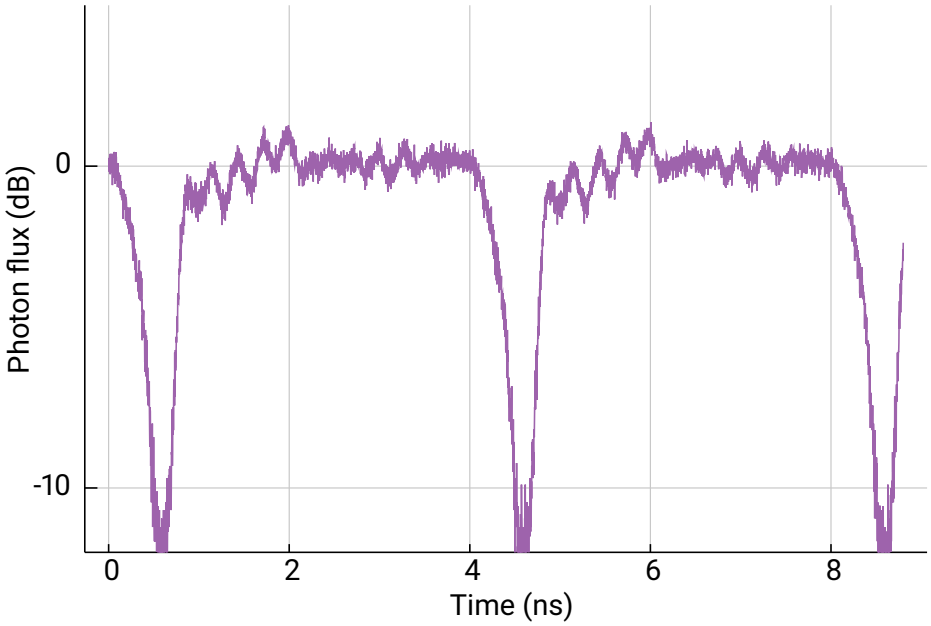


Figure 3.19: Photon flux of the on-chip laser during gain-switching as measured by an SPD. A 200 ps −1.5 V RF signal is applied to the cavity at 250 MHz. The laser power oscillates for 1 ns after lasing resumes due to mode competition. After stabilising, a 2 ns window can be used for coherent state encoding.

will have interfered at the beam splitter so we can verify the HOM visibility. This is shown in purple. However, we can also look at events that are separated by a time bin (i.e. coincident events between t_i and t_{i-1}) which is shown in red. If the lasers have a coherence time that is much longer than the separation between the time bins, we would expect to see the same HOM interference. This is because there will be a fixed phase relationship between the states sent in time bin t_i and t_{i-1}.

However, if we were to phase randomise between these states, it would no longer be true that there would be a fixed phase relationship so we would see no correlation between subsequent time bins.

Laser gain-switching is a technique used to cause phase randomisation by keeping the laser below threshold and only applying current when a WCP is desired. As the pulses are limited to the timing of a spontaneous emission, the timing jitter of the pulses is usually large. There is also a wavelength broadening meaning that optical filtering is required for HOM interference [119].

Instead of gain-switching to generate pulses, we can reverse the high-speed pulse to provide a negative voltage between pulse carving. These pulses removes the carriers in the diode and allows the optical cavity to empty to make phase randomised windows. The upper-state lifetime of semiconductors is short, as is the cavity lifetime, meaning this can still be done at a

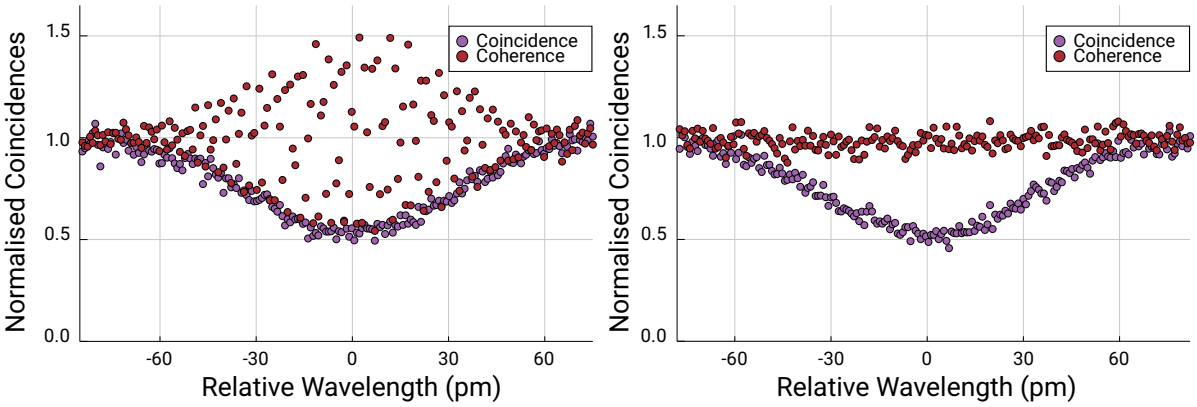


Figure 3.20: HOM interference both without (left) and with (right) phase randomisation between pulses. We show the coincidences between pulses that interfered and check the coherence with subsequent pulses. In case without phase randomisation, we find a fitted visibility of 47.3 ± 1.0 % while when actively phase randomising we find 48.1 ± 1.1 % visibility.

high repetition rate.

In figure 3.19, we demonstrate gain-switching the on-chip laser by providing a −1.5 V RF signal. This drains the cavity so that when lasing resumes the phase will come from a spontaneous emission and will be random compared with the previous window. The internal clock of the PPG was set to 2 GHz for this experiment, with a pulse being sent by each transmitter every 8 clock cycles giving a state repetition rate of 250 MHz.

After the negative signals, the lasing oscillates before returning to a continuous (and useful) lasing mode. These oscillations can be attributed to mode competition in the laser cavity and also ringing in the RF signal. Therefore, we can still generate states at 250 MHz and demonstrate good state preparation through intensity modulation.

In figure 3.20, we demonstrate two HOM fringes without (left) and with (right) active phase randomisation between states. The two independent lasers are never coherent as they are independently driven. Both experiments see a visibility of more than 47 %. When the pulses are coherent, we see a partial relationship between the pulses as the relative wavelength between the lasers changes. If there was complete coherence, this would be a sinusoidal fringe as subsequent pulses tune in and out of phase (similar to the error fringe from Bell state projections seen in the next chapter). After phase randomisation, we find no relationship between coincidences of subsequent pulses.

We have demonstrated that by combining gain-switching and intensity modulation of an integrated CW laser can produce phase randomised WCPs. The states are capable of HOM interference maintaining a comparable visibility to state-of-the-art without requiring any external wavelength filtering.

3.11 Outlook

In this chapter, we have demonstrated state-of-the-art Hong-Ou-Mandel interference between independent, integrated photonic devices. By utilising monolithically fabricated lasers and EOPMs, we generated WCPs with precise control over all degrees of freedom. By changing the relative wavelength of the devices, we demonstrated a HOM dip with a visibility of 46.5 ± 0.8 %. Further, we demonstrate gain-switching of the on-chip laser to provide actively phase randomised pulses. We show that the introduction of phase randomisation doesn't reduce the visibility of the interference and also doesn't require the pulses to be wavelength filtered.

The stability and scalability of this integrated platform makes it a good contender for accessible metropolitan QKD. This demonstration is the first step towards chip-based MDI-QKD which facilitates resource sharing without sacrificing security by introducing trusted nodes. Access can be provided through the cheap and scalable InP platform, while expensive resources, such as SPDs, optical switches and time taggers can be shared between all users. The flexibility of the integrated photonic platform allows increased rates through wavelength division multiplexing [153] and enables fully integrated systems through on-chip detection [154] further reducing a major barrier towards widespread quantum secure communications.

3.11.1 Active Stabilisation

Performing this experiment in a controlled laboratory environment is obviously favourable for prolonged operation over several hours. However, as the aim will be to create devices that can be deployed on real-world networks, the systems will need to compensate for drifts in the fibres and electronic control.

Polarisation drifts could be stabilised by using the unused arm of the PBS. An electrically controlled polarisation rotator could employ a feedback loop to reduce the power of the unused arm. At the single-photon level, the number of detection events on an SPD can be used as feedback to the control system and the polarisation rotated to maximise the extinction ratio. It has been demonstrated in field trials that polarisation in deployed fibre is more favourable with regards to polarisation drift than spooled lab fibre [155].

Wavelength can be stabilised using the visibility of HOM interference by minimising coincidences. By changing the current one transmitter, the wavelength can be precisely tuned. While this will change the power of the laser, if only small changes in current are required then this power change will be negligible.

Timing stabilisation can be achieved by looking at the time of arrival of the pulses. In particular, the FWHM can be used to ensure that the pulses are overlapped i.e. minimising the FWHM in the histogram of detection events means that the pulses will be maximally overlapped.

Given a good current source to drive the laser, the average photon number is unlikely to

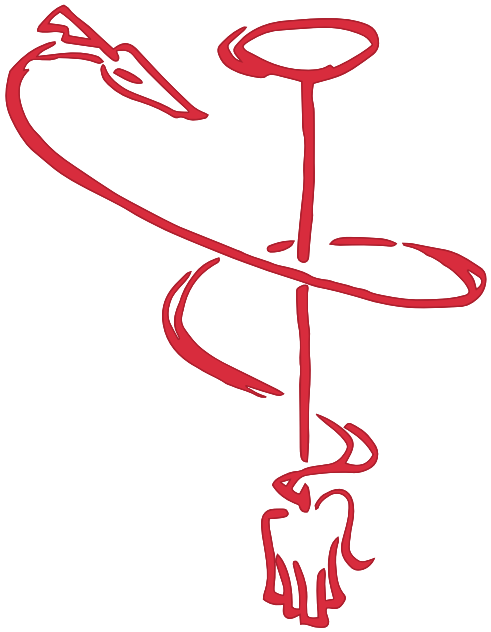
change dramatically. On-chip fast photodiodes can be used to locally monitor the power to provide any required feedback. Having fibres fixed to the chips with UV cured glue will remove any change in loss from fibre coupling.

3.11.2 Wavelength Division Multiplexing

As mentioned previously, there is no need to filter the pulses to see interference. This is important as it allows the transmitters to be easily wavelength tuned making it compatible with WDM and possible classical-quantum multiplexing. An interesting demonstration of this would be to multiplex the quantum signals with classical data to verify that quantum interference can still be seen. This could be an important consideration for compatibility with future networks. One would need to consider cross-talk from neighbouring channels to ensure maximal interference.

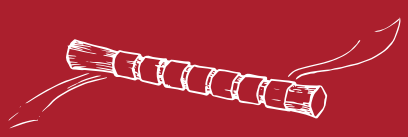
3.11.3 DFB Laser

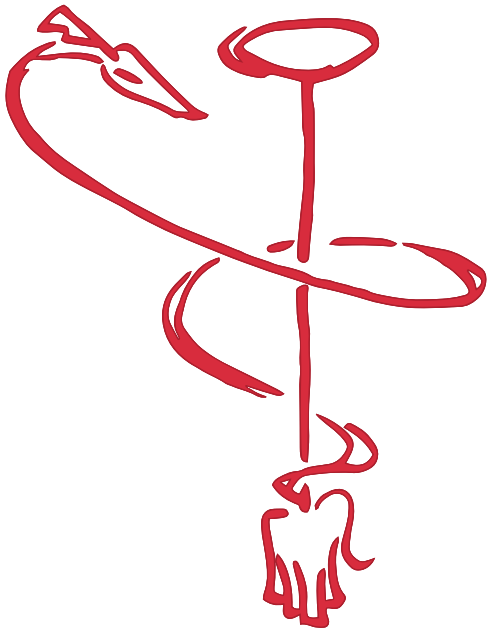
The delay caused by the laser relaxation after phase randomisation could be reduced by using a distributed feedback (DFB) laser. DBR lasers will take time to relax after gain-switching as the cavity will support many modes until a single mode becomes dominant. This behaviour is shown in figure 3.19 where the laser oscillates before becoming more stable. DFB lasers typically have a higher bandwidth which would reduce the amount of time required for the laser to stabilise.



4

Chip-Based Measurement-Device-Independent Quantum Key Distribution





Statement of Work

The work in this chapter made used of devices conceived and designed by Mark Thompson and Mark Godfrey. Mark Godfrey compiled the chip mask that was then fabricated by Oclaro. The experimental setup was modified from the previous chapter with support from Philip Sibson. FPGA and RF electronic design was supported by Andy Hart. I performed the experiment and analysed the data to estimate key rates. Security analysis of the transmitters was performed in collaboration with The National Physical Laboratories using an FPGA programmed by Andy Hart. I developed the experiment and operated the integrated transmitters. The integrated receiver concept was designed by Nicola Tyler, Philip Sibson, Jorge Barreto and Mark Thompson. Silicon devices were fabricated in Glasgow in the group of Robert Hadfield. I performed analysis and simulation of an measurement-device-independent quantum key distribution system with estimated parameters to inform fabrication decisions. Initial tests of components was performed by Ben Slater and Robert Heath but are not included in this thesis. Parts of this chapter have been published and are available in references [103,104,156]. Where appropriate, text and figures have been reused that had been written or created by me.

4.1 Introduction

Quantum technologies promise a paradigm shift compared to their classical counterparts that will undermine our current methods of secure communication [1]. It will soon become necessary to deploy key exchange systems that are immune to such increases in computing power. As introduced previously, quantum key distribution (QKD) is one such approach which exploits quantum phenomena to exchange secret keys between distant parties without relying on assumed computationally hard problems [3, 4]. However, the stringent requirements for precise control has predominately limited QKD systems to small networks and laboratories. To realise ubiquitous quantum devices, new platforms are required for robust operation in harsh environments.

The integrated photonics platform, that was utilised in chapter 3, has seen vast improvements in recent years and represents a promising platform for mass-adoption of quantum technologies [157]. In particular, indium phosphide (InP) offers crucial benefits for communication in a robust, phase-stable and compact platform including monolithically integrated lasers with mW powers and narrow linewidths. We saw that fast electro-optic phase modulation allow manipulation of light at a bandwidth of 10 GHz. Using the same components, we can encode timing and phase on states of light which makes the platform well suited for quantum communication protocols [9].

Quantum-secured communication has been a leading quantum technology since its advent [3, 4] and has seen many proof-of-principle demonstrations, networks and commercial

systems [136, 137, 158–160]. However, implementation security of these systems is an active area of research due to potential information leakage that is not considered in security proofs. Such side-channels may allow an eavesdropper to gain sensitive information during a key exchange [161] or an attacker to manipulate a system and determine the secret key through classical means [81, 162].

To counter these attacks from Mallory through uncharacterised side-channels, device-independent QKD schemes have been developed to limit the number of assumptions required for security [163]. One such prominent vulnerability is with single-photon detectors (SPDs) for which measurement-device-independent QKD (MDI-QKD) has been proposed [7]. This approach removes all possible attacks against the detection system.

In this chapter, we experimentally demonstrate MDI-QKD using cost-effective, mass manufacturable, chip-based transmitters that could facilitate commercial quantum-secured communication. We show that 1 kbps of secret key can be exchanged at 100 km and predict positive key rates at more than 350 km. The system removes detector vulnerabilities and represents a viable solution for near-term metropolitan quantum networks.

4.2 Measurement-Device-Independent Quantum Key Distribution

Device-independent QKD (DI-QKD) protocols were invented out of a necessity to counter developments by the quantum hacking community [6]. Systems that were thought to be secure would readily leak information to an adversary through uncharacterised or overlooked side-channels [161]. While there are proven methods of removing these attacks from a system [88], the attacks must first be publicly known. Therefore, any such countermeasures provide no guarantee against future attacks that may be present in a system.

DI-QKD removes all assumptions about the physical system apart from two. The only assumptions required about the system are

1. Alice and Bob have their own devices that are spatially isolated.
2. All parties (Alice, Bob, Charlie, Eve and Mallory) must obey quantum mechanics.

The assumptions don't require Alice or Bob to trust the devices they are given, and it could be assumed that an adversary was preparing the quantum states. Through a Bell test, Alice and Bob can verify that their protocol was secure, regardless of whether they trust the equipment. While DI-QKD maximises security, the difficulties of performing a loophole free bell test mean that proposed protocols are not yet a practical method of key exchange. Loophole-free tests have been performed but require low-loss links and high detection efficiency [41–43].

To increase security in a practical way, new device-independent protocols were developed. MDI-QKD removes all potential side channels on the detection system which could be ex-

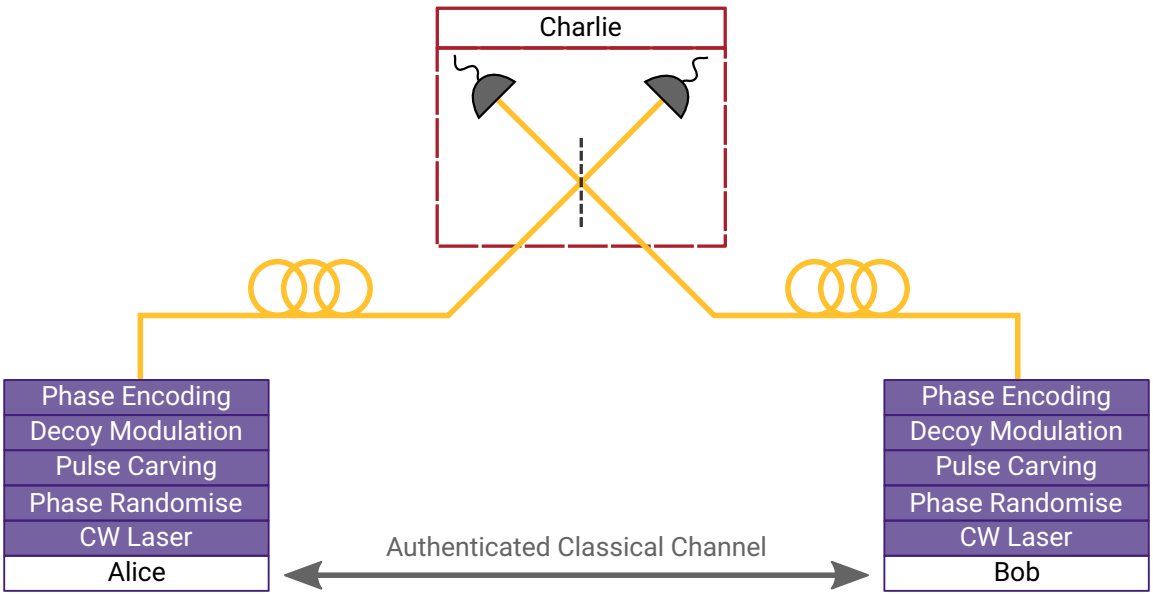


Figure 4.1: MDI-QKD protocol schematic for time-bin encoding. Alice and Bob act symmetrically by generating BB84 states and sending them to Charlie, an untrusted third party, over quantum channels. Charlie projects the states in the Bell basis and announces all successful events. Alice and Bob can then infer a key after sharing state basis information over an authenticated classical channel which can be public.

ploited by a malicious adversary [7]. A schematic of the experiment is shown in figure 4.1. Unlike traditional point-to-point protocols, Alice and Bob act symmetrically by sending Bennett-Brassard 1984 (BB84) states to a third party, Charlie. Upon receipt of the states, Charlie measures the states in the Bell basis and publicly announces all successful events. The outcomes indicate quantum correlations between states but, without encoding knowledge known only by Alice and Bob, reveal no information about the secret key. This allows Charlie to be completely untrusted and it could even be assumed that Eve or Mallory is operating the receiver without compromising the security. By sharing the basis information for each state, Alice and Bob are able to infer a secret key which can be used in a symmetric key algorithm.

As we use a weak coherent source, we need to estimate the number of single-photon events. We employ a four-intensity decoy state analysis [164] to bound the single-photon errors and yields. In this protocol, the Z basis is used to generate key while the X basis bounds the knowledge of an eavesdropper.

While MDI-QKD typically offers a lower key rate at short distances when compared with point-to-point systems [9], it can generate a positive key rate at greater distances [158] as the errors are proportional to the square of the dark count probability. It also offers the potential for the measurement equipment to be shared between multiple parties through optical switching without compromising security. The protocol removes the asymmetry between Alice and

Bob which allows for simpler metropolitan networks without reducing security by introducing trusted nodes.

4.2.1 Protocol

Here, we outline more explicitly the protocol that Alice and Bob will use to distribute their random secret. A schematic of the protocol is shown in figure 4.1.

1. Preparation Alice and Bob, independently and randomly, choose weak coherent states (WCSs) from the four BB84 states: $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. They will also choose an intensity, at random, to satisfy a decoy state protocol. The bases choices do not need to be equally weighted and the optimal choices will depend on the gains and errors in a finite key regime. Both the state and intensity choice should remain secret at this stage. These states are then sent to Charlie via the quantum channels.

2. Measurement Upon receipt of the states from Alice and Bob, Charlie performs a joint Bell state projection. The physical projection will depend on the encoding used. In a time-bin encoding scheme, coincidences between early and late clicks of two detectors indicates $|\psi^{\pm}\rangle$ projections, as shown in figure 4.2. Using linear optics, it is only possible to project onto two of the four Bell states [165, 166]. However, security can be guaranteed even if projection onto only one Bell is possible.

3. Announcement Each successful projection is publicly announced by Charlie, along with timing information. Unsuccessful events (those that are not coincidence clicks) are not required for the key exchange. However, they can be useful as feedback to Alice and Bob to calibrate their systems.

4. Basis Discussion Alice and Bob each announced the basis chosen for each successful projection, but not their chosen bit. When their bases choices were the same, they can use the rules in table 4.1 to determine a shared key. In each case (except where they both sent in the X basis and the outcome was $|\psi^{+}\rangle$) either Alice or Bob flips their bit.

5. Parameter Estimation Using the public information from Charlie about successful projections, Alice and Bob can calculate error rates and gains to bound the knowledge of Eve. They can then apply error correction and privacy amplification on their secret bit string, as required.

MDI-QKD has been used to demonstrate key rates at distances much further than those possible with traditional point-to-point systems [158]. This is due to how the signal rate compares with the error rate. The distance limitation of a QKD system is when the probability of a successful event becomes on the order of a error due to the dark count rate of the system. In a

Basis	$\|\psi^-\rangle$	$\|\psi^+\rangle$
Z	Bit flip	Bit flip
X	Bit flip	-

Table 4.1: Post-selection rules of measurement outcomes in different bases. If Alice and Bob sent states in the same basis, one of them will have to bit-flip unless they both chose the X basis and the result was $|\psi^+\rangle$.

QKD system, we need to compare the probability of a pulse being transmitted over an optical fibre and being detected by the system. So for some WCS with intensity μ and detector with efficiency η, we have the probability of a successful event being

$$1 - e^{-10^{0.2 \cdot L/10} \cdot \mu \cdot \eta} \tag{4.1}$$

for some distance L between Alice and Bob and assuming 0.2 dB/km loss from optical fibres.

A given detection system will have a probability of dark count that we will call $P^{d.c.}$. So for a protocol such as BB84, when we have

$$P^{d.c.} \approx 1 - e^{-10^{0.2 \cdot L/10} \cdot \mu \cdot \eta} \tag{4.2}$$

then the system will no longer be able to generate a positive key rate as the dark counts will dramatically increase the error rate in the system.

In comparison, an MDI-QKD system looks for coincidence measurements between detectors to indicate successful events. Therefore, for the same distance of fibre between Alice and Bob, the limit will be on the square of the dark count rate i.e. $(P^{d.c.})^2$. While the requirement for coincidences for a projection will also limit the number of successful events, the quadratic reduction in errors will allow key generation at much further distances.

This is only a limiting factor if the dark count rate of the detector system is significant. Recent advances in superconducting nanowire single-photon detectors (SNSPDs) have shown that SNSPDs can run for many hours without a single dark event [110]. Then standard point-to-point links can show positive key rates at more than 400 km [167].

4.2.2 Bell State Projection

To understand how the states are projected in the Bell basis, consider the entangled states in a time-bin encoding

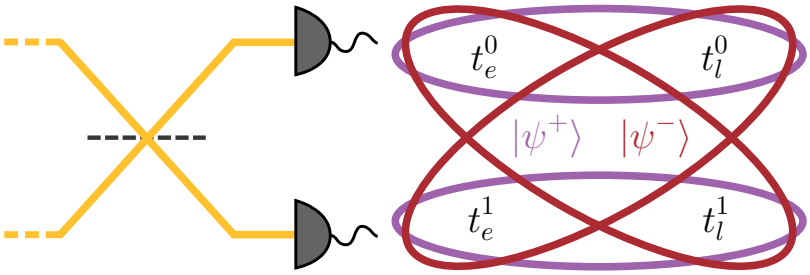


Figure 4.2: Coincidences between detectors for successful Bell state projections in a time-bin encoding. Both $|\psi^+\rangle$ (purple) and $|\psi^-\rangle$ (red) are shown as coincidences between time-bins of the detectors. t_j^i corresponds to a detection event in the ith detector, where j is either an early (e) or late (l) time-bin.

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}_e^\dagger \hat{b}_l^\dagger \pm \hat{a}_l^\dagger \hat{b}_e^\dagger\right)|00\rangle \tag{4.3}$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}_e^\dagger \hat{b}_e^\dagger \pm \hat{a}_l^\dagger \hat{b}_l^\dagger\right)|00\rangle \tag{4.4}$$

where e and l refer to early and late time-bins of the state. Considering the Bell states incident on a beam splitter, we find

$$|\Phi^{\pm}\rangle \rightarrow \frac{1}{2}(\hat{c}_e^\dagger \hat{c}_e^\dagger - \hat{d}_e^\dagger \hat{d}_e^\dagger \pm \hat{c}_l^\dagger \hat{c}_l^\dagger \mp \hat{d}_l^\dagger \hat{d}_l^\dagger)\,|00\rangle \tag{4.5}$$

$$|\psi^{+}\rangle \rightarrow \frac{1}{\sqrt{2}}(\hat{c}_e^\dagger \hat{c}_l^\dagger - \hat{d}_e^\dagger \hat{d}_l^\dagger)\,|00\rangle \tag{4.6}$$

$$|\psi^{-}\rangle \rightarrow \frac{1}{\sqrt{2}}(\hat{c}_e^\dagger \hat{d}_l^\dagger - \hat{c}_l^\dagger \hat{d}_e^\dagger)\,|00\rangle \tag{4.7}$$

So we find that by just using a beam splitter and threshold detectors, it isn't possible to distinguish $|\Phi^{\pm}\rangle$ states. We can actually go further with this statement to say that only two of the four Bell states can be detected simultaneous with linear optics [165, 166]. However, through coincidences between time of arrival of the photons at the detectors, we can project onto $|\psi^{\pm}\rangle$ states. These projections are shown in figure 4.2 where the photons interfere on a 50:50 beam splitter and timing information of successful detections can be correlated.

4.2.3 Security and Key Rate Estimation

The security of QKD protocols is founded in the no-cloning theorem of quantum mechanics. When Alice and Bob send their single photons, they can be sure that Eve cannot faithfully

duplicate the states to copy the information. However, Alice and Bob will not be sending true single photons, but instead will send weak coherent states. As there is the possibility of multi-photon events, regardless of how small, Alice and Bob will need to bound the number of events that were true single photon events. It is commonplace to use a decoy state protocol, where Alice and Bob vary the average intensities of their states at random [168]. It is possible to perform secure QKD without decoy state analysis, but the key rates are drastically reduced [59].

For a decoy state protocol, the estimated key rate of MDI-QKD per pulse in the asymptotic case is given as [161]

$$R = (p_z)^2 Y_{11}^Z \left(1 - H_2(E_{11}^X)\right) - Q_{s,s}^Z f_e H_2(E_{\mu_s\mu_s}^Z) \tag{4.8}$$

where Y_{11}^Z and E_{11}^X are the yield in the Z basis and error in the X basis, respectively, when Alice and Bob both sent single photons. These quantities are not directly measurable so we will need to bound them using a decoy state protocol. $Q_{S,S}^Z$ and $E_{S,S}^Z$ are the gain and error in the Z basis and both can be measured directly. p_z is the probability that Alice and Bob choose to send a state in the Z basis. In a biased-basis scheme, this can be chosen arbitrarily to maximise key rate provided that finite key effects are accounted for. In the asymptotic limit, this will be set to 1. Finally, we introduce the error correction inefficiency, $f_e > 1$, which is typically 1.16 and the binary entropy function defined as

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x). \tag{4.9}$$

As we are not using single photons, we cannot determine the single photon errors and yields exactly. Therefore, we need to use a decoy state technique [59] to give lower and upper bounds of Y_{11}^Z and E_{11}^X, respectively. We then need to define the lower bound of the secret key rate as

$$\underline{R} \leq R \tag{4.10}$$

In essence, decoys states are measuring the loss of the channel during a key exchange to bound the knowledge that could be gain by an eavesdropper. By Alice and Bob sending different intensities in a decoy state protocol, they can measure

$$Q_{\mu_a\mu_b}^{\{X,Z\}} = \sum_{n,m} e^{-(\mu_a+\mu_b)} \frac{\mu_a^n}{n!}\frac{\mu_b^m}{m!} Y_{n,m}^{\{X,Z\}} \tag{4.11}$$

$$Q_{\mu_a\mu_b}^{\{X,Z\}} E_{\mu_a\mu_b}^{\{X,Z\}} = \sum_{n,m} e^{-(\mu_\mathrm{a}+\mu_\mathrm{b})} \frac{\mu_\mathrm{a}^n}{n!}\frac{\mu_\mathrm{b}^m}{m!} Y_{n,m}^{\{X,Z\}} E_{n,m}^{\{X,Z\}} \tag{4.12}$$

where μ_a (μ_b) are the intensities of Alice's (Bob's) pulses. The gain, $Q_{\mu\sigma}^i$, is defined to be the number of successful Bell state projections when Alice and Bob send states in either the basis

i with intensities μ and σ, respectively. These measurable values provide a set of linear equations which can be used to bound the yield and errors for single photon events.

In this experiment, we used a four intensity decoy state protocol [164] where we consider four sources: ν, σ, μ, s. The ν source is vacuum, σ and μ are decoy pulses in the X basis with average photon numbers σ and μ, respectively. Finally, the s source emits pulses with intensity s in the Z basis only. We will assume that Alice and Bob use the same intensities. In an MDI-QKD protocol, we use the X basis to bound the knowledge of Eve or Mallory and the Z basis to generate key. This is due to the minimum possible error of 25% in the X basis [136] which in turn is due to the reduced Hong-Ou-Mandel (HOM) visibility possible with coherent states [134]. This can be understood by separating the possible cases into those that interfered, and those that didn't. Of those that interfered, we would expect no errors. Of those that didn't interfere, there is a 50 % chance of error.

From the measurable equations 4.11 and 4.12, we can calculate an lower bound on the single photon yield in the X basis as

$$\begin{aligned} Y_{11}^X \geq \frac{1}{P_1^\mu P_1^\omega (P_1^\omega P_2^\omega - P_1^\mu P_2^\omega)} \Big(& P_1^\mu P_2^\mu (Q_{\omega\omega}^X - P_0^\omega (Q_{\nu\omega}^X + Q_{\omega\nu}^X) + (P_0^\omega)^2 Q_{\nu\nu}^X) \\ & - P_1^\omega P_2^\omega (Q_{\mu\mu}^X - P_0^\mu (Q_{\nu\mu}^X + Q_{\mu\nu}^X) + (P_0^\mu)^2 Q_{\nu\nu}^X) \Big) \end{aligned} \tag{4.13}$$

where P_i^m is the probability a coherent state with intensity m contains i photons. In the asymptotic limit $Y_{11}^Z = Y_{11}^X$, which we can use in the key rate formula [169]. We can then calculate an upper bound for the single-photon errors as

$$e_{11}^X \leq \frac{e_{\omega\omega}^X Q_{\omega\omega}^X - P_0^\omega \left(e_{\nu\omega}^X Q_{\nu\omega}^X + e_{\omega\nu}^X Q_{\omega\nu}^X \right) - (P_0^\omega)^2 e_{\nu\nu}^X Q_{\nu\nu}^X}{(P_1^\omega)^2 Y_{11}^X} \tag{4.14}$$

where the lower bound of Y_{11}^X from above is used. Both the single-photon yield and error is calculated from experimental values (such as those provided in appendix A) to determine an estimated key rate.

4.2.4 Model

From the parameters of the system (photon numbers and errors), we can create a model to verify that the system behaves as expected. This will also allow us to predict the performance of the system at further distances without needing to gather data for days or weeks.

The detectors used in this system are SNSPDs due to their high efficiency and low recovery-time and jitter [111]. The detectors operate at 80% efficiency, with a dead-time of $<$100 ns and jitter of 30 ps. The average photon number per state is calibrated before a key exchange by

$E^X_{\mu_a\mu_b}$	μ	σ	ν
μ	30%	40%	50%
σ	40%	30%	50%
ν	50%	50%	50%

Table 4.2: Estimated errors that were used to characterise the Z basis errors that are based on HOM interference and similar papers.

estimating the losses through the system and detection efficiency. The efficiency of detection should also include the losses associated with fibre components preceding detection i.e. polarisation control. In this system, the loss is around 1 dB.

The gain of the system, $Q^{\{X,Z\}}_{\mu_a,\mu_b}$, is the probability of projection onto a Bell state in either the X or Z basis. We can estimate the gain from the average photon number of each transmitter, the detection efficiency and the transmitters loss. We will assume that the transmission loss is the standard 0.2 dB/km, although fibre optic losses can be as a low as 0.14 dB/km [170] while fibres with 0.17 dB/km loss are commercially available [171]. The gain is independent of error, so we can estimate the gain as

$$Q^{\{X,Z\}}_{\mu_a,\mu_b} = \frac{3}{8} \times \left(1 - \exp\left(-10^{-\frac{0.2\times L}{2\times 10}}\mu_a\eta\right)\right) \times \left(1 - \exp\left(-10^{-\frac{0.2\times L}{2\times 10}}\mu_b\eta\right)\right) + Q^{d.c.} \tag{4.15}$$

where $Q^{d.c.}$ are the successful projections that are because of dark counts in the system. As SNSPDs have dark counts of 100 Hz this value is typically $\left(10^{-6}\right)^2$ for the chosen gating window. The value is quoted as squared as we are looking for coincidences between the two detectors.

The 3/8 pre-factor is due to the probability of a successful projection given two random states sent by Alice and Bob. One half of the time, the states will be projected onto a Bell state that cannot be determined by the measurement device [165,166]. Of the remainder, one half will be projected successfully onto $|\psi^-\rangle$ (1/4 of the total states), while with probability 1/2 they will be successfully projected onto $|\psi^+\rangle$ (1/8 of the total states). We will see later that by increasing the number of detectors in the receiver, this can be increased closer to the maximum of 1/2.

To calculate the probability of coincidence from the coherent states, we will use the same derivation from chapter 3. However, here the distance L, which measures the distance between Alice and Bob, is halved. This is because Charlie will sit at a centralised location. We will assume that this is half way between Alice and Bob, so the WCSs from Alice and Bob need to only travel half the distance.

To model the errors, we need to include contributions from dark counts in the system which will have an error probability of 50 %. Therefore, the corrected error rate will be

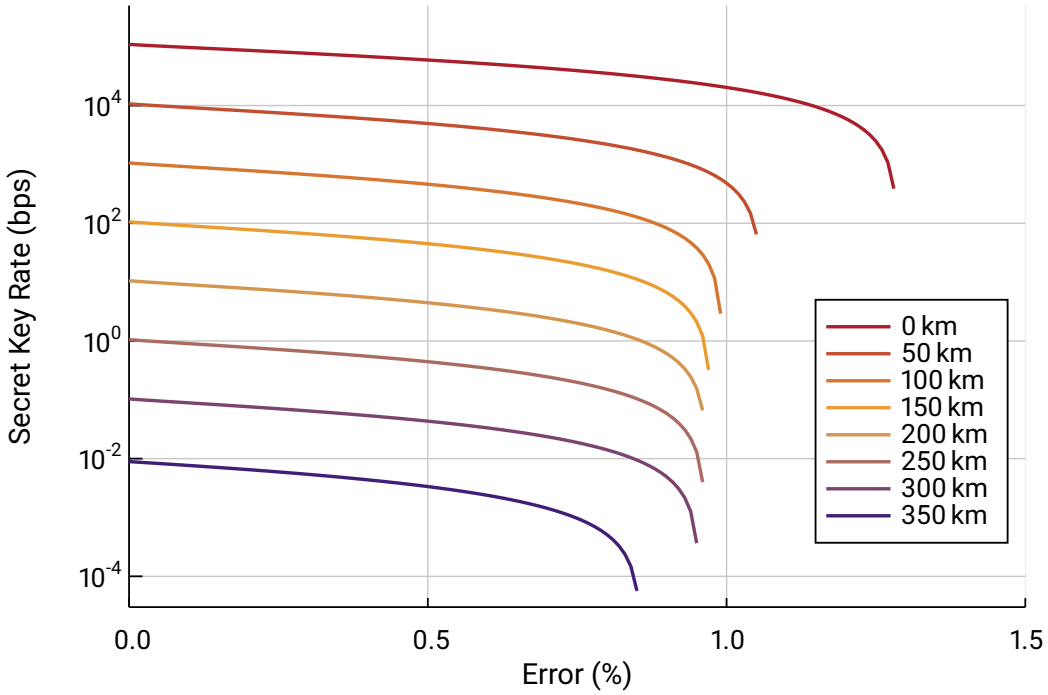


Figure 4.3: By varying the error rate in the signal Z basis, while maintaining consistent errors in the X basis, we can see the dependence of the secret key rate on the quantum bit errors. As the Z basis is used only to generate key, the error must be kept low, especially at longer distances.

$$E_{\mu_a,\mu_b}^{\{X,Z\}} = \frac{\left(Q_{\mu_a,\mu_b}^{\{X,Z\}} - Q^{d.c}\right) \times \epsilon_{\mu_a,\mu_b}^{\{X,Z\}} + Q^{d.c} \times 0.5}{Q_{\mu_a,\mu_b}^{\{X,Z\}}} \tag{4.16}$$

where $\epsilon_{m,n}^{\{X,Z\}}$ are the error rates during a key exchange which will need to estimated from an experiment to accurately model the system. In the equation, the dark events are subtracted from the gain which can then be multiplied by the system error rate. The dark count events can then be considered separately. Positive key rate should be possible until the signal gain is on the order of the dark events.

By using this model, we can start to understand how the system should behave. As we have shown that we can control independent devices well enough to show good HOM interference, the rest of the errors will come from encoding the states. From similar papers, we can estimate what we would expect the X basis errors to be [136,137]. These are given in table 4.2. Setting the photon numbers to 0.2 in the Z basis and 0.1 and 0.01 for the X basis decoy states, we can model what error rates are required in the Z basis.

In figure 4.3, we show the dependence of Z basis errors on the key rate at varying distances. By using predicted values for the X basis, we can vary the Z basis error to find the limit of

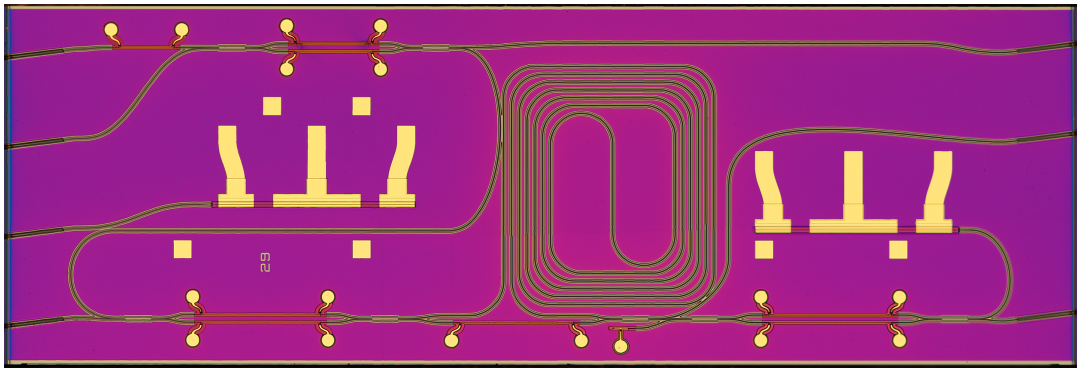


Figure 4.4: Microscope image of the $6 \times 2\,\mathrm{mm}^2$ indium phosphide transmitter. The complexity possible with integrated photonics is demonstrated by having two separate distributed Bragg reflector (DBR) cavity lasers, three Mach-Zehnder interferometers (MZIs), an asymmetric Mach-Zehnder interferometer (aMZI) and a high-bandwidth photodiode (PD). Light is coupled to fibre through spot-size converters (SSCs) at the edges of the chip.

positive key generation. We find that to generate positive key rates at more than 100 km we will require that the error must be below 1 %. This means that we will need to improve the extinction ratio of the pulses in chapter 3 to reduce the time-encoding error. At distances of more than 300 km, even more stringent requirements on the Z basis error are found.

4.2.5 Shared Resources

As MDI-QKD introduces Charlie to mediate the key exchange, this easily facilitates sharing resources by switching between users connecting to a centralised node. In a metropolitan network, each user can access the quantum network with a transmitter device and simple optical switching allows all users to exchange secret keys with every other user. Such optical switches are already available commercially with less than 1 dB insertion loss which is acceptable for QKD systems [172].

While superconducting detectors are currently considered research equipment, there have been many advances in the technology of both the detector fabrication and cryogenic coolers which means that widespread adoption of SNSPDs should be anticipated. More advanced quantum networks will be heavily dependant on the unrivalled specifications that SNSPDs offer. Moreover, the potential for waveguide integrated detectors [111–113], fast modulation at cryogenic temperatures [173] and wavelength demultiplexing [174] means that an MDI-QKD system could benefit from further photonic integration.

4.3 Integrated Transmitters

InP transmitters provide all the required optical components to create high fidelity BB84 states as required for MDI-QKD. By using chip-based transmitters the power, size and weight of the re-

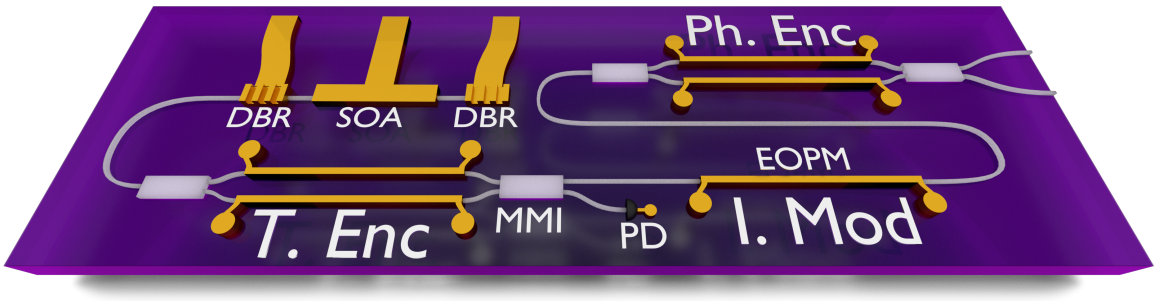


Figure 4.5: A schematic view of each chip used in the MDI-QKD protocol. Electro-optic phase modulators (EOPMs) and multi-mode interferometers (MMIs) are used to encode time-bin states. *T. Enc* is used to intensity modulate the continuous wave laser to encode timing information, *I. Mod* varies the pulse intensity for decoy state preparation and *Ph. Enc* encodes phases between the time-bins. The semiconductor optical amplifier (SOA) can be gain switched for phase randomisation and a fast photodiode (PD) provides on-chip feedback.

quired optical components can be dramatically reduced compared to fibre (and free-space) alternatives. Monolithic fabrication also facilitates mass manufacture without requiring manual assembly which would further decrease cost and increase availability.

It is worth noting that the technology is still maturing and optimisation of designs is still required before devices can be confidently reproduced to a required standard for secure communication. The transmitters used for this experiment (figure 4.4) were originally designed to operate as transceiver modules which would allow two-way operation. The delay line in the centre of the device could be used for encoding and decoding time-bin encoded states. However, the waveguides were found to be too lossy to be useful, showing how further optimisation of designs is required. The design of such a delay line is challenging as the loss in a waveguide can be as high as 2 dB/cm [125]. For a 500 ps delay in a material with a refractive index of 3, the loss could be as high as 10 dB before considering bend losses. These losses are mostly linked to waveguide roughness and two-photon and free carrier absorption in InP [128].

A schematic of the chip is shown in figure 4.5 to clarify which parts of the chip shown in figure 4.4 are used for this experiment. Cascaded Mach-Zehnder interferometers (MZIs) are used to encode time, phase and intensity onto WCSs. We will encode our quantum states in a time-bin encoding scheme and the four BB84 states are shown in figure 4.6. The early and late time-bins of the states will be our $|0\rangle$ and $|1\rangle$ states where a superposition of these creates more complicated states. A relative phase can be applied between the time-bins for a full encoding. We will define the $|+\rangle$ state to be when the two time-bins are in phase. To encode a $|-\rangle$ state, we need to apply a π phase shift between time-bins.

In this section, we will describe the operation of the transmitters to create weak coherent states that can be used for quantum key distribution and expanding the functionality of the

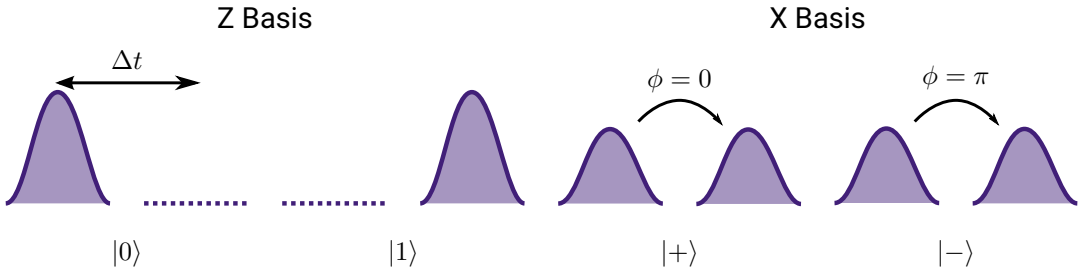


Figure 4.6: BB84 states in a time-bin encoded scheme. Pulses are separated by a time Δt where the timing forms the computational basis. A late pulse indicates a $|0\rangle$ while an early pulse indicates a $|1\rangle$. $|+\rangle$ and $|-\rangle$ states can be realised through superposition of early and late pulses with relative phases. The intensity of the pulses in the X basis is halved so that the average photon number over the states remains constant between bases.

devices for use in MDI-QKD systems.

4.3.1 On-Chip Laser

To generate WCSs, we will utilise the on-chip laser that was described in chapter 3. The Fabry-Pérot laser demonstrates a narrow linewidth to ensure coherence within a time-bin encoded state. The wavelength tunability of the laser through DBR current injection, temperature and semiconductor optical amplifier (SOA) current injection will allow the wavelengths of separate devices to be precisely overlapped. We will also be able to exploit the short upper state and cavity lifetimes to create phase randomised pulses. This method is described in more detail in section 3.10.

4.3.2 Timing Encoding

The early and late time-bins of the state will be the logical $|0\rangle$ and $|1\rangle$ states, respectively. Therefore, we need to be able to create distinct pulses in either time-bin i.e. there should be a good extinction ratio between the two time-bins. As we are using a continuous wave (CW) laser as our light source, it will need to be intensity modulated to encode time. From the previous section, we saw that the error of the timing encoding will need to be very low to ensure positive key generation at long distances.

As in the previous chapter, time encoding the states will be performed using an Mach-Zehnder interferometer to carve the CW laser into 130 ps pulses. To increase the extinction ratio of the pulses compared to the previous experiment, the RF signal from the driving electronics was amplified to increase the possible voltage swing to 4 V_{pp}.

To encode a state in the diagonal basis, the MZI carves two pulses in quick succession. This requires that the coherence length of the laser is longer than the pulse separation to ensure coherence within a state.

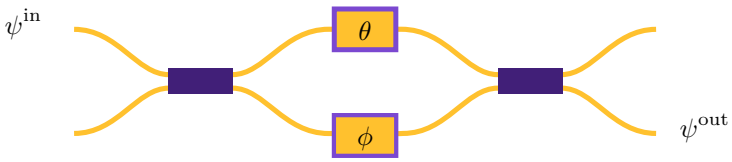


Figure 4.7: Schematic for the MZI which is used to encode a π phase. θ and phi are phases applied by the modulators and $\psi^{\{\text{in,out}\}}$ are the input and output states from the MZI, as shown.

The reduction in intensity for the decoy states could be realised by reducing the voltage of the RF signal driving the *T. Enc* MZI. However, this would reduce the extinction ratio of the pulses in the Z basis and would introduce more errors for the decoy states. Instead, we will introduce another component below to perform intensity modulation below allowing the entire state to be intensity modulated and maintaining a high extinction ratio.

4.3.3 Phase Encoding

Typically, phase encoding would be performed using a fast, phase modulator. However, the losses associated with the quantum-confined stark effect (QCSE) mean that applying a π phase between early and late time-bins would also cause a drastic change in intensity. This could compromise security as the intensities between $|+\rangle$ and $|-\rangle$ states would be different.

Therefore, instead of using a single modulator to encode phases between time-bins, we can use an MZI in a push-pull method. Consider an MZI with θ phase on the top arm and ϕ phase on the bottom where ψ^{in} and ψ^{out} are the input and output states as shown in figure 4.7. The output will then be

$$\psi^{\text{out}} = \frac{1}{\sqrt{2}}\left(e^{i\theta} - e^{i\phi}\right)\psi^{\text{in}} \tag{4.17}$$

We can consider applying two sets of phases to the modulators. Firstly, if we apply ϑ to the top modulator, but no phase to the bottom, the output becomes

$$\psi^{\text{out}} = \frac{1}{\sqrt{2}}\left(e^{i\vartheta} - 1\right)\psi^{\text{in}} \tag{4.18}$$

While, if we were to reverse how the phases were applied, and have no phase on the top modulator and ϑ on the bottom, we would get

$$\psi^{\text{out}} = \frac{1}{\sqrt{2}}\left(1 - e^{i\vartheta}\right)\psi^{\text{in}} \tag{4.19}$$

By taking the ratio of the outputs, we can compare their relative phases. Explicitly, we find

$$\frac{\frac{1}{\sqrt{2}}\left(e^{i\vartheta} - 1\right)}{\frac{1}{\sqrt{2}}\left(1 - e^{i\vartheta}\right)} = e^{i\pi} \tag{4.20}$$

which represents a π phase shift between the two outcomes. Therefore, to apply a phase shift to encode the $|-\rangle$, we should switch between the two cases for the early and late time-bins. This avoids the loss associated with the QCSE effect whilst also reducing the voltage required for phase encoding. The value of ϑ will not affect the phase relationship but will change the intensity of the output state ψ^{out}.

4.3.4 Phase Randomisation

For the security of the protocol, we need to ensure that the states are phase randomised so that the output photon statistics are Poissonian for decoy state estimation. We can use the gain switching demonstrated in chapter 3 to ensure that subsequent states are phase randomised. We of course still require that early and late time-bins within a state are phase coherent.

A negative pulse can be used to gain switch the on-chip laser in between states to randomise the phase. This RF signal allows the cavity and conduction band time to empty meaning that lasing will continue from a spontaneous emission. As the lasing resumes, mode competition and electrical ringing will cause oscillations in the output power. After around 1 ns, these oscillations relax and the laser resumes in a continuous wave operation. We can then encode timing and phase information. As the laser has relaxed into continuous operation, the states will be single moded in frequency allowing phase coherent time-bins and meaning that wavelength filtering is not required beyond the integrated laser cavity. More detail can be found in chapter 3.

4.3.5 Chip-Generated BB84 States

In figure 4.8, we show histograms of the four time-bin encoded BB84 states generated from the InP devices. We demonstrate a 500 ps separation, 130 ps full width at half maximum (FWHM) pulses with an extinction ratio of more than 30 dB. For the diagonal states, the intensity between early and late time-bins remains constant. The intensities are normalised and the intensities of the diagonal states will be determined through the decoy state preparation in the next section. Laser gain switching is applied between each state to ensure phase randomisation. This has the added effect of reducing the total number of counts per second allowing higher photon number per pulse before detector saturation.

4.3.6 Decoy State Preparation

While the absorption of the QCSE is an issue when encoding phase, it can be used to vary the intensity for decoy state preparation. The effect has a bandwidth of $>$10 GHz so a single electro-optic phase modulator (EOPM) can be used. By biasing a modulator in the circuit to 9 V below the chip ground, we can quickly modulate with around 2 V_{pp} to vary the intensity by 15 dB. We are also able to choose whether we pulse the intensity MZI which creates the

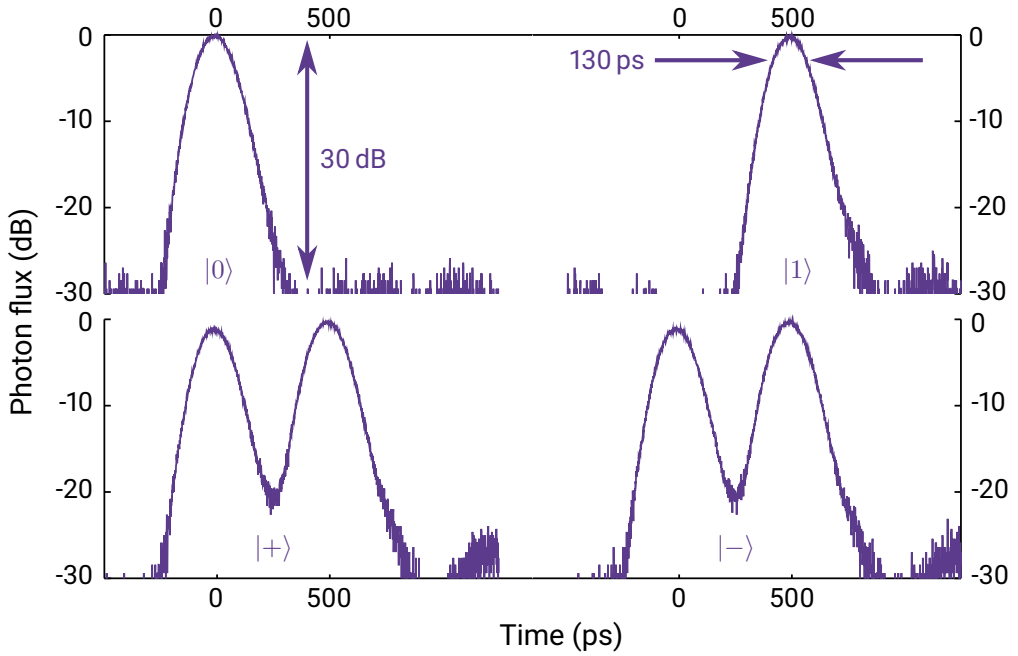


Figure 4.8: Histogram of the phase randomised BB84 states generated from the InP transmitters using cascaded Mach-Zehnder interferometers (MZIs). The timing encoding demonstrates a 30 dB extinction ratio and a 130 ps FWHM. The timing information is not corrected for detector or timing jitter. Intensities of states are normalised as their true intensities will change during the decoy state preparation.

pulses which can be useful for encoding a vacuum state with an intensity of 30 dB below that of signal states.

As the intensities of the decoy states are not fixed by the protocol, we will need to model how these intensities will vary the secret key rate. It has been previously shown that reducing the intensity of decoy states will increase the secret key rate [175]. However, we will still require enough successful events to bound the knowledge of Eve or Mallory.

4.3.7 State Choice

In a QKD system, the states should be chosen randomly. However, for simplicity in this proof-of-principle experiment the states send by Alice and Bob are a fixed pattern chosen to gather statistics of all of the possible combination of states required for key rate estimation. States that play no part in key rate estimation (for example when Alice sends a state in X and Bob in Z) are deliberately removed. In the asymptotic limit, sending these states would not impact the key rate. We will discuss later how these sorts of states would need to be considered in a finite key rate estimation.

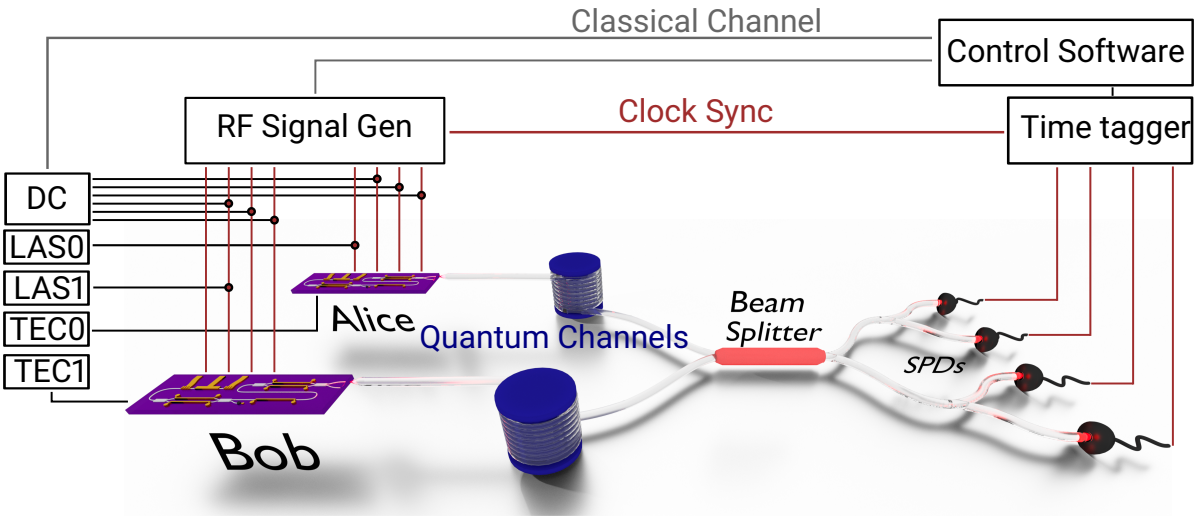


Figure 4.9: The experiment required a number of pieces of equipment to control the transmitters and provide synchronisation signals for the detection. This figure shows the "control plane" of the experiment and how Alice, Bob and Charlie were connected. The experiment used a single computer to control all three parties.

4.4 Control Electronics

In order to operate the transmitters, there is a selection of control devices needed. In this section we will describe them. An overview of the electronic control is shown in figure 4.9 which shows how the transmitters are controlled, as well as the data links to the receiver. A centralised computer controls Alice, Bob and Charlie.

4.4.0.1 Temperature Control

Two Arroyo 6301 are used to stabilise the temperature of each transmitter independently. A 10 kΩ thermistor is put into the base of the transmitter package as close as possible to the transmitter. Thermal paste is used to ensure a good thermal contact to the mount and the silver epoxy used for the chips provides a good thermal contact to the chip. A peltier is used to heat and cool the package through a thermo-electric effect and can be driven with up to 3 A of current. The transmitters dissipate very little heat as most of the operation relies on electro-optic effects. Some heating is caused by thermo-optic modulation ($<$100 mW per thermo-optic phase modulator (TOPM)) and laser driving. The temperatures are chosen to be above the ambient room temperature and also to overlap the wavelengths between the two lasers. Typical temperatures were between 25 °C and 30 °C, required around 100 mA from the Arroyo controller and had an instability of less than 0.01 °C. Good temperature stability of the chips is important as much of the optical circuit is temperature sensitive. A change in temperature will cause the cavity to expand or contract to change the wavelength. It can also cause a change in the operating conditions of the MZIs due to phase differences in the top and bottom arms

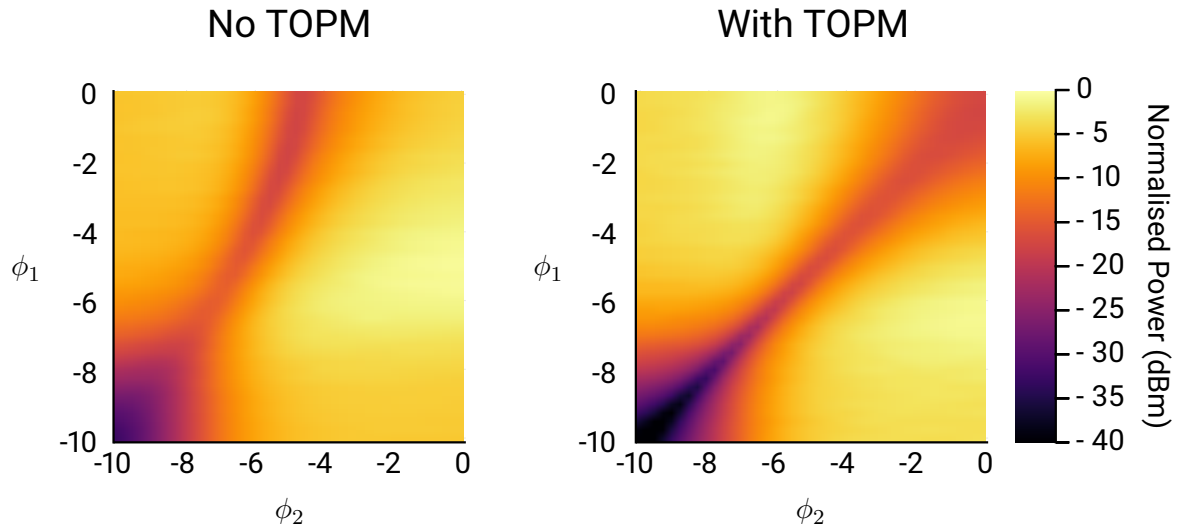


Figure 4.10: By applying a DC bias over each arm of the MZI we can characterise the performance. When no thermo-optic phase compensation is applied, the possible extinction ratio is reduced. The loss between the arms means that the QCSE can't be used to compensate their phase difference. When current is passed over one arm to compensate for the phase mismatch (44 mA), the MZI is symmetric and allows a much larger intensity swing at lower voltages.

or varying splitting ratios in the multi-mode interferometers (MMIs).

4.4.0.2 Laser Driver

The same Arroyo 6301 boxes also provided stable current sources to drive the on-chip lasers. The lasers show a threshold current around 12 mA (figure 3.4) and can be driven with voltages above 100 mA. As well as an increase in power, an increase in current will provide a wavelength shift due to heating in the cavity. With a current precision of 0.01 mA, the wavelength of the laser can be controlled in steps of 80 fm through heating and carrier effects in the SOA. This provides the find control for high-fidelity overlap between independently operated transmitters.

4.4.0.3 Phase Modulator Biasing

For the QCSE, a reverse bias over the modulator was required. DC driving electronics provided the reverse bias while bias tees combined the DC and RF signals for high-speed operation. A range from 0 to −10 V was possible and optimal conditions depended on device and purpose. For example, extinction ratio was found to be best at −9 V for intensity modulation. However, phase encoding would only require −7 V.

Ideally, the light in an MZI would experience the same phase in both arms. However, due to fabrication imperfections and tolerances, the light in each arm accumulates a different phase, meaning that the output is no longer minimised. While this could be corrected using the QCSE,

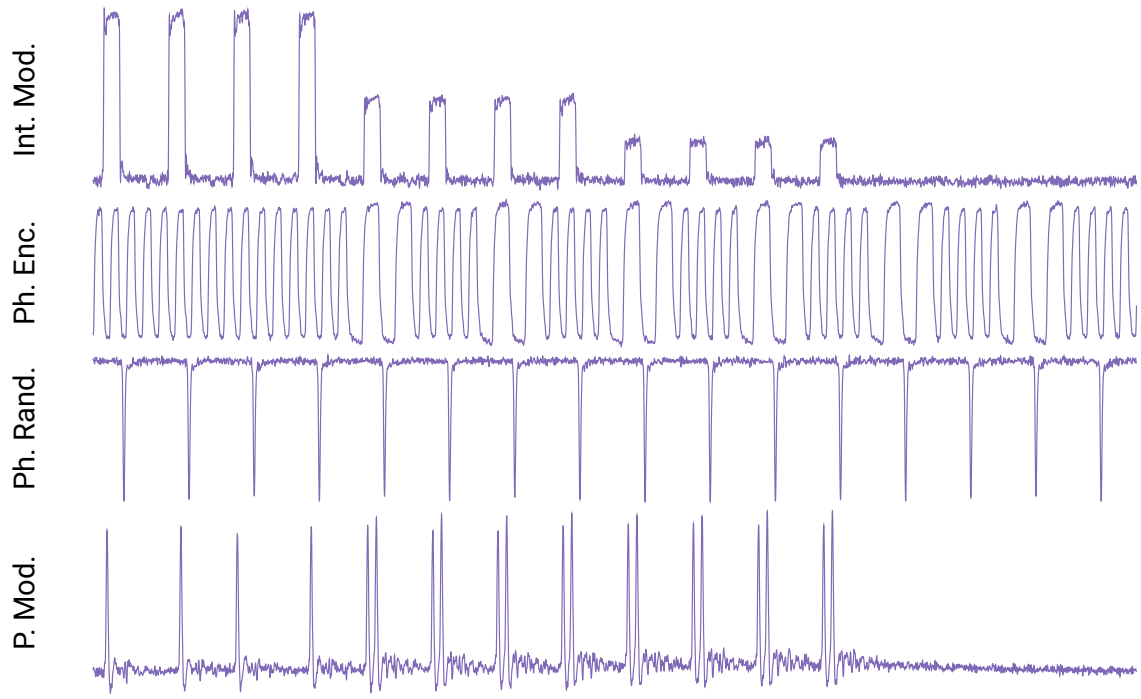


Figure 4.11: Oscilloscope data of the electrical signals required for the BB84 states. P. Mod is used to create the pulses, Ph. Rand for gain switching the laser, Ph. Enc. for phase encoding and Int. Mod for decoy state preparation.

the phase dependent loss mean that the extinction ratio would be reduced as the intensity of light would be different in each arm. Instead, we can exploit an imperfection in the EOPMs which causes a resistance of around 10 Ω. By passing a current through the modulator on one arm of a MZI, we can adjust the relative phase which will minimise the MZI output intensity.

Figure 4.10 shows how heating along one side of the MZI corrects for the different phases. When the MZI is operated without correction, the phase dependent loss associated with the QCSE doesn't allow for the light to be easily minimised. However, after thermo-optic phase modulation is applied, the MZI acts more predictably where equal electro-optic phases mean that output light is always minimised. This optimisation, will also make finding optimal phase conditions to apply a π phase between time-bins easier.

4.4.0.4 RF Electronics

Each transmitter requires four high-speed signals for phase randomisation, timing encoding, intensity modulation and phase encoding. Oscilloscope traces of the electrical pulses used are shown in figure 4.11. Only the intensity modulation, which is used for the decoy state preparation, requires more than a two-level signal. To create the signal and two decoy intensities, we will require four different levels which will need to have a high degree of precision. RF sig-

nals will also be required for synchronisation to the timetagger to consolidator the detection events with the states that were sent.

In order to generate enough synchronised signals, an arbitrary waveform generator (AWG) provided a 250 MHz signal to two pulse pattern generators (PPGs) and an field-programmable gate array (FPGA). Each was then clocked at 2 GHz allowing early and late time-bins to be 500 ps separated. The AWG could then provide the multi-level signal required for the intensity modulation.

The phase randomisation and phase encoding was controlled by the PPGs. The laser cavities and SOAs were drained with 1.5 V, 200 ps pulses and remained around 0 V for the qubit encoding. The pulse for this needs to have minimal noise as this could interfere with the lasing. The relative phases between the time-bins were encoded using square waves where the pattern was designed such that there are equal on and off states. This meant that the average voltage for the RF signal remain around 0 V meaning modulator biasing didn't need changing between sequences. The PPG also provided a 31.25 MHz synchronisation signal to the timetagger through an optical channel.

The FPGA generated the signal for pulse carving which were around 100 ps FWHM. From figure 4.11, the difference between cost-effective solutions and commercial products is evident. The inter-symbol interference (ISI) from the FPGA means that the second pulse for diagonal states has a higher intensity. We also find that the noise after the pulse is increased. The security implications for these imperfections will be discussed later. For this experiment, the ISI could be compensated with the rest of the circuit.

4.5 Receiver

The receiver that Charlie will use for MDI-QKD is a projection onto Bell states. Depending on the encoding, this device used for projection will be slightly different. In a time-bin encoding scheme, a projection onto $|\psi^{\pm}\rangle$ depending on coincidences between time-bins of the detectors which is shown in figure 4.2.

4.5.1 Fibre components

The schematic of the Bell state measurements is simple. However, other fibre optic components were required to ensure good overlap of the states from Alice and Bob. To correct for polarisation drift in the fibre, two polarisation controllers were used to rotate the states. Independent polarising beam splitters (PBSs) for Alice and Bob polarised the light which is then sent into the polarisation maintaining fibre. The PBSs had an extinction ratio of 35 dB. A polarisation-maintaining fibre beam splitter was used to interfere the states.

The polarisation controllers used here were manually operated. However, commercial po-

larisation rotators are available which could be used to actively compensate for drifts in fibre. The unused port of the PBS can be used for active feedback with further single-photon detectors. Alternatively, the polarisation could be converted to a path encoding and compensated for on chip [176].

After interference, standard single mode fibre can be used as only the time of arrival of the photons is important. Further 50:50 beam splitters will be used to separate each arm of the beam splitter to multiple detectors to increase rates.

4.5.2 Detection

SNSPDs are used for detection due to their high efficiency (80 %), low dark counts (100 cps), good timing jitter (30 ps) and short recovery time (100 ns) [106]. Time of arrival is tagged using a Picoquant Hydraharp which is synchronised with the transmitters using a separate optical link.

The detectors are biased so to be close to their critical current to maximise detection efficiency which can exceed 80 % with these particular detectors. However, there is also an optimisation to reduce the number of dark counts. Typically, 80 % efficiency can be achieved with only 100 dark counts per second. The Photonspot systems do not ship with a shunt resistor in parallel with the nanowire which allows the detector to recover when under bright illumination. Without this shunt resistor, the detector can latch where the DC current can cause continual heating in the nanowire which stops it from superconducting. A 50 Ω resistor was added to the system which allows the bias current to pass to ground after the detector has stopped superconducting.

4.5.3 Banked detectors

Despite the record short recovery time that SNSPDs offer, this time can still be destructive for fast clocked systems. In a time-bin encoded scheme, it is difficult to detect a $|\psi^+\rangle$ state as it would require a coincidence of concurrent time-bins of the same detector, as shown in figure 4.2. In a 1 GHz clocked system, the time-bins are separated by only 1 ns meaning the recovery time of the detector would need to be less than this. SNSPDs typically have a detector recovery time on the order of 100 ns meaning that a coincidence between time-bins is impossible. While superconducting detectors exist with sub-nanosecond dead time, they will typically sacrifice efficiency by reducing the length of the nanowire or wavelength tunability by creating a photonic cavity [112, 113].

In order to increase the possible rates of a time-bin encoded MDI-QKD system, we can introduce a pseudo-photon-number resolving bank of detectors. Each detection arm of the measurement beam splitter is further split to many detectors. This allows $|\psi^+\rangle$ to be detected with some probability depending on the number of detectors available. This kind of banked

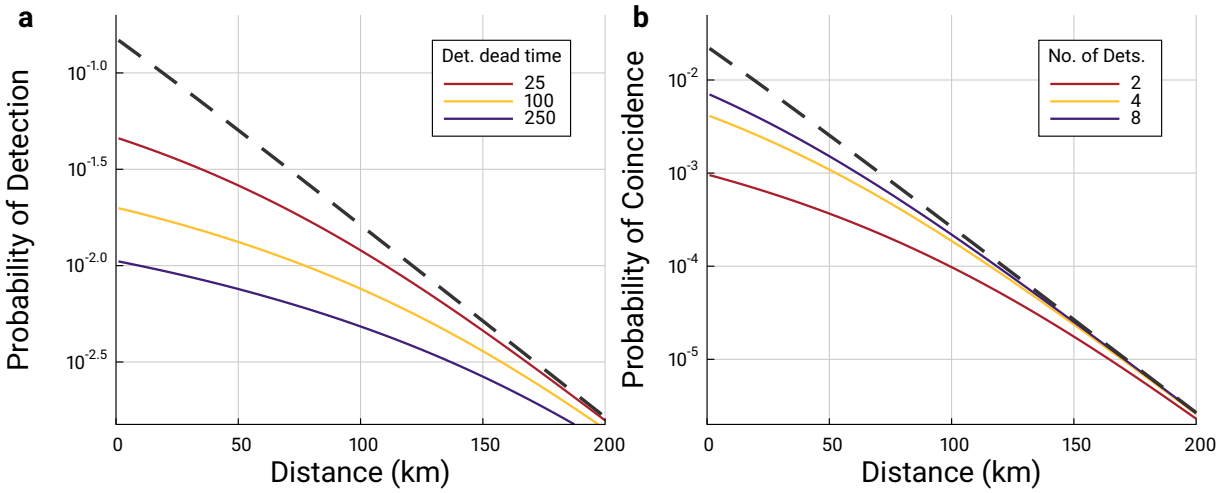


Figure 4.12: a We plot the effect of the probability of detection, given a detector dead time (in number of cycles) against distance. **b** The probability of coincidence is plotted against time with varied number of detectors in a receiver bank. A photon number of 0.2 is assumed in both cases and the dashed line is a detector with zero dead time.

detection system also means that we can increase the number of events before saturation of the detectors.

To characterise the benefits of a banked detector system, we should consider the effect of deadtime on a SPD. First, we consider the probability of a click, ξ, in an SPD given a coherent state with average photon number, μ, some detection efficiency, η, and dead time of the system, k. Consider that that the system is unable to detect a photon for some time after a successful event and that the probability of detection is the same for each clock cycle. The efficiency is then modelled as

$$\xi = (1 - \exp(10^{-\frac{0.2 \cdot L}{2 \cdot 10}} \cdot \eta \cdot \mu)) \cdot (1 - \xi)^k \tag{4.21}$$

where k is the number of cycles that the detector is dead i.e. system clock rate multiplied by detector deadtime. For example, given a 250 MHz clock rate and a dead time of 100 ns, we would have $k = 25$. The loss from Alice and Bob to Charlie is estimated in the usual way with 0.2 dB/km and L is the distance between Alice and Bob. For large dead times, this model has no analytical solution. However, we can numerically estimate what we would expect the efficiency to be.

First, we consider the effect of dead time against the probability of a detection event as shown in figure 4.12a. We find that at short distances, the number of dead cycles has a drastic impact on the probability of detection as the detector is required to recover. If we were to consider a 1 GHz system and detectors with 100 ns recovery time, the probability of a successful event is reduced by about ten times when compared to a system with no dead time at 0 km. As the distance increases, the probability of detection when considering deadtime will converge

on the ideal case as the photon number will reduce with loss.

In an MDI-QKD system, we will be concerned with detection coincidences to determine successful Bell state projections. We can use the same model above, but square the probability of a single event assuming that both detectors have the same dead time and efficiency. We will only look for events where exactly two detectors click, one from either side of the beam splitter. Therefore, for a bank of m detectors, we can model the probability of coincidence as

$$P(\text{coindience}) = \left(\frac{m}{2}\right)^2 \cdot \xi^2 \cdot (1-\xi)^{m-2} \tag{4.22}$$

where ξ is the efficiency of a single click from equation (4.21), taking into account that the average photon number at each detector will be reduced as the number of detectors is increased.

By changing the number of detectors in the bank, we can see how this will affect the coincidence probability as a function of distance. This is shown in figure 4.12b. For short distances, introducing a bank detection system can increase the probability of detection when compared to two detectors. This advantage will decrease at further distances as the photon number reduces with loss.

There are two things that this model doesn't consider. First, is the loss of the optical network required to separate the states to the bank of detectors. Commercial fibre components are well engineered and would introduce minimal losses for the simple task of separating the light. Second is the increase probability of detecting $|\psi^+\rangle$. As the number of detectors in a bank increases, the prefactor of 3/8 can be made arbitrarily close to the theoretical limit of 1/2.

4.5.4 Time Tagging

In order to correlate the detection events, time tagging is required to reconstruct the sequence of events. This experiment used a PicoQuant Hydraharp to time-tag the four detector events relative to a synchronisation signal sent from the transmitter control electronics. This can then be used to determine the time of arrival and correlate each detection event to others and to the states sent.

For short distances between Alice, Bob and Charlie (low loss links), the number of detection events can exceed ten million counts per second (0.1 photons per pulse at 100 MHz). It can be challenging to extract all events from the time tagger whilst simultaneously correlating events. To avoid buffer overflow in the timetagger, the timing events were saved directly to a computer so that the data could be analysed offline. In a commercial system, an FPGA or application-specific integrated circuit (ASIC) could be developed to directly correlate events to replace the timetagger and reduce the computational intensity of data analysis.

It is important that the absolute time delay is known so that the states can be faithfully reconstructed relative to the states sent. For this experiment, the delay between transmitter

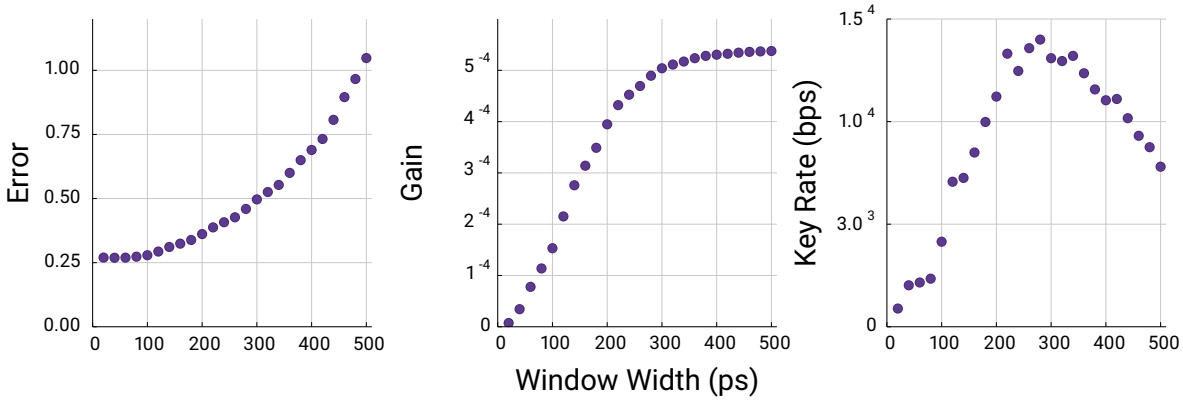


Figure 4.13: By changing the window that we accept a successful measurement, the error rate, gain and secret key rate will be affected. The Z basis error rate increases exponentially while the gain will plateau. From this, we can find an optimal point of around 240 ps window width.

channels is minimal by design. However, in a real-world key exchange this would need to be more thoroughly characterised.

As the detection events are first-in first out, we only need to check for coincidences when we know that the event was in the late time-bin of the qubit. This is because both $|\psi^{\pm}\rangle$ have a click in both the early and late time-bins. This will reduce the number of unnecessary calculations we can increase the rate at which the data can be analysed.

4.5.5 Synchronisation

To be able to reconstruct the measurements and match them with the transmitters, a synchronisation signal was provided to the timetagger. The timetagger was then able to provide exact timing of events for later analysis. An RF signal from one of the PPGs was sent to an SFP to SMA breakout board (Hi-tech Global SMA-SFP) which converted the electrical signal to optical. A fibre was used to send the signal to the receiver system and another breakout used to provide the electrical signal to the timetagger.

4.5.6 Qubit Gating

From time of arrival relative to the sync signal, the detection events are collected into predetermined windows which correspond to the early and late time-bins of the qubits. The window width was varied as there will be a trade-off between the detection probability and the error rate. As shown in figure 4.3, there is a limit to the error rate that the decoy protocol can tolerate to generate a positive key rate.

Figure 4.13 shows the effect of changing the gating windows within which events are accepted. By increasing the window size, the Z basis error will increase as the extinction ratio in the state generation will be reduced. Similarly, the gain will also increase and both will de-

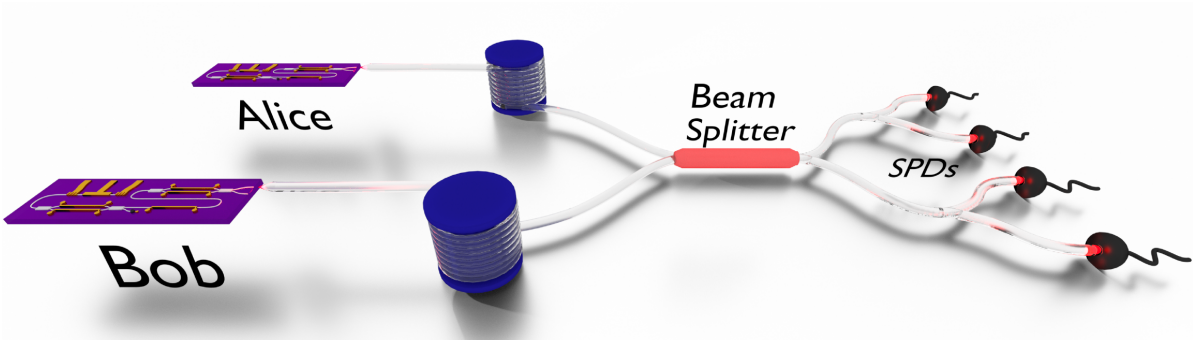


Figure 4.14: Schematic of the integrated MDI-QKD experiment. Alice and Bob each operate an integrated transmitter and send BB84 states over quantum channels to Charlie. The states are projected in the Bell basis using a banked detection system.

termine the secret key rate. By looking at the key rate generation, we can find a compromise of window size to maximise performance. After the gain plateaus, the key rate decreases as it will be determined by the exponentially rising error.

For this experiment, a gating window of 240 ps was chosen to maximise gain whilst also minimising the error at longer distances. From figure 4.3, we found that at longer distances a lower Z basis error is required.

4.6 Results

Here, we will discuss the results of the key generation between the two integrated transmitters. A schematic of the experiment is shown in figure 4.14. Two InP transmitters independently generate weak coherent BB84 states. These are sent over quantum channels to the receiver, Charlie. In this experiment, the states are projected in the Bell basis using a fibre beam splitter where banked detectors are used to determine successful events which can be publicly announced.

4.6.1 Calibration and Optimisation

As mentioned before, the MDI-QKD protocol is very dependent on high fidelity HOM interference. Therefore, we must make sure that the two different transmitters have a good overlap in all degrees of freedom. In this section we will discuss methods used to create indistinguishable pulses.

The states from each transmitter are polarised using a PBS and timing can be controlled using picosecond delays in the RF driving electronics. Photon number is calibrated from the detectors, where fibre loss and detection efficiency had been previously calibrated.

Phase encoding was the most challenging to calibrate as this would require an independently calibrated reference. For example, we could use an aMZI and compare the output be-

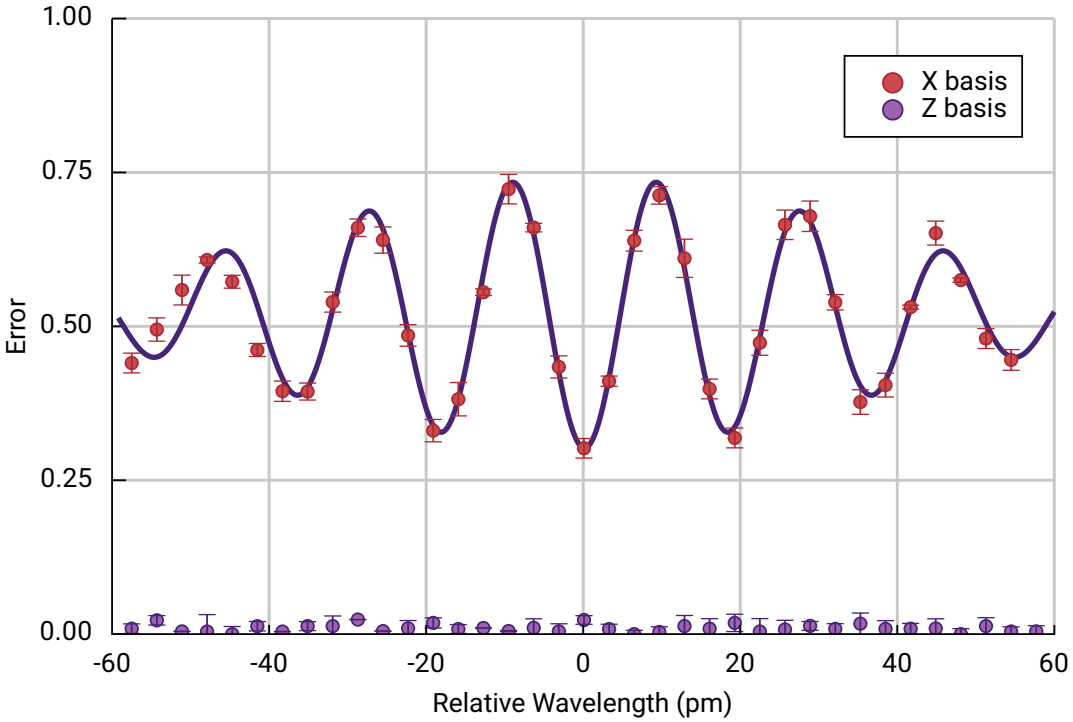


Figure 4.15: To overlap the two transmitters in wavelength, we can prepare BB84 states and tune the relative wavelength of the lasers. The change in wavelength will cause HOM interference. However, this will also cause changes in the relative phases between early and late time-bins. This causes a sinusoidal fringe as the lasers become indistinguishable.

tween $|+\rangle$ and $|-\rangle$ input states. However, this added complexity to the receiver would either require optical switching or increased losses.

Alternatively, we can create $|\pm\rangle$ states with one transmitter, and tune the other transmitter to minimise the error rate. Through the MZI phase encoding, we can create an approximate π phase just by looking at the intensities of the early and late pulses. When the intensities are the same, we should expect a good phase encoding, as shown in section 4.3.3 for MZI phase encoding. This will depend on the time encoding states being the same for the early and late time-bins. However, ISI can cause the electrical driving voltages to change depending on the bit string meaning that the intensities can vary. This is shown in figure 4.11 where the P. Mod. pulses change intensity throughout the sequence. This can also introduce side-channels and will be discussed later.

In figure 4.15, we show the error dependence on wavelength for both the X and Z bases. Alice and Bob send a known set of BB84 states to Charlie which allows an error rate to be calculated. We will assume that Alice's wavelength will remain fixed and will stand as the target state preparation for Bob. As Bob tunes the wavelength of his states, the relative phases between early and late time-bins will also change. This will mean that his $|+\rangle$ and $|-\rangle$ states will tune in and out of phase relative to Alice's fixed states. This fringe will have the Gaussian shape from

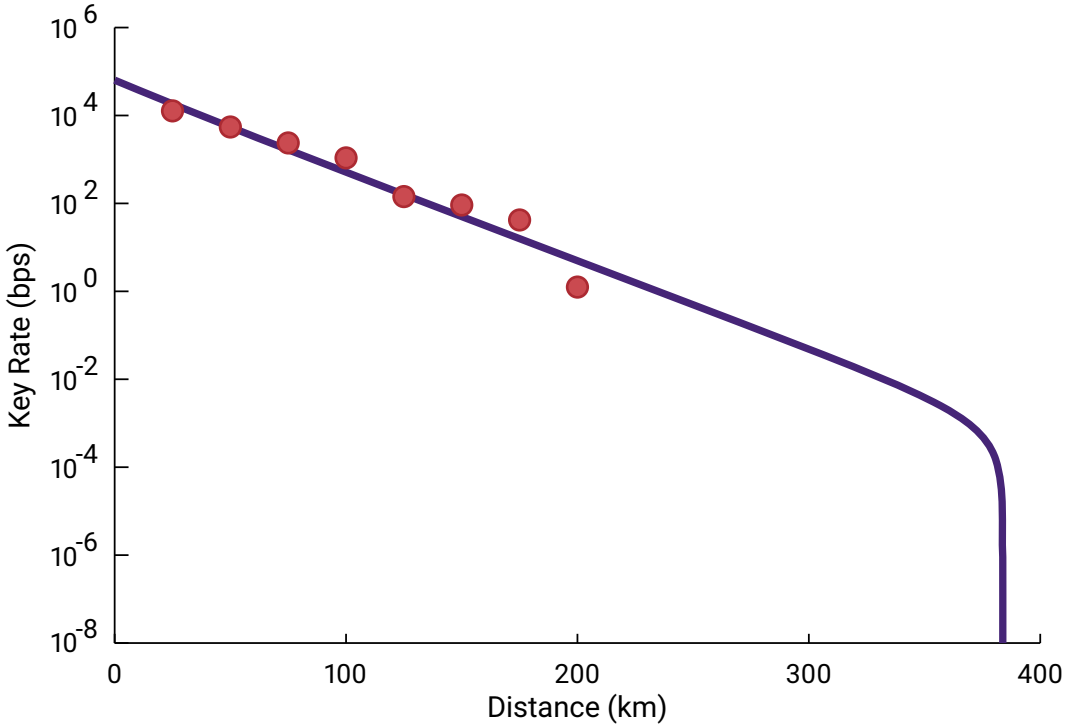


Figure 4.16: We demonstrate positive key rates up to 200 km over an emulated fibre link. At metropolitan distances (25 km), we show a key rate of 12.7 kbps is achievable while at 100 km, more than 1 kbps can be exchanged. Using the errors and gains from the system, we model that positive key generation is possible at more than 350 km.

the HOM interference, as previously derived. However, the error will oscillate sinusoidally with the varying phases as the change in wavelength causes different phase dependency between early and late time-bins. Therefore, the fringe will look like

$$E^X = \frac{1}{2} - \frac{1}{4} \cdot \exp\left(-\frac{t_p^2 \cdot (\Delta\omega)^2}{16 \cdot \ln(2)}\right) \cdot \cos(\beta \cdot \Delta\omega) \tag{4.23}$$

where β will depend on the separation of the time-bins. This fringe allows a precise overlap of wavelength through the HOM interference whilst verifying good state preparation in the diagonal basis. A fit is also shown in figure 4.15 which shows good agreement with the data.

The Z basis measurements are not dependent on HOM interference as successful events should only occur between non-interfering states ($|0\rangle$ and $|1\rangle$). This is only dependent on the intensity modulation of the weak coherent pulses (WCPs). So the error remains constant through the sweep with an average of less than 1 %.

4.6.2 Key Rate

MDI-QKD was demonstrated between two independent InP devices. Secret key rates were estimated over an emulated fibre link (using variable optical attenuators assuming 0.2 dB/km) and are shown in figure 4.16. At metropolitan distances (25 km), key rates of more than 12 kbps are estimated in the asymptotic limit with positive key rates demonstrated up to 200 km. Beyond this distance, the integration time required for a reasonable number detection events increases exponentially. For example, at 300 km we would need to integrate for six days. However, by characterising the experimental performance, we predict that a quantum-secured key exchange is possible at distances of more than 350 km.

We show that interference between independent transmitters is possible for 500 ps separated (2 GHz clocked) time-bin encoded states with state of the art quantum bit error rates. We find an error of 30 % in the X basis, which is limited to a theoretical minimum of 25 %, demonstrating a good indistinguishability in all degrees of freedom. In the Z basis, we achieve a quantum-bit error rate of 0.5 %.

The mean photon number was 0.2 in the Z basis for the signal states. In the X basis the mean photon numbers were 0.1 and 0.01 for decoy state analysis. The vacuum state intensities are measured as 5×10^{-4}. Low photon numbers were used to limit the saturation of the detectors at low channel losses and allow positive key generation at further distances. The transmitter electronics is clocked at 2 GHz with a state being sent every 8 clock cycles giving a 250 MHz qubit rate. The bases were biased to produce an equal number of Z and X states, and therefore each of the X decoy states were sent one third as often as a Z signal state. The error rates and gains used to calculate the key rate can be found in appendix A.

4.7 Outlook

In this proof-of-principle demonstration, we have extended the functionality of integrated transmitters for measurement-device-independent QKD making it a promising platform for a metropolitan scale quantum-secured network. Building on the Hong-Ou-Mandel interference shown in chapter 3, we are able to show good interference between independent transmitters whilst also encoding BB84, time-bin encoded states. The devices show state-of-the-art error rates allowing predicted positive key rates at distances beyond 350 km.

Integrated photonics offers benefits for future networks with reduced power, weight and size requirements while simultaneously facilitating increased complexity with inherent phase stability. Indium phosphide devices are shown as a feasible platform for QKD networks, allowing relatively cost-effective devices to be easily mass manufactured. Integrated laser sources and efficient phase modulation satisfy all the requirements of high-fidelity quantum state preparation in a single monolithically fabricated platform.

The topology of MDI-QKD means that citywide resource sharing can be achieved through commercially available optical switches at an untrusted centralised location. Furthermore, banks of detectors can be used to increase secret key rates. Advances in cryogenic cooling mean superconducting detectors are becoming more readily available and will likely be a vital part of future quantum-compatible networks. Such nodes will form the basis for more complex communication protocols that will require quantum repeaters and photonic information processing [144].

It is becoming increasingly vital that the future of secure communication is addressed to counter advances in classical and quantum computing. While quantum key distribution has been demonstrated as a potential candidate in future networks it has yet to be widely adopted. Concerns of side-channel attacks on physical implementations undermines the security promises of QKD systems. Here, we have improved on previous demonstrations of integrated QKD systems by removing all detection side-channels which vastly increases confidence in the security of the system. Mass-manufacturability and robust operation mean that integrated systems are poised to create an accessible platform for widespread quantum-secured communication.

4.7.1 Full System Demonstration

This experiment focused on the technology and, thus, it is a proof-of-principle experiment that dealt with the demonstration of the chips. There are many aspects of a full protocol that will still need to be added before a key can be exchanged. Not least of which is the distribution of Alice, Bob and Charlie to separate locations. Such a separation will require extensive feedback and synchronisation between Alice, Bob and Charlie to minimise error rates. The MDI-QKD protocol as presented previously would need to be expanded to allow for initialisation between Alice and Bob.

When estimating the key rate from the experiment, we assumed that we could accurately estimate the asymptotic limit. To ensure that the single-photon events are accurate Alice and Bob would need to have an infinite number of events. In a realistic key exchange, it is necessary that the number of events will be finite. Therefore, the bounds must be modified to consider statistical fluctuations in the data set. A method of calculating these statistical variations for MDI-QKD is given in ref. [164].

Interestingly, when one considers finite-key effects the optimisation of intensities for decoy states becomes practically challenging. This is, in part, due to a trade-off of security against size of data set. By increasing the photon number, Alice and Bob can generate a larger data set more quickly. However, this also gives Eve more opportunity to exploit multi-photon terms. Such effects have been studied and fast algorithms developed for optimisation [169].

To demonstrate the key exchange, we chose a pre-determined set of states that Alice and

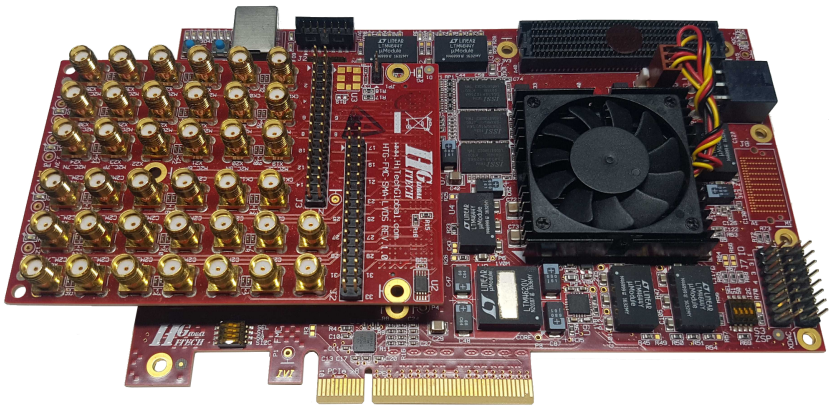


Figure 4.17: Picture of the specialised FPGA controller (HTG-K800 Xilinx Kintex UltraScale 060 FPGA in A1517 package) for integrated QKD. The driver can provide RF and DC signals for high-speed operation as well as stabilisation and laser driving. The board measures only 20 cm in length which is much more compact that general rack mounted equipment.

Bob would send to Charlie so as to estimate the errors and gains efficiently. However, the security of QKD requires that the states being sent are independently and randomly chosen. Quantum random number generator (QRNG) devices have been demonstrated to produce randomness at Gb/s [120,177,178] which also utilise the InP platform. One could imagine a QRNG and the transmitters in a single design so that all of the optical components could be on a single photonic integrated circuit (PIC).

One might argue that demonstrating the transmitters without state randomisation would be invalid as the destructive effects such as ISI could have a detrimental effect on the system. However, such effects will be present in the driving electronics but should not be inherent in a modulator provided that the termination and bandwidth are sufficient. InP devices have previously been demonstrated for QKD with QRNG derived randomness which demonstrates that ISI effects are not inherent in the devices [9]. The effect of ISI within the driving electronics will be discussed further in the next section.

4.7.2 Miniaturised Electronics

To truly utilise integrated photonics, dedicated and specialised electronics will need to be developed which would reduce the power, weight and cost of a system. Here we will discuss one such attempt to provide specialised driving electronics and consider how choices of driving electronics will need to be informed by security analysis.

4.7.2.1 Purpose-built FPGA

The integrated transmitters only require a limited number of signals to operate, as shown in figure 4.11. Therefore, the generalised AWG are overkill and lots of functionality is not utilised.

By considering what the requirements are, the driving electronics can be reduced to a single FPGA which is shown in figure 4.17. The board can provide RF signals for high-speed operation. It also has the capability to provide DC signals for thermo-optic phase modulation and laser driving. Together with a PID controller for temperature stability, an entire QKD transmitter could be drastically reduced in size. Benefits of specialised driving electronics could also reduce the driving voltages for modulation as the chip could be closer to the driver. This would reduce the losses associated with PCB waveguides and connections, especially for the high bandwidth requirements of communication devices.

However, while the stringent requirements for state generation means that one needs to be careful with the design of RF electronics for QKD systems. Detrimental effects with RF electronics can introduce side-channels that can be exploited by Eve or Mallory. By reducing the cost of the control electronics can also potentially open up the system to attacks due to inaccuracies in control.

4.7.3 Security Trade-off

While MDI-QKD removes all possible attacks on the detectors, there is still the possibility of Mallory gaining information by targeting the transmitters. Therefore, the security of the transmitters will still need to be characterised to ensure the security of a key exchange. Many attacks have been demonstrated on different QKD system [179]. However, to date there have been none demonstrated against integrated devices. Without the technology to relieve all attacks with DI-QKD, we must attempt to characterise the transmitters to mitigate potential attacks or side-channels.

In collaboration with The National Physical Laboratories (NPL), we have performed preliminary characterisation of the integrated devices and their performances. In particular, the collaboration looked at how cost-effective driving electronics can introduce side-channels through ISI. This work discusses the necessary trade-off between the cost a system and its security. The work has been published in reference [156].

ISI is an interference effect where symbols used for communication are distorted by those sent before. In classical communication, this causes an increase in errors making the channel less reliable. Such effects can also affect QKD systems.

The quantum states are encoded in WCPs with relative phases between them. Early and late time-bins are used to create a binary basis and can be used in MDI-QKD, BB84, coherent-one-way (COW) and differential-phase-shift (DPS) protocols. The intensity preparation of the states is shown in figure 4.18. The WCPs have, on average, intensities that are less than one photon. The exactly intensity will depend on the protocol, distance and error rate. However, it is vital that the intensity of the states is well calibrated to faithfully estimate the number of single-photons events. A system's ability to maintain precise levels will be paramount for

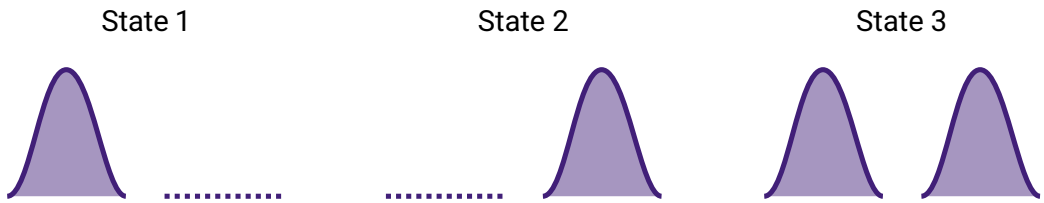


Figure 4.18: States sent to characterise the performance of the chip and FPGA and check for ISI. The early and late time-bins are as before. We are only testing the timing encoding and the early and late time-bins are as before.

its security. By sending and measuring all nine combinations of states we can see where ISI might impact performance and security of a system.

Recent progress with single-photon measurement devices mean that NPL are able to characterise the system at the single-photon level so as to more accurately test a functioning QKD system. A gated single-photon avalanche diode (SPAD) (IDQuantique 210, 300 ps FWHM) was synchronised to the transmitter FPGA with a tunable delay. The efficiency was 0.02 % for this short gate time. By scanning with the tunable delay, the detector could measure a sequence of pulses. However, as the gate has some finite width, the detector profile needed to be deconvolved to recover the true measured signal from the transmitter. The transmitter was operated at 1.031 GHz.

In figure 4.19, we can see measured histograms of state sequences generated from an InP transmitter operated with a specialised FPGA board. By sending all combinations of possible states we can see evidence of ISI having an effect. When a pulse is succeeded by an empty time-bin a “shoulder” appears that is about 2 dB above the noise floor. Furthermore, The background power and maximum intensity of pulses seems heavily dependent on what state has preceded it. It is not possible to deconvolve the ISI from chip packaging or electronic interference. Further investigation would be required as to whether the chip or PCB electrical design is required to change to reduce electrical reflections or if the FPGA requires attention.

While ISI is a well known effect in classical communication, it may have more serious impacts in quantum communication where the security may be compromised. This initial characterisation demonstrates that measurements of QKD systems at the single-photon level are possible. This work helped inform standardisation by the Industry Specification Group on QKD of the European Telecommunication Standards Institute (ETSI-ISG-QKD) [180].

4.8 Fully Integrated QKD

The simplicity of the receiver in MDI-QKD lends itself towards an integrated platform [181]. Waveguide integrated single-photon detectors [111], on-chip wavelength demultiplexing [174]

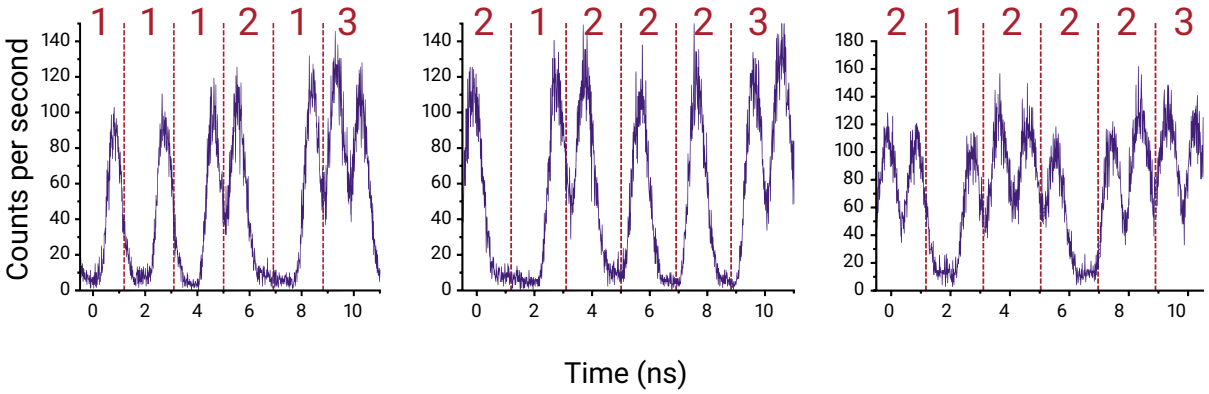


Figure 4.19: Histogram of states sent by an integrated device using specialised electronics. By sending different sequences of states we can analyse ISI which might compromise security through side-channels. Figure has been reproduced from [156].

and cryogenic optical switching [173] mean that a completely integrated receiver device could further decrease the cost of QKD systems. Fully integrated measurement devices facilitate a drastic increase in the number of detectors to allow a higher count rate before saturation and relax the need for sub-nanosecond deadtimes. Key rates could be further increased through wavelength division multiplexing which can also allow coexistence with classical signals [153].

Integrated transmitters will facilitate the wide adoption of QKD transmitters where a centralised resource can be shared between many users. In this section, we will discuss the first steps towards a fully optically integrated QKD system where InP and silicon-on-insulator (SOI) can be complementary in a single system.

4.8.1 Receiver Device

With integrated transmitters demonstrated, is seems reasonable to consider how a receiver for MDI-QKD could utilise integrated photonics. The SOI photonic platform has been well developed in the last decade meaning that such a circuit can be created with minimal losses [8]. Such advances will likely play a crucial role in widespread quantum communication deployment.

As we have seen, projecting time-bin encoded states in the Bell basis requires a very simple optical circuit. The interference of the states requires a 50:50 beam splitter where SPDs record the time of arrival. Coincidences between time-bins indicate successful projections. In comparison, this measurement device is much simpler than protocols such as BB84, COW or DPS which would require delay lines and stable phase shifters. It is possible to make a PIC to decode these signals [9] without the SPD. However, waveguide integrated of detectors likely requires cryogenic temperatures which limits the use of typical phase shifters due to carrier freeze out.

Here, we will discuss how each part of an MDI-QKD receiver can be replaced with an integ-

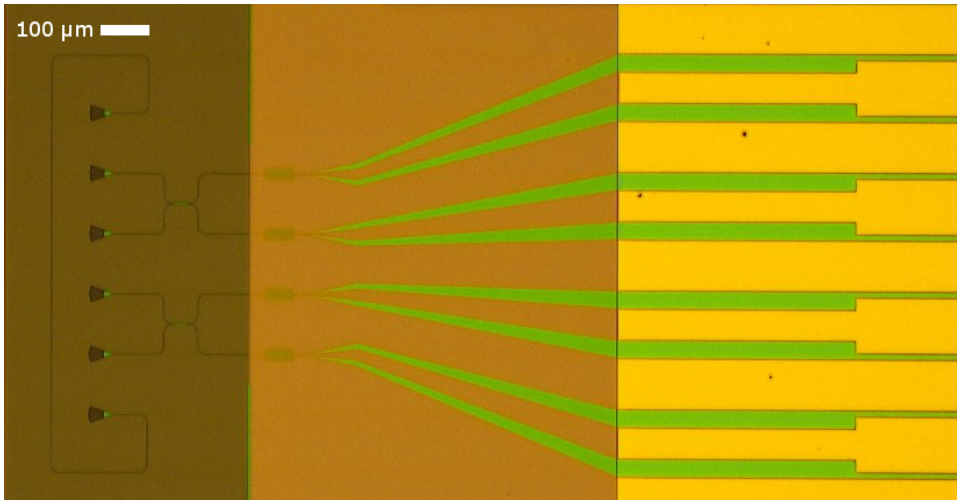


Figure 4.20: Microscope image of the MDI-QKD receiver silicon chip. Grating couplers are used to couple pulses into the waveguides which are then interfered in an MMI before detected by waveguide integrated detectors. The device includes two copies of a receiver, demonstrating the scalability of the platform. There is also a cut back waveguide to ensure maximal coupling onto the device. This image was provided by R. Heath of devices fabricated by J. Paul and designed by D. Sahin and J. Barreto.

rated component in SOI PIC. A microscope image of the first test receiver is shown in figure 4.20.

Grating Couplers

By exploiting the high index contrast of SOI, grating couplers can be used to efficiently convert a fibre optic mode into a waveguide mode. Coupling losses tend to be higher than when using edge couplers. However, designs have been reported with losses as low as 0.36 dB [121]. The grating period determines the peak wavelength which can be quite narrow. The gratings were designed for 1550 nm for compatibility with the transmitters.

To ensure maximal coupling, two grating couplers at the top and bottom were connected to a waveguide allowing cut back measurements and feedback for blind alignment.

Multi-Mode Interferometer

The states can be interfered on an MMI where the splitting ratio of the component is design for a particular wavelength. The exact ratio is a function of the wavelength and size of the component. If the input wavelength changes, so will the splitting ratio. Due to fabrication tolerances, the researchers at Glasgow were unsure whether the splitting ratio of 50:50 could be easily achieved. This uncertainty is what motivated figure 3.1 where visibility was calculated as the splitting ratio changed. We could see that high visibility could be maintained even if the splitting ratio was off by a few percent.

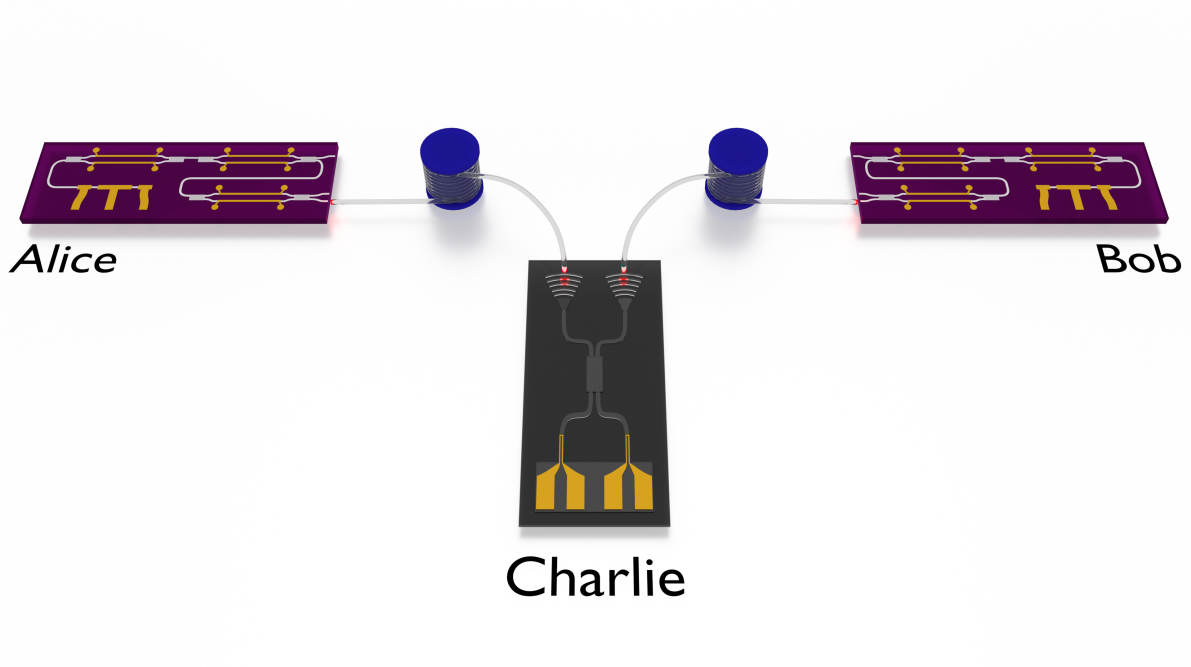


Figure 4.21: Experimental schematic for fully integrated quantum key distribution. Alice and Bob use independent InP devices which generate BB84 states on-chip. The receiver (Charlie) is an SOI device with grating couplers and waveguide-integrated detectors.

Waveguide Integrated Detectors

A niobium-titanium-nitride (NbTiN) thin film on SOI was used to make the device which allowed the waveguide integrated SNSPDs to be etched directly on the substrate. The optical circuit could then be created around the SNSPDs. The confinement in the waveguide should mean that there is a strong coupling to the nanowire meaning a high efficiency. To increase coupling, the nanowire is made in a meander on top of the waveguide which should increase the interaction between the nanowire and photons.

4.8.2 Experimental Setup

Combining the InP transmitters and the SOI receiver would allow a QKD system where all of the optical components are on integrated devices. The states can be generated with the InP PICs while the states can be interfered and measured on a simple SOI circuit. Figure 4.21 shows the schematic of the experimental demonstration.

From the model that was developed in section 4.2.4, we can estimate what we would expect the performance of the system to be. We saw previously that HOM interference is not severely impacted by a splitting ratio that is a few percent either side of 50:50. Therefore, we can assume that the error rate would be equivalent to what was found with the fibre-optic receiver. However, the losses within the chip will potentially be high which would reduce the

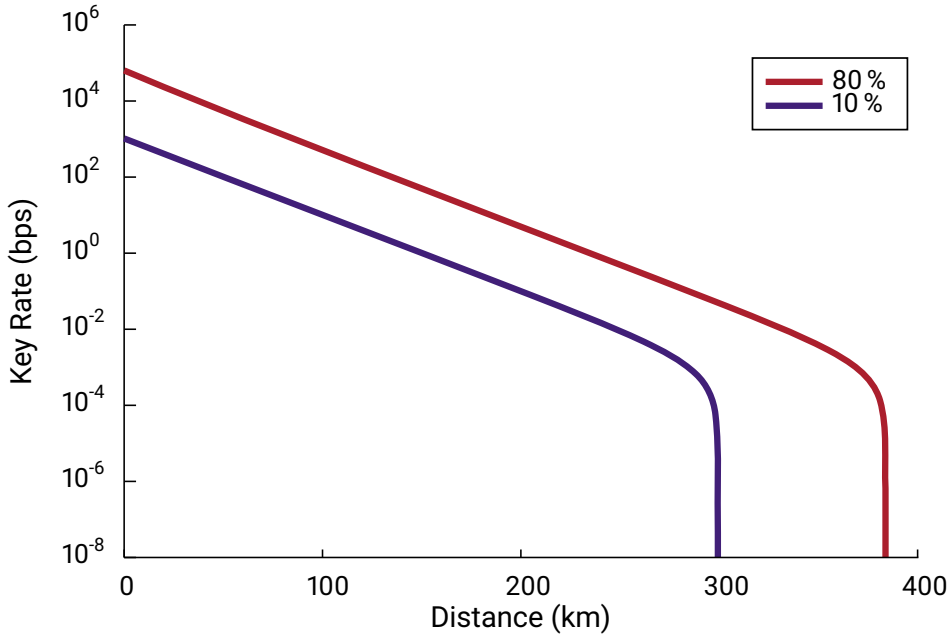
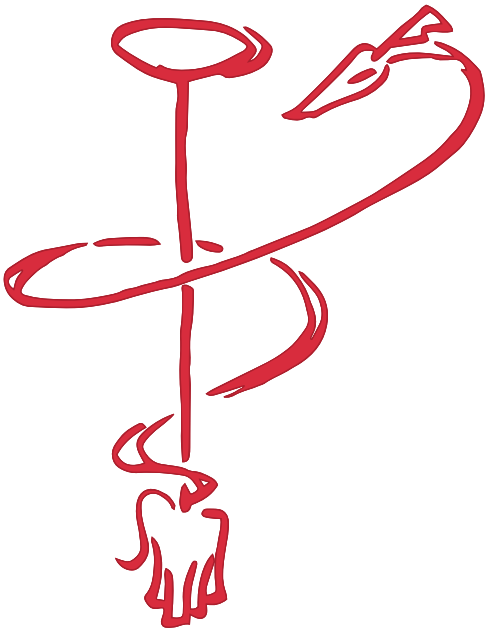


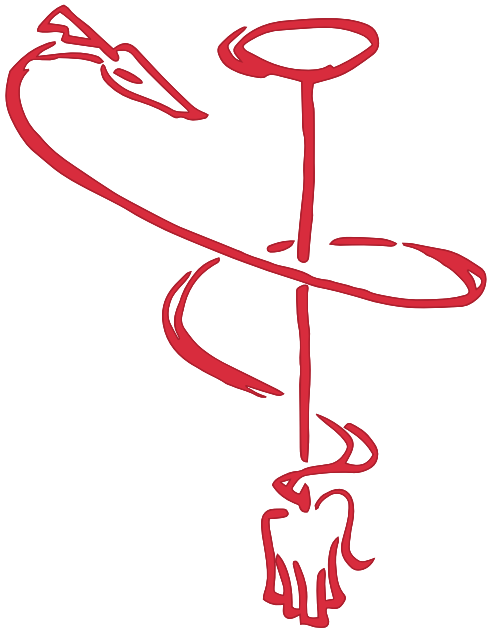
Figure 4.22: The estimated efficiency of the integrated detectors is low which is due to chip coupling and waveguide losses. Here, we compare how this will effect the key rate against the fibre system, given the same number of dark counts. The key rates possible are about 1 % and positive generation only possible to 300 km.

expected gain. While grating couplers can be designed with low loss, it is quite likely that the first devices will exhibit higher loss. The efficiency of the waveguide detectors is also unknown. We will assume that the efficiency will be around 10 % to be pessimistic and that the detectors will have the same dark count rate.

Figure 4.22 compares the previous demonstration with the revised efficiency. The reduced efficiency gives a key rate approximately 20 dB below the previous experiment until around 300 km. After this point, the dark count rate of the detectors becomes dominant and so positive key generation is no longer possible.

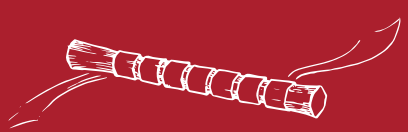
Unfortunately, due to fabrication difficulties, the experiment as described was never able to come to fruition. Challenges when etching the NbTiN to create the SNSPDs meant that the chip was over etched which reduced the thickness of the silicon. This changed the peak coupling wavelength for the grating couplers by around 100 nm. This wavelength is not compatible with the InP transmitters and would also have serious implications for rest of the circuit. New devices have been fabricated to compensate for this over-etch and can now be characterised before being used in future MDI-QKD experiments.

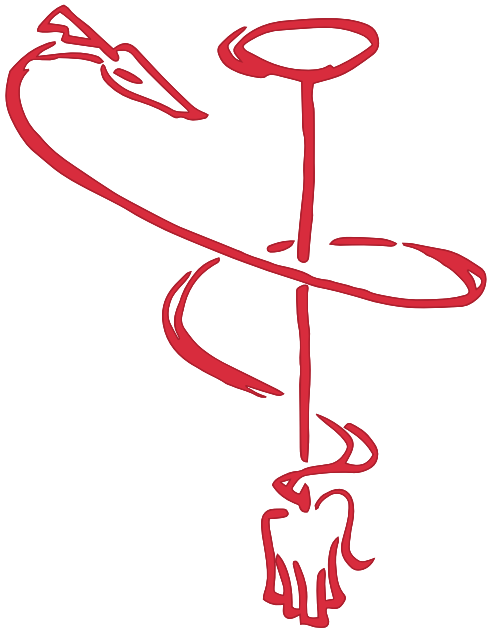




5

Next Generation Integrated Transmitters





Statement of Work

Philip Sibson and I designed the photonic chips and compiled the chip mask that was fabricated by Fraunhofer Heinrich Hertz Institute. I designed the PCB for electrical operation and optical connection. I packaged the chip with support from Alasdair Price and Graham Marshall. I performed characterisation of the initial components of the circuits which included laser driving under both DC and RF operation and a preliminary test of laser seeding capability.

5.1 Introduction

Recent developments in monolithic fabrication have facilitated a drastic increase in the optical complexity which has been thoroughly utilised for quantum information experiments [8]. The inherent phase stability allows a level of control on a scale simply not possible with fibre or bulk alternatives. However, the technology is still under heavy development to improve the performances of devices at both component and circuit levels. As such, further optimisation is required to fully benefit from the integration of quantum key distribution (QKD) systems.

While the demonstrations in previous chapters showed state-of-the-art performances from indium phosphide (InP) devices, several non-idealities were noted which are in need of improvement. The phase imperfections in the Mach-Zehnder interferometers (MZIs) meant that a resistance over the electro-optic phase modulators (EOPMs) needed to be used to maximise the performance of the device. By including dedicated thermo-optic phase modulators (TOPMs), the performance may be further increased and allow a true “push-pull” method of modulation to be used. Similarly, the dimensions of the laser components could be optimised to increase laser performance. Tuning the lengths of the front and rear distributed Bragg reflectors (DBRs) and increasing the semiconductor optical amplifier (SOA) length should increase the laser intensity. These considerations may be crucial for continuous-variable QKD (CV-QKD) demonstrations where a bright local oscillator is required.

Performance gains can also be made from the continual development of the InP platform. Modulator bandwidths are continually increasing and laser linewidths and sideband suppression always improving meaning that the optimal performance of integrated photonics is yet to be achieved. Even passive losses through waveguides have halved since the initial designs from 2 to 1 dB/cm. This makes integrated photon delay lines more accessible which may allow simpler operation.

In this chapter, we will introduce the next generation designs of InP QKD transmitters. Optical components are added to improve performance over the previous designs. New methods of generating BB84 states are also introduced by exploiting both circuit design and laser interaction. The packaging process will be described to demonstrate how devices can be optically and electrically connected for robust operation.

Figure 5.1: List of components used for the chip schematics: distributed feedback (DFB) laser, multi-mode interferometer (MMI), distributed Bragg reflector (DBR), current-injection phase modulator (CI-PM), semiconductor optical amplifier (SOA), photodiode (PD), thermo-optic phase modulator (TOPM).

5.2 Pulsed Laser Seeding

In the previous chapter, we saw how states could be encoded through intensity and phase modulation of a continuous wave (CW) laser. This allows 2 GHz clocked states to be generated with high fidelity. However, for a QKD system, we required the state to be phase randomised which meant that the state rate needed to be reduced to 250 MHz. Alternatively, phase randomisation can be achieved with a separate phase modulator where a set of finite phases are randomly chosen which approximates a random phase [9]. This requires a multi-level signal to operate the modulator which increases the complexity of the system and detrimental phase-dependent losses can compromise security. To ensure high bandwidth key exchanges, whilst maintaining simplicity, we might consider a different method of state generation.

Pulsed laser seeding (PLS) is an optical technique that is based on optical-injection locking of lasers which can be used to create narrow pulses with low timing jitter when compared with gain-switching or intensity modulation [182,183]. A schematic is shown in figure 5.2a. An initial (master) laser operates in CW mode which is injected into a second (slave) laser. The slave is electrically pulsed which creates an optical pulse from the injected photons and inherits the phase of the master. As the process is not reliant on a spontaneous emission, the pulse width can be very narrow [145]. However, as the master laser is running in CW operation, the phase of the pulsed slave laser will only drift slowly with the changing phase of the master laser. This will not be sufficient for QKD pulses which require phase randomisation between states.

The pulses generated from optical-injection locking could be phase randomised using a further modulator. This increases the complexity of the optical system and driving electrics so is not ideal. Instead, we can consider phase randomising the phase of the master laser before the optical injection. This is the idea behind the PLS technique.

Instead of operating the maser laser in a CW mode, it is given a DC offset below the lasing threshold and an RF signal gain-switches to provide a long, phase randomised pulse. The pulse is variably attenuated and passed through a circulator to isolate it from the slave laser pulses. A DC offset below the lasing threshold is provided to the slave and an electrical pulse then gain-switches the slave laser when the master optical pulse is in the cavity. This causes the slave to produce a narrow pulse that inherits the optical properties of the master laser. As

the master laser is being gain switched, the pulses produced by the slave laser will be phase randomised.

This method of PLS provides the base pulses for a QKD system but encoding is still required. Previous demonstrations have used a polarisation encoding to generate the BB84 states in adition to PLS [137]. However, for a time-bin encoding one can consider encoding the states directly with the master laser. To maintain phase coherence between time-bins, the master laser can be kept above threshold for two cycles. The pulses generated from the slave laser will then also have a phase coherence. By adjusting the driving voltage for the master laser between time-bins, a phase shift can be created between early and late time-bins. By fine tuning the parameters of a system, all of the BB84 states can be generated in a time-bin encoding scheme by just using PLS.

PLS provides a method of generating BB84 states by overcoming some of the issues with gain-switching or intensity modulation of lasers while also reducing the optical complexity of a circuit. As we saw in chapter 4 when gain switching the laser, the repetition rate of the states was reduced as the laser was required to relax into a coherent CW state. Only then could coherent state be encoded. Previous demonstrations [137, 145] have overcome this limitation as the master laser does not need to relax to a continuous state before seeding the slave laser allowing GHz state rate.

The electrical requirements for the PLS remain stringent with RF signals requiring high resolution vertical precision to sufficiently control the phases of the master laser. PLS has been demonstrated using fibre optic components to show high-fidelity Hong-Ou-Mandel (HOM) interference and measurement-device-independent QKD (MDI-QKD) [137, 145].

5.2.1 Integrated Laser Seeded Transmitter

In this section, we will present two designs for integrated laser seeding transmitters for time-bin encoded QKD. The devices were fabricated by Fraunhofer Heinrich Hertz Institute (HHI) from InP and measure only $6 \times 4\,\mathrm{mm}^2$. Edge couplers on the side of the chip allow optical access while the electrical connections are routed to the remaining three sides. Test structures are included in the design to measure the laser characteristics, photodiode performance and cutbacks allow the waveguide and coupling losses to be estimated. This device also contains a quantum random number generator (QRNG) which will be discussed in section 5.3.

Figure 5.3 shows the GDS for the device and aptly demonstrates the complexity achievable with photonic integrated circuits (PICs). The optical components are shown in blue, while the electrical connections are in red. Schematics of the transmitters are shown in figure 5.2 and the integrated QRNG is discussed further in section 5.3. In total, the device contains eight Fabry-Pérot lasers. The fabrication process meant that all spot-size converters (SSCs) had to be on the same side of the device. Therefore, each SSC was separated with multi-mode

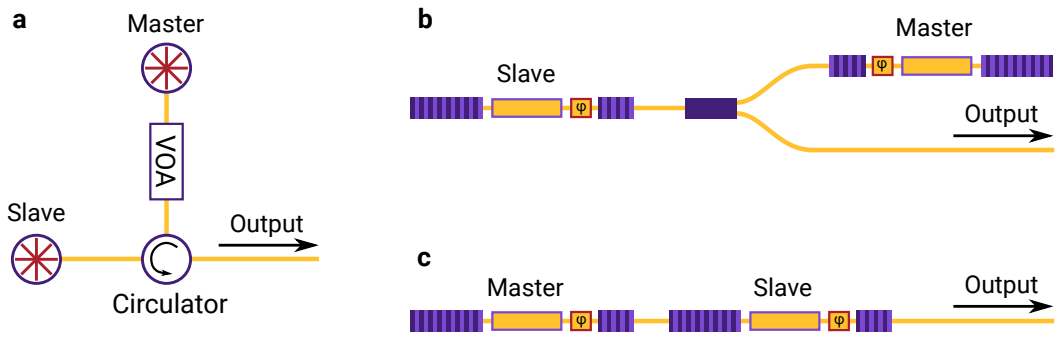


Figure 5.2: a Fibre schematic for pulsed laser seeding (PLS). A master laser provides a pulse which is attenuated and sent to the slave through a circulator. The slave then generates a pulse from this seed which is sent to the output. As there is no non-linearity to exploit for a circulator, the usual method of laser seeding cannot be achieved in integrated photonics. These are the simplest conceivable circuits to attempt PLS in a PIC. **b** The master can inject light through a 1×2 MMI which also allows half of the slave light to the output. **c** The master and slave are in series. Light is injected into the rear DBR of the slave which is also connected directly to the output.

interferometers (MMIs) to the different parts of the chip. This will increase the losses in the circuit and should be considered for the characterisation of the device.

Electrical connections were routed to the side of the chip in staggered rows to help with wirebonding. Waveguide crossings were added where appropriate as the stack does not have a separated electrical layer. Due to the number of electrical connections, shared grounds were implemented to reduce the number of bond pads required.

Currently, there are no standard methods to integrate optical isolation or circulators. Therefore, the standard design for PLS cannot be replicated exactly in the circuit. In this PIC, we include the two simplest methods to allow the master to inject light into the slave. These are shown in figure 5.2. First, (fig. 5.2b) we consider the two lasers connected by a 1×2 MMI. The master can inject light into the front of the slave, which can then be pulsed. Half of the light will then leave the device through the output port. The second design (fig. 5.2c) considers the lasers in series along a waveguide. The master injects light through the rear DBR from which the slave can then create a pulse.

Without isolation between the master and slave laser, back reflections are a potential issue. Such reflections could make it more difficult for the phase randomisation as remnants of previous pulses may impart their phase on subsequent ones. This may be less problematic in design 5.2c as the rear DBR will suppress reflections from the edge facet of the device.

Since this chip was designed and fabricated, similar work was published demonstrating an integrated PLS transmitter based on the InP platform [184]. The designs are similar to those present here but use distributed feedback (DFB) lasers in series with an MZI in between to

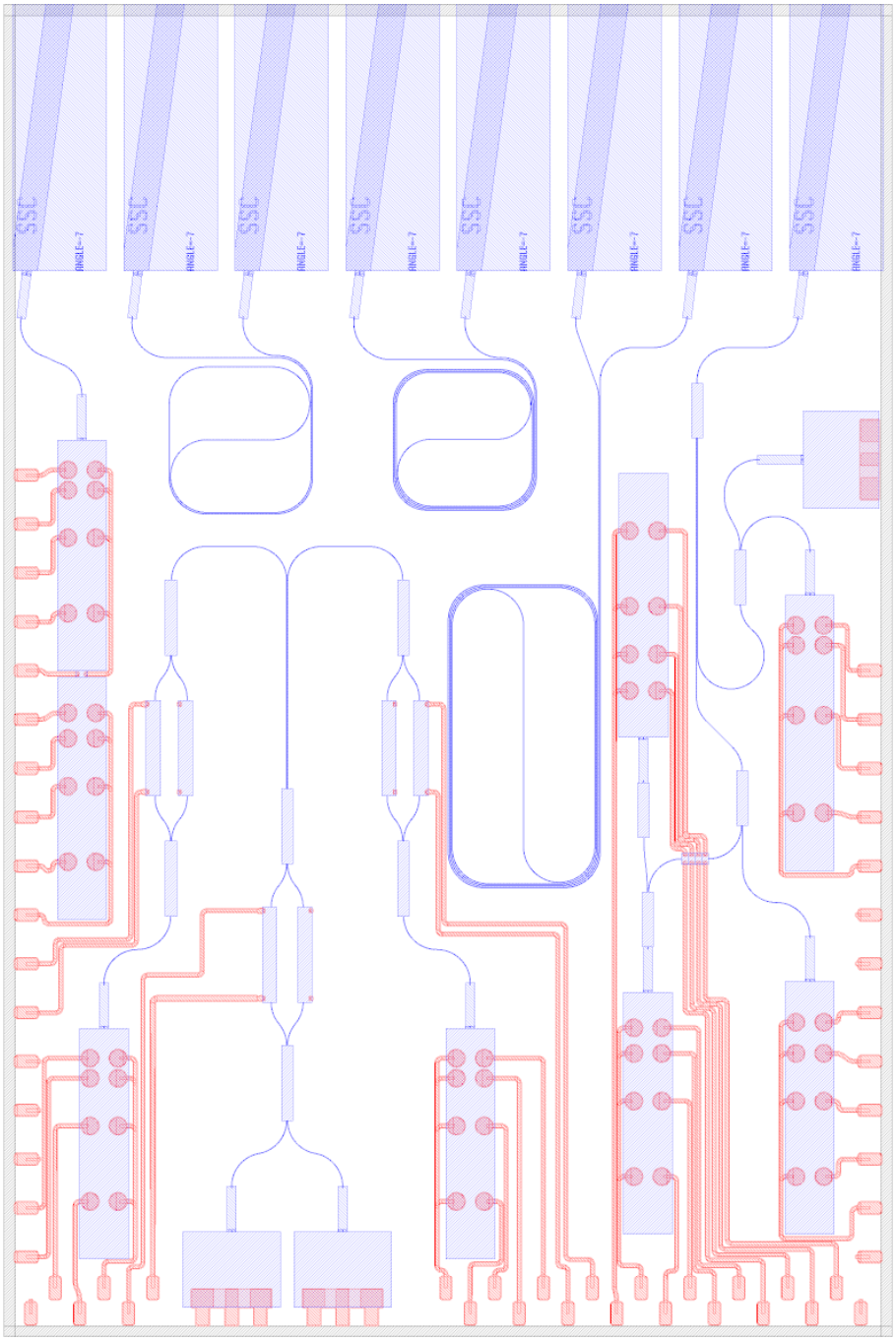


Figure 5.3: This shows the layout of the laser seeded transmitter device fabricated by HHI. The optical components are shown in blue while the electrical connections are in red. The chip measures $6 \times 4\,\mathrm{mm}^2$ and contains two laser seeding prototype circuits, a homodyne QRNG and test structure to measure laser and waveguide performances. Wires are routed to the side of the chip to allow wirebonding. Light is converted from the waveguide mode to a 10 µm mode with SSCs at the side of the chip.

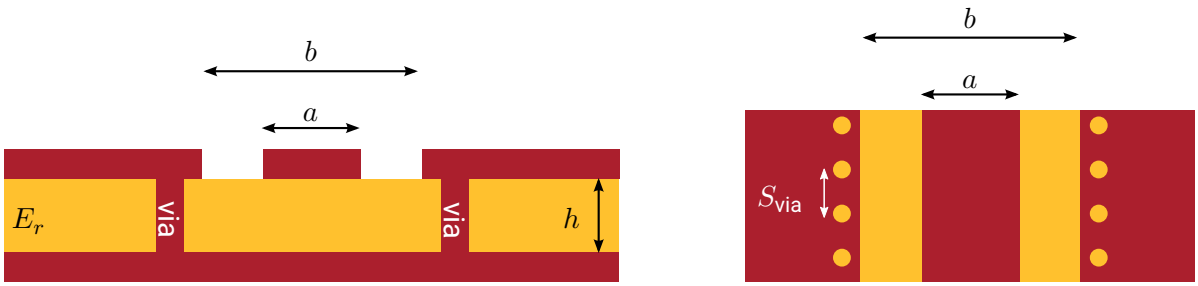


Figure 5.4: Cross-section and top view schematic of the grounded coplanar waveguide (GCPW) structure. The track width, a, total width b, substrate height, h, and dielectric constant E_r determine the characteristic impedance of the track. Vias provide a shield to suppress surface wave modes. Vias are spaced S_{via} which determines their performance.

attenuate the master laser, as required.

5.2.2 Optical and Electrical Packaging

The complexity of the device requires careful consideration to ensure optical and electrical packaging for high-speed operation. This section will describe the design choices for the PCB and how the device was put together. This allows initial tests to be performed.

PCB Design

The electrical connections for integrated devices is challenging, especially in test devices where on-chip real estate is valuable and therefore fully utilised. In figure 5.5 we show the PCB designed to connect most (but not all) components of the chip shown in figure 5.3. For this initial test, the QRNG section of the chip was not connected to reduce the number of electrical connections. In total, 33 electrical lines were included in the design for the initial testing of the integrated lasers, modulators and photodiodes (PDs).

The PCB was made from Rogers 6006 for its high dielectric constant (6.45) and contained four layers. The top layer of the PCB is electroless nickel immersion gold (ENIG) plated for the wirebond connections. The first two layers were dedicated to the RF tracks. The top layer provided signal lines through coplanar waveguide (CPW) while the second layer provided isolation from the DC tracks below. The CPW dimensions can be calculated using equations presented in chapter 3. The high dielectric constant allowed narrow CPWs while maintaining a 50 Ω impedance.

To improve the performance over previous designs, a via fence was included along the RF tracks to create a grounded CPW (GCPW) which should increase the bandwidth [185]. A schematic is shown in figure 5.4. This via fence reflects the signal and stops a surface wave being created along the track. The spacing between the vias is important to maximise bandwidth, as is the spacing between the track and via. Generally speaking, microwaves will reflect

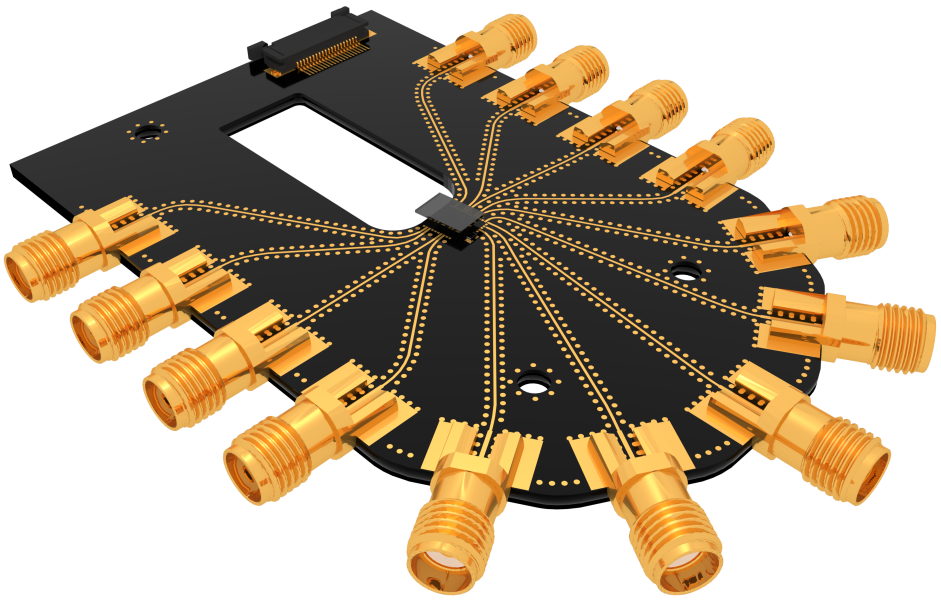


Figure 5.5: PCB designed to connect the HHI device to control and measurement equipment. The chip sits in the middle of the PCB so that RF track length can be minimised. RF lines are shielded with vias to create GCPW for high bandwidth and are connected to edge-launch SMA connectors. DC lines are routed through a lower layer of the PCB and connected to an FFC receptacle. A section of the PCB is milled out to allow a VGA to be mounted for optical connection. Screw holes allow the package to be mounted to a heat sink for thermal management.

off of gaps which are less than ¼ of their wavelength [186]. Therefore, the spacing between each via can be calculated as

$$S_{\text{via}} = \frac{\lambda}{4} = \frac{c}{4f\sqrt{E_r}} \tag{5.1}$$

where f is the maximum frequency of operation and E_r is the dielectric constant of the substrate. For this PCB design, the vias were placed 500 µm from the track and spaced 1 mm apart meaning the GCPW should have a bandwidth up to 25 GHz. SMA edge-launch connectors rated to 26.5 GHz were soldered to the tracks and grounds for high speed signals.

The DC tracks were routed through the third and fourth layers of the PCB. To save space on the top layer of the PCB, the bond pads for the DC connections were capped vias that had been previously plated and plugged. This allows the connections to be immediately routed to a lower layer. These were then routed to an FFC connector on the side of the PCB.

The chip contains a PIN PD for test purposes. To isolate this from the rest of the circuit, a separate ground was created so that it could be tested separately from the rest of the circuit. A GCPW was used to connect this where both ground pads on the chip could be connected to the grounds of the G-S-G line.

The chip was placed in the center of the PCB to minimise the RF track lengths required. One

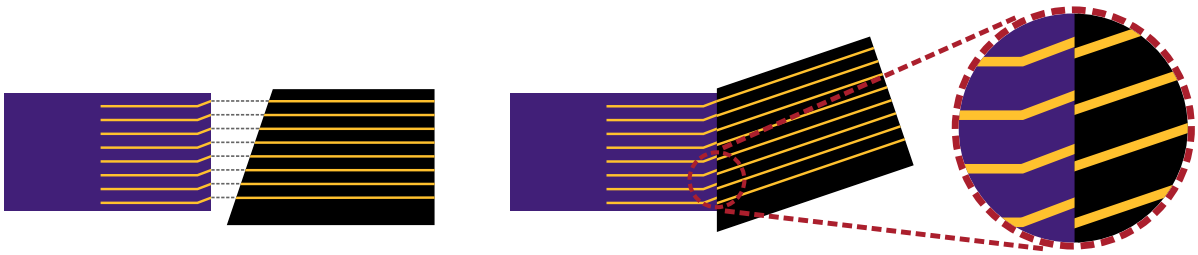


Figure 5.6: The chip facets are designed as 500 µm spaced so as to be compatible with standard VGAs. The facets are at a 7° angle to the edge of the chip to reduce back reflections into the chip. To maximise coupling, the VGA chosen was polished to match this angle. However, once rotated, the vertical spacing of the fibres in the VGA are no longer 500 µm spaced. This meant only one fibre could be connected to the device for these initial tests.

side of the PCB was curved to further reduce the distance to the chip. This section of the PCB was partially milled out the width, length and thickness of the chip so that the top of the chip would be flush with the top of the PCB. This makes wirebonding the chip easier and allows wirebond length to be minimised. This section was plated for thermal conductivity and plated vias added to the bottom of the PCB for thermal management and temperature stabilisation.

As in the previous chips, the SSCs were angled at 7° from the edge of the chip. This is to reduce the back reflections into the chip. To increase the coupling from the chip to the v-groove array (VGA), the chip was rotated by 7° in the PCB design. The VGA could then be polished at a 7° in the opposite direction and be aligned parallel to the PCB. Unfortunately, the geometry of this design was not fully considered meaning that once rotated, the VGA was no longer 500 µm *vertically* spaced. This is shown in figure 5.6. When the first fibre is aligned to the chip, the subsequent fibres no longer line up with the chip facets. Future designs should consider this in the compilation of the chip mask. By adjusting the spacing between SSCs on the chip, a standard polished VGA can be used to connect all the optical ports. Alternatively, one can sacrifice coupling efficiency by leaving the chip parallel with the PCB and using a standard flat-faced VGA.

One should also note that 7° is not the optimal angle for coupling from the chip to the VGA. The refractive index of the InP waveguides is 3.26 whereas standard optical fibre has a refractive index of 1.44. Therefore, through Snell's law, the optimal angle for coupling from an SSC to fibre would be 16°.

A section at the edge of the chip was milled out to provide a space for the VGA to be held while being glued to the chip. The cutout was designed to allow the chip to hang over the side by about 0.5 mm to ease gluing the VGA to the chip. A section at the edge of the PCB was also partially milled out to a depth of around 0.5 mm. This was to allow the bare fibres to remain horizontal and not change the pitch of the VGA when aligned to the chip. It also provides a place for the fibres to be fixed to the PCB for strain relief to make the packaged device more

robust.

Solder pads were placed as close to the chip as possible for a thermistor to be used for thermal stabilisation. Tracks were routed to the bottom of the PCB to provide good thermal connectivity to the chip and peltier. Screw holes were provided to allow the device to be connected to a heat sink and were surrounded by vias to shield the PCB from RF radiation.

Chip Mounting

Unlike the device from Oclaro, where the bottom of the device was the ground plane, there is no need to electrically connect the bottom of the devices from HHI. However, silver epoxy was still used for its strong adhesive properties and good thermal conductivity to aid with temperature stabilising the device. A section of the PCB was partially milled out meaning that placing the chip was more challenging as the sides of the chip would be below the top of the PCB.

To accurately place the chip onto the PCB, vacuum tweezers were used. A silicone cup was used to pick up the chip from the top which could be released when the chip was in position. Silver epoxy was spread onto the milled out section where the chip was then placed. The chip was allowed to overhang the PCB by 0.5 mm to ease VGA connection. The PCB was then heated to 100 °C for 30 min to allow the silver epoxy to cure.

Wirebonding

25 µm gold wire is used to connect the chip bond pads to the PCB which was heated to 100 °C. A high-voltage electrode provides a spark to the end of the wire creating a 50 µm ball at the end of a capillary. The capillary is positioned above the chip bond pad connected to the chip bond pad through thermosonic bonding, which using a combination of heat, pressure and ultrasonic energy to form a bond. The wire is then fed through the capillary to form a loop so the wire can be connected to the PCB pad with a wedge bond, again using thermosonic bonding. This method can be used to create connections to devices with bandwidths above 60 GHz [187], while coax wirebonds have been developed to support bandwidths above 100 GHz [188].

Optical Connection

The device contains eight SSCs on the side of the chip which are designed to convert from the 2.5 µm waveguide mode to a 10 µm mode that is more circular. This means that we don't need to use lensed fibres and can connect the SSCs directly to SMF fibre. The SSCs are 500 µm spaced so as to be compatible with the standard VGA which was provided by Oz Optics for this device.

A brass vacuum chuck was designed from the dimensions of the VGA so that it could be securely held during alignment and gluing. The chuck was placed on a 6-axis micro-positioner

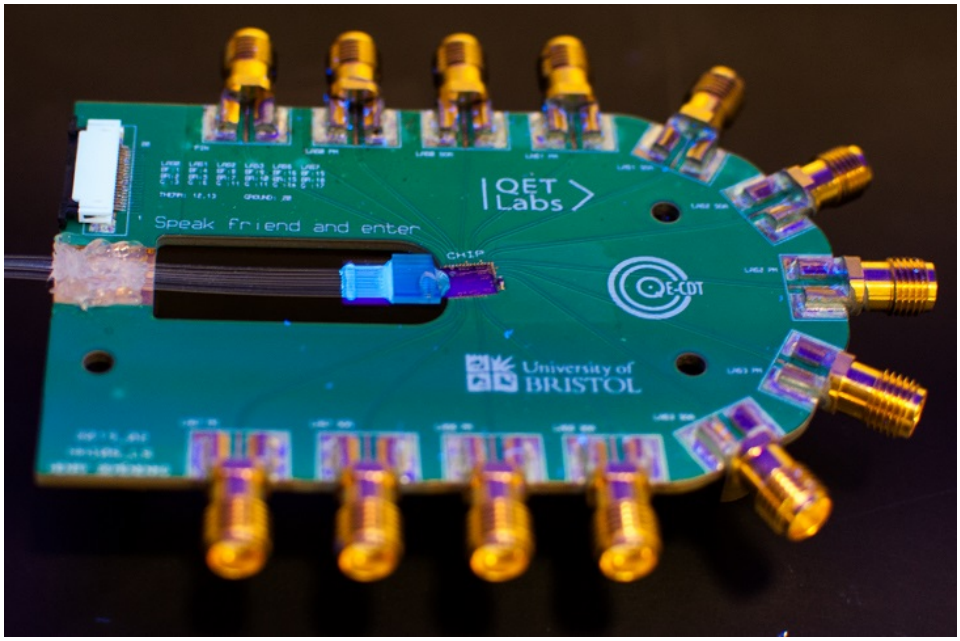


Figure 5.7: Photograph of the packaged PLS test device. The InP chip is glued to the centre of the PCB with the VGA glued to the edge couplers for optical access. Fibre strain relief is shown to the left were the bare fibres from the VGA are attached to the PCB. The electrical pads on the chip have been wirebonded to the PCB for electrical control through SMA and FFC connections.

(Thorlabs NanoMax) so that it could be well aligned with the orientation of the chip.

The integrated lasers were used to align the VGA to the chip. A stable current source provided each laser with 75 mA. The device had been designed with lasers at both the top and bottom of the chip to allow the orientation of the VGA to match that of the chip. As mentioned before, and shown in figure 5.6, it was not possible to align all of the fibres in the VGA with the SSCs. Therefore, the SSC with the most test structures was chosen to be the only fibre aligned.

Once the fibre was sufficiently aligned, the VGA was moved back from the chip to allow glue to be applied between the VGA and the chip. Index matched, UV-cured glue (Dymax OP-4-20632) was used to attach the fibres and the chip. Only a small gap between the VGA and chip was required due to the low viscosity of the glue allowing it to permeate between them.

Once the glue had been applied, the VGA moved forward to be in contact with the chip. A UV LED lamp illuminated the area to cure the glue which was left for 12 hours. Silicone glue was then applied to the bare fibres at the edge of the PCB for strain relief and left to dry. Once the silicone had dried, the vacuum was turned off and the brass chuck could be lowered away from the device. To ensure that the UV cured glue was completely cured, the entire device was placed into a UV steriliser and left for a further 12 hours.

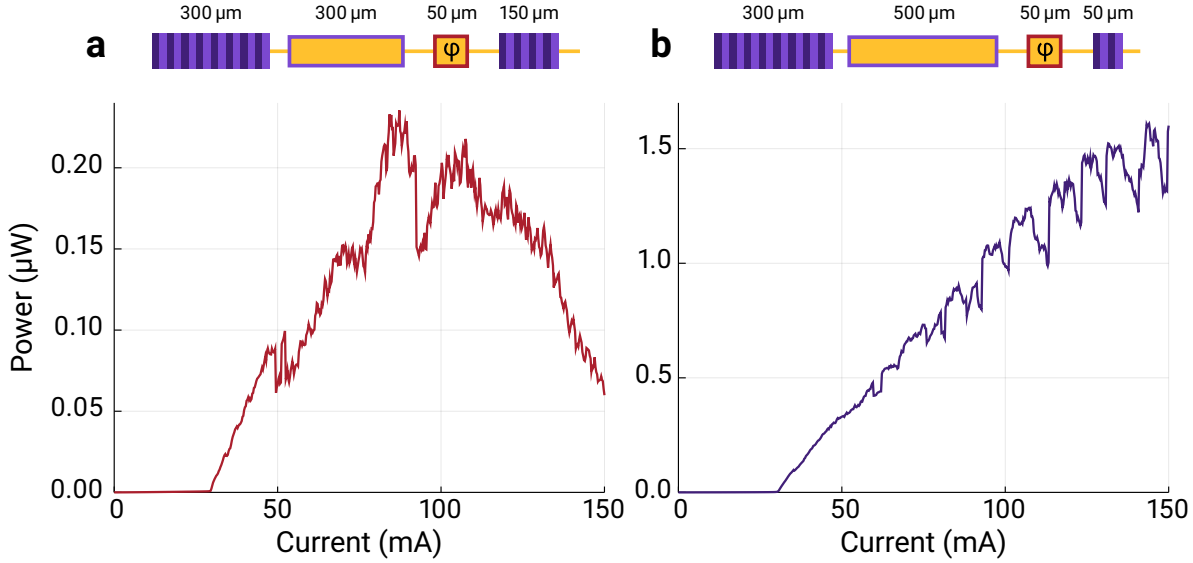


Figure 5.8: Current sweep of the on-chip, Fabry-Pérot test lasers. The two designs have different SOA and front DBR lengths which are shown at the top of the figure. Both show a lasing threshold of around 30 mA. We find that the longer SOA provides considerably more power despite the shorter front DBRs. Fluctuations in power are likely due to the mode competition in the cavity. Reduction in power for 300 µm SOA are likely attributed to heating of the diode reducing efficiency. The effect is elastic so reducing the current recovers the original efficiency.

A photograph of the packaged chip under the steriliser is shown in figure 5.7. The HHI chip sits in the middle of the device and is glued and wirebonded to the PCB. The VGA is attached with UV cured glue and the bare fibres are attached to the PCB with silicone glue to provide strain relief. Electrical connections can be made through the SMA and FFC connections on the edge of the PCB.

The packaged device was screwed to a heat sink with nylon screws to avoid thermal loops. A peltier placed directly under the chip. An Arroyo 6305 was connected to both the thermistor and peliter and a PID loop was calibrated to stabilise the temperature. A case was placed over the PCB to reduce air flow over the device which can cause thermal instability. The temperature was set to 25 °C and the PID loop maintained a temperature instability of less than 0.01 °C. The device could then be electrically and optically tested to characterise the performance.

5.2.3 Laser Operation

This device contains two Fabry-Pérot laser test structures to assess their characteristics. A cavity is formed from two current-injection tunable DBRs which are of different lengths. The rear DBR is 300 µm in length for both test lasers which should provide 95 % reflectivity. Two different front DBR lengths were chosen, as well as different lengths for the SOA. The first laser (figure 5.8a) had a front DBR length of 150 µm with an SOA length of 300 µm. The second laser

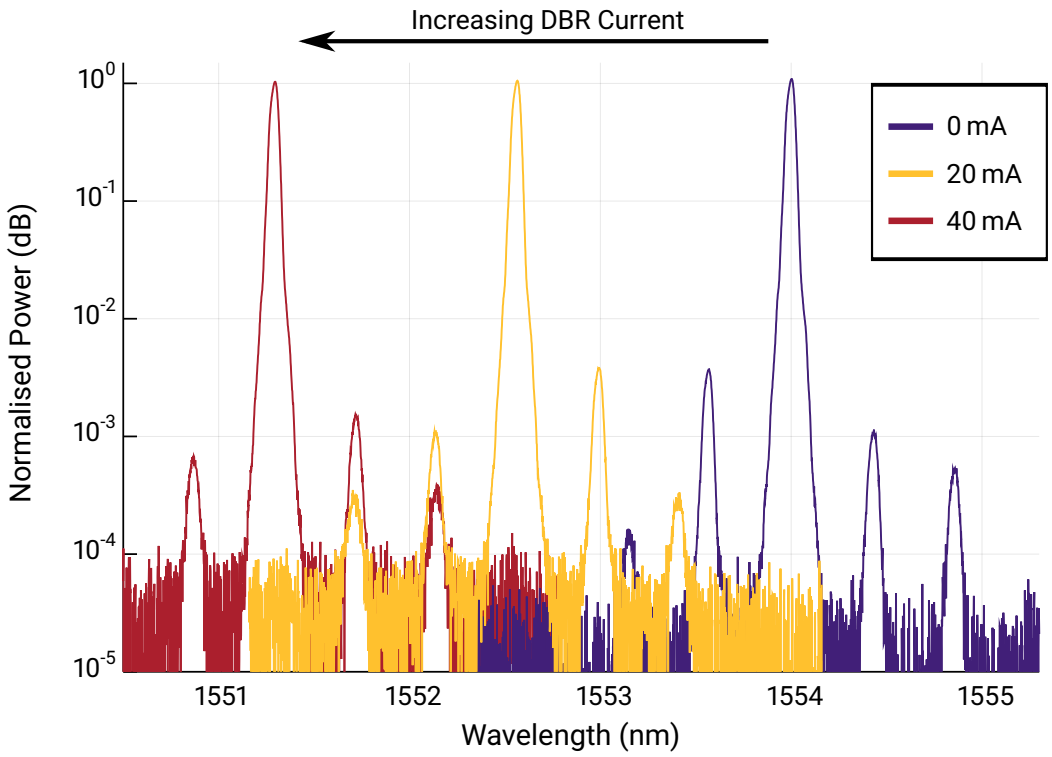


Figure 5.9: Spectra from an OSA of an on-chip laser 5.8a whilst tuning the wavelength with the DBRs. Current injection of the tunable DBRs causes a change of peak reflected wavelength and, therefore, laser wavelength. The lasers are single-mode, with a FWHM of $<$30 pm which was limited by the optical spectrum analyser (OSA) precision. However, the sideband suppression is only 30 dB and varies with DBR tuning. The wavelength can be tuned by 3 nm with a current of 40 mA.

(figure 5.8b) had a front DBR length of 50 µm and SOA length of 500 µm. The reduction in DBR length from 150 µm to 50 µm is estimated by the foundry to reduce the reflectivity from 75 % to 25 %. Both cavities also contain a current-injection phase modulator (CI-PM) which can be used to precisely tune the wavelength of the laser. This method is preferred over current injection of the SOA as it will not affect the output power of the laser. The schematics of the two lasers designs are shown in figure 5.8.

A current sweep of each of the test laser SOAs was performed to measure threshold and power characteristics which are shown in figure 5.8. Both laser designs show a lasing threshold of around 30 mA and gain is initially linear. At high driving currents, both lasers exhibit fluctuations in power. This is likely attributed to mode competition within the laser cavity caused by cavity heating. The increased SOA length in configuration 5.8b allows the laser to reach around three times higher power for the same driving current. This will be partially due to the longer gain medium allowing a higher amplification and also the reduced reflectivity of the front DBR allowing more light to escape the cavity. The power given in figure 5.8 is not

corrected for coupling or routing component loss and so the power on-chip is expected to be higher.

At currents above 100 mA, the 300 µm SOA begins to decrease in power and by 150 mA the optical power has drastically reduced. While more investigation is required, this is likely due an increase in temperature of the diode reducing its efficiency. The effect is elastic so reducing the driving current recovers the efficiency of the laser. This breakdown could possibly be remedied through better thermal management.

Figure 5.9 shows typical specta of the lasers while tuning the DBRs through current injection as measured by an OSA. The lasing is single-mode with a full width at half maximum (FWHM) of $<$30 pm which is limited to the resolution of the OSA used (Anritsu MS9740A). However, the laser only achieves 30 dB of sideband suppression when DBRs are suitably tuned. Both the laser configurations exhibit similar spectra so only laser configuration 5.8a is shown. This suppression is much less than the 50 dB found in the Oclaro lasers of similar design. These sidebands are likely due to the reflected wavelength of the DBRs being quite broad allowing multiple modes to co-exist.

By tuning the front and rear DBRs, the lasing wavelength can be changed. Passing a current through the DBRs causes them to heat, expanding the grating period and reducing the peak reflected wavelength. With a current up to 40 mA, the wavelength of the laser can be tuned by around 3 nm. Fine tuning of the wavelength can be achieved by adjusting the temperature of the device or current injection of the CI-PM within the cavity.

5.2.4 Gain Switching

By applying a DC offset and RF signal to the SOA of a laser, we can test its ability to gain-switch. This ability will be important in creating phase randomised pulses either for use in PLS or for further manipulation in another QKD transmitter scheme.

The SOA within the laser cavity is connected to a GCPW line on the PCB for high-speed operation. Using a bias tee, the DC offset provided by a stable current source (Arroyo 6305) and an RF signal provided by a pulse pattern generator (PPG) (Keysight 81134A) are combined. The laser is attenuated with a variable optical attenuator (VOA) (OzOptics DA-100) and measured with a superconducting nanowire single-photon detector (SNSPD) (Photospot). The detection events are correlated with a time-tagger (PicoQuant Hydraharp) which creates a histogram where the time of arrival is relative to a sync signal provided by the PPG. The device is temperature stabilised at 25 °C with an instability of less than 0.01 °C.

By changing the DC offset below, around and above the lasing threshold, we can characterise the effect of gain-switching, as shown in figure 5.10. A 2 V_{pp} 1 GHz square wave is applied to the SOA for each DC offset. When then DC offset is well below threshold (20 mA), the RF signal does not bring the laser above threshold so the laser cannot start lasing. At the lasing

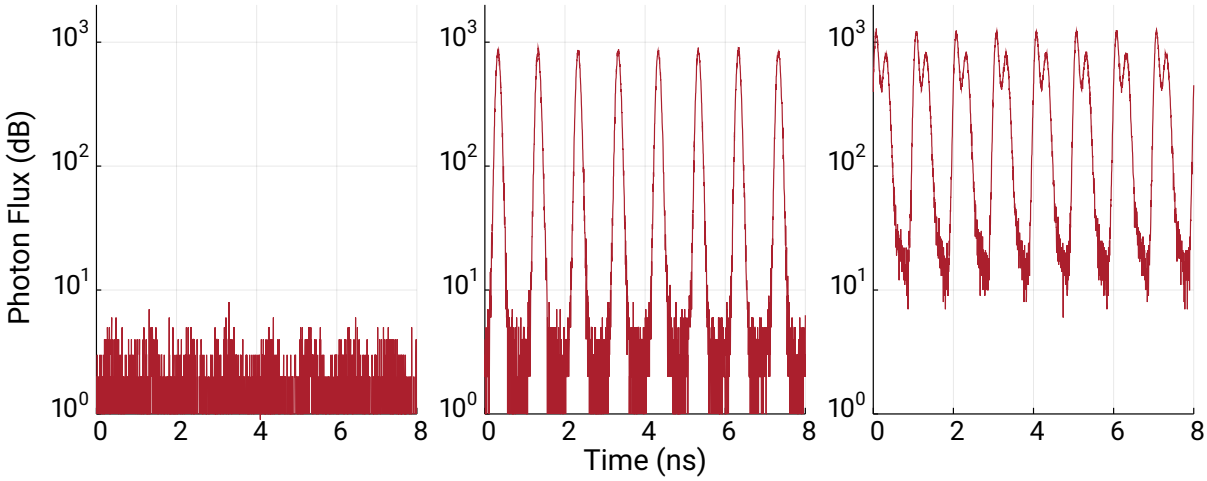


Figure 5.10: Gain switching test of the on-chip lasers. A bias tee mixes a DC offset with an RF signal. A 1 GHz 2 V_{pp} square wave was used and the DC offset was varied around the lasing threshold. 20 mA (left), 30 mA (middle), 40 mA (right). When the DC offset is just below the threshold, 120 ps pulses can be generated with an extinction ratio of around 25 dB.

threshold (30 mA), the square wave creates pulses of around 120 ps FWHM but only during the positive section of the square wave. Otherwise, the laser remains below threshold implying that the pulses would be phase randomised. This, however, would need to be verified. A 25 dB extinction ratio is also achieved. Once the DC offset is above the threshold (40 mA), the RF signal will still generate pulses. However, in between pulses, the laser does not return below threshold. Therefore, we would expect a phase relationship between subsequent pulses which could be checked with an asymmetric MZI (aMZI).

A spectrum of the gain switched laser is shown in figure 5.11. By gain-switching the laser, the spectrum is broadened from $<$30 pm to 80 pm FWHM. The sideband suppression is also reduced to only 10 dB. Such effects would imply that spectral filtering would be required before use as a QKD source to ensure high-fidelity interference is possible but also to remove potential side-channel attacks.

5.2.5 Laser Seeding

As described above, the device contains two methods of performing PLS as shown in figure 5.2b and c. In the absence of a circulator or isolator on chip, these two methods are the simplest conceivable designs. Unfortunately, due to the misalignment of the VGA and the chip, only design 5.2a was accessible for testing.

In this design, the master and slave lasers are connected with a 1×2 MMI which allows the master pulses to reach the slave, but also for half of the slave light to be emitted from the device. Both the SOA are connected with GCPW to allow for high-speed operation. The setup is as with the gain-switching tests above, with a second stable current source and RF signal

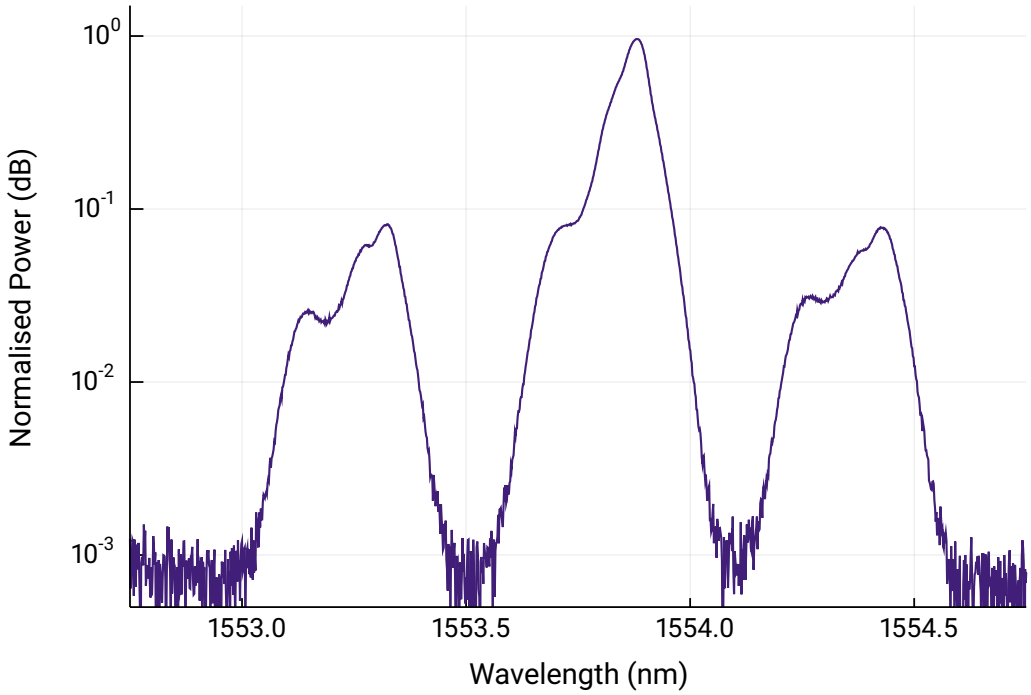


Figure 5.11: A spectrum of the gain switched laser when the DC offset is just below threshold (30 mA) with a 2 V_{pp} 1 GHz square wave. The spectrum is broadened which is usual for a gain switched laser where the central peak has a FWHM of 80 pm. The sideband suppression is also reduced to only around 10 dB.

provided to the device to control the master and slave lasers independently. Electronic delays were used to overlap the master and slave gain-switching in time. Single-photon events can again be measured with an SNSPD and time-tagger to correlate events with the PPG.

In figure 5.12, we show a histogram of single-photon events when 1 GHz square waves are applied to both the master and slave lasers. The master laser had a DC offset of 30 mA, which is lasing threshold, to reduce the turn-on time. This should, however, ensure that the pulses are phase randomised. The slave offset is set at 20 mA which, as we saw previously, should mean that no pulses are created despite the RF signal.

The histogram shows characteristics that are similar to that of the gain-switched pulses above. The FWHM is around 120 ps and the extinction ratio is around 20 dB. Therefore, it is unclear if the device is successfully performing PLS as a reduction of pulse width is common when compared with gain-switching. Similar demonstrations have shown pulse widths of 40 ps [145,184].

Further testing of this PLS is required to verify its operation. One might consider first demonstrating that pulses can be created through optical-injection locking [182,183] to show a reduced pulse width. This should then allow an easier verification of PLS when the mas-

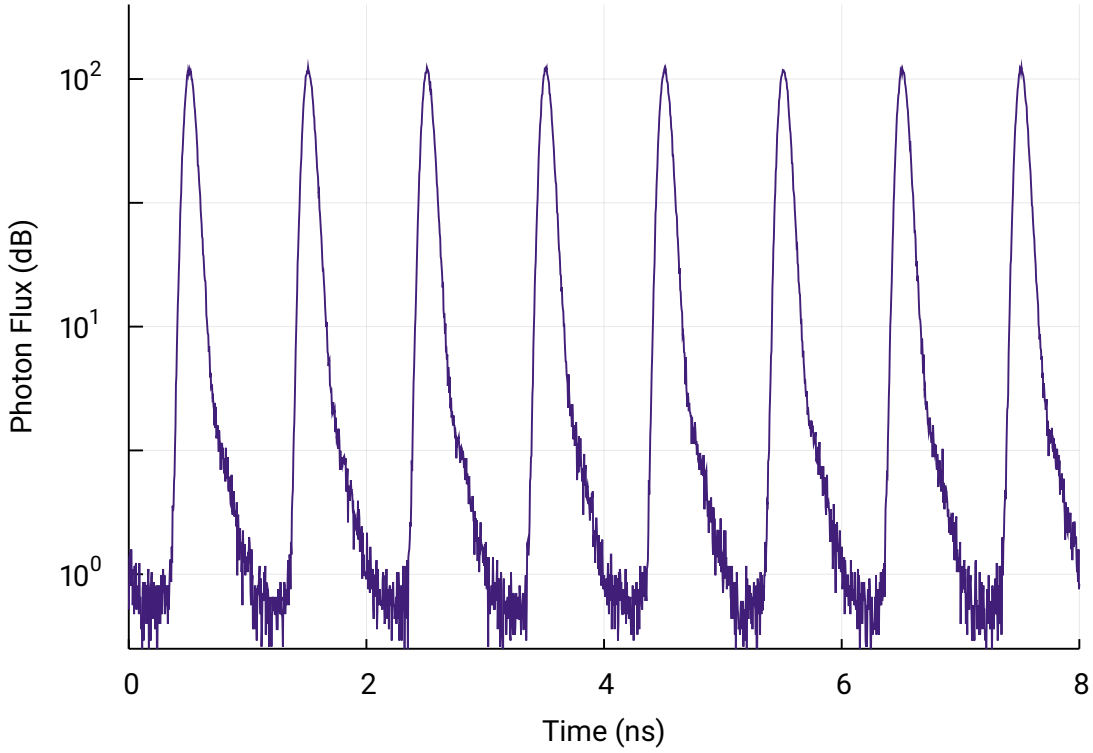


Figure 5.12: Histogram of single-photon events from the PLS design. The master and slave lasers have a DC offset of 30 mA and 20 mA, respectively. By applying 1 GHz square waves to both lasers, we can get pulses that should be phase randomised. However, this will need testing. Pulses show 120 ps FWHM with a 20 dB extinction ratio.

ter laser is pulsed. The final step towards creating a transmitter, would be to demonstrate phase control between the time-bins for X basis encoding. This encoding could either utilise a change in the RF driving voltage of the SOA, or the CI-PM within the laser cavity itself. Revised packaging could allow the second PLS design to be tested and loss measurements from the coupling and waveguides could help with characterisation.

5.3 Quantum Random Number Generation

The security of any QKD system is reliant on having a stream of unbiased randomness available in real-time to determine the states to be sent and the measurement basis. For a GHz-clocked transmitter generating BB84 states about 4 Gb/s of randomness in required to determine the basis, state and decoy level. Generating high bandwidth randomness is real-time remains practically challenging.

Pseudo-random number generators (PRNGs) are readily available which provide perceived randomness at high-bandwidths through a predetermined algorithm based off an initial seed. As the algorithm is predetermined, the numbers are not sufficient for a QKD system as a

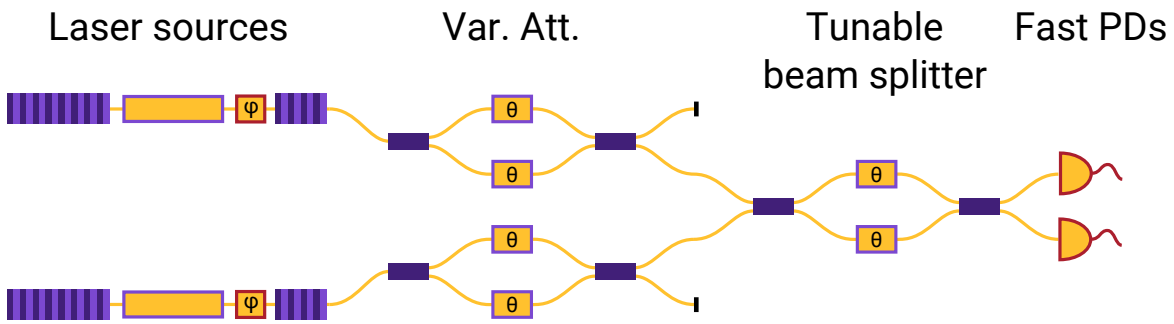


Figure 5.13: Schematic for the QRNG using on-chip laser sources and fast PDs for homodyne measurement. Each laser can be independently controlled and variably attenuated with MZIs allowing the lasers to be tuned in power. A further MZI acts as a beam splitter with a tunable splitting ratio to interfere the two light sources.

compromised initial seed would compromise the entire protocol [189,190]. Therefore, another source of randomness is required.

Instead, methods have been developed to exploit the randomness that is inherent in quantum mechanics. As such, a number of QRNGs have been developed mostly based off sampling quantum states of light [178]. The most viable for QKD systems seem to be based off measurements of continuous-variable states of light, with bandwidths of 68 Gb/s having been demonstrated [191].

The inclusion of laser sources and fast PDs in the InP platform mean that a QRNG can be completely integrated in a single PIC. One such design is included within the chip design shown in figure 5.3 and a schematic is given in figure 5.13. Two laser sources are directly integrated into the waveguides which can be individually, variably attenuated with an MZI. The two arms are combined with another MZI which can act as a beam splitter with a tunable splitting ratio. Measurements are performed by two fast PDs with bandwidths of $>$35 GHz.

This design allows randomness to be generated through three different techniques: amplified vacuum state measurement with homodyne detection [192, 193], laser intensity fluctuations [120] or homodyne phase measurements [194]. All three have been demonstrated to generate random bits at Gb/s rates with the main restriction being the post-processing computational intensity [178].

The full integration of a QRNG mean that the optics for a QKD transmitter have here been completely contained within a single PIC. Processing the random numbers could be achieved with a dedicated field-programmable gate array (FPGA) or application-specific integrated circuit (ASIC) which could increase the randomness generation bandwidth. Signals from the QRNG could be used to directly drive modulators in the QKD transmitter.

5.4 Next Generation QKD Transmitters

In the experiments shown in chapters 3 and 4, there were non-ideal choices in the design which limited the performance. For example, the delay line in the transmitter was too lossy to be used and the MZIs needed to exploit an imperfection in the EOPMs to adjust the phases through thermo-optic effects. With the first demonstrations in mind, we can improve on the design to increase the performance.

We can also use advances in the design and fabrication of the individual components. Waveguide loss has been decreased from 2 to 1 dB/cm [125] meaning that optical delay lines are more achievable.

In figure 5.14, we show the GDS of the next generation QKD transmitters based on InP and fabricated by Fraunhofer HHI. The design is similar to the PLS device with the optical connections occupying one side and the electrical connections along the remaining three. As before, Fabry-Pérot lasers can be used as a light source. However, the HHI foundry offers the option of DFB lasers, of which one is included in the design for optical testing. The phase modulators offered don't yet include EOPMs so a combination of TOPMs and CI-PMs are used which will likely have a lower bandwidth.

The design utilises the optical complexity offered by integrated photonics to allow three separate methods of generating BB84 states in a single devices. The following sections will describe each.

5.4.1 Composite Laser Transmitter

In an effort to reduce the required electronic control, this circuit introduces independent sources to generate each of the four BB84 states. These are combined in a passive, optical circuit with MMIs into a single output mode. A schematic of the transmitter is shown in figure 5.15 with each of the four sources labelled.

Each of the different sources is a Fabry-Pérot laser which enters the optical circuit at different points to create different timing and phase relations for a time-bin encoding. The timing is achieved with an aMZI while the relative phases are created from the phase in the beam splitter transformation.

We have demonstrated that the Fraunhofer HHI lasers are capable of generating gain-switched pulses at 1 GHz with an extinction ratio of 25 dB allowing phase randomised pulses to be generated at high rates. The timing of the electronics is easily controlled to 1 ps resolution allowing the pulses from the sources to be overlapped in time. Also, from chapter 3 we found it was possible to overlap independent sources in all degrees of freedom with high-fidelity. Therefore, we should not expect using independent sources to introduce side-channels to be exploited by Eve or Mallory.

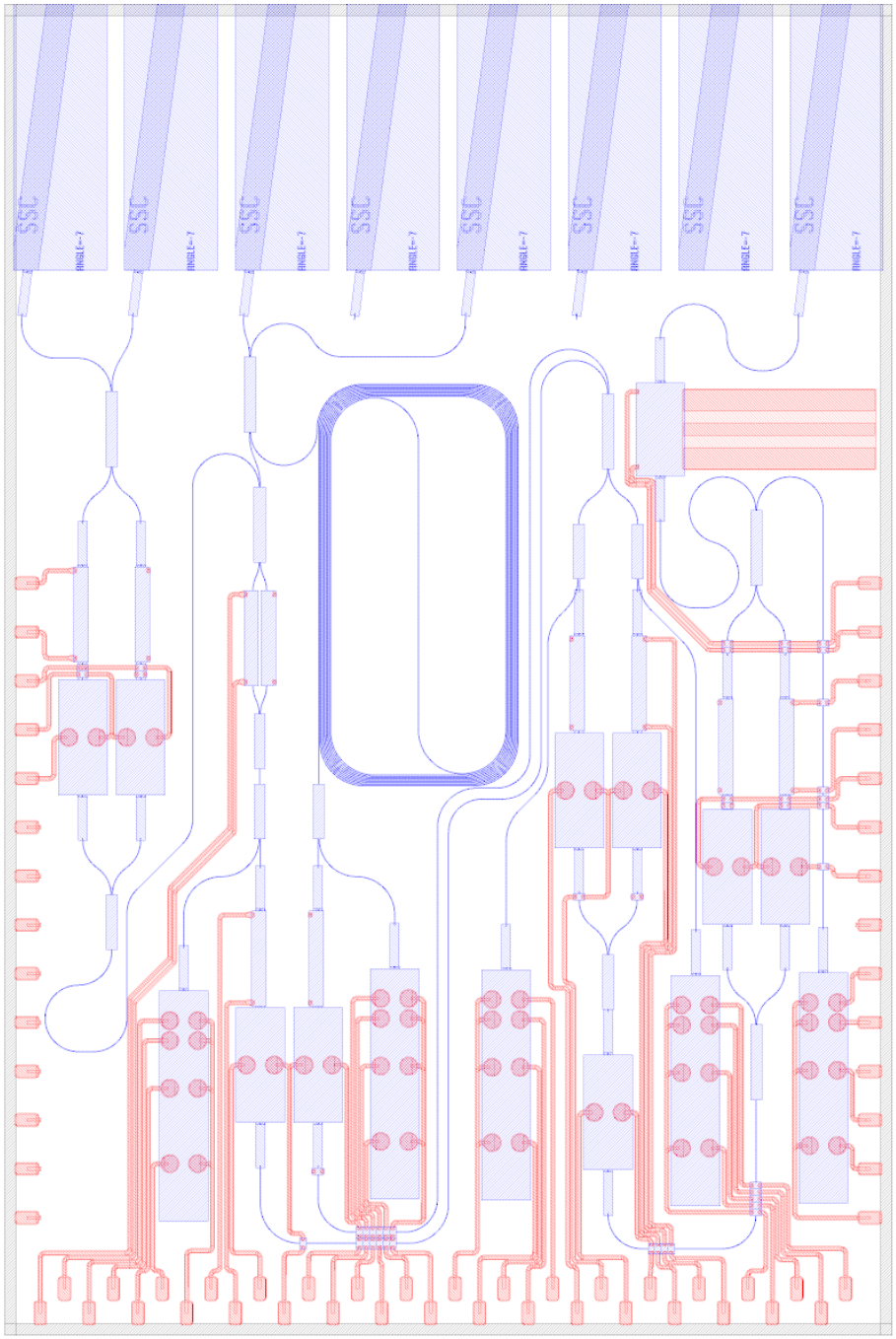


Figure 5.14: Latest generation InP transmitter fabricated by Fraunhofer HHI. The $6 \times 4\,\mathrm{mm}^2$ chip contains three ways to create BB84 states for QKD. The optical components are shown in blue, while the electrical connects are in red. Light created with on-chip lasers and manipulated with CI-PMs and TOPM. States are coupled off the chip through SSCs into fibre.

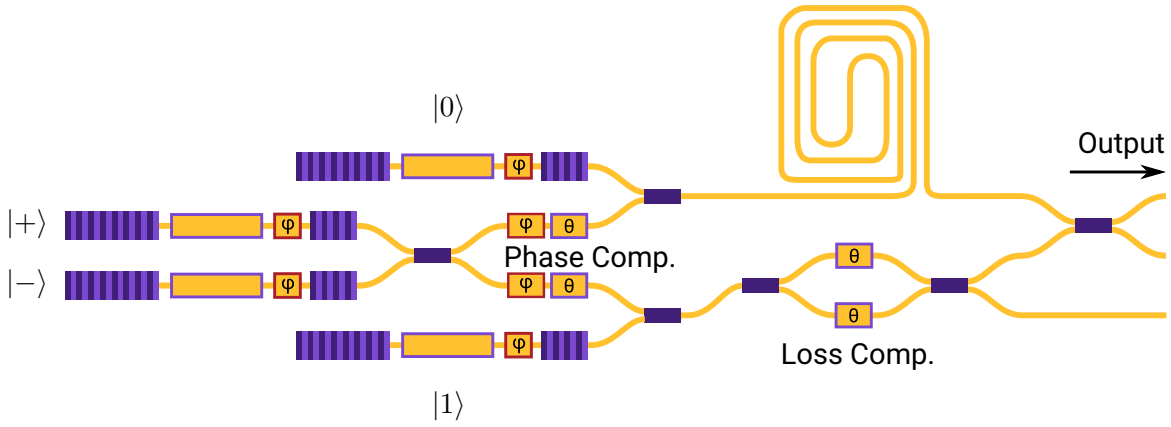


Figure 5.15: Schematic of the composite laser source transmitter. By using independent lasers to generate each of the different states, we can gain-switch each to ensure phase randomisation. A relatively simple optical circuit can then be used to encode the four BB84 states in time-bins. The loss compensation MZI can match the losses between the two paths in the aMZI while the phase compensation modulators allows fine tuning of the relative phases.

To consider how each laser source generates each BB84 state, consider the operator transformations of the circuit. The beam splitter transformations are given as

$$\hat{a}^\dagger \rightarrow \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{b}^\dagger\right) \quad \text{and} \quad \hat{b}^\dagger \rightarrow \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{b}^\dagger\right) \tag{5.2}$$

where $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are the creation operators for the top and bottom paths, respectively.

The delay line in the circuit will convert pulses in the top path from early to late while the bottom path will be unaffected i.e.

$$\hat{a}_e^\dagger \rightarrow \hat{a}_l^\dagger \quad \text{and} \quad \hat{b}_e^\dagger \rightarrow \hat{b}_e^\dagger \tag{5.3}$$

where will assume for the purpose of analysis that the circuit is lossless. Of course, the loss between the long and short arm of the aMZI will be different. A nested MZI is included to compensate for this loss.

These transformations can be applied to each laser source, where we consider that each can be independently pulsed in the early time-bin. First consider the lasers in the Z basis, which enter the circuit before the delay line. The pulse from the $|0\rangle$ laser transforms as

$$\hat{a}_e^\dagger \xrightarrow{\text{Delay}} \hat{a}_l^\dagger \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}\left(\hat{a}_l^\dagger + \hat{b}_l^\dagger\right) \tag{5.4}$$

whereas the $|1\rangle$ laser pulse becomes

$$\hat{b}_e^\dagger \xrightarrow{\text{Delay}} \hat{b}_e^\dagger \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}\left(\hat{a}_e^\dagger - \hat{b}_e^\dagger\right) \tag{5.5}$$

Equivalently, we can apply the transformations to the X basis laser pulses which will experience the entire aMZI. For the $|+\rangle$ pulse, the transformation is

$$\hat{a}_e^\dagger \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}(\hat{a}_e^\dagger + \hat{b}_e^\dagger) \xrightarrow{\text{Delay}} \frac{1}{\sqrt{2}}(\hat{a}_l^\dagger + \hat{b}_e^\dagger) \xrightarrow{\text{BS}} \frac{1}{2}(\hat{a}_e^\dagger + \hat{a}_l^\dagger - \hat{b}_e^\dagger + \hat{b}_l^\dagger) \tag{5.6}$$

while for the $|-\rangle$ pulse we find

$$\hat{b}_e^\dagger \xrightarrow{\text{BS}} \frac{1}{\sqrt{2}}(\hat{a}_e^\dagger - \hat{b}_e^\dagger) \xrightarrow{\text{Delay}} \frac{1}{\sqrt{2}}(\hat{a}_l^\dagger - \hat{b}_e^\dagger) \xrightarrow{\text{BS}} \frac{1}{2}(-\hat{a}_e^\dagger + \hat{a}_l^\dagger + \hat{b}_e^\dagger + \hat{b}_l^\dagger) \tag{5.7}$$

By looking at the output port from the top path, we find that we can generate the states

$$|0\rangle = \hat{a}_e^\dagger, \quad |1\rangle = \hat{a}_l^\dagger, \quad |+\rangle = \frac{1}{\sqrt{2}}(\hat{a}_e^\dagger + \hat{a}_l^\dagger), \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(\hat{a}_e^\dagger - \hat{a}_l^\dagger) \tag{5.8}$$

where the states have been renormalised considering only the top path. There is no need to compensate the intensity of the Z and X basis as was the case with the intensity modulated states.

As is usual for QKD transmitters, we will be using weak coherent states (WCSs) instead of single photons so the bottom path ($\hat{b}^\dagger$) can be considered a loss. However, this loss is before the states have been sent through the quantum channel so can be compensated with an increased pulse intensity. Phase modulators within the aMZI allow fine adjustments of the relative phases between the long and short arms which are unlikely to be phase matched due to fabrication tolerances.

One final thing to consider with this transmitter is the spectral broadening and sideband suppression reduction seen whilst gain-switching. Without proper filtering, such spectra would exhibit reduced interference during measurement and possible information leakage to Eve and Mallory. Commercially available filters should resolve these issues and also allow the laser wavelengths to be precisely overlapped.

Future designs could considering including a master laser to seed each source in a PLS scheme. Pulse length could be shortened, as well as delay length, which would allow the device to operate at higher clock rates. Provided that the measurement devices could support the high rates, this could further increase the rates of QKD systems.

5.4.2 Delay Line Time-Bin Encoding

While the previous generation of devices included delay lines to encode timing information, they were too lossy to be used. We have included a delay line in the design of this chip which should have lower losses. This should reduce the complexity of the control electronics and mean phase randomised pulses can be generated from a laser source which can subsequently be encoded into phase coherent time-bins. A schematic of the transmitter is shown in figure 5.16a.

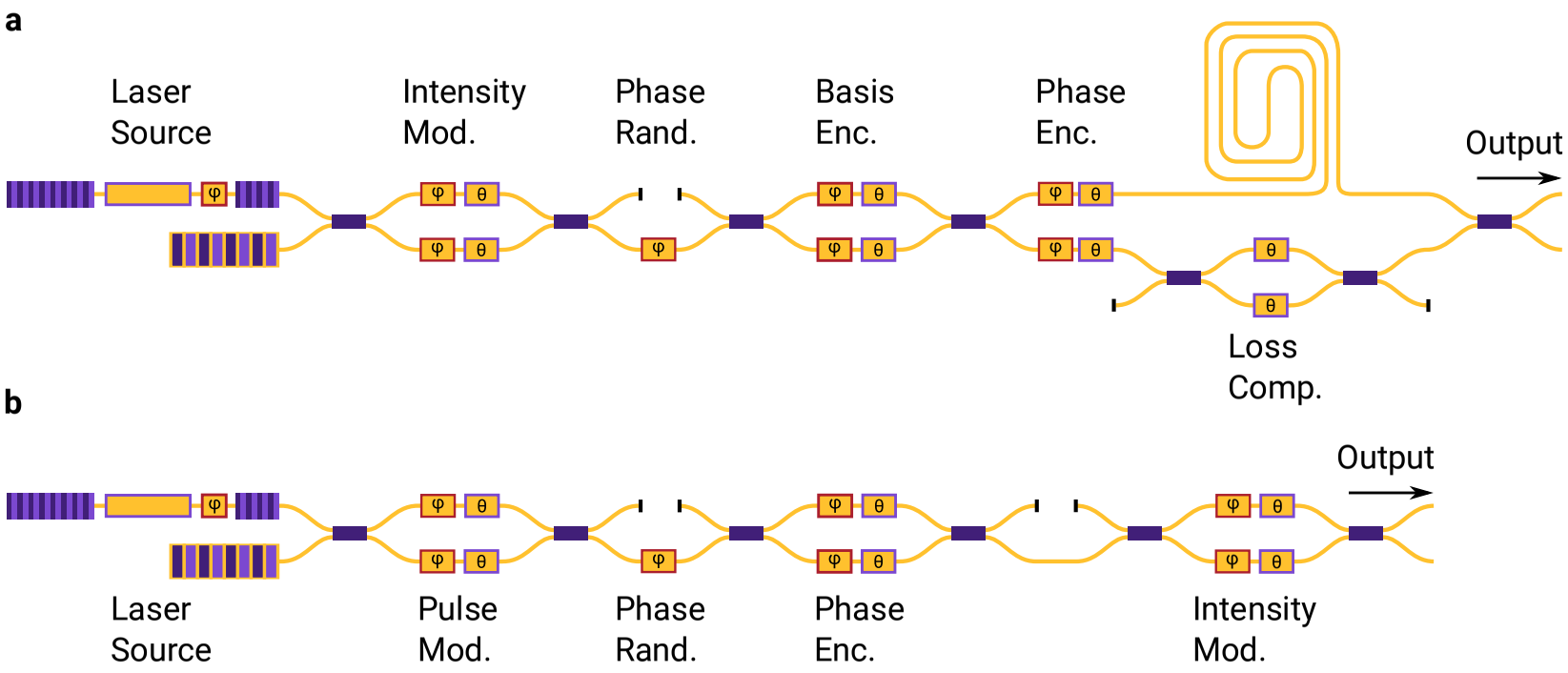


Figure 5.16: Schematic of the operating modes of the HHI transmitter. **a** Either a DBR or DFB laser source provides a phase randomised WCP through gain-switching. The pulse is attenuated with an MZI for decoy state preparation (Intensity Mod.) and a fast CI-PM can be used if further phase randomisation is required. Basis Enc. switches between the long and short arms of an aMZI, where superposition is used for X basis states. A CI-PM within the aMZI then encodes relative phases between early and late time-bins. An MZI allows for loss compensation between the long and short arms. **b** A laser source provides CW light which is modulated into pulses (Pulse Mod.). A CI-PM can then provide phase randomisation over the entire state and an MZI can encode relative phases. A final MZI provides intensity modulation for decoy state preparation.

To test the performance of two laser sources, both Fabry-Pérot and DFB lasers are included each of which can generate phase-randomised WCSs. Cascaded MZIs and a delay line can then encode information in time-bins. Each MZI includes both TOPMs to perform calibration and CI-PMs for high-speed operation.

The first MZI is used to attenuate the pulses accordingly for a decoy state protocol while the second acts as a high-speed tunable beam splitter. For the X basis states, the MZI splits the states, with half being delayed. This means that the early and late time-bins will be phase coherent as they have come from the same pulse.

5.4.3 Intensity Modulation

Finally, this device can operate in the same way as the Oclaro chip from chapter 4. The laser sources are run in CW and WCSs are modulated from an MZI, with a pulse in both time-bins being used to encode X basis states. Phase randomisation is achieved either through gain-switching the laser source or with a CI-PM. Relative phases are again encoded with an MZI to avoid phase-dependent losses and a final MZI modulates the intensity of the states for a decoy protocol.

The design has been improved over the previous circuit with TOPMs included in each MZI to correct phase differences between the two paths. A DFB laser is also included so that phase randomisation performance can be tested and compared to the results previously demonstrated in chapter 4.

5.5 Outlook

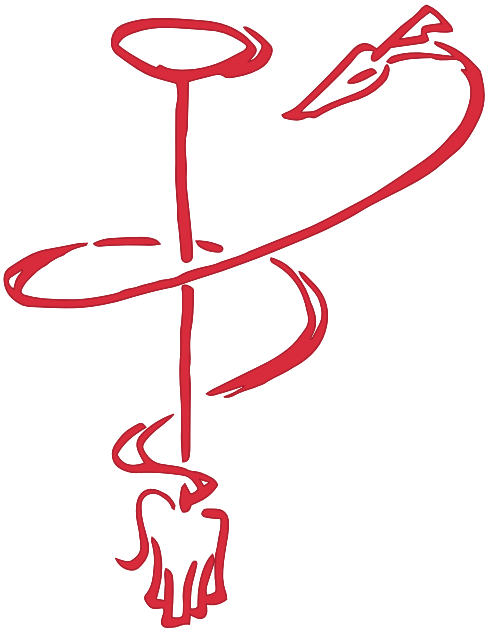
While a number of QKD demonstrations have been presented in recent years (notably references [9,102,104,195,196]) progression in the technology will always allow higher-bandwidth designs and new protocol demonstrations. This chapter has introduced new circuits that improve on previous devices, whilst also facilitating new operating techniques.

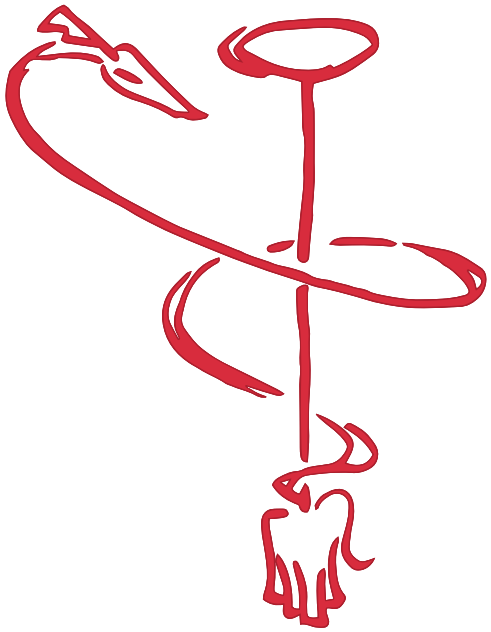
A recent demonstration presented PLS as a useful source of WCS through an MDI-QKD protocol [137]. Despite the lack of isolation or circulators in integrated photonics, we have presented two circuits to achieve similar pulse preparation. The high-speed operation of the integrated lasers show promising initial characterisation, albeit in need of wavelength filtering. With further work on their operation, the circuits should be capable of high-fidelity state generation.

Demonstrations of high-fidelity laser overlap from chapter 3 mean that a composite transmitter with multiple laser sources becomes viable without introducing side-channels to be exploited by Eve and Mallory. While the optical circuit becomes more complex, the high-speed electronics required is reduced. Phase coherent time-bins can be encoded from phase ran-

domised pulses with optical delay lines where most of the encoding is performed passively.

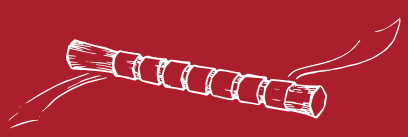
Improvements over the initial QKD transmitters have been included both utilising a better understanding of the operation of integrated photonics and new components available from the foundry. Such modification should help to improve both the bandwidth and fidelity of the states. The devices have been fabricated and so can now be packaged and tested by techniques introduced in this thesis.

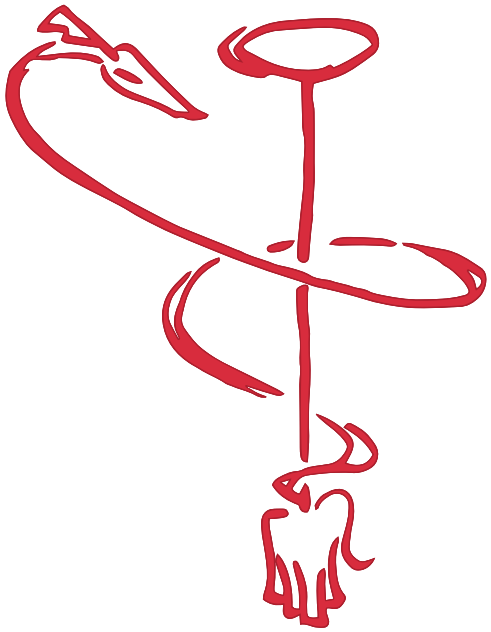




6

Conclusion





6.1 Summary

This thesis has advanced the application of integrated photonic devices for quantum-secured key exchange. We introduced the Hong-Ou-Mandel (HOM) interference effect as a fundamental tool in quantum optics. Interference was demonstrated between independently controlled, integrated devices with a visibility of 46.5 ± 0.8 %, close to the theoretical maximum of 50 %. The devices used entirely integrated components to generate weak coherent pulses (WCPs) at 431 MHz and did not require any wavelength filtering beyond the laser cavity. Active phase randomisation of the on-chip laser was achieved through gain-switching at a reduced rate of 250 MHz to maintain compatibility with time-bin encoding. Again, interference was demonstrated with a high visibility.

Using further integrated components, we encoded 2 GHz clocked, time-bin encoded quantum states from the on-chip laser and interfered them to demonstrate measurement-device-independent quantum key distribution (MDI-QKD). We show a phase error rates less than 30 % with bit error rates around 0.5 %. We introduced a bank of detectors at the receiver to increase key rates. At short distances (25 km), over 12 kbps could be securely exchange, while at 100 km 1 kbps was shown. Positive key generation was demonstrated at 200 km and, from the performance of the system, we predict that positive key generation is possible at distances beyond 350 km. The trade-off between cost-effective electronics and security was discussed. Inter-symbol interference (ISI) was shown as a potential side-channel which would need to be addressed in future systems. Finally, a fully-integrated system was presented by utilising waveguide integrated detectors. A silicon device could replace the fibre-optic receiver used in the first demonstration. This would facilitate further accessibility in a future network and potential benefits for photonic routing and detection efficiency.

We explored how developments in integrated photonics can improve the performances of quantum key distribution (QKD) transmitters and introduced new photonic circuit designs. Through pulsed laser seeding (PLS), we aim to increase the generation rate of phase randomised quantum states so that integrated devices can fulfil the bandwidth requirements of modern networks. The devices were electrically and optically packaged and initial characterisation showed promising results for these new devices. Quantum random number generator (QRNG) designs were integrated with QKD transmitters on a single monolithically fabricated device to allow modulation directly from true randomness. All of the photonic components have been combined in a single chip. Dedicated electronics chips would allow truly mass-manufacturable QKD systems. Finally, new circuit designs for simplified state generation were introduced. With an increased optical complexity, we can drastically reduce the requirements on the driving electronics.

6.2 Outlook

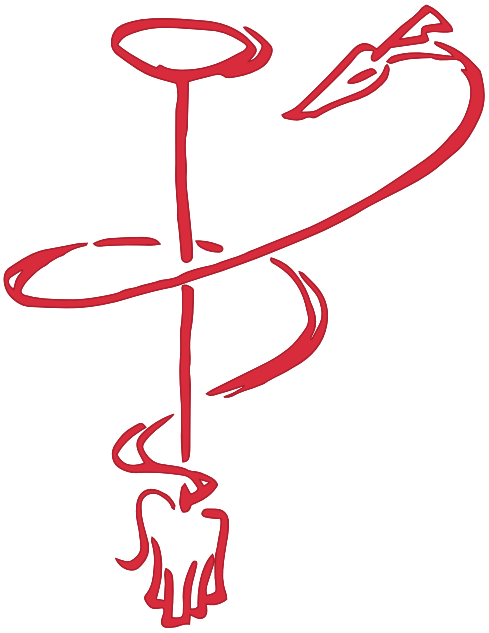
It is paramount that the security of crucial network infrastructure is addressed as computing power inevitably increases. Quantum computing is one known threat against modern communication protocols. However, the situation is more dire than arguments over the 'if' or 'when' of quantum computing. The underlying security of all widely used cryptographic systems is based from assumed computationally-hard, mathematical problems. There is no guarantee of the validity of these assumptions, or even that they currently remain valid.

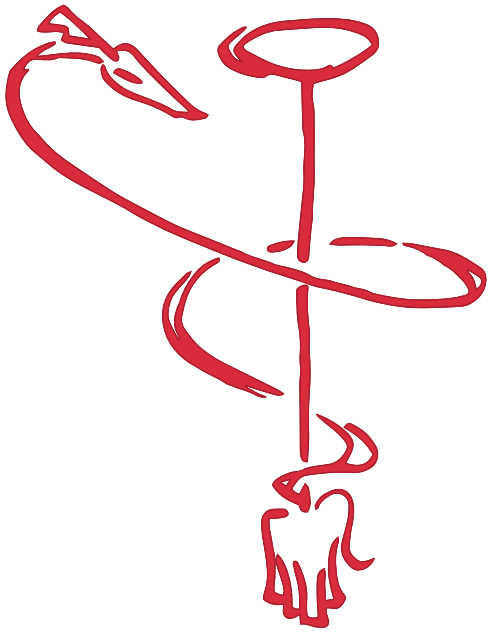
In developing a new precedent for secure cryptography, dubbed 'quantum-safe', there are two available routes. The first, which is favourable to the current network architecture, creates public-cryptography based off of new problems that are thought to be even more difficult to solve than those in current protocols. While these protocols will utilise the same classical computers, there is still no guarantee of their security. Even under full scrutiny of the scientific community, a new quantum algorithm may be imminent.

QKD offers an entirely different solution with security founded in well established laws of physics. However, there are several key issues that need to be addressed before quantum-secured networks can be widely deployed. First, we must ensure that we can the theoretical security of a protocol is maintained in physical QKD systems. Second, there must be a way to mass-manufacture devices with the precision required to create, manipulate and detect quantum states.

This thesis aims to alleviate both of these concerns. By implementing new protocols and carefully considering the operation of the transmitter, we can ensure that a system satisfies the conditions of protocol security. We have demonstrated this new system based on the integrated photonics platform. Monolithic fabrication will be the only that we can truly satisfy the mass-manufacturability of QKD devices.

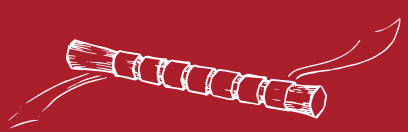
The final concern with introducing QKD networks is that creating "quantum-ready" networks will either be too costly or impractical. I will finish by arguing that quantum-secured communication is only the first use case for developing these new networks. As quantum technologies advance, new protocols will drive the development of these networks based on the same components. Single-photon detection and quantum state manipulation will all be requirements of any future quantum network. The integrated QKD devices presented here will form the building blocks of the quantum internet so that in the future we may share videos of quantum cats.

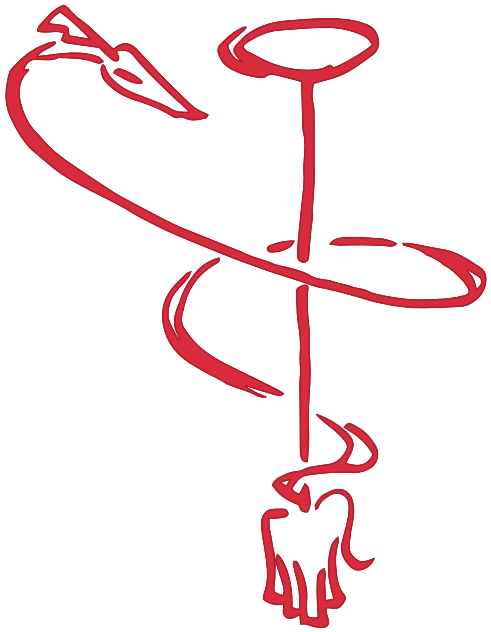




A

MDI-QKD Gains and Errors





Here, we provide the experimental values used to estimate the secret key rates. The errors, $E_{\mu\mu}^{X,Z}$, and gains, $Q_{\mu\mu}^{X,Z}$, are as defined previously in the protocol description. The secret key rates, S, are provided as well as acquisition time, T, for reference. Photon numbers are fixed at 0.2 for the signal states and $\{0.1, 0.01\}$ for the decoy states.

Attenuation (Distance)	S (bps)	e_{ss}^{Z} (%)	Q_{ss}^{Z}	T (seconds)
5 dB (25 km)	12721.46	0.416	4.61×10^{-4}	60
10 dB (50 km)	5471.16	0.535	2.45×10^{-4}	60
15 dB (75 km)	2374.80	0.451	9.66×10^{-5}	600
20 dB (100 km)	1084.58	0.518	3.16×10^{-5}	600
25 dB (125 km)	143.23	0.426	1.20×10^{-5}	1800
30 dB (150 km)	92.37	0.564	3.64×10^{-6}	1800
35 dB (175 km)	42.79	0.523	1.32×10^{-6}	3600
40 dB (200 km)	1.25	0.431	3.58×10^{-7}	3600

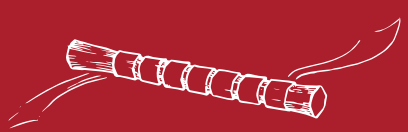
Table A.1: Z basis errors and gains, secret key rate, S, and the data acquisition time, T.

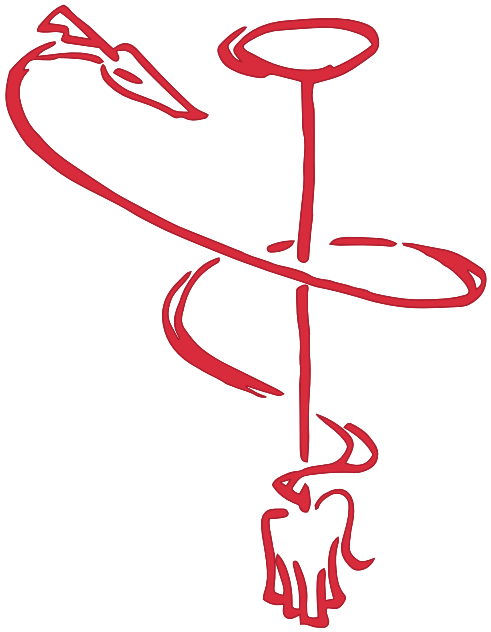
	e_{ij}^X	μ	ω	ν	Q_{ij}^X	μ	ω	ν
5 dB	μ	29.2%	44.4%	52.0%	μ	1.68×10^{-4}	3.96×10^{-5}	2.53×10^{-5}
(25 km)	ω	43.9%	32.0%	50.9%	ω	4.02×10^{-5}	1.63×10^{-6}	3.41×10^{-7}
	ν	50.3%	50.5%	50.0%	ν	3.24×10^{-5}	3.72×10^{-7}	1.20×10^{-9}
10 dB	μ	31.9%	45.3%	51.6%	μ	7.72×10^{-5}	2.01×10^{-5}	1.36×10^{-5}
(50 km)	ω	44.9%	31.7%	60.8%	ω	1.91×10^{-5}	7.56×10^{-7}	9.84×10^{-8}
	ν	50.6%	49.2%	50.0%	ν	1.59×10^{-5}	1.80×10^{-7}	0.00
5 dB	μ	29.7%	44.4%	51.1%	μ	3.34×10^{-5}	8.62×10^{-6}	5.80×10^{-6}
(75 km)	ω	43.7%	32.9%	53.1%	ω	8.47×10^{-6}	3.56×10^{-7}	6.89×10^{-8}
	ν	50.5%	49.1%	55.6%	ν	6.88×10^{-6}	7.32×10^{-8}	4.80×10^{-10}
20 dB	μ	30.0%	45.7%	51.3%	μ	1.16×10^{-5}	3.26×10^{-6}	2.36×10^{-6}
(100 km)	ω	42.5%	32.6%	54.5%	ω	2.61×10^{-6}	1.35×10^{-7}	2.76×10^{-8}
	ν	49.9%	50.5%	50.0%	ν	2.03×10^{-6}	2.28×10^{-8}	1.20×10^{-10}
25 dB	μ	35.1%	46.4%	51.5%	μ	3.53×10^{-6}	9.42×10^{-7}	6.59×10^{-7}
(125 km)	ω	46.0%	34.6%	56.5%	ω	9.45×10^{-7}	3.32×10^{-8}	4.28×10^{-9}
	ν	50.1%	50.7%	50.0%	ν	8.40×10^{-7}	9.08×10^{-9}	0.00
30 dB	μ	31.7%	43.2%	51.5%	μ	1.04×10^{-6}	2.84×10^{-7}	1.93×10^{-7}
150 km)	ω	45.8%	31.6%	65.0%	ω	2.98×10^{-7}	1.06×10^{-8}	1.12×10^{-9}
	ν	50.7%	62.1%	50.0%	ν	2.60×10^{-7}	1.76×10^{-9}	0.00
35 dB	μ	30.3%	45.5%	51.7%	μ	4.62×10^{-7}	1.35×10^{-7}	9.63×10^{-8}
(175 km)	ω	44.7%	31.9%	48.0%	ω	1.06×10^{-7}	5.34×10^{-9}	1.30×10^{-9}
	ν	51.5%	50.0%	50.0%	ν	8.27×10^{-8}	1.12×10^{-9}	0.00
40 dB	μ	30.7%	47.2%	52.1%	μ	1.20×10^{-7}	2.99×10^{-8}	2.21×10^{-8}
(200 km)	ω	42.8%	35.5%	45.7%	ω	3.36×10^{-8}	1.42×10^{-9}	3.80×10^{-10}
	ν	51.3%	37.0%	50.0%	ν	2.57×10^{-8}	3.40×10^{-10}	0.00

Table A.2: X basis errors and gains for MDI-QKD key rates estimation.

B

100 Tips for Doing a PhD





1. Always go to the bar with someone more senior than you
2. Ask forgiveness, not permission
3. Remember that you will forget things
4. Always make figures on a white background
5. Timelines are useful to give you perspective
6. It is impossible to keep to a timeline
7. Work out how long you think something will take, and then multiple by 10 [197]
8. Academic clocks run *at least* 5 minutes late
9. Be nice to the admin team, they know where your supervisor is
10. Long days $\neq$ productivity
11. Coffee is your friend
12. No one else has a clue what they're talking about either
13. You will make stupid mistakes
14. Equipment will break
15. Where a paper is published has no relation to the work's quality
16. If someone on Stack Overflow hasn't solved your problem, you're probably in too deep
17. Learn LaTeX and never look back
18. The complexity of coding LaTeX is inversely proportional to how long you expect it to take
19. Aesthetics are almost as important as content
20. Remember to take a holiday
21. Don't feel guilty about ignoring emails on holiday
22. Take holidays *after* conferences so that you're already over the jet lag
23. Backup your data
24. Most meetings are optional
25. Imposter syndrome is real [198]

26. Only be sassy in person, don't leave written evidence
27. If you leave something until the last minute it only takes a minute
28. Give your files sensible names
29. Don't rely on collaborators
30. If it's important it's worth a second email
31. Your supervisor isn't always right
32. If it is stupid but it works, it isn't stupid
33. Don't fix what ain't broke
34. Don't update software unless you have to
35. Publications don't fairly represent the number of failed attempts
36. Try not to be over ambitious i.e. 100 is a big number
37. Don't ask questions that are "more of a comment, really"
38. The poster title *is* the abstract
39. "Everything not saved will be lost" - Nintendo "Quit Screen"
40. Dolly Parton didn't specify *which* 9 to 5 i.e. working hours are flexible
41. The best way to find a typo is to click submit
42. Your family won't understand what your PhD is about no matter how many times you try
43. Finish first, perfect later
44. It's never going to be perfect
45. Someone's lack of provisions during their PhD doesn't excuse your lack of provisions
46. Do something badly enough once and no one will ask you to do it again
47. Always tell someone the deadline is earlier than it actually is
48. Original doesn't mean good
49. Tradition is a terrible reason to do something
50. Always save the data, not just a plot

51. Start saving early for when you run out of funding
52. It’s important to admit when you don’t know or understand something
53. Remember it’s not your money when buying something
54. Make sure to spend all of your travel budget
55. Free food tastes better
56. It’s never too early to start writing your thesis
57. Don’t compare yourself to others
58. Save plots as vector images
59. Don’t expect anything to work the first time
60. Find something positive to say when giving feedback
61. Simple doesn’t mean easy
62. Bodge jobs don’t save time in the long run
63. Your postdoc is your real supervisor
64. Keep up with a hobby
65. Experiments on a Friday never work, best not to bother
66. Don’t volunteer information to the safety officer about that stupid thing you did
67. Be nice to fellow PhD students, they’ll be reviewing your future papers
68. Never half-ass two things, whole-ass one thing
69. Get over your fear of asking stupid questions
70. Learn to code sooner rather than later
71. For the love of God, put useful comments in your code
72. Sometimes working on weekends is necessary
73. Writing a thesis takes longer than you think
74. “A picture is worth a thousand words” doesn’t apply to your thesis word count
75. Prioritise work that you can actually write about in your thesis

76. Your thesis is as much for you as it is for your examiners
77. No one is going to do it for you
78. Learn when to take a break
79. "How's writing going?" never gets less annoying
80. The stages of thesis writing are surprisingly similar to those of grief
81. Don't work in your office if you want to get work done
82. 80% of a talk should be motivation
83. Tell 'em what you're going to say, then tell 'em, then tell 'em what you told 'em
84. Don't expect your supervisor to make your life easier
85. It isn't unusual for you to know more than your supervisor
86. It only has to be 'good enough'
87. Always write the abstract last
88. Have your viva in the afternoon so that your external has to leave to travel back
89. There is a fine line between writing a background chapter and plagiarism
90. Check your figures in black and white
91. It is quite alright to admit that you were wrong
92. Nothing will ever feel finished
93. "The best thesis defence is a good thesis offence" [199]
94. Remember to label the label maker first
95. A good way to be more productive is to lower your standards
96. Lent equipment has a tendency to disappear
97. You don't finish a thesis, you abandon it
98. Don't waste time writing a list of 100 tips
99. You should be writing your thesis now instead of reading this
100. The only way to find out how to do a PhD is to do one. Therefore, all advice is useless [200]

Bibliography

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, (Washington, DC, USA), pp. 124–134, IEEE Computer Society, 1994. Cited on pages 3, 17, 20, 27, 49, and 87.

[2] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019. Cited on pages 3, 20, and 27.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. Cited on pages 3, 29, 49, and 87.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991. Cited on pages 3, 31, 49, and 87.

[5] F. Xu, X. M. Q. Zhang, H.-K. Lo, and J.-W. Pan, "Quantum cryptography with realistic devices," 2019. arXiv:1903.09051. Cited on pages 3 and 34.

[6] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98, (Washington, DC, USA), pp. 503–, IEEE Computer Society, 1998. Cited on pages 3, 34, and 88.

[7] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012. Cited on pages 3, 35, 49, 88, and 89.

[8] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," *Nature Photonics*, pp. 1–12, 2019. Cited on pages 3, 42, 119, and 127.

[9] 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," *Nature Communications*, vol. 8, p. 13984, Feb 2017. Cited on pages 3, 41, 50, 60, 62, 87, 89, 116, 119, 128, and 149.

[10] S. Singh, *The Code Book*, vol. 7. Doubleday New York, 1999. Cited on page 9.

[11] Herodotus, *Histories Terpsichore (Book V)*. c. 440 BC. Cited on page 10.

[12] A. of Naucratis, *The Deipnosophistae (Books I-X)*, vol. Vol. I-IV. c. 3rd century AD. Translations provided by C. B. Gulick, Harvard University Press, 1927. Cited on page 10.

[13] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 5–83, January 1883. Cited on page 10.

[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949. Cited on pages 10 and 15.

[15] G. S. Tranquillus, *The Twelve Caesars*. 121. Cited on page 11.

[16] G. Belaso, "La cifra del sig. Giovan Battista Bellaso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima brevità et perfettione." Cited on page 13.

[17] B. d. Vigenère, "Traité des chiffres, ou secrètes manières d'écrire par Blaise de vigenère, Bourbonnais," 1586. Cited on page 13.

[18] F. Miller, *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. CM Cornwell, 1882. Cited on page 14.

[19] G. S. Vernam, "Secret signaling system," 1919. United States Patent 1310719A. Cited on page 14.

[20] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *Journal of the AIEE*, vol. 45, no. 2, pp. 109–115, 1926. Cited on page 14.

[21] H. Feistel, *Cryptographic coding for data-bank privacy*. IBM Thomas J. Watson Research Center, 1970. Cited on page 15.

[22] National Institute of Standards and Technology (NIST), "Data encryption standard (DES)," *Federal Information Processing Standards Publication 46*, 1977. Cited on page 16.

[23] W. Diffie and M. E. Hellman, "Special feature exhaustive cryptanalysis of the NBS data encryption standard," *Computer*, vol. 10, pp. 74–84, June 1977. Cited on page 16.

[24] National Institute of Standards and Technology (NIST), "Specification for the advances encryption standard (AES)," 2001. Cited on page 16.

[25] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. Cited on page 17.

[26] J. H. Ellis, "The possibility of secure non-secret digital encryption," *Communications-Electronic Security Group Research Report*, January 1970. Cited on page 17.

[27] M. J. Williamson, "Non-secret encryption using a finite field," *Communications-Electronic Security Group Research Report*, January 1974. Cited on page 17.

[28] 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. Cited on page 18.

[29] C. C. Cocks, "A note on 'non-secret' encryption," *Communications-Electronic Security Group Research Report*, November 1973. Cited on page 18.

[30] S. Goldwasser and S. Micali, "Probabilistic encryption & how to play mental poker keeping secret all partial information," in *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pp. 365–377, ACM, 1982. Cited on page 19.

[31] G. Alagic, J. M. Alperin-Sheriff, D. C. Apon, D. A. Cooper, Q. H. Dang, C. A. Miller, D. Moody, R. C. Peralta, R. A. Perlner, A. Y. Robinson, D. C. Smith-Tone, and Y.-K. Liu, *Status report on the first round of the NIST post-quantum cryptography standardization process*. US Department of Commerce, National Institute of Standards and Technology, 2019. Cited on page 20.

[32] L. Eldar and P. W. Shor, "An efficient quantum algorithm for a variant of the closest lattice-vector problem," *arXiv:1611.06999*, 2016. Cited on page 20.

[33] A. Zimmermann, "Zimmermann telegram," January 1917. Cited on page 21.

[34] A. Hodges, *Alan Turing: The Enigma*. Random House, 2012. Cited on page 21.

[35] Y. Manin, "Computable and uncomputable," *Sovetskoye Radio, Moscow*, vol. 128, 1980. Cited on page 21.

[36] R. P. Feynman, "Simulating physics with computers," *International journal of theoretical physics*, vol. 21, no. 6, pp. 467–488, 1982. Cited on page 21.

[37] 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. Cited on page 25.

[38] E. Schrödinger, "Discussion of probability relations between separated systems," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, pp. 555–563, Cambridge University Press, 1935. Cited on page 25.

[39] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964. Cited on pages 25 and 31.

[40] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969. Cited on pages 25 and 31.

[41] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of Bell's theorem with entangled photons," *Phys. Rev. Lett.*, vol. 115, p. 250401, Dec 2015. Cited on pages 25, 34, and 88.

[42] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism," *Phys. Rev. Lett.*, vol. 115, p. 250402, Dec 2015. Cited on pages 25, 34, and 88.

[43] 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. Cited on pages 25, 34, and 88.

[44] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018. Cited on page 27.

[45] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, p. 032324, 2012. Cited on page 27.

[46] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," 2019. arXiv:1905.09749. Cited on page 27.

[47] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. D. Ladd, and Y. Yamamoto, "Layered architecture for quantum computing," *Phys. Rev. X*, vol. 2, p. 031007, Jul 2012. Cited on page 27.

[48] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, (New York, NY, USA), pp. 212–219, ACM, 1996. Cited on page 27.

[49] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997. Cited on page 27.

[50] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, pp. 78–88, Jan. 1983. Cited on page 27.

[51] 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. Cited on page 29.

[52] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," 2019. arXiv:1906.01645. Cited on pages 29 and 34.

[53] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, Feb 2004. Cited on page 29.

[54] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, p. 037902, Jun 2002. Cited on pages 29 and 33.

[55] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005. Cited on pages 29 and 33.

[56] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992. Cited on page 29.

[57] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr 2000. Cited on pages 30 and 34.

[58] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug 2000. Cited on pages 30 and 34.

[59] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, Jun 2005. Cited on pages 30, 50, and 93.

[60] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, p. 136, IEEE, 2004. Cited on page 31.

[61] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018. Cited on page 32.

[62] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, p. 010303, Dec 1999. Cited on pages 32 and 61.

[63] M. Hillery, "Quantum cryptography with squeezed states," *Phys. Rev. A*, vol. 61, p. 022309, Jan 2000. Cited on page 32.

[64] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature photonics*, vol. 7, no. 5, p. 378, 2013. Cited on page 32.

[65] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, p. 070501, Feb 2015. Cited on page 33.

[66] A. Leverrier, "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction," *Phys. Rev. Lett.*, vol. 118, p. 200501, May 2017. Cited on page 33.

[67] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, p. 16025, 2016. Cited on page 33.

[68] D. Genkin, A. Shamir, and E. Tromer, "Rsa key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology – CRYPTO 2014* (J. A. Garay and R. Gennaro, eds.), (Berlin, Heidelberg), pp. 444–461, Springer Berlin Heidelberg, 2014. Cited on page 33.

[69] G. Brassard, “Brief history of quantum cryptography: a personal perspective,” in *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pp. 19–23, Oct 2005. Cited on page 33.

[70] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, “Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses,” *npj Quantum Information*, vol. 4, no. 1, p. 8, 2018. Cited on page 34.

[71] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems,” *Phys. Rev. A*, vol. 73, p. 022320, Feb 2006. Cited on pages 34 and 49.

[72] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, “Trojan-horse attacks threaten the security of practical quantum cryptography,” *New Journal of Physics*, vol. 16, no. 12, p. 123030, 2014. Cited on page 34.

[73] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, “Invisible trojan-horse attack,” *Scientific reports*, vol. 7, no. 1, p. 8403, 2017. Cited on page 34.

[74] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, “Time-shift attack in practical quantum cryptosystems,” *Quantum Info. Comput.*, vol. 7, pp. 73–82, Jan. 2007. Cited on page 34.

[75] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” *Phys. Rev. A*, vol. 78, p. 042333, Oct 2008. Cited on pages 34 and 49.

[76] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Thermal blinding of gated detectors in quantum cryptography,” *Opt. Express*, vol. 18, pp. 27938–27954, Dec 2010. Cited on page 34.

[77] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system,” *Nature communications*, vol. 2, p. 349, 2011. Cited on page 34.

[78] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography,” *Phys. Rev. Lett.*, vol. 112, p. 070503, Feb 2014. Cited on page 34.

[79] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, “Creation of backdoors in quantum communications via laser damage,” *Phys. Rev. A*, vol. 94, p. 030302, Sep 2016. Cited on page 34.

[80] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, Aug 2006. Cited on pages 34 and 49.

[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, p. 686, 2010. Cited on pages 34, 49, and 88.

[82] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New Journal of Physics*, vol. 13, p. 113042, nov 2011. Cited on page 34.

[83] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light," *Opt. Express*, vol. 19, pp. 23590–23600, Nov 2011. Cited on page 34.

[84] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, p. 065003, jun 2009. Cited on page 34.

[85] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, p. 013043, jan 2011. Cited on page 34.

[86] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Avoiding the blinding attack in QKD," *Nature Photonics*, vol. 4, no. 12, p. 801, 2010. Cited on page 34.

[87] Z. Yuan, J. Dynes, and A. Shields, "Avoiding the blinding attack in QKD," *Nature Photonics*, vol. 4, no. 12, p. 800, 2010. Cited on page 34.

[88] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical security bounds against the trojan-horse attack in quantum key distribution," *Phys. Rev. X*, vol. 5, p. 031030, Sep 2015. Cited on pages 34 and 88.

[89] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun 2007. Cited on page 34.

[90] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," *Phys. Rev. Lett.*, vol. 95, p. 010503, Jun 2005. Cited on page 34.

[91] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, no. 4, p. 045021, 2009. Cited on page 34.

[92] S. E. Miller, "Integrated optics: An introduction," *The Bell System Technical Journal*, vol. 48, no. 7, pp. 2059–2069, 1969. Cited on page 35.

[93] C. Gerry, P. Knight, and P. L. Knight, *Introductory Quantum Optics*. Cambridge university press, 2005. Cited on page 35.

[94] M. Fox, *Quantum Optics: An Introduction*, vol. 15. OUP Oxford, 2006. Cited on page 35.

[95] R. Loudon, *The Quantum Theory of Light*. OUP Oxford, 2000. Cited on page 35.

[96] E. Schrödinger, "Der stetige übergang von der mikro- zur makromechanik," *Naturwissenschaften*, vol. 14, pp. 664–666, Jul 1926. Cited on page 36.

[97] M. Smit, X. Leijtens, H. Ambrosius, E. Bente, J. van der Tol, B. Smalbrugge, T. de Vries, E.-J. Geluk, J. Bolk, R. van Veldhoven, L. Augustin, P. Thijs, D. D'Agostino, H. Rabbani, K. Lawniczuk, S. Stopinski, S. Tahvili, A. Corradi, E. Kleijn, D. Dzibrou, M. Felicetti, E. Bitincka, V. Moskalenko, J. Zhao, R. Santos, G. Gilardi, W. Yao, K. Williams, P. Stabile, P. Kuindersma, J. Pello, S. Bhat, Y. Jiao, D. Heiss, G. Roelkens, M. Wale, P. Firth, F. Soares, N. Grote, M. Schell, H. Debregeas, M. Achouche, J.-L. Gentner, A. Bakker, T. Korthorst, D. Gallagher, A. Dabbs, A. Melloni, F. Morichetti, D. Melati, A. Wonfor, R. Penty, R. Broeke, B. Musk, and D. Robbins, "An introduction to InP-based generic integration technology," *Semiconductor Science and Technology*, vol. 29, p. 083001, jun 2014. Cited on pages 37, 41, 43, 50, 63, and 65.

[98] G. Lifante, *Integrated Photonics: Fundamentals*. Wiley Online Library, 2003. Cited on page 38.

[99] L. B. Soldano and E. C. Pennings, "Optical multi-mode interference devices based on self-imaging: principles and applications," *Journal of lightwave technology*, vol. 13, no. 4, pp. 615–627, 1995. Cited on page 39.

[100] L. A. Eldada, "Advances in telecom and datacom optical components," *Optical Engineering*, vol. 40, no. 7, pp. 1165 – 1178, 2001. Cited on pages 41 and 44.

[101] A. Kanno, T. Sakamoto, A. Chiba, T. Kawanishi, K. Higuma, M. Sudou, and J. Ichikawa, "120-Gb/s NRZ-DQPSK signal generation by a thin-lithium-niobate-substrate modulator," *IEICE Electronics Express*, vol. 7, no. 11, pp. 817–822, 2010. Cited on pages 41 and 44.

[102] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," *Optica*, vol. 4, pp. 172–177, Feb 2017. Cited on pages 41 and 149.

[103] H. Semenenko, P. Sibson, M. G. Thompson, and C. Erven, "Integrated photonic devices for measurement-device-independent quantum key distribution," in *CLEO:*

QELS_Fundamental Science, pp. FM4C–4, Optical Society of America, 2019. Cited on pages 41 and 87.

[104] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, "Chip-based measurement-device-independent quantum key distribution," 2019. arXiv:1908.08745. Cited on pages 41, 87, and 149.

[105] H. Semenenko, P. Sibson, M. G. Thompson, and C. Erven, "Interference between independent photonic integrated devices for quantum key distribution," *Optics letters*, vol. 44, no. 2, pp. 275–278, 2019. Cited on pages 41 and 49.

[106] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature photonics*, vol. 3, no. 12, p. 696, 2009. Cited on pages 42 and 107.

[107] 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. Cited on page 42.

[108] N. J. D. Martinez, M. Gehl, C. T. Derose, A. L. Starbuck, A. T. Pomerene, A. L. Lentine, D. C. Trotter, and P. S. Davids, "Single photon detection in a waveguide-coupled Ge-on-Si lateral avalanche photodiode," *Opt. Express*, vol. 25, pp. 16130–16139, Jul 2017. Cited on page 42.

[109] P. Vines, K. Kuzmenko, J. Kirdoda, D. C. Dumas, M. M. Mirza, R. W. Millar, D. J. Paul, and G. S. Buller, "High performance planar germanium-on-silicon single-photon avalanche diode detectors," *Nature communications*, vol. 10, no. 1, p. 1086, 2019. Cited on page 42.

[110] E. E. Wollman, V. B. Verma, A. D. Beyer, R. M. Briggs, B. Korzh, J. P. Allmaras, F. Marsili, A. E. Lita, R. P. Mirin, S. W. Nam, and M. D. Shaw, "UV superconducting nanowire single-photon detectors with high efficiency, low noise, and 4 k operating temperature," *Opt. Express*, vol. 25, pp. 26792–26801, Oct 2017. Cited on pages 42 and 91.

[111] J. P. 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. Cited on pages 42, 94, 97, and 118.

[112] A. Vetter, S. Ferrari, P. Rath, R. Alaee, O. Kahl, V. Kovalyuk, S. Diewald, G. N. Goltsman, A. Korneev, C. Rockstuhl, and W. H. P. Pernice, "Cavity-enhanced and ultrafast superconducting single-photon detectors," *Nano letters*, vol. 16, no. 11, pp. 7085–7092, 2016. Cited on pages 42, 97, and 107.

[113] Y. Yun, A. Vetter, R. Stegmueller, S. Ferrari, W. H. Pernice, C. Rockstuhl, and C. Lee, "Superconducting nanowire single-photon spectrometer exploiting cascaded photonic crystal cavities," *arXiv:1908.01681*, 2019. Cited on pages 42, 97, and 107.

[114] N. A. Tyler, J. Barreto, G. E. Villarreal-Garcia, D. Bonneau, D. Sahin, J. L. O'Brien, and M. G. Thompson, "Modelling superconducting nanowire single photon detectors in a waveguide cavity," *Optics express*, vol. 24, no. 8, pp. 8797–8808, 2016. Cited on page 42.

[115] M. Cazzanelli and J. Schilling, "Second order optical nonlinearity in silicon by symmetry breaking," *Applied Physics Reviews*, vol. 3, no. 1, p. 011104, 2016. Cited on page 43.

[116] C. Castellan, A. Trenti, C. Vecchi, A. Marchesini, M. Mancinelli, M. Ghulinyan, G. Pucker, and L. Pavesi, "On the origin of second harmonic generation in silicon waveguides with silicon nitride cladding," *Scientific reports*, vol. 9, no. 1, p. 1088, 2019. Cited on page 43.

[117] J. W. Silverstone, *Entangled light in silicon waveguides*. PhD thesis, University of Bristol, 7 2015. Cited on page 43.

[118] Y. Fan, R. M. Oldenbeuving, C. G. Roeloffzen, M. Hoekman, D. Geskus, R. G. Heideman, and K.-J. Boller, "290 Hz intrinsic linewidth from an integrated optical chip-based widely tunable InP-Si3N4 hybrid laser," in *Conference on Lasers and Electro-Optics*, p. JTh5C.9, Optical Society of America, 2017. Cited on page 43.

[119] C. Agnesi, B. D. Lio, D. Cozzolino, L. Cardi, B. B. Bakir, K. Hassan, A. D. Frera, A. Ruggeri, A. Giudice, G. Vallone, P. Villoresi, A. Tosi, K. Rottwitt, Y. Ding, and D. Bacco, "Hong-Ou-Mandel interference between independent III-V on silicon waveguide integrated lasers," *Opt. Lett.*, vol. 44, pp. 271–274, Jan 2019. Cited on pages 43, 59, and 80.

[120] F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. Matthews, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," *Optics express*, vol. 26, no. 16, pp. 19730–19741, 2018. Cited on pages 43, 116, and 143.

[121] J. Notaros, F. Pavanello, M. T. Wade, C. M. Gentry, A. Atabaki, L. Alloatti, R. J. Ram, and M. A. Popović, "Ultra-efficient cmos fiber-to-chip grating couplers," in *Optical Fiber Communication Conference*, p. M2I.5, Optical Society of America, 2016. Cited on pages 43 and 120.

[122] L. M. Rosenfeld, D. A. Sulway, G. F. Sinclair, V. Anant, M. G. Thompson, J. G. Rarity, and J. W. Silverstone, "Mid-infrared quantum optics in silicon," *arXiv:1906.10158*, 2019. Cited on pages 43 and 44.

[123] D. Tan, K. Ooi, and D. Ng, "Nonlinear optics on silicon-rich nitride—a high nonlinear figure of merit CMOS platform," *Photonics Research*, vol. 6, no. 5, pp. B50–B66, 2018. Cited on page 43.

[124] X. Lu, Q. Li, D. A. Westly, G. Moille, A. Singh, V. Anant, and K. Srinivasan, "Chip-integrated visible–telecom entangled photon pair source for quantum communication," *Nature Physics*, vol. 15, no. 4, p. 373, 2019. Cited on page 43.

[125] JePPIX, "JePPIX Roadmap 2018." https://www.jeppix.eu/vision/. Cited on pages 43, 50, 98, and 144.

[126] J. van der Tol, Y. Jiao, and K. Williams, *InP photonic integrated circuits on silicon*, pp. 189–219. Semiconductors and Semimetals, Netherlands: Elsevier, 9 2018. Cited on page 44.

[127] J. Van der Tol, R. Zhang, J. Pello, F. Bordas, G. Roelkens, H. Ambrosius, P. Thijs, F. Karouta, and M. Smit, "Photonic integration in indium-phosphide membranes on silicon," *IET optoelectronics*, vol. 5, no. 5, pp. 218–225, 2011. Cited on page 44.

[128] R. R. Kumar, M. Raevskaia, V. Pogoretskii, Y. Jiao, and H. K. Tsang, "Entangled photon pair generation from an InP membrane micro-ring resonator," *Applied Physics Letters*, vol. 114, no. 2, p. 021104, 2019. Cited on pages 44 and 98.

[129] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. DeMicheli, D. B. Ostrowsky, and N. Gisin, "PPLN waveguide for quantum communication," *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, vol. 18, no. 2, pp. 155–160, 2002. Cited on page 44.

[130] H. Jin, F. Liu, P. Xu, J. Xia, M. Zhong, Y. Yuan, J. Zhou, Y. Gong, W. Wang, and S. Zhu, "On-chip generation and manipulation of entangled photons based on reconfigurable lithium-niobate waveguide circuits," *Physical review letters*, vol. 113, no. 10, p. 103601, 2014. Cited on page 44.

[131] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Opt. Express*, vol. 15, pp. 9388–9393, Jul 2007. Cited on page 49.

[132] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, pp. 2044–2046, Nov 1987. Cited on pages 49, 50, and 57.

[133] 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. Cited on page 49.

[134] J. G. Rarity, P. R. Tapster, and R. Loudon, "Non-classical interference between independent sources," *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 7, pp. S171–S175, jun 2005. Cited on pages 50, 52, 56, 76, and 94.

[135] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, "Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications," *Phys. Rev. Applied*, vol. 2, p. 064006, Dec 2014. Cited on page 50.

[136] 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. Cited on pages 50, 88, 94, and 96.

[137] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photonics*, vol. 10, pp. 312 – 315, Apr 2016. Cited on pages 50, 88, 96, 129, and 149.

[138] J. G. Rarity and P. R. Tapster, "Fourth-order interference in parametric downconversion," *J. Opt. Soc. Am. B*, vol. 6, pp. 1221–1226, Jun 1989. Cited on page 57.

[139] W. C. Jiang, X. Lu, J. Zhang, O. Painter, and Q. Lin, "Silicon-chip source of bright photon pairs," *Optics express*, vol. 23, no. 16, pp. 20884–20904, 2015. Cited on page 57.

[140] V. Leong, S. Kosen, B. Srivathsan, G. K. Gulati, A. Cerè, and C. Kurtsiefer, "Hong-Ou-Mandel interference between triggered and heralded single photons from separate atomic systems," *Phys. Rev. A*, vol. 91, p. 063829, Jun 2015. Cited on page 57.

[141] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaítre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart, "Near-optimal single-photon sources in the solid state," *Nature Photonics*, vol. 10, no. 5, pp. 340–345, 2016. Cited on page 57.

[142] H. Bernien, L. Childress, L. Robledo, M. Markham, D. Twitchen, and R. Hanson, "Two-photon quantum interference from separate nitrogen vacancy centers in diamond," *Phys. Rev. Lett.*, vol. 108, p. 043604, Jan 2012. Cited on page 57.

[143] Y. Chen, M. Zopf, R. Keil, F. Ding, and O. G. Schmidt, "Highly-efficient extraction of entangled photons from quantum dots using a broadband optical antenna," *Nature communications*, vol. 9, no. 1, p. 2994, 2018. Cited on page 57.

[144] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018. Cited on pages 58 and 115.

[145] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," *Opt. Express*, vol. 24, pp. 17849–17859, Aug 2016. Cited on pages 59, 128, 129, and 141.

[146] N. Ismail, C. C. Kores, D. Geskus, and M. Pollnau, "Fabry-Pérot resonator: spectral line shapes, generic and related airy distributions, linewidths, finesses, and performance at low or frequency-dependent reflectivity," *Opt. Express*, vol. 24, pp. 16366–16389, Jul 2016. Cited on page 61.

[147] T. Okoshi, K. Kikuchi, and A. Nakayama, "Novel method for high resolution measurement of laser output spectrum," *Electronics Letters*, vol. 16, pp. 630–631, July 1980. Cited on page 62.

[148] D. A. B. Miller, D. S. Chemla, T. C. Damen, A. C. Gossard, W. Wiegmann, T. H. Wood, and C. A. Burrus, "Band-edge electroabsorption in quantum well structures: The quantum-confined Stark effect," *Phys. Rev. Lett.*, vol. 53, pp. 2173–2176, Nov 1984. Cited on pages 63 and 65.

[149] D. C. Hutchings, M. Sheik-Bahae, D. J. Hagan, and E. W. Van Stryland, "Kramers-Krönig relations in nonlinear optics," *Optical and Quantum Electronics*, vol. 24, pp. 1–30, Jan 1992. Cited on page 64.

[150] 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. Cited on page 64.

[151] B. C. Wadell, *Transmission line design handbook*. Artech House, 1991. Cited on page 69.

[152] M. Riaziat, I. Feng, R. Majidi-Ahy, and B. Auld, "Single-mode operation of coplanar waveguides," *Electronics letters*, vol. 23, no. 24, pp. 1281–1283, 1987. Cited on page 70.

[153] A. B. Price, P. Sibson, C. Erven, J. G. Rarity, and M. G. Thompson, "High-speed quantum key distribution with wavelength-division multiplexing on integrated photonic devices," in *Conference on Lasers and Electro-Optics*, p. JTh2A.24, Optical Society of America, 2018. Cited on pages 82 and 119.

[154] M. K. Akhlaghi, E. Schelew, and J. F. Young, "Waveguide integrated superconducting single-photon detectors implemented as near-perfect absorbers of coherent radiation," *Nature communications*, vol. 6, p. 8233, 2015. Cited on page 82.

[155] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio,

H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, "Entanglement distribution over a 96-km-long submarine optical fiber," *Proceedings of the National Academy of Sciences*, vol. 116, no. 14, pp. 6684–6688, 2019. Cited on page 82.

[156] A. Vaquero-Stainer, R. Kirkwood, V. Burenkov, C. Chunnilall, A. Sinclair, A. Hart, H. Semenenko, P. Sibson, C. Erven, and M. Thompson, "Measurements towards providing security assurance for a chip-scale qkd system," in *Quantum Technologies 2018*, vol. 10674, p. 106741A, International Society for Optics and Photonics, 2018. Cited on pages 87, 117, and 119.

[157] 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. Cited on page 87.

[158] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, p. 190501, Nov 2016. Cited on pages 88, 89, and 90.

[159] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: challenges and solutions," *Optics express*, vol. 26, no. 18, pp. 24260–24273, 2018. Cited on page 88.

[160] Some examples of commercial entities developing QKD systems are ID Quantique, KETS Quantum Security, MagiQ Technologies, QuintessenceLabs and Toshiba. Cited on page 88.

[161] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595 – 604, Jul 2014. Cited on pages 88 and 93.

[162] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," *New Journal of Physics*, vol. 13, no. 11, p. 113042, 2011. Cited on page 88.

[163] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature communications*, vol. 2, p. 238, 2011. Cited on page 88.

[164] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Phys. Rev. A*, vol. 93, p. 042324, Apr 2016. Cited on pages 89, 94, and 115.

[165] S. Walborn, W. Nogueira, S. Pádua, and C. Monken, "Optical Bell-state analysis in the coincidence basis," *EPL (Europhysics Letters)*, vol. 62, no. 2, p. 161, 2003. Cited on pages 90, 92, and 95.

[166] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," *Phys. Rev. Lett.*, vol. 76, pp. 4656–4659, Jun 1996. Cited on pages 90, 92, and 95.

[167] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, p. 190502, Nov 2018. Cited on page 91.

[168] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, Aug 2003. Cited on page 93.

[169] W. Wang, F. Xu, and H.-K. Lo, "Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks," *Phys. Rev. X*, vol. 9, p. 041012, Oct 2019. Cited on pages 94 and 115.

[170] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii, and T. Hasegawa, "The first 0.14-dB/km loss optical fiber and its impact on submarine transmission," *Journal of Lightwave Technology*, vol. 36, no. 1, pp. 44–49, 2018. Cited on page 95.

[171] "SMF-28® ULL optical fiber." https://www.corning.com/worldwide/en/products/communication-networks/products/fiber/smf-28-ull.html. Accessed: 2019/09/16. Cited on page 95.

[172] "Polatis Series 6000." https://www.polatis.com/polatis-series-6000-optical-matrix-switch-192x192-sdn-enabled-industry-leading-performace-lowest-loss-switches.asp. Accessed: 2019/09/16. Cited on page 97.

[173] F. Eltes, G. E. Villarreal-Garcia, D. Caimi, H. Siegwart, A. A. Gentile, A. Hart, P. Stark, G. D. Marshall, M. G. Thompson, J. Barreto, J. Fompeyrine, and S. Abel, "An integrated cryogenic optical modulator," *arXiv:1904.10902*, 2019. Cited on pages 97 and 119.

[174] A. Sugita, A. Kaneko, K. Okamoto, M. Itoh, A. Himeno, and Y. Ohmori, "Very low insertion loss arrayed-waveguide grating with vertically tapered waveguides," *IEEE Photonics Technology Letters*, vol. 12, no. 9, pp. 1180–1182, 2000. Cited on pages 97 and 118.

[175] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, "Modeling a measurement-device-independent quantum key distribution system," *Opt. Express*, vol. 22, pp. 12716–12736, Jun 2014. Cited on page 102.

[176] 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, pp. 407–413, Apr 2016. Cited on page 107.

[177] C. Abellan, W. Amaya, D. Domenech, P. M. noz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an InP photonic integrated circuit for random number generation," *Optica*, vol. 3, pp. 989–994, Sep 2016. Cited on page 116.

[178] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, p. 015004, Feb 2017. Cited on pages 116 and 143.

[179] A. Huang, Álvaro Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser seeding attack in quantum key distribution," 2019. arXiv:1902.09792. Cited on page 117.

[180] "ETSI - quantum key distribution | quantum cryptography." https://www.etsi.org/technologies/quantum-key-distribution. Accessed: 2019/11/03. Cited on page 118.

[181] C.-Y. Wang, J. Gao, Z.-Q. Jiao, L.-F. Qiao, R.-J. Ren, Z. Feng, Y. Chen, Z.-Q. Yan, Y. Wang, H. Tang, and X.-M. Jin, "Integrated measurement server for measurement-device-independent quantum key distribution network," *Opt. Express*, vol. 27, pp. 5982–5989, Mar 2019. Cited on page 118.

[182] Dong-Sun Seo, D. Y. Kim, and Hai-Feng Liu, "Timing jitter reduction of gain-switched DFB laser by external injection-seeding," *Electronics Letters*, vol. 32, pp. 44–45, Jan 1996. Cited on pages 128 and 141.

[183] P. Gunning, J. K. Lucek, D. G. Moodie, K. Smith, R. P. Davey, S. V. Chernikov, M. J. Guy, J. R. Taylor, and A. S. Siddiqui, "Gainswitched DFB laser diode pulse source using continuous wave light injection for jitter suppression and an electroabsorption modulator for pedestal suppression," *Electronics Letters*, vol. 32, pp. 1010–1011, May 1996. Cited on pages 128 and 141.

[184] T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," *npj Quantum Information*, vol. 5, no. 1, p. 42, 2019. Cited on pages 130 and 141.

[185] W. H. Haydl, "On the use of vias in conductor-backed coplanar circuits," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 6, pp. 1571–1577, 2002. Cited on page 132.

[186] A. Sain and K. L. Melde, "Impact of ground via placement in grounded coplanar waveguide interconnects," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 6, pp. 136–144, Jan 2016. Cited on page 133.

[187] G. Chen, Y. Yu, S. Deng, L. Liu, and X. Zhang, "Bandwidth improvement for germanium photodetector using wire bonding technology," *Optics express*, vol. 23, no. 20, pp. 25700–25706, 2015. Cited on page 135.

[188] S. S. Cahill, E. A. Sanjuan, and L. Levine, "Development of 100+ GHz high-frequency microcoax wire bonds," in *Proc. of the Int. Symp. On Microelect*, p. 668, 2006. Cited on page 135.

[189] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, "Weak randomness seriously limits the security of quantum key distribution," *Phys. Rev. A*, vol. 86, p. 062308, Dec 2012. Cited on page 143.

[190] H.-W. Li, Z.-Q. Yin, S. Wang, Y.-J. Qian, W. Chen, G.-C. Guo, and Z.-F. Han, "Randomness determines practical security of BB84 quantum key distribution," *Scientific reports*, vol. 5, p. 16200, 2015. Cited on page 143.

[191] 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. Cited on page 143.

[192] 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, p. 711, 2010. Cited on page 143.

[193] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation," *Review of Scientific Instruments*, vol. 90, no. 4, p. 043105, 2019. Cited on page 143.

[194] 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. Cited on page 143.

[195] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nature Photonics*, vol. 13, no. 12, pp. 839–842, 2019. Cited on page 149.

[196] C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," *Optica*, vol. 3, no. 11, pp. 1274–1278, 2016. Cited on page 149.

[197] D. Hofstadter, *Gödel, Escher, Bach*. Basic Books, 1979. Cited on page 165.

[198] J. Langford and P. R. Clance, “The imposter phenomenon: recent research findings regarding dynamics, personality and family patterns and their implications for treatment.,” *Psychotherapy: Theory, Research, Practice, Training*, vol. 30, no. 3, p. 495, 1993. Cited on page 165.

[199] “Thesis Defence.” https://xkcd.com/1403/. Accessed: 2019/12/04. Cited on page 168.

[200] “I did a PhD and did NOT go mad.” http://www.richardbutterworth.co.uk/blog/13-i-did-a-phd. Accessed: 2019-08-04. Cited on page 168.