# Experimental Advances in Broadband Continuous Variable Quantum Key Distribution

**Timothy J. Williams, BSc**

**A thesis submitted for the degree of**
**Bachelor of Science with Honours in Physics of**
**The Australian National University**

**May, 2006**

# Declaration

This thesis is an account of research undertaken between May 2005 and May 2006 at The Department of Physics, Faculty of Science, The Australian National University, Canberra, Australia. Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university.

Timothy J. Williams
May, 2006

# Acknowledgements

Throughout this thesis "we" should be taken to mean Dr Thomas Symul and myself. Thomas has been invaluable to me and this project as mentor and lab partner. From him I learnt (or relearnt as the case may be) the majority of techniques needed to build a quantum optics experiment. Over nine months of, at times, intensive laboratory work I can only recall one occasion where he taught me a technique that was not optimal... in the face of such a ratio I can't hold a grudge for losing three weeks doing beam-profiling the really, really long way! Thanks for all your help, Thomas.

I also thank James Dickson for assisting with the experiment electronics. His advice on PID and elliptic filter design, and his practical help with the high-speed photodetectors was greatly appreciated. The Departmental electronics and machine workshops built crucial electronics, mounts, and of course the mode cleaner. In particular I thank Shane Grieves, Paul McNamara and Paul Tant for their help during my various liaison visits.

Andrew Lance, as the builder of the first CVQKD-SQM experiment, offered invaluable advice and insight into my problems. I wish him all the best as he takes up a post-doctoral position with 'the competition' in Orsey. Thanks also to Vikram Sharma for aiding my understanding of the various available secret key distillation protocols. Lastly of the major contributors, I thank my supervisor Ping Koy Lam for motivating and planning this project, guiding its overall direction and keeping my enthusiasm up through its continuous problems.

The mode cleaner design drawings were made by Kirk McKenzie, who also aided me on one particular associated problem in the laboratory. I thank Nicolai Grosse for aiding my initial understanding of quantum optics and for his contributions during team meetings. Others working in Room 176 who also provided me with occasional (but timely) advice were Christian Weedbrook, Katie Pilypas, Vincent DeLaubert, Magnus Hsu and Gabriel Hetet. And thanks again to the cryptography team for proof-reading the thesis. On the administration side I thank Sharon Lopez, Huma Cheema and Damien Hughes for the various tasks they performed on my behalf. Finally, I thank the numerous scientists, mathematicians and engineers around the world on whose work, cited herein, this project has its foundations.

This project was supported by the Australian Government Department of Defence.

# Abstract

Quantum key distribution is the first major area of quantum information science to find practical use outside of its field. Quantum key distribution involves transmitting cryptographic keys using quantum states. Any attempt to eavesdrop on the transmission will, necessarily by the laws of quantum mechanics, disturb or destroy the states. By identifying and only using keys that have not been disturbed, a perfectly secure cryptographic system can be realised.

Discrete variable quantum key distribution was proposed in 1984. Since then attempts to exploit this technology have been beset with the difficulties of working with the discrete variables in question—single photon states. In the late 90's the idea of continuous variable quantum key distribution was developed, in which the key-carrying quantum information states are properties of a bright, continuous wave laser beam. Bright laser beams are relatively simple to manipulate and can carry large amounts of information even when subject to high loss. 'Broadband' continuous variable quantum key distribution refers to the large information rates obtainable by using broad laser modulation sidebands.

In 2005 the ANU Quantum Optics group published an experimental demonstration of broadband continuous variable quantum key distribution. This thesis documents the project work undertaken to rebuild an improved version of this experiment, and also the work undertaken to prepare for more advanced experiments. The main goal of the improved experiment was to increase the key distribution rate, while the advanced experiments were directed towards practical implementation of the system in optical fibre.

The experiment rebuild was achieved with most improvements for higher bandwidth successfully implemented. Some improvements were unplanned, being necessitated by problems with the initial improvements. Although preliminary experimental data was acquired, time constraints precluded a successful cryptographic key distribution. Pilot design and major purchasing for future experiments was also completed.

# Contents

# List of Figures

# List of Tables

Chapter 1

# Introduction

This thesis describes an experimental method of using the laws of quantum mechanics to secure information. Information security is of great importance to modern civilisation, and consequently methods of securing information have widespread application.

## 1.1 Communications Networks

There can be little doubt that a fundamental feature of civilisation is the communication of information. Through communications knowledge can be shared, authority exercised and opinion expressed. Communication is greatly facilitated by communications networks. A network consists of the communicating entities, called *nodes*, and the means by which the entities communicate, called *links* or *connections*.

A network could be as simple as a forum held in a room between people, where people use the opportunity of being face-to-face with others to communicate with them through speech. Or it could be as complex as a multi-continent distribution of computers connected together with a diverse array of communications technologies (the Internet for example). An important feature of any communications network is that a given node need not be directly connected to every other node (Fig. 1.1).

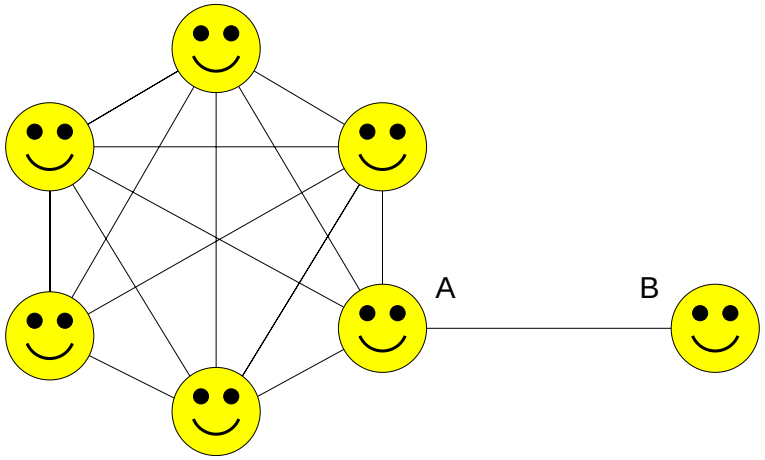


**Figure 1.1:** A communications network. All entities (nodes) have access to each other despite all not being directly connected (linked) to each other. Node B will receive information at a slower rate than the other nodes unless node A is specially equipped to relay larger amounts of information.

The advance of technology has meant that civilisation is no longer limited to face-to-

face meetings for its communications. The printing press, telephone, radio, fax, television and now personal computers provide many different networking possibilities. Heavy investments continue to be made into Internet Protocol (IP) networking. This is due to the flexibility of computers and the communications links connecting them: IP networks are capable of carrying the majority of our communications—from spoken to written words, from still to moving images.

## 1.2 Information Assurance

From the undisputed need for people to exchange information, it directly follows that nodes in a network have a critical interest in the state of the information being exchanged. How *assured* can a node be of the information it is receiving? *Information Assurance (IA)* is defined as the measure of a network's trustworthiness for carrying communications. IA can be broken into the following aspects:[21]

**Availability Assurance** that a link will be available for data transmission when needed

**Integrity Assurance** that the data a node receives is in fact the data it was sent

**Authentication Assurance** that the data a node receives from another node was actually transmitted by that node

**Confidentiality Assurance** that a private communication between one node and another will remain private

**Non-Repudiation Assurance** that a data transaction between nodes cannot later be denied by one or more of the nodes

This thesis deals largely with methods of providing confidentiality assurance to a communications network. Strong precedents of the requirement for network confidentiality can be found throughout history, and the reasons—military, security, finance, justice, privacy—are as valid today as ever. The problem of providing confidentiality is one of how to *secure* information, either single or multiple links in a network or an entire network itself (which may or may not be connected to other networks). Fig. 1.2 shows how information security can be implemented in different situations.

*Steganography*, the art of hiding information, has been used in the past to secure information. History records the story of a Greek king shaving the head of a slave, tattooing a message on his head and then dispatching him once the hair had grown back. Lemon juice can be used as 'invisible ink', as a message written with it will only become visible once the paper is heated. In World War II whole pages of information were shrunk to the size of a period (.) and incorporated into the sentences of other typed papers.

Recently there was a resurgence of interest in steganography after public suggestions that terrorists were hiding information in images posted on the Internet.[54] Steganography offers poor security, however, as once the concealment technique is known it is no longer secure. As a technique relying on stealth and subtlety the process becomes much more difficult when larger amounts of information must be secured. It is entirely unsatisfactory for securing the regular information flows found in most communications networks.

*Cryptography* offers a solution for information security. Cryptography is the art of changing information in such a way that it can only be understood by the intended recipient. A standard cryptographic process employs both a *cipher* and a *key*. The key is

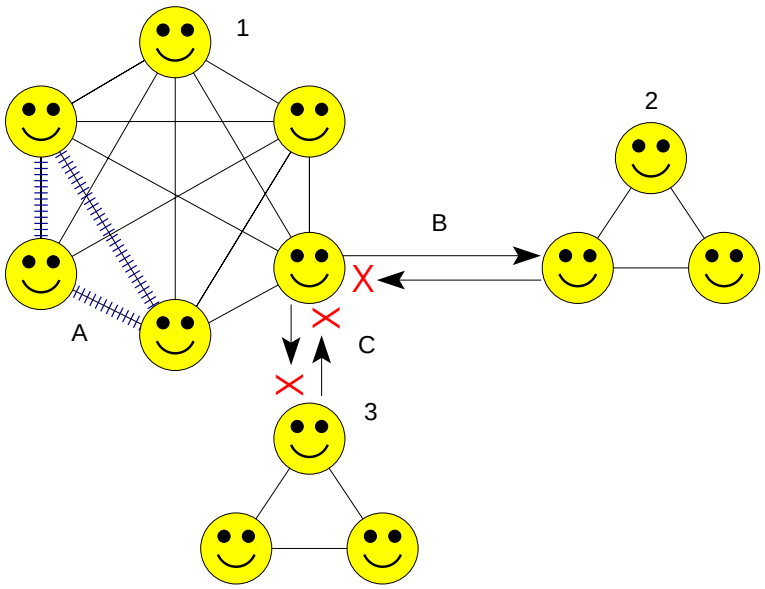


**Figure 1.2:** **A**: The hatched line represents intra-network secured links - no other node can obtain the information on these links. **B**: A 'data-diode' arrangement where information is allowed to flow from network 1 to network 2, but is secured from flowing back to network 1. **C**: Network 3 does not allow any external connections. Isolated networks like this are usually 'air-gapped' - the nodes are physically separate to other networks rather than simply being configured to disallow external connections.

applied to the message (the *plaintext*) according to the rules of the cipher, resulting in a message that is illegible to anyone but the holder of the corresponding key (the *ciphertext*). An advantage of cryptography is that the ciphertext can in general be written in the same 'alphabet' as the plaintext.

The most important example of this today is the binary language used by computer networks. Binary plaintext can be encrypted into binary ciphertext, meaning common communications technologies can be used for communicating both encrypted and unencrypted information (it will be assumed for this thesis that all cryptography systems produce ciphertext in the same alphabet as the plaintext). Cryptography is also able to contribute to the authenticity of communications (section 2.2.4). It is a good candidate for improving the IA of a communications network.

Any complete information security infrastructure should not rely solely on one particular mechanism. Cryptography is ineffective if, say, the computer screen displaying the secret information can be read through the window by casual passers-by. While this thesis describes an experimental demonstration of the most powerful type of cryptography yet discovered, it must be considered in the context of a holistic approach to information security.

## 1.3 Cryptology

Cryptography is one half of the broader field of cryptology, the other half being *cryptanalysis*—the art of revealing information protected by cryptography without the use of the key. This thesis is almost entirely concerned with building cryptographic systems, so

before turning to the mechanics of cryptography a brief discussion of its adversary is due.

Taking, for example, a simple cryptographic cipher that applies a fixed substitution for each letter in the English alphabet:

```
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
                        ⇓
Y W U S R Q A P O N L K Z J I H T G F V E D C X B M
```

Then the plaintext

```
A SECRET MESSAGE
```

will be encrypted to

```
Y FRUGRV ZRFFYAR
```

This cipher is weak since it does not change the statistical distribution of letters within the plaintext. Fig. 1.3 shows how common English communications have a characteristic statistical distribution of letters. `E` is the most common letter. Analysing the ciphertext `Y FRUGRV ZRFFYAR` reveals that `R` is the most common letter, and unsurprisingly it decrypts to `E`. Even with the spaces removed from the plaintext, it is clear that with perhaps just a few paragraphs it could be decrypted without using the key. With a computer looking for matches against a dictionary, the problem becomes trivial.

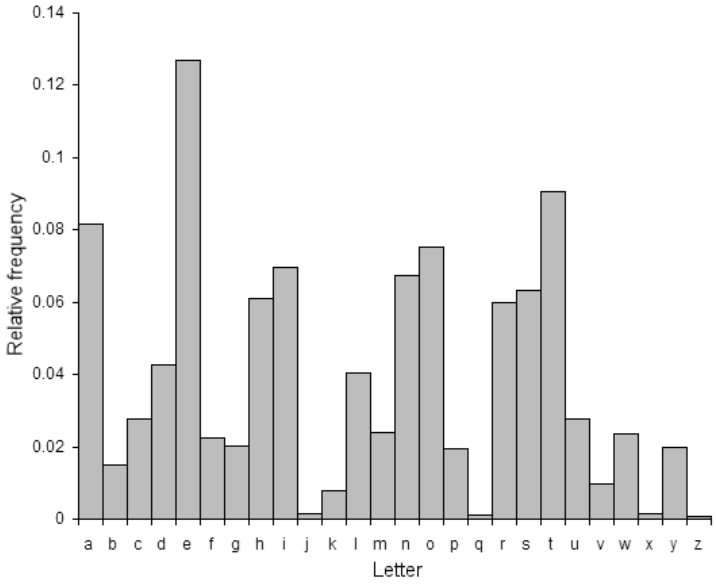


**Figure 1.3**: Frequency of letters occurring in common English communication.[109]

The cryptanalysis can be made more difficult by using an addition cipher with a multiple-letter key. The key, some combination of letters, is added to the plaintext *modulo* 26. Defining this operation as $\otimes$,

```
A SECRET MESSAGE
      ⊗
K EYKEYK EYKEYKE
      ⇓
L XENWEF REFXZRJ
```

By poor chance the encrypt of `E` is still the most common letter in the ciphertext, although the frequency of other letters has become smeared out. `A` occurs twice in the plaintext but it is encrypted differently each time. Security can be improved by choosing a longer key, as it reduces the frequency at which a particular letter is encrypted to another particular letter.

```
A SECRET MESSAGE
      ⊗
L ONGKEY LONGKEY
      ⇓
M HSJCJS YTGZLLE
```

In this ciphertext the most common letters are jointly `S`, `J` and `L`, which correspond to decrypts `N`, `E`, `G`, `Y` and `K`. `E`, however, is still among the most common and with more plaintext and some computational power the ciphertext can still be broken. For complete security the key must be as long as the plaintext and be randomly chosen, a result that is mathematically proven in section 2.1.3. In this case the ciphertext exhibits no patterns and every possible plaintext is as likely as another.

```
A SECRET MESSAGE
      ⊗
G KSGETS JEBPJDT
      ⇓
H EXJWYM WJUIKKY
```

Modern cryptographic systems rarely use keys that are as long as the plaintext. The keys must be delivered in secret to the recipient of a message before it can be decrypted, and so for modern data communications, running at Gigabits per second, the key size would quickly become restrictive. It turns out that keys ten to twenty times larger than those seen here can encrypt large amounts of plaintext and retain good security.

The problem of cryptanalysis then enters the domain of algebra and computer science. Mathematicians probe for fundamental weaknesses in the algorithms, and computer scientists build supercomputers to process huge numbers of possibilities. The primary goal of a classical cryptographer is to find a cipher that is secure enough to beat the best efforts of cryptanalysts, yet employs as small a key size as possible. The primary goal of cryptanalysts is to be one step ahead of the cryptographers while having them believe they are not. Future technologies such as quantum computers[95] and quantum supercomputers[2][80] are likely to heavily assault classical cryptographic techniques.

## 1.4 Quantum Key Distribution

Unbreakable cryptography is possible if the cryptographer has a means of secretly transmitting fresh key at speeds paralleling the ciphertext transmission. Quantum key distri-

bution has the potential to offer this capability.

Fundamental to quantum mechanics is the effect of measurement on a quantum state. If some property of a general quantum state (consisting of a superposition of eigenstates) is measured, it collapses to an eigenstate of the property and cannot be 'rebuilt' into the original state.[1] An indistinguishability condition follows: that some superpositions of eigenstates cannot be perfectly distinguished from the eigenstates to which they collapse.

Information can be encoded into a general quantum state ('quantum information') so that each possible eigenstate represents a character in the information language. A measurement of the general state will produce a particular character only with an associated probability; the outcome of the measurement cannot be pre-determined with complete certainty. In this way information can be passed from one party to another, while the measuring party alone is certain about the outcome of the measurement. Since the original state cannot be rebuilt from a particular measurement, the interference of any third party will be revealed by premature collapse of the state.

From these fundamental principles a cryptographic key distribution system using quantum information can be built. By extracting information only from states reaching an intended recipient unmeasured, a key can be built that is shared only by the transmitter and intended receiver. The challenge for quantum cryptographers is in building such a system that is competitive with classical key distribution systems for cost, efficiency, security and speed.

The first quantum key distribution system was proposed in 1984 by Bennett and Brassard. They showed that polarisation states of single photons could be used to carry quantum information and ultimately establish a secure key between two parties. Work on using single photons for quantum key distribution continues to this day. Single photons, however, are difficult to create, fragile, and can carry only limited amounts of information.

Quantum information can also be carried in the continuous eigenstates ('continuous variables') of a bright laser beam. Using amplitude and phase modulation, quantum information can be transmitted at speeds comparative to classical communications. Continuous variable quantum key distribution holds great promise for high speed quantum key distribution, opening the possibility for unbreakable cryptography to become ubiquitous throughout the world's communications networks.

## 1.5 Project Goals and Outcomes

In 2005 the Australian National University became the third research group in the world to experimentally demonstrate the use of continuous variables to establish a secret key. At the time the experiment produced the fastest key distribution yet reported. The goal of the Honours project reported in this thesis was to advance quantum key distribution at the ANU to second and third generation experiments.

The second generation experiment was a complete rebuild of the 2005 demonstration, with the addition of a mode cleaning cavity for noise reduction and higher bandwidth electronics. The experiment was not completed during the course of this project due to time constraints, although we did show that several new approaches to running the experiment are viable. In the near future this experiment is likely to result in the fastest quantum key distribution yet reported, and will continue to be of use as a test-bed for improvements to the system.

[1] This is the Third Postulate of Quantum Mechanics.

The third generation experiment involves changing the laser wavelength from 1064 nm to 1550 nm. This is to implement the experiment in an optical fibre transmission channel. The majority of design and purchasing for the third generation experiment was completed, and we had begun characterisation of the new laser and optics before running out of time.

## 1.6 Thesis Overview

This thesis begins with coverage of the two theoretical underpinnings of quantum key distribution: theories of information and of light. The chapter on information theory develops a mathematical formalism for modelling cryptographic systems and their security. It then uses this formalism to introduce the theory of secret key distillation, on which quantum key distribution is based. The chapter on light encompasses both classical and quantum treatments, since both are important for understanding the behaviour of continuous variables. Theoretical underpinnings to this chapter can be found in the appendices.

Chapter 4 tells the story of continuous variable quantum key distribution, with a review of the literature and history of the ANU work. It describes in greater detail than Chapter 2 the secret key distillation techniques investigated by the ANU. Here the project goals are restated with reference to its history, and the factors motivating the particular implementation of the experiment chosen.

Chapters 5 and 6 describe the second generation experiment, as it could be broadly considered a two-part project. The first part was the production and installation of the mode cleaning cavity; the second part was the replication and advancement of results from the first generation experiment.

The final chapter on future directions describes our work on the third generation experiment and where the technology might be taken further. It finishes with a summary of the thesis and concluding remarks.

Chapter 2

# Information Theory

This chapter covers several topics in cryptography and Shannon information theory. Following on from the discussion of cryptology in section 1.3, various historical and modern techniques of cryptography are detailed. Secret key distillation (from a quantum communications channel) is introduced as an ideal cryptographic key distribution system. The chapter ends with a brief discussion on requirements for the keys themselves.

## 2.1 Classical Cryptography

### 2.1.1 Notation

In 1949 Claude Shannon published his *Communication Theory of Secrecy Systems*, which formalised various mathematical techniques for analysing cryptographic systems.[92]. In the interests of purity, mostly his notation will be adopted when discussing the mathematics of cryptography (although his terms "encipher", "decipher" and "cryptogram" will be replaced by the more modern terms *encrypt*, *decrypt* and *ciphertext*).

Defining $M$ (for Message) as the plaintext, $K$ as the cryptographic key and $E$ as the ciphertext (Encrypted message) the process of encryption can be considered a function $f$ such that

$$E = f(M, K) \tag{2.1.1}$$

In general the security of a cipher will rely on the difficulty of finding which key was used for encryption out of the many possible keys. Poor ciphers rely jointly on the choice of key and on the obscurity of the cipher for security. This security is similar to steganographic security in that it can only be a matter of time before the cipher is discovered, resulting in compromise. It follows that the most secure ciphers can be publicly known without compromise to their security. To make the distinction between cipher and key clear, Shannon considered an arbitrary cipher as a set of transformations $T_i$ where the index $i$ corresponds to the particular key in use. That is,

$$E = T_i M. \tag{2.1.2}$$

Each $T_i$ will specify how the $j$th element of the plaintext $m_j$ is to transform into the $k$th element $e_k$ of the ciphertext. It follows that there must be a minimum of $n$ transformations available for each key, where $n$ is the total number of elements in the plaintext language (the size of the plaintext 'alphabet'). The set of all keys is called the *keyspace*. Using this formalism, a cryptographic system can be represented by the schematic in Fig. 2.1. Modern cryptological literature refers to the legitimate transmitting party as Alice, the legitimate receiving party as Bob and any illegitimate transmitting or receiving party as

Eve, who are also shown on the figure.

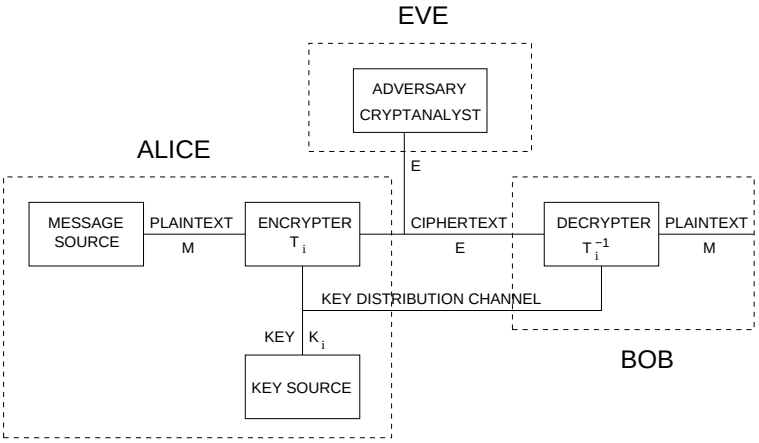


**Figure 2.1:** Shannon's general cryptographic system, with reference to the modern convention of considering an Alice/Bob/Eve system.

Each $T_i$ will have an associated probability, $p_i$, that it will be the one used for a particular encryption/decryption operation. This is equivalent to saying that every possible key for a given cipher has a probability $p_i$ that it will be used. The key source will then generate keys according to this probability distribution. It should be clear that for good security the choice of key must be as unpredictable as possible, therefore a good key source will have available many keys of equal probabilities.

In order that Bob can correctly decrypt the message, each $T_i$ must have a unique inverse $T_i^{-1}$. Therefore the decryption operation can be written

$$M = T_i^{-1} E. \tag{2.1.3}$$

With the introduced notation Shannon's definition of a cryptographic system is written as follows:

> A cryptographic system is a family of uniquely reversible transformations $T_i$ of a set of possible plaintexts into a set of ciphertexts, the transformation $T_i$ having an associated probability $p_i$.

### 2.1.2 Mathematical Definition of Security

Shannon's 1949 paper was a continuation of another major paper in information science, his *Mathematical Theory of Communication.*[91] In [92] Shannon showed that, from the point of view of a cryptanalyst, a cryptographic system was equivalent to a noisy unencrypted communications system. Cryptographic systems could therefore be analysed using the techniques presented in [91]. A fundamental idea of this paper is that entropy can be used as a measure of information, placing the tools of statistical mechanics at the hands of information scientists. While Shannon's papers are quite readable, Nielsen and Chuang [71] features a concise introduction to Shannon Entropy that forms the basis of this section.

Consideration begins with a system having a single random variable $X$, with an associated probability distribution $p(x)$. For convenience this analysis will be initially lim-

ited to discrete systems, which can later be generalised to continuous variable systems. In a discrete system the probability distribution becomes $\{p_1, \ldots, p_n\}$ for each value of $X\{x_1, \ldots, x_n\}$. The shape of this distribution determines the uncertainty of $X$—if there is a high probability that $X = x_i$ and not $\{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n\}$ then one can be fairly certain about the value of $X$. Conversely, if all values of $X$ are equally likely, one is very uncertain about the outcome of a measurement of $X$. It follows that making a measurement on a fairly certain system, in order to become completely certain, results in a smaller information gain than measuring an uncertain system for the same result.

Shannon defined information entropy as a quantitative measure of the uncertainty in $X$, can therefore be used as a quantitative measure of information. When used in this context this measure is called the Shannon Entropy $H$. It is defined by

$$H(X) \equiv H(p_1, \ldots, p_n) \equiv -\sum_x p_x \log p_x \tag{2.1.4}$$

where the convention in [91], of quantifying information with the binary system of counting, means the log is taken to base 2 and the resulting entropy is in units of bits (the log could also be taken to base 26 so that when referring to English communications the entropy would be measured in 'letters'). This convention should not be confused with the *binary entropy*, which is the special case

$$H_{binary}(p) \equiv -p \log p - (1-p) \log(1-p). \tag{2.1.5}$$

This is the Shannon Entropy for an $n = 2$ system with $p_1 = p, p_2 = (1-p)$.

Now considering a system with two independent random variables $X$ and $Y$, and a 2-dimensional probability distribution

$$p(x, y) = \{p_{x1}, \ldots, p_{xn}\} \{p_{y1}, \ldots, p_{yn}\}. \tag{2.1.6}$$

the *joint entropy* can be defined by

$$H(X, Y) \equiv -\sum_{x,y} p(x, y) \log p(x, y). \tag{2.1.7}$$

The joint entropy quantifies the total information content of the $X$,$Y$ system. At this point the analysis can be related to cryptography, with $X = M$ and $Y = E$. The communications $M$ and $E$, in their entirety, can be considered as single variables with many possible values. Obtaining a mathematical definition of cryptographic security requires consideration of the information that can be obtained, about $M$, after measurement of $E$. In other words, security can be measured by considering how much Eve can know about the plaintext after intercepting the ciphertext. If Eve knows no more after interception than before then the security is perfect. This means that regardless of Eve's computational abilities she can not access the plaintext. If she knows everything about the plaintext after interception then the security is non-existent i.e. the plaintext was transmitted without encryption.

A useful measure is found in the *mutual information* of $M$ and $E$. Adding $H(M)$ to $H(E)$ results in the sum of the information content of $M$ and $E$, with information common to both $M$ and $E$ being added twice (the mutual information). Subtracting the total information content $H(M, E)$ leaves this mutual information, defined by

$$H(M : E) \equiv H(M) + H(E) - H(M, E). \tag{2.1.8}$$

The security of a cipher can be defined by the value of $H(M : E)$. It is a measure of the amount of information available, from the ciphertext, about the plaintext. If no information is available then the sum $H(M) + H(E)$ will include no common information, and after subtraction of the total information $H(M, E)$ the mutual information will be 0. This is *perfect security.*

The analysis is more complex for ciphers such that $H(E) > H(M : E) > 0$. Since the cipher is not perfect, it is breakable. The amount of time and resources required to break an arbitrary ciphertext are dependent on how close $H(M : E)$ is to 0. The use of such ciphers must be risk managed with constant review on the state of the art of cryptanalysis.

### 2.1.3 Symmetric Ciphers

In the context of a cipher, symmetry refers to the key types (and therefore the type of encryption/decryption transformation) employed in encryption/decryption operations. If the same key (or a trivial transformation of the key such as a matrix inversion) is employed for both encryption and decryption the cipher is symmetric. In the symmetric case the key *must* be kept secret, a restrictive condition that means Alice and Bob must pre-share their key using an independent, already-secure communications channel (in practice usually a courier network).

If different keys are employed (and one can't be easily obtained by knowledge of the other), the cipher is asymmetric. In the asymmetric case only the key used for decryption must be kept secret. Shannon's paper covers symmetric ciphers in detail, but asymmetric ciphers were not discovered until the 1970's.[25] Asymmetric ciphers will be discussed in section 2.1.4.

The simplest of symmetric ciphers employs a single transformation for each language element $e_j$. $j$ here is the index of the element in the language alphabet between 1 and $n$, the number of distinct elements in the language. In English $\{e_1, \ldots, e_j, \ldots, e_n$ corresponds to the alphabet $\{\mathrm{A}, \ldots, \mathrm{Z}\}$. The transformation is reused each time the element reoccurs.

For example the $i$th available key $K_i$ in a fixed substitution cipher is the $i$th distinct permutation of the language alphabet. An encryption operation becomes a constant transformation from each distinct language element appearing in the plaintext $e_j$ to the corresponding $j$th key element $K_{ij}$:

$$T_i : e_j = K_{ij} \tag{2.1.9}$$

The fixed substitution cipher is weak since every element of the plaintext will always transform into the same ciphertext element. Therefore any pattern in the plaintext will reoccur identically in the ciphertext. The classic example of such a pattern is the frequency distribution of letters in the English language (see section 1.3). In binary communication it could be a standard bit sequence in the header of a TCP/IP data packet, or a watermark on a digital video stream.

More complex ciphers have multiple transformations for a given plaintext element, or transformations that evolve or change depending on the position of the operation in the plaintext or how many times a given element has occurred. This is in order to reduce the frequency of patterns in the plaintext reoccurring as patterns in the ciphertext. An example is the Viginère cipher, where each available key $K_i$ consists of $d$ letters, repeated

to form a key series $k_i$ of length $|M|$, the number of letters in the plaintext. The $j$th element in the key series $k_{ij}$ is then added modulo $n$ to the corresponding $j$th element in $M$, $M_j$, to produce the $j$th element of the ciphertext $E_j$.

$$T_i : E_j = M_j + k_{ij} \mod n \tag{2.1.10}$$

Modern symmetric ciphers use transformations that encrypt multiple plaintext elements in a single operation. These are called *block ciphers* and they are an improvement over single-element encryption in that element-level patterns are greatly attenuated. Block ciphers include *Rijndael*[24], *DES*[73] and *Twofish*[89]. Rijndael was chosen by the US Government to become its Advanced Encryption Standard (AES)[74] and is the current standard symmetric cipher for government and military applications. Despite the sophistication of block ciphers, however, they still do not feature perfect security as large amounts of plaintext may be encrypted with a single, small key. Non-perfect ciphers in current use are generally *computationally secure*, which means the cipher cannot be broken without the aid of a computer many, many orders of magnitude more powerful than available today. Their use is risk-managed, with strict programmes for constant rekeying.

### The One-Time Pad Cipher

The maximum Viginère key length is $d = |M|$ (and therefore the key is only used once). This choice provides the greatest security, but also the greatest inconvenience. In this case the key distribution must be conducted using a secure communications channel of the same capacity as the channel it is securing, which is to some extent a self-defeating exercise. To avoid this problem the 'Running Key' cipher uses meaningful text such as that from a literary novel as the key. The key need not then be distributed, only the knowledge of which novel to use. Unfortunately the language patterns in the novel are imprinted on the ciphertext, offering clues as to which novel was used for encryption. Only when the key is random - completely free from patterns - is the system truly secure. Such a cipher is known as the 'Vernam' system.[105]. The particular system patented by Vernam, however, referred to a teletype machine that performed a binary Exclusive-Or (XOR) operation on the plaintext and key bits. The binary XOR operation is analogous to modulo 26 addition with the English alphabet (in fact it is identical to binary modulo 2 addition). Therefore any cipher employing such an operation, with a random key of length $|M|$ will be referred to as a *One-Time Pad* (OTP) cipher. OTP ciphers make an important contribution to the claims of perfect security in quantum cryptography, and so the OTP proof-of-security follows.

Starting with some definitions, the plaintext $M$ is defined as a list of elements $\{M_1, \ldots, M_{|M|}\}$ displaying a probability distribution $\{p_1(M), \ldots, p_n(M)\}$. Since $M$ contains meaningful information this distribution must be non-random. The key $K$ is defined as a list of elements $\{K_1, \ldots, K_{|M|}\}$. The key is the same length as the plaintext, however the distribution of language elements is random— $\{p_1(K) = \frac{1}{n}, \ldots, p_n(K) = \frac{1}{n}\}$ (recalling that $n$ is the number of elements in the language). The general encryption operation is defined as addition modulo $n$. Therefore the ciphertext $E$ will be the list $\{E_1 = M_1 + K_1 \mod n, \ldots, E_{|M|} = M_{|M|} + K_{|M|} \mod n\}$.

It can be shown that in such a transformation there are $n$ possible pairs of language elements $(e_j, e_{j'})$ producing any other element $e_{j''}$. Then the probability of a given ciphertext element $E_i$ occurring is the sum of the probabilities of each of the $n$ distinct pairs occurring, which is the product of the probability distributions $p_j(M)$ and $p_{j'}(K)$ of

plaintext and key elements. Therefore the distribution of ciphertext elements will be

$$\begin{aligned}
&\left\{ \left( \sum_j^n p_j(M) p_{j'}(K) \right)_1, \ldots, \left( \sum_j^n p_j(M) p_{j'}(K) \right)_n \right\} \\
&= \left\{ \left( \sum_j^n p_j(M) \frac{1}{n} \right)_1, \ldots, \left( \sum_j^n p_j(M) \frac{1}{n} \right)_n \right\} \\
&= \sum_j^n p_j(M) \left\{ \frac{1}{n}, \ldots, \frac{1}{n} \right\} \\
&= \left\{ \frac{1}{n}, \ldots, \frac{1}{n} \right\}.
\end{aligned} \tag{2.1.11}$$

Calculating the individual and joint entropies gives

$$H(M) = -\sum_i^n p_i(M) \log_n p_i(M), \tag{2.1.12}$$

$$\begin{aligned}
H(E) &= -\sum_i^n p_i(E) \log_n p_i(E) \\
&= -\sum^n \left\{ \frac{1}{n} \log_n \frac{1}{n}, \ldots, \frac{1}{n} \log_n \frac{1}{n} \right\} \\
&= -\log_n \frac{1}{n},
\end{aligned} \tag{2.1.13}$$

and

$$\begin{aligned}
H(M,E) &= -\sum_{i,j}^n p_i(M) p_j(E) \log_n \left( p_i(M) p_j(E) \right) \\
&= -\sum_{i,j}^n p_i(M) p_j(E) \left( \log_n p_i(M) + \log_n p_j(E) \right) \\
&= -\sum_i^n \left[ p_i(M) \log_n p_i(M) \right] \sum_j^n p_j(E) - \sum_i^n \left[ p_i(M) \right] \sum_j^n p_j(E) \log_n p_j(E) \\
&= -\sum_i^n \left[ p_i(M) \log_n p_i(M) \right] - n \left( \frac{1}{n} \log_n \frac{1}{n} \right) \\
&= -\sum_i^n \left[ p_i(M) \log_n p_i(M) \right] - \log_n \frac{1}{n}.
\end{aligned} \tag{2.1.14}$$

Therefore the mutual information is

$$\begin{aligned}
H(M:E) &= H(M) + H(E) - H(M,E) \\
&= -\sum_i^n p_i(M) \log_n (p_i(M) - \log_n \frac{1}{n} + \sum_i^n p_i(M) \log_n p_i(M) + \log_n \frac{1}{n} \\
&= 0
\end{aligned} \tag{2.1.15}$$

and OTP security is proven to be perfect. Such perfect security is often referred to as *information-theoretic* security. To reiterate, this perfection is only valid if the key is only used once and is purely random ($p_i(K) = \frac{1}{n}$). In practice perfect randomness is difficult to achieve, see section 2.3 for further discussion.

### 2.1.4 Asymmetric Ciphers

Asymmetric cryptography involves Bob generating two keys, a *public* and a *private* key. The keys are designed so that the private key is not obtainable from the public key. As a result Bob can safely distribute his public key to Alice, who uses it to encrypt her message to Bob. Once received Bob uses his private key to decrypt the message. Therefore secure communications can be conducted without the need for prior key distribution over an independent, already-secure channel. A problem arises here in that Alice and Bob have no means of identifying each other. Eve could encrypt a message with Bob's freely available public key and send a message to him purportedly to be from Alice. Solutions to this problem are in the form of *authentication* techniques which will be discussed in 2.2.4. Asymmetric cryptography is commonly known as 'public-key cryptography'.

Diffie and Hellman published the first paper on asymmetric cryptography in 1976.[25] They detailed a mathematical method by which Alice and Bob can exchange public information in order to to generate a shared private key (see Fig. 2.2). The private key (the *session* key) can then be used in a symmetric cipher to ensure the security of any following message from Alice to Bob. The method is known as Diffie-Hellman Key Exchange. Rivest, Shamir and Adleman extended this idea to invent the *RSA Cryptosystem.*[85]

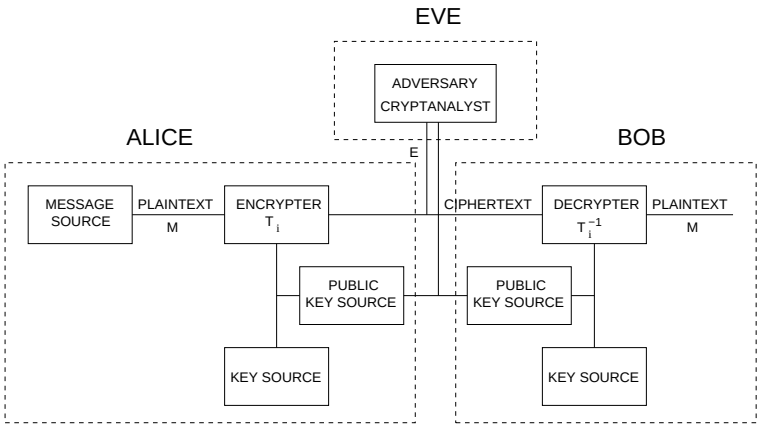


**Figure 2.2**: Diffie and Hellman's redefined general cryptographic system.[25]

RSA has a broader scope in that it was designed to support a large key distribution infrastructure. Alice may wish to communicate with multiple Bobs on multiple occasions. By initially exchanging RSA public keys, Alice and Bob(s) can establish different session keys each time they communicate without any further exchange of public keys. This is in contrast to Diffie-Hellman Key Exchange where public keys must be exchanged each time. This is an important difference because public key cryptography is vulnerable to attack during the public key exchange process, although the vulnerability can be minimised (see section 2.2.4). A convenient way to highlight the difference between the two is to think of Diffie-Hellman as a key *exchange* protocol while RSA is a key *distribution* protocol.

The mathematics of RSA and Diffie-Hellman Key Exchange are well described in [85] and numerous textbooks on cryptography and information systems. Briefly, the security of both protocols is based on the computational difficulty of factoring the product of two large prime numbers - essentially a mathematical *one-way* function. Such functions allow Bob to create a public/private key pair where the public key is the 'result' of some function based on the private key. The public key can be released without compromise to the private key as it would be computationally infeasible to calculate the private key from the public key (find the inverse of the one-way function). Through Bob's knowledge of the function, however, he can use the private key to decrypt any message encrypted by the public key.

The statement that it would be computationally infeasible for Eve to obtain Bob's private key from his public key requires some explanation, and leads this chapter to the concept of *computational* security in lieu of *information-theoretic* security. Any cipher that is not perfect can be broken—that is, the plaintext can be recovered from the ciphertext without use of the key. Any such attack, however, requires a certain amount of computational power, meaning the time and means to try multiple possible keys in an attempt to find the one message, of many possible messages, decrypting correctly from the ciphertext. For simple ciphers the computational power of a human, or a team of humans, may suffice. For more complex ciphers computers or supercomputers are needed. As discussed in section 2.1.3 the more possible keys a cipher features, the more secure it is—because cryptanalysis will require more computations and therefore more time in order to break the cipher. The overall security of the system can therefore be evaluated in terms of the time required to break an arbitrary message with some benchmark computational power. If the benchmark is linked to current and predicted real-world technologies then reasonably rigorous estimates can be made about the practical security of a given cipher. The risk of a compromise can then be managed.

A new generation of public key cryptography can be found in *Elliptic Curve Cryptography* (ECC). ECC employs a one-way function based on elliptic functions but is otherwise similar to other asymmetric systems. The advantage of ECC is that it requires more computational power to break than RSA, meaning equivalent security can be obtained with smaller keys. The driving force for this improvement is the employment of cryptography in smaller devices such as RFID tags, where a smaller key will free more memory for other information.[111]

Asymmetric ciphers require a significantly smaller key management infrastructure than symmetric ciphers. Only the authentication key must be delivered secretly, as opposed to the symmetric case where all keys must be delivered secretly. Unfortunately asymmetric ciphers may become unusable in the future if a fast factoring algorithm for products of large primes is discovered. It was also shown in 1997 by Shor that if a quantum computer could be built it would be able to solve this problem very quickly.[95] Therefore symmetric ciphers are still the best guarantor of security available for long term protection of information.

## 2.2 Secret Key Distillation

Quantum cryptography offers the convenience of asymmetric key distribution (small key management infrastructure) with the strength of a symmetric cipher (in which eventually the information-theoretic OTP will dominate). A quantum cryptographic system uses a symmetric key delivered via quantum key distribution (QKD). Specific QKD systems will be discussed in Chapter ch:background. What follows is a general discussion on how per-

fectly secure methods of symmetric key distribution might compete with computationally secure asymmetric key distribution in minimising the demand on security resources.

It was shown in section 2.1.3 that a shared secret key can be used to secure communications between Alice and Bob. The problem of symmetric cryptography lies in finding a reliable way to share the secret in the first place. The techniques considered so far have involved the generation of a random number which is securely passed to Bob before he can begin to decrypt Alice's message. This section on secret key distillation techniques shows that it is possible to establish a shared secret between Alice and Bob using an insecure communications channel, provided the channel has certain properties.

In 1993 Maurer published the paper "Secret Key Agreement by Public Discussion from Common Information",[65] where he considered a communications channel that had the following properties:

- Some information received by Bob is different to that received by Eve
- Alice and Bob are initially unaware of which information has been received by Eve, and which information they alone share

Maurer introduced a public discussion algorithm that enables Alice and Bob to discuss the transmitted information and distil from it a known subset of information shared by Alice and Bob but not Eve.[1] Such an algorithm seems to be ideal for key distribution, since the distilled secret can then be used as a symmetric key (and for a OTP cipher if it is large enough). Two problems remain with such an approach. The discussions between Alice and Bob, while public, must be *authentic*. Otherwise Eve could use a man-in-the-middle attack to hijack the discussion and ensure she has a copy of the distilled key. This problem can be resolved with the symmetric authentication techniques introduced in section 2.2.4.

The second problem is finding a communications channel that provably has the properties listed above (the crucial property being that some of Bob's information be different from Eve's). Csiszár and Körner, whose work Maurer's extends, considered a channel where Eve's information was degraded compared to Bob's.[22]. In practice such channels do exist - where Alice and Bob are communicating via an analogue telephone circuit, and Eve is a wiretapper appropriating a small amount of the signal. Such circuits, however, have limited relevance in the digital age.

Another possibility is a satellite transmitting a weak signal, so that the noise received by Alice, Bob and Eve's is independent, allowing Alice and Bob to use their authentic public discussions to find a string of data known to them but not to Eve. Again, this requires assumptions about Eve's ability to affect the measurements taken by Alice and Bob. In the search for practical information-theoretic security no such assumptions are allowed. Analogue channels with classical noise are therefore not a suitable option for secret key distillation.

Quantum communications channels (defined as channels through which quantum information, in the form of quantum states, is transmitted) do have the properties in question and do not require the assumptions of analogue channels for secret key distillation to be feasible. Schemes for building these channels are presented in chapter 4 so only a brief summary follows. If Alice can prepare a quantum state and somehow pass it to Bob, any attempt by Eve to measure the state in transit will affect it (by Heisenberg's Uncertainty Principle[43]).

[1] Maurer's algorithm was actually a generalisation of previous work by Bennett, Brassard and Robert.[4][5]

After many states are passed, a key distillation procedure can determine a bound on how many states were lost to Eve and how many passed to Bob unread. The unread, or secret, states can form the basis for a symmetric key. Eve is also unable to regenerate the states she has affected since, by the No-Cloning Theorem[112], she cannot make a perfect copy of any state sent by Alice. The distillation procedure will also determine bounds on states that have been inserted by Eve onto the channel leaving, in theory, a perfectly secret key. It is clear then that if the distillation procedure uses information-theoretic authentication, then quantum communication channels offer the possibility of information-theoretic security without the requirement for continuous key redistribution over another, already secure, means. This is a significant result for the information assurance field.

### 2.2.1 Secret Key Distillation Standard Model

Numerous papers on secret key distillation (SKD) have been published since Maurer's.[38][98][13][61][7][17] SKD is a complex process and also somewhat dependant on how the channel handles transmitting and receiving data. For example Post-Selection, a subprotocol operating as a part of SKD, was designed for continuous variable quantum channels.[98] BB84 was designed for discrete variable quantum channels.[3]

As some subprotocols encompass more of the SKD process than others, comparison can be difficult. In order to effectively analyse competing methods of SKD a standard model is required, in which subprotocols can be fitted as protocol layers. The layer approach has been proven effective from its application to computer networking protocols, where multiple technologies and ideas must converge to provide reliable communications. The standard model adopted is taken directly from descriptions in early SKD literature of the key agreement process having three phases.[7][17] The phases are:

**Advantage distillation** where Alice and Bob use authentic public discussion to obtain an information advantage over Eve (Eve may begin with more shared information than Bob). This layer must deliver a set of data in which the information shared by Alice and Bob, $I_{AB}$, or Alice-Bob correlations are stronger than the Alice-Eve or Bob-Eve correlations $I_{AE}, I_{BE}$.

**Information reconciliation** where Alice and Bob reconcile their shared information to determine exactly which pieces they share. This phase can also be thought of as 'error correction', and standard signal processing error correction techniques are usually employed. This layer must deliver a set of data which is known exactly to both Alice and Bob, and known partially to Eve.

**Privacy amplification** where Alice and Bob discard any data known to Eve, leaving them with data known solely to them. This layer must deliver a set of data which is known only to Alice and Bob. This is the distilled secret key which can then be used in a symmetric cipher.

SKD protocols and subprotocols can encompass any part of the standard model (less than one; one; or more than one layers) although most occupy one layer. The protocols occupying more than one layer generally have subroutines corresponding to the layers.

### 2.2.2 Shannon Capacity

Before examining the different protocols available for SKD it is worthwhile to set a performance benchmark, against which the protocols could be evaluated.[2] At this point it is convenient to introduce the Shannon Capacity of a channel, which is a suitable such benchmark and also happens to be fundamental to information science. The Shannon Capacity is the mathematical limit to how much information can be reliably transmitted over a practical communications channel (*practical* meaning a channel with noise and finite bandwidth).[91]

Since noise on a communications channel leads to uncertainty of the original transmission, then entropy, as a measure of uncertainty, is ideal for generalising the effects of noise. The value of a message before transmission, from Alice to Bob, and after transmission can be expressed as the dependant variables $X, X'$. The value of $X$ and $X'$ will be identical unless the message has been affected by noise. Bob wishes to know $X$ but can only measure $X'$. Bob's uncertainty about $X$ can be quantified by the entropy of $X$ conditional on knowing $X'$, or the *conditional entropy* $H(X|X')$. Since $X, X'$ are dependant variables, knowledge of $X'$ contributes to knowledge of $X$. To quantify the remaining unknown, the known ($H(X')$) is subtracted from the total knowledge of the system (the joint entropy ($H(X, X')$) for a definition

$$H(X|X') \equiv H(X, X') - H(X'). \tag{2.2.1}$$

The Shannon Information $I_S$ is defined as the amount of information remaining to the channel, from Alice's original transmission, after Bob's uncertainty is subtracted (the uncertainty resulting from the channel noise):

$$I_S = H(X) - H(X|X'). \tag{2.2.2}$$

Substituting the conditional entropy $H(X|X')$ into the definition of the mutual information $H(X : X')$ reveals that the Shannon Information is simply Alice and Bob's remaining mutual information, after the uncertainty introduced by the noise is removed:

$$I_S = H(X : X'). \tag{2.2.3}$$

The Shannon Capacity $C$ is the maximum amount of information that can be transmitted by the channel

$$C = \max\{H(X : X')\}. \tag{2.2.4}$$

The Shannon Information can be further quantified if assumptions are made about the nature of the signal and noise. Both can be assumed to have white noise statistics, a reasonable assumption in the context of distributing random keys over a noisy channel. Shannon then showed that in such a case

$$C = W \log\left(\frac{P+N}{N}\right) = W \log\left(1 + \frac{P}{N}\right) \tag{2.2.5}$$

[2]Such evaluations, however, are currently scarce since the groups involved in this research have generally invested in a single course of action and are unable to implement other protocols easily. The ANU Quantum Optics Group recently positioned itself to compare three different types of SKD using the same experimental set up (Reverse Reconciliation, Post-Selection and Liu's *et al* Advantage Distillation. At the time of writing no conclusive results were available.

where $W$ is the signal bandwidth (in Hertz), $P$ is the average signal power and $N$ is the average noise power. $\frac{P}{N}$ is the Signal-to-Noise Ratio (SNR) received by Bob, the logarithm is taken in the base of the channel alphabet (base 2 for a binary channel) and $C$ is measured in symbols/second. The capacity increases linearly with bandwidth. Fig. 2.3 shows how it increases logarithmically with SNR.

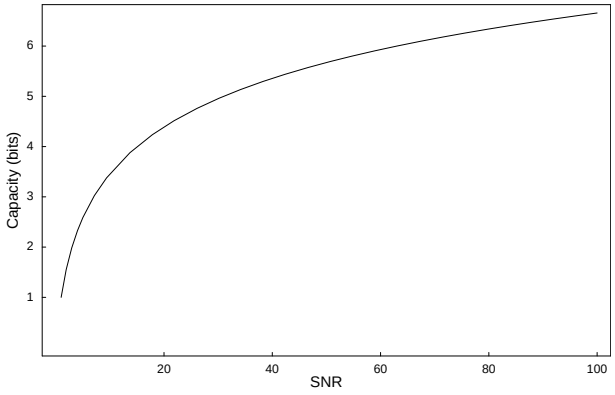


**Figure 2.3**: Shannon Capacity against SNR, per Hertz of bandwidth, per second.

For Bob channel losses are equivalent to noise, since in both cases he loses the information sent by Alice. The SNR is therefore able to encompass both channel noise and loss for calculating the capacity.

The Shannon Capacity represents an ultimate limit for any SKD protocol, in that no channel with a given loss/noise profile will be able to distil a secret key faster than the channel's Shannon Capacity. SKD protocols can be evaluated by observing how closely the secret key rate compares to the channel capacity. Efficient protocols can not be expected to waste large amounts of channel information.

### 2.2.3 Secret Key Distillation Protocols

It is beyond the scope of this (experimental) thesis to evaluate the performance and efficiency of various SKD protocols. Table 2.1 presents some of the major protocols, and how they integrate into the SKD standard model presented in section 2.2.1.

### 2.2.4 Authentication

In symmetric cryptography Bob can be assured of the identity of Alice by virtue that Alice was able to encrypt her message with the secret key shared by her and Bob, and therefore the resulting text from Bob's decryption made sense. In asymmetric cryptography, where anyone in the public, having Bob's public key, can encrypt a message for Bob he has no such assurance. Fortunately, using techniques closely related to cryptography, Bob can be given assurances that the message is indeed from Alice. Not surprisingly authentication techniques come in both symmetric and asymmetric flavours. Asymmetric authentication is the more common and so will be covered first.

The mathematics of asymmetric authentication techniques (also known as *digital signing*) are well covered in literature from the RSA paper [85] onwards. It involves Alice

| **Advantage Distillation** | **Information Reconciliation** | **Privacy Amplification** |
|---|---|---|
| Post-Selection[98](Sec. 4.3.2) | | |
| Maurer's $N$-bit Repeat Code[65](Sec. 4.3.3) | | |
| Bit-pair Iteration[28] | | |
| Direct Sliced Reconciliation[19](Sec. 4.3.1) | | |
| Reverse Sliced Reconciliation[37](Sec. 4.3.1) | | |
| Liu's *et al* Advantage Distillation[61](Sec. 4.3.7) | | |
| | Cascade[13](Sec. 4.3.4) | |
| | Forward error correction[8](Sec. 4.3.7) | |
| | | Various classes of universal hashing functions[7](Sec. 4.3.5) |
| Calderbank-Shor-Steane (CSS) Codes[99] | | |

**Table 2.1**: Summary of major SKD protocols and their position in the standard model

'signing' her message with her private key in such a way that Bob, who is in possession of Alice's public key, can tell that the message was signed by the person in possession of Alice's private key. That is, the key pairs are linked in such a way that Bob's knowledge of Alice's public key is enough to recognise an action taken with her private key. The system is still vulnerable during the exchange of public keys. Eve could intercept the two public keys and replace them with her own. She would therefore be able to pretend to be Alice to Bob and vice versa. This is called a 'man-in-the-middle' attack. Current practice for applications requiring reasonable security (such as internet banking) involve a trusted third party holding Alice and Bob's public keys, which have been sent on a previous occasion. When Alice wants to talk to Bob securely, they each download the other's public key from the trusted third party. They can then be assured of the other's identity since they both trust the third party to give them the right public key. Eve must perform two simultaneous man-in-the-middle attacks in order to effectively breach this system.

The most secure way of conducting asymmetric authentication, however, is to perform the initial exchange of public keys using an already-secure means, in the same way a symmetric key is distributed. Although this method seems to undermine the main advantage of asymmetric cryptography over symmetric, once established many authentications can take place without the need for constant rekey as in a symmetric circuit. Asymmetric authentication with secure public key exchange permits large, secure public key distribution infrastructures which use far less resources than equivalent symmetric infrastructures. The same cautions as for public key cryptography apply: a fast-factoring algorithm may be discovered or a quantum computer may be built, rendering all asymmetric techniques unusable.

A symmetric authentication scheme is based on symmetric keys - if Alice and Bob share knowledge of a pre-distributed symmetric key then that secret knowledge can form the basis of a digital signature. The mathematics - the field of universal hash functions - were introduced by Carter and Wegman in 1979, [18]. Naor and Yung later proposed a digital signature scheme based on the introduced one way universal hash functions, called "One-Time Signature" (OTS). In a manner similar to Shannon they provided a mathematical

proof for the perfect (information-theoretic) authenticity of a OTS, based as it is on the one-time use of a symmetric key.

Authentication is crucial to the security of asymmetric cryptography, since a standard public key exchange, over an insecure channel, offers provides no verifiable information about the identity of the exchangers. Either symmetric or asymmetric techniques can be used to authenticate an asymmetric system, although asymmetric authentication is the sensible option. There is no point paying the higher resource price for information-theoretic symmetric authentication when the cryptography itself is only computationally secure. And since symmetric cryptography has built-in authentication[3] it is not immediately obvious why symmetric authentication might be useful today. Considering the promise of section 2.2, however, that information-theoretically secure keys can be distributed by authentic public discussion of common information, the relevance of an information-theoretic authentication system becomes clear. All public discussion during an SKD process *must* be authenticated or the system becomes vulnerable to a man-in-the-middle attack. The distilled key cannot be considered information-theoretically secure unless the authentication method was also information-theoretically secure.

#### Distillation-Style Authentication

Some research has been conducted on using the techniques of SKD for authentication as well as key agreement.[60],[66]. Such a scheme would remove the requirement for Alice and Bob to initially share a secret to authenticate their public discussions for key agreement. This scheme could be considered the ultimate cryptographic system—information-theoretic security without the need to establish any security infrastructure beyond the communications themselves. In an era when *ad-hoc* networks are becoming increasingly popular such a system would be in high demand.

Unfortunately distillation-style authentication relies on Bob having an information advantage over Eve to begin with, and using that advantage to reveal himself as the legitimate recipient of Alice's information. Therefore these schemes only work when Eve's channel is noisier than Bob's, an assumption that is in general unreasonable for information-theoretic security.

## 2.3 Random Number Generation

So far this chapter has been concerned solely with the distribution and authentication of cryptographic keys. This final section is concerned with the keys themselves. Even if the distribution scheme is information-theoretically secure, and the distributed key is used in a OTP cipher, it was pointed out in section 2.1.3 that the OTP is not perfectly secure if the key is not perfectly random. Simply, if the key is not random it has an element of predictability, which creates patterns in the ciphertext that can be cryptanalysed.

In terms of Shannon theory, the information-theoretic security requirement is that Eve be allowed no less than fully one bit of uncertainty for each bit of key employed. Any less and Eve has obtained some amount of certainty about the key and therefore some

[3]It can be assumed that a symmetric key is only possessed by someone who has received it from the secret distribution channel, and is therefore the legitimate recipient or originator of the message. The legitimate recipient is authenticated by their ability to decrypt the message. Similarly, only an originator who possesses the key is able to encrypt the message so that the same key decrypts it correctly. A legitimate originator is therefore authenticated by their ability to encrypt the message with the right key.

information which she can build on towards breaking it, even if the distribution scheme is information-theoretic. Fig. 2.4 is a graph of the binary entropy against the probability of an arbitrary key bit being '0' ($p$) or '1' ($1-p$). It is clear that for perfect security an

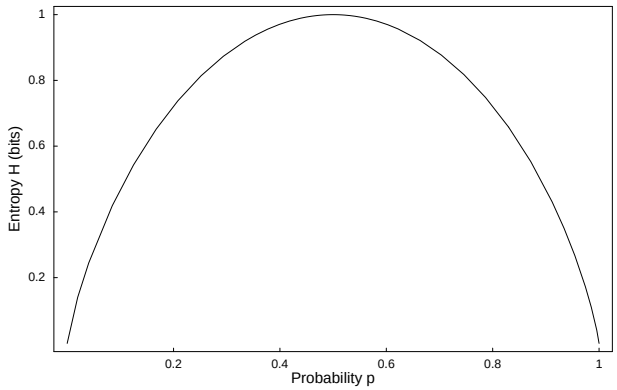


**Figure 2.4:** The binary entropy of an arbitrary key bit against the probability of it being a '1' or '0'.

arbitrary key bit must have equal probability of being '1' or '0'. This is consistent with the formula $p_i(K) = \frac{1}{n}$ derived in section 2.1.3.

Generating large amounts of good-quality random numbers for cryptographic keys has historically been a difficult problem, since computers by nature are machines of deterministic repetition. Often designers will settle for poorer quality random numbers. A famous example is an early version of Netscape's internet browser. The cryptographic keys generated by the browser for secure applications such as internet banking were based on three easily guessable values (the time of day, the application process number and parent process number). The flaw was discovered by two Berkeley PhD students.[34]

### 2.3.1 Classical Random Number Generation

Since a deterministic computer cannot generate pure random numbers algorithmically it must base its numbers on random physical phenomena. Classic examples are the decay of a radioactive element or thermal (Johnson) noise. A more modern possibility is a direct measurement of quantum vacuum noise. In 1999 Intel, a major manufacturer of computer chips, introduced an onboard physical random number source.[51] The cited paper gives an accessible explanation of classical randomness and the operation of Intel's source.

The source is based on the thermal output of current-carrying resistors. Two adjacent resistors are used and the signals subtracted. This is because non-random signals could be coupled onto a single resistor (due to a stray, or not so stray, electromagnetic field) and affect the output. The subtraction removes any signals correlated between the resistors, leaving only the pure Johnson noise. While Intel's random number generator (RNG) design minimises the possibility of a coupled signal biasing the randomness, thermal signals can still produce a bias.

### 2.3.2 Quantum Random Number Generation

Quantum theory attributes to the physical universe some fundamental uncertainties. Heisenberg's Uncertainty Principle states that there are some circumstances where an absolute limit to knowledge can be reached, that there are situations in which no physical observer can precisely predict the outcome.[43] In these situations this unpredictability manifests itself as *quantum noise*, where the results of a measurement will be found to have some inherent noise despite all precautions. The quantum noise can be harnessed as a source of truly random numbers.

Radioactive decay has quantum uncertainty and so would be a suitable process on which to base a quantum random number generator (QRNG). Radioactive materials, however, are hazardous and expensive. With the advance of optical detection technology, optical QRNG is now possible. Such a device, based on the unpredictability of a single photon being transmitted or reflected from a 50% beamsplitter, is discussed in [81]. A faster and more robust device based on continuous variables has also been proposed,[55] and a trial version was used in the later stages of this project (see sections 6.1.2 and 7.2.3).

QRNG offers the possibility of perfect $p_i = \frac{1}{n}$ random number generation in a device that would be very difficult to manipulate. An optical QRNG could only be biased by optical interference, which is much easier to prevent than thermal interference as described in section 2.3.1. With optical QRNG the final piece of an information-theoretically secure cryptographic system can be put in place.

## 2.4 Summary

Cryptography is a method of securing communications, and cryptographic ciphers can be classed as either symmetric or asymmetric. Every cipher can be ranked by how secure it is, from insecure, to computationally secure, to information-theoretically secure. The condition for information-theoretic security is that the cipher be symmetric and use a perfectly random key the same size as the plaintext. The randomness condition can be practically satisfied with an optical quantum random number generator.

Asymmetric key distribution is much simpler than symmetric key distribution and so a problem arises if information-theoretic security is desired. The problem is that the key, being the same size as the message, must be communicated by an independent and already-secure channel of the same capacity as the message channel. Such a demand on resources generally makes the establishment of information-theoretic security a self-defeating exercise. Secret key distillation techniques offer a solution to this problem.

Using a quantum information channel an arbitrarily large key for use in symmetric cryptography can be distributed, provided an authentic public channel is available. For the key and the following communications to be information-theoretically secure the method of authentication must also be information-theoretic. Such methods are available, at the cost of initially securely distributing a (relatively) small symmetric key. A small key, distributed by traditional symmetric distribution methods, is expanded into an arbitrarily large key without any further need for the independently secure distribution channel.

Chapter 3

# Topics in Classical and Quantum Optics

This chapter covers several topics in classical and quantum optics that are relevant to the project. In the first half a classical description of light is taken to simplify the theoretical treatments. The chapter shifts to a quantum description in order to examine how light behaves in the quantum regime, and how it can carry quantum information. Appendix A covers some of the more fundamental topics in this area, and if the reader is unfamiliar with optics it is recommended they read the appendix first.

## 3.1 Modulation

There are numerous ways in which to use a wave to communicate information. Two of these are amplitude and phase modulation, where the amplitude and phase of the wave are varied between levels that represent symbols in the communication alphabet (discrete or continuous).

### 3.1.1 Electro-Optic Modulation

An electro-optic modulator is able to modulate the amplitude and phase of a laser beam. It consists of an electro-optic crystal with an electric field applied to it (Fig. 3.1). The

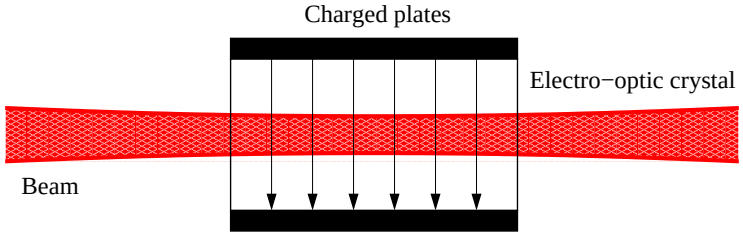


**Figure 3.1:** An electro-optic modulator, where charged plates can apply an electric field to vary the crystal refractive index.

crystal properties are such that the electric field causes its refractive index to vary with the strength of the field. Accordingly, the light passing through the modulator can be slowed by a chosen amount. The change in refractive index causes the passing beam wavefronts to slow, thus varying the phase of the beam—phase modulation (PM).[87]

Amplitude modulation (AM) can be achieved by passing circularly polarised light through a phase modulator and then a beam splitter. The electro-optic crystal's birefringence means that only a p- or s-polarised beam (depending on the crystal orientation) will be phase modulated. If the beam consists of both, such as in circular polarisation, the phase difference between the components will be modulated. This will result in elliptical light for which the ellipse shape varies with time (Fig. 3.2). The ellipse will be oriented

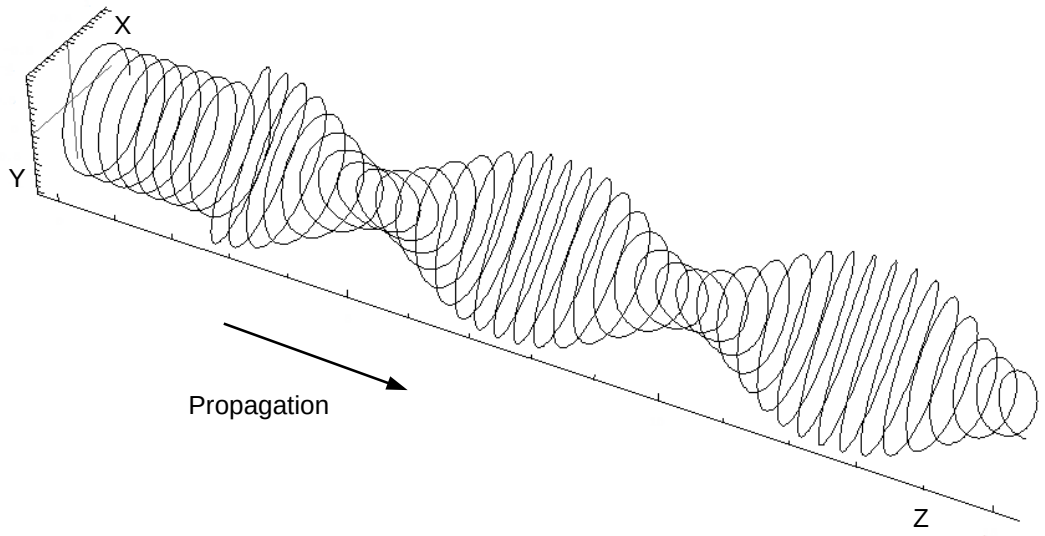


**Figure 3.2**: Circularly polarised light before and after electro-optic modulation.

at 45° to the p- and s-axes, and so often the crystals are mounted at this angle when AM is required. By examining the variance in the diagonal basis of Fig. 3.2, it can be seen that once rotated, a beam splitter selecting either axis will produce amplitude modulated light.[1]

### 3.1.2 Sidebands

The spectrum of a wave can be examined by applying the Fourier Transform.[15] The spectrum of a single mode laser (section B.4) will have a sharp spike at the laser frequency and be zero elsewhere. The picture changes when modulation is introduced, as it creates other frequencies on which the information is carried. Mathematically, the modulation process is a multiplication of the modulated wave, the *carrier*, and the modulating wave, the *signal*. Using complex amplitude notation, the amplitude of the modulated wave's electric field will be

$$\begin{aligned} E &= \Re\left(\left(\sum_{\omega} a_{\omega}(t)\cos(\omega t)\right)\mathrm{e}^{\imath\omega_c t}\right) \\ &= \left(\sum_{\omega} a_{\omega}(t)\cos(\omega t)\right)\cos(\omega_c t) \end{aligned} \tag{3.1.1}$$

where $\omega_c$ is the carrier angular frequency. $\sum_{\omega} a_{\omega}(t)\cos(\omega t)$ is the summed set of signal waves having angular frequencies $\omega$, and time-varying amplitudes $a_{\omega}(t)$ communicating

the required information (which could be analogue or digital).

The spectrum of an electromagnetic wave modulated with three different frequencies is shown in Fig. 3.3 over an arbitrary time interval $\Delta t$. The different frequencies were given different magnitudes, so within the space of $\Delta t$ they could potentially communicate a message. A more complicated signal would contain more frequency components, generally

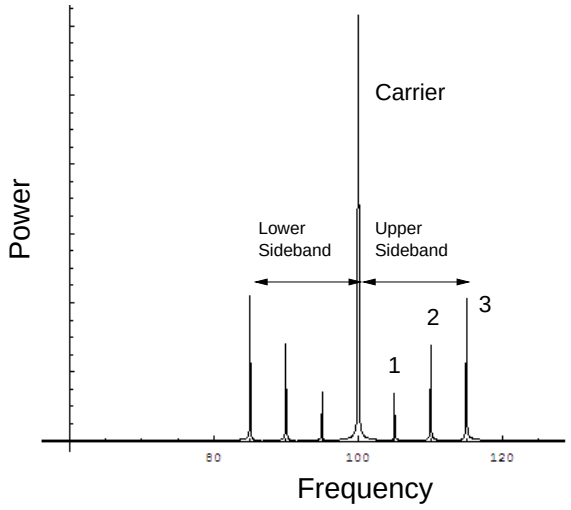


**Figure 3.3:** A 100 Hz carrier modulated with a signal consisting of 5, 10 and 15 Hz waves, over an arbitrary time interval $\Delta t$. The signal waves were given different amplitudes to communicate the message "1-2-3".

using up the entire spectrum between the carrier and the difference between the carrier and the highest modulating frequency. This band of frequencies is called the modulation *sideband*. AM produces an upper and lower sideband, as seen in Fig. 3.3.

Fig. 3.3 shows the information at frequencies around the carrier frequency. Both AM and PM will produce such sidebands, but only AM will be manifest as intensity modulations on the carrier's complex magnitude. Examining this intensity modulation cannot distinguish between AM and PM information. This is achieved by *demodulation*, which is the process of mixing another carrier with the signal/carrier combination.[1] This new carrier is called the *local oscillator*. From (3.1.1), demodulation will produce

$$\begin{aligned}&\left(\sum_\omega a_\omega(t)\cos(\omega t)\right)\cos(\omega_c t)\,\mathrm{e}^{i\omega_c t}\\&=\frac{1}{2}\left(\sum_\omega a_\omega(t)\cos(\omega t)\right)+\frac{1}{2}\left(\sum_\omega a_\omega(t)\cos(\omega t)\right)\mathrm{e}^{2i\omega_c t},\end{aligned}\tag{3.1.2}$$

and after filtering out the $2\omega_c$ frequency terms the original modulating frequencies are recovered.

Mathematically PM works in the same way, except the complex carrier magnitude is

[1]Technically this is modulating the signal/carrier with another carrier, however the term 'modulation' is usually used when referring to the imprint of information onto a wave. Modulating with a carrier adds no information and so the preferred term is 'mixing'.

modulated with imaginary values

$$\imath\left(\sum_{\omega} p_{\omega}(t)\cos\left(\omega t\right)\right)$$

which is equivalent to modulating with a $\frac{\pi}{2}$ phase shift. The information is contained in the time varying amplitudes of the phase modulations $p_{\omega}(t)$. An electric field which is both amplitude and phase modulated becomes

$$\begin{aligned}&\Re\left(\sum_{\omega} a_{\omega}(t)\cos\left(\omega t\right)\right)+\imath\left(\sum_{\omega} p_{\omega}(t)\cos\left(\omega t\right)\right)\mathrm{e}^{\imath\omega_c t}\\&=\left(\sum_{\omega} a_{\omega}(t)\cos\left(\omega t\right)\right)\cos\left(\omega_c t\right)-\left(\sum_{\omega} p_{\omega}(t)\cos\left(\omega t\right)\right)\sin\left(\omega_c t\right).\end{aligned}\tag{3.1.3}$$

The sideband PM information remains independent of the AM (Fig. 3.4). Both can be

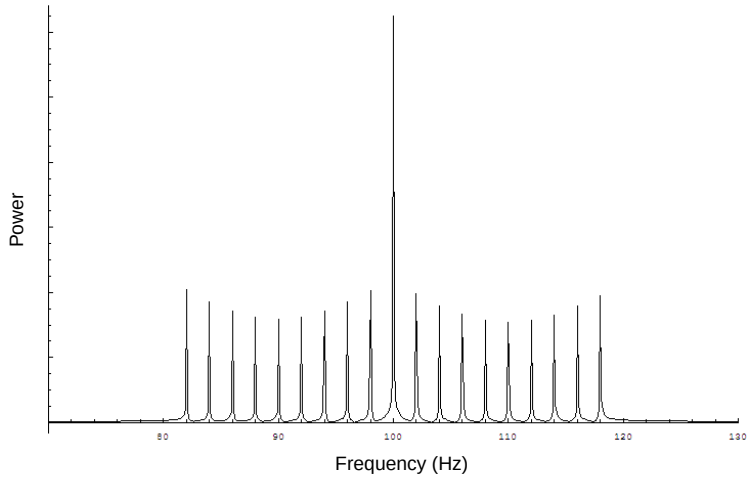


**Figure 3.4:** A 100 Hz carrier that has been both amplitude and phase modulated with multiple frequencies. The sequence '987654321' was amplitude-encoded while the sequence '123456789' was phase-encoded. A direct measurement of the spectrum such as this cannot distinguish the amplitude and phase information.

recovered even if the modulating frequencies are identical. After demodulation the wave becomes

$$\begin{aligned}&\frac{1}{2}\left(\sum_{\omega} a_{\omega}(t)\cos\left(\omega t\right)+\imath\sum_{\omega} p_{\omega}(t)\cos\left(\omega t\right)\right)+\\&\frac{1}{2}\left(\sum_{\omega} a_{\omega}(t)\cos\left(\omega t\right)+\imath\sum_{\omega} p_{\omega}(t)\cos\left(\omega t\right)\right)\mathrm{e}^{2\imath\omega t}.\end{aligned}\tag{3.1.4}$$

After low-pass filtering the complex magnitude can be measured to determine the AM signal (also called, in this context, the *amplitude quadrature*)(Fig. 3.5a). The PM signal (or *phase quadrature*)(Fig. 3.5b) is accessible by $\frac{\pi}{2}$ phase shifting the local oscillator before

demodulation[2]. This produces low-frequency terms

$$\begin{aligned}&\frac{1}{2}\left(\sum_{\omega} a_\omega(t)\cos(\omega t) + \imath\sum_{\omega} p_\omega(t)\cos(\omega t)\right)\mathrm{e}^{-\imath\frac{\pi}{2}}\\ &= \frac{1}{2}\left(\sum_{\omega} p_\omega(t)\cos(\omega t) - \imath\sum_{\omega} a_\omega(t)\cos(\omega t)\,.\right)\end{aligned} \tag{3.1.5}$$

In this case a measurement of the complex magnitude will be a measurement of the phase quadrature of the signal (Fig. 3.5).

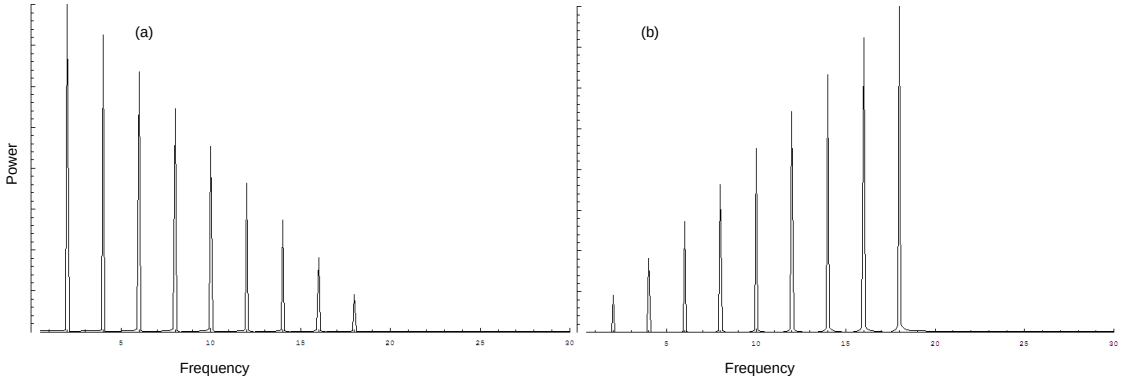


**Figure 3.5:** The carrier/signal of Fig. 3.4 after (a) AM and (b) PM demodulation. AM information can be distinguished from PM information even if identical modulation frequencies are used.

Simultaneous measurements of both phase and amplitude quadratures are possible if the signal/carrier is split into two, one mixed with an in-phase local oscillator and the other with a $\frac{\pi}{2}$ phase-shifted local oscillator. The resulting values can be represented as a complex number $\alpha_\omega = a_\omega + \imath p_\omega$ where $\alpha_\omega$ is the complex amplitude of the wave's frequency component $\omega$. The set of all such complex numbers is called *phasespace.*[1]

## 3.2 Project Lasers

A brief description of the lasers used in this projet follows. If the reader is unfamiliar with laser operation they are referred to Appendix B before continuing with this chapter.

This project has used two different lasers, both of the solid state variety. In solid state lasers the gain medium consists of a (usually) crystalline atomic structure, doped with an atom chosen so that its excited state within the structure matches the required laser wavelength. The Innolight Mephisto (Fig. 3.6a) Nd:YAG (Yttrium Aluminium Garnet crystal doped with Neodymium ions) laser radiates at $\lambda = 1064$nm; the NP-Photonics Scorpion (Fig. 3.6b) Er:Glass (optical fibre doped with Erbium ions) radiates at 1550nm.

The Nd:YAG laser uses a Non-Planar Ring Oscillator (NPRO) resonator (Fig. 3.7), created within the YAG crystal itself. The non-planar design produces a very high level of

[2]In mathematical terms this means multiplying the signal/carrier by the imaginary part of the local oscillator

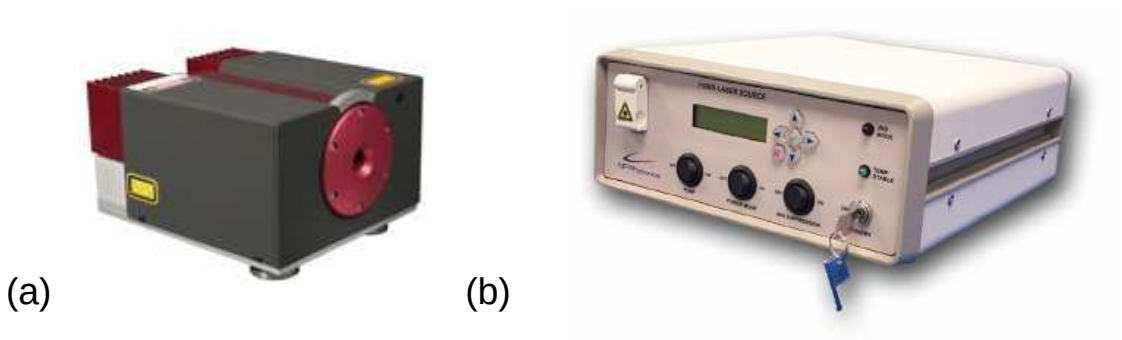


**Figure 3.6**: (a) Innolight Mephisto. (b) NP Photonics Scorpion.

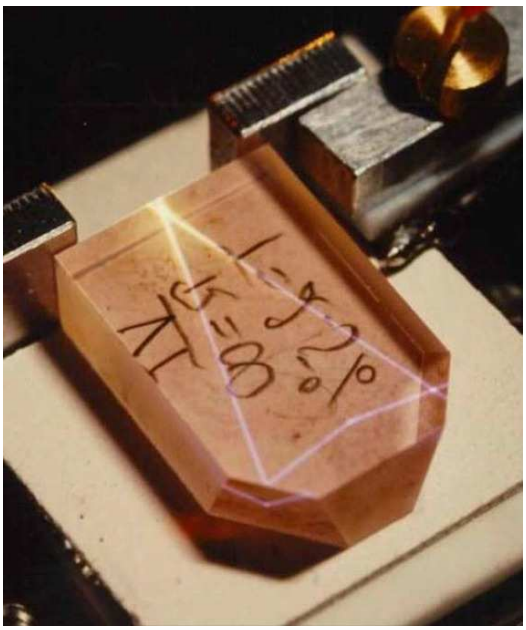

**Figure 3.7:** A Nd:YAG Non-Planar Ring Oscillator crystal. The crystal is cut so that the beam undergoes total internal reflection throughout the path of circulation, out-coupling at the pump entry point.

frequency purity and stability. [52] The Mephisto is diode-pumped and capable producing of 1.3W of optical power. Fig. 3.8 shows the relationship between optical power and pump current, while Fig. 3.9 shows single mode temperature regimes.

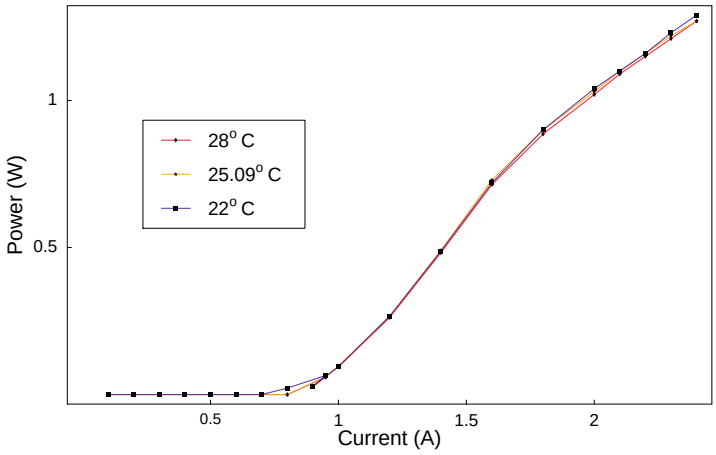


**Figure 3.8**: Mephisto optical power against pumping current at different crystal temperatures.

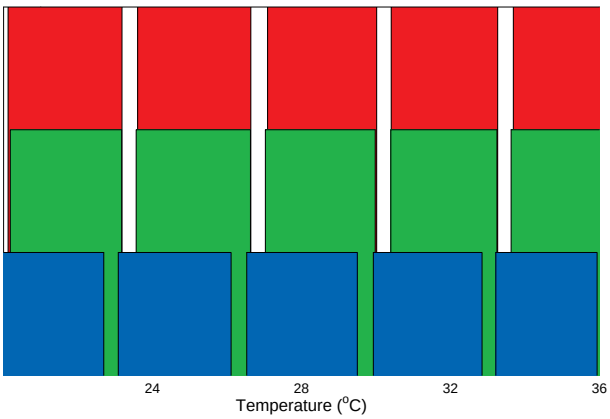


**Figure 3.9**: Mephisto temperature regimes for single-mode operation.

The Er:Glass laser uses a length of optical fibre doped with Erbium ions as the gain medium. The resonator consists of two fibre Bragg gratings, one at each end of the fibre. A Bragg grating is a series of partially reflecting objects in the propagation direction, ordered so that each reflected wave will constructively interfere at a desired angle or wavelength.[87] Bragg gratings can be made from optic fibre (a Fibre Bragg Grating—FBG) by exposing periodic sections of the fibre to a UV laser, which causes permanent change to the refractive index in the exposed sections (Fig. 3.10).[86]

The Scorpion uses an Erbium doped fibre with a FBG fusion-spliced to each end. One

grating is spectrally narrow, the other wide. The laser is diode-pumped through the wide grating and out-coupled through the narrow (Fig. 3.10). The spectral properties of the gratings are such that a resonating cavity is created across the doped fibre.

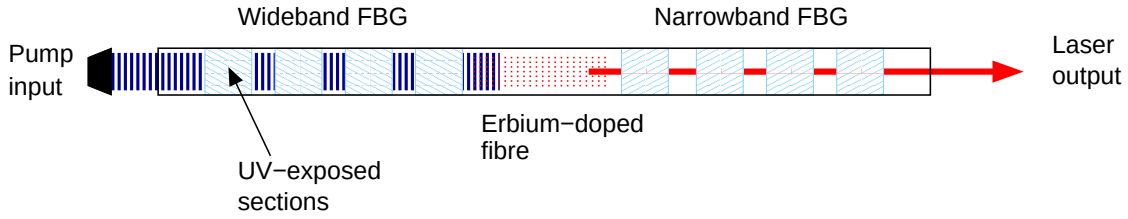


**Figure 3.10:** The Scorpion uses an Erbium doped fibre cavity created by two fibre Bragg gratings, diode-pumped from the rear.

## 3.3 Gaussian Beams

The light emitted from a laser can be closely approximated by a *Gaussian beam*, which is a solution to the paraxial wave equation (a wave equation for waves with wavefronts at small angles to the direction of propagation).[87] The intensity of a Gaussian beam propagating along the Z-axis is dependent on the *waist* size $W_0$, the radial distance $r$ from the axis and the distance along the axis $z$:

$$I(r,z,W_0) = I_0\left(\frac{W_0}{W(z)}\right)^2 \exp\left(-\frac{2r^2}{W^2(z)}\right), \quad \text{where} \quad W(z) = W_0\sqrt{1+\frac{z}{\pi W_0^2/\lambda}^2} \quad \text{(the beam radius at } z\text{)} \tag{3.3.1}$$

At the waist the wavefronts are normal to the direction of propagation; they become parabolic curves as a result of diffraction. Fig. 3.11 shows an intensity profile of a Gaussian beam.

### 3.3.1 Gaussian Modes

A planar mirror resonator is often not satisfactory since the slightest deviation from the normal of the beam will cause it to 'walk off' the mirror (Fig. 3.12). When the resonator is required to sustain oscillations, a curved mirror design is often used. It can be shown that a Gaussian beam, reflecting off a curved mirror matching the shape of the wavefront, will be reflected back to form a beam with identical waist size and position (Fig. 3.13). A standing wave of this form is called a *Gaussian mode*.[87] Resonators can also support more complex solutions, called *Hermite-Gaussian* modes. Hermite-Gaussian modes are described in Appendix C.

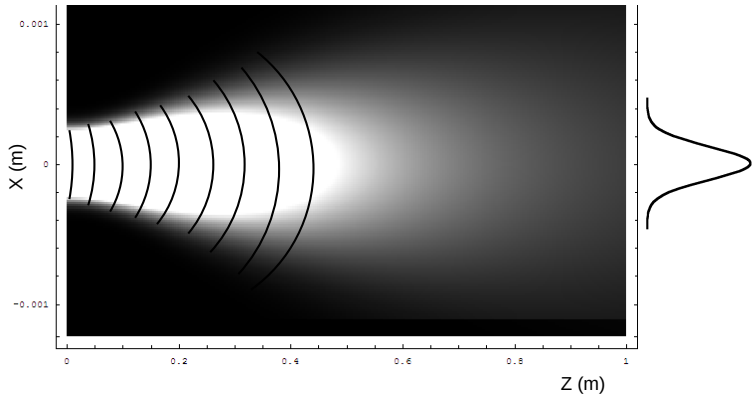


**Figure 3.11:** A cross section of a Gaussian beam in the X-Z plane with $\lambda = 1064$nm and $W_0 = 200\mu$m. Lighter points represent greater intensity. The lines representing the wavefronts show how it becomes more curved far from the waist. The graph to the side shows how in any X-Y plane (Y out of the page) the beam profile is a Gaussian curve.

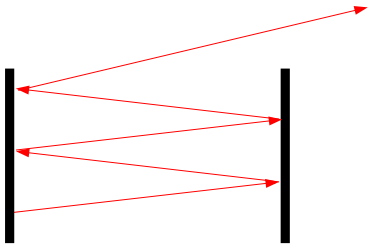

**Figure 3.12**: Beam walk off in a planar mirror resonator.

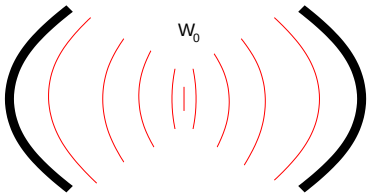


**Figure 3.13:** A curved mirror resonator. The curvature of the mirrors match that of the wavefront at the points of reflection, to create a self-reproducing beam.

### 3.3.2 Lenses

If a Gaussian beam is transmitted through a set of circularly symmetric optical components, aligned with the beam axis, the beam will remain Gaussian.[87] A lens, or system of lenses, is able to take a Gaussian beam and focus it into a new waist. This is a useful property since many optical components have specific requirements for the beam shape. A curved mirror resonator requires a specific waist size for the beam to be self-reproducing, and a modulator requires the wavefronts it is modulating to be as near planar as possible.

A lens will transform a Gaussian beam so that the new waist size is

$$W_0' = W_0 \frac{|\frac{f}{z-f}|}{\sqrt{1+\left(\frac{z_0}{z-f}\right)^2}}, \tag{3.3.2}$$

and the new waist location is

$$z' = \frac{|\frac{z}{z-f}|}{\sqrt{1+\left(\frac{z_0}{z-f}\right)^2}}(z-f)+f \tag{3.3.3}$$

where $W_0$ is the beam waist before the lens, $z$ the distance from this waist to the lens, $f$ the lens focal length and $z_0$ the *Rayleigh range* $\frac{\pi W_0^2}{\lambda}$. Fig. 3.14 shows the transformation graphically.

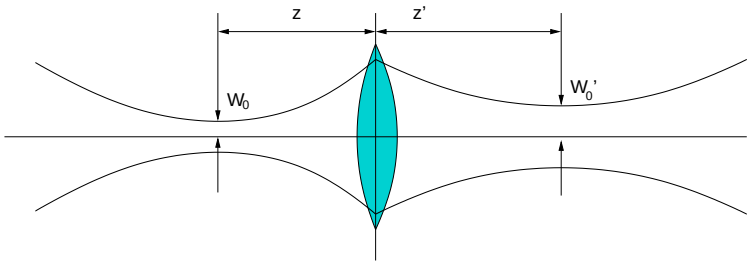


**Figure 3.14**: Lens transformation of a Gaussian beam.

## 3.4 Continuous Variables

**Notation change**: For the remainder of this thesis the amplitude of a side frequency (section 3.1.2), in the amplitude or phase quadrature, will be referred to as $a_\omega = X_\omega^+, p_\omega = X_\omega^-$, or in general the amplitude and phase quadratures as $\mathbf{X}^+, \mathbf{X}^-$.

### 3.4.1 Quantum Mechanical Quadratures

The quantum mechanical equivalents of amplitude and phase quadratures are

$$\begin{aligned} \hat{\mathbf{X}}^+ &= \hat{\mathbf{a}}^\dagger + \hat{\mathbf{a}} \\ \hat{\mathbf{X}}^- &= \imath\left(\hat{\mathbf{a}}^\dagger - \hat{\mathbf{a}}\right). \end{aligned} \tag{3.4.1}$$

$\hat{\mathbf{a}}^\dagger$, $\hat{\mathbf{a}}$ are the *creation* and *annihilation* operators respectively. They are ladder operators that act to increase or reduce the number of photons in a number state (section B.1) and can be derived from the Schröedinger Equation.[1]

The non-zero commutator $[\hat{\mathbf{X}}^+, \hat{\mathbf{X}}^-] = 2\imath$ means the quadratures are governed by a quadrature uncertainty principle (suitably scaled)

$$\langle \Delta\hat{\mathbf{X}}^{+\,2}\rangle\langle \Delta\hat{\mathbf{X}}^{-\,2}\rangle \geq \frac{1}{2}. \tag{3.4.2}$$

$\langle \Delta\hat{\mathbf{X}}^{\pm\,2}\rangle$ is the *variance* of the quadratures

$$\langle \hat{\mathbf{X}}^{\pm\,2}\rangle - \langle \hat{\mathbf{X}}^{\pm}\rangle^2, \tag{3.4.3}$$

defined in terms of the *expectation value* $\langle \hat{\mathbf{X}}^{\pm}\rangle$, which is the classical complex amplitude $\alpha$. The amplitude and phase quadratures are considered *continuous variables* since they do not have exact eigenstates, meaning the set of possible values are not discrete.[1]

### 3.4.2 Quantum States of Light

The quadrature uncertainty principle places a fundamental limit on the precision to which a quadrature can be measured. Noise on measurements resulting from this limit is called *quantum noise*, and it is present even in the vacuum. A classical vacuum, measured at the frequency $\omega$, is complete darkness $\alpha_\omega = 0$. The quantum vacuum $|0\rangle_\omega$ ($\langle \hat{\mathbf{X}}^{\pm}\rangle_\omega = 0$), however, is represented by a Wigner function in phasespace

$$W_{vacuum}(\omega) = \frac{\mathrm{e}^{-\mathbf{X}^{+\,2}_\omega - \mathbf{X}^{-\,2}_\omega}}{\pi} \tag{3.4.4}$$

and is plotted in Fig. 3.15a for some arbitrary $\omega$ (which will be dropped from the following theory). The Gaussian distributions of $\hat{\mathbf{X}}^{\pm}$ about the expectation value $\langle \hat{\mathbf{X}}^{\pm}\rangle = 0$ is the quadrature quantum noise. $\langle \Delta\hat{\mathbf{X}}^{\pm\,2}\rangle$ are the full-width half-maximums (FWHM) of the Gaussians. The Wigner function represents the probability of measuring a particular value $\mathbf{X}^{\pm}$ in the measurement $\hat{\mathbf{X}}^{\pm}|\mathbf{\Psi}\rangle = \mathbf{X}^{\pm}|\psi\rangle$,[3][110] and its general form is (3.4.5).[108]

$$W\left(\mathbf{X}^+, \mathbf{X}^-\right) = \left(\frac{1}{2\pi}\right)\int_{-\infty}^{\infty} \exp\left(\imath x \mathbf{X}^-\right) \pi^{-\frac{1}{4}} \exp\left(-\frac{1}{2}\left(\mathbf{X}^+ + \frac{x}{2}\right)^2\right) \pi^{-\frac{1}{4}} \exp\left(-\frac{1}{2}\left(\mathbf{X}^+ - \frac{x}{2}\right)^2\right) \mathrm{d}x \tag{3.4.5}$$

The vacuum is a minimum uncertainty state (also called a quantum-noise-limited state). A non-vacuum ($\langle \hat{\mathbf{X}}^{\pm}\rangle \neq 0$) minimum uncertainty state is called a *coherent* state $|\alpha\rangle$. Mathematically, coherent states are the result of the displacement operator $\hat{\mathbf{D}}$ acting on the vacuum state $\hat{\mathbf{D}}|0\rangle$.

The Wigner function for a coherent state is

$$W_{coherent} = \frac{1}{\pi}\exp\left(-\left(\mathbf{X}^+ - \Re\{\langle \hat{\mathbf{X}}^+\rangle\}\right)^2 - \left(\mathbf{X}^- - \Im\left\{\langle \hat{\mathbf{X}}^-\rangle\right\}\right)^2\right) \tag{3.4.6}$$

[3]Therefore the Wigner function is defined in terms of $\mathbf{X}^{\pm}$, not $\hat{\mathbf{X}}^{\pm}$, since it is the probability of a *measured* quadrature and not a superposition of possible states—see standard texts on quantum mechanics.

| Semiconductor | Bandgap Wavelength (nm) |
|---|---|
| Germanium (Ge) | 1880 |
| Silicon (Si) | 1150 |
| Gallium Arsenide (GaAs) | 870 |
| Indium Arsenide (InAs) | 3500 |
| Indium Gallium Arsenide (InGaAs) | 900 - 1700 |

**Table 3.1:** Wavelength ranges of photodiode semiconductor materials. InGaAs bandgaps can be chosen between the stated range by varying the ratio of InAs to GaAs, and the lattice constant.[87]

and is plotted in Fig. 3.15b. It can be seen that a coherent state is a vacuum displaced in phasespace by $\alpha = \langle \hat{\mathbf{X}}^+ \rangle + \imath \langle \hat{\mathbf{X}}^- \rangle$, and is also quantum noise limited.[110] The displacement vector can be changed with amplitude or phase modulation, enabling the the state to carry quantum information. Coherent states are reasonably easy to produce with high quality lasers, although not at all frequencies. More will be said on this topic in chapter 5. The term *purity* is used to describe how closely the state comes to the minimum uncertainty limit—an impure coherent state is called a thermal state.

A thermal state (Fig. 3.15c) has non-minimum uncertainty:

$$W_{thermal} = \frac{1}{\pi} \exp\left( -\mathrm{e}^{-s} \left( \mathbf{X}^+ - \Re\{\langle \hat{\mathbf{X}}^+ \rangle\} \right)^2 - \mathrm{e}^{-s} \left( \mathbf{X}^- - \Im\{\langle \hat{\mathbf{X}}^- \rangle\} \right)^2 \right) \tag{3.4.7}$$

where the parameter $s$ serves to expand the FWHM so that each quadrature is noisier than the quantum limit. The extra noise is classical noise which can come from a variety of sources. As the variance of the classical noise becomes much larger than the quantum noise, all quantum effects are lost and the state becomes a purely classical source of light.

Since only the product of the quadrature variances is limited by the uncertainty principle, theoretically the uncertainty in one quadrature could become 0 if it became infinite in the other. Any state for which a quadrature's variance has been reduced below the vacuum quantum noise level is called a *squeezed* state (Fig. 3.15d). The Wigner function for a squeezed state is

$$W_{squeezed} = \frac{1}{\pi} \exp\left( -\mathrm{e}^{s} \left( \mathbf{X}^+ - \Re\{\langle \hat{\mathbf{X}}^+ \rangle\} \right)^2 - \mathrm{e}^{-s} \left( \mathbf{X}^- - \Im\{\langle \hat{\mathbf{X}}^- \rangle\} \right)^2 \right). \tag{3.4.8}$$

In this case $s$ is the squeezing parameter. In practice squeezed states are difficult to produce, although numerous laboratories around the world have achieved them. Squeezed states can be used to create continuous variable entanglement. Entanglement is a well-known phenomenon unique to quantum physics and it is employed by some QKD protocols (section 4.3).

### 3.4.3 Intensity Detection

Light can be detected with a *photodiode*, which can be made from various semiconductor materials with bandgaps corresponding to optical wavelengths. The diode will produce a current (the *photocurrent*) proportional to the intensity of light shining on it. Table 3.1 shows the bandgap wavelength of some common types of photodiodes. Photodiodes using a particular semiconductor are sensitive, in varying degrees, to a range of optical wavelengths about the bandgap wavelength. The exact properties depend on how the semiconductor is engineered.[87]

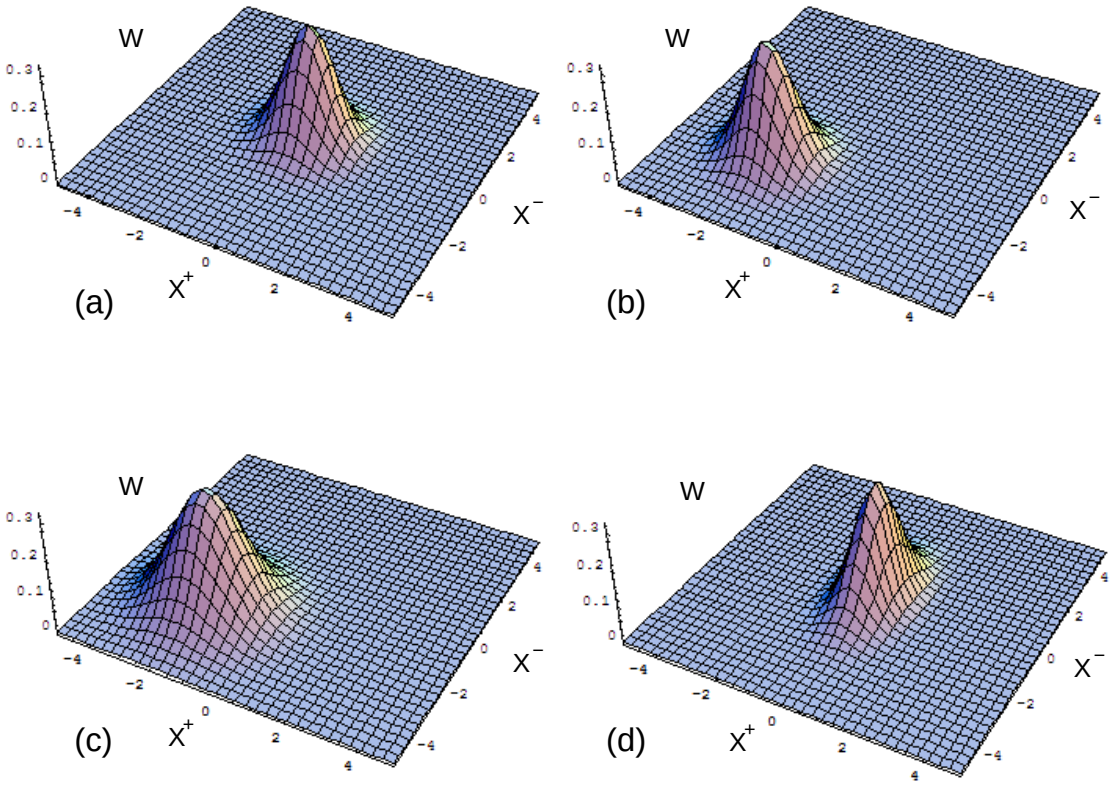


**Figure 3.15:** (a) Vacuum state. (b) Coherent state. (c) Thermal state. (d) Squeezed vacuum state.

By connecting a photodiode to a suitable amplifier, a practical photodetector can be made. Modulations, and noise, on the intensity of the light will appear as modulations and noise on the output of the amplifier. This is called *direct detection*.[1] The detection bandwidth is dependent not only on the bandwidth of the photodiode and amplifier, but also the response time of the photodiode (the time the semiconductor material takes to "reset" after a detection event). A high frequency modulation may change the intensity too quickly for the photodiode to detect it.[87]

Photodetectors exhibit *dark noise*, which is an output from the diode (and amplifier) even in the absence of any light. This is mainly due to heating of the photodiode, which can cause an electron to excite across the semiconductor bandgap (Johnson noise), and electronic noise on the amplifier. Any signal on the beam must be larger than the dark noise of the detector or it will not be detected.[87]

Photodetectors also have a *quantum efficiency*. This is the probability that a single photon incident on the photodiode will contribute to the detector current. The quantum efficiency is largely a property of the semiconductor in use. No semiconductor can have perfect quantum efficiency since some incident photons will fail to be absorbed by the semiconductor due to the probabilistic nature of the absorption process.[87]

### 3.4.4 Quantum Noise Detection

*Balanced detection* is a technique for separating quadrature quantum noise (section 3.4.2) from quadrature classical noise. A laser is split via a 50:50 beam splitter onto two detectors (Fig. 3.16). Any classical noise on the laser, say a spike at frequency $\omega$ relative

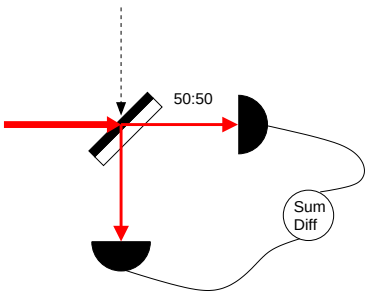


**Figure 3.16:** A balanced detection scheme. Vacuum noise enters the system via the unused port (dotted line) of the beam splitter.

to the carrier, will be split onto both detectors and produce a correlated variation in the photocurrent of each detector. The peak will therefore be present in the 'sum' signal of Fig. 3.16 but not the 'diff' (erence) signal.

Quantum noise behaves differently since it is an individually random fluctuation of every independent measurement. At any given time each detector will be affected by a different quantum fluctuation. Therefore a given spike of noise on one detector will not be correlated with the other, and the sum and difference signal will be identical. Provided the quantum efficiency of the detectors is high enough, and the dark noise low enough, quantum noise can be amplified and observed by a balanced detection scheme.

### 3.4.5 Continuous Variable Interferometric Detection

Intensity modulations can be analysed with direct detection; such classical signals can be distinguished from the quantum noise using balanced detection. Section 3.1.2 shows that the techniques covered so far are inadequate for resolving phase or simultaneous amplitude/phase information. An amplitude (and/or phase) modulated laser beam is a signal/carrier combination, and distinguishing the two quadratures requires local oscillator mixing at an appropriate phase difference (0° for AM, 90° for PM).

*Homodyne detection* is such a mixing technique for demodulating amplitude and phase information. It is covered in [1]. Fig. 3.17 shows the layout of a homodyne detector, along with the amplitude and phase modulators for encoding the information. The local

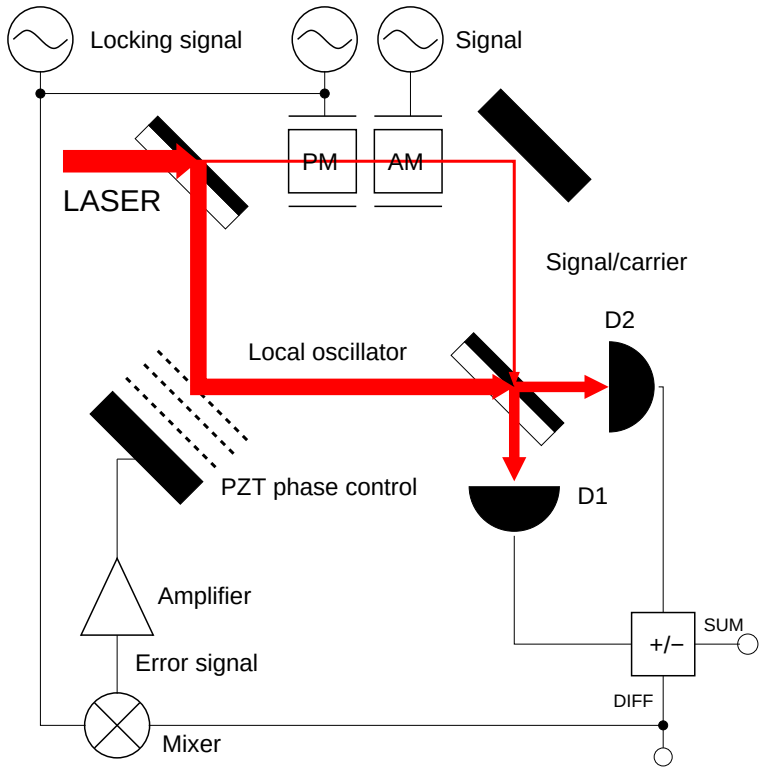


**Figure 3.17:** In homodyne detection the local oscillator beam, amplitude $\alpha_{lo}$, is phase shifted by an angle $\phi_{lo}$. Here the phase shift is brought about by piezoelectric transducer (PZT) control of the the local oscillator path length. The signal/carrier beam, amplitude $\alpha_{sig}$, is then mixed with the local oscillator on the beam splitter at $\phi_{lo}$ phase angle. The angle is kept constant by active feedback to the PZT phase controller.

oscillator $\alpha_{lo}$ is mixed with the signal/carrier $\alpha_{sig}$ on the beam splitter at an angle of $\phi_{lo}$.

The beam splitter acts on the two beams so that

$$\begin{aligned}\alpha_{d1} &= \sqrt{\frac{1}{2}}\alpha_{lo}(t) + \sqrt{\frac{1}{2}}\alpha_{sig}(t)\\ \alpha_{d2} &= \sqrt{\frac{1}{2}}\alpha_{lo}(t) - \sqrt{\frac{1}{2}}\alpha_{sig}(t)\end{aligned} \tag{3.4.9}$$

where

$$\begin{aligned}\alpha_{sig}(t) &= \alpha_{sig} + \delta\mathbf{X}^{+}{}_{sig}(t) + \imath\delta\mathbf{X}^{-}{}_{sig}(t)\\ \alpha_{lo}(t) &= \left(\alpha_{lo} + \delta\mathbf{X}^{+}{}_{lo}(t) + \imath\delta\mathbf{X}^{-}{}_{lo}(t)\right)\mathrm{e}^{\imath\phi_{lo}}\end{aligned}$$

and $\delta\mathbf{X}^{\pm}{}_{sig,lo}(t)$ are the instantaneous fluctuations of the signal and local oscillator quadratures. This treatment is valid only if the local oscillator power is much larger than the signal. After substitution and neglecting nonlinear terms the difference current from d1,d2 is

$$i_{-}(t) \approx 2\alpha_{lo}\left(\delta\mathbf{X}^{+}{}_{sig}(t)\cos(\phi_{lo}) + \imath\delta\mathbf{X}^{-}{}_{sig}(t)\sin(\phi_{lo})\right). \tag{3.4.10}$$

It can be seen that the beam splitter is an effective demodulator of AM and PM. By adjusting the phase of the local oscillator either amplitude ($\phi_{lo} = 0°$) or phase ($\phi_{lo} = 90°$) fluctuations can be cancelled, allowing both amplitude and phase information to be resolved.[1]

Practically, maintaining a particular value of $\phi_{lo}$ in the face of thermal and vibrational noise requires active-feedback phase control of the local oscillator. The electronics surrounding the homodyne detector in Fig. 3.17 are for this purpose. Feedback control is introduced in section 5.5, and interferometer locking in section 6.1.2.

Chapter 4

# Quantum Key Distribution Literature Review and Project Plan

This chapter looks at the development of quantum key distribution and its current status. The history of the ANU work is described, leading up to the 2005 first generation experiment which is explained in detail. Finally, plans for second and third generation experiments are outlined, being the subject of this Honours project.

## 4.1 Discrete Variable Quantum Key Distribution

The history and purposes of cryptography, and cryptographic key distribution, were discussed in Chapter 2. The concept of secret key distillation was presented in section 2.2, where Alice utilises a quantum channel to transmit information to Bob in the presence of Eve. Due to the quantum effects of the channel, Bob's information is not perfectly correlated with Eve's, and neither are perfectly correlated with Alice's due to errors introduced by noise in the channel (Fig. 4.1).

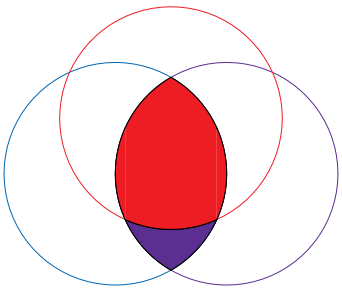

**Figure 4.1:** After transmission of some information $I$ over a quantum channel Alice (purple), Bob (blue) and Eve (red) all share partially correlated information. The blue shaded area is information known only to Alice and Bob, and can form the basis of a secret key. The red information is known to all three and would result in a compromise of security if used as a key.

The first such quantum channel was proposed in 1984 by Bennett and Brassard [3] and the protocol was hence called 'BB84'. BB84 is extensively covered in QKD literature. Although originally proposed using four photon polarisation states (vertical, horizontal,

diagonal, anti-diagonal) , [71] describes its operation for any four states such that

$$\begin{aligned} |\psi_{00}\rangle &= |0\rangle, \\ |\psi_{10}\rangle &= |1\rangle, \\ |\psi_{01}\rangle &= (|0\rangle + |1\rangle)/\sqrt{2}, \text{ and} \\ |\psi_{11}\rangle &= (|0\rangle - |1\rangle)/\sqrt{2}. \end{aligned} \tag{4.1.1}$$

In all practical implementations of BB84 so far these states are various properties of photons, which at the moment are by far the most useful of particles for communication.

The $|\psi_{x0}\rangle$ basis is non-orthogonal to the $|\psi_{x1}\rangle$ basis, meaning no measurement can distinguish the states with perfect certainty (by Heisenberg's Uncertainty Principle). Essentially, Alice sends one of these states without announcing the basis in which she encoded. Bob, who is randomly switching between measurement bases, announces that he has received the state and compares bases with Alice. If the measurement bases match then the result of the measurement, which was not announced, is kept for use as part of a secret key. If not, it is discarded.

The obvious attack for Eve here is to intercept the state sent by Alice and resend it to Bob after measurement. Eve, however, can not be sure of which basis Alice used to send the original state and so can only guess which basis she should use to encode the resent state. As a result she will introduce errors into the transmission that cannot be accounted for by the existing noise on the channel. If Alice intersperses check bits throughout her transmission to monitor for errors, she and Bob can identify whether the distributed secret key was compromised by Eve or not.

Ideal BB84 quantum key distribution does not require any secret key distillation to be performed on the transmitted data, since Eve's information is always zero. 'Ideal' in this case means that Bob has an ideal detection system and the channel is noiseless (also that Alice indeed has a source of truly single states). This means that for a given state $|\psi\rangle$ sent by Alice there will be one of three outcomes:

1. Bob measures in the incorrect basis and so the measurement is discarded
2. The state is lost in the channel
3. Bob correctly measures the transmitted state $|\psi\rangle$

In any case Eve's only choice of attack is the active attack discussed above, which can be defeated with random check bits. Any passive attack, where she measures the transmitted state without passing it on to Bob, will fail since Alice and Bob only use the states that actually reach Bob.

If Bob's detection system is non-ideal, equivalently if there is noise on the channel, then there will be some probability that despite using the same basis as Alice he will measure a different state to the one sent by Alice. Therefore the information reconciliation layer of secret key distillation is needed to correct the errors between Alice and Bob's data.

An attack by Eve is only identifiable by the introduction of errors between Alice and Bob's data. It can be seen that Eve is free to attack their communications up to the point of introducing the expected number of errors from the channel noise and Bob's detection system. Also the information reconciliation process releases more information to Eve. Hence the privacy amplification layer is required, to take the upper bound of Eve's knowledge of the communication and select out the information that will reduce her information to zero.

Finally, quantum cryptographers do not yet have a single photon source and instead rely on lasers attenuated to the point where the probability of transmitting a single photon is significantly higher than the probability of a double photon transmission. With such attenuation, of course, the probability of getting no photon at all is significantly higher again.

Unfortunately, the probability of a double transmission is non-zero, meaning that sometimes Alice will send a pair of photons that each carry identical states. Eve could employ an attack where she blocks all single photons and only lets through one photon from any pair transmitted by Alice—storing the other photon until measurement bases are announced and then performing her own measurement in the correct basis. In this case the majority of Eve's measurements will replicate that of Bob's, completely undetected. This is called the *photon number splitting* attack.[14]

If Eve blocks too many single photons, however, the uncharacteristic loss on the transmission line will be noticed. This attack can therefore be defeated by only operating in the low channel loss regime, a restriction that severely limits the distance over which BB84 can operate. A more sophisticated defence against the number-splitting attack uses *decoy states* where multi-photon pulses are deliberately inserted into the channel, and the loss characterised to determine the extent of Eve's interference.[48]

BB84 is a *discrete variable* protocol, in that the states transmitted by Alice are exact eigenstates (qubits). Other discrete variable protocols include B92[6], Ekert's EPR (Einstein-Podolsky-Rosen)[27] and Ping-Pong[10]. Discussion of these protocols are beyond the scope of this thesis, apart from noting that they do not offer dramatically increased key rates from BB84. A comprehensive review of discrete variable quantum cryptography was presented in Gisin's Reviews of Modern Physics paper.[29]

Key rate, the number of secure bits distributed per second, is a critical factor to applications for quantum key distribution. BB84's single photon communications means classically encrypted optical communications, using bright laser beams, are orders of magnitude faster. Fig. 4.2 plots out some recently obtained experimental quantum key rates. As a rough guide, practical (channel loss >50%) quantum key distribution currently occupies the kilobit regime while classical communications typically have Gigabit speeds.

Quantum key distribution uses the fragility of quantum states to ensure security. Unfortunately this fragility makes the channel very susceptible to loss, greatly reducing its capacity to carry information. A more robust alternative to the single photon state, that retains quantum effects, is a bright, weakly-modulated coherent state—a continuous variable (section 3.4.2). In Fig. 4.2 two of the fastest experiments shown are continuous variable systems.[56][62]

## 4.2 Continuous Variable Quantum Key Distribution

Continuous variable quantum key distribution (CVQKD) was first proposed during 1999.[78]. It works by using weakly modulated coherent states, containing quadrature modulations close to the quantum noise, so that the quantum noise is the dominant source of noise on the signal.

By nature the quantum noise is uncorrelated between all attempts to measure it (section 3.4.4), meaning any measurement by Bob and Eve affected by noise will be uncorrelated (although not necessarily different). Such a channel is ideally suited to use for secret key distillation.

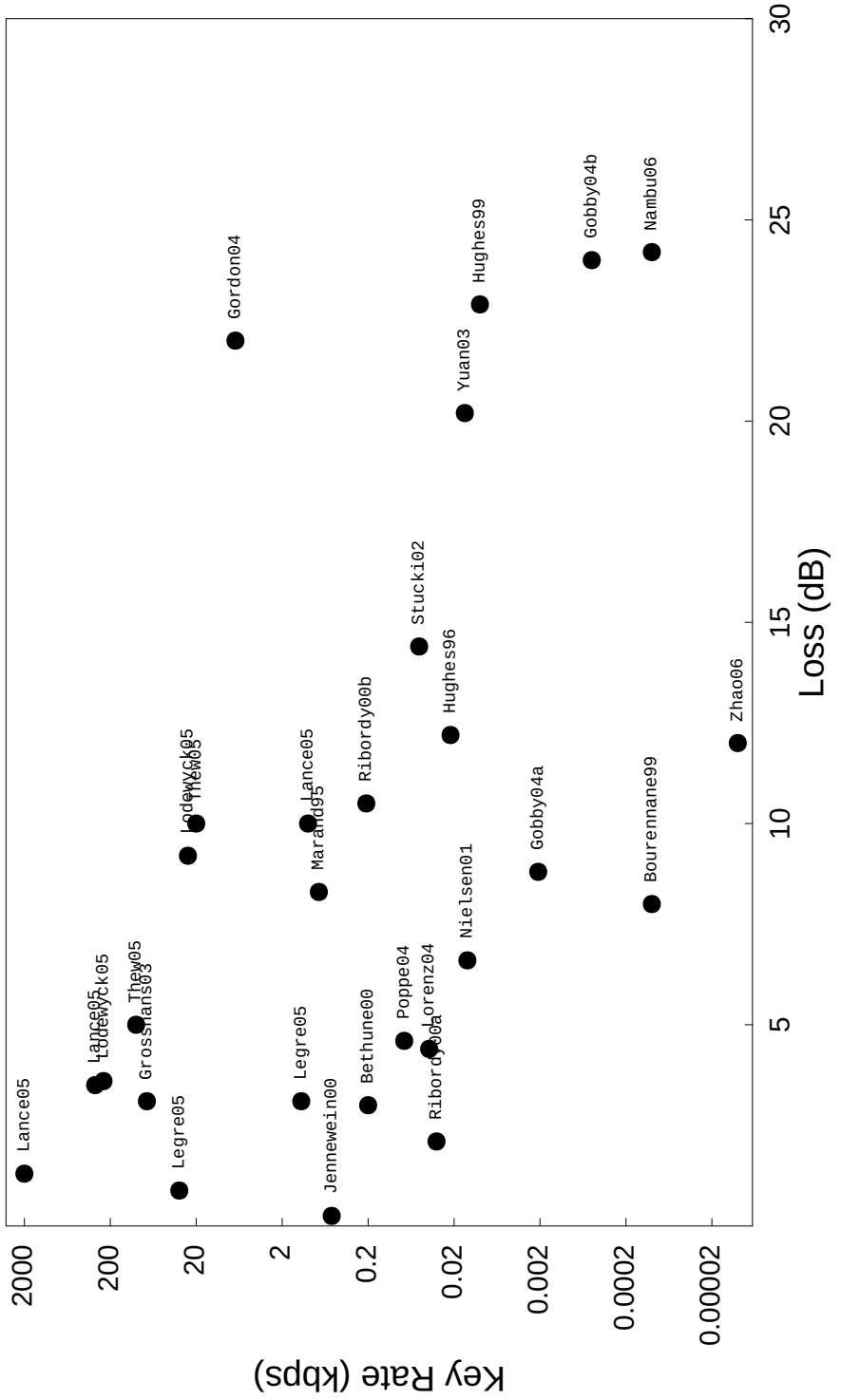


**Figure 4.2:** Some recently obtained quantum key rates: Bethune00[9]; Bourennane99[11]; Gobby04a[30]; Gobby04b[31]; Gordon04[32]; Grosshans03[39]; Hughes96[46]; Hughes99[47]; Jennewein00[50]; Lance05[56]; Legre05[58]; Lodewyck05[62]; Lorenz04[63]; Marand95[64]; Nambu06[68]; Nielsen01[72]; Poppe04[77]; Ribordy00a[83]; Ribordy00b[84]; Stucki02[100]; Thew05[101]; Yuan03[113], Zhao06[114]. Broad ranges of assumptions are implicit in many of these experiments, and so the comparison is only valid to within 1–2 orders of magnitude.

The main advantages to CVQKD are that many coherent states can be sent in the sidebands of a laser beam, equating to potentially Gigabit-magnitude raw data rates. Under low losses each coherent state can contain many bits. Detection efficiency is also much higher for bright states than for single photons. The main disadvantage of CVQKD is that the security proofs are not yet quite as strong as for BB84,[41] which has been shown to be absolutely secure under no assumptions other than that the fundamental laws of quantum mechanics hold.[96]. These points will be further discussed as they arise in the next sections.

Only three groups in the world have demonstrated CVQKD experimentally: the Australian National University Quantum Optics Group[56] (the 'ANU group'), the Erlangen-Nürnberg Institute of Optics, Information and Photonics[63] (the 'Erlangen group') and the Orsey Laboratoire Charles Fabry de l'Institut d'Optique[39] (the 'Orsey group'). The groups have collaborated at various stages of the development of CVQKD, but are currently pursuing the technology individually. The history of the ANU project involves work done at both of the other groups. A discussion of this history will therefore be illuminating for understanding their different approaches to CVQKD.

## 4.3 Project Background—CVQKD at the ANU

The coherent state scheme introduced in [78] was shown in [79] to be "not very secure". A squeezed state protocol, also proposed in [78] and security-analysed in [79], was shown to be comparable to discrete variable QKD. A number of theory papers followed this work, detailing other squeezed state-[44][19] and EPR-[82] based protocols.

In 2002 it was shown that coherent states could indeed be used for CVQKD.[38] The protocols discovered to this point, however, were only secure for channels with less than 50% loss. Giving all the loss to Eve, they were not robust enough to distil a secret key when Eve received more raw data than Bob.

Before the year was out two protocols for CVQKD with coherent states and greater than 50% channel loss were discovered: Reverse Reconciliation (RR)[37] and Post-Selection (PS)[98]. The protocols were subsequently implemented in experimental demonstrations at Orsey (RR, 2003)[39] and Erlangen (PS, 2004)[63].

The experimental setup of CVQKD was simplified by the discovery in 2004 of the Simultaneous Quadrature Measurement (SQM) protocol (informally called the 'No-Switching Protocol'), from a collaboration between the University of Queensland (UQ) Centre for Quantum Computing Technology (CQCT) and the ANU group.[106]

The ANU experimental demonstration followed in 2005, distilling secret keys for channel losses of up to 90%.[56] The initial theoretical work for SQM considered RR,[106] however the group later chose to implement PS first, with plans to compare it with RR on the same data. At this point Cascade[13] and Universal Hashing[7] were the only serious contenders for information reconciliation and privacy amplification respectively. The Orsey and ANU group implemented these protocols for their experimental demonstrations[39][56]; the Erlangen group reported a "theoretically predicted" secret key rate based on their Post-Selected data.[63][1]

[1] Although a more recent publication from Orsey also reports secret key rates based on predictions for "perfect" information reconciliation and privacy amplification protocols[62]

### 4.3.1 Direct/Reverse Sliced Reconciliation

Secret key distillation techniques, in conjunction with proofs for information-theoretic bounds on Eve's information, lead to the introduction of secure coherent-state CVQKD protocols.[104][20][38]. The direct sliced reconciliation protocol reported in [104] shows how transmitted continuous Gaussian variables can be discretised into sets ('slices') of binary strings that are partially correlated between Alice and Bob (and also possibly Eve). The partial lack of correlation is caused by channel noise and Eve's interference, resulting in Bob not receiving exactly what Alice sent.

An arbitrary error correction protocol can then be used to completely correlate the strings, although the protocol should be chosen to minimise the additional information given to Eve. In direct reconciliation, Bob corrects the errors in his strings based on either public interactions with Alice or additional, redundant information present in her initial transmissions. The reconciliation process gives further information to Eve, either through the interactions or the redundant information. To ensure secrecy the strings must finally be processed with a privacy amplification algorithm (section 4.3.5) before use.

Privacy amplification amplifies an information advantage (more Alice-Bob correlations $I_{AB}$ than Alice-Eve correlations $I_{AE}$), making $I_{AE}$ arbitrarily small. Since all loss on a channel is assumed to have been read by Eve, such an information advantage is only available for channels with losses of less than 50%. Actually, this figure is smaller, since it assumes that the remaining 50% of the channel is error-free. If the channel produces errors then error correction must be employed, which gives even *more* information to Eve. If the sum of Eve's information is greater than 50% then a direct information advantage is unobtainable.

Reverse reconciliation was proposed by the Orsey group to counter this shortcoming. The sliced reconciliation is performed in reverse: Alice uses the error correction protocol to correct her strings to match the errors in Bob's strings. It is clear that Alice will always be able to make a better guess than Eve as to Bob's measurements, even with channel loss greater than 50% (although the advantage approaches zero under very high losses). Therefore an information advantage can almost always be leveraged—resulting in a practical protocol for CVQKD.[37][39]

### 4.3.2 Post-Selection

In a collaboration between the Erlangen group and UQ, another protocol for creating a pre-SKD information advantage with >50% channel loss was reported in 2002.[98] Essentially, Bob calculates the states *post-transmission* for which his measurement was more favourable than Eve's. 'Favourable' refers to Shannon's result that a precise measurement contains more information than an imprecise measurement.[91] Alice and Bob then *select* these states for further secret key distillation, since they have an information advantage which can be distilled and amplified to produce a shared secret key.

The transmitted states are quadrature-modulated coherent states $|\alpha + \delta\mathbf{X}_A^+ + \delta\mathbf{X}_A^-\rangle$, with the quadrature modulations $\delta\mathbf{X}_A^\pm = x_A^\pm$ continuously drawn by Alice from two zero-mean Gaussian distributions of variance $V_A^\pm$. See section 3.4.2 for a treatment of modulated coherent states.

The optimal noncollective attack (section 4.3.8) for Eve is to replace the lossy channel with her own lossless channel (perhaps using teleportation) and split off a fraction $1 - \eta$. She would then pass on the remaining $\eta$ to Bob, where $\eta$ is the channel transmission expected by Bob without Eve's interference.[38]

Alice now announces the absolute values $\{|x_A^{\pm}|\}$ of her states, allowing Bob and Eve to narrow down their measurements $x_B^{\pm}, x_E^{\pm}$ to $\pm x_A^{\pm}$. In this case the maximum possible information $I_{AE}$ Eve can obtain for a given state is given by the protocol-independent *Levitin bound*,[59]

$$I_{AE}(\mathbf{X}_A^{\pm}) = \frac{1}{2}\left(1+\sqrt{1-z^2}\right)\log_2\left(1+\sqrt{1-z^2}\right) + \frac{1}{2}\left(1-\sqrt{1-z^2}\right)\log_2\left(1-\sqrt{1-z^2}\right),$$

where

$$z(\mathbf{X}_A^{\pm}) = \mathrm{e}^{-(1-\eta)\mathbf{X}^{\pm 2}_A} \tag{4.3.1}$$

is the quadrature overlap function.

Alice and Bob must have a prior agreement on their communication protocol—how Bob will interpret the coherent states as binary data. A simple choice is to define positive displacements in phasespace as the binary digit '1' and negative displacements as '0'. The probability of Bob's measurement being in error is calculated in [98] as

$$p(\mathbf{X}_A^{\pm}, \mathbf{X}_B^{\pm}) = \left(\mathrm{e}^{-4|\mathbf{X}_A^{\pm}\mathbf{X}_B^{\pm}|\sqrt{2\eta}}\right) / \left(1+\mathrm{e}^{-4|\mathbf{X}_A^{\pm}\mathbf{X}_B^{\pm}|\sqrt{2\eta}}\right). \tag{4.3.2}$$

The mutual information $I_{AB}$ between Alice and Bob for a given transmitted state $\mathbf{X}_A^{\pm}$ and a given measurement $\mathbf{X}_B^{\pm}$ can be determined by Shannon's formula for a binary channel with Gaussian noise (section 2.2.2),

$$I_{AB}(\mathbf{X}_A^{\pm}, \mathbf{X}_B^{\pm}) = 1 + p\log_2 p + (1-p)\log_2(1-p). \tag{4.3.3}$$

An information advantage over Eve exists for each element $\{\mathbf{X}_A^{\pm}, \mathbf{X}_B^{\pm}\}$ such that

$$\Delta I(\mathbf{X}_A^{\pm}, \mathbf{X}_B^{\pm}) = I_{AB}(\mathbf{X}_A^{\pm}, \mathbf{X}_B^{\pm}) - I_{AE}(\mathbf{X}_A^{\pm}) > 0. \tag{4.3.4}$$

If Bob post-selects only states for which $\Delta I > 0$ then, after interpretation, he and Alice will share binary strings that have a greater degree of correlation than Alice and Eve's strings. The $\Delta I$ can be made to approach the Shannon capacity for a 4-state channel by segmenting the phasespace into 'banded information channels' (BICs). This allows different areas, having different error rates, to be post-selected with individual sets of parameters.

After post-selection the advantage can then be leveraged by secret key distillation techniques to create an arbitrarily secure key.[98][56]

### 4.3.3 Maurer's $N$-bit Repeat Code

Another technique for distilling an information advantage is by Maurer's $N$-bit Repeat Code.[65] It differs from Post-Selection in that it requires Alice and Bob to possess discretised data strings. It can be used to amplify $\Delta I$ from a set of post-selected data or, more generally, to distil an advantage from the partially correlated strings resulting from any physical communication process where Bob and Eve are affected differently by noise.

The protocol is described in detail in [65]. A basic overview is presented here. After Bob and Eve have received their partially correlated strings, Alice randomly builds a string $C_A$ from codewords $C^N$, selected from the set of codewords $\mathcal{C}$. Each codeword contains $N$ repeated elements of the communication alphabet. For example, for $N = 3$ and a binary

communication alphabet, $\mathcal{C} = \{000, 111\}$.

Now, say Alice had previously transmitted the binary string $S_A$ and Bob measured $S_B$. Alice performs a bitwise addition (equivalent to the Exclusive-Or, or XOR, operation) between $S_A$ and $C_A$ and sends the result, $S_A \oplus C_A$, to Bob via the classical channel (requirements on the classical channel are discussed in section 2.2). Bob takes the string $S_A \oplus C_A$ (he can assume he has received $S_A$ perfectly, since classical communications techniques can be used to achieve an arbitrarily low probability of bit-error) and performs the XOR operation with $S_B$.

If $S_A$ and $S_B$ were perfectly correlated, Bob will recover $C_A$ from this operation. If not, Bob's string $C_B = (S_A \oplus C_A) \oplus S_B$ will contain elements not in $\mathcal{C}$. Bob sends the indices of these elements to Alice and they both discard the corresponding elements of $C_A, C_B$ to produce a correlated string $C$. The redundant bits in each codeword are also discarded. For example, say Alice sent

$$S_A = 010\ 101\ 011\ 010\ 101\ 001\ 010\ 010\ 110\ 101$$

and Bob received

$$S_B = 010\ \underline{001}\ 011\ 010\ \underline{001}\ 001\ 010\ \underline{000}\ 110\ 101.$$

Alice builds $C_A$, performs $S_A \oplus C_A$, and sends the string to Bob. As long as her choice of codewords is completely random, the security of $S_A$ will be maintained (the mutual information between $S_A$ and $(S_A \oplus C_A)$ will equal zero).

$$\begin{aligned} S_A &= 010\ 101\ 011\ 010\ 101\ 001\ 010\ 010\ 110\ 101 \\ C_A &= 111\ 000\ 111\ 111\ 000\ 111\ 000\ 000\ 000\ 111 \\ S_A \oplus C_A &= 101\ 101\ 100\ 101\ 101\ 110\ 010\ 010\ 110\ 010 \end{aligned}$$

Bob performs $C_B = (S_A \oplus C_A) \oplus S_B$ and examines the result,

$$\begin{aligned} (S_A \oplus C_A) &= 101\ 101\ 100\ 101\ 101\ 110\ 010\ 010\ 110\ 010 \\ S_B &= 010\ 001\ 011\ 010\ 001\ 001\ 010\ 000\ 110\ 101 \\ C_B = (S_A \oplus C_A) \oplus S_B &= 111\ \underline{100}\ 111\ 111\ \underline{100}\ 111\ 000\ \underline{010}\ 000\ 111 \end{aligned}$$

It can be seen that elements $(C_B)_{2,5,8} \notin \mathcal{C}$. After Bob communicates this to Alice over the classical channel, they discard $(C_A)_{2,5,8}$ and $(C_B)_{2,5,8}$ respectively. This leaves them with

$$\begin{aligned} C_A &= 111\ 111\ 111\ 111\ 000\ 000\ 111 \\ &= C_B \\ &= C. \end{aligned}$$

And discarding the redundant bits gives

$$C = 1111001.$$

The protocol may be run over several rounds, as it can be seen that if all the bits in a given $N$-length element is measured incorrectly a valid codeword will still be produced—so errors may still be present in the final strings. Another error correction protocol may also be employed to further correlate the strings.

Using this protocol Alice and Bob can distil a greater information advantage over Eve.

### 4.3.4 Cascade

Cascade[13] is an information reconciliation protocol, designed to bring Alice and Bob's strings $S_A, S_B$ into practically perfect correlation while disclosing as little as possible information to Eve. Information reconciliation protocols differ from advantage distillation, as the cost of efficiently reconciling data is a slightly decreased information advantage.

Cascade was initially the reconciliation protocol of choice for all three CVQKD groups.[38][104][56] It is efficient to implement and at the time of publication compromised less information to Eve than the best available standard error correction techniques.[13] It works as follows.

Alice and Bob choose the number of passes for the protocol based on the characterised error probability of the channel. They then choose a block size for the pass, $k_1$, and divide their strings into blocks of $k_1$ bits. Alice then calculates a *parity bit* for each block (protocols for calculating the parity bit, with minor variations, usually involve taking the binary sum, modulo 2, of the block) and sends it to Bob.

Bob calculates the parities of each of his blocks, and compares them to Alice's parities. For every block having a non-matching parity, Alice and Bob split it in half and repeat the process. Eventually they will locate the bit error, enabling them to correct it.

Each pass will identify blocks that have an odd number of errors. After each pass Alice and Bob agree on a random function to select bits for the pass's new set of blocks, essentially scrambling the order of bits. This spreads the remaining errors in $S_B$ across the entire string, so that fewer rounds per block are needed to find the errors.

A bound on the information compromised to Eve is given in [13]. Obviously this bound will be dependent on the number of passes, and the number of rounds per pass required to correlated $S_A$ and $S_B$. This is in turn dependent on the number of errors in $S_B$, which is dependent on the properties of the quantum communication channel. For high loss channels, not only are more bits initially lost due to the channel, but in the correlated string $S$ more have been compromised due to the reconciliation process.

### 4.3.5 Universal Hashing Privacy Amplification

Privacy amplification is the art of distilling highly secret shared information from a larger body of shared information that is only partially secret.[7] Alice and Bob begin with a perfectly correlated $n$-bit string $S$, for which Eve knows a string $V$ containing at most $t < n$ bits of information about $S$. Privacy amplification allows Alice and Bob to decide on a string $K$ of $r$ bits, of which Eve's knowledge is arbitrarily small. It works even if Alice and Bob do not know the details of the joint distribution $P_{SV}$ or Eve's distribution $P_V$.

Privacy amplification was linked to the information reconciliation layer of secret key distillation by Cachin and Maurer, who considered both the information obtained by Eve during the initial transmission and the information leaked to Eve during the reconciliation process. The latter is known as 'side information' and contributes to Eve's knowledge via an auxiliary string $U$, which gives Eve $k$ bits of information about $S$.[17]

Alice and Bob obtain an initial string $K'$ by applying a *universal hashing function*[18] $g$ to $S$. $g$ is randomly chosen from a class of universal hashing functions $\mathcal{G}$. The definition of a class of universal hashing functions is given below. The effect of hashing $S$ into $K'$ is to spread Eve's uncertainty of specific bits in $S$ over the entire length of $K'$.

**Definition** A class $\mathcal{G}$ of functions $\mathcal{A} \to \mathcal{B}$ is universal if, for any distinct $x_1, x_2 \in \mathcal{A}$, the probability that $g(x_1) = g(x_2)$ is at most $1/|\mathcal{B}|$, when $g$ is chosen from $\mathcal{G}$ according to the uniform distribution.

The ANU group uses $\mathcal{G} = \mathrm{GF}(q)[x]$, the set of all polynomials $a_0+a_1x+a_2x^2+\cdots+a_qx^q$, where the coefficients $a_i$ are elements of the Galois field $\mathrm{GF}(q)$ (see standard algebra texts on finite fields). The hashing function is

$$\left(S_0^p + S_1^p x + S_2^p x^2 + \cdots + S_q^p x^q\right) \times \left(a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_q x^q\right) \pmod{x^q + x^b + 1} \quad (4.3.5)$$

$S_0^p, \ldots S_q^p$ are the bits of the $p$th $q$-size block of $S$. Each coefficient $r_i$ is chosen randomly from $\mathrm{GF}(q)$ to select $g$ from $\mathcal{G}$. The function retains the polynomial order $q$. The result is then

$$f_0 + f_1 x + f_2 x^2 + \cdots + f_q x^q, \quad (4.3.6)$$

with the new coefficients $f_i$, dependent on every bit in $S^p$, forming the hashed string $K'$.[93]

Alice and Bob now bound Eve's knowledge of the correlated string $K'$ by calculating her Rényi entropy, based on her knowledge of the initial string $S$ and side information $U$. Rényi entropy is used since the existence of eavesdropping strategies reducing Rényi entropy significantly more than Shannon entropy was shown in [7]. It is defined (for a binary variable $X$) as

$$R(X) = -\log_2 P_c(X) \quad (4.3.7)$$

where $P_c(X)$ is the *collision probability*, the probability that $X$ takes on the same value twice in two independent experiments

$$P_c(X) = \sum_{x \in \{0,1\}} P_X(x)^2. \quad (4.3.8)$$

It can then be shown that with probability of at least $1 - 2^{-s}$ Eve's total Rényi entropy is given by

$$R(K'|V,U) \geq t - 2k - 2s \quad (4.3.9)$$

where $s$ is a chosen security parameter. Furthermore, Alice and Bob can decide on $r$ bits of $K'$ to use as a secret key $K$, about which Eve's knowledge is less than

$$\frac{2^{r-(t-2k-2s)}}{\ln 2} \text{ bits.} \quad (4.3.10)$$

For absolute security $s$ and $r$ must be chosen such that Eve's total knowledge of $K$ is less than one bit.

### 4.3.6 Simultaneous Quadrature Measurement

Simultaneous Quadrature Measurement (SQM), or "No-Switching", was introduced by Weedbrook *et al* in 2004, at the ANU.[106]. It involves simultaneously measuring the amplitude and phase quadratures, rather than randomly switching between them, to establish Alice and Bob's strings of 'raw data' for input to a secret key distillation process.

In a switching protocol (discrete or continuous) Alice and Bob randomly switch measurement bases (or state manipulation), and later discard states for which their bases were not the same. Before the introduction of SQM this switching was thought to be essential to security. This was shown to not be the case, and that for CVQKD the SQM key rate was higher than for an equivalent switching protocol, approaching double for large signal variances and high channel efficiency.[106][107]

The SQM protocol simplifies the experimental configuration, since a single phase-locked loop can be used to continuously detect both amplitude and phase quadratures. Randomly switching quadratures requires precise phase control of the local oscillator (which is of course possible with good experimental design), but also time. The Orsey group recently reported a quadrature switching time of 1 $\mu$s.[62] The Erlangen group switch between polarisation state measurement bases and have reported an effective switching time of 500 $\mu$s. SQM is currently only used by the ANU group.

While the SQM technique causes some signal loss due to the loss of precision mandated by the uncertainty principle, this loss is within Bob's station and so does not need to be attributed to Eve.

### 4.3.7 Second Generation Protocols

The ANU and Orsey groups are currently investigating alternatives to some of the basic secret key distillation layer protocols presented thus far.[62][57][93] These alternatives can be considered 'second generation protocols', since they have been published more recently than the main body of SKD literature and promise higher key rates.

- Liu's *et al* Advantage Distillation
- $M$-state Post-Selection
- Turbo codes

In 2003 Liu, Van Tilborg and Van Dijk published a protocol linking the advantage distillation and information reconciliation phases of SKD.[61] The ANU group is investigating an implementation of this protocol. Initial results show that it may produce up to 50% more key than the current combination of Maurer's $N$-bit Repeat Code and Cascade.[93]

The Post-Selection data rate can be further increased by post-selecting states from a $M$-ary Quantum Quadrature Amplitude Modulation (QAM) communication protocol.[53] The '$M$-state' protocol, currently being developed by the ANU group, improves on previous versions of Post-Selection by increasing the number of distinguishable coherent states from 4 to $M$ ($M = 4, 9, 16, 25 \ldots$).[57]

Turbo codes are a forward error correction technique currently being used by the Orsey group.[62] Forward error correction differs from the interactive style used by Cascade. Instead of Alice and Bob interactively determining a correlated substring from their shared information, Alice includes enough redundancy in her initial transmission for Bob to correct all the errors. It was shown in [75] that Turbo codes are superior to Cascade for many situations.

### 4.3.8 CVQKD Security

The security of CVQKD is a difficult area to study, beyond finding the bounds on information explicitly compromised to Eve during a protocol's operation. The various theoretical

analyses have not yet been drawn together for a conclusive proof-of-security, as in Shor and Preskill's proof for discrete variable QKD.[96]

Various studies on CVQKD security[79][40][49][41] examine assumptions about Eve's inability to perform a certain type of attack. Importantly, these assumptions are distinct from classical proofs of computational security, in that Eve is always given unlimited (classical) computational resources. In many cases, applying stronger assumptions simply leads to a lower secure key rate.

For example, if it is assumed that Eve has access to a quantum memory (the construction of such a device has not yet been reported by any group in the world) then a class of attacks called 'collective attacks' are available to Eve. In a collective attack Eve uses her quantum memory to store the states she has intercepted without measuring them, until Alice and Bob have conducted their reconciliation. Grosshans examines some of the circumstances for which coherent state CVQKD is still secure assuming collective attacks in [41]. An analysis of CVQKD security is beyond the scope of this thesis, apart from the following point.

#### Thermal State Attack

One security assumption currently relevant to the ANU group is that Alice's transmissions are perfect coherent states. In [56] they reported a (symmetric) quadrature variance of $1.01 \pm 0.01$ with respect to a minimum uncertainty state.

Section 3.4.2 describes how states with symmetric variances greater than one (thermal states, or *impure coherent states*) contain both quantum and classical noise. Section 3.4.4 describes how when a beam is split, say between Bob and Eve, the classical noise is correlated while the quantum noise is not.

If Alice transmits an impure coherent state, and therefore Bob expects an impure coherent state, Eve can measure the classical noise without affecting Bob's measurement. Eve then gains an amount of information about Bob's measurements that will not be taken into account when her bounds are calculated, compromising the security of the final key.

## 4.4 Project Plan—Second Generation SQM

The previous section presented an overview of the ANU group's progress in CVQKD to the point of my Honours commencement. The experiment by Lance *et al* reported in [56] can be considered the group's first generation CVQKD-SQM experiment. After the experiment was completed it was pulled apart and moved, in pieces, to another laboratory.

The group's plan was to rebuild the experiment with some improvements to increase the key rate and security—a second generation experiment. The previous experiment had been built in the gravitational wave detection facility on a high-quality optics table, meaning the experiment was relatively free of vibrational noise. The new lab (Fig. 4.3), situated on the first floor of the department building and with a lower quality table, was intended to bring experimental ambient conditions slightly closer to those present in real-world applications.

Following the second generation experiment, the group would change laser wavelength from 1064 nm to 1550 nm, being the optimal frequency for optic fibre transmission. A third generation experiment would be built, using a similar design to the second generation, to test CVQKD-SQM over long distances of fibre (20–50 km).

**Figure 4.3:** The new quantum cryptography laboratory. The Mephisto laser, not quite unpacked, can be seen in the foreground.

Features of the second and third generations are discussed in the following sections. Ambitiously, I set out to build both experiments on the two tables in the new quantum cryptography laboratory. While rebuilding the Lance *et al* experiment I undertook the purchasing of a 1550 nm laser, 1550 nm optics, optic fibre, fibre coupling optics, mounts and electronics.

Unfortunately (perhaps fortunately?), the 1550 laser arrived four months late. At the same time, numerous difficulties occurred in building the second generation experiment and so eventually I have had to pass on responsibility for building the third generation experiment to my successor. My work on the second generation experiment is detailed in Chapters 5 and 6; my work on the third generation experiment is reported in section 7.1 as part of my discussion on future directions for CVQKD at the ANU.

### 4.4.1 Optical Noise Reduction

Section 5.2 shows how a mode-cleaning cavity can increase the purity of a coherent state. The thermal state attack discussed in section 4.3.8 can therefore be defeated by the addition of a suitable mode-cleaning cavity to the experiment.

The first generation experiment was also troubled by spikes of noise below 10 MHz.[56]Fig. 1(inset) A suitable mode cleaning cavity can reduce the laser noise to the quantum noise limit at much lower frequencies than this.

The first milestone for the second generation experiment was therefore to design, build and operate a high-finesse mode-cleaning cavity, in order to reduce laser noise. The methods and results for this milestone are detailed in Chapter 5.

### 4.4.2 Bandwidth Increase

Another way to increase the key rate for CVQKD-SQM is to increase the modulation bandwidth, so that more raw information can be sent with the laser. The first generation experiment used a 17 MHz modulation band from 33 MHz to 50 MHz. The signal band was lower bounded by low-frequency detector roll-off and upper bounded by the 100 Msps data acquisition system (the maximum frequency that can be sampled at 100 Megasamples

is 50 MHz[76]).

For the second generation experiment the acquisition system was upgraded to 200 Msps and detectors with a flatter response to a lower frequency were built. This meant nearly the full 100 MHz bandwidth of the acquisition system could be used for key distribution, approximately 5 times that of the first generation experiment.

The higher modulation frequencies brought in another problem. From approximately 80–110 MHz is the FM radio band, and significant interference could be observed in this frequency. This inductive noise could be suppressed with good shielding. Section 5.1.2 discusses the method and results of inductive noise suppression.

The second milestone of the experiment was therefore to rebuild entirely the first generation experiment, using the mode-cleaned beam. Similar data would then be taken, with the increased bandwidth, to compare key rates.

## 4.5 Summary

This chapter has discussed the development of quantum key distribution, from its beginnings with BB84 to the current work in continuous variable QKD. The story of the ANU Quantum Optics Group's efforts in CVQKD is told, along with the major protocols in use. The evolution of the group's secret key distillation model is described, with some educated speculation, in Table 4.1.

| **Year** | **Measurement** | **Advantage Distillation** | **Information Reconciliation** | **Privacy Amplification** |
|---|---|---|---|---|
| 2004 | Simultaneous Quadrature Measurement | Reverse Reconciliation/Cascade | | Galois polynomial hashing |
| 2005 | Simultaneous Quadrature Measurement | Post-Selection/$N$-bit Repeat Code | Cascade | Galois polynomial hashing |
| 2006 | Simultaneous Quadrature Measurement | $M$-state Post-Selection/ Liu's *et al* Advantage Distillation | | Galois polynomial hashing |

**Table 4.1**: Evolution of the ANU group's secret key distillation model.

After the success of the first generation experiment, the group planned to rebuild it with a mode-cleaning cavity and higher bandwidth systems. These additions should improve the security and key rate. The goal of my Honours project is to achieve these improvements.

I set two milestones towards achieving this goal: install and run the mode-cleaning cavity; and reproduce the experimental results of the first generation. By repeating the experiment in this way both the integrity of the work and the technology itself can be advanced.

Chapter 5

# Optical Noise Reduction

This chapter details the work undertaken to reduce optical noise in the quantum key distribution experiment.

## 5.1 Optical Quadrature Noise

### 5.1.1 Definition

'Noise' can be defined as the uncertainty of a measurement that results from some process interfering with the measured variable or state. If Alice prepares a quadrature variable $\mathbf{X}_A^{\pm}$, Bob will measure $\mathbf{X}_B^{\pm} = \mathbf{X}_A^{\pm} + \delta\mathbf{X}_B^{\pm}$ where $\delta\mathbf{X}_B^{\pm}$ is a variation from $\mathbf{X}_A^{+}$ due to noise. Therefore for each measurement Bob makes he can only be certain of the value to within $\pm\langle|\delta\mathbf{X}_B^{\pm}|\rangle$ of $\mathbf{X}_B^{\pm}$. The noise has made him uncertain of the exact value $\mathbf{X}_A^{\pm}$.

For this thesis noise will be considered having separate 'classical' and 'quantum' components. Defining 'quantum' noise as the uncertainty in a measurement due to Heisenberg's Uncertainty Principle, 'classical' noise is then defined as noise from all other sources.

### 5.1.2 Sources of Classical Noise

#### Thermal Noise

Thermal noise, also called Johnson or Nyquist noise, is due to random motion of electrical current carriers which increases with temperature. The current has a mean value of 0—it is just as likely to flow in one direction as the other.[87]. By methods of statistical mechanics, it can be shown that at a temperature $T$ over a resistance $R$ the Johnson noise power spectral density is

$$\mathrm{S}(f) = \frac{4}{R}\frac{hf}{\exp(hf/kT) - 1} \tag{5.1.1}$$

at frequency $f$ ($k, h$ are Boltzmann's and Plank's constants).

For an electrical circuit of bandwidth $B$, and when $f, B \ll kT/h = 6.25$ THz at room temperature, the noise variance is spectrally flat and equal to

$$\frac{4kTB}{R}. \tag{5.1.2}$$

Thermal noise is most apparent in this project as dark noise on photodetectors. Even without illumination of the detectors, the signal of equation (5.1.2) can be found in the detection band. Therefore the detector circuit must be designed to amplify the quantum noise above the dark noise (which can then be observed by the techniques of section 3.4.4).

The power difference between the amplified quantum noise and the dark noise is called the *clearance*.

### Mechanical Noise

Mechanical noise enters the experiments as undesired motion of the optics (particularly mirrors). The motion is caused by acoustic vibrations travelling through the building structure, laboratory floor, optics table and ultimately through the optics mounts. These vibrations come from many sources, from people running along the corridor outside the laboratory to seismic sources. Mechanical noise can be minimised by isolating the optics table with pneumatic mounts, using good quality optics mounts and screwing them firmly to the table.

### Inductive Noise

Inductive noise is the coupling of electromagnetic fields present in the laboratory into the laser pump, modulation, locking or detection circuits. Interference can be broadband or single-frequency, but inductive noise from a single source is usually limited to a small part of the spectrum. We found three major sources of inductive noise in the cryptography laboratory:

- Power supplies (50 Hz)
- FM radio (80-110 MHz)
- Modulator balun (modulation frequencies)

The 50 Hz inductive noise, being much lower than than the cryptography detection band, has little effect on operations provided it is not too strong. The radiofrequency (RF) noise is a different matter, since with the current acquisition system we can modulate at up to 100 MHz. Suppression of the RF noise is crucial to obtaining maximum bandwidth.

Inductive noise and its suppression is well understood and covered in standard texts on electrical engineering. Good grounding—having low-impedance connections from all electrical equipment to a common zero potential—is the first step. This directs any induced currents to the ground, rather than the acquisition equipment.

For stronger, high frequency interferences shielding is required. Using a result from Gauss' Law, it can be shown the electric field inside a conducting cavity is zero regardless of external fields. If an appropriate shield of conducting material is built around a circuit, the only fields inside the shield will be those due to the circuit itself.[36] Good circuit design will then prevent the circuit from interfering with itself.

We suppressed the high frequency inductive noise by designing and building shields for the detectors from copper sheet (Fig. 5.1). Aluminium foil was also used to shield the modulator balun and cable connections. The shielding worked well, as Fig. 5.2 shows.

### Laser Relaxation Oscillation

Section B.2 discusses how in a laser there are two processes producing photons. Stimulated emission produces the required coherent amplification while spontaneous emission produces photons at random, averaging at the transition lifetime $\tau$ of the laser excitation states.

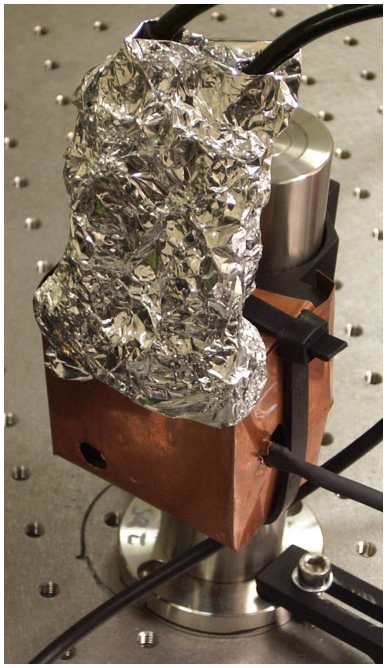

**Figure 5.1:** Detector RF shielding was achieved with a combination of folded copper sheet and aluminium foil.

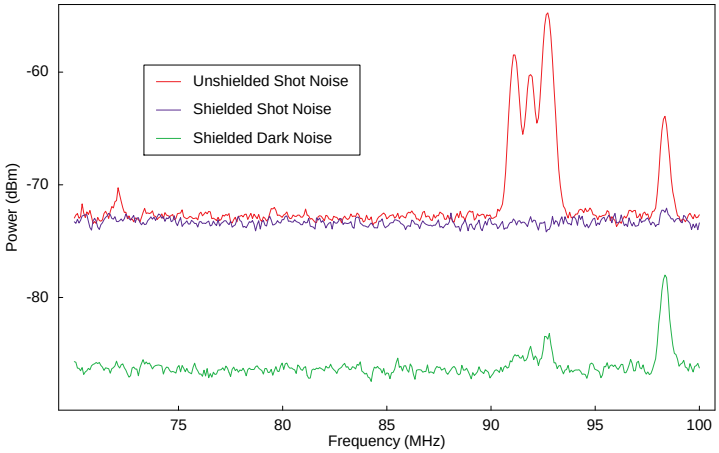


**Figure 5.2:** Detector spectra with and without RF shielding. The shielding was very effective at suppressing the FM radio noise to below the shot noise. It could not be suppressed entirely, as it can still be seen above the weaker dark noise level.

In the frequency domain this spontaneous emission produces a Gaussian intensity modulation about $1/\tau$ Hz, and is called the relaxation oscillation (since it is the gain medium de-exciting without stimulation).

The relaxation oscillation can be suppressed by feedback-controlled intensity modulation, in what is called a *noise-eating circuit*.[1] More information on feedback control is found in section 5.5.

### 5.1.3 Mephisto Noise Analysis

To examine the Mephisto's relaxation oscillation we built a balanced detection scheme (section 3.4.4) using low-frequency detectors. We then spectrum analysed the sum and difference signals (Fig. 5.3). The Mephisto incorporates a noise-eating circuit which can be switched on as required. Fig. 5.4 shows its effectiveness in suppressing the relaxation oscillation.

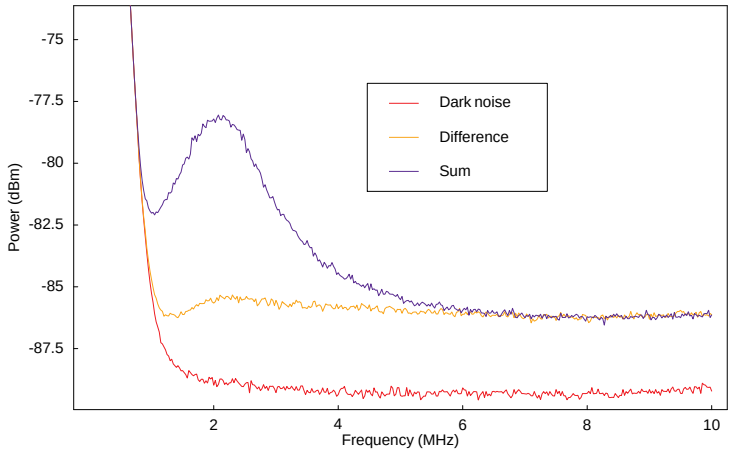


**Figure 5.3:** Plot showing the Mephisto's relaxation oscillation, detected by a low-frequency balanced detection system.

It is clear from Fig. 5.3 that the relaxation oscillation is classical noise since it is greatly suppressed in the difference signal (i.e. it is correlated on the two detectors). It is also clear that at higher frequencies the laser is approximately quantum noise-limited, since the sum and difference signal are equal (detector noise is uncorrelated). This is the case for all single-mode lasers.

## 5.2 Optical Noise Reduction Using A Resonant Cavity

Resonant cavities can filter a laser's spectrum to the quantum noise limit at low frequencies, and can also improve the purity of the subsequent coherent state (since the cavity is free from thermal noise sources present in the laser). In this thesis such a cavity will be designated a *mode cleaner*, since it cleans frequency noise from the laser mode.

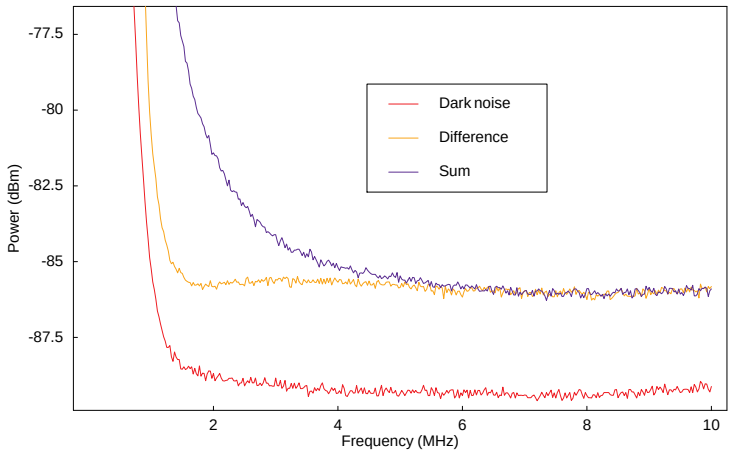


**Figure 5.4:** Plot showing the effect of the Mephisto noise-eater in suppressing the relaxation oscillation.

Calculating the design parameters of the cavity requires an analysis of its effect on the quadratures variances of an input laser beam. When operating near the quantum noise limit the classical analysis of a cavity described in section B.3 does not suffice. The quantum transfer function for a cavity is derived in [1]. It involves a study of the cavity equations of motion and consideration of how fluctuations propagate through the cavity. For a low-loss cavity and single mode input, the amplitude quadrature transfer function can be simplified to

$$\langle \Delta \mathbf{X}^{\pm 2} \rangle_t(\nu) = \frac{\kappa^2 \langle \Delta \mathbf{X}^{\pm 2} \rangle_i + (2\pi\nu)^2 \langle \Delta \mathbf{X}^{\pm 2} \rangle_v}{\kappa^2 + (2\pi\nu)^2},$$
$$\text{where} \qquad (5.2.1)$$
$$\kappa = \frac{(1-g)c}{2L} \quad \text{and}$$
$$g = \sqrt{\exp(-\beta L) R_1 R_2}.$$

The transfer parameters are described in table 5.1.

From the transfer function the mode-cleaning properties of the cavity can be examined. Importantly, a comparison between the variance of the output beam and the quantum noise limit can be drawn against different transfer parameters. To simplify the calculations the quantum noise limit is set to 1—so that $\langle \Delta \mathbf{X}^{\pm 2} \rangle_v = 1$ and $\langle \Delta \mathbf{X}^{\pm 2} \rangle_t(\nu)$ is in units of vacuum quanta.

The first generation QKD experiment measured a quadrature variance of $1.01 \pm 0.01$.[56] Figs. 5.5a and b show that increasing the cavity reflectivity or FSR decreases the frequency at which this thermal state would approach a coherent state.

The physical dimensions of a two-mirror confocal cavity can be reduced by using a half-symmetric resonator (Fig. 5.6). Further improvement to cavity properties can be made with the triangular design shown in Fig. 5.7. The non-normal incidence of the beam

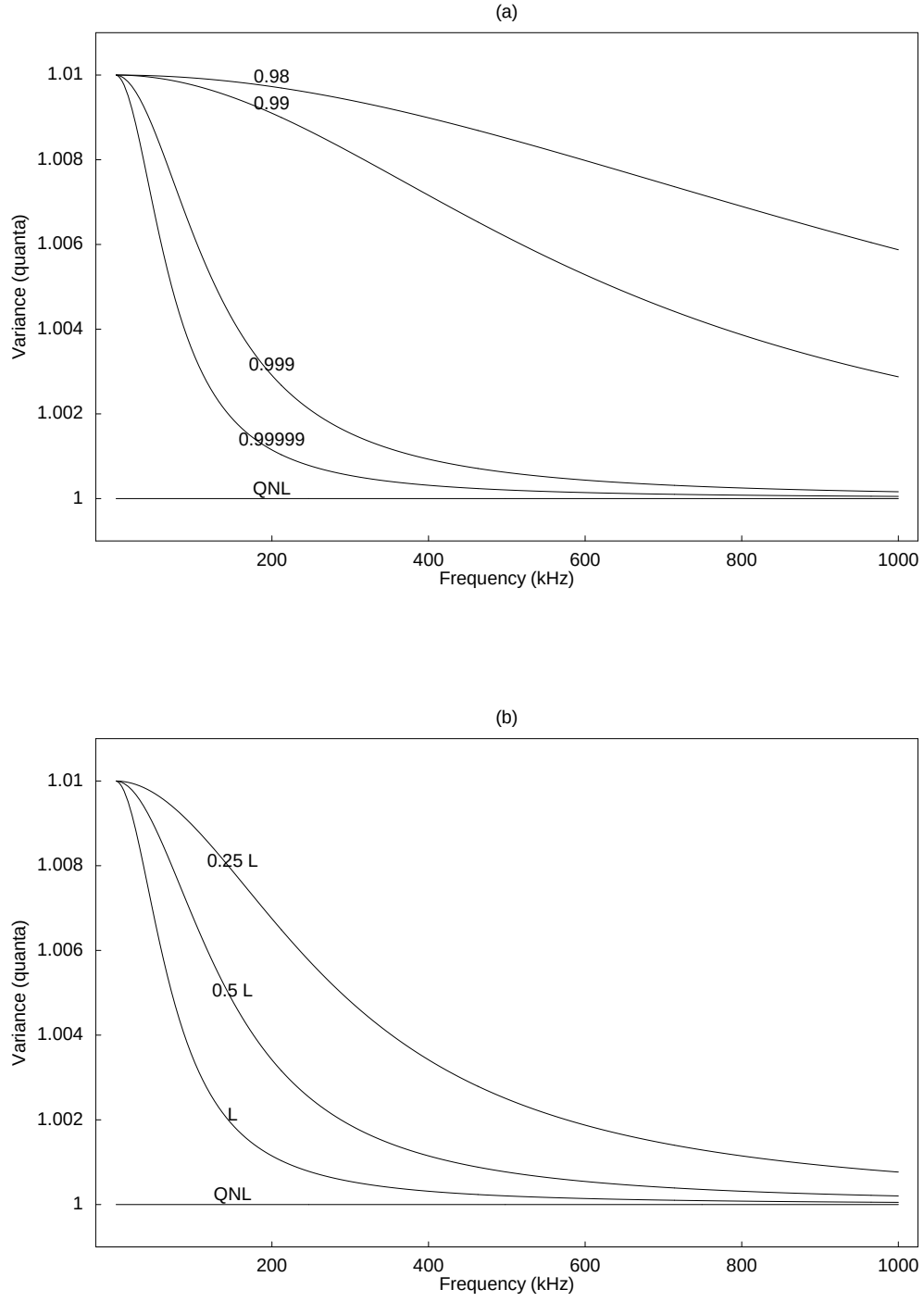


**Figure 5.5:** Cavity power spectra, compared to the quantum noise limit $\langle \Delta \mathbf{X}^{\pm 2} \rangle_v = 1$, for varying transfer parameters. The QNL is produced by setting $\langle \Delta \mathbf{X}^{\pm 2} \rangle_i = 1$, showing that a quantum noise limited input will remain at the QNL. (a) Varying mirror reflectivities $R$ ($L = 0.84$m, $\langle \Delta \mathbf{X}^{\pm 2} \rangle_i = 1.01$, $\beta = 0.003$). (b) Varying cavity path length $L = 0.84$m ($R = 0.99999$, $\langle \Delta \mathbf{X}^{\pm 2} \rangle_i = 1.01$, $\beta = 0.003$).

| Parameter | Description |
|---|---|
| $\langle \Delta \mathbf{X}^{\pm 2} \rangle_t(\nu)$ | Quadrature variance of the transmitted beam at frequency $\nu$ |
| $\langle \Delta \mathbf{X}^{\pm 2} \rangle_i$ | Quadrature variance of the input beam |
| $\langle \Delta \mathbf{X}^{\pm 2} \rangle_v$ | Quadrature variance of the secondary input beam (for a mode cleaning cavity this is generally vacuum) |
| $\beta$ | Round-trip loss coefficient |
| $R_1$, $R_2$ | Reflectivities of input/output mirrors, usually both equal to $R$ |
| $L$ | Cavity path length |

**Table 5.1**: Description of the transfer parameters appearing in equation (5.2.1).

on the mirrors causes a polarisation rotation of any non-vertical polarisation component. A non-vertical polarisation mode will not resonate unless the sum of the rotations satisfies the regenerative condition (a polarisation eigenstate).

The cavity therefore has two polarisation modes: a low finesse vertical mode and a high finesse horizontal mode. In either case the output polarisation is purely vertical or horizontal. This design is also known as a *planar ring* cavity.

Using schematics based on a design developed in the Ginzton Labs, Stanford [103], we had the departmental workshop build the ring cavity shown in Fig. 5.8, in order to mode-clean the 1064 nm Mephisto beam. The cavity design parameters are listed in table 5.2.

| Parameter | Value |
|---|---|
| I/O Reflectivities | 0.99999 |
| Loss (per mirror) | 0.001 |
| Path length | 840 mm |
| Waist | 525 $\mu$m |
| FSR | 357 MHz |
| FWHM | 343 kHz |
| Finesse | 790 |

**Table 5.2:** 1064 nm mode cleaner design parameters. The finesse is based on a slightly more rigorous analysis of the cavity than is presented here.[67]

## 5.3 Mode Matching

When a mode of oscillation in one oscillator (free space laser field) excites a mode in another oscillator (cavity field) the two modes are said to be *coupled*. The quality of coupling—how closely the modes match each other, and the extent of loss due to the transfer mechanism—determines how much power is coupled from one to the other. To obtain maximum transmission through a cavity, then, the free space mode must match

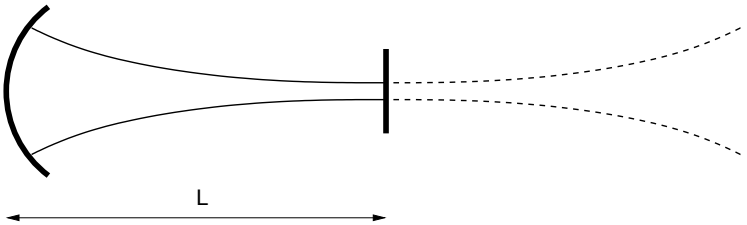


**Figure 5.6**: A half symmetric resonator with effective path length $2L$.

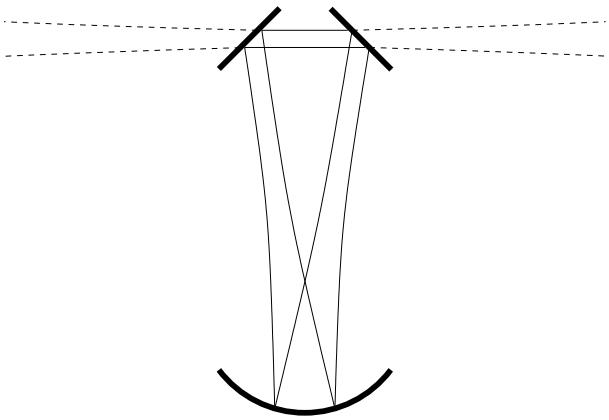

**Figure 5.7**: A triangular resonator.

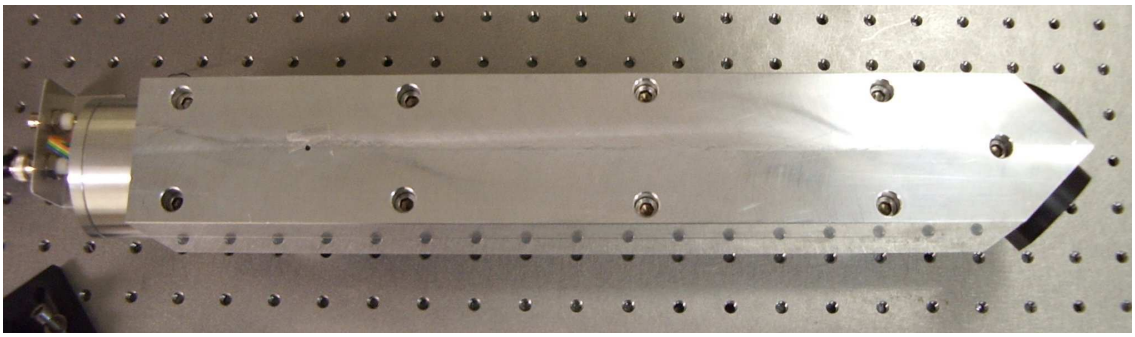

**Figure 5.8**: 1064 nm mode cleaning cavity

the cavity mode as closely as possible, causing the cavity to resonate.

Matching waists (size and position) are required for spatial mode matching - ensuring the beams have the same shape. The lens equations (3.3.2) and (3.3.3) allow calculations to be made for combinations of lenses that will produce the desired waist. Once the lenses have been placed, however, the positioning must usually be fine-tuned by physically measuring the beam waist, adjusting and repeating. It is essential for good cavity transmission that the spatial modes match as closely as possible. Practical techniques of beam waist measurement are discussed in section 5.4.

Since this is a triangular cavity, the input beam must be matched to either low or high finesse polarisation modes. The polarisation of the input beam can be rotated with a half-wave plate.

The cavity length can be piezoelectrically adjusted to phase-match the cavity and free space modes. The length can be either 'scanned', where the mirror is moved back and forth in sawtooth fashion in order to briefly cross a resonance, or it can be 'locked'. In this case electronic feedback is used to keep the cavity length locked on resonance in the face of thermal and laser drift.

This cavity design employs a push-pull piezoelectric transducer (PZT) system (Fig. 5.9), the first such implementation in the department. The goal of the design was to eliminate the low frequency resonance encountered in the past with a single PZT design (low frequency resonances adversely affect locking stability). Section 5.5.2 examines the success of the new design.

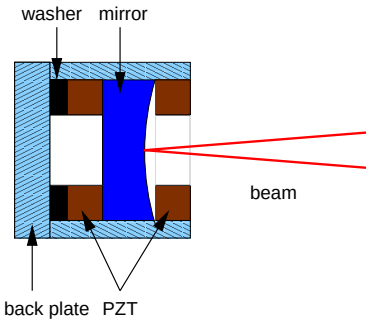


**Figure 5.9:** Piezoelectric push-pull mode cleaner design. The control voltage is reversed on one of the PZT actuators so that one compresses as the other expands.

## 5.4 Spatial Mode Matching

The ability to accurately measure the size and position of a beam waist is crucial to spatially mode matching a free space propagating beam into a cavity. The general procedure for spatial mode matching is listed as follows:

1. Measure waist size and position of beam
2. Calculate position(s) and focal length(s) of lens(es) required to shape measured beam into cavity mode
3. Repeat as necessary

### 5.4.1 Beam Profiling

I used three different methods to make beam waist measurements: CCD camera beam profiling; razor blade curve profile fitting; and razor blade 84-16 power measurement. I settled on the 84-16 method for reasons to be made clear shortly.

Each method only measures the beam width at a particular point $z$ along the path of propagation. A number of such measurements must be made and the waist either interpolated or extrapolated from the data. I wrote a *Mathematica* script to fit such data points to the expression for a Gaussian beam's width

$$W(z) = W_0\sqrt{1 + \left(\frac{\lambda z}{\pi W_0^2}\right)^2} \tag{5.4.1}$$

which produced an estimate of the waist size and position. Fig. 5.10 is example of such a fit.

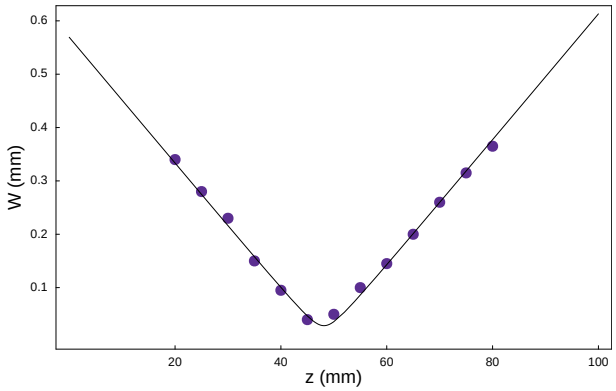


**Figure 5.10:** Beam width measurements fitted to the expression for the width of a Gaussian beam. This set of data measures a fitted waist of 29$\mu$m at $z = 48$mm.

#### CCD Camera Beam Profiling

Using a CCD camera we can examine the cross-profile of the beam at a particular point $z$ along the length of propagation. Software running on the computer connected to the camera can determine the width of the beam in the $X$ and $Y$ axes. The problem with the profiler we used was that it had a small dynamic intensity range at 1064 nm, and so produced values with very high deviation from the width equation (5.4.1).

#### Razor Blade Curve Fitting

After discarding the CCD profiler we mounted a razor blade onto a translation stage (Fig. 5.11). By moving the blade across the beam we can measure the change in power on a power meter mounted behind the blade.

This process corresponds to integration of the Gaussian cross-section, and so, using a

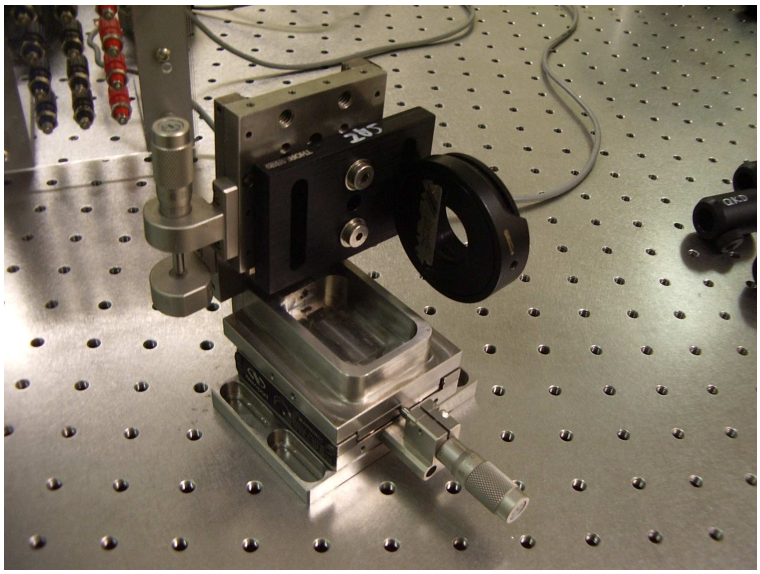

**Figure 5.11:** Razor blade mounted on a translation stage. The blade can be moved across the beam with 10-$\mu$m precision.

*Mathematica* script, power measurements taken can be fitted to the Gaussian integral

$$P(x) = \frac{1}{2}\left(1 - \mathrm{Erf}\left(\frac{\sqrt{2}x}{W}\right)\right) \tag{5.4.2}$$

where

$$\mathrm{Erf}\,(\xi) = \frac{2}{\sqrt{\pi}}\int_0^{\xi} \exp\left(-t^2\right) \mathrm{d}t \tag{5.4.3}$$

is the error function. The beam width $W$ can then be determined from the fit. A sample plot of data and fit is shown in Fig. 5.12.

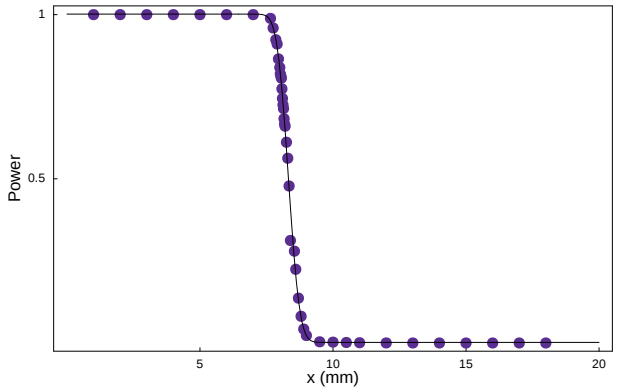


**Figure 5.12:** Power measurements (normalised) taken by moving a razor blade across the beam. The solid line is the fitted curve, in this case finding a beam width of approximately 660$\mu$m.

Once enough beam width measurements have been taken the widths can be fitted to the width equation 5.4.1 to find the size and position of the waist. The main disadvantage of this method is the number of data points required. A single profile measurement can take 20-30 minutes so if five to ten profiles are taken, making a single waist measurement can take several hours. This time is again multiplied by the number of times the waist measurement is revisited after a lens adjustment, to a point where it could be considered an impractical technique.

### Razor Blade 84-16 Power Measurement

Substituting $x = \pm\frac{1}{2}W$ into equation 5.4.2 gives $P = 0.841$ and 0.159. Simply, as the razor blade integrates across the beam the power will be increased to 16% and then 84% of its full value as the blade passes the two points delineating the beam's width. Fig. 5.13 shows these points on the integral curve.

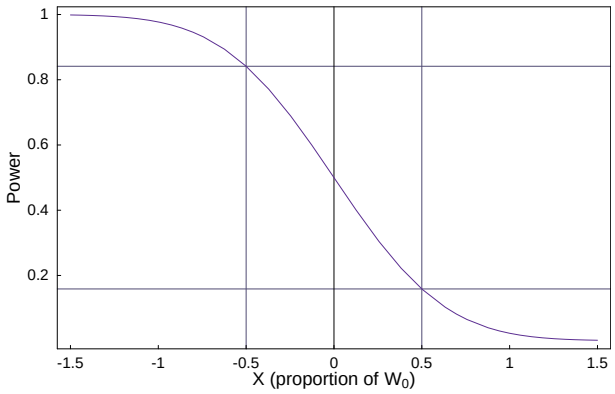


**Figure 5.13:** The distance between the points at which a razor blade blocks 84% and 16% of beam power is the beam width.

The advantage of this method over the curve fit method is the number of data points taken: three (100%, 84%, 16%) instead of many. With some practice we could measure a beam's waist using this method about as quickly as it had taken with the CCD profiler. This method is also accurate—when I compared an 84-16 measurement to a curve fit measurement the difference was only 0.9%.

## 5.4.2 Lens Placement

There are many combinations of lenses that will convert one beam shape into another. When choosing a combination I took two factors into account:

- Total distance between existing beam source and cavity waist
- Rate of change of waist size/position due to change of lens position

The total mode-matching distance should be minimised as much as possible to avoid taking up large amounts of space on the experiment table. Increasing the number of lenses tends to decrease the mode-matching distance, since lenses are only available with

set focal lengths which reduces flexibility in their placement. The rate of change of waist size should not be too flat, otherwise large changes to lens positions are needed to fine-tune the waist size.

I wrote a *Mathematica* script to calculate waist size and position for a two-lens combination. There a number of parameters that can be varied to shape the beam, shown in Fig. 5.14.

By holding $f_1, f_2$ constant I could produce graphs as shown in Fig. 5.15 to find the optimal combination of lens positions for those focal lengths. These graphs were useful in the fine-tuning process as well, since they give an understanding of how the beam will behave under small lens displacements.

### 5.4.3 Alignment

The final step of spacial mode matching is aligning the (now correctly shaped) beam into the cavity. We used an infrared camera while scanning the cavity to observe the output beam while adjusting beam-steering mirrors to align the input beam. Initially the output was a mixture of many TEM modes. With further alignment we could cause the $\text{TEM}_{00}$ to dominate.

Once aligned we recorded the behaviour of the beam reflected from the cavity as the length was scanned, in order to measure the cavity finesse. As it passes through resonance the beam will be coupled in to the cavity, and the reflected power approach zero. Fig. 5.16a is a wide view of the scan, showing a full FSR of the cavity. Fig. 5.16b is a close up of one of the peaks, showing the FWHM.

Several sets of measurements were taken, the most precise being $836 \pm 53$, a range encompassing the design value of 790. Cavity coupling efficiency was measured at 96%.

## 5.5 Feedback Control of Cavity Resonance

Producing a continuous transmitted beam from a cavity requires that it be locked on resonance, even if the cavity length changes or the laser wavelength drifts. The 1064 nm cavity was built from aluminium and so changes in temperature affect its length. This thermal drift can be suppressed by building the cavity from invar - an alloy that does not change size with temperature.

Laser drift is still unavoidable, due to minor temperature changes in the laser resonator. To keep the cavity on resonance the end mirror must be continuously moved to adjust for these changes. The process of continuously adjusting a parameter to achieve a constant outcome is called *control*.

Control theory is covered in standard texts of electrical engineering, see for example [33]. A summary of control theory in the context of quantum optics can be found in [1]. There are four elements to a control system:

**Plant** which is the system to be controlled

**Sensor** which measures some property of the plant

**Actuator** which corrects the state of the plant in response to changes in the sensed property

**Filter** which interprets the sensor signal for the actuator

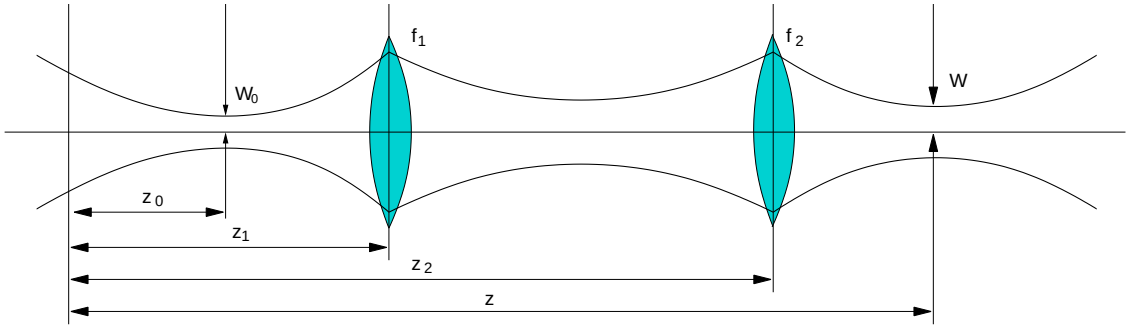


**Figure 5.14:** Beam shaping parameters with a two-lens combination: $z_0$ and $W_0$ are the waist position and size of the beam to be shaped. $z_{1,2}$ are the positions of the lenses and $f_{1,2}$ the focal lengths.

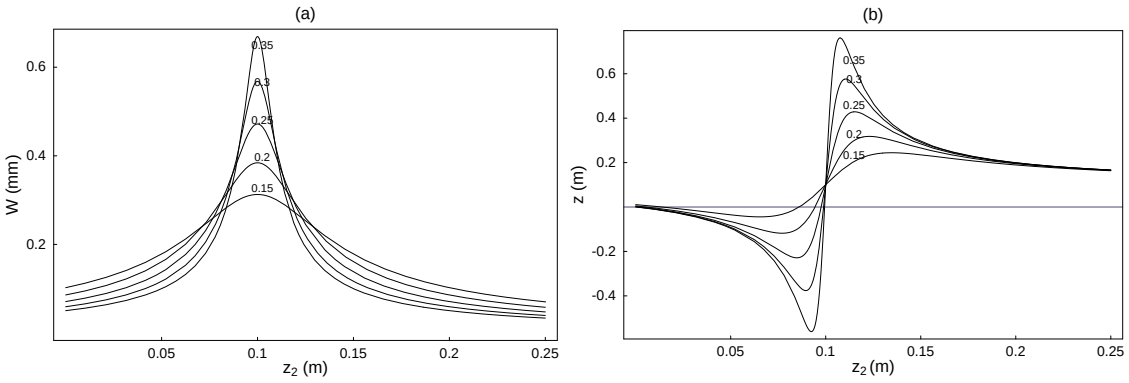


**Figure 5.15:** Graphs showing the effect of two lenses ($f_1 = 75.6$mm, $f_2 = 100$mm) on the beam emerging from the Mephisto laser ($W_0 = 225\mu$m, $z_0 = -980$mm from the front face of the laser) (a) Waist size $W$ against lens 2 position $z_2$, with each curve representing a different position of lens 1 $z_1$ (m). (b) Waist position $z$ against lens 2 position $z_2$, with each curve representing a different position of lens 1 $z_1$ (m).

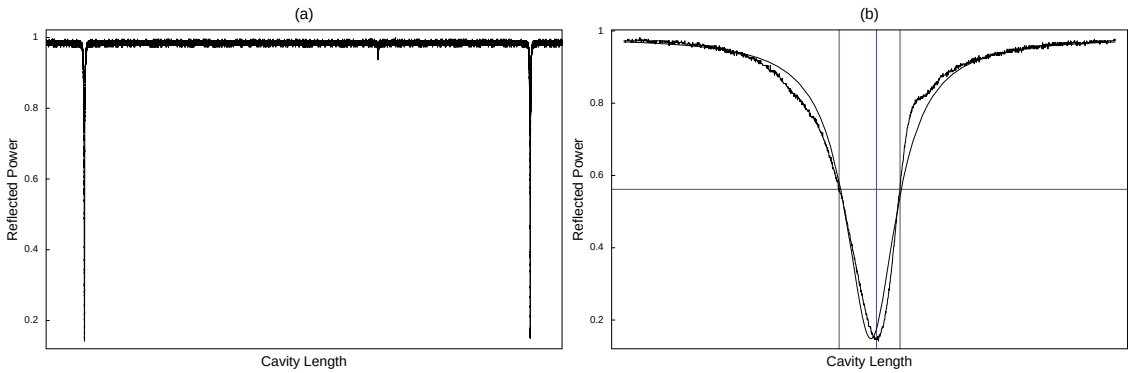


**Figure 5.16:** The cavity finesse can be measured by dividing the FSR (graph a) by the FWHM (graph b). In (b) an Airy function was fitted to the peak to get a more precise result for the FWHM.

In this set up the plant is the cavity length, the sensor is a split photodetector measuring the reflected beam of the cavity, the actuator is the push-pull PZT system and the filter a Proportional-Integral-Differential (PID) gain amplifier. Our work on establishing the sensor and filter is presented next.

### 5.5.1 Sensor: Tilt Locking

The goal of a control sensor is to produce an *error signal*, called so because it indicates how far the plant is from the desired state. An error signal is locally antisymmetric about zero, with zero output when the plant is in the desired state.

The asymmetry means that the error signal will be positive for a disturbance of the plant in one direction, and negative for the opposite disturbance. Thus a disturbance in either direction—say the cavity becoming longer (shorter) than desired—can be corrected with the appropriate action—expansion (compression) of the PZT.

There are a number of techniques for producing an error signal that is a function of the cavity resonant condition. PDH phase locking, described in [26] and [1], is a popular method. An alternative that requires less equipment is *tilt locking*[90][1] which was the method used here.

Although the cavity can be aligned to cause almost complete domination of the $TEM_{00}$ mode, a slight misalignment in the horizontal plane will cause a small amount of $TEM_{10}$ circulating field. Since this mode is far off resonance it will be entirely reflected by the cavity, and can be directed onto a split photodetector with the two lobes of the mode aligned to the two halves of the detector (Fig. 5.17).

The split detector can produce a difference signal of the intensity measured by its two halves. The modal interference conditions in the cavity are such that when it is resonating on the $TEM_{00}$ mode, the two lobes of the rejected $TEM_{10}$ mode have equal amplitude and the split detector difference signal is zero.

As the cavity drifts off resonance, one $TEM_{10}$ lobe will decrease while the other increases. The bias direction is dependent on the side of the resonance to which the cavity drifts. The difference signal from the split detector will therefore be positive for one direction of drift and negative for the other—an error signal. Fig. 5.18 is an example of the

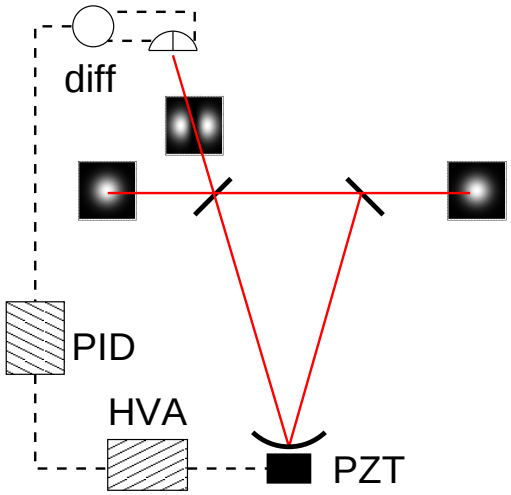


**Figure 5.17:** Tilt locking: The difference output on the split photodetector is an error signal dependent on $TEM_{00}$ resonance. The PID and High Voltage Amplifer (HVA) act as the filter to convert the detector error signal into a PZT voltage.

error signal obtained from this cavity.

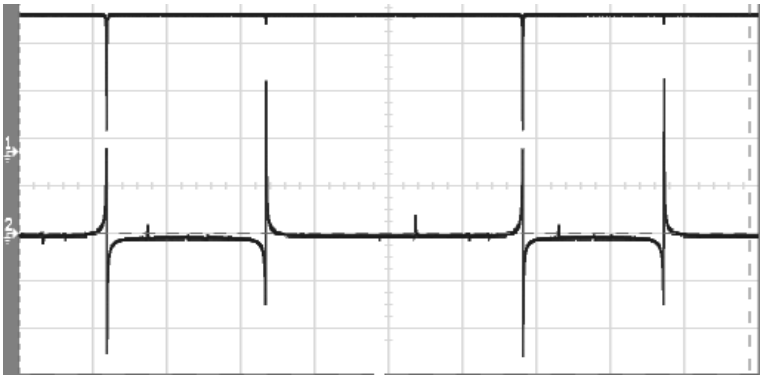

**Figure 5.18:** The tilt lock error signal. The top graph is the sum signal from the split detector, with both $TEM_{00}$ and $TEM_{10}$ modes visible. The bottom graph is the difference signal. The error signal as the cavity scans over its $TEM_{00}$ mode is asymmetric about zero, with the zero corresponding to mode resonance, as required. The $TEM_{10}$ mode also produces an error signal, with opposite polarity.

### 5.5.2 Filter: PID Controller

Once we could reliably produce an error signal from the split detector, the final step was to ensure the PID produced a good quality control signal to the push-pull PZT actuator. The PID is an amplifier with integrated gain at low frequencies, proportional gain at middle frequencies and differential gain at high frequencies.

The gain must also roll off at high frequencies, be suppressed at any resonant frequencies of the actuator system, and have a less than $\pi$ phase shift at the unity gain point.[1]

The unity gain point is the point in frequency space at which the gain value has decreased to 1. The frequency-dependent nature of impedance, however, means a high frequency signal travelling through the circuit will be phase shifted—possibly greater the $\pi$ at the unity gain frequency. Consequently, PID design is a complex process and a generic PID must be customised to a particular system—as we discovered.

Our initial attempts to mode-lock the cavity found the locking to be unstable. To analyse the system we built a Mach-Zehnder interferometer (Fig. 5.19) and chirped the mode cleaner PZT (a 'chirp' is a sinusoidal signal with linearly increasing frequency over time). The motion response of the mirror was recorded with the data acquisition system. The Fourier transform of this response, divided by the Fourier transform of the chirp signal, is called the actuator *transfer function*. The plot is shown in Fig. 5.20.

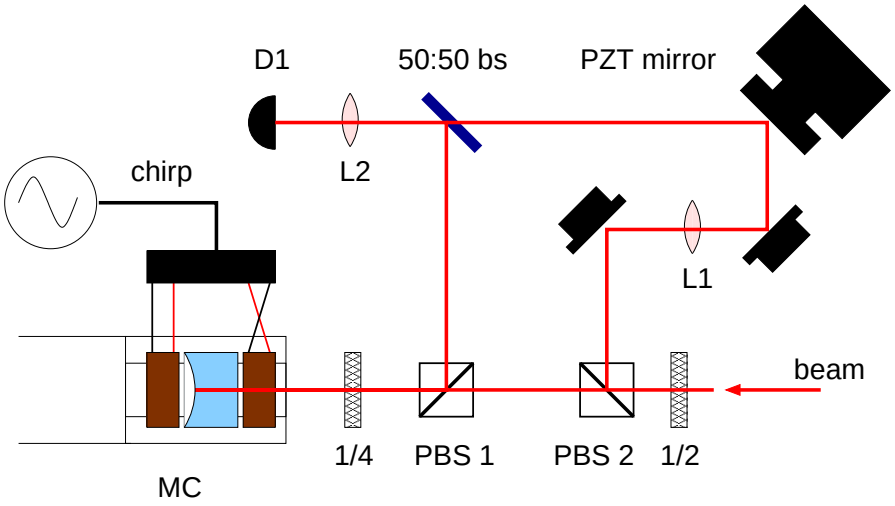


**Figure 5.19:** Mach-Zehnder for analysing mode cleaner mirror motion. Lens L1 is placed to counteract the diverging effect of reflecting the beam from the back of the mode cleaner mirror. The PZT mirror was manually adjusted to keep phase lock for the duration of the chirp. The resulting intensity variations on D1 are proportional to the mode cleaner PZT displacement.

It can be seen from Fig. 5.20 that the first actuator resonance was recorded at 17 kHz. This was a disappointing result since other single-PZT mode cleaners built in the department have had first resonances of up to 25-30 kHz. The push-pull system was not performing as hoped.

The next step of analysis was to measure the transfer function of the PID, to see if it satisfied the conditions described earlier. We used a network analyser to observe amplitude and phase response across the kHz spectrum and saw that the PID we were using, in its current configuration, did not adequately suppress the 17 kHz resonance. This meant that as the error signal oscillated about zero, the 17 kHz component was greatly magnified and caused the cavity length to move out of the error signal locking region.

### Elliptic Filter

Part of the PID circuit uses an elliptic filter to suppress such PZT resonances. An elliptic filter suppresses a small part of the spectrum with a very sharp roll-off (see Fig. 5.21)—an elliptic function. The circuit component values must be carefully chosen for the

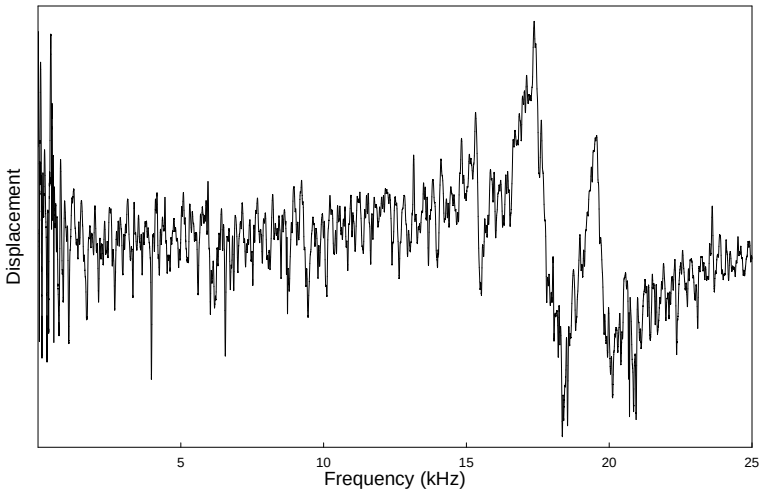


**Figure 5.20:** Frequency plot of the mode cleaner PZT motion in response to a chirp signal—the actuator transfer function. The resonance is at 17.4 kHz.

filter to perform as desired (design and values can be found in tables from electronics textbooks).[45][88]

We replaced the components in the PID elliptic filter with values generated from a programme provided by James Dickson, and reanalysed the transfer function. Numerous iterations of the filter were required before a suitable transfer function could be produced.

In the early designs we did not pay enough attention to finding precise component values, resulting in a badly-matched filter that oscillated at 10 kHz. Later designs featured a $\pi$ phase delay before the unity gain point, also causing locking instability. Finally we produced the transfer function shown in Fig. 5.21.

#### Butterworth Filter

At this point the PID suppressed the actuator resonance, but it still did not roll off quickly enough at high frequencies for locking to be stable—a 40 kHz resonance seemed to be causing further problems. The PID circuit design incorporates a low-pass filter which we did not change. I built an additional low-pass Butterworth filter external to the circuit, with roll-off beginning at 18 kHz, to suppress high frequency actuator oscillations.

The circuit design, and component values, was obtained from [45] and is shown in Fig. 5.22 with the transfer function in Fig. 5.23. With the addition of this filter, our cavity locking became stable enough for the experiment to continue.

### 5.5.3 Final Comments on Mode Locking

A number of other problems came up during our work on locking the cavity. The PID had too much gain and so the amplifying circuits needed to be adjusted. The cavity end cap design has a plate that is screwed to the end cap against the back PZT (Fig. 5.9). We believe this plate was 'rattling', causing the 17 kHz resonance.

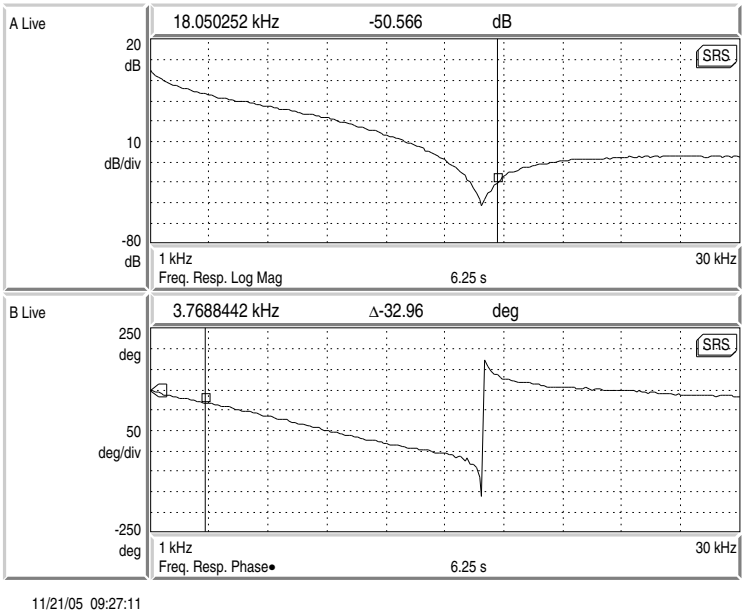


**Figure 5.21:** Elliptic band-pass filter transfer function. 'A Live' shows the amplitude response, with the maximum suppression at approximately 17 kHz. 'B Live' shows the phase response, with a unity gain phase delay of approximately $\pi/2$.

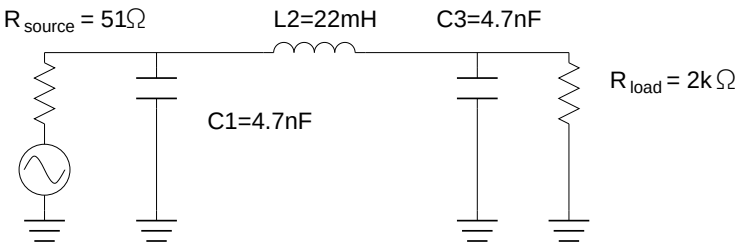


**Figure 5.22**: Circuit diagram for low-pass Butterworth filter, 3-pole $\pi$-configuration.

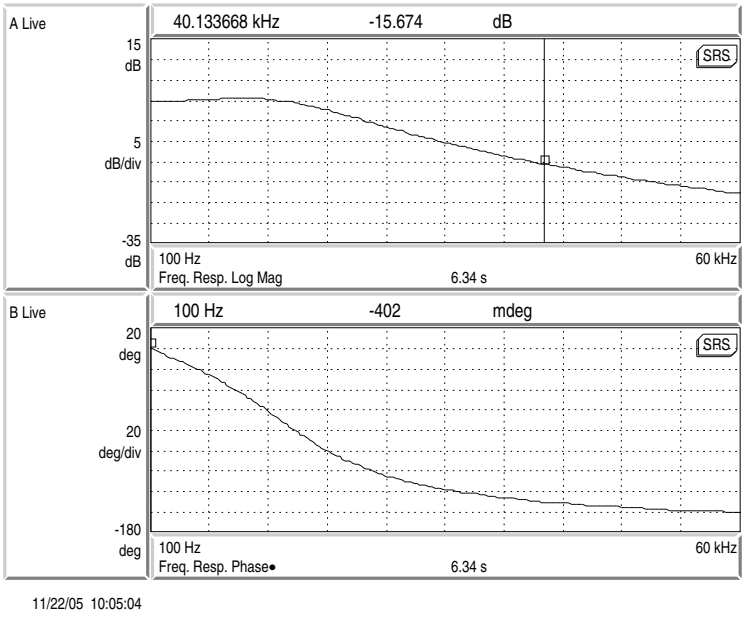


**Figure 5.23:** Butterworth low-pass filter transfer function. 'A Live' shows the amplitude response, with 3 dB roll-off at approximately 18 kHz and 15 dB supression at 40 kHz. 'B Live' is the phase response, showing a smooth, gradual increase in phase delay along the spectrum.

We worked on tightening the back plate, although this had to be done very carefully since uneven tension on the screws tilted the mirror, causing the beam to be clipped by the walls of the cavity. The tightening had to be done while observing the cavity transmission with an infrared camera.

Unfortunately, the Mach-Zehnder interferometer used to analyse the mode cleaner transfer function had been dismantled before we tried to improve the back plate—the transfer function of Fig. 5.20 was measured before the back plate was tightened. It is likely that the first resonance has increased since tightening, possibly to a level higher than can be obtained with a single-PZT actuator (this also means that the elliptic filter in its current configuration is probably not doing very much). The verdict on the push-pull system must remain inconclusive for the time being, since the problems we had with this cavity put us many weeks behind schedule. Now that we could lock it, although not perfectly, we immediately continued on to the main experiment.

paragraph on how well it cleaned the beam, graph of variances at different frequencies against theoretical curve

## 5.6 Summary

This chapter has described the sources and effects of optical quadrature noise. The relaxation oscillation of the Mephisto 1064 nm laser was measured with and without the noise-eating circuit. The quantum noise limit for quadrature measurement was calculated.

It was shown that resonant cavities offer the ability to mode-clean an impure coherent state. Generally the quadrature variance of a laser will approach the quantum noise limit with increasing modulation frequency. A cavity can speed this approach so that the beam

becomes effectively quantum noise limited at a lower frequency. The functional behaviour of the roll-off is determined by the cavity finesse.

To increase the purity of the laser coherent state from the previous generation QKD experiment, a mode cleaning cavity was built by the departmental workshop. The cavity featured the first push-pull actuator built in the department, although results proving the advantage of this design are still inconclusive.

The techniques employed for the subsequent mode-coupling effort are described. The coupling resulted in 96% transmission through the cavity, and a measured finesse of $836 \pm 53$, which compared well to the design value of 790.

Mode locking was undertaken with the tilt locking technique, using a departmental PID design. Stable locking was achieved only after numerous iterations of PID circuit component values, principally the elliptic filter design. At this point the quadrature variance was not available, as the remainder of the experiment needed to be running to make this measurement.

Chapter 6

# Second Generation CVQKD-SQM

This chapter details the layout, conduct, results and analysis of the second generation SQM experiment. As described in Chapter 5, the Mephisto laser was mode-cleaned with a high finesse optical cavity. The cleaned beam was then used to rebuild the first generation experiment with higher-bandwidth electronics.

Once the experiment was built, the beam was amplitude- and phase-modulated with white noise from Agilent function generators. These were shown to be inadequate for the task and a trial quantum random noise generator was used. Alice's modulations and Bob's received signals were simultaneously sampled at 200 Mbps. The data was analysed with a modified version of the analysis and post-selection code used for the first generation experiment. Frequency division multiplexing was introduced into the analysis to counter the effects of nonconstant gain across the spectrum.

## 6.1 Experimental Design and Methods

The design of the first generation experiment is broadly described in [56] and reported with greater detail in [94]. Apart from the addition of the mode cleaner, detailed in Chapter 5, the experiment remained largely the same. The mixing, locking and modulation techniques described below are unchanged from the first experiment. The distance between Alice and Bob was slightly shorter than in the first experiment (30 cm as opposed to 1 m) due to it being built on a smaller table.

Initially the same detectors were also used. These detectors had a low frequency roll-off from 30 MHz and a nonflat response between 33 and 50 MHz. This response meant it was necessary for the detector transfer function to be characterised and applied to the sampled data.[56] Halfway through the experiment we replaced the detectors with a new design by James Dickson. The new detectors have a flat response to 400 MHz and low frequency roll-off from 10 MHz down. Our characterisation is reported below.

The data acquisition system used in the first generation experiment had a 100 Mbps sample rate. This was replaced with a 200 Mbps system. Thomas rewrote the LabView acquisition programme to improve sampling performance and usability.

### 6.1.1 Table Layout and Optical Alignment

The layout of the experiment optics is depicted in Fig. 6.1. The electronics are described in section 6.1.2, so the discussion in this section will be limited to the purpose and alignment of the optics.

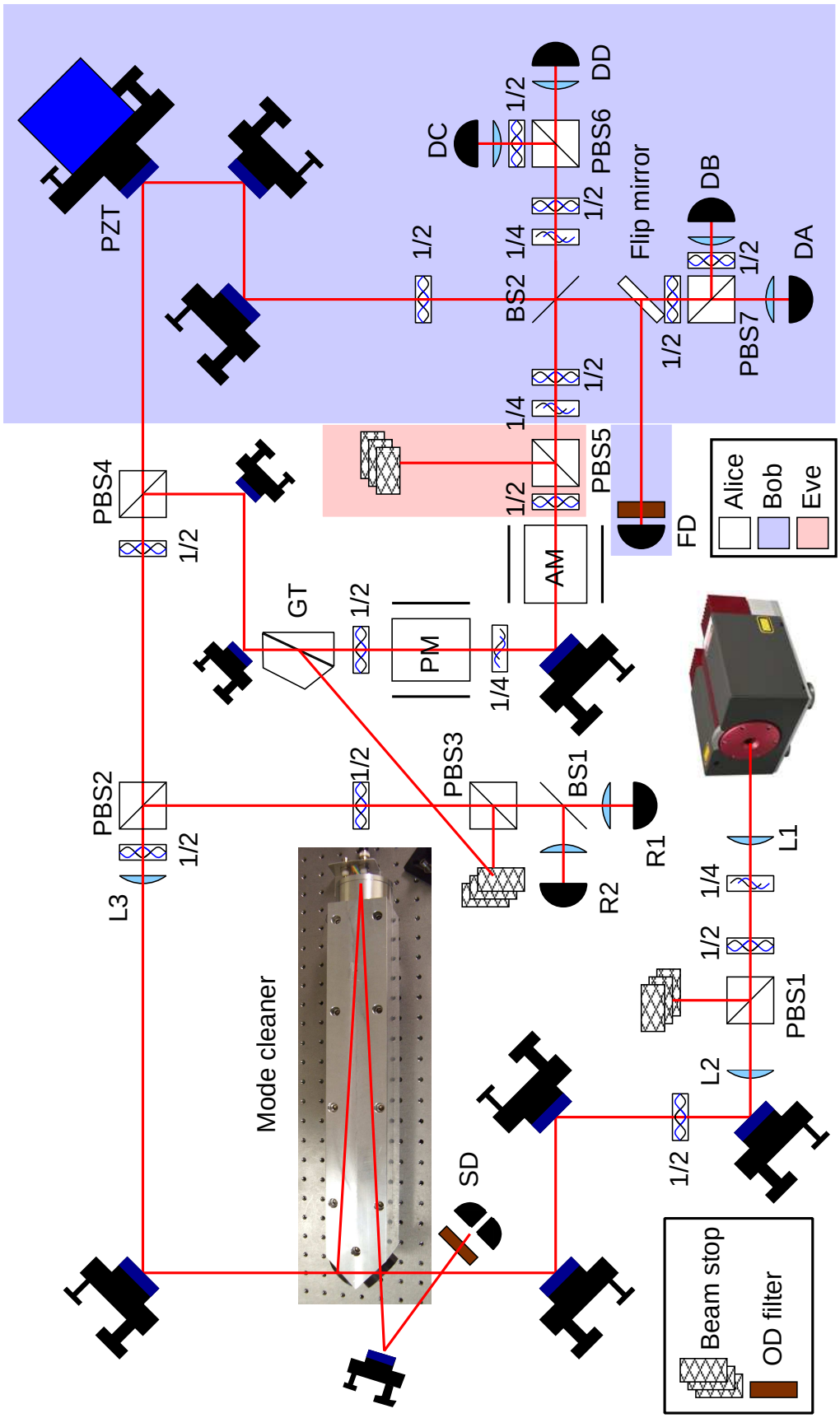


**Figure 6.1**: Optics layout of the second generation experiment.

**Alice**

Alice obtains laser light with the Innolight Mephisto 1200NE laser described in section 3.2. We powered the diode with 1.8 A of current and kept a crystal temperature of 24.7°C. This combination is in the centre of a single-mode temperature regime for the laser (Fig. 3.9). The beam from the Mephisto had a slightly elliptical polarisation which is linearised by the quarter-wave plate following L1.

At 1.8 A of pump current the laser produces approximately 1 W of optical power (Fig. 3.8). PBS1 is used to dump some of this power, since reducing the diode current any further from the maximum of 2.4 A risks entering a regime of unstable laser operation. Ultimately Alice only requires 40 mW of power since Bob's detectors are in danger of saturating past 10 mW.

The lenses L1 and L2 are used to shape the beam for in-coupling to the mode cleaner (section 5.4). The mirrors following L2 are used to spatially align the beam to the mode cleaner. The half-wave plate is used to align the polarisation of the beam to the the vertical (low-finesse) mode of the cavity. Although vertical polarisation is emerging from PBS1, minor imperfections in the table, cavity mirror mounts and PBS mean it must be adjusted slightly for maximum transmission. The half-wave plate can also be used to access the high-finesse horizontal mode of the cavity.

The split detector SD, measuring the reflected beam from the mode cleaner in-coupling mirror, is used for the tilt locking (section 5.5.1). The locking loop is shown in Fig. 5.17 and again in Fig. 6.8. The characteristics and operation of the mode cleaner are described in Chapter 5. In theory the beam exiting the cavity is quantum noise limited to relatively low frequencies.

Lens L3 is used to re-shape the beam, in order that its new waist be between the modulators and the beam wavefronts through the modulators be as near-planar as possible. If the wavefronts are significantly non-planar then different parts of a given wavefront will be modulated differently, due to the phase delay. This will in turn cause unintended ellipticity in the beam and inefficient modulation.

PBS2 was initially used to dump more power from the beam so that Bob's detectors were not saturated. There are two reasons why we used a multi-PBS power-dumping system. Firstly, changing the power entering the cavity often caused it to lose lock, and so we required a means of changing Alice's power without having to relock the cavity every time. Secondly, if PBS1 was used to highly attenuate the beam, then the bad polarisation (section A.2) becomes a significant component of the beam. By using multiple PBS to gradually attenuate the beam this can be avoided.

After finding the Agilent noise function generators to be inadequate for modulation to 100 MHz, we installed a pair of detectors for measuring the quantum noise on the beam exiting the mode cleaner. The flat response of the detectors and good *shot noise clearance* (the power difference between detected quantum noise and detector electronic noise) made them suitable as broadband quantum noise generators. Section 6.1.2 discusses this further. PBS3 then became the second stage of power dumping, while detectors R1 and R2 provide the initial white noise for Alice to send to Bob.

PBS4 is used to split the signal from the local oscillator. When distributing key, the local oscillator contains about 38 mW while the signal contains 0.5 mW. Each day that the experiment is run, however, it must first be aligned. Aligning the modulators requires that the signal have full power, so during alignment it contains about 40 mW. The bad polarisation in the signal from PBS4 is cleaned by the subsequent Glan-Thompson prism.

The Linos Gsanger phase modulator is very sensitive to input polarisation. To align it, a large sine modulation is applied and the sum signal from a subsequent balanced detection is displayed on a spectrum analyser. For convenience we used Bob's AB pair of detectors, but in a complete implementation Alice would have to build her own balanced detection to check her alignment. The displayed signal from the balanced detector is the amplitude modulation being produced by the phase modulator. By adjusting the modulator mount and input half-wave plate this signal can be minimised.

Misalignment of the modulator causes the beam to be unevenly modulated, resulting in ellipticity and unwanted amplitude modulation. Similarly with the input polarisation adjusted by the half-wave plate. It should be noted that in changing the input polarisation there are two minima of amplitude modulation—one is when the beam is orthogonally polarised to the modulation axis and very little modulation is actually occurring. The other is when the modulator is producing as pure PM as possible, which is the required situation for our experiment.

The beam exiting the modulator is linearly polarised and so only requires a quarter-wave plate to create the circular polarisation required for amplitude modulation. The amplitude modulator is identical to the phase modulator apart from a small PBS glued to the end. As described in section 3.1 this combination is adequate for producing amplitude modulation. The amplitude modulator cannot be immediately aligned since the homodyne detection must be locked to distinguish between amplitude and phase. After the amplitude modulator, the signal beam leaves Alice's station. The local oscillator is a phase reference for Bob and it is transmitted directly to him after being split from PBS4.

### Eve

PBS5 attenuates the signal beam to simulate the channel losses of long distance communication. As described in section 4.3.2, all such channel losses are given to Eve when distilling the secret key. Therefore PBS5 also simulates Eve's optimal noncollective attack of replacing the lossy transmission line with her own lossless line, passing on the equivalent amount of signal expected by Bob for the lossy line, and measuring the remainder to increase her information. We do not simulate any of Eve' noncollective active attacks since they have been shown to be nonoptimal.[107] We cannot currently investigate a collective attack since we do not have access to a suitable quantum memory.

### Bob

Bob's detection system is a double-homodyne for simultaneous detection of amplitude and phase quadratures. The signal and local oscillator are equally split by BS2. The two half-wave plates prior to BS2 are used to give the signal and local oscillator orthogonal polarisations. The quarter-wave plate on the signal is used to linearise any ellipticity remaining from imperfect alignment of the modulators.

The orthogonal polarisation is needed to prevent the signal and local oscillator from mixing on BS2. Any parallel polarisation components will be demodulated in accordance with equation (3.4.10), causing the AM component to leak onto the phase homodyne and vice versa. The flip mirror and detector FD are used to check for mixing on BS2. By scanning the PZT and applying equal power to the signal and local oscillator beam we can check the maximum *fringe visibility* of BS2. The PZT scan allows a complete cycle of local oscillator phase $\phi_{lo}$. If any mixing is present then dark and bright fringes on detector

FD will appear, as the beams cycle through constructive and destructive interference conditions.

Despite the risk of premature mixing on BS2, this arrangement is quite efficient in that Bob does not need a local oscillator, with individual phase control, for each homodyne. Checking the BS2 fringe visibility is part of the alignment process for Bob's station. Concurrently we also must maximise the fringe visibilities on PBS6 and 7. It is on these beam splitters that the quadrature demodulation occurs. Continuing to scan the PZT we use the mirrors following it to align the local oscillator with the signal. By displaying any DC output of the four detectors DA,DB,DC,DD we can calculate the fringe visibility by the formula

$$\frac{V_{max} - V_{min}}{V_{max} + V_{min}}, \tag{6.1.1}$$

where $V$ is the DC voltage on the detector. 100% visibility results when $V_{min} = 0$, complete destructive interference from the beams being perfectly aligned and out of phase. Typically we could obtain 96–97% visibility, the remaining unmixed components mainly due to imperfections in the wave plates. The quarter-wave plate before Bob's CD detector pair is used to create a quarter-wave phase difference between the signal and local oscillator. Since post-BS2 the polarisations of the signal and local oscillator are still orthogonal, the quarter-wave plate can be rotated so that only one beam is delayed. Therefore the essential phase difference for demodulating PM information can be introduced (section 3.1). Fig. 6.2 shows how polarisation propagates through Bob's station.

Finally, the combined but unmixed beams are rotated to 45° so that they are equally split by PBS6 and 7 onto detectors DC,DD and DA,DB respectively. During alignment the rotation angle must be checked in order to balance the detectors. This is achieved by applying broadband noise to the amplitude modulator and viewing a large section of spectrum of the difference signal from each detector pair (without the local oscillator). If the detectors are balanced the difference signal will approach the quantum noise detected by the pair (which can be accessed by displaying the difference signal without any modulation). The half-wave plates prior to PBS6 and 7 must be rotated to minimise the difference signal.

When the experiment is running, the local oscillator and signal are mixed on PBS6 and 7 so that the AB pair measure the demodulated amplitude quadrature, and simultaneously the CD pair measure the demodulated phase quadrature.

### 6.1.2 Electronics and Data Acquisition

This section covers the electronics controlling and supporting the experiment, and how data is taken.

#### Detector Characterisation

On receiving our new detectors we checked the linearity of their response to changes in optical power. We did this by detecting a broadband noise amplitude modulation and examining the DC response to changes in noise power. The resultant graphs, Fig. 6.3, show that the detectors respond linearly to changes in optical power across a large part of the spectrum.

We found the shot noise clearance of the detectors to be approximately 14 dB across our spectrum of interest. The clearance can be seen in Figs. 6.5 and 6.6. High clearance is important since Bob is detecting weakly modulated states, very close to the quantum

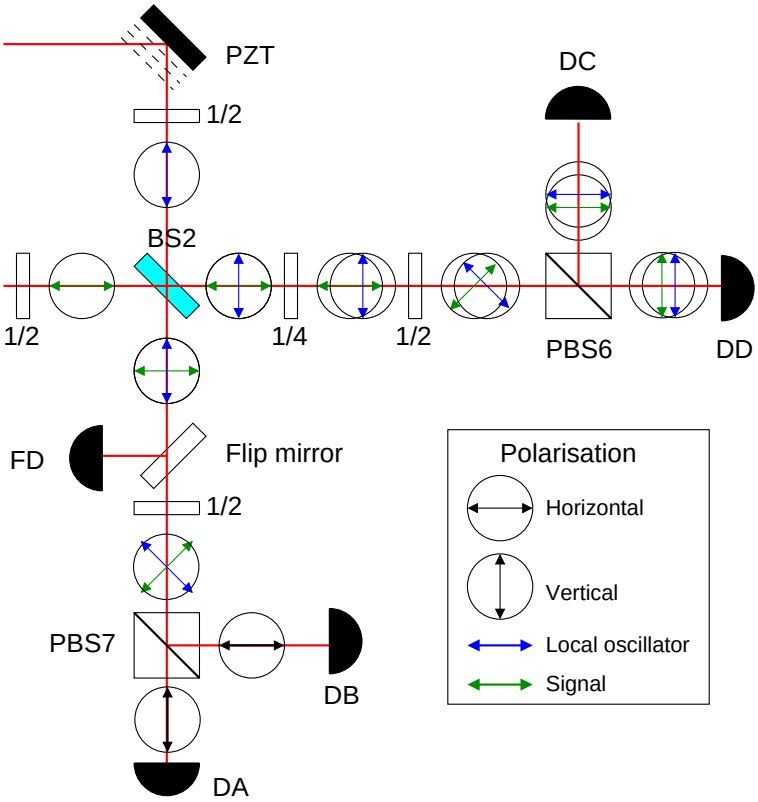


**Figure 6.2:** Polarisation mixing for simultaneous quadrature demodulation in Bob's station. Bob begins by rotating the signal and local oscillator to orthogonality. They are then equally split on BS2. For amplitude detection with the AB detector pair, the combined but unmixed beams are rotated to 45° so that they are then equally split onto detectors DA and DB. The polarisation splitting causes a component of each of the diagonally polarised beams to mix, demodulating them prior to detection. For phase detection one of the beams is delayed by a quarter-wavelength before a similar process occurs.

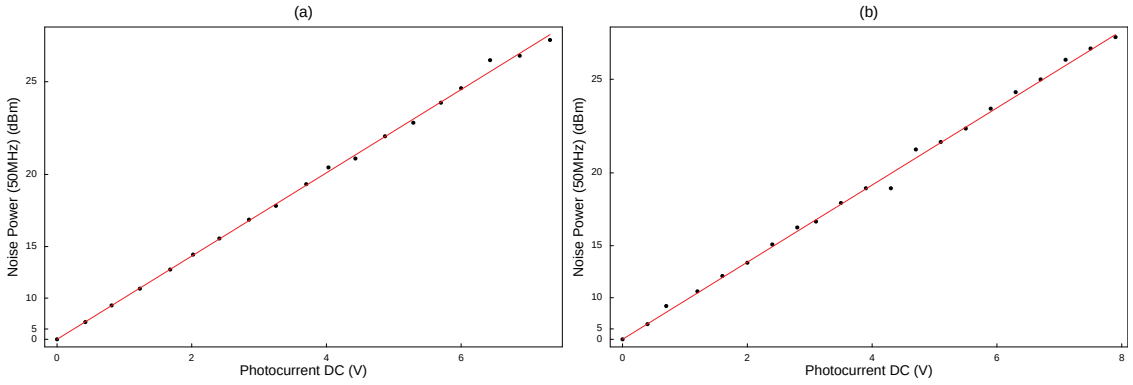


**Figure 6.3:** Characterised linearity of our new detectors. We applied a broadband noise amplitude modulation to the beam and measured the DC response to the noise power. The graphs show that the detectors respond linearly to broadband changes in optical power. (a) AB pair (b) CD pair.

noise level. The data rate would drop significantly if his measurements were contaminated with the electronic noise of his detectors.

It can also be seen in Figs. 6.5 and 6.6 that the detectors have a very flat response across our spectrum of interest.

### Noise Modulation

An analysis of the post-selection information advantage equation (4.3.4) reveals that for a particular channel transmission $\eta$, the information advantage $\Delta I$ is a function of Alice's noise modulation variance $V_A^{\pm}$. Therefore for a given $\eta$ there is an optimal noise power, shown in Fig. 6.4. In the experiment the modulation should be set to this optimal level before sampling data.

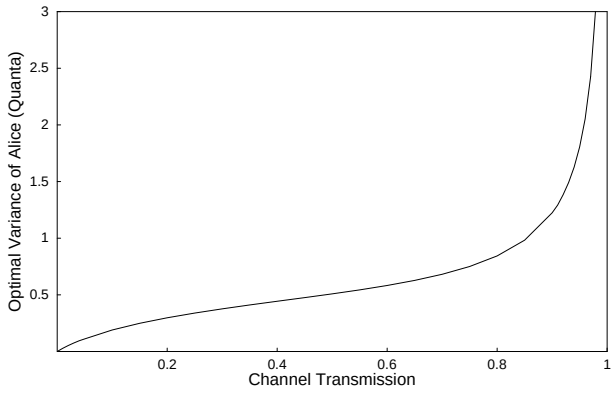


**Figure 6.4**: Alice's optimal modulation noise variance against channel transmission.

Fig. 6.5 shows the full 100 MHz acquisition spectrum of noise signal, shot noise and detector dark noise when Alice is using an Agilent function generator to send broadband noise on the amplitude quadrature. The flatness of the detector response to the quantum noise is in marked contrast to the roll-off of the function generator from 30 MHz. Since under normal operation Alice sends weakly modulated states, this 12 dB roll-off made using the higher part of the spectrum unfeasible.

Section 2.3 describes how any cryptographic key must be drawn from a high-entropy source. A continuous variable quantum random number/noise generator (QRNG) offers the possibility of high-bandwidth random number generation from quantum vacuum fluctuations. After trying several combinations of amplifiers we found that the quantum noise detected by one of our new detectors could be amplified to the required levels for Alice's quadrature modulation (Mini-Circuits ZFL-500 preamplifier followed by a ZHL-1A high power amplifier). We needed to put a 100 MHz low-pass filter before each amplifier since with such wideband noise amplifier saturation is reached at relatively low powers. Fig. 6.6 shows Bob's detected phase quadrature with Alice phase-modulating quantum random noise.

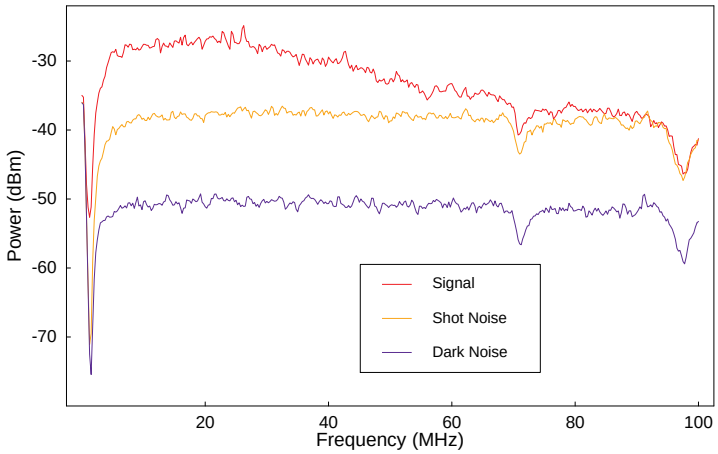


**Figure 6.5:** Bob's detected signal while Alice modulates the amplitude quadrature with broadband noise from the Agilent function generator. The sharp dips in power between 70 and 100 MHz are an unwanted characteristic of a filter in the detection electronics, and can be neglected. The graph of Bob's detected shot noise also displays the flatness of the detector response.

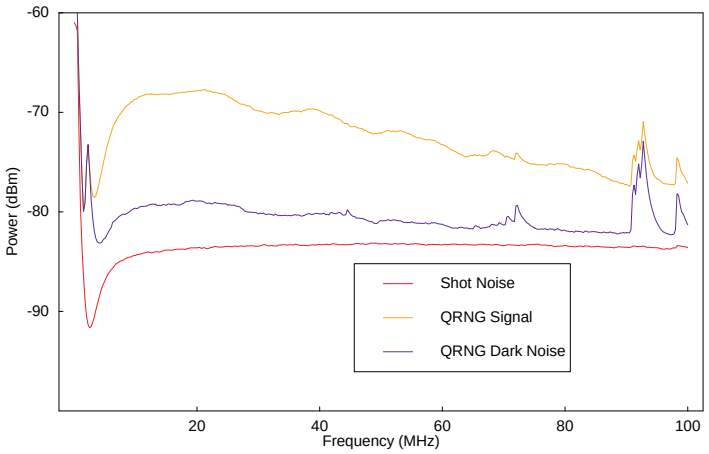


**Figure 6.6:** Bob's detected signal while Alice modulates the phase quadrature with detected quantum noise from the beam exiting the mode cleaner cavity. The remaining roll-off towards higher frequency is due to the modulator. The QRNG detector was not RF shielded at the time, and so the FM radio interference is present on the signal. Bob's detectors are shielded and so without the modulation (his detected shot noise), his spectrum is free of the interference.

### Interferometer Locking

Section 3.4.5 comments that vibrational and thermal noise can cause the phase of a homodyne's local oscillator to drift. Active feedback phase control is required in Bob's station of Fig. 6.1, to keep the signal and local oscillator in phase prior to beam splitter BS2. After BS2 the local oscillator and signal are mixed for amplitude detection by the AB detector pair, and simultaneously one beam is delayed by a quarter-wave for phase detection by the CD detector pair.

Phase control of the local oscillator can be achieved by inserting an additional phase modulation into the signal beam (recalling the electronic pictured in Fig. 3.17). The frequency of this locking signal must be outside of the information modulation band, or the information modulations would interfere with the locking (we used 2.1 MHz). The phasor diagram in Fig. 6.7 describes the effect of this phase modulation over a full scan of the phase difference between signal and local oscillator.

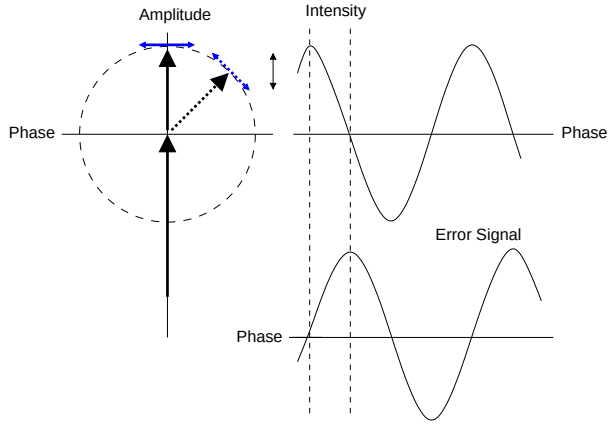


**Figure 6.7:** Phasor diagram of signal and local oscillator. For clarity the size of the signal and locking modulation have been exaggerated. It can be seen that as the signal phasor rotates with respect to the local oscillator, the phase difference produces a change in the DC intensity of the detected photocurrent. More importantly, the pure PM of the locking modulation transitions to AM, resulting in a nonzero error signal at the locking modulation frequency. The error signal can be used to lock the signal to the local oscillator, or vice versa.

When the signal and local oscillator are out of phase the locking modulation becomes a mixture of PM and AM. The AM is detected and becomes a modulation on the detector photocurrent at the locking signal frequency. The phase difference also causes the DC photocurrent to vary, as shown by the intensity plot in Fig. 6.7. Using a mixer the original locking signal down-mixes the modulation to a DC voltage—the error signal. The error signal is zero if the local oscillator and signal are in-phase (or a half-wave out of phase, which for demodulation purposes is equivalent—see section 3.1). The error signal quickly becomes asymmetrically non-zero if a phase difference is introduced. Connecting this error signal to a suitable PID controller, Bob can use the PZT shown in Fig. 6.1 to lock the local oscillator to the signal.

Fig. 6.8 shows the full layout of the experiment electronics linked to the systems shown in Fig. 6.1. Once Bob's interferometer is locked the cross-modulation suppression must be checked. If Alice's modulators are well-aligned then the amplitude (phase) modulator will produce minimal PM (AM). The phase modulator can be aligned by minimising its

output AM; the amplitude modulator requires a locked homodyne to detect the output PM to be minimised. The cross modulation suppression can only be checked with the interferometer locked—the last point before running the experiment.

The cross-modulation suppression must be as large as possible. If a large portion of the information Alice was sending over the phase quadrature leaked onto the amplitude quadrature, then it follows that the quadratures will display some correlation. In this case the security of the key distribution is lost, since Eve can measure each cross-quadrature without affecting the corresponding signal quadrature. With or without switching such a situation is disastrous for performing secure QKD.

Our typical values of cross-modulation suppression are shown in Fig. 6.9. The amplitude suppression of 24 dB is well below the shot noise clearance of Bob's detectors (14 dB), meaning the dominant non-signal component of Bob's measurement is his detectors' own dark noise. This noise is also independent of Eve (and Alice) and so will not introduce any unbounded correlations with Eve, as would occur if the cross-quadrature component was significant compared to Bob's dark noise.

#### Data Acquisition

For the key distillation to be successful Alice and Bob's data must be synchronised, meaning they agree on the time at which a particular bit was sent. Otherwise they will end up trying to distil key from a highly uncorrelated set of data. The propagation delay through Alice's transmission and Bob's detection systems must be taken into account, and one party must advance or delay their data appropriately.

Since we used a single acquisition system (National Instruments PXI-5124) to record both Alice and Bob's data, we used a software delay combined with a physical delay box to give the greatest synchronisation freedom possible. The acquisition software can measure the correlation coefficient of sampled channels (Fig. 6.10). By adjusting the delay settings we optimised the correlation coefficients of the channels to approximately 0.7 for each quadrature.

Once all optics had been aligned we attenuated the signal beam to simulate channel loss, applied the appropriate amount of noise to the modulators and sampled the data, which could then be post-processed by the key distillation algorithms described in Chapter 4. Our results are reported in section 6.2.

## 6.2 Analysis

The data analysis algorithms we used were recycled from the first generation experiment. They consist of *Mathematica* notebooks for calculating the quadrature variances and subsequent information advantage $\Delta I$. Thomas made some improvements to the code and I added a demultiplexing stage which will be explained below.

Analysing the 100% transmission data allows calculation of the system transfer functions, from Alice's white QRNG noise to Bob's detected quadrature signals. They are displayed in Fig. 6.11, showing slight roll-offs in gain and flat phase responses for frequencies over 20 MHz.

We discovered too late that the acquisition system features a software anti-aliasing filter that causes the acquisition gain to decrease from 60 MHz upwards. Above 80 MHz the low signal level caused the detection resolution to be too low for effective data processing. The filter can be removed by reprogramming the core operating software for the acquisition

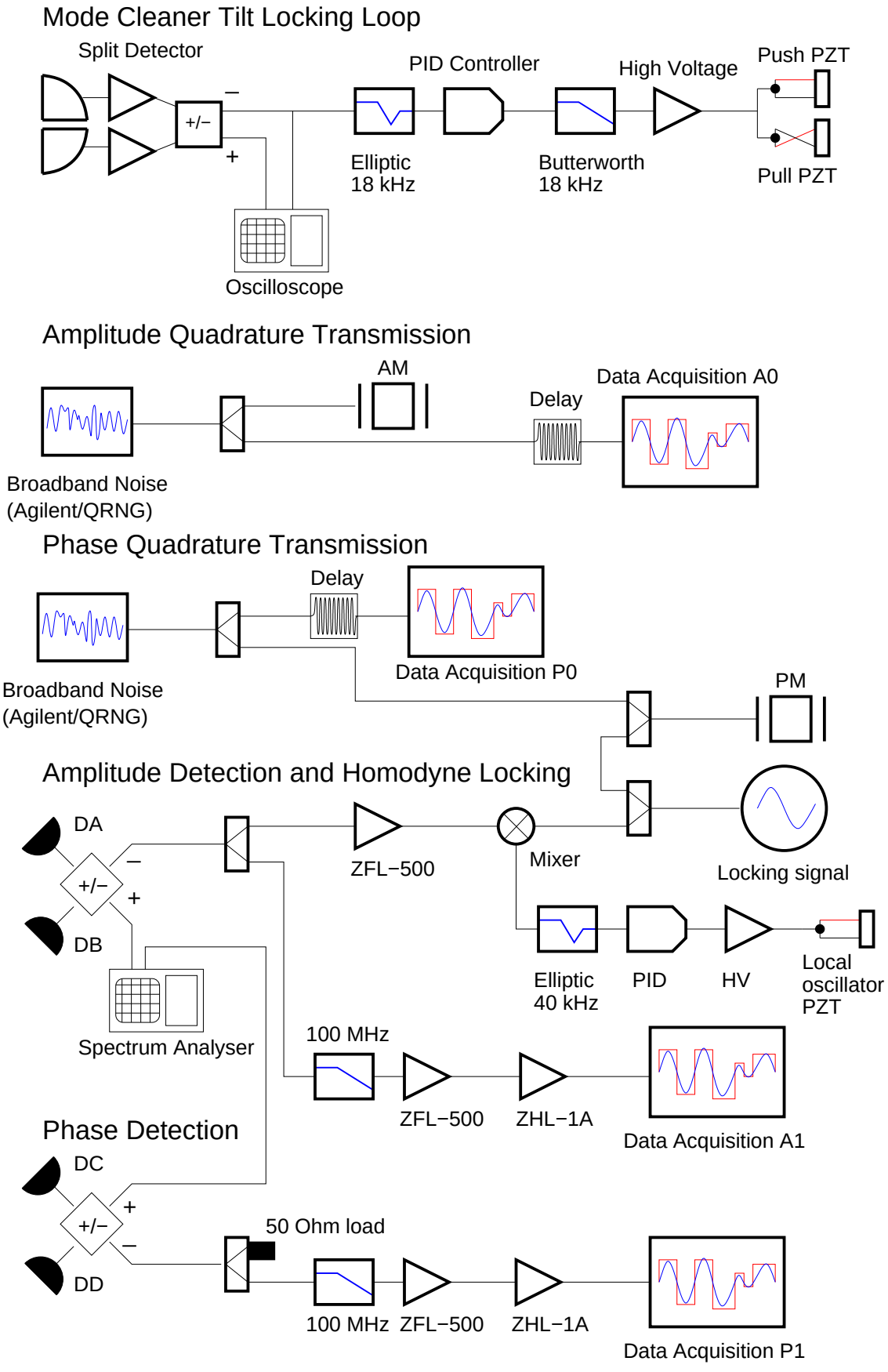


**Figure 6.8**: Circuit diagram of the experiment electronics.

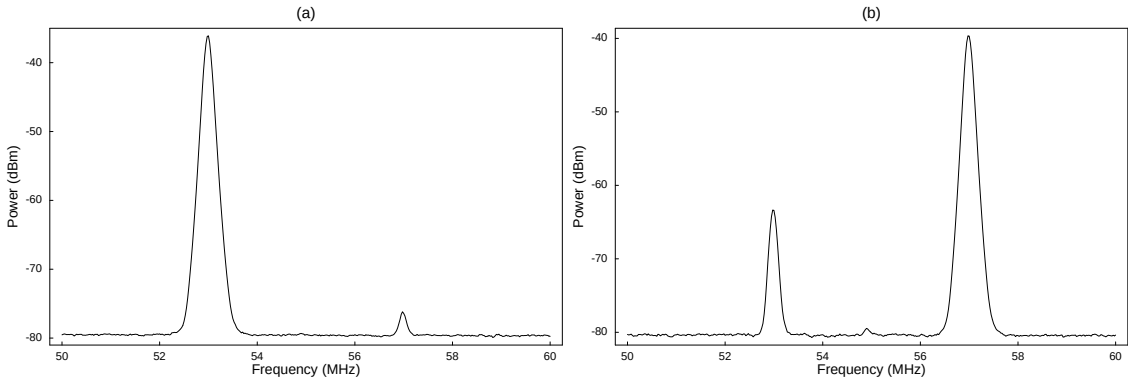


**Figure 6.9:** Cross-modulation suppression for Bob's double-homodyne system. Alice is amplitude modulating at 53 MHz and phase modulating at 57 MHz. (a) Amplitude detector showing 40 dB suppression of phase modulation. (b) Phase detector showing 24 dB suppression of amplitude modulation.

cards but we ran out of time to do this. So we chose to analyse the 30–80 MHz band for key distillation.

To correctly normalise Alice and Bob's variances required finding an accurate value for the quadrature gains. The analysis tool assumes the transfer function is sufficiently flat to assume constant gain across the signal band. The wider bandwidth of this experiment meant this assumption did not hold. We decided to split the band into multiple independent channels of 5 MHz width, over which the gain could be assumed flat. Although this processing was conducted entirely *a posteriori* to the data transmission it is equivalent to standard frequency division multiplexing (FDM) techniques in communications.

At this point the time remaining to me for data analysis was extremely short, and so at the time of writing we were unable to produce trustworthy results. Despite working very hard on the data analysis, using analysis code proven reliable for the previous experiment, we could only obtain two results that seemed reasonable. It is likely that some physical process in the experiment is yet to be understood, perhaps from the quantum random noise generator, the phase-locking in the homodyne detection or some other source.

We took five sets of data for five different channel transmissions: 100%, 75%, 50%, 25% and 10% transmission. The data analysis programme was not capable of analysing the demultiplexed 100% and 10% data and we did not have time to conduct a full-bandwidth analysis of the 10% data. Therefore we obtained four data points, three using the frequency division multiplex analysis and one using a full bandwidth analysis.

From the 100% channel an information advantage of $0.61 \pm 0.001$ bits was post-selected using 10 banded information channels (BIC's)(section 4.3.2). Over the 50 MHz of bandwidth this produced an information advantage rate of $60.5 \pm 0.1$ Mbits/sec. This figure is probably a lower bound on the actual information advantage since the analysis programme, from a calculation of the conditional variance between Alice and Bob, determined the channel transmission to be 80% and so unnecessarily allocated 20 Mbits/sec to Eve.

A $\Delta I$ rate of 80 Mbits/sec would be reasonable, since in the first generation experiment post-selection with 10 BICs approached the Shannon capacity $C$ (in our case 100 Mbits/sec). We would not expect to approach $C$ too closely since the gain roll-off of our

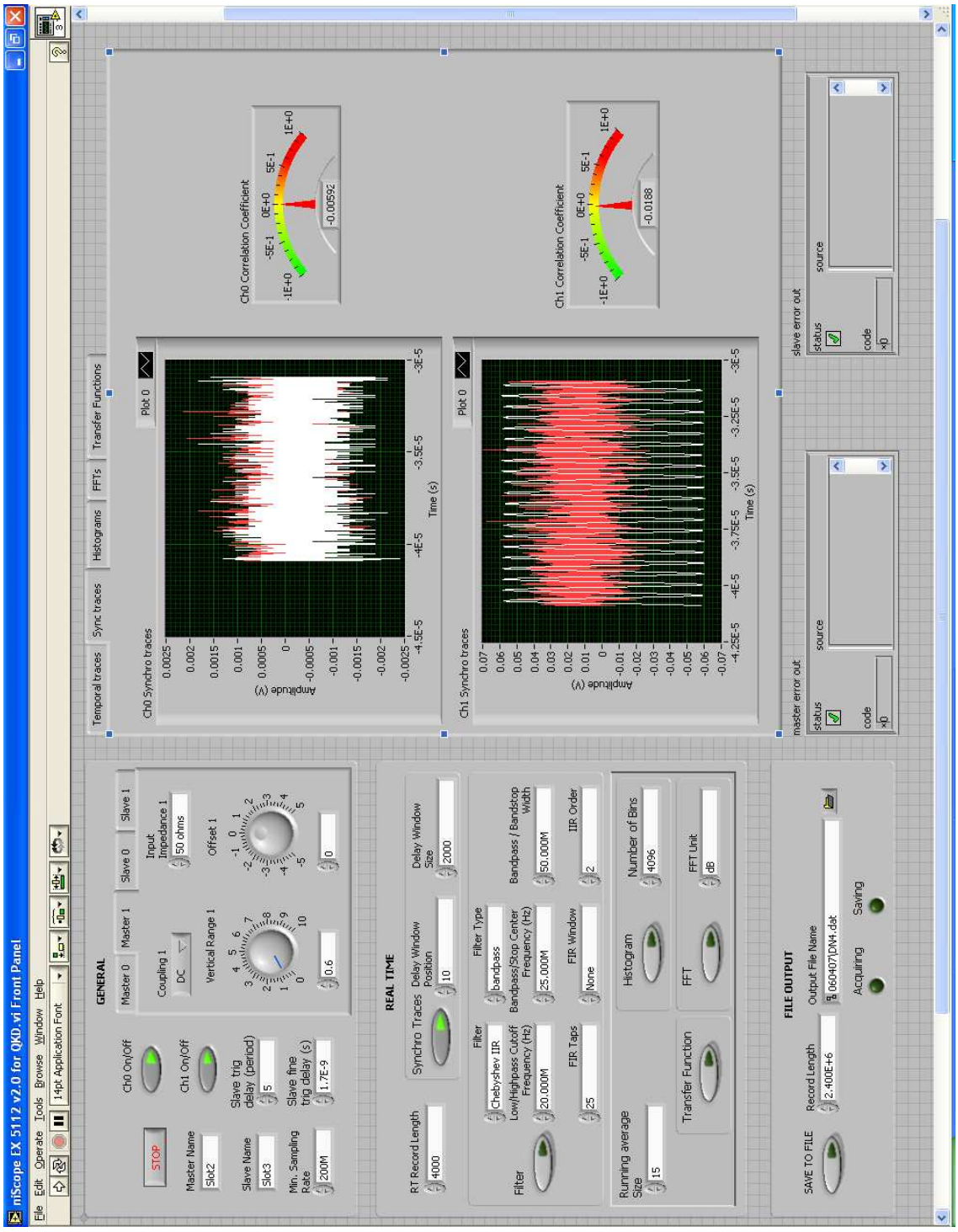


**Figure 6.10:** Screenshot of the LabView acquisition programme, showing the Alice/Bob quadrature correlation coefficients.

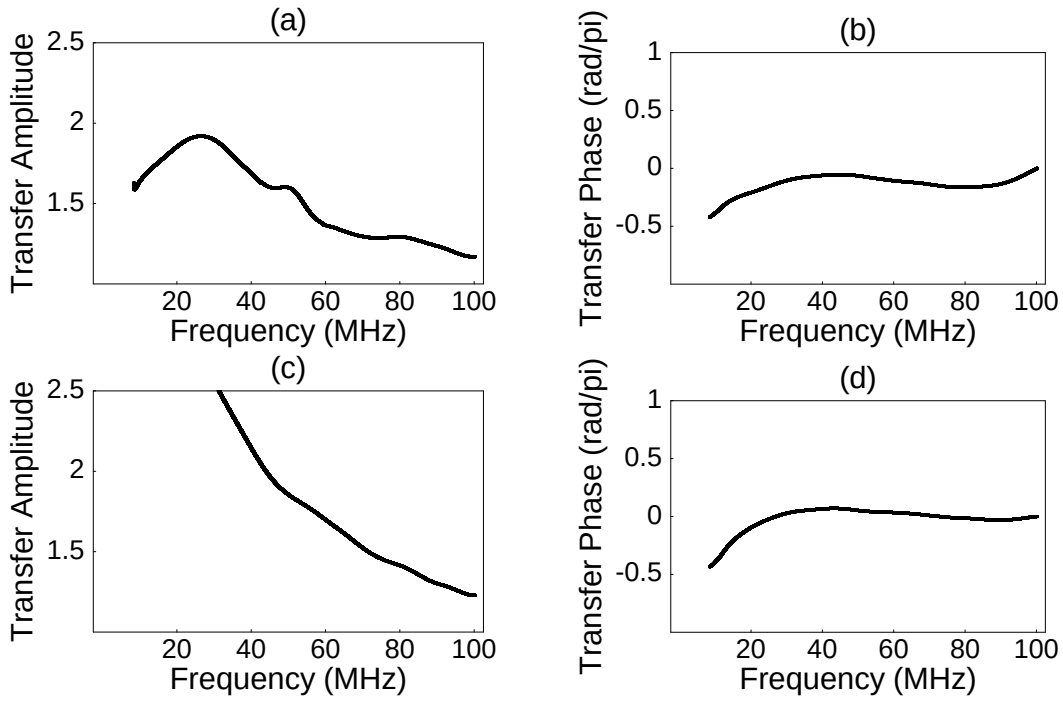


**Figure 6.11:** Transfer functions for the amplitude and phase quadrature communications channels (smoothed). (a) $\mathbf{X}^+$ amplitude response (b) $\mathbf{X}^+$ phase response (c) $\mathbf{X}^-$ amplitude response (d) $\mathbf{X}^-$ phase response. The units for the phase response should be $\pi$ rad, not rad/$\pi$ as shown.

system (Fig. 6.6) meant we could not modulate at optimal variance (Fig. 6.4) across the complete 50 MHz spectrum. The 100% $\Delta I$ result, although almost certainly not accurate to within the calculated precision, may be considered reasonably valid.

The three multiplexed data sets were beset by the problem of accurately calculating the gain for each 5 MHz channel. Fig. 6.12 shows the post-selected information advantage for each channel between 30 and 80 MHz (channels 7 to 16). The graphed solid line shows the information advantage obtainable if Bob was able to decode at $C$ for the particular transmission. The 75% case is fairly reasonable since once again, despite using 10 BICs, Alice's modulated variance was not optimal and so it would not be expected that Bob received information at $C$. The 50% case, however, is less reasonable since Bob regularly receives more information than $C$. This may be due to the imprecise channel gains. The 25% case is not graphed since all points are well above $C$, making the result quite unphysical.

For the multiplexed data the information advantage rate is obtained by adding up the advantage rates from each 5 MHz channel. The 75% data produces a total $\Delta I$ rate of $14.6 \pm 0.8$ Mbits/sec while the 50% data produces $7.9 \pm 0.8$ Mbits/sec. Unfortunately the total 50% figure is above the Shannon capacity for 50 MHz bandwidth of 6.6 Mbits/sec, and must be considered unphysical. Therefore only two data points feasibly remain from the analysis, and they are plotted with $C$ in Fig. 6.13. Although they do not approach $C$ as did the equivalent points in the first generation experiment, the larger bandwidth of this experiment means the overall information advantage rate is greater, as shown in Table 6.1.

One problem not discussed so far was that the noise variance on the phase quadrature

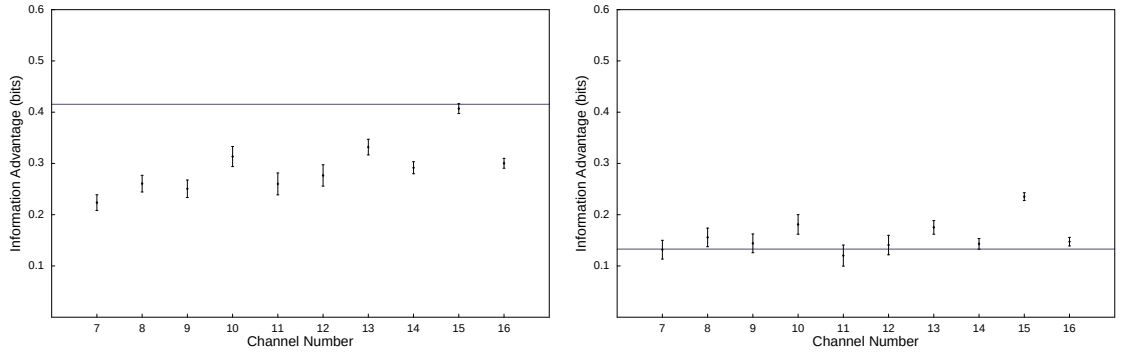


**Figure 6.12:** The information advantage Post-Selected from each of the 10 demultiplexed channels (5-MHz channels occupying 30–80 MHz) in the case of: (left) 75%; (right) 50% transmission. The solid line is the channel Shannon capacity. The almost identical oscillations in $\Delta I$ may be due to the acquisition system anti-aliasing filter, which has a corner frequency near 60 MHz (channel 12).

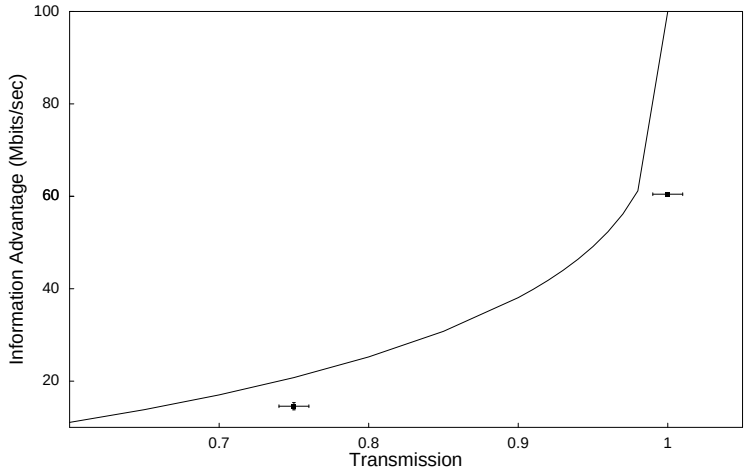


**Figure 6.13:** Total information advantage rates plotted against channel transmissions: (points) experimentally obtained values; (solid line) channel Shannon capacity.

| **Channel Transmission** | **Second Generation Post-Selected $\Delta I$ Rate** | **First Generation Post-Selected $\Delta I$ Rate** |
|---|---|---|
| 100% | $60.5 \pm 0.1$ Mbits/sec | 30 Mbits/sec |
| 75% | $14.6 \pm 0.8$ Mbits/sec | 7 Mbits/sec |
| 50% | $7.9 \pm 0.8$ Mbits/sec | 2 Mbits/sec |

**Table 6.1:** Post-Selected information advantage results. The 100% figure was based on a full-bandwidth analysis, while the 75% and 50% figures were based on analysis for frequency division multiplexing.

was often markedly different to the amplitude quadrature. It is possible that unstable phase locking in Bob's homodyne detectors was adding phase noise to the signal.

We ran out of time to calculate the absolute shot noise variance of Alice's laser and so were unable to quantify the effect of the mode cleaner. It is, however, a reasonable assumption that it was performing as required at the higher frequencies (poor locking resulted in some introduced noise at lower frequencies). That is, Alice's coherent states in this experiment were probably more pure than the coherent states used in the first generation experiment.

## 6.3 Summary

A number of improvements to the first generation experiment were made in this second generation experiment. Some were planned while others were implemented to address problems created by the planned improvements. The planned improvements were:

- Install mode cleaner to improve security
- Install higher-bandwidth detectors and acquisition system.

To utilise the higher bandwidth we had to:

- Shield detector circuits from FM radio interference
- Build quantum random noise generators to produce flat noise across the full bandwidth
- Multiplex data communications channels
- Remove acquisition system anti-aliasing filter.

The last item on this list was not achieved, limiting us to 50 MHz of the available bandwidth. Also the QRNG did not produce perfectly flat modulation, although we suspect that some if not all of the observed frequency roll-off was due to the modulator responses. To investigate this possibility, the 100 MHz transfer function of the modulators would need to be characterised.

From this experiment we produced two feasible results: information advantage rates for 100% and 75% transmission. Both of these rates improved on the equivalent rates of the first generation experiment. If, with further analysis or experimentation, stronger evidence could be found to support these figures then (after secret key distillation processing) they would represent the fastest quantum key distribution yet reported anywhere in the world.

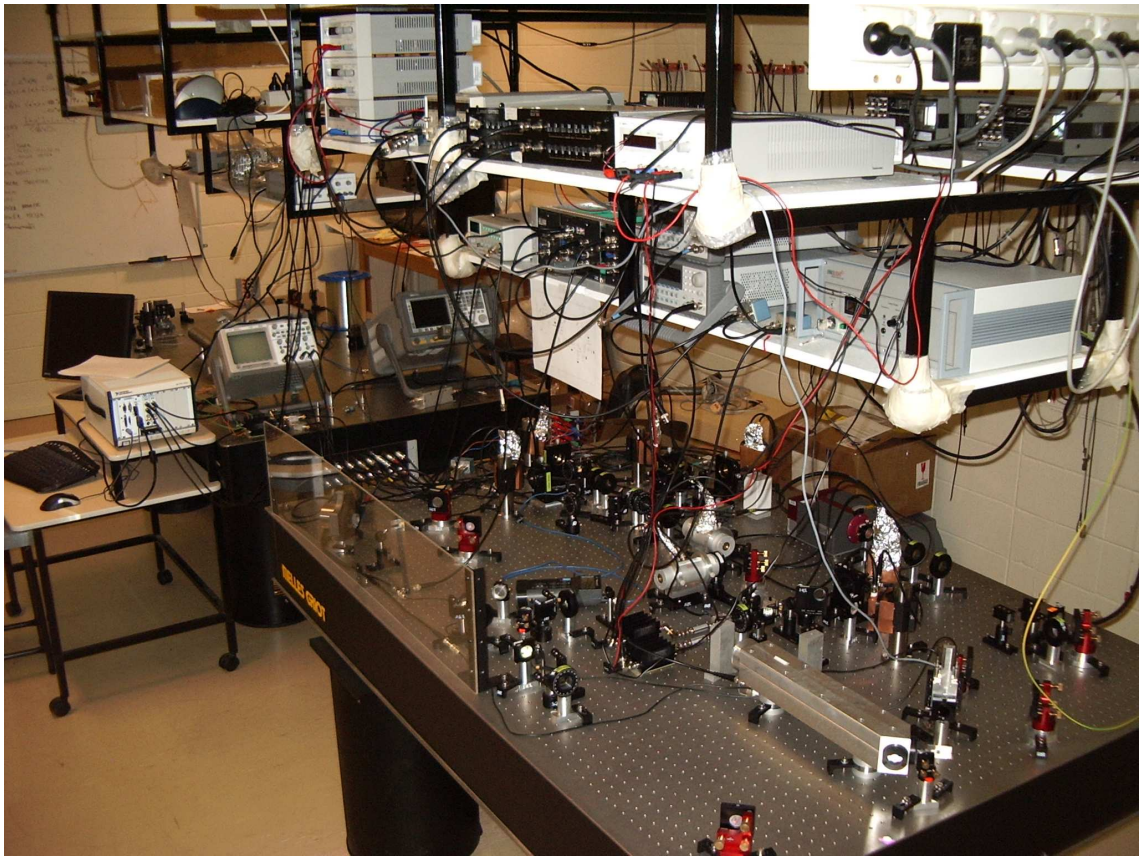

**Figure 6.14:** The quantum cryptography laboratory with the 1064 nm experiment in the foreground.

Chapter 7

# Future Directions and Conclusion

This chapter begins by detailing the initial design, purchasing and measurement work I undertook for the third generation SQM experiment. It then discusses some practical applications of broadband continuous variable quantum key distribution, and possible experiments to advance the technology towards such implementations. The chapter ends with a summary and some concluding remarks on the project.

## 7.1 Third Generation SQM

As described in section 4.4, the plan for my project was to rebuild the Lance *et al* experiment of [56] and then build the experiment again using a 1550 nm laser transmitting over optical fibre. I began work concurrently on both tasks, working on the design and purchasing of equipment for the third generation experiment while building the second generation experiment.

### 7.1.1 Optical Fibre

The principles of fibre optics are well covered in literature (for example [87]). A single-mode step-index fibre consists of a long glass cylinder (the *core*) surrounded by a cylindrical glass *cladding* of differing refractive index. Maxwell's equations for light propagation through homogenous media with the index boundary condition can be used to show that light will propagate through the fibre even if it is not straight. The only loss to the intensity is caused by absorption mechanisms in the glass which, with good engineering, can be minimised to the current accepted value of 0.2 dB per km. The 90% loss simulated in the first generation experiment (section 4.3 and [56]) corresponds to a channel loss of 10 dB, or 50 km of optical fibre.

The solution to Maxwell's equations with these boundary conditions is the fibre mode. A single mode fibre has a core diameter so small (typically 9 $\mu$m) that it will only support one mode of propagation. Such a small aperture means that it can be difficult to couple a free space beam into the fibre without introducing large coupling loss. Fortunately coupling loss need not be included in the information allocated to Eve, since it is clear that the light is lost within Alice's station.

The standard bandwidth of classical optical fibre communications technologies is currently 10 GHz. With upgrades to the modulators, detectors and acquisition system this experiment could quickly produce an information advantage up to twenty times larger than the 50 MHz results reported in Chapter 6. With the implementation of the second-generation protocols described in section 4.3.7, Mbit QKD becomes possible even under high losses.

### 7.1.2 Experimental Design

Bob's homodyne detectors require a phase reference for him to demodulate both quadratures, the local oscillator. The design of the third generation experiment therefore required a solution for Alice to transmit the local oscillator. The design initially decided on by the group is shown in Fig. 7.1. In this experiment the local oscillator and signal are polarised orthogonally to each other before in-coupling to the fibre. Bob can then separate them, unmixed, with a PBS for quadrature splitting and demodulation mixing in the manner of the first two generations, described in section 6.1.1.

Stress on the fibre induces local changes to its birefringence, causing polarisation rotation. Such rotation would cause premature mixing on the PBS following the out-coupler. It is hoped that for a typical fibre transmission line installation, the stress changes will be gradual enough that the polarisation can be corrected by feedback to an electronic polarisation controller. For the initial experiment, manual polarisation control with the wave plates following the out-coupler should be adequate.

An alternative to this design is to detune the local oscillator with an acousto-optic modulator (AOM) and send it at the same polarisation as the signal. Any rotations from fibre stress will cause them to be rotated synchronously. A cavity can then be used to split them, followed by upconversion of the local oscillator with another AOM.

### 7.1.3 Preparation

After the Group decision to implement the experiment described in Fig. 7.1 I began the purchasing, which was a time-consuming process since most of the equipment needed to be acquired. Table 7.1 is a summary of the purchases. A number of items needed to be built in the workshop and so they also were designed and built. This included the mode cleaner, which for greater locking stability was made from invar, a metal alloy that does not expand with temperature. The mode cleaner is shown in Fig. 7.2.

| **Equipment** | **Vendor** |
|---|---|
| 1550 nm fibre laser | NP Photonics |
| Invar mode cleaner | Physics workshop |
| Modulators | New Focus |
| Free space optics<br>(mirrors, lenses, wave plates, beam splitters) | CVI Laser |
| Fibre optics<br>(couplers, connectors, patch cables) | OFR |
| Fibre isolater | ThorLabs |
| Optics mounts | ThorLabs |
| SMF-28e optical fibre | Corning |
| Electronics<br>(amplifiers, filters, splitters, mixers) | Mini-Circuits |
| Additional electronics<br>(detectors, PID, HVA) | Physics electronics workshop |
| Mirror mounts | Radiant Dye |
| Additional mounts | Physics workshop |

**Table 7.1**: Summary of purchases for the third generation SQM experiment.

The final task I undertook for the third generation experiment before handing it over

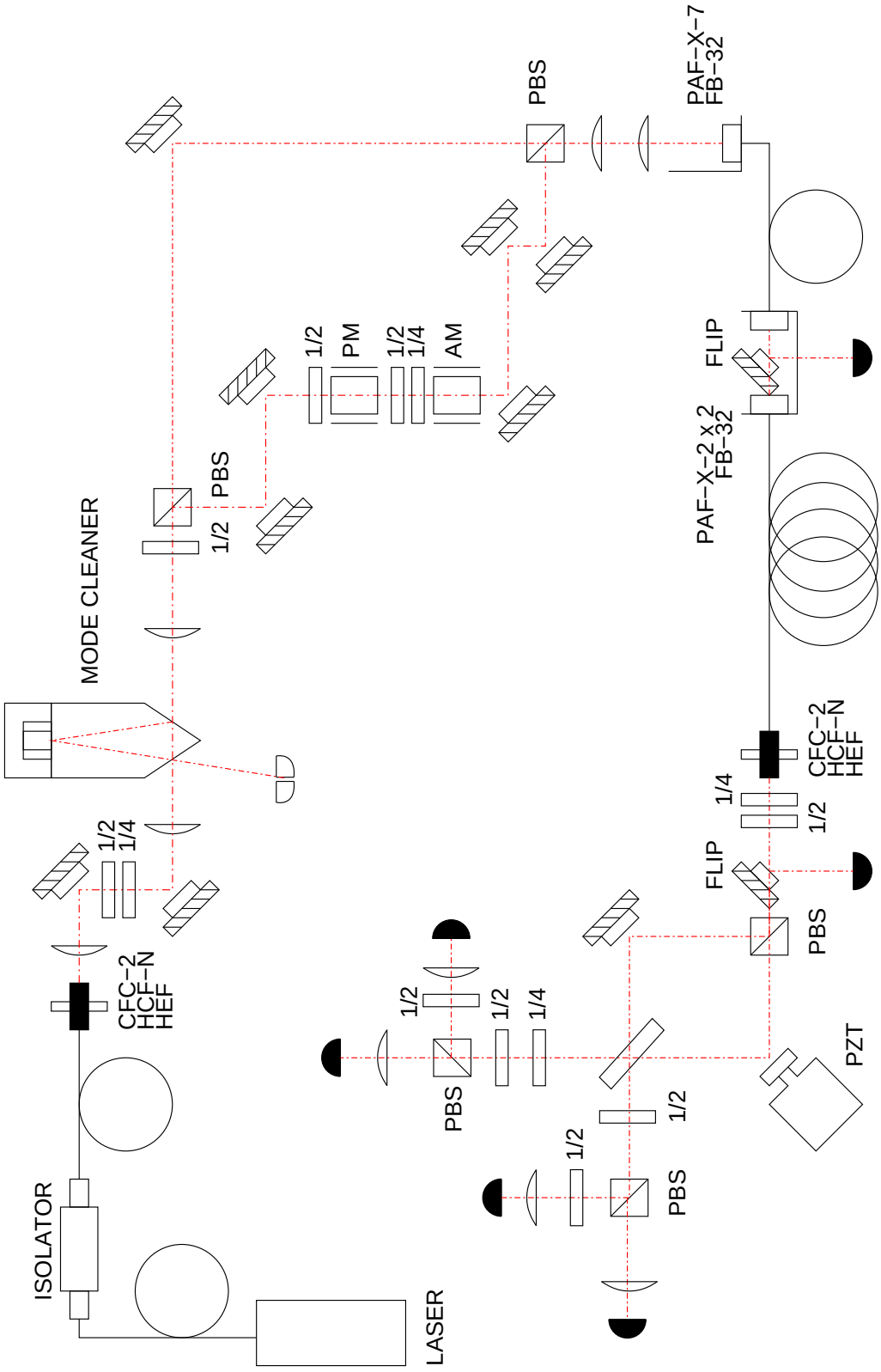


**Figure 7.1:** Initial design of the third generation SQM experiment. This layout couples the signal and local oscillator into the channel fibre at orthogonal polarisations. Small polarisation rotations over time in the fibre can be corrected by wave plates following the out-coupler.

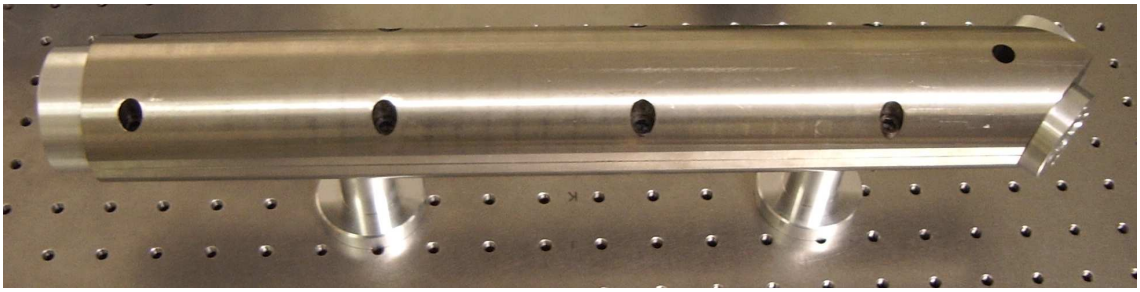

**Figure 7.2:** The 1550 nm mode cleaner, made from invar with an aluminium single-PZT end cap.

to the following Honours student, Daniel Alton, was investigate the behaviour of the OFR CFC-2 fibre out-coupler. My goal was to see if it could be configured to produce a beam of the required waist size for the mode cleaner (634 $\mu$m). I was successful in this, producing a beam with waist of approximately 640 $\mu$m. Fig. 7.3 shows the beam profile measurements and fit that I used to determine the waist size, using the technique described in section 5.4.

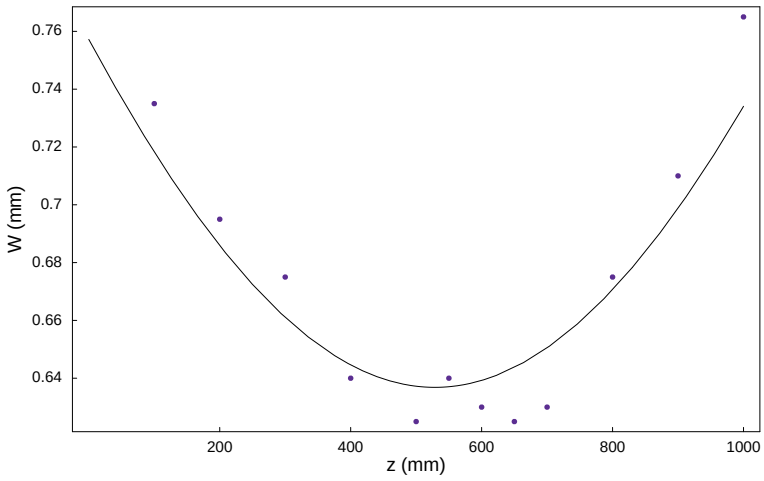


**Figure 7.3:** Adjusting the out-coupling lens of the fibre I was able to create a beam with waist of approximately 640 $\mu$m, 53 cm from the out-coupler.

## 7.2 Beyond Third Generation SQM

Quantum key distribution is without doubt the most mature of the quantum information technologies. Commercial discrete-variable QKD systems are already available, whereas other technologies such as quantum memory, quantum error correction, quantum logic gates and quantum computing are in the first stages of experimental demonstration. It is clear then that considering the immediate future of CVQKD-SQM involves moving

beyond the realm of scientific interest and into practical applications for government, military, business and industry sectors.

### 7.2.1 Practical QKD Networks

This thesis began with an introduction to communications networks and the need for information assurance within those networks. The purpose of key distribution technologies, whether classical or quantum, is to provide this information assurance. Classical cryptography is widespread and used for securing communications networks at all scales, as shown in Table 7.2.

| **Scale** | **Example Secure Networks** |
|---|---|
| International | Financial networks for monetary transactions<br>Diplomatic communications |
| National | Government databases for immigration, road transport and infrastructure<br>National security communications for threat monitoring, intelligence sharing, personnel tracking |
| Metropolitan | Police communications<br>Mobile telephone and other wireless networks |
| Local | Computer LAN for connecting individuals to larger-scale networks |
| Personal | Electronic purchasing<br>Biometric information |

**Table 7.2**: Scales of secure communications networks

The 0.2 dB loss per km generally limits the range of optical fibre QKD to metropolitan-scale networks and smaller. The likely cost (and size) of a first generation practical device is also likely to preclude its application from local and personal networks. These networks generally consist of large numbers of low-value terminals. There may be an exception in biometric networks, since although the information remains local (for example access control of a building) it has immensely high value (a person's identity). In this case the cost of deploying QKD into a small, low bandwidth network may be justified. In general, however, metropolitan networks carrying large amounts of sensitive commercial, police, military, security or government communications promise the first applications for broadband QKD.

Like many new technologies, the first application for QKD is likely to be one-for-one replacement of the old technology. It is often the case that novel applications for a new technology, that take full advantage of its superiority, are only discovered after it has been firmly established as a successor to the old. In this employ it delivers enhancement rather than revolution.

Fig. 7.4 describes a typical metropolitan secure network (an 'intranet'). It considers an organisation with agencies spread across a city, or alternatively a group of agencies having in common a particular sensitive interest. The interest could be for example intelligence, criminal records, financial transactions or commercial operations.

The building at site **S** contains the intranet server. The majority of network services are located here, such as hosting of **A**,**B**,and **C**'s intranet websites; voice and email services; and database storage and access. For classical cryptography the major trunks from **S** to

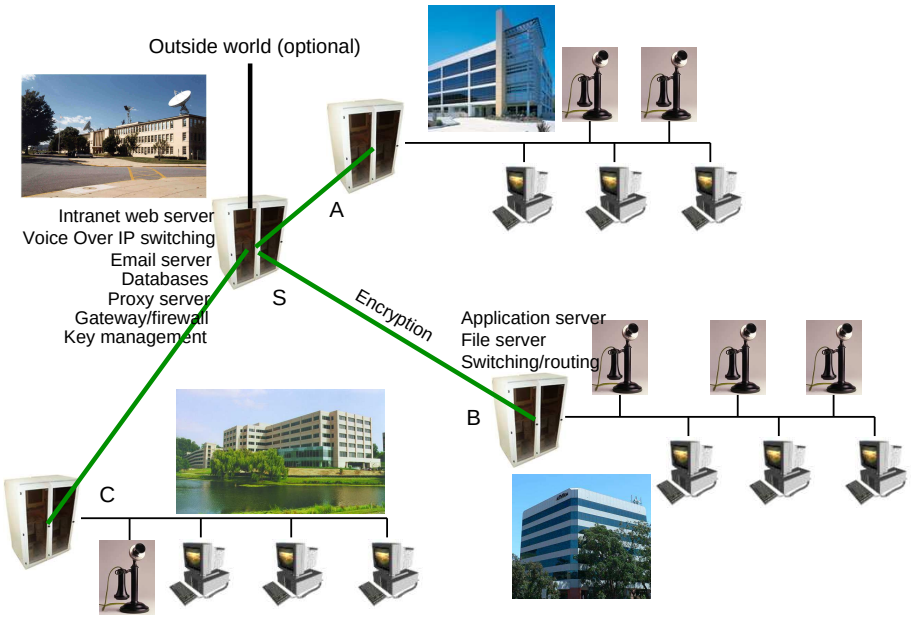


**Figure 7.4:** A metropolitan-scale secure network. While the links between offices are encrypted, physical security measures on the building allow the inside of the office to be considered secure. Therefore only the high-bandwidth trunks between offices require encryption, not the individual communications of a terminal.

**A**,**B**,and **C** generally consist of bandwidth hired from the telecommunications company owning the city's physical communications infrastructure.

Information passing through the trunks is secured with a network or data encryption device such as General Dynamics' Sectéra In-Line Network Encrypter. Legacy data encryption systems tend to use symmetric keys whereas modern systems have shifted to asymmetric keys (see section 2.1).

Symmetric systems require much more frequent rekey, since asymmetric systems use a different session key for each communication and only the initial authentication key must be replaced. The infrequency of its use means that in terms of time it 'lasts' much longer before compromise becomes possible. This is a great advantage for asymmetric systems, since symmetric rekeying cannot be conducted over the network. It is generally done by trusted courier, which is expensive and still prone to compromise.

Since the trunks themselves are unlikely to be direct optical fibre connections, a one-for-one replacement of such classical cryptographic systems with quantum cryptography would require the additional expense of laying optical fibre from **S** directly to each of the other agencies. Beyond this expense, however, a first generation QKD application would be competitive with classical cryptography.

The trunks would carry the reconciliation information needed for each end to distill a secret key from their fibre, and their role of carrying encrypted information would remain unchanged. Instead of a trusted courier network delivering the key to unlock this information, it would instead be delivered by optical fibre. In this way an organisation can use cryptography without needing a complex key management infrastructure, and guard its information against the possibility of public key cryptography being compromised by mathematical or quantum-computational analysis.

### 7.2.2 Free Space QKD

The international- and national-scale networks identified in section 7.2.1 are generally no more complex in topology than the metropolitan-scale network of Fig. 7.4. The secure trunks linking local networks are of course much larger. Microwave repeaters, undersea cables and satellites are the necessary components for these longer trunks. While an undersea optical fibre cable hundreds of kilometres long is likely to introduce too much loss for QKD, recent experiments have shown that at laser wavelengths atmospheric loss between ground and satellite can be as little as 6.5 dB.[102]

Quantum key distribution via satellite would provide high bandwidth key distribution for even the largest international networks. Even without the threats to public key cryptography, the challenges and costs of international symmetric key management warrant that serious consideration be given to satellite-based QKD.

Such a system would not even require mounting a laser on a satellite. Fig. 7.5 describes how a single trunk might be encrypted with satellite QKD. If the cost of the equipment could be brought low enough per unit of data, satellite QKD would be suitable for even metropolitan-scale networks where, in time, the cost of laying fibre may become greater than implementing satellite-based QKD.

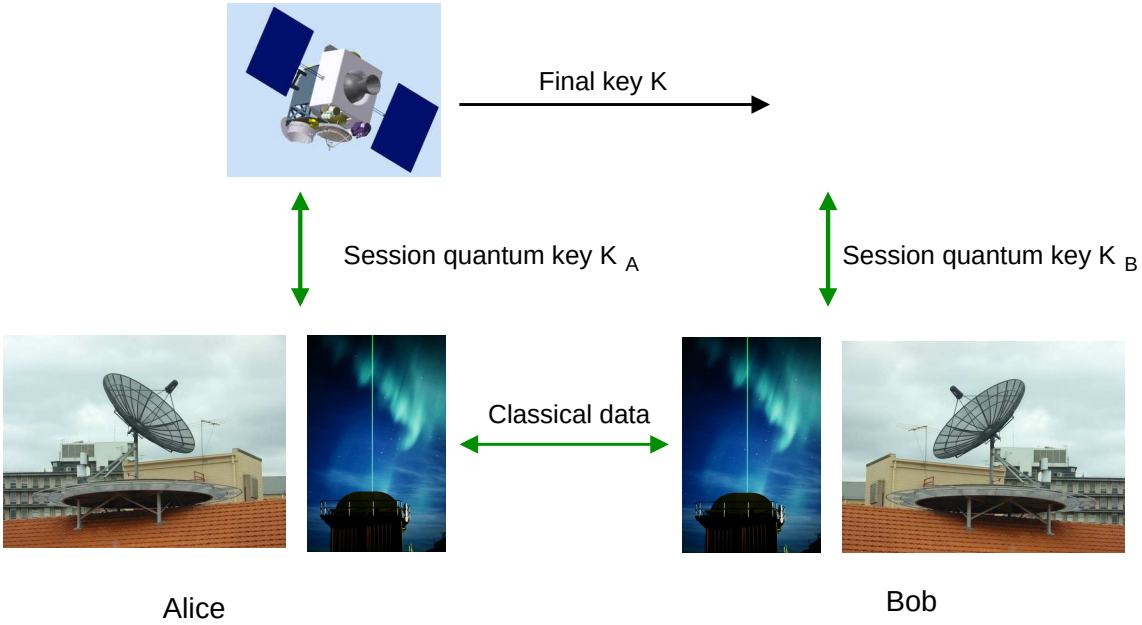


**Figure 7.5:** Satellite quantum key distribution. Alice generates a binary key $K$. When the satellite passes over she acquires the satellite and transmits broadband noise with her laser. She and the satellite then use a classical radio-frequency channel to distil a secret session key $K_A$. Alice then transmits her final key $K$ over the radio channel, one-time-pad encrypted with $K_A$. The satellite decrypts $K$ with the session key and stores it. When it passes over Bob, he repeats the process of distilling a session key $K_B$ which the satellite then uses to one-time-pad encrypt $K$. Bob receives $K$ and is able to use it for secure communications with Alice over any data channel. The data channel could be the same satellite, a different satellite, an undersea cable or any method appropriate to the physical situation.

### 7.2.3 Quantum Random Number Generation

The work begun in this project on quantum random number generation also has some future direction. The randomness of the output needs to be investigated and also methods of converting the continuous noise into binary strings without sacrificing entropy. There are numerous randomness tests detailed in information theory literature and available from standards institutes. It would be interesting to see how our QRNG compares to other RNG for randomness, if any difference exists.

To make a final link between QRNG and QKD, it would be interesting to examine the statistics of the random numbers before and after the key distribution process. Such an examination would make a good check for the integrity of the secret key distillation algorithms, that no hidden bias was being introduced either from the equipment or from bugs in the software.

## 7.3 Conclusion

Communication is a fundamental feature of civilisation. Methods for providing assuredness to communications have wide application. Cryptography is such a method and cryptographic technology dominates as the means for protecting communications throughout modern networks. Historically this technology has provided practical security but rarely perfect security. In future the current technologies may fail to provide even reasonable security.

Quantum key distribution promises a new class of cryptographic technologies, based on the physical laws of quantum mechanics, for which perfect security will be ubiquitous. The initial proposals for quantum key distribution devices, based on discrete quantum variables, have not yet shown any potential for widespread use in modern high bandwidth communications networks. Continuous variable technologies offer greater applicability in the short term, and are likely to continue their superiority in the long term.

In 2005 the ANU Quantum Optics group was among the first in the world to experimentally demonstrate continuous variable quantum key distribution. From this first proof-of-principle there lies a natural progression of advances to improve the technology for practical use. The first such advances are to reduce channel noise and increase channel bandwidth. Later advances include optical fibre integration, miniaturisation and further increases to the bandwidth with commercially available 10 GHz communications equipment.

This thesis reports on the work undertaken thus far towards the ANU's second and third generation Simultaneous Quadrature Measurement CVQKD experiments. Noise reduction and increased channel bandwidth was successfully achieved. Furthermore, radio frequency shielding, quantum random noise generation and frequency division multiplexing were added to the experiment with intermediate success. Unfortunately the experiment could not be completed in the time allocated and so the results of this work cannot be considered conclusive. Finally, design and purchasing for the third generation experiment was completed.

Whilst this project fell short of its ambitious goals to complete both second and third generation experiments, numerous technological advances were made towards practical continuous variable quantum key distribution. The preliminary results from analysis of the data taken for this experiment suggest that it is capable of running the fastest quantum key distribution yet reported.

# Bibliography


[1] Bachor, H. A. and Ralph, T. C., "A Guide to Experiments in Quantum Optics" Ed. 2, Wiley-VCH, Weinheim, 2004.

[2] Bacon, D., *Physical Review A* Vol. 70 Art. 032309, 2004.

[3] C.H. Bennett and G. Brassard "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, December 1984.

[4] C. H. Bennett, G. Brassard, and J.-M. Robert, "How to reduce your enemys information", in Advances in Cryptology—Proceedings of Crypto'85 (*Lecture Notes in Computer Science* Vol. 218), Springer-Verlag, Berlin, Germany, 1986.

[5] C. H. Bennett, G. Brassard, and J.-M. Robert, *SIAM Journal of Computing* Vol. 17 No. 2, April 1988.

[6] Bennett, C. H., *Physical Review Letters* Vol. 68 No. 21, 1992.

[7] Bennett, C. H., Brassard, G., Crépeau, C. and Maurer, U. M., *IEEE Transactions on Information Theory* Vol. 41 No. 6, November 1995.

[8] Berrou, C., Glavieux, A. and Thitimajshima, P., IEEE International Conference on Communications (*ICC 93* Vol. 2), 1993.

[9] Bethune, D. S. and Risk, W. P., *IEEE Journal Of Quantum Electronics* Vol. 36 No. 3, Match 2000.

[10] Boström, K. and Felbinger, T., *Physical Review Letters* Vol. 89 No. 18, October 2002.

[11] Bourennane, M., Ljunggren, D., Karls Son, A., Jonsson, P., Hening, A. and Ciscar, J. P., *Journal Of Modern Optics* Vol. 47 No. 2/3, 2000.

[12] Bowen, W. P., "Experiments towards a Quantum Information Network with Squeezed Light and Entanglement", Australian National University PhD thesis, October 2003.

[13] Brassard, Gilles and Salvail, Louis, *Lecture Notes in Computer Science* Vol. 765 (Proceedings of EuroCrypt '93), 1994.

[14] Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B. C., *Physical Review Letters* Vol. 85 No. 6, August 2000.

[15] Buck, J. R., Daniel, M. M. and Singer, A. C., "Computer Explorations in Signals and Systems—Using Matlab", Prentice Hall, Jersey, 1997.

[16] California Institute of Technology, *Space Radiation Laboratory LISA project* at http://www.srl.caltech.edu/lisa/graphics/e3.jpg, March, 2006.

[17] Cachin, C. and Maurer, U. M. *Journal of Cryptology* Vol 10, 1997.

[18] Carter, J. L. and Wegman, M. N., *Journal of Computer and System Sciences* Vol. 18, 1979.

[19] Cerf, N. J., Levy, M. and Van Assche, G., *Physical Review A* Vol. 63 Art. 052311, 2001.

[20] Cerf, N. J., Iblisdir, S. and Van Assche, G., *The European Physical Journal D* Vol. 18, 2002.

[21] Committee on National Security Systems Instruction No. 4009 Revised May 2003, National Security Agency/Central Security Service, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf, May 2006.

[22] Csiszár, I. and Körner, J., *IEEE Transactions on Information Theory* Vol. IT-24 No. 3, May 1978.

[23] CVI Optical Components and Assemblies, *Glan-Thompson Prism* at http://www.cvilaser.com/common/pdfs/CPBS.pdf, 2006.

[24] Daemen, J. and Rijmen, V., *Lecture Notes in Computer Science* Vol. 1820, 2000.

[25] Diffie, W. and Hellman, M. E., *IEEE Transactions on Information Theory* Vol. 22 No. 6, November 1976.

[26] Drever, R. W. P., Hall, J. L., Kowalski, F. V., Hough, J., Ford, G. M., Munley, A. J., Ward, H., *Applied Physics B—Photophysics & Laser Chemistry* Vol. 31 No. 2, 1983.

[27] Ekert, A. K., *Physical Review Letters* Vol. 67 No. 6, 1991.

[28] Gander, M. J. and Maurer, U. M., "On The Secret Key Rate Of Binary Random Variables", Proceedings of ISIT'94, 1994.

[29] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. *Reviews of Modern Physics* Vol. 74, March 2002.

[30] Gobby, C., Yuan Z. L. and Shields A. J., *Electronics Letters* Vol. 40 No. 25, 2004.

[31] Gobby, C., Yuan Z. L. and Shields A. J., *Applied Physics Letters* Vol. 84 No. 19, May 2004.

[32] Gordon, K. J., Fernandez, V., Townsend, P. D. and Buller, G. S., *IEEE Journal Of Quantum Electronics* Vol. 40 No. 7, July 2004.

[33] Franklin, G. F., Powell, J. D. and Emami-Naeini, A.,"Feedback Control of Dynamic Systems" Ed. 4, Prentice Hall, 2002.

[34] Goldberg, I. and Wagner, D., "Randomness and the Netscape Browser—How secure is the World Wide Web?", *Dr. Dobb's Journal* at http://www.ddj.com, January 1996.

[35] Gottesman, D. and Preskill, J., *Physical Review A* Vol. 63 Art. 022309, 2001.

[36] Griffiths, D. J., "Introduction to Electrodynamics" Ed. 3, Prentice-Hall, New Jersey, 1999.

[37] Grosshans, F. and Grangier, Ph. "Reverse reconciliation protocols for quantum cryptography with continuous variables", *e-Print Archive* Quantum Physics Art. 0204127 at http://www.arxiv.org/archive/quant-ph, 2002.

[38] Grosshans, F. and Grangier, Ph., *Physical Review Letters* Vol. 88 No. 5, February 2002.

[39] Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N.J. and Grangier, Ph, *Nature* Vol. 421, January 2003.

[40] Grosshans, F. and Cerf, N. J., *Physical Review Letters* Vol. 92 No. 4, January 2004.

[41] Grosshans, F., *Physical Review Letters* Vol. 94 Art. 020504, January 2005.

[42] Hecht, E., "Optics" Ed. 4, Addison Wesley, San Francisco, 2002.

[43] Heisenberg, Werner, *Zeitschrift für Physik* Vol. 43, March 1927.

[44] Hillery, M., *Physical Review A* Vol. 61 Art. 022309, 2000.

[45] Horowitz, P. and Hill, W., "The Art of Electronics" Ed. 2, Cambridge University Press, July 1989.

[46] Hughes, R.J., Luther, G.G., Morgan, G.L., Peterson, C.G. and Simmons, C., *Lecture Notes in Computer Science* Vol. 1109, 1996.

[47] Hughes, R. J., Morgan, G. L. and Peterson C. G., *Journal Of Modern Optics* Vol. 47 No. 2/3, 2000.

[48] Hwang, W-Y, *Physical Review Letters* Vol. 91 No. 5, August 2003.

[49] Iblisdir, S., Van Assche, G. and Cerf, N. J., *Physical Review Letters* Vol. 93 No. 17, October 2004.

[50] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H. and eilinger, A., *Physical Review Letters* Vol. 84 No. 20, May 2000.

[51] Jun, B. and Kocher, P.,"The Intel Random Number Generator", *Cryptography Research, INC. White Paper*, April 1999.

[52] Kane, T. J., and Byer, R. L., *Optics Letters* Vol. 10 No. 2, 1985.

[53] Kato, K., Osaki, M., Sasaki, M. and Hirota, O. *IEEE Transactions on Communications* Vol. 47 No. 2, February 1999.

[54] Knight, W., "Massive Search Reveals No Secret Code In Web Images", *New Scientist*, September 2001.

[55] Lam, P. K., personal communication, 2005.

[56] Lance, A. M., Symul, T., Sharma, V., Weedbrook, Ch., Ralph, T. C. and Lam, P. K., *Physical Review Letters* Vol 95 Art. 180503, October 2005.

[57] Lance, A. M., personal communication, 2006.

[58] Legré, M., Zbinden, H. and Gisin, N., "Implementation of continuous variable quantum cryptography in optical fibres using a go-&-return configuration", *e-Print Archive* Quantum Physics Art. 0511113 at www.arxiv.org/archive/quant-ph, 2005.

[59] Levitin, L. B., in *Quantum Communication and Measurement*, edited by Belavkin, V. P., Hirota, O. and Hudson, R. L., Plenum Press, New York, 1995.

[60] Liu, S. and Wang, Y., *Lecture Notes in Computer Science* Vol. 1719, 1999.

[61] Liu, S., Van Tilborg, H. C. A. and Van Dijk, M., *Designs, Codes and Cryptography* Vol. 30, 2003.

[62] Lodewyck, J., Debuisschert, T., Tualle-Brouri, R. and Grangier, Ph., "Controlling Excess Noise in Fiber Optics Continuous Variables Quantum Key Distribution" *e-Print Archive* Quantum Physics Art. 0511104 at http://www.arxiv.org/archive/quant-ph, 2005.

[63] Lorenz, S., Korolkova, N. and Leuchs, G., *Applied Physics B* Vol. 79, 2004.

[64] Marand C. and Townsend, P. D., *Optics Letters* Vol. 20 No. 16, August 1995.

[65] Maurer, U. M., *IEEE Transactions on Information Theory* Vol. 39 No. 3, May 1993.

[66] Maurer, U. M., *Lecture Notes in Computer Science* Vol. 1233, 1997.

[67] McKenzie, K., personal communication, 2006.

[68] Nambu, Y., Yoshino, K. and Tomita, A., "One-way Quantum Key Distribution System based on Planar Lightwave Circuits", *e-Print Archive* Quantum Physics Art. 0603041 at http://www.arxiv.org/archive/quant-ph, 2006.

[69] Naor, M. and Yung, M., *Proceedings of the Twenty First Annual (ACM) Symposium on Theory of Computing*, 1989.

[70] Newport Corporation, *Polarising Beam Splitter Cube* at http://www.newport.com/images/webclickthru-EN/images/1277069.gif, 2006.

[71] Nielsen, M. A. and Chuang, I. L., "Quantum Computation and Quantum Information", Cambridge University Press, United Kingdom, 2000.

[72] Nielsen, P. M., Schori, C., SøRensen, J. L., Salvail, L., DamgåRd, I. and Polzik, E., *Journal Of Modern Optics*, Vol. 48, No. 13, 2001.

[73] National Institute of Standards and Technology (NIST), "Announcing the DATA ENCRYPTION STANDARD (DES)", Federal Information Processing Standards Publication (FIPS) 46-2, 1993.

[74] National Institute of Standards and Technology (NIST), "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication (FIPS) 197, 2001.

[75] Nguyen, K.-C., Van Assche, G. and Cerf, N. J., "Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution", *e-Print Archive* Information Theory Art. 0406001 at http://www.arxiv.org/list/cs.IT/, February 2004.

[76] Nyquist, H., *Transactions of the AIEE* Vol. 47, April 1928.

[77] Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H. R., Lorünser, T., Maurhardt, O., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., Jennewein, T. and Zeilinger, A., *Optics Express* Vol. 12 No. 16 August 2004.

[78] Ralph, T. C., *Physical Review A*, Vol. 61 Art. 010303, 1999.

[79] Ralph, T. C., *Physical Review A* vol. 62 Art. 062306, 2000.

[80] Ralph, T. C., "Time Displaced Entanglement and Non-Linear Quantum Evolution" *e-Print Archive* Quantum Physics Art. 0510038 at http://www.arxiv.org/archive/quant-ph, 2005.

[81] Rarity, J. G., Owens, P. C. M. and Tapster, P. R.,*Journal of Modern Optics* Vol. 41 No. 12, January 1994.

[82] Reid, M. D., *Physical Review A* Vol. 62 Art. 062308, 2000.

[83] Ribordy, G., Brendel, J., Gautier, J.-D., Gisin, N. and Zbinden, H., *Physical Review A* Vol. 63 Art. 012309, 2000.

[84] RIBORDY, G., Gautier, J.-D., Gisin, N., Guinnard, O. and Zbinden H., *Journal Of Modern Optics* Vol. 47 No. 2/3, 2000.

[85] Rivest, R. L., Shamir, A. and Adleman, L., *Communications of the ACM* Vol. 21 No. 2, February 1978.

[86] RP Photonics, "Fiber Bragg gratings", *Encyclopedia of Laser Physics and Technology* at http://www.rp-photonics.com/fiber_bragg_gratings.html, 2006.

[87] Saleh, B. E. A., and Teich, M. C., "Fundamentals of Photonics", John Wiley & sons, USA, 1991.

[88] Schaumann, R. and Van Valkenburg, M. E., "Design of Analog Filters", Oxford University Press, New York, 2001.

[89] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson, N., *Lecture Notes in Computer Science* Vol. 1556, 1999.

[90] Shaddock, D. A., "Advanced Interferometry for Gravitational Wave Detection", Australian National University PhD thesis, November 2000.

[91] Shannon, Claude E., *Bell System Technical Journal* Vol. 27, October 1948.

[92] Shannon, Claude E., *Bell System Technical Journal* Vol. 28, October 1949.

[93] Sharma, V., personal communication, 2006.

[94] Sharma, V., unpublished CVQKD long paper, 2006.

[95] Shor, P. W., *SIAM Journal of Computing* Vol. 26 No. 5, October 1997.

[96] Shor, P. W. and Preskill, J., *Physical Review Letters* Vol. 85 No. 2, July 2000.

[97] Siegman, A. E., "Lasers", University Science Books, California, 1986.

[98] Silberhorn, Ch. , Ralph, T. C., Lütkenhaus, N. and Leuchs, G., *Physical Review Letters* Vol. 89 No. 16, October 2002.

[99] Steane, A. M., *Physical Review Letters* Vol. 77, 1996.

[100] Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. and Zbinden, H., *New Journal of Physics* Vol. 4, 2002.

[101] Thew, R. T. , Tanzilli, S., Krainer, L., Zeller, S. C., Rochas, A., Rech, I., Cova, S., Zbinden, H. and Gisin, N., "Ghz QKD at Telecom Wavelengths Using Up-Conversion Detectors", *e-Print Archive* Quantum Physics Art. 0512054 at www.arxiv.org/archive/quant-ph, 2005.

[102] Toyoshima, M., Yamakawa, S., Yamawaki, T., Arai, K., García-Talavera, M. R., Alonso, A., Sodnik, Z. and Demelenne, B., *IEEE Transactions On Antennas And Propagation* Vol. 53 No. 2, February 2005.

[103] Uehara, N., "Ring Mode Cleaner for the Initial LIGO 10 Watt Laser", Stanford University internal report, February 1997.

[104] Van Assche, G., Cardinal, J. and Cerf, N. J., *IEEE Transactions on Information Theory* Vol. 50 No. 2, February 2004.

[105] Vernam, G. S., *Journal American Institute of Electrical Engineers* Vol. XLV, 1926.

[106] Weedbrook, Ch., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C. and Lam, P. K., *Physical Review Letters* Vol. 93 No. 17, October 2004

[107] Weedbrook, Ch., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C. and Lam, P. K., *e-Print Archive* Quantum Physics Art. 0508169 at http://www.arxiv.org/archive/quant-ph, August 2005.

[108] Wigner, E., *Physical Review* Vol. 40, 1932.

[109] *Wikipedia* at http://en.wikipedia.org/wiki/Image:English-slf.png.

[110] Williams, T. J., "Transformation of Squeezed Quadratures under Feed-Forward Amplification and Post-Selection", Australian National University internal report, June 2005.

[111] Wolkerstorfer J., "Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags?", presentation at the Institute for Applied Information Processing and Communications Workshop on RFID and Light-weight Cryptography, Graz, Austria, at http://www.iaik.tugraz.at/research/krypto/events/RFID-SlidesandProceedings/Wolkerstorfer-ECC and RFID.pdf, August 2005.

[112] Wootters, W. K. and Zurek, W. H., *Nature* Vol. 299, October 1982.

[113] Yuan, Z., Gobby, C. and Shields, A. J., *Optical Society of America* Art. QThPDB8, 2003.

[114] Zhao, Y., Qi, B., Ma, X., Lo, H.-K., Qian, L., "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber", *e-Print Archive* Quantum Physics Art. 0601168 at http://www.arxiv.org/archive/quant-ph, 2006.

Appendix A

# Electromagnetic Radiation and Polarisation

## A.1 Electromagnetic Waves

The scientific fields of electricity and magnetism were unified by Maxwell in the form of Maxwell's Equations, (A.1.1).

$$\left.\begin{array}{ll} \text{(i)} \quad \nabla \cdot \mathbf{E} = 0 & \text{(iii)} \quad \nabla \times \mathbf{E} = -\dfrac{\partial \mathbf{B}}{\partial t} \\ \text{(ii)} \quad \nabla \cdot \mathbf{B} = 0 & \text{(iv)} \quad \nabla \times \mathbf{B} = \mu_0 \epsilon_0 \dfrac{\partial \mathbf{E}}{\partial t} \end{array}\right\} \quad \text{Maxwell's Equations (free space)} \tag{A.1.1}$$

The equations can be decoupled by taking the curl of (iii) and (iv) and substituting (i) and (ii).[36]

$$\nabla^2 \mathbf{E} = \mu_0 \epsilon_0 \frac{\partial^2 \mathbf{E}}{\partial t^2} \qquad \nabla^2 \mathbf{B} = \mu_0 \epsilon_0 \frac{\partial^2 \mathbf{B}}{\partial t^2} \tag{A.1.2}$$

In this form each $x, y, z$ component of $\mathbf{E}$ and $\mathbf{B}$ satisfies the three-dimensional wave equation,

$$\nabla^2 f = \frac{1}{v^2} \frac{\partial^2 f}{\partial t^2}, \tag{A.1.3}$$

where $v$ is the wave velocity and $f$ the displacement of the propagation medium. This suggests electric and magnetic fields are capable of wavelike behaviour. By (A.1.3), an electromagnetic wave has a velocity of

$$\begin{aligned} v &= \frac{1}{\sqrt{\epsilon_0 \mu_0}} \\ &= 2.998 \times 10^8 \text{ ms}^{-1} \\ &= c, \end{aligned} \tag{A.1.4}$$

the measured velocity of light. Maxwell's Equations therefore imply that light is an electromagnetic wave. Such waves can be visualised from the equations as transverse-propagating electric and magnetic vector fields (Fig. A.1).

Experiments have confirmed that light can indeed be considered an electromagnetic wave, having a wavelength of between 400 and 750 nanometres depending on its colour. Other physical phenomena such as radiocommunications signals, microwaves and x-rays are also electromagnetic waves, with the only difference being the wavelength. The entire suite of electromagnetic phenomena is called the *electromagnetic spectrum*. In free space the velocity is always $c$, so the wave relation $v = f\lambda$ (f frequency, $\lambda$ wavelength) shows that

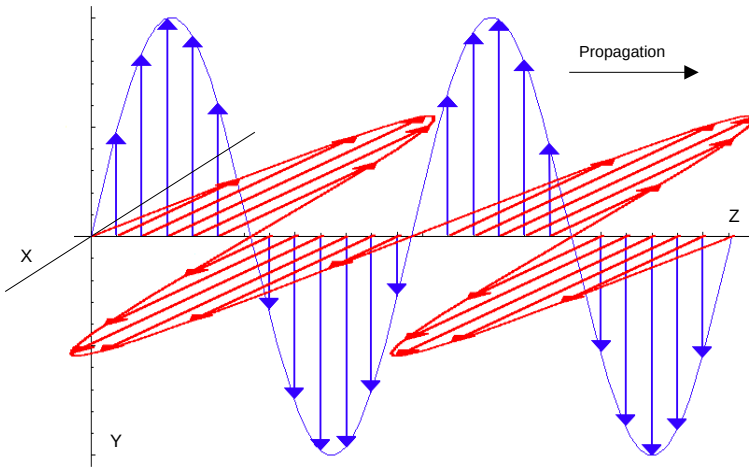


**Figure A.1:** A snapshot of an electromagnetic wave at some time $t$. The blue arrows represent an electric vector field, the red arrows a magnetic vector field. The fields oscillate sinusoidally, each inducing the other, causing a wave of fields to propagate in the mutually perpendicular direction.

the wavelength and frequency of oscillation are inversely proportional $\lambda = c\frac{1}{f}$. Accordingly, frequency and wavelength are often used interchangeably when describing the different parts of the electromagnetic spectrum.

The oscillating fields take the form of

$$\begin{aligned} &\tilde{\mathbf{E}}(z,t) = \tilde{\mathbf{E}}_{\mathbf{0}} \mathrm{e}^{\imath(kz-\omega t)} \qquad \tilde{\mathbf{B}}(z,t) = \tilde{\mathbf{B}}_{\mathbf{0}} \mathrm{e}^{\imath(kz-\omega t)} \\ &\text{where} \\ &\tilde{\mathbf{E}}_{\mathbf{0}} = \left(E_{0x}\hat{\mathbf{i}} + E_{0y}\hat{\mathbf{j}}\right) \mathrm{e}^{\imath\phi} \qquad \tilde{\mathbf{B}}_{\mathbf{0}} = \left(B_{0x}\hat{\mathbf{i}} + B_{0y}\hat{\mathbf{j}}\right) \mathrm{e}^{\imath\phi}. \end{aligned} \tag{A.1.5}$$

$\mathbf{E_0}, \mathbf{B_0}$ (the real parts of $\tilde{\mathbf{E}}_{\mathbf{0}}, \tilde{\mathbf{B}}_{\mathbf{0}}$) are the amplitude of the wave (also, as vector quantities, incorporating the initial directions of the fields) and $k = \frac{2\pi}{\lambda}$ is the *wave number*. The wave also transports energy as it propagates. The average power delivered per unit area is called the *intensity* $I \equiv \frac{1}{2}c\epsilon_0 E_0^2$. Equations (A.1.5) produce, in general, complex values for the $\mathbf{E}$ and $\mathbf{B}$ fields. The real part is manifest as the field's physical amplitude while the imaginary part contains phase information. The equation for, say, $\mathbf{E}$ could be rewritten as the purely real function

$$\mathbf{E}(z,t) = \mathbf{E_0} \cos(kz - \omega t + \phi). \tag{A.1.6}$$

In this case $\phi$ contains the phase information.

Turning now to electromagnetic waves in matter, it can be shown that for a linear, homogeneous medium Maxwell's Equations (A.1.1) hold apart from the substitution $\mu\epsilon$ for $\mu_0\epsilon_0$. This is replacing the permeability and permittivity of free space with the permeability and permittivity of the medium through which the wave is travelling. From the

wave equation (A.1.3) the velocity of light in such matter is

$$v = \frac{1}{\sqrt{\mu\epsilon}} = \frac{c}{n}$$
$$\text{where} \tag{A.1.7}$$
$$n \equiv \sqrt{\frac{\mu\epsilon}{\mu_0\epsilon_0}}$$

is the *refractive index* of the medium. For free space $n = 1$ and so $v = c$. In general for matter $n > 1$, and so $v < c$ meaning light slows as it travels through matter.

When light passes through the interface of two media of differing refractive indices, and at non-normal incidence, the propagation direction changes. This phenomenon is called *refraction*. It results from solutions to Maxwell's Equations in matter, using boundary conditions that reflect the change of medium. A simpler way of understanding refraction is shown in Fig. A.2.

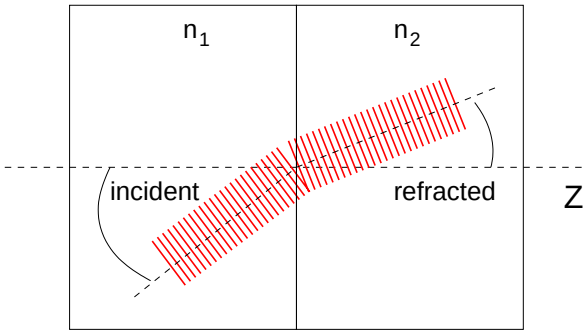


**Figure A.2:** Refraction: in this case $n_1 < n_2$ and so as the right hand side of the wavefront reaches the interface, it slows down relative to the left hand side which is still in the $n_1$ medium. This causes the wave to bend, changing the propagation direction.

The field of electromagnetism enabled many outstanding 20th century technologies, particularly communications technologies. It is well understood and widely covered in literature ([36] is an excellent introduction), and it is beyond the scope of this thesis to deliver a broad understanding of the field. Several classical phenomena are, however, of particular relevance to this project and so will be discussed for the remainder of this section.

## A.2 Polarisation

Fig. A.1 shows the electric field remaining in the X-Z plane throughout the length of propagation. If the Y-axis is defined as the vertical axis then such a wave is described as vertically *polarised*. The electric field is used by convention since there is no extra information in the position of the magnetic field - it is always perpendicular to the electric. Fig. A.3 is an X-Y slice at an arbitrary point along the Z-axis of Fig. A.1, showing the axis of polarisation.

The axis of polarisation, in simple cases, is determined by the source of the electromagnetic wave. When the polarisation stays on the same axis (in Fig. A.3 the Y-axis)

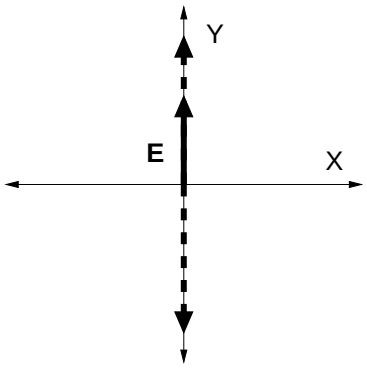


**Figure A.3:** An arbitrary X-Y slice in the graph of Fig. A.3, showing only the electric field vector. The dotted vector arrows indicate other possible values of the electric field, at other points on the Z-axis.

throughout the length of propagation the wave is said to be *linearly polarised*. The cases of vertical (also called s-polarisation), horizontal (also called p-polarisation) and diagonal polarisation are all linear. Diagonal polarisation is no different since, like any vector, the electric field can be separated into a linear combination of orthogonal components (Fig. A.4).

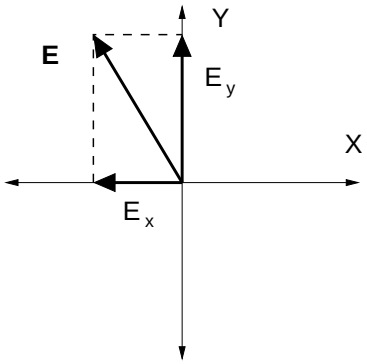


**Figure A.4:** Linear-diagonally polarised light can be considered a linear combination of vertically and horizontally polarised light.

The orthogonal components can be thought of as independent waves

$$\begin{aligned} \mathbf{E_x}\,(z,t) &= E_{0x}\cos\left(kz-\omega t+\phi_x\right)\hat{\mathbf{i}}, \\ \mathbf{E_y}\,(z,t) &= E_{0y}\cos\left(kz-\omega t+\phi_y\right)\hat{\mathbf{j}}. \end{aligned} \tag{A.2.1}$$

In the case of linear polarisation the resultant field vector at any point is $E_x\mathbf{i}+E_y\mathbf{j}$, since the two components are in-phase $\phi_x=\phi_y$.

The Lorentz electron oscillator model can be used to describe how polarised light is reflected. A result from the model is that there are certain situations in which s- and p-polarisation can be physically separated. This is useful not only for resolving the x,y components of diagonally polarised light, but also for operating on randomly-polarised

light. Randomly polarised light has the polarisation vector changing rapidly over time. It generally results from each atom in an emission medium transmitting at a different, changing polarisation. The net polarisation of all the atomic transmissions, while linear (since the atoms transmit in phase), constantly changes.

### A.2.1 Polarising Beam Splitter

A polarising beam splitter cube (Fig. A.5) consists of two prisms with a thin multilayered dielectric film between. A Lorenz treatment of such a situation can be found in [42]. The

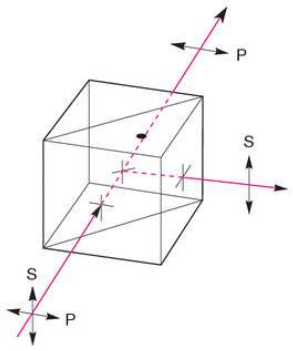


**Figure A.5:** A Polarising Beam Splitter cube (PBS) resolves incident light into s- and p- polarised beams, separated by 90°.[70]

cube is able to take diagonally or randomly polarised light and reflect (transmit) s- (p-) polarised light, at the convenient angle of 90°.

The ability of the cube to do this is dependant on the quality of the dielectric multilayer. The reflected (transmitted) beam will always retain some portion of p (s) light. A contemporary PBS has an extinction ratio of 1000:1, meaning unwanted polarisations will be present in the output beams with $\frac{1}{1000}$th of its original power. This is known as *bad polarisation*.

### A.2.2 Elliptic Polarisation

In the case of linear polarisation the X- and Y-components of the electric field, although treated as independent waves, are in phase $\phi_x = \phi_y$. It is possible that $\phi_x \neq \phi_y$ in which case the polarisation will be in different planes depending on $(z, t)$. It can be shown that in the X-Y plane **E** will sweep out an ellipse (Fig. A.6a) which manifests as a helical trace along the length of propagation (Fig. A.6b).

A special case of an ellipse is a circle. Circular polarisation is possible if $E_{0x} = E_{0y}$ and $\phi_x - \phi_y = \pm\frac{\pi}{2}$. The sign of $\frac{\pi}{2}$ will determine whether the helix twists in a left- or right-handed fashion. Another special case is a straight line. By the careful introduction of a phase difference, linearly polarised light can be rotated to change the angle of polarisation.

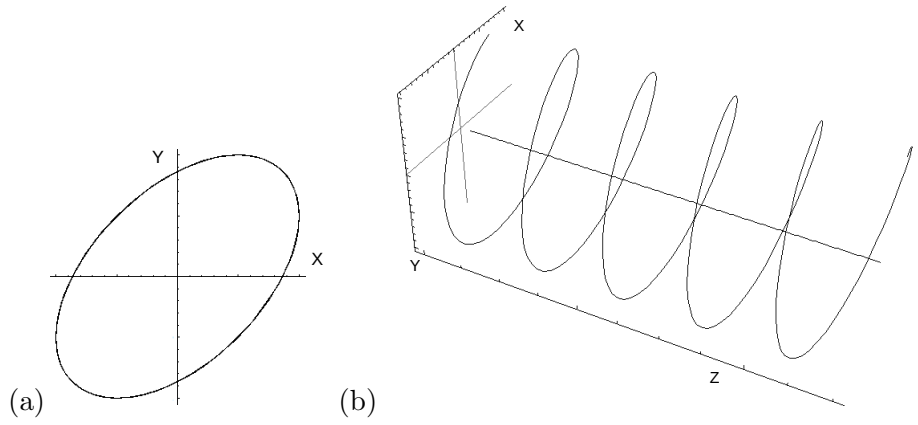


**Figure A.6:** Elliptic polarisation: (a) The X-Y trace of **E** when $\phi_x - \phi_y = \frac{\pi}{3}$ (b) Trace of **E** along the length of propagation at an arbitrary time $t$.

## A.3 Birefringence

*Refringence* is a legacy term meaning refraction. *Birefringence* refers to media having two indices of refraction, usually depending on the polarisation of the light entering. Historically one refractive index is called the ordinary, $n_o$ and the other extraordinary $n_e$. The difference $\triangle n = (n_e - n_o)$ is known as the birefringence of the material. The axis of the material in which light with a parallel electric field will travel faster is the *fast axis*; the axis perpendicular is the *slow axis*.

Since the speed at which an electromagnetic wave travels through matter is dependent on the refractive index, a physical mechanism for creating elliptically polarised light is apparent in birefringent materials. By slowing, say, the p-polarised component of a diagonally polarised beam a phase difference between the p and s components will be induced, leading to the effects described in A.2.2.

Birefringent materials may be cut with appropriate dimensions to cause a desired p-s phase difference for a given wavelength. A quarter-wave plate causes a $\frac{\pi}{2}$ phase difference which will convert linear light into elliptical light, except in the special case of the linear light being polarised at 45° to the slow/fast axes (so that $E_{0x} = E_{0y}$), when circular light will be produced.

A half-wave plate causes a $\pi$ phase difference. If linear light polarised at some angle $\theta$ to the fast axis is passed through, the effect will be to rotate the polarisation by $2\theta$, back through the fast axis. Elliptic light will be similarly flipped.

Quarter- and half-wave plates are generally manufactured in such a way as to be easily rotated. If linear light is present in an optics experiment, for example, a quarter-wave plate can be placed and rotated until circular light is achieved. Similarly a half wave plate can be rotated to take linear light at a set angle and produce linearly polarised light at any desired angle. This is a useful situation when variable-ratio beam splitting is needed. The combination of a half-wave plate and PBS allows optical power to be split at 90° at a desired ratio. The half-wave plate rotates the linear polarisation to the desired angle, with greater or smaller $x$ and $y$ component values; the PBS separates out the components to deliver the desired power-splitting ratio.

Birefringent materials themselves also present another method of separating out polar-

isations. The *Nicol*, *Glan-Foucault*, *Glan-Thompson* and *Wollaston* polarisers/polarising beam splitters all rely on birefringence to distinguish orthogonal polarisation components. The Glan-Thompson prism (Fig. A.7 is of particular use to this project since it has a much greater extinction ratio (as large as 1000,000:1) than the PBS, for use when very pure polarisation is required.

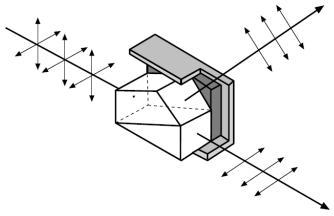

**Figure A.7**: A Glan-Thompson prism for removing bad polarisation.[23]

Appendix B

# LASER—Light Amplification by Stimulated Emission of Radiation

## B.1 Photons

Experiments with very low intensity light uncovered the fact that light is quantised. Reducing the intensity of a light source smoothly reduced the average power of the beam, as expected, but it did not smoothly reduce the instantaneous delivered energy. At very low intensities energy was delivered in packets, one at a time. Lowering the intensity further just decreased the frequency of packets arriving - the packets themselves did not reduce in energy. These packets are called *photons*, and their energy found to be dependent on their associated frequency $\nu$, via Plank's constant $h = 6.63 \times 10^{-34}$J-s,

$$E = h\nu. \tag{B.1.1}$$

Photons are not to be considered as classical 'billiard balls', however, since all such elementary/fundamental particles are subject to the laws of quantum mechanics, where particles are distinctly wave-like.

At high intensities the photons arrive so close together that any instantaneous measurement of energy is indistinguishable from that of a smooth wave. Every possible (quantised) value for the intensity corresponds to a state with energy

$$E_n = \left(n + \frac{1}{2}\right) h\nu, \tag{B.1.2}$$

where $n$ is the number of photons in the state, called a *number* state.

## B.2 Photon Emission

In section A.1 it was shown that electromagnetic radiation is the result of a changing electric/magnetic field. In the quantum model a photon is produced by an atom relaxing from an excited state. The frequency of the radiated photon corresponds to the energy of the atomic transition by (B.1.1). There are two processes by which an atom can emit a photon: spontaneous and stimulated emission.

Spontaneous emission comes about without any outside influence on the excited atom. Timewise it occurs as an exponential decay about the *transition lifetime*. The transition lifetime is dependant on the transition, the type of atom, and the number of atoms in the material that are also in excited states.

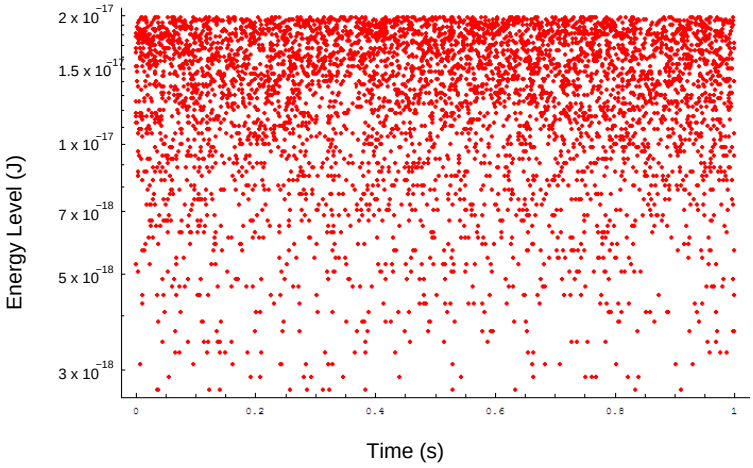


**Figure B.1:** Each dot represents a single photon's time of arrival at a detector after being emitted from a source of power $E$. The photons in this case are infrared $\nu = 3 \times 10^{14}$Hz. As the (quantised) power of the source increases, more photons arrive in the time frame, to the point where they are indistinguishable from a continuous power source.

Stimulated emission is a result of a photon interacting with an excited atom. If the photon's energy is within the transition linewidth the atom will de-excite and emit a second photon. The second photon will be identical to the first, and travelling in-phase. The two photons are considered to be *coherent*. If the material contains enough excited atoms, if most of the emitted photons are somehow recycled to stimulate more atoms, and if the relaxed atoms can be continually re-excited (this is called *pumping*), then a single photon can be amplified to numbers limited only by physical considerations. Materials that can be pumped in this way are called *gain media*. The pumping process may be either optical or electrical. figure - amount stimulated emissions vs frequency

## B.3 Optical Resonators

Section B.2 described how photons within a small range of frequencies can cause stimulated emission when encountering excited atoms. An optical resonator also has the ability to use photons within a small range of frequencies, and in general this range can be much smaller than the transition linewidth. It also has the convenient ability to 'recycle' photons through a piece of material.

The simplest resonator consists of two plane mirrors facing one another (Fig. B.2). This is called a *Fabry-Perot etalon*. Returning to Maxwell's Equations, using the mirrors as boundary conditions results in a system where only photons of certain frequencies will continually bounce between the mirrors. In other words, only electromagnetic waves of certain frequencies will form the required standing wave between the mirrors.

The solution to a lossless Fabry-Perot results in discrete values for the frequency of the standing wave (Fig. B.3(light blue)).

$$\nu_q = q\frac{c}{2d}, \qquad q = 1, 2, \ldots, \tag{B.3.1}$$

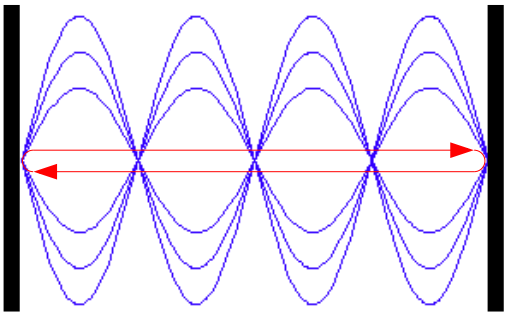

**Figure B.2:** A planar resonator (Fabry-Perot etalon). The blue graph represents values of the (vertical) electric field as the resonator oscillates. The red path indicates the path taken by photons in the equivalent quantum model.

where d is the distance between the mirrors. Each wave-solution is called a *mode*; the integer $q$ is the *mode number*.[87]

Practically, the Fabry-Perot mirrors are not perfect reflectors and so each time the wave oscillates it will reduce slightly in amplitude. In the quantum model this means that each time a photon bounces between the mirrors there will be a probability that it will be absorbed by the mirror. Using $\mathcal{R}$ as the amplitude attenuation factor ($\mathcal{R} = 1$ a perfect resonator) of each mirror and $\nu_F = \frac{c}{2d}$ as the free spectral range (FSR) (the spectral mode spacing), [87] writes the formula for the intensity of the light in the Fabry-Perot as

$$I = \frac{I_0}{(1-\mathcal{R})^2} \frac{1}{1 + (2\mathcal{F}/\pi)^2 \sin^2(\pi\nu/\nu_F)},$$
where
$$\mathcal{F} = \frac{\pi\sqrt{\mathcal{R}}}{1-\mathcal{R}}. \tag{B.3.2}$$

$\mathcal{F}$ is called the *finesse*. A perfectly reflecting resonator has infinite finesse, with the quality decreasing as finesse decreases (good quality resonators support large oscillations for a narrow range of frequencies). It follows that the finesse can also be defined as the ratio of the FSR to the Full Width Half Maximum $\Delta\nu$(the width of the resonance peak at half-height)

$$\mathcal{F} = \nu_F/\Delta\nu. \tag{B.3.3}$$

If, by a mechanism such as stimulated emission of a gain medium, photons continue to be emitted from inside the resonator at a greater rate than they are absorbed by the medium and resonator mirrors, then Light Amplification by the Stimulated Emission of Radiation (LASER) is obtained. This point is called *threshold*.

## B.4 Lasers

A simple alliance between stimulated emission and an optical resonator might look like Fig. B.4.

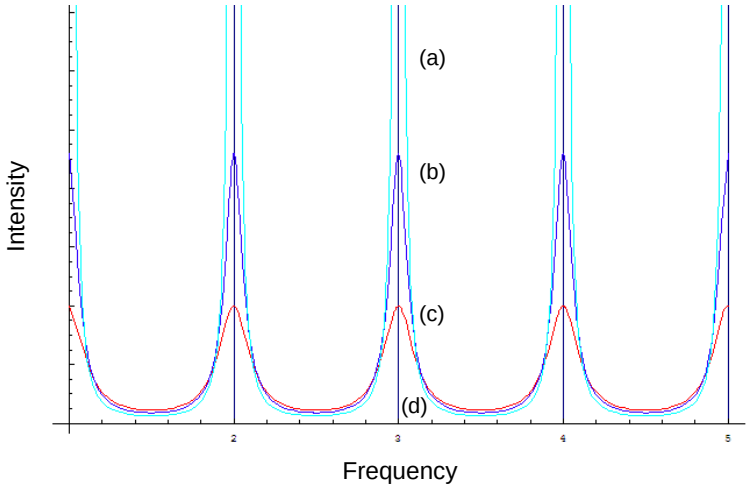


**Figure B.3:** Fabry-Perot modes for (a)(aqua) $\mathcal{R} = 0.99$, (b)(blue) $\mathcal{R} = 0.67$, (c)(red) $\mathcal{R} = 0.5$, (d)(light blue) $\mathcal{R} = 1$ over modes 1-5

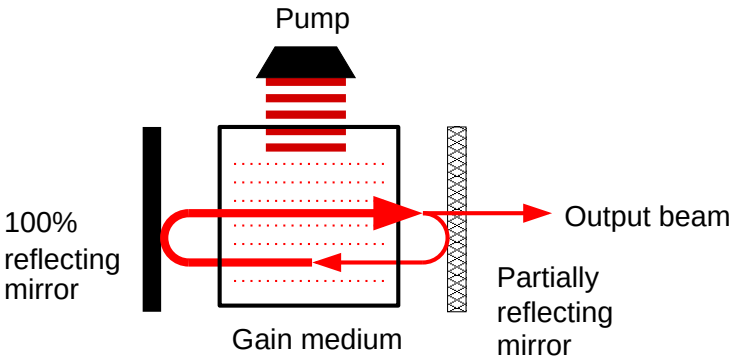


**Figure B.4:** A simple laser, where a pumped gain medium provides a supply of photons from within a resonator. The stimulated emission must produce more photons than are absorbed by the gain medium and mirrors or lost through the partially reflecting output mirror in order for the laser to operate continuously.

The light passing through the partially reflecting mirror can only have frequencies allowed by both the pumped gain medium and the resonating cavity (Fig. B.5). By adjusting the resonator design and gain medium properties, the laser can be customised to almost any application. For a given laser, the wavelength of radiation can usually be adjusted within a small range by manipulating the resonator, gain medium or pump with thermal and electrical effects. Two common methods of 'tuning' the laser is to either thermally adjust the length of the resonator (so that each mode's position on the spectrum will be moved), or to thermally adjust the pump to maximise gain around a different resonator mode.

If the bandwidth of the gain media is too wide, or the FSR too small, *multi-mode* operation occurs where the laser radiates at multiple frequencies (Fig. B.5c). This situation is satisfactory for many laser applications such as welding, medicine, communications, printing, pointing or alignment. Many scientific applications (interferometry, spectroscopy, quantum communication) require *single-mode* operation where the gain bandwidth is narrow enough so that only one mode of the cavity dominates (Fig. B.5a).

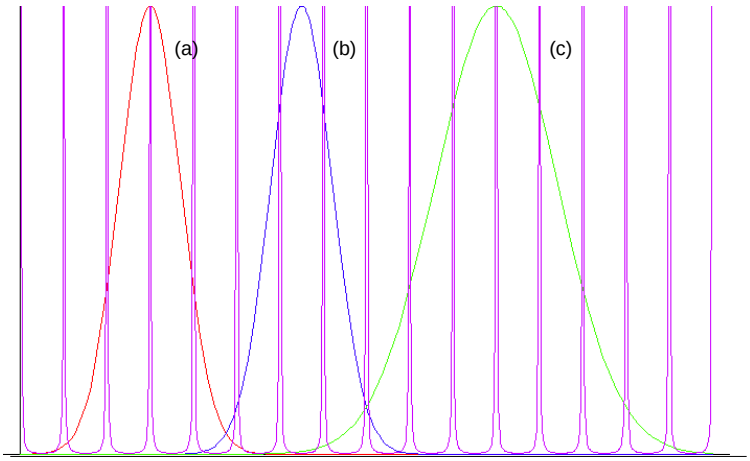


**Figure B.5:** Gain media spectra overlaid on a resonator spectrum: (a)(red) Single-mode stable operation; (b)(blue) Mode hop during single-mode laser tuning; (c)(light green) Multi-mode operation.

A single-mode laser is still capable of multi-mode operation. As the gain medium is tuned there will be some bands for which two cavity modes compete and the laser will fluctuate between the two (Fig. B.5b). The switch from the domination of one mode to another during the tuning process is called a *mode hop*.

**Appendix C**

# Hermite-Gaussian Modes

The Gaussian beam is not the only solution to the paraxial wave equation. Other self-reproducing beams can also exist in a resonator that has mirrors matching the curvature of the wavefront at reflection. This family of solutions are called Hermite-Gaussian beams.

$$I_{l,m}(x,y,z) = |A_{l,m}|^2 \left(\frac{W_0}{W(z)}\right)^2 \mathrm{G}_l^2\left(\frac{\sqrt{2}x}{W(z)}\right) \mathrm{G}_m^2\left(\frac{\sqrt{2}y}{W(z)}\right) \tag{C.0.1}$$

where $\mathrm{G}_i(u)$ is the Hermite-Gaussian function

$$\mathrm{H}_i(u)\exp\left(\frac{-u^2}{2}\right), \quad i = 0,1,2,\ldots, \tag{C.0.2}$$

and $\mathrm{H}_i(u)$ is one of the Hermite polynomials, which are defined by the recurrence relation

$$\mathrm{H}_{i+1}(u) = 2u\mathrm{H}_i(u) - 2i\mathrm{H}_{i-1}(u).[87] \tag{C.0.3}$$

The Hermite-Gaussian resonator modes are also called $\mathrm{TEM}_{lm}$ (Transverse Electric Magnetic) modes. The Gaussian mode of section 3.3.1 is the $\mathrm{TEM}_{00}$ mode, profiles of this mode and higher order modes are shown in Fig. C.1.[87]

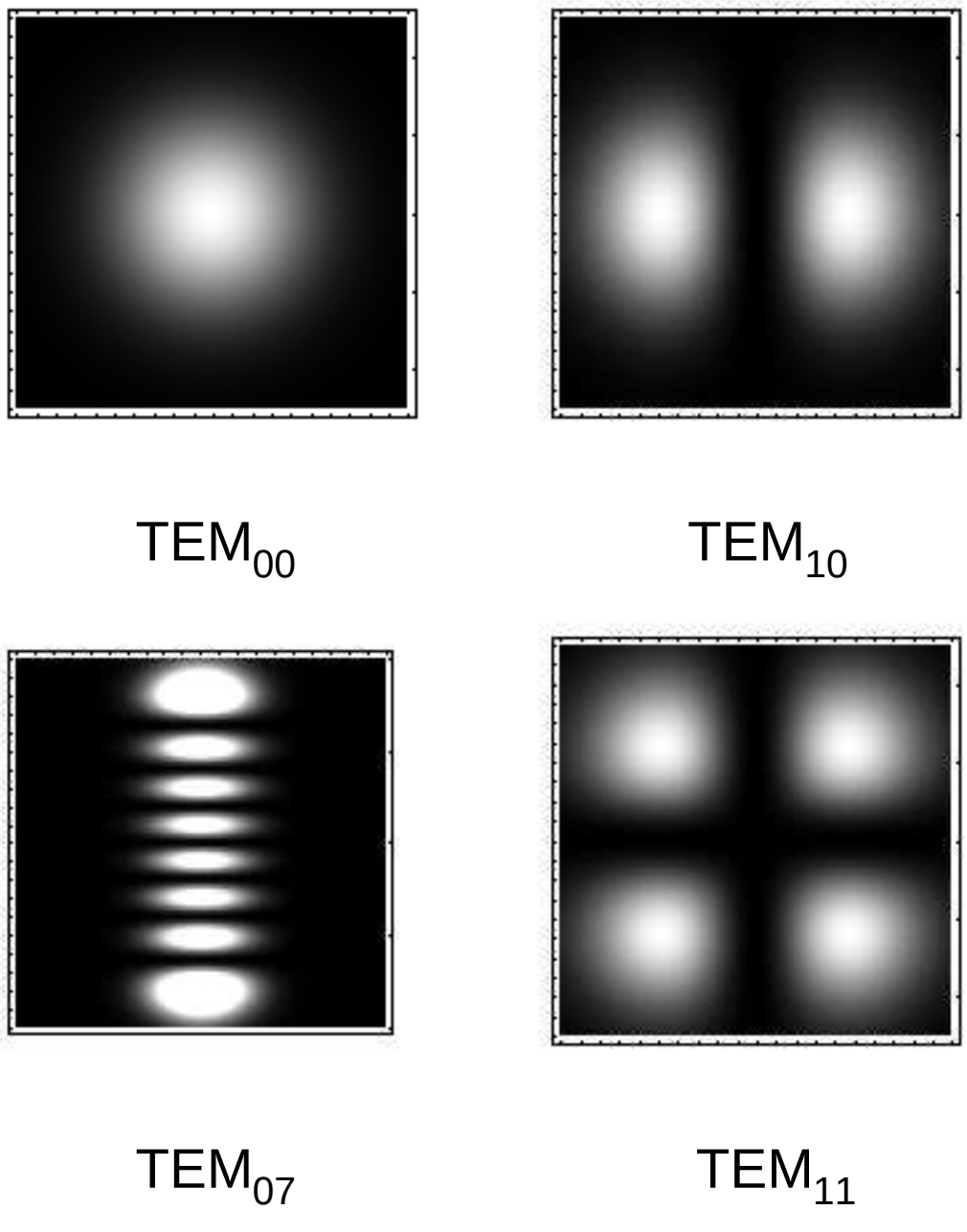


**Figure C.1**: X-Y profiles of Hermite-Gaussian beams.

# Demultiplexing Code

This is the *Mathematica* code used to demultiplex the 100 MHz of acquired data into 20 files of 5 MHz each.

## Filenames and Other Constants

```
<< CleanSlate.m
link =
Install["C:\\Program Files\\Wolfram Research\\Mathematica\\4.2\\
AddOns\\Applications\\binary"];
Off[General::spell];
Off[General::spell1];
DataFilePath =
"C:\\Documents and Settings\\User\\My Documents\\Experimental Data
\\060502";
Data$\eta$FileName = "T100-"; (* Signal Record *)
DataSNFileName = "SN";
DataDNFileName = "DN";
ExportDataFileName = "dm"; (* < existingfilename > dm < channelnumber > *)
NumberOfRecords = 1;
DataLength = 2400000;

PhaseChannelin = 2;
AmpChannelin = 1;
PhaseChannelout = 4;
AmpChannelout = 3;

SincOrder = 200;

InitialSampleRate = 200 (* MSample/sec *);
ChannelWidth = 5; (*MHz*)

<< Statistics`DescriptiveStatistics`
```

## Functions

```
Sinc[x_]:=If[x==0, 1, Sin[Pix]/(Pix)];

SincTable = Table[{x, Sinc[x]}, {x, (-1.5SincOrder), (1.5  SincOrder), 0.01}];

SincInterp = Interpolation[SincTable];

BandPass[intab_]:=ListConvolve[BPTable, intab];

Demodulate[data_, freq_]:=
Table [√2data[[i]] * Cos[freq/InitialSampleRatePi * 2 * i],
{i, 1, Length[data]}];

DownSample[intab_, inF_, outF_]:=
If[FractionalPart[inF/outF] ≠ 0,
√2outF/inF
Table[Sum[intab[[i + Floor[j * inF/outF]]]
SincInterp[outF/inF(i - FractionalPart[j * inF/outF])]
, {i, -SincOrder, SincOrder}
]
, {j, 1 + Floor[(SincOrder)outF/inF],
Floor[(Length[intab] - SincOrder)outF/inF]}
],
SincTable = Table[Sinc[outF/inFi], {i, -SincOrder, SincOrder}];
LCTable = ListCorrelate[SincTable, intab];
√2outF/inFTable[LCTable[[iinF/outF]], {i, Length[LCTable]outF/inF}]
];

PowerSpectrum[Intab_, Bandwidth_]:=
Module[{FIntab, LFintab}, LFIntab = Floor[Length[Intab]/2];
FIntab = (10Log[10, Take[Abs[Fourier[Intab]]^2, LFIntab]]);
Table[{(i - 1)Bandwidth/LFIntab, FIntab[[i]]}, {i, 1, LFIntab}]];

TransfertFunction[Intab_, Outtab_, Bandwidth_]:=
Module[{FIntab, LFintab, FOuttab}, LFIntab = Floor[Length[Intab]/2];
FIntab = Fourier[Intab];
FOuttab = Fourier[Outtab];
Table[{(i - 1)Bandwidth/LFIntab, FOuttab[[i]]/FIntab[[i]]},
{i, 1, Length[Intab]}]];

Smooth[Intab_, SmoothFactor_]:=
Module[{kern},
kern = Table[Exp[-n^2/(SmoothFactor^2/3)]/Sqrt[PiSmoothFactor^2/6],
{n, -SmoothFactor, SmoothFactor}];
Transpose[{Drop[Drop[Transpose[Intab][[1]], SmoothFactor], -SmoothFactor],
ListConvolve[kern, Transpose[Intab][[2]], {-1, 1}]}]];
```

```
KIRSmooth[Intab_, SmoothFactor_]:=
Module[{kern, kernFactor, Intab2, temp},
kernFactor = Sum[Exp[-nn^2/(SmoothFactor^2/3)],
{nn, -SmoothFactor, SmoothFactor}];
kern = Table[Exp[-n^2/(SmoothFactor^2/3)]/kernFactor,
{n, -SmoothFactor, SmoothFactor}];
Intab2 = Drop[Transpose[Take[Intab, Length[Intab]/2]][[2]], 1];
temp = Join[
Table[Sum[kern[[SmoothFactor + 1 + j]]Intab2[[i + j]],
{j, -(i - 1), SmoothFactor}]/
Sum[kern[[SmoothFactor + 1 + j]], {j, -(i - 1), SmoothFactor}],
{i, 1, SmoothFactor}],
ListConvolve[kern, Intab2, {-1, 1}],
Table[Sum[kern[[SmoothFactor + 1 + j]]Intab2[[Length[Intab2] + i + j]],
{j, -SmoothFactor, -i}]/Sum[kern[[SmoothFactor + 1 + j]],
{j, -SmoothFactor, -i}], {i, -SmoothFactor + 1, 0}]];
Transpose[{Transpose[Intab][[1]],
Join[{Transpose[Intab][[2, 1]]}, temp,
{Transpose[Intab][[2, Length[Intab]/2 + 1]]},
Reverse[N[Conjugate[N[temp]]]]
}]];
```

## QKD Data Import/Demultiplexing/Export

```
SetDirectory[DataFilePath];
Xsig = ReadListBinary[Data$\eta$FileName <> "1" <> ".dat", SignedInt16,
DataLength * 4, ByteOrder -> MostSignificantByteFirst];
tab$\eta$Ampin = Table[N[Xsig[[i]]/2048], {i, AmpChannelin, Length[Xsig], 4}];
tab$\eta$Phasein = Table[N[Xsig[[i]]/2048], {i, PhaseChannelin, Length[Xsig], 4}];
tab$\eta$Ampout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tab$\eta$Phaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
Print["XaAmp is ", Length[tab$\eta$Ampin], " points"];
Clear[Xsig];

Xsig = ReadListBinary[DataSNFileName <> "4" <> ".dat", SignedInt16,
DataLength * 4, ByteOrder -> MostSignificantByteFirst];
tabSNAmpout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabSNPhaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
Print["XbAmp is ", Length[tabSNAmpout], " points"];
Clear[Xsig];

Xsig = ReadListBinary[DataDNFileName <> "1" <> ".dat", SignedInt16,
DataLength * 4, ByteOrder -> MostSignificantByteFirst];
tabDNAmpout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabDNPhaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
```

```
Print["XbAmp is ", Length[tabDNAmpout], " points"];
Clear[Xsig];
For[i = 1, i ≤ (InitialSampleRate/2)/ChannelWidth, i++,
HighFrequency = i * ChannelWidth;
LowFrequency = HighFrequency − ChannelWidth;

BPTable = Table[2(HighFrequency − LowFrequency)/InitialSampleRate
Sinc[(HighFrequency − LowFrequency)/InitialSampleRatei]
Cos[Pi(HighFrequency + LowFrequency)/InitialSampleRatei],
{i, −(1 + Floor[InitialSampleRate/(HighFrequency − LowFrequency)])SincOrder,
(1 + Floor[InitialSampleRate/(HighFrequency − LowFrequency)])SincOrder}];

tabηAmpinBP = BandPass[tabηAmpin];
tabηPhaseinBP = BandPass[tabηPhasein];
tabηAmpoutBP = BandPass[tabηAmpout];
tabηPhaseoutBP = BandPass[tabηPhaseout];
Print["."];

tabηAmpindemod = Demodulate[tabηAmpinBP, LowFrequency];
tabηPhaseindemod = Demodulate[tabηPhaseinBP, LowFrequency];
tabηAmpoutdemod = Demodulate[tabηAmpoutBP, LowFrequency];
tabηPhaseoutdemod = Demodulate[tabηPhaseoutBP, LowFrequency];
Print["."];
Clear[tabηAmpinBP, tabηPhaseinBP, tabηAmpoutBP, tabηPhaseoutBP];

tabηAmpindemodds = DownSample[tabηAmpindemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
 tabηPhaseindemodds = DownSample[tabηPhaseindemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
 tabηAmpoutdemodds = DownSample[tabηAmpoutdemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
 tabηPhaseoutdemodds = DownSample[tabηPhaseoutdemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
Print["Signal channel ", i, " demultiplexed ", SessionTime[]];
ChannelDataLength = Length[tabηAmpindemodds];
Clear[tabηAmpindemod, tabηPhaseindemod, tabηAmpoutdemod,
tabηPhaseoutdemod];

ExportSig = Table[0, {ChannelDataLength * 4}];
For[j = 0, j < Length[ExportSig], j = j + 4,
ExportSig[[j + AmpChannelin]] = tabηAmpindemodds[[j/4 + 1]];
ExportSig[[j + PhaseChannelin]] = tabηPhaseindemodds[[j/4 + 1]];
ExportSig[[j + AmpChannelout]] = tabηAmpoutdemodds[[j/4 + 1]];
ExportSig[[j + PhaseChannelout]] = tabηPhaseoutdemodds[[j/4 + 1]]];
WriteBinary[DataηFileName <> "1" <> ExportDataFileName <> ToString[i] <>
".dat", Round[ExportSig * 2048], SignedInt16,
ByteOrder → MostSignificantByteFirst];
Print["Signal channel ", ToString[i], " file written ", SessionTime[]];
```

```
Clear[ExportSig, tabηAmpindemodds, tabηPhaseindemodds, tabηAmpoutdemodds,
tabηPhaseoutdemodds];



tabSNAmpoutBP = BandPass[tabSNAmpout];
tabSNPhaseoutBP = BandPass[tabSNPhaseout];
Print["."];

tabSNAmpoutdemod = Demodulate[tabSNAmpoutBP, LowFrequency];
tabSNPhaseoutdemod = Demodulate[tabSNPhaseoutBP, LowFrequency];
Clear[tabSNAmpoutBP, tabSNPhaseoutBP];
Print["."];

tabSNAmpoutdemodds = DownSample[tabSNAmpoutdemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
tabSNPhaseoutdemodds = DownSample[tabSNPhaseoutdemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
Clear[tabSNAmpoutdemod, tabSNPhaseoutdemod];
ChannelDataLength = Length[tabSNAmpoutdemodds];
Print["Shot noise channel ", i, " demultiplexed ", SessionTime[]];
Print["Shot noise ds data ", Take[tabSNAmpoutdemodds, 5], ", ",
Take[tabSNPhaseoutdemodds, 5]];

ExportSN = Table[0, {ChannelDataLength ∗ 4}];
For[j = 0, j < Length[ExportSN], j = j + 4,
ExportSN[[j + AmpChannelin]] = 0;
ExportSN[[j + PhaseChannelin]] = 0;
ExportSN[[j + AmpChannelout]] = tabSNAmpoutdemodds[[j/4 + 1]];
ExportSN[[j + PhaseChannelout]] = tabSNPhaseoutdemodds[[j/4 + 1]]];
WriteBinary[DataSNFileName <> "4" <> ExportDataFileName <> ToString[i] <>
".dat", Round[ExportSN ∗ 2048], SignedInt16,
ByteOrder → MostSignificantByteFirst];
Print["Shot noise channel ", ToString[i], " file written ", SessionTime[]];
Print["Shot noise written data ", Take[ExportSN, 4]];
Clear[ExportSN, tabSNAmpoutdemodds, tabSNPhaseoutdemodds];



tabDNAmpoutBP = BandPass[tabDNAmpout];
tabDNPhaseoutBP = BandPass[tabDNPhaseout];
Print["."];

tabDNAmpoutdemod = Demodulate[tabDNAmpoutBP, LowFrequency];
tabDNPhaseoutdemod = Demodulate[tabDNPhaseoutBP, LowFrequency];
Clear[tabDNAmpoutBP, tabDNPhaseoutBP];
Print["."];
```

```
tabDNAmpoutdemodds = DownSample[tabDNAmpoutdemod, InitialSampleRate/2,
HighFrequency - LowFrequency];
tabDNPhaseoutdemodds = DownSample[tabDNPhaseoutdemod, InitialSampleRate/2,
HighFrequency - LowFrequency];
Clear[tabDNAmpoutdemod, tabDNPhaseoutdemod];
ChannelDataLength = Length[tabDNAmpoutdemodds];
Print["Dark noise channel ", i, " demultiplexed ", SessionTime[]];
Print["Dark noise ds data ", Take[tabDNAmpoutdemodds, 5], ", ",
Take[tabDNPhaseoutdemodds, 5]];

ExportDN = Table[0, {ChannelDataLength * 4}];
For[j = 0, j < Length[ExportDN], j = j + 4,
ExportDN[[j + AmpChannelin]] = 0;
ExportDN[[j + PhaseChannelin]] = 0;
ExportDN[[j + AmpChannelout]] = tabDNAmpoutdemodds[[j/4 + 1]];
ExportDN[[j + PhaseChannelout]] = tabDNPhaseoutdemodds[[j/4 + 1]]];
WriteBinary[DataDNFileName <> "1" <> ExportDataFileName <> ToString[i] <>
".dat", Round[ExportDN * 2048], SignedInt16,
ByteOrder → MostSignificantByteFirst];
Print["Dark noise channel ", ToString[i], " file written ", SessionTime[]];
Print["Dark noise written data ", Take[ExportDN, 3]];
Clear[ExportDN, tabDNAmpoutdemodds, tabDNPhaseoutdemodds];
]
Clear[tabDNAmpout, tabDNPhaseout, tabηAmpin, tabηPhasein, tabηAmpout,
tabηPhaseout];
```

**Appendix E**

# Data Analysis Code

This is the *Mathematica* code used to examine the demultiplexed data and calculate channel information rates. Although I made a number of modifications, the majority of this code has been reused from the first generation experiment.

## Filenames and other constants

```
StartTime = SessionTime[];
<< CleanSlate.m
link =
Install["C:\\Program Files\\Wolfram Research\\Mathematica\\4.2\\
AddOns\\Applications\\binary"];
Off[General::spell]; Off[General::spell1];
DataFilePath =
"C:\\Documents and Settings\\User\\My Documents\\Experimental
Data\\060502";
Data$\eta$FileName = "T100-"; (* Signal Record *)
DataSNFileName = "SN";
DataDNFileName = "DN";
NumberOfRecords = 1;
DataLength = 100000;


<< Statistics`DescriptiveStatistics`
<< Statistics`MultiDescriptiveStatistics`
<< Statistics`NormalDistribution`
<< Statistics`ConfidenceIntervals`
<< Graphics`Graphics`
<< Graphics`FilledPlot`
<< Graphics`MultipleListPlot`



PhaseChannelin = 2;
AmpChannelin = 1;
PhaseChannelout = 4;
AmpChannelout = 3;
```

```
LowFrequency = 30(*MHz*);
HighFrequency = 80(*MHz*);
InitialSampleRate = 200 (* MSample/sec *);

SincOrder = 100;
GridOTXa = 201;
GridOTη = 101;


kthreshold = .02;
thresholdmin = 0;
thresholdmax = 2;

ErrorSteps = .01;
```

## Functions

```
Sinc[x_]:=If[x==0, 1, Sin[Pix]/(Pix)];
SincTable = Table[{x, Sinc[x]}, {x, (−1.5SincOrder), (1.5 SincOrder), 0.01}];
SincInterp = Interpolation[SincTable];
BPTable =
Table[2(HighFrequency − LowFrequency)/InitialSampleRate
Sinc[(HighFrequency − LowFrequency)/InitialSampleRatei]
Cos[Pi(HighFrequency + LowFrequency)/InitialSampleRatei],
{i, −(1 + Floor[InitialSampleRate/(HighFrequency − LowFrequency)])SincOrder,
(1 + Floor[InitialSampleRate/(HighFrequency − LowFrequency)])SincOrder}];
BandPass[intab_]:=ListConvolve[BPTable, intab];
Demodulate[data_]:=
Table [√2data[[i]] ∗ Cos[LowFrequency/InitialSampleRatePi ∗ 2 ∗ i],
{i, 1, Length[data]}];
DownSample[intab_, inF_, outF_]:=
If[FractionalPart[inF/outF] ≠ 0,
√2outF/inF
Table[Sum[intab[[i + Floor[j ∗ inF/outF]]]
SincInterp[outF/inF(i − FractionalPart[j ∗ inF/outF])]
, {i, −SincOrder, SincOrder}
]
, {j, 1 + Floor[(SincOrder)outF/inF],
Floor[(Length[intab] − SincOrder)outF/inF]}
],
SincTable = Table[Sinc[outF/inFi], {i, −SincOrder, SincOrder}];
LCTable = ListCorrelate[SincTable, intab];
√2outF/inFTable[LCTable[[iinF/outF]], {i, Length[LCTable]outF/inF}]
];
Delt[a_]:=a[[2]]−a[[1]]/2;
```

### Transfer Function Characterisation Functions

```
PowerSpectrum[Intab_, Bandwidth_]:=
Module[{FIntab, LFintab}, LFIntab = Floor[Length[Intab]/2];
FIntab = (10Log[10, Take[Abs[Fourier[Intab]]^2, LFIntab]]);
Table[{(i - 1)Bandwidth/LFIntab, FIntab[[i]]}, {i, 1, LFIntab}]];

TransfertFunction[Intab_, Outtab_, Bandwidth_]:=
Module[{FIntab, LFintab, FOuttab}, LFIntab = Floor[Length[Intab]/2];
FIntab = Fourier[Intab];
FOuttab = Fourier[Outtab];
Table[{(i - 1)Bandwidth/LFIntab, FOuttab[[i]]/FIntab[[i]]},
{i, 1, Length[Intab]}]];

Smooth[Intab_, SmoothFactor_]:=
Module[{kern},
kern = Table[Exp[-n^2/(SmoothFactor^2/3)]/Sqrt[PiSmoothFactor^2/6],
{n, -SmoothFactor, SmoothFactor}];
Transpose[{Drop[Drop[Transpose[Intab][[1]], SmoothFactor], -SmoothFactor],
ListConvolve[kern, Transpose[Intab][[2]], {-1, 1}]}]];

KIRSmooth[Intab_, SmoothFactor_]:=
Module[{kern, kernFactor, Intab2, temp},
kernFactor = Sum[Exp[-nn^2/(SmoothFactor^2/3)],
{nn, -SmoothFactor, SmoothFactor}];
kern = Table[Exp[-n^2/(SmoothFactor^2/3)]/kernFactor,
{n, -SmoothFactor, SmoothFactor}];
Intab2 = Drop[Transpose[Take[Intab, Length[Intab]/2]][[2]], 1];
temp = Join[
Table[Sum[kern[[SmoothFactor + 1 + j]]Intab2[[i + j]],
{j, -(i - 1), SmoothFactor}]/
Sum[kern[[SmoothFactor + 1 + j]], {j, -(i - 1), SmoothFactor}],
{i, 1, SmoothFactor}],
ListConvolve[kern, Intab2, {-1, 1}],
Table[Sum[kern[[SmoothFactor + 1 + j]]Intab2[[Length[Intab2] + i + j]],
{j, -SmoothFactor, -i}]/Sum[kern[[SmoothFactor + 1 + j]],
{j, -SmoothFactor, -i}], {i, -SmoothFactor + 1, 0}]];
Transpose[{Transpose[Intab][[1]],
Join[{Transpose[Intab][[2, 1]]}, temp,
{Transpose[Intab][[2, Length[Intab]/2 + 1]]},
Reverse[N[Conjugate[N[temp]]]]]
}]];
```

## Data and Modules Import/Data Extraction

### Full Bandwidth Data Extraction

```
SetDirectory[DataFilePath];
Xsig = ReadListBinary[Data$\eta$FileName <> "1" <> ".dat", SignedInt16,
```

```
DataLength * 4, ByteOrder → MostSignificantByteFirst];
tabηAmpin = Table[N[Xsig[[i]]/2048], {i, AmpChannelin, Length[Xsig], 4}];
tabηPhasein = Table[N[Xsig[[i]]/2048], {i, PhaseChannelin, Length[Xsig], 4}];
tabηAmpout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabηPhaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
Print["XaAmp is ", Length[tabηAmpin], " points"];
Clear[Xsig];

tabηAmpinBP = BandPass[tabηAmpin];
Print[SessionTime[]];
tabηPhaseinBP = BandPass[tabηPhasein];
Print[SessionTime[]];
tabηAmpoutBP = BandPass[tabηAmpout];
Print[SessionTime[]];
tabηPhaseoutBP = BandPass[tabηPhaseout];
Print[SessionTime[]];
Print["."];
Clear[tabηAmpin, tabηPhasein, tabηAmpout, tabηPhaseout];

tabηAmpindemod = Demodulate[tabηAmpinBP];
Print[SessionTime[]];
tabηPhaseindemod = Demodulate[tabηPhaseinBP];
Print[SessionTime[]];
tabηAmpoutdemod = Demodulate[tabηAmpoutBP];
Print[SessionTime[]];
tabηPhaseoutdemod = Demodulate[tabηPhaseoutBP];
Print[SessionTime[]];
Print["."];
Clear[tabηAmpinBP, tabηPhaseinBP, tabηAmpoutBP, tabηPhaseoutBP];

tabηAmpindemodds = DownSample[tabηAmpindemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
Print[SessionTime[]];
 tabηPhaseindemodds = DownSample[tabηPhaseindemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
Print[SessionTime[]];
 tabηAmpoutdemodds = DownSample[tabηAmpoutdemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
Print[SessionTime[]];
 tabηPhaseoutdemodds = DownSample[tabηPhaseoutdemod, InitialSampleRate/2,
HighFrequency − LowFrequency];
Print[SessionTime[]];
Print["."];
Clear[tabηAmpindemod, tabηPhaseindemod, tabηAmpoutdemod,
tabηPhaseoutdemod];
```

```
Xsig = ReadListBinary[DataSNFileName <> "1" <> ".dat", SignedInt16,
DataLength * 4, ByteOrder → MostSignificantByteFirst];
tabSNAmpout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabSNPhaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
Clear[Xsig];

Print["."];
tabSNAmpoutBP = BandPass[tabSNAmpout];
tabSNPhaseoutBP = BandPass[tabSNPhaseout];
Clear[tabSNAmpout, tabSNPhaseout];
Print["."];
tabSNAmpoutdemod = Demodulate[tabSNAmpoutBP];
tabSNPhaseoutdemod = Demodulate[tabSNPhaseoutBP];
Clear[tabSNAmpoutBP, tabSNPhaseoutBP];
Print["."];
tabSNAmpoutdemodds = DownSample[tabSNAmpoutdemod, InitialSampleRate/2,
HighFrequency - LowFrequency];
tabSNPhaseoutdemodds = DownSample[tabSNPhaseoutdemod, InitialSampleRate/2,
HighFrequency - LowFrequency];
Clear[tabSNAmpoutdemod, tabSNPhaseoutdemod];
Print["."];

Xsig = ReadListBinary[DataDNFileName <> "1" <> ".dat", SignedInt16,
DataLength * 4, ByteOrder → MostSignificantByteFirst];
tabDNAmpout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabDNPhaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
Clear[Xsig];

tabDNAmpoutBP = BandPass[tabDNAmpout];
tabDNPhaseoutBP = BandPass[tabDNPhaseout];
Clear[tabDNAmpout, tabDNPhaseout];

tabDNAmpoutdemod = Demodulate[tabDNAmpoutBP];
tabDNPhaseoutdemod = Demodulate[tabDNPhaseoutBP];
Clear[tabDNAmpoutBP, tabDNPhaseoutBP];

tabDNAmpoutdemodds = DownSample[tabDNAmpoutdemod, InitialSampleRate/2,
HighFrequency - LowFrequency];
tabDNPhaseoutdemodds = DownSample[tabDNPhaseoutdemod, InitialSampleRate/2,
HighFrequency - LowFrequency];
Clear[tabDNAmpoutdemod, tabDNPhaseoutdemod];
```

### Transfer Function Characterisation

```
Ptabηampindemodds = PowerSpectrum[tabηAmpindemodds, 50*^6];
Ptabηphaseindemodds = PowerSpectrum[tabηPhaseindemodds, 50*^6];
```

```
Ptabη Ampoutdemodds = PowerSpectrum[tabη Ampoutdemodds, 50*^6];
Ptabη Phaseoutdemodds = PowerSpectrum[tabη Phaseoutdemodds, 50*^6];
ListPlot[Ptabη Ampindemodds]
ListPlot[Ptabη Phaseindemodds]
ListPlot[Ptabη Ampoutdemodds]
ListPlot[Ptabη Phaseoutdemodds]
Xsig = ReadListBinary[Data η FileName <> "1" <> ".dat", SignedInt16,
DataLength * 4, ByteOrder → MostSignificantByteFirst];
tabη Ampin = Table[N[Xsig[[i]]/2048], {i, AmpChannelin, Length[Xsig], 4}];
tabη Phasein = Table[N[Xsig[[i]]/2048], {i, PhaseChannelin, Length[Xsig], 4}];
tabη Ampout = Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabη Phaseout = Table[N[Xsig[[i]]/2048],
{i, PhaseChannelout, Length[Xsig], 4}];
Print["XaAmp is ", Length[tabη Ampin], " points"];
Clear[Xsig];
TFamp = TransfertFunction[tabη Ampindemodds, tabη Ampoutdemodds, 50*^6];
TFphase = TransfertFunction[tabη Phaseindemodds, tabη Phaseoutdemodds, 50*^6];
TFamp = TransfertFunction[tabη Ampin, tabη Ampout, 100*^6];
TFphase = TransfertFunction[tabη Phasein, tabη Phaseout, 100*^6];
Clear[tabη Ampin, tabη Phasein];
smoothTFamp = KIRSmooth[TFamp, 100];
smoothTFphase = KIRSmooth[TFphase, 100];
Clear[TFamp, TFphase];
smoothTFamp = Smooth[TFamp, 10000];
smoothTFphase = Smooth[TFphase, 10000];
Clear[TFamp, TFphase];
absTFamp = Table[{TFamp[[i]][[1]], Abs[TFamp[[i]][[2]]]},
{i, 1, Length[TFamp]}];
absTFphase = Table[{TFphase[[i]][[1]], Abs[TFphase[[i]][[2]]]},
{i, 1, Length[TFphase]}];
argTFamp = Table[{TFamp[[i]][[1]], Arg[TFamp[[i]][[2]]]},
{i, 1, Length[TFamp]}];
argTFphase = Table[{TFphase[[i]][[1]], Arg[TFphase[[i]][[2]]]},
{i, 1, Length[TFphase]}];
Clear[TFamp, TFphase];
smoothabsTFamp = Smooth[absTFamp, 10000];
smoothargTFamp = Smooth[argTFamp, 10000];
smoothabsTFphase = Smooth[absTFphase, 10000];
smoothargTFphase = Smooth[argTFphase, 10000];
Clear[absTFamp, argTFamp, absTFphase, argTFphase]
labelfontsize = 16;
tickfontsize = 14;
tfpaa = ListPlot[Take[smoothabsTFamp, Length[smoothabsTFamp]/2],
Frame → True, AxesOrigin → {0, 0},
FrameLabel →
{StyleForm["Frequency (MHz)", FontSize → labelfontsize,
FontFamily → Helvetica], StyleForm["Transfer Amplitude",
FontSize → labelfontsize, FontFamily → Helvetica]}, PlotRange → {1, 2.5},
```

```
PlotLabel->StyleForm["(a)", FontSize → labelfontsize,
FontFamily → Helvetica],
FrameTicks →
{{{100*^6, StyleForm["100", FontSize → tickfontsize,
FontFamily → Helvetica]},
{20*^6, StyleForm["20", FontSize → tickfontsize, FontFamily → Helvetica]},
{60*^6, StyleForm["60", FontSize → tickfontsize, FontFamily → Helvetica]},
{40*^6, StyleForm["40", FontSize → tickfontsize, FontFamily → Helvetica]},
{80*^6, StyleForm["80", FontSize → tickfontsize,
FontFamily → Helvetica]}},
{{0, StyleForm["0", FontSize → tickfontsize, FontFamily → Helvetica]},
{0.5, StyleForm["0.5", FontSize → tickfontsize, FontFamily → Helvetica]},
{1, StyleForm["1", FontSize → tickfontsize, FontFamily → Helvetica]},
{1.5, StyleForm["1.5", FontSize → tickfontsize, FontFamily → Helvetica]},
{2, StyleForm["2", FontSize → tickfontsize, FontFamily → Helvetica]},
{2.5, StyleForm["2.5", FontSize → tickfontsize, FontFamily → Helvetica]}},
None, None}];

tfpap = ListPlot[Take[smoothargTFamp, Length[smoothargTFamp]/2],
Frame → True, AxesOrigin → {0, −π},
FrameLabel →
{StyleForm["Frequency (MHz)", FontSize → labelfontsize,
FontFamily → Helvetica], StyleForm["Transfer Phase (rad/pi)",
FontSize → labelfontsize, FontFamily → Helvetica]}, PlotRange → {−π, π},
PlotLabel->StyleForm["(b)", FontSize → labelfontsize,
FontFamily → Helvetica],
FrameTicks →
{{{100*^6, StyleForm["100", FontSize → tickfontsize,
FontFamily → Helvetica]},
{20*^6, StyleForm["20", FontSize → tickfontsize, FontFamily → Helvetica]},
{60*^6, StyleForm["60", FontSize → tickfontsize, FontFamily → Helvetica]},
{40*^6, StyleForm["40", FontSize → tickfontsize, FontFamily → Helvetica]},
{80*^6, StyleForm["80", FontSize → tickfontsize,
FontFamily → Helvetica]}},
{{−π, StyleForm["-1", FontSize → tickfontsize, FontFamily → Helvetica]},
{−π/2, StyleForm["-0.5", FontSize → tickfontsize,
FontFamily → Helvetica]},
{0, StyleForm["0", FontSize → tickfontsize, FontFamily → Helvetica]},
{π/2, StyleForm["0.5", FontSize → tickfontsize, FontFamily → Helvetica]},
{π, StyleForm["1", FontSize → tickfontsize, FontFamily → Helvetica]}},
None, None}];

tfppa = ListPlot[Take[smoothabsTFphase, Length[smoothabsTFphase]/2],
Frame → True, AxesOrigin → {0, 0},
FrameLabel →
{StyleForm["Frequency (MHz)", FontSize → labelfontsize,
FontFamily → Helvetica], StyleForm["Transfer Amplitude",
FontSize → labelfontsize, FontFamily → Helvetica]}, PlotRange → {1, 2.5},
```

```
PlotLabel->StyleForm["(c)", FontSize → labelfontsize,
FontFamily → Helvetica],
FrameTicks →
{{{100*^6, StyleForm["100", FontSize → tickfontsize,
FontFamily → Helvetica]},
{20*^6, StyleForm["20", FontSize → tickfontsize, FontFamily → Helvetica]},
{60*^6, StyleForm["60", FontSize → tickfontsize, FontFamily → Helvetica]},
{40*^6, StyleForm["40", FontSize → tickfontsize, FontFamily → Helvetica]},
{80*^6, StyleForm["80", FontSize → tickfontsize,
FontFamily → Helvetica]}},
{{0, StyleForm["0", FontSize → tickfontsize, FontFamily → Helvetica]},
{0.5, StyleForm["0.5", FontSize → tickfontsize, FontFamily → Helvetica]},
{1, StyleForm["1", FontSize → tickfontsize, FontFamily → Helvetica]},
{1.5, StyleForm["1.5", FontSize → tickfontsize, FontFamily → Helvetica]},
{2, StyleForm["2", FontSize → tickfontsize, FontFamily → Helvetica]},
{2.5, StyleForm["2.5", FontSize → tickfontsize, FontFamily → Helvetica]}},
None, None}];

tfppp = ListPlot[Take[smoothargTFphase, Length[smoothargTFphase]/2],
Frame → True, AxesOrigin → {0, −π},
FrameLabel →
{StyleForm["Frequency (MHz)", FontSize → labelfontsize,
FontFamily → Helvetica], StyleForm["Transfer Phase (rad/pi)",
FontSize → labelfontsize, FontFamily → Helvetica]}, PlotRange → {−π, π},
PlotLabel->StyleForm["(d)", FontSize → labelfontsize,
FontFamily → Helvetica],
FrameTicks →
{{{100*^6, StyleForm["100", FontSize → tickfontsize,
FontFamily → Helvetica]},
{20*^6, StyleForm["20", FontSize → tickfontsize, FontFamily → Helvetica]},
{60*^6, StyleForm["60", FontSize → tickfontsize, FontFamily → Helvetica]},
{40*^6, StyleForm["40", FontSize → tickfontsize, FontFamily → Helvetica]},
{80*^6, StyleForm["80", FontSize → tickfontsize,
FontFamily → Helvetica]}},
{{−π, StyleForm["-1", FontSize → tickfontsize, FontFamily → Helvetica]},
{−π/2, StyleForm["-0.5", FontSize → tickfontsize,
FontFamily → Helvetica]},
{0, StyleForm["0", FontSize → tickfontsize, FontFamily → Helvetica]},
{π/2, StyleForm["0.5", FontSize → tickfontsize, FontFamily → Helvetica]},
{π, StyleForm["1", FontSize → tickfontsize, FontFamily → Helvetica]}},
None, None}];



Export["tfampamp.eps", tfpaa, ImageRotated → True]
Export["tfampphase.eps", tfpap, ImageRotated → True]
Export["tfphaseamp.eps", tfppa, ImageRotated → True]
Export["tfphasephase.eps", tfppp, ImageRotated → True]
```

### Import Demultiplexed Data

```
SetDirectory[DataFilePath];
tabηAmpindemodds = Table[0, {20}];
tabηPhaseindemodds = Table[0, {20}];
tabηAmpoutdemodds = Table[0, {20}];
tabηPhaseoutdemodds = Table[0, {20}];
tabSNAmpoutdemodds = Table[0, {20}];
tabSNPhaseoutdemodds = Table[0, {20}];
tabDNAmpoutdemodds = Table[0, {20}];
tabDNPhaseoutdemodds = Table[0, {20}];
For[iChannel = 7, iChannel ≤ 16, iChannel++,
Xsig = ReadListBinary[DataηFileName <> "1" <> "DM" <> ToString[iChannel] <>
".dat", SignedInt16, DataLength * 4,
ByteOrder → MostSignificantByteFirst];
tabηAmpindemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, AmpChannelin, Length[Xsig], 4}];
tabηPhaseindemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, PhaseChannelin, Length[Xsig], 4}];
tabηAmpoutdemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabηPhaseoutdemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, PhaseChannelout, Length[Xsig], 4}];
(*Print["tabηAmpindemodds is ", Length[tabηAmpindemodds], " points"];*)
Clear[Xsig];

Xsig = ReadListBinary[DataSNFileName <> "4" <> "DM" <> ToString[iChannel] <>
".dat", SignedInt16, DataLength * 4,
ByteOrder → MostSignificantByteFirst];
tabSNAmpoutdemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabSNPhaseoutdemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, PhaseChannelout, Length[Xsig], 4}];
(*Print["tabSNAmpoutdemodds is ", Length[tabSNAmpoutdemodds],
" points"];*)
Clear[Xsig];

Xsig = ReadListBinary[DataDNFileName <> "1" <> "DM" <> ToString[iChannel] <>
".dat", SignedInt16, DataLength * 4,
ByteOrder → MostSignificantByteFirst];
tabDNAmpoutdemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, AmpChannelout, Length[Xsig], 4}];
tabDNPhaseoutdemodds[[iChannel]] =
Table[N[Xsig[[i]]/2048], {i, PhaseChannelout, Length[Xsig], 4}];
(*Print["tabDNAmpoutdemodds is ", Length[tabDNAmpoutdemodds],
" points"];*)
Clear[Xsig];
]
```

## Variances and Post-Selection Information Rates

```
For[iChannel = 7, iChannel ≤ 16, iChannel++,
VdnAmp = Variance[tabDNAmpoutdemodds[[iChannel]]];
VdnPhase = Variance[tabDNPhaseoutdemodds[[iChannel]]];
DVdnAmp =
Delt[VarianceCI[tabDNAmpoutdemodds[[iChannel]],
ConfidenceLevel → 0.682689]];
DVdnPhase =
Delt[VarianceCI[tabDNPhaseoutdemodds[[iChannel]],
ConfidenceLevel → 0.682689]];
Print["Dark noise variance ", VdnAmp, ",", VdnPhase];


VsnAmp = Variance[tabSNAmpoutdemodds[[iChannel]]] − VdnAmp;
VsnPhase = Variance[tabSNPhaseoutdemodds[[iChannel]]] − VdnPhase;
DVsnAmp =
√(Delt[VarianceCI[tabSNAmpoutdemodds[[iChannel]],
ConfidenceLevel → 0.682689]]^2 + DVdnAmp^2) ;
DVsnPhase =
√(Delt[VarianceCI[tabSNPhaseoutdemodds[[iChannel]],
ConfidenceLevel → 0.682689]]^2 + DVdnPhase^2) ;
Print["Shot noise variance ", VsnAmp, ",", VsnPhase];
(*Clear[tabSNAmpoutdemodds[[iChannel]], tabSNPhaseoutdemodds[[iChannel]],
tabDNAmpoutdemodds[[iChannel]], tabDNPhaseoutdemodds[[iChannel]]]; *)


XbAmp = tabηAmpoutdemodds[[iChannel]]/Sqrt[VsnAmp]/2;
 XbPhase = tabηPhaseoutdemodds[[iChannel]]/Sqrt[VsnPhase]/2;

VbAmp = Variance[XbAmp] − VdnAmp/VsnAmp;
DVbAmp =
√((VbAmpDelt[VarianceCI[tabηAmpoutdemodds[[iChannel]],
ConfidenceLevel → 0.682689]]/
Variance[tabηAmpoutdemodds[[iChannel]]])^2 + (VbAmp DVdnAmp/VdnAmp)^2 +
(VbAmp DVsnAmp/VsnAmp)^2) ;

VbPhase = Variance[XbPhase] − VdnPhase/VsnPhase;
DVbPhase =
√((VbPhaseDelt[VarianceCI[tabηPhaseoutdemodds[[iChannel]],
ConfidenceLevel → 0.682689]]/
Variance[tabηPhaseoutdemodds[[iChannel]]])^2+
(VbPhase DVdnPhase/VdnPhase)^2 + (VbPhase DVsnPhase/VsnPhase)^2) ;

VaAmp = Variance[tabηAmpindemodds[[iChannel]]];
VaPhase = Variance[tabηPhaseindemodds[[iChannel]]];
```

```
XaAmp = tabηAmpindemodds[[iChannel]] * Sqrt[VbAmp/VaAmp];
XaPhase = tabηPhaseindemodds[[iChannel]] * Sqrt[VbPhase/VaPhase];

VaAmp = Variance[XaAmp];
DVaAmp =
Delt[VarianceCI[tabηAmpindemodds[[iChannel]],
ConfidenceLevel → 0.682689]];


VaPhase = Variance[XaPhase];
DVaPhase =
Delt[VarianceCI[tabηPhaseindemodds[[iChannel]],
ConfidenceLevel → 0.682689]];

(*Clear[tabηAmpoutdemodds, tabηPhaseoutdemodds, tabηAmpindemodds,
tabηPhaseindemodds]; *)

CondVarAmp[g_]:=Variance[XbAmp - gXaAmp];
 ηAmp = (g/.FindMinimum[CondVarAmp[g], {g, {0, 1}}][[2]])^2;
 NoiseAmp = CondVarAmp[√ηAmp];
 CondVarPhase[g_]:=Variance[XbPhase - gXaPhase];
 ηPhase = (g/.FindMinimum[CondVarPhase[g], {g, {0, 1}}][[2]])^2;
 NoisePhase = CondVarPhase[√ηPhase];

DNoiseAmp = Delt[VarianceCI[XbAmp - ηAmp XaAmp, ConfidenceLevel → 0.682689]];

DηAmp = √((DVbAmp/VaAmp)^2 + (DNoiseAmp/VaAmp)^2 + ((VbAmp-NoiseAmp)/VaAmp^2 DVaAmp)^2);


DNoisePhase =
Delt[VarianceCI[XbPhase - ηPhase XaPhase, ConfidenceLevel → 0.682689]];

DηPhase = √((DVbPhase/VaPhase)^2 + (DNoisePhase/VaPhase)^2 + ((VbPhase-NoisePhase)/VaPhase^2 DVaPhase)^2);



 kDC =
k/.
FindMinimum[
1/(k^2+1/k^2) (√(Variance[kXaAmp - XbAmp/k] Variance[kXaPhase - XbPhase/k])),
{k, {0.00001, 10}}][[2]];
DuansCriterion =
1/(kDC^2+1/kDC^2)
(√(Variance[kDCXaAmp - XbAmp/kDC] Variance[kDCXaPhase - XbPhase/kDC]));
DDuansCriterion =
DuansCriterion/2
```

```
√(((Delt[VarianceCI[kDCXaAmp − XbAmp/kDC, ConfidenceLevel → 0.682689]]/
Variance[kDCXaAmp − XbAmp/kDC])^2 +
(Delt[VarianceCI[kDCXaPhase − XbPhase/kDC, ConfidenceLevel → 0.682689]]/
Variance[kDCXaPhase − XbPhase/kDC])^2);


Print[
"*************************
*****"];
Print[""];
Print["Parameters summary for File " <> Data$\eta$FileName <> "1" <>
"DM" <> ToString[iChannel] <> ".dat"];
Print["Variance Xb Amp = ", VbAmp, " ± ", DVbAmp, " std"];
 Print["Variance Xb Phase = ", VbPhase, " ± ", DVbPhase, " std"];
 Print["Variance Xa Amp = ", VaAmp, " ± ", DVaAmp, " std"];
 Print["Variance Xa Phase = ", VaPhase, " ± ", DVaPhase, " std"];
 Print["Variance Noise Amp = ", NoiseAmp, " ± ", DNoiseAmp, " std"];
 Print["Variance Noise Phase = ", NoisePhase, " ± ", DNoisePhase, " std"];
 Print["$\eta$Amp = ", $\eta$Amp, " ± ", D$\eta$Amp, " std"];
 Print["$\eta$Phase = ", $\eta$Phase, " ± ", D$\eta$Phase, " std"];
 Print["DuansCriterion = ", DuansCriterion, " ± ", DDuansCriterion,
" std"];
Print[""];

(*-- − IntegrationLimits-- − *)
XaMax = Sqrt[2]5√Max[VaAmp, VaPhase];
XbMax = 5√Max[VbAmp, VbPhase];


(***** ∗ THEORY**** ∗ *)

(*-- − Probabilityoferrorbtw AliceandBob-- − *)
Pep[x_, F_, $\eta$_]:=
(e^(−2(x+√(η/2)Abs[F]))^2 / (e^(−2(x−√(η/2)Abs[F]))^2 + e^(−2(x+√(η/2)Abs[F]))^2));
Pem[x_, F_, $\eta$_]:= (e^(−2(x−√(η/2)Abs[F]))^2 / (e^(−2(x−√(η/2)Abs[F]))^2 + e^(−2(x+√(η/2)Abs[F]))^2));
Pe[x_, F_, $\eta$_]:=If[x > 0, Pep[x, F, η], Pem[x, F, η]];

(*-- − Probability distributions-- − *)
Pae[x_, F_, d_, $\eta$_] = √(1/(2dπ)) e^(−F^2/2d)/2 √(2/π) (e^(−2(x−√(η/2)F))^2 + e^(−2(x+√(η/2)F))^2);
Pab[Xb_, Xa_, Va_, $\eta$_]:=√(1/(2πVa)) e^(−Xa^2/2Va) √(2/π) (e^(−2(Xb−√(η/2)Xa)^2));

(*-- − Mutual informations btw Alice, Bob and Eve-- − *)
Iab[x_, F_, $\eta$_] = 1 + Pe[x, F, η]Log[2, Pe[x, F, η]]+
```

```
(1 - Pe[x, F, η])Log[2, (1 - Pe[x, F, η])];
IaeSQM[F_, η_] = 1/2 (1 + Sqrt[1 - (e^-2((1-η)/2)F^2)^2]) Log[2, (1 + Sqrt[1 - (e^-2((1-η)/2)F^2)^2])] +
1/2 (1 - Sqrt[1 - (e^-2((1-η)/2)F^2)^2]) Log[2, (1 - Sqrt[1 - (e^-2((1-η)/2)F^2)^2])];
DeltaISQM[x_, F_, η_] = Iab[x, F, η] - IaeSQM[F, η];
ABRate[x_, F_, d_, η_] = Pae[x, F, d, η]Iab[x, F, η];
AERateSQM[x_, F_, d_, η_] = Pae[x, F, d, η]IaeSQM[F, η];
DeltaIRateSQM[x_, F_, d_, η_] = ABRate[x, F, d, η] - AERateSQM[x, F, d, η];

(*-- - Probability Cuts-- - *)
hp[F_, P_, η_]:=Limit [Log[(1-P)/P]^(1/4) / Sqrt[2η] Abs[xx], xx → F];

(*-- - Optimal Threshold-- - *)
Timing[
OT = Interpolation[
Partition[
Flatten[
Table[
{Xa, η, If[Xa ≠ 0, Xb/.FindRoot[DeltaISQM[Xb, Xa, η] == 0,
{Xb, {0.1, XbMax}}, MaxIterations → 300, WorkingPrecision → 100,
AccuracyGoal → 15],
Xb/.FindRoot[DeltaISQM[Xb, XaMax/100, η] == 0, {Xb, {0.1, XbMax}},
MaxIterations → 300, WorkingPrecision → 100, AccuracyGoal → 15]]},
{Xa, 0, XaMax, XaMax/GridOTXa},
{η, ηMin = Min[Max[ηAmp - DηAmp, 0.00000001],
Max[ηPhase - DηPhase, 0.00000001]],
ηMax = Max[ηAmp + DηAmp, ηPhase + DηPhase], (ηMax - ηMin)/GridOTη}]],
3]]];

(*---- - Net Information Rate Between Alice and Eve---- - *)
(*-- - Optimal Threshold-- - *)
IaeTheoryOTSQM[d_, η_]:=
4 * NIntegrate[NIntegrate[AERateSQM[x, F, d, η], {x, OT[F, η], XbMax},
Method->GaussKronrod, PrecisionGoal → 3, WorkingPrecision → 100,
MaxRecursion → 50], {F, 0, XaMax}, Method->GaussKronrod,
WorkingPrecision → 100, PrecisionGoal → 3, MaxRecursion → 50];

IabPRLTheoryOT[d_, η_]:=
4 * NIntegrate[NIntegrate[ABRate[x, F, d, η], {x, OT[F, η], XbMax},
Method->GaussKronrod, PrecisionGoal → 3, WorkingPrecision → 100,
MaxRecursion → 50], {F, 0, XaMax}, Method->GaussKronrod,
WorkingPrecision → 100, PrecisionGoal → 3, MaxRecursion → 50];

(*-- - Probability of error-- - *)
PeOfI =
```

```
Interpolation[
Table[
{IRate,
Chop[Pe/.FindRoot[1 + PeLog[2, Pe] + (1 − Pe)Log[2, 1 − Pe]==IRate,
{Pe, .25}, MaxIterations → 50, WorkingPrecision → 30,
AccuracyGoal → 10]]}, {IRate, 0, 1, .001}]];

DPeOfI[x_] = Derivative[1][PeOfI][x];

(*-- − DeltaI for one channel-- − *)
IaeTheoryOTSSQM[d_, η_, Pmin_, PMax_]:=
4NIntegrate[NIntegrate[AERateSQM[x, F, d, η],
{x, Min[Max[OT[F, η], hp[F, PMax, η]], XbMax],
Max[Min[XbMax, hp[F, Pmin, η]], OT[F, η]]}, Method->GaussKronrod,
WorkingPrecision → 100, PrecisionGoal → 3, MaxRecursion → 50],
{F, 0, XaMax}, WorkingPrecision → 100, Method->GaussKronrod,
PrecisionGoal → 3, MaxRecursion → 50];

IabTheoryOTS[d_, η_, Pmin_, PMax_]:=
4NIntegrate[NIntegrate[ABRate[x, F, d, η],
{x, Min[Max[OT[F, η], hp[F, PMax, η]], XbMax],
Max[Min[XbMax, hp[F, Pmin, η]], OT[F, η]]}, Method->GaussKronrod,
WorkingPrecision → 100, PrecisionGoal → 3, MaxRecursion → 50],
{F, 0, XaMax}, WorkingPrecision → 100, Method->GaussKronrod,
PrecisionGoal → 3, MaxRecursion → 50];

ΔITheoryOTSSQM[d_, η_, Pmin_, PMax_]:=
4NIntegrate[NIntegrate[DeltaIRateSQM[x, F, d, η],
{x, Min[Max[OT[F, η], hp[F, PMax, η]], XbMax],
Max[Min[XbMax, hp[F, Pmin, η]], OT[F, η]]}, Method->GaussKronrod,
WorkingPrecision → 100, PrecisionGoal → 3, MaxRecursion → 50],
{F, 0, XaMax}, Method->GaussKronrod, WorkingPrecision → 100,
PrecisionGoal → 3, MaxRecursion → 50];

PaeTheoryOTS[d_, η_, Pmin_, PMax_]:=
4NIntegrate[NIntegrate[Pae[x, F, d, η],
{x, Min[Max[OT[F, η], hp[F, PMax, η]], XbMax],
Max[Min[XbMax, hp[F, Pmin, η]], OT[F, η]]}, Method->GaussKronrod,
WorkingPrecision → 100, PrecisionGoal → 3, MaxRecursion → 50],
{F, 0, XaMax}, WorkingPrecision → 100, Method->GaussKronrod,
PrecisionGoal → 3, MaxRecursion → 50];

(*-- − Probability of error-- − *)
PeOfI =
Interpolation[
Table[
{IRate,
Chop[Pe/.FindRoot[1 + PeLog[2, Pe] + (1 − Pe)Log[2, 1 − Pe]==IRate,
```

```
{Pe, .25}, MaxIterations → 50, WorkingPrecision → 30,
AccuracyGoal → 10]]}, {IRate, 0, 1, .001}]];

DPeOfI[x_] = Derivative[1][PeOfI][x];




(***** * POST-SELECTION******)

(*-- − Optimal Threshold and slicing-- − *)
InformationRateSOT[Xin2_, Xout2_, Va_, DeltaVa_, ηExp_, DeltaηExp_,
NPe_, LInit_]:=
Module[
{Xinout, XinoutPe, BitsKept, BadBits, BadBitsTable, Perror,
DeltaPerror, DeltaI, I, ITable, IaeTable, RelIabTable, DeltaIaeTable,
PerrTable, DPerrTable, RelIaeTable, RelDeltaIaeTable},

BadBits = Table[0, {i, NPe}];

BadBitsTable = Table[{}, {i, NPe}];

Xinout = Select[Transpose[Append[{Xin2}, Xout2]],
((Abs[#][[2]] < XbMax)&&(Sqrt[2]  Abs[#][[1]] < XaMax))&];


XinoutPe = Table[{Pe[Xinout[[i, 2]], Sqrt[2]Abs[Xinout[[i, 1]]], ηExp],
Xinout[[i, 1]], Xinout[[i, 2]]}, {i, Length[Xinout]}];


Xinout = Sort[XinoutPe];


BitsKept =
Table[If[i==1, Length[Xinout] − (NPe − 1)Round[Length[Xinout]/NPe],
Round[Length[Xinout]/NPe]], {i, NPe}];

XinoutPe = Table[{}, {i, NPe}];
For[i = 1, i ≤ NPe, i++,
XinoutPe[[i]] = Take[Xinout, BitsKept[[i]]];
BadBitsTable[[i]] =
Table[If[Sign[XinoutPe[[i, j, 2]]] ≠ Sign[XinoutPe[[i, j, 3]]],
BadBits[[i]]+=1; 1, 0], {j, BitsKept[[i]]}];
Xinout = Drop[Xinout, BitsKept[[i]]]
];
```

```
Perror = Table[Min[If[BitsKept[[i]] ≠ 0, BadBits[[i]]/BitsKept[[i]], .5],
.5], {i, 1, NPe}];

DeltaPerror =
Table[If[BitsKept[[i]] > 1,
(MeanCI[BadBitsTable[[i]], ConfidenceLevel → 0.682689][[2]]−
MeanCI[BadBitsTable[[i]], ConfidenceLevel → 0.682689][[1]])/2, 1],
{i, 1, NPe}];

ITable =
N[Table[BitsKept[[i]]/LInit∗
Limit[(1 + PerrLog[2, Perr] + (1 − Perr)Log[2, 1 − Perr]),
Perr → Perror[[i]]], {i, NPe}]];
DeltaI =
Abs[Table[BitsKept[[i]]/LInit
If[Perror[[i]] == 0, 0, (Log[2, Perror[[i]]] − Log[2, 1 − Perror[[i]]])
DeltaPerror[[i]]], {i, 1, NPe}]];

Print["Bits Kept per slice :"];
Print[BitsKept];
Print["{PeMin,PeMax} per slice :"];
Print[Table[{XinoutPe[[i, 1, 1]], XinoutPe[[i, BitsKept[[i]], 1]]},
{i, NPe}]];
Print["{I,DeltaI} per slice :"];
Print[Transpose[Append[{ITable}, DeltaI]]];
Print["{ΔI_Exp, DeltaΔI_Exp} per slice :"];
IaeTable = Table[IaeTheoryOTSSQM[Va, ηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]], {i, NPe}];
DeltaIaeTable =
Table[
(Max[IaeTheoryOTSSQM[Va + DeltaVa, ηExp − DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]],
IaeTheoryOTSSQM[Va − DeltaVa, ηExp − DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]]−
Min[IaeTheoryOTSSQM[Va + DeltaVa, ηExp + DeltaηExp,
XinoutPe[[i, 1, 1]], XinoutPe[[i, BitsKept[[i]], 1]]],
IaeTheoryOTSSQM[Va − DeltaVa, ηExp + DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]])/2, {i, NPe}];
Print[Transpose[Append[{Table[ITable[[i]] − IaeTable[[i]], {i, NPe}]},
Table[Sqrt[DeltaI[[i]]^2 + DeltaIaeTable[[i]]^2], {i, NPe}]]];
Print["ΔI_Theo per slice :"];
Print[Table[ΔITheoryOTSSQM[Va, ηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]], {i, NPe}]];

Print["⟨Pe_Eve⟩_Theo per slice"];
PaeTable = Table[PaeTheoryOTS[Va, ηExp, XinoutPe[[i, 1, 1]],
```

```
XinoutPe[[i, BitsKept[[i]], 1]]], {i, NPe}];
RelIaeTable = IaeTable/PaeTable;
(*RelDeltaIaeTable =
Table[
(Max[IaeTheoryOTSSQM[Va + DeltaVa, ηExp − DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]/
PaeTheoryOTS[Va + DeltaVa, ηExp − DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]],
IaeTheoryOTSSQM[Va − DeltaVa, ηExp − DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]/
PaeTheoryOTS[Va − DeltaVa, ηExp − DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]]−
Min[IaeTheoryOTSSQM[Va + DeltaVa, ηExp + DeltaηExp,
XinoutPe[[i, 1, 1]], XinoutPe[[i, BitsKept[[i]], 1]]]/
PaeTheoryOTS[Va + DeltaVa, ηExp + DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]],
IaeTheoryOTSSQM[Va − DeltaVa, ηExp + DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]/
PaeTheoryOTS[Va − DeltaVa, ηExp + DeltaηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]])/2, {i, NPe}]; *)
PerrTable = Table[PeOfI[RelIaeTable[[i]]], {i, NPe}];
(*DPerrTable =
Abs[Table[RelDeltaIaeTable[[i]]DPeOfI[IaeTable[[i]]], {i, NPe}]]; *)

Print[PerrTable];

Print["⟨Pe_Bob⟩_theo per slice"];
Print[
Table[
PeOfI[IabTheoryOTS[Va, ηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]/
PaeTheoryOTS[Va, ηExp, XinoutPe[[i, 1, 1]],
XinoutPe[[i, BitsKept[[i]], 1]]]], {i, NPe}]];


I = Sum[ITable[[i]], {i, NPe}];
{I, {I − N[Sqrt[Sum[DeltaI[[i]]^2, {i, 1, NPe}]]],
I + N[Sqrt[Sum[DeltaI[[i]]^2, {i, 1, NPe}]]]}}


];
InoutSOT[Xin2_, Xout2_, ηExp_, NPe_, LInit_]:=Module[
{Xinout, XinoutPe, BitsTablein, BitsTableout},



BitsTablein = Table[{}, {i, NPe}];
BitsTableout = Table[{}, {i, NPe}];
```

```
Xinout = Select[Transpose[Append[{Xin2}, Xout2]],
((Abs[#][[2]] < XbMax)&&(Sqrt[2]Abs[#][[1]] < XaMax))&];


XinoutPe = Table[{Pe[Xinout[[i, 2]], Sqrt[2]Abs[Xinout[[i, 1]]], ηExp],
Xinout[[i, 1]], Xinout[[i, 2]]}, {i, Length[Xinout]}];


Xinout = Sort[XinoutPe];


BitsKept =
Table[If[i==1, Length[Xinout] − (NPe − 1)Round[Length[Xinout]/NPe],
Round[Length[Xinout]/NPe]], {i, NPe}];

XinoutPe = Table[{}, {i, NPe}];
For[i = 1, i ≤ NPe, i++,
XinoutPe[[i]] = Take[Xinout, BitsKept[[i]]];
BitsTablein[[i]] = Table[If[Sign[XinoutPe[[i, j, 2]]] == 1, 1, 0],
{j, BitsKept[[i]]}];
BitsTableout[[i]] = Table[If[Sign[XinoutPe[[i, j, 3]]] == 1, 1, 0],
{j, BitsKept[[i]]}];
Xinout = Drop[Xinout, BitsKept[[i]]]
];
Append[{BitsTablein}, BitsTableout];


];


(***** * OPTIMAL THRESHOLD RESULTS******)
Timing[DIabExpSOTAmpOTOpt =
InformationRateSOT[XaAmp, XbAmp, 2VaAmp, 2DVaAmp, ηAmp, Dη Amp, 10,
Length[XaAmp]]];

InOutAmp = InoutSOT[XaAmp, XbAmp, ηAmp, 10, Length[XaAmp]];
IaeExpSOTAmpOTOpt = IaeTheoryOTSQM[2VaAmp, ηAmp];
DPIaeExpSOTAmpOTOpt = Max[IaeTheoryOTSQM[2(VaAmp + DVaAmp), (ηAmp + Dη Amp)],
IaeTheoryOTSQM[2(VaAmp − DVaAmp), (ηAmp + Dη Amp)],
IaeTheoryOTSQM[2(VaAmp + DVaAmp), Max[(ηAmp − Dη Amp), 0]],
IaeTheoryOTSQM[2(VaAmp − DVaAmp), Max[(ηAmp − Dη Amp), 0]]];
DMIaeExpSOTAmpOTOpt = Min[IaeTheoryOTSQM[2(VaAmp + DVaAmp), (ηAmp + Dη Amp)],
IaeTheoryOTSQM[2(VaAmp − DVaAmp), (ηAmp + Dη Amp)],
IaeTheoryOTSQM[2(VaAmp + DVaAmp), Max[(ηAmp − Dη Amp), 0]],
IaeTheoryOTSQM[2(VaAmp − DVaAmp), Max[(ηAmp − Dη Amp), 0]]];
DeltaIExpSOTAmpOTOpt = DIabExpSOTAmpOTOpt[[1]] − IaeExpSOTAmpOTOpt;
DDeltaIExpSOTAmpOTOpt =
```

$$\sqrt{\left(\left(\frac{\texttt{DPIaeExpSOTAmpOTOpt}-\texttt{DMIaeExpSOTAmpOTOpt}}{\mathbf{2}}\right)^{\mathbf{2}}+\left(\tfrac{\mathbf{1}}{\mathbf{2}}(\texttt{DIabExpSOTAmpOTOpt}[[\mathbf{2},\mathbf{2}]]-\texttt{DIabExpSOTAmpOTOpt}[[\mathbf{2},\mathbf{1}]])\right)^{\mathbf{2}}\right)};$$

```
Timing[DIabExpSOTPhaseOTOpt =
InformationRateSOT[XaAmp, XbAmp, 2VaAmp, 2DVaAmp, ηAmp, DηAmp, 10,
Length[XaAmp]]];

InOutPhase = InoutSOT[XaPhase, XbPhase, ηPhase, 10, Length[XaPhase]];
IaeExpSOTPhaseOTOpt = IaeTheoryOTSQM[2VaPhase, ηPhase];
DPIaeExpSOTPhaseOTOpt =
Max[IaeTheoryOTSQM[2(VaPhase + DVaPhase), (ηPhase + DηPhase)],
IaeTheoryOTSQM[2(VaPhase − DVaPhase), (ηPhase + DηPhase)],
IaeTheoryOTSQM[2(VaPhase + DVaPhase), Max[(ηPhase − DηPhase), 0]],
IaeTheoryOTSQM[2(VaPhase − DVaPhase), Max[(ηPhase − DηPhase), 0]]];
DMIaeExpSOTPhaseOTOpt =
Min[IaeTheoryOTSQM[2(VaPhase + DVaPhase), (ηPhase + DηPhase)],
IaeTheoryOTSQM[2(VaPhase − DVaPhase), (ηPhase + DηPhase)],
IaeTheoryOTSQM[2(VaPhase + DVaPhase), Max[(ηPhase − DηPhase), 0]],
IaeTheoryOTSQM[2(VaPhase − DVaPhase), Max[(ηPhase − DηPhase), 0]]];
DeltaIExpSOTPhaseOTOpt = DIabExpSOTPhaseOTOpt[[1]] − IaeExpSOTPhaseOTOpt
DDeltaIExpSOTPhaseOTOpt =
```

$$\sqrt{\left(\left(\frac{\texttt{DPIaeExpSOTPhaseOTOpt}-\texttt{DMIaeExpSOTPhaseOTOpt}}{\mathbf{2}}\right)^{\mathbf{2}}+\left(\tfrac{\mathbf{1}}{\mathbf{2}}(\texttt{DIabExpSOTPhaseOTOpt}[[\mathbf{2},\mathbf{2}]]-\texttt{DIabExpSOTPhaseOTOpt}[[\mathbf{2},\mathbf{1}]])\right)^{\mathbf{2}}\right)};$$

```
(*** * DISPLAY RESULTS****)
Print[
"*******************************
*****"];
Print[""];
Print["Parameters summary for Sum of all Files of record " <>
DataηFileName];
Print["Variance XbAmp = ", VbAmp, " ± ", DVbAmp, " std"];
 Print["Variance XbPhase = ", VbPhase, " ± ", DVbPhase, " std"];
 Print["Variance Xa Amp = ", VaAmp, " ± ", DVaAmp, " std"];
 Print["Variance Xa Phase = ", VaPhase, " ± ", DVaPhase, " std"];
 Print["Variance Noise Amp = ", NoiseAmp, " ± ", DNoiseAmp, " std"];
 Print["Variance Noise Phase = ", NoisePhase, " ± ", DNoisePhase, " std"];
 Print["ηAmp = ", ηAmp, " ± ", DηAmp, " std"];
 Print["ηPhase = ", ηPhase, " ± ", DηPhase, " std"];
 Print["DuansCriterion = ", DuansCriterion, " ± ", DDuansCriterion,
" std"];
Print["Max ΔIExp Amp for OT = ", DeltaIExpSOTAmpOTOpt, " ± ",
DDeltaIExpSOTAmpOTOpt, " std"];
Print["Max ΔIExp Phase for OT = ", DeltaIExpSOTPhaseOTOpt, " ± ",
DDeltaIExpSOTPhaseOTOpt, " std"];
```

```
Print[""];
Print[
"****************************
*****"];
StopTime = SessionTime[];
DeltaTime = ToDate[StopTime - StartTime];
Print["Time Elapsed = ",DeltaTime[[4]]," h ",DeltaTime[[5]],
" min ",DeltaTime[[6]],"sec"]


]; (* end Channel For *)
```