Thermal State Quantum Key Distribution

Adam Walton

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

The University of Leeds

School of Physics and Astronomy

May 2024

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

In this thesis, the sections based on written articles are as follows:

- Chapter 4 is based on the paper "Thermal State Quantum Key Distribution" published in J. Phys. B (2021) [1], authored by Adam Walton, Anne Ghesquière, George Brumpton, David Jennings, and Ben Varcoe. The lead author for the paper was myself, and I coded and performed all simulations carried out in the paper. Assistance from the supporting authors was in conceiving the original experimental setup, verifying calculations, and editing of the writing.

- Chapter 5 is based on the unpublished paper "Towards quantum key distribution with noisy communication sources" (2022) [2], authored by Adam Walton, Anne Ghesquière, David Jennings, Benjamin Varcoe. As with the previous entry, I was the lead author and scripted and performed the simulations to produce the experimental results, with assistance from the supporting authors in proofreading and editing.

- Chapter 6 is based on the paper "Quantum key distribution with displaced thermal states", published in Entropy (2024) [3]. This was authored by Adam Walton, Anne Ghesquière, and Benjamin Varcoe. Ben was the lead author for the paper, based on earlier reports and results by myself. Anne and I provided feedback and edits.

- Chapter 7 is based on the currently unpublished paper "Topological State Reconstruction For Wireless Stabilization of Distant Atomic Clocks" (2024) by Adam Walton and Benjamin Varcoe [4], which is awaiting some final edits before deciding on a journal to submit to. The concept for the experiment was by Ben, with the setup, experiments, and coding performed by me. I was the lead author for the paper, with contributions and editing by Ben.

Acknowledgements

This research has been carried out by a team which has included Ben Varcoe, Anne Ghesquière, George Brumpton and David Jennings. My own contributions have been setting up and performing experiments along with coding and running simulations when relevant. The writing within this thesis is by myself, along with the majority of writing across associated articles as described on the previous page. The contributions of the other members of the group were conceiving of the ideas for the Quantum Key Distribution protocol and the frequency distribution protocol which will be analysed, as well as providing edits and clarifications to written articles.

Abstract

This thesis covers two separate fields of research, first focusing on quantum key distribution before covering research on atomic clock synchronisation.

Initially, a method of performing thermal state key distribution was analysed. A protocol for radio key distribution inspired by quantum methods which could be performed using easily accessible equipment was known, with some evidence that it could realistically be carried out, but this had yet to be confirmed in testing. In this writing, we first simulate the protocol in Python, and verify that the results of simulation suggests that a practical setup would be reasonable. After confirming that off-the-shelf broadcasting equipment may be used for the protocol, we performed both wired and wireless tests of the protocol and was able to distribute bit strings suitable for key distillation. This provides a method for performing quantum key distribution using only common radio equipment and open-source software – a procedure which typically requires specialist equipment, is not compatible with current communication setups, and does not currently exist in a widely accessible form for public use.

For clock synchronisation, current accessible methods of wireless synchronisation have poor precision, relying on GPS for timing information. Optical protocols for synchronisation offer far more precise results, but require either line of sight or a fibre connection, which is not always reasonable to implement. This can lead to issues in which accessible methods of synchronisation are not sufficient for parties which require higher precision, such as in market trading. Here, we devise and test a radio-based method of clock synchronisation with commonly-used broadcast

protocols based on experimental results observed in the first section of the thesis. From this testing, we find that the protocol is able to reach precision approximately 10^3 times smaller than the minimum advertised by the clocks used, which itself was already more precise than can be reached using GPS synchronisation.

Overall, this represents new methods of solving known problems; producing the security conferred by Quantum Key Distribution (QKD) and clock synchronisation, without requiring specialised equipment which may prevent other potential solutions from being viable in real-world applications. The ability to perform the experiments set up here with off-the-shelf radio equipment and open-source software provides a straightforward way to apply the protocols for any party interested in either of these fields. This will be shown to be especially true in the case of clock synchronisation, in which we find evidence that our protocol outperforms currently used methods by a significant margin while using similar equipment.

Contents

List of Figures

Glossary

Allan variance A measure of clock stability over measurements separated by a given time interval.. 103

Amplitude Square root of the sum of squares of the quadrature values. 57

Fock states States with a defined number of photons N, with $|n_i\rangle$ denoting n photons in the state i. 25

Heterodyne detection A method of encoding information by combining a pair of out-of-phase carrier waves by adjusting their amplitudes. 56

Quadrature Amplitude Modulation A method of encoding information by combining a pair of out-of-phase carrier waves by adjusting their amplitudes. 17

Chapter 1

Introduction

1.1 Structure

In this thesis, the aim is to first introduce a variety of relevant background material, before progressing to discussion of the main topic of thermal state quantum key distribution. During the course of this research, additional possible applications of the methods in use were discovered. This led to consideration of the use of thermal states for atomic clock synchronisation. While these two fields appear unrelated, precision timekeeping is vital in order to properly interpret a received broadcast, and we see results that compare favourably to existing methods of wireless clock synchronisation. Here, very similar methods will be used to both distribute a key, and allow the parties involved to synchronise the clocks which their receivers will be using as a time reference.

A large portion of this writing is dedicated to explaining background information, due to this work representing a crossover of different fields. It begins with an introduction to classical cryptography, detailing the goals of the field, and a variety of methods through which they are accomplished, as well as the weaknesses which Quantum Key Distribution aims to address. Chapter 2 discusses the necessary quantum optics background, beginning with an approach to creation and annihilation operators, and progressing to discussion of quadratures, the measurement of which is used in the experimental work to be performed. This continues to an explanation of the thermal sources which will be used in our broadcasts. This includes an explanation of modulation of radio signals, covering Amplitude Modulation, Frequency Modulation, and Quadrature Amplitude Modulation . We finish the background material in Chapter 3, which explains the field of Quantum Key Distribution. The early protocols are described, progressing to commonly used recent methods, before introducing thermal quantum key distribution.

We then progress to the original research, with Chapter 4 covering initial efforts to simulate key distribution with a non-displaced thermal source. This is refined in Chapter 5, which expands on the theory to accommodate displaced thermal states that are used in real broadcasts. Also included is an analysis of loss in the system. This leads into Chapter 6, in which the protocol is carried out experimentally, in both wired and wireless systems.

Finally, Chapter 7 describes how the aforementioned experimental work led to discovery of potential applications in atomic clock synchronisation, also using both wired and wireless broadcasts. This came about due to analysis of errors caused by clock frequency differences when trying to arrange key distribution. We devise a protocol for clock synchronisation using off-the-shelf radio equipment and a common encoding method widely used in wireless communications. Testing over short ranges showed considerable improvements in precision over what is attainable by GPS synchronisation, which is currently used when optical transmissions are not available.

In both of these cases, while the methods we are using will not outperform state-of-the-art results that have been achieved through other methods, our experimental setups give a unique advantage in ease of implementation. The use of common radio equipment and known protocols throughout this work gives immediate opportunities for practical use, demonstrating an approach which is straightforward to emulate with accessible equipment for those with knowledge of communications.

A common thread combining both of these fields will be the involvement of noise. While noise is typically seen as a detrimental side effect to be minimised in most scenarios, we will see that the randomness of Gaussian classical noise is what allows us to perform cryptography through providing uncertainty in measurements which no eavesdropper could accurately account for. When progressing to discussion of clocks and frequency distribution, state reconstruction using measurements of such broadcasts is what will allow careful tracking of time differences.

1.2 Cryptography

In communication, a consistent problem is securing channels such that multiple legitimate parties, commonly referred to as Alice and Bob in the case of two person communication, may exchange messages while excluding an unwanted eavesdropper (Eve).

For communication to safely take place in the presence of an eavesdropper, a method is required which can obfuscate the message before it is sent. Additionally, this method somehow needs to be agreed upon by the communicating parties without an eavesdropper knowing the method, or ideally having knowledge of the method being insufficient information for an eavesdropper who wishes to recover the original messages.

The idea of concealing a message through simple replacement of letters (A substitution cipher) has been known for centuries. One such example, Rotate13 (ROT13), is shown in Figure 1.1, in which each letter is swapped with the letter 13 spaces after it in the alphabet. One-to-one replacement of letters is of course a very insecure method, and the original message is easily found through brute force given the low number of possibilities for the original message, given any intercepted message. Older methods of concealing the contents of messages by simple switching of letters are commonly vulnerable to frequency analysis, in which the rate at which letters appear in an intercepted message is considered. Given a long enough message, reasonable guesses can be made at which substitutions were used by assuming the most common letters in the alphabet are also the most common letters in an intercepted message, leading to the cipher gradually being uncovered and the original message being found.

A	B	C	...	X	Y	Z
↕	↕	↕	...	↕	↕	↕
N	O	P	...	K	L	M

Figure 1.1: **ROT13.** In this simple cipher, each letter switches places with the letter 13 places after it in the alphabet.

As simple substitution is clearly unreliable, modern cryptography relies on more advanced versions of encryption. Encrypting a message ideally ensures that an eavesdropper with access to the encrypted message cannot read the original contents (plaintext) without knowledge of a key – a string of data. Through Alice combining the message in some predetermined method with the key, another string of characters (ciphertext) is produced which is sent to Bob. If the ciphertext and plaintext are completely uncorrelated, an eavesdropper cannot recover the plaintext when only provided with the ciphertext and no additional information. Bob is also in possession of a key, which in the case of symmetric key cryptography, is identical to Alice's. Bob then uses their knowledge of the key and encryption method to retrieve the original message.

Alternative, more common methods rely on having two separate keys – commonly by publicly sharing one key which can be used to encrypt but not decrypt a message, while keeping a second, private key which can be used for decryption. RSA, in which modular arithmetic involving large prime numbers are used to produce public and private keys, and Diffie-Hellman, in which both parties start with their own keys in order to produce a symmetric key, are both common examples of asymmetric methods.

For a symmetric key, the simple example is a one-time pad, in which a key of greater or equal length to the intended message is used for encryption through modular addition of the key values to the message bits. This is seen in equation 1.1 with the example message M and key K producing the ciphertext $C_i \equiv M_i + K_i \pmod{2}$.

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ \vdots \\ 1 \end{bmatrix}_M + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ \vdots \\ 0 \end{bmatrix}_K \Rightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 1 \end{bmatrix}_C \tag{1.1}$$

This method is considered perfectly secure, as an eavesdropper given any ciphertext C could derive any message M of equal or shorter length by guessing the key $K \equiv C - M \pmod 2$. As the eavesdropper could produce any message from a truly random ciphertext, there would be no way for them to learn the correct choice. Given possession of the same key however, it is trivial for Bob to acquire the original message through once again adding the key to the ciphertext.

This method quickly leads to a problem, in that it assumes Alice and Bob already share a matching key of suitable length which Eve does not know, despite the fact that they have yet to secure the channel between them. The obvious question arises for symmetric key methods: how can both parties agree on a key privately, if they require the key to make the private channel? For this to be possible, methods are needed through which Alice and Bob can agree on a key while an eavesdropper is monitoring communication between them. This is the issue we will be addressing over the course of this writing.

An additional factor which needs to be taken into account is authentication, as encryption will not help conceal information if a legitimate party was unintentionally securing a channel with an eavesdropper who was impersonating the intended recipient. Many key distribution methods assume the existence of an authenticated channel, and it is not the focus of this writing. However, of interest in that field is Carter-Wegman authentication, which offers information-theoretic secure authentication – security regardless of the amount of computing power or time available to an eavesdropper [6, 7]. This is a higher level of security than is provided by cryptographic protocols when attempting to secure an already authenticated channel, which intend to be safe from realistic attackers who do not have access to unlimited time or computing power.

In classical asymmetric key distribution, this security is based off of mathematical problems which are impractical to solve in a reasonable time frame using current computer equipment, such as solving

$$\left(a^b\right)^c \equiv a \pmod{d} \tag{1.2}$$

for c in RSA, which is difficult even given values for the remaining variables. However, by comparison it is straightforward to select large variables which satisfy the equation. In this setup, a represents the message, with $a^b \pmod{d}$ as the ciphertext. Here, b and d make up the public key, with the value of c kept private. Finding the value of a without knowledge of c is currently not feasible given reasonably large integers are used in encryption, but simple if c is known along with the public key.

Public key encryption typically relies on such methods – “Trapdoor functions” which are trivial to calculate in one direction, but unreasonably difficult to invert unless a specific piece of extra information is provided, which in encryption is the private key.

This leads to potential future-proofing problems, in that security depends on a continued lack of methods to solve such functions, either through new algorithms or through increased computing power. As there is no way to guarantee that this will be the case indefinitely, it is of interest to research methods of security that rely on something other than difficult mathematics. Quantum key distribution, a protocol for which this writing will be analysing, instead aims to base security on the laws of quantum mechanics, under the assumption that an eavesdropper has unlimited computing power, and is limited by the laws of physics, and the inability to interfere with the measurement equipment of the legitimate parties. In order to properly describe this, some elements of quantum mechanics are required background knowledge, which will be explained in the following chapters.

Research into quantum information began several decades before cryptography was proposed as an application, at which point the concept of storing information with quantum states was already known [8]. This was combined with the no-cloning theorem, which forbids perfect copying of quantum states [9] in order to create the concept of Quantum Key Distribution – sharing information through quantum states which an eavesdropper cannot accurately intercept and copy. Initially, this was accomplished through Alice broadcasting single photon pulses with information encoded on each pulse in one of two possible methods. Secrecy is introduced if Alice conceals the choice of method, as eavesdroppers randomly selecting the incorrect measurement method introduces errors, as well as complicating any attempt to intercept and resend Alice's pulses.

Protocols later adjusted to employ multiple-photon pulses, with a popular choice of experimental setup involving fibre cables. While such protocols can be carried out experimentally, the practical uses can be limited by the costs needed to install such cabling over longer distances.

In order to address this, we will instead consider microwave broadcasts as the channel through which keys will be distributed. Due to their common use in radio broadcasting, the equipment and software required to set up such a protocol experimentally is both well-understood and easily accessible. Through this, we aim to produce and demonstrate a simple QKD protocol which could be implemented without requiring specialised equipment. Before further discussion of these methods, the quantum optics underpinning such methods should be explored. This follows in the next chapter.

Microwaves, or optical broadcasts approaching microwave frequencies, have seen prior use in key distribution and quantum information. We see early demonstrations of this in [10], in which random key bits are encoded in noise in a microwave broadcast before being sent to the receiving party, and demonstrating that an attempt to interrupt the communication through intercepting and re-sending the original broadcast leads to clearly visible differences in the receiving parties expected output. Later tested was further experimental applications for microwave transmissions, including single photon detection in the microwave region [11, 12, 13] and the production of entangled states through mixing microwave light [14]. More recently, further effort was made into key distribution using optical microwave methods, seeing keys feasible across 200km of free space between satellites [15], as well as over 200m of free space at room temperature [16].

It should also be noted that, while the no-cloning theorem is typically assumed to prevent any perfect copying attempt involving single photons, imperfect cloning has been demonstrated as possible [17] . This can allow a potential "copying machine" which can produce potentially useful outputs when given a state to copy. Additionally, this does not prohibit siphoning of part of a multi-photon broadcast, a factor which the microwave protocol to be analysed will be tested against.

Chapter 2

Introduction to quantum optics

Here, we will introduce some of the notation and concepts used throughout this writing, covering creation and annihilation operators, Fock states, quadratures, thermal states and displacement operators.

2.1 Creation and Annihilation operators

To analyse the electromagnetic field in quantum mechanics, we begin with the time-independent Schrödinger equation for the quantum harmonic oscillator, commonly used to derive the possible energy levels of particles in realistic potential wells:

$$\hat{H}\Psi_n\left(x\right) = \left(\frac{\hat{P}^2}{2m} + \frac{m\omega^2\hat{X}^2}{2}\right)\Psi_n\left(x\right) = E_n\Psi_n\left(x\right). \tag{2.1}$$

Here, the Hamiltonian H is the total energy of a system, depending on position ($\hat{X}$) and momentum ($\hat{P}$) of the particle being analysed. Performing a change in coordinates allows the Hamiltonian to be simplified:

$$\hat{X}_1 = \sqrt{\frac{m\omega\hat{X}}{2\hbar}}, \tag{2.2}$$

$$\hat{P}_1 = \sqrt{\frac{\hat{P}}{\sqrt{2m\hbar\omega}}}, \tag{2.3}$$

$$\hat{H} = \hbar\omega\left(\hat{P}_1^2 + \hat{X}_1^2\right). \tag{2.4}$$

Attempting to simplify further while being aware of possible issues with non-commuting operators, we define the creation and annihilation operators, $\hat{a}^\dagger$ and $\hat{a}$ respectively, as:

$$\hat{a}^\dagger = \hat{X}_1 - i\hat{P}_1, \tag{2.5}$$

$$\hat{a} = \hat{X}_1 + i\hat{P}_1. \tag{2.6}$$

By considering the values of $\hat{a}\hat{a}^\dagger$ and $\hat{a}^\dagger\hat{a}$, the Hamiltonian is written in a more simple form:

$$\hbar\omega\left[\hat{a}^\dagger\hat{a} + \frac{1}{2}\right]\Psi_n\left(x\right) = E_n\Psi_n\left(x\right), \tag{2.7}$$

with the creation and annihilation operators satisfying the commutation relations:

$$\left[\hat{a}, \hat{a}^\dagger\right] = 1, \tag{2.8}$$

$$\left[\hat{a}^\dagger, \hat{a}^\dagger\right] = \left[\hat{a}, \hat{a}\right] = 0, \tag{2.9}$$

$$\left[\hat{H}, \hat{a}\right] = -\hbar\omega\hat{a}, \tag{2.10}$$

$$\left[\hat{H}, \hat{a}^\dagger\right] = \hbar\omega\hat{a}^\dagger. \tag{2.11}$$

From this, the following relations can be derived:

$$\hat{H}\hat{a}\Psi_n(x) = (E_n - \hbar\omega)\,\hat{a}\Psi_n(x) \tag{2.12}$$

$$\hat{H}\hat{a}^\dagger\Psi_n(x) = (E_n + \hbar\omega)\,\hat{a}^\dagger\Psi_n(x) \tag{2.13}$$

Here, $\hat{a}^\dagger$ and $\hat{a}$ are ladder operators for $\hat{H}$, operators that raise or lower the eigenvalues of another function.

2.2 Fock States

For ease of analysis, we switch to Dirac notation, denoting $\Psi_n(x)$ as $|n\rangle$. This changes Equation 2.1 to:

$$\hat{H}\,|n\rangle = E_n\,|n\rangle\,. \tag{2.14}$$

If the states $\Psi_{n-1}(x)$ and $\Psi_{n+1}(x)$ are given by $|n-1\rangle$ and $|n+1\rangle$, with energies $E_n - \hbar\omega$ and $E_n + \hbar\omega$ respectively, the effects of applying creation and annihilation operators to Fock states can be described:

$$\hat{a^\dagger}\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \tag{2.15}$$

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,. \tag{2.16}$$

For an n-photon state, we can define a Fock state as an eigenstate for the photon number operator $\hat{n}$.

$$\hat{n}\,|n\rangle = \hat{a}^\dagger\hat{a}\,|n\rangle = n\,|n\rangle\,, \tag{2.17}$$

$$|n\rangle = \frac{\hat{a}^{\dagger n}}{\sqrt{n!}}\,|0\rangle \tag{2.18}$$

These form an orthonormal basis, with a general state $|\Psi\rangle$ given by:

$$|\Psi\rangle = \sum_{n=0}^{\infty} a_n |n\rangle \tag{2.19}$$

We use these to define a coherent state $|\alpha\rangle$ as an eigenstate of the annihilation operator:

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle . \tag{2.20}$$

Using the completeness relation $|\alpha\rangle = \sum |n\rangle \langle n|\alpha\rangle$, we can find that:

$$|\alpha\rangle = \langle 0|\alpha\rangle \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}. \tag{2.21}$$

Applying normalisation gives the final expression:

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n \hat{a}^\dagger}{n!} |0\rangle , \tag{2.22}$$

with inner product:

$$\begin{aligned} \langle\alpha|\beta\rangle &= e^{-\frac{1}{2}\left(|\alpha|^2+|\beta|^2\right)} \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{\alpha^{\dagger n}\beta^m}{\sqrt{n!m!}} \langle n|m\rangle , \\ \langle\alpha|\beta\rangle &= e^{-\frac{1}{2}\left(|\alpha|^2+|\beta|^2\right)+\alpha^\dagger\beta}, \end{aligned} \tag{2.23}$$

using $\langle n|m\rangle = \delta_{nm}$ due to orthonormality.

2.3 Quadratures

In second quantization, we define the quadrature operators as:

$$\hat{X}_1 = \frac{1}{2}\left(\hat{a} + \hat{a}^\dagger\right), \tag{2.24}$$

$$\hat{P}_1 = \frac{1}{2i}\left(\hat{a} - \hat{a}^\dagger\right). \tag{2.25}$$

With eigenstates:

$$\hat{X}\left|x\right\rangle = x\left|x\right\rangle, \tag{2.26}$$

$$\hat{P}\left|p\right\rangle = p\left|p\right\rangle. \tag{2.27}$$

Where $\left|x\right\rangle$ and $\left|p\right\rangle$ are the states with eigenvalues x and p respectively.

Together, these are two components of the amplitude of the electric field. These operators are analogous to the position and momentum operators from Equation 2.1, and fulfill the relations:

$$\left[\hat{X}, \hat{P}\right] = \frac{i}{2} \tag{2.28}$$

$$\left\langle x_1 | x_2 \right\rangle = \delta\left(x_1 - x_2\right) \tag{2.29}$$

$$\left\langle p_1 | p_2 \right\rangle = \delta\left(p_1 - p_2\right) \tag{2.30}$$

By checking expectation values of these quadratures when applied to the coherent state $\left|\alpha\right\rangle$, we can verify that these values are real and imaginary components of α.

$$\begin{aligned} \langle\hat{X}_1\rangle &= \langle\alpha|\hat{X}_1|\alpha\rangle = \frac{1}{2}\left\langle\alpha|\hat{a}+\hat{a}^\dagger|\alpha\right\rangle \\ \langle\hat{X}_1\rangle &= \frac{1}{2}\left(\alpha+\alpha*\right) = \Re\left(\alpha\right) \end{aligned} \tag{2.31}$$

$$\begin{aligned} \langle\hat{P}_1\rangle &= \langle\alpha|\hat{P}_1|\alpha\rangle = \frac{1}{2i}\left\langle\alpha|\hat{a}-\hat{a}^\dagger|\alpha\right\rangle \\ \langle\hat{P}_1\rangle &= \frac{1}{2i}\left(\alpha-\alpha*\right) = \Im\left(\alpha\right) \end{aligned} \tag{2.32}$$

For measurement, we rely on homodyne detection, as shown in Figure 2.1. The incoming signal to be measured is mixed with a coherent source $\left|\alpha\right\rangle$ at a beam splitter and the difference in intensity of the outputs is measured. Beam intensity is proportional to photon number, allowing it to be inferred from measurements:

$$i_3 - i_4 \propto \langle \hat{n}_3 - \hat{n}_4 \rangle \, . \tag{2.33}$$

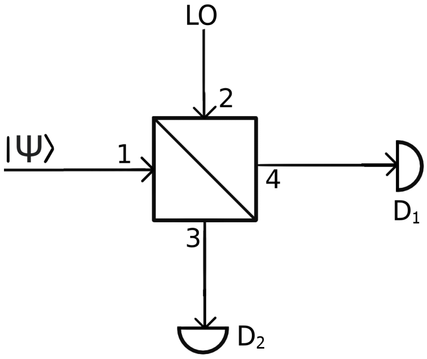


Figure 2.1: **Homodyne Detection.** The method of measuring quadratures, through mixing an input state $|\Psi\rangle$ with a local oscillator, here, a coherent state.

For a 50:50 beam splitter, with transmittance and reflectance $T = \frac{1}{\sqrt{2}}$ and $R = \frac{i}{\sqrt{2}}$ respectively, we express the output number operators in terms of the input number operators.

$$\hat{n}_4 = \hat{a}_4^\dagger \hat{a}_4 \tag{2.34}$$

$$\hat{a}_4 = T\hat{a}_1 + R\hat{a}_2 = \frac{1}{\sqrt{2}} \left(\hat{a}_1 + i\hat{a}_2 \right) \tag{2.35}$$

$$\hat{a}_3 = R\hat{a}_1 + T\hat{a}_2 = \frac{1}{\sqrt{2}} \left(i\hat{a}_1 + \hat{a}_2 \right) \tag{2.36}$$

$$\hat{n}_3 - \hat{n}_4 = i \left(\hat{a}_2^\dagger \hat{a}_1 - \hat{a}_1^\dagger \hat{a}_2 \right) \tag{2.37}$$

With the beam to be measured, and a coherent source, entering the first and second ports respectively, we find the expectation values of the quadrature operators:

$${}_1\langle \Psi|_2 \langle \alpha| \, \hat{n}_3 - \hat{n}_4 \, |\alpha\rangle_2 \, |\Psi\rangle_1 \propto_1 \langle \Psi| \, \frac{1}{2i} \left(\hat{a}_1 e^{-i\phi} - \hat{a}_1^\dagger e^{i\phi} \right) |\Psi\rangle_1 \, . \tag{2.38}$$

Setting $\phi = \frac{\pi}{2}$ or $\phi = 0$, gives amplitude difference measurements proportional to $\langle\Psi|\hat{X}|\Psi\rangle$ and $\langle\Psi|\hat{P}|\Psi\rangle$ respectively. With the expectation values of the quadrature operators found, we have our method of quadrature measurements, which will be required for our analysis.

Continuing with relevant background information, we now proceed to discussion of entropy, calculations of which allow for analysis of results in order to verify that secrecy for a broadcast has been established.

2.4 Shannon information

Entropy is a measure of uncertainty in the outcome of a random event. For such an event A with n possible outcomes, the Shannon entropy $H\left(A\right)$ is given by:

$$H\left(A\right) = -\sum_{i=1}^{n} P\left(x_i\right) \log_2 P\left(x_i\right), \tag{2.39}$$

where the outcome x_i occurs with probability $P\left(x_i\right)$. For a binary event with outcomes 0 and 1, such as a coin flip, the outcome possibilities are given by $p_0 = p$ and $p_1 = 1 - p$. The Shannon entropy reduces to:

$$H\left(A\right) = -p \log_2 p - \left(1 - p\right) \log_2 \left(1 - p\right). \tag{2.40}$$

As expected, plotting such a function shows maximum uncertainty is reached when both outcomes are equally likely, with zero uncertainty when one outcome occurs with probability 1. This is shown in Figure 2.2.

This can be extended to multiple variables. If $H\left(B\right)$ is defined in the same manner as $H\left(A\right)$, with m outcomes y_j occurring with probability $P\left(y_j\right)$, the joint Shannon entropy for both events, $H\left(A,B\right)$, can be given by:

$$H\left(A,B\right) = -\sum_{i=1}^{n} \sum_{j=1}^{m} p\left(x,y\right) \log_2 p\left(x,y\right), \tag{2.41}$$

where $p\left(x,y\right)$ is the joint probability distribution describing the pair of variables.

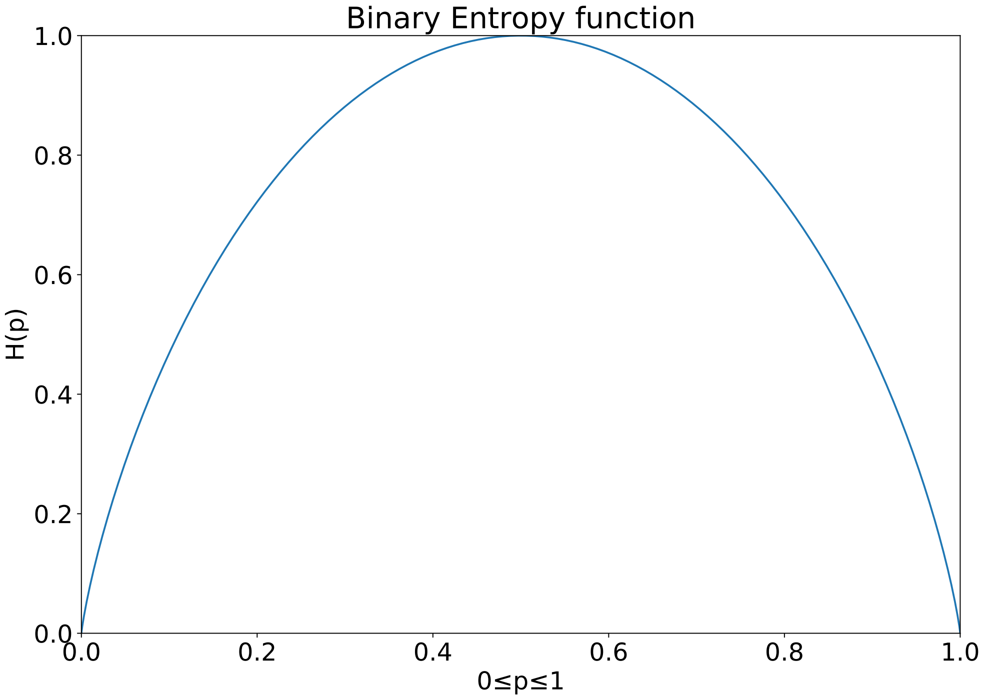


Figure 2.2: **Binary Entropy.** Measurement of entropy for a system with two possible outcomes, with one outcome having the probability p.

Also of note is the Shannon mutual information, $H(A;B)$. This functions as a way to quantify how much can be learned about a variable through observation of a second variable on which it has dependence. For two discrete variables, we define this as:

$$H(A;B) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log_2 \frac{p(x_i, y_j)}{p_A(x_i)\, p_B(y_j)}. \tag{2.42}$$

Here, the marginal distributions for each variable are given by $p_A(x_i)$ and $p_B(y_j)$.

Finally, we introduce a third variable, C, to define the conditional mutual information:

$$H(C) = -\sum_{k=1}^{l} P(z_i) \log_2 P(z_i), \tag{2.43}$$

$$H(A;B \mid C) = H(A,C) + H(B,C) - H(A,B,C) - H(C), \tag{2.44}$$

as the mutual information of two events when the value of a third is known.

2.5 Von Neumann information

The concepts of mutual information can be extended to describe quantum mechanical systems. For a quantum mechanical system described by the n-dimensional density matrix ρ, the von Neumann entropy $S(\rho)$ is given by:

$$S(\rho) = -\mathrm{Tr}\rho \log_2 \rho \tag{2.45}$$

As with the previous version, we can see that this reduces to zero when there is no uncertainty. In this case, meaning that the ρ is a pure state. This can be seen through a choice in basis that diagonalises ρ:

$$\rho = \sum_{i=1}^{n} \lambda_i |i\rangle \langle i| , \tag{2.46}$$

for eigenvalues λ_i. This reduces to the Shannon entropy of the λ_i values.

$$S(\rho) = -\sum_{i=0}^{n} \lambda_i \log_2 \lambda_i \tag{2.47}$$

For a pure state, taking $\lambda_i = \delta_{i,j}$ for some $0 \leq j \leq n$ clearly shows $S(\rho) = 0$. Additionally, taking $\rho = \frac{I_n}{n}$ for a maximally mixed state gives the expected maximum entropy of $\log_2 n$.

The other concepts from Shannon entropy can also be extended to quantum states. For a three-part system (A,B,C) with density matrix ρ_{AB} we can define the joint von Neuman entropy and the mutual information between two parts, and the conditional mutual information, $S(A,B)$, $S(A;B)$, and $S(A;B|C)$:

$$S(A,B) = -\mathrm{Tr}\left(\rho_{AB} \log_2 \rho_{AB}\right) \tag{2.48}$$

$$S(A;B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \tag{2.49}$$

$$S\left(A;B|C\right) = S\left(A;B\right) - S\left(C\right) \tag{2.50}$$

Where ρ_A and ρ_B describe the partial traces.

2.6 Covariance matrices

In this work, the mean and variance is enough information to fully define the states we are employing. Beginning with quadrature operators for a single state, the mean is simply defined as the expectation value of the quadrature operators $\hat{x}$ and $\hat{p}$:

$$\langle\hat{x}\rangle = \mathrm{Tr}\left(\rho\hat{x}\right), \tag{2.51}$$

$$\langle\hat{p}\rangle = \mathrm{Tr}\left(\rho\hat{p}\right). \tag{2.52}$$

Taking

$$\hat{r} = \begin{bmatrix} \hat{x} \\ \hat{p} \end{bmatrix} \tag{2.53}$$

gives the formula for the covariance matrix elements:

$$\gamma_{ij} = \mathrm{Cov}\left[\hat{r}_i, \hat{r}_j\right] = \langle\left(\hat{r}_i - \langle\hat{r}_i\rangle\right)\left(\hat{r}_j - \langle\hat{r}_j\rangle\right)\rangle \tag{2.54}$$

where the elements $\langle\hat{r}_i\rangle$ form the displacement vector.

For the thermal states we are interested in, the covariance matrix for a single mode with average photon number $\bar{n}$ is given by

$$\gamma = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix}, \tag{2.55}$$

where $V = 2\bar{n} + 1$ is the thermal state variance. This reduces to the identity with zero photons, the covariance matrix for a vacuum state.

2.7 N mode states

For the approaching work, we will need to extend this treatment to multiple modes. For an n mode state with $\hat{x}_i$ and $\hat{p}_i$ as the quadrature operators for the i^{th} mode, we find:

$$\hat{r} = \begin{bmatrix} \hat{x}_0 \\ \hat{p}_0 \\ \hat{x}_1 \\ \hat{p}_1 \\ \vdots \\ \hat{x}_n \\ \hat{p}_n \end{bmatrix}. \tag{2.56}$$

We can also define the n-mode covariance matrix:

$$\gamma = \begin{bmatrix} \gamma_0 & C_{01} & \cdots & C_{0n} \\ C_{01}^T & \gamma_1 & \cdots & C_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{0n}^T & C_{1n}^T & \cdots & \gamma_n \end{bmatrix}, \tag{2.57}$$

where γ_i is the covariance matrix for the i^{th} mode in the system, and C_{ij} describes covariance between different modes. This will allow us to consider entangled thermal states in different locations, such as those observed in the outputs of a beam splitter.

For this work, we will use the beam splitter transformation along with covariance matrices to make mutual information calculations. This transformation is given by:

$$B\left(T,R\right) = \begin{bmatrix} T & R \\ R & T \end{bmatrix} \otimes I_{2\times 2}, \tag{2.58}$$

$$\begin{bmatrix} \hat{x}_0 \\ \hat{p}_0 \\ \hat{x}_1 \\ \hat{p}_1 \end{bmatrix}_{out} = B\left(T,R\right) \begin{bmatrix} \hat{x}_0 \\ \hat{p}_0 \\ \hat{x}_1 \\ \hat{p}_1 \end{bmatrix}_{in} . \tag{2.59}$$

Here, $B\left(T,R\right)$ is the transformation for a beam splitter acting on a pair of input modes with transmittance and reflectance T and R, defined such that $T^2 + R^2 = 1$.

2.8 Gaussian States

Thermal States

The majority of work concerning quantum information is performed using Gaussian states, which includes coherent, thermal, and squeezed states, each of which are easily accessible in a lab environment.

The specific type we will be employing, thermal sources, are currently widely used in modern wireless communication including satellite transmissions, mobile phones, Wi-Fi and Bluetooth. However, such states are not commonly considered for applications in QKD, due to the addition of noise in broadcast and detection. Instead, coherent states, accessible through lasers and fibre-optics, are commonly used. Of particular note is one such example, the Gaussian modulated Coherent State (GMCS) protocol, which relies on broadcasting coherent states with amplitudes randomly selected from a Gaussian distribution. This is relevant as the output of the source in a GMCS protocol is statistically equivalent to that of a thermal source, meaning from an eavesdropper's point of view, the protocols are equivalent. This allows security proofs from a known coherent state protocol to be applied to the work we are about to present.

2.9 Displacement

While it is interesting to test if thermal states could be used to create keys, such unmodulated sources are not typically used in microwave communication. Phase-shift keying (PSK) is a process usually used for such broadcasts. Here, multiple displaced thermal states, commonly separated only by phase, are used to transmit information.

The displacement operator is a unitary operator given by:

$$\hat{D}\left(\alpha\right) = e^{\alpha \hat{a}^{\dagger} - \alpha^{*} \hat{\alpha}}, \tag{2.60}$$

$$\hat{D}^{\dagger}\left(\alpha\right) = \hat{D}\left(-\alpha\right), \tag{2.61}$$

$$\hat{D}^{\dagger}\left(\alpha\right) = \hat{D}^{-1}\left(\alpha\right). \tag{2.62}$$

Where $\alpha \in \mathbb{C}$ is the displacement parameter. Intuitively, displacement operators can be combined into a single displacement operator with the total displacement:

$$\begin{aligned} \hat{D}\left(\alpha\right)\hat{D}\left(\beta\right) &= e^{\alpha \hat{a}^{\dagger} - \alpha^{*} \hat{\alpha}} e^{\beta \hat{a}^{\dagger} - \beta^{*} \hat{\beta}}, \\ \hat{D}\left(\alpha\right)\hat{D}\left(\beta\right) &= e^{\frac{1}{2}\left(\alpha\beta^{*} - \alpha^{*}\beta\right)}\hat{D}\left(\alpha + \beta\right). \end{aligned} \tag{2.63}$$

The added scale factor does not end up impacting calculations, allowing combining of displacement operators to work as expected. Figure 2.3 shows the effects of the displacement operator in phase space, with states and operators being displaced by α:

$$\hat{D}^{\dagger}\left(\alpha\right)\hat{a}\hat{D}\left(\alpha\right) = \hat{a} + \alpha, \tag{2.64}$$

$$\hat{D}^{\dagger}\left(\alpha\right)\hat{a}^{\dagger}\hat{D}\left(\alpha\right) = \hat{a}^{\dagger} + \alpha^{*}. \tag{2.65}$$

We can use this operator to define a coherent state $|\alpha\rangle$ as a displaced vacuum state:

$$\hat{D}(\alpha)|0\rangle = |\alpha\rangle \,. \tag{2.66}$$

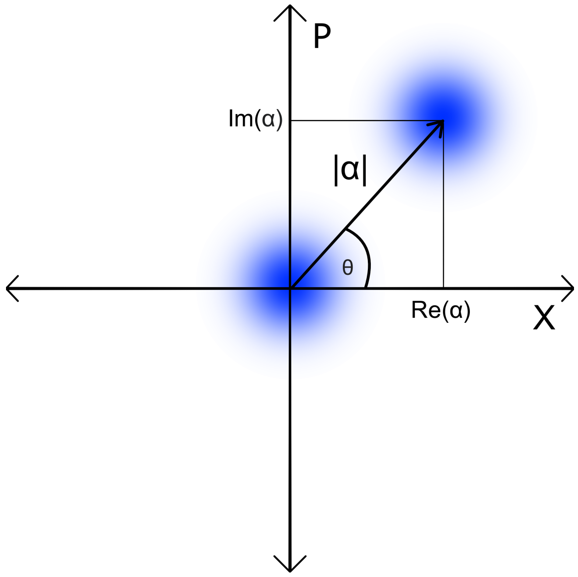


Figure 2.3: **Displacement.** A vacuum state being displaced with displacement parameter α. This forms the coherent state $|\alpha\rangle$

2.10 Thermal Broadcasting

In broadcasting, information is commonly transmitted through modulation of a carrier signal, typically a sinusoidal wave with constant amplitude and frequency before modulation. There are many approaches to accomplishing this, with the simple options being Frequency Modulation (FM) and Amplitude Modulation (AM), in which information is encoded through different choices of frequency or amplitude respectively. For AM broadcasts, this involves multiplying the carrier signal by the baseband, as shown in Figure 2.4. Note that the baseband has been translated up such that it is never negative. This avoids issues of ambiguity, as when the signal is received, measuring amplitude would not reveal if the carrier signal had been multiplied by a positive or negative value.

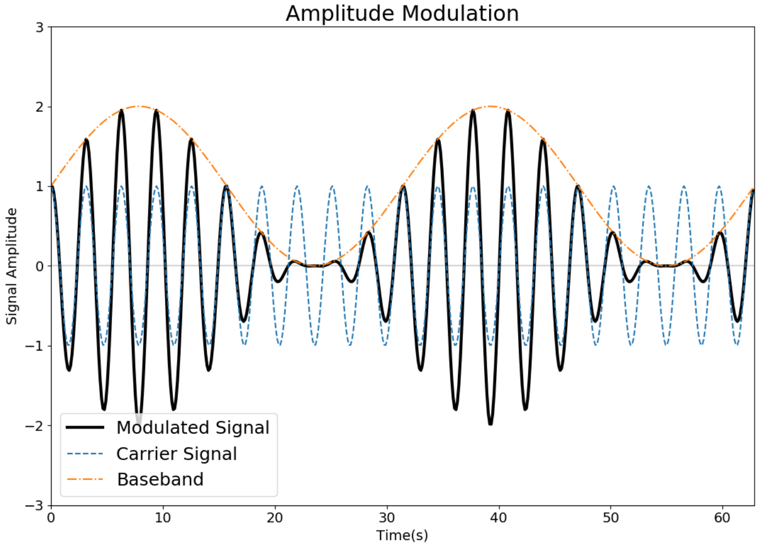


Figure 2.4: **Amplitude Modulation.** A carrier signal is multiplied by a non-negative baseband signal to produce the final broadcast.

For FM broadcasts, the frequency of the carrier is adjusted as shown in Figure 2.5. Defining the frequency at any point in time as the rate of change of phase allows adjustment of frequency by adding the integral of the baseband as a time-dependent phase offset. Equations 2.67 and 2.68 show the forms that these waves take for AM and FM broadcasts respectively, for a carrier with amplitude A_C and angular frequency ω_C, and a baseband of amplitude $A_{BB}\left(t\right)$.

$$\Phi_{AM}\left(t\right) = A_{BB}\left(t\right) A_C \cos\left(\omega_C t\right) \tag{2.67}$$

$$\Phi_{FM}\left(t\right) = A_C \cos\left(\omega_C t + \int_0^t A_{BB}\left(\tau\right) d\tau\right) \tag{2.68}$$

More complex variants of these modulations are available, Quadrature Amplitude Modulation (QAM) and Phase-Shift Keying (PSK).

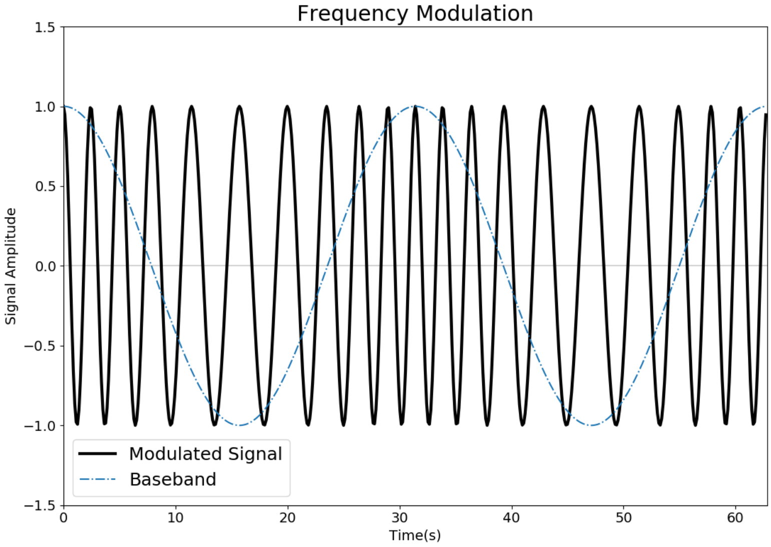


Figure 2.5: **Frequency Modulation.** The offset in frequency given to carrier wave is proportional to the baseband amplitude.

These methods are commonly seen in modern communications systems, most notably Wi-Fi. For both of these methods, the broadcast consists of a pair of sinusoidal carrier waves which are $\frac{\pi}{2}$ out of phase with each other, referred to as the In Phase (I) and Quadrature (Q) components of the broadcast. A pair of such carriers can be amplitude-modulated and summed together to create a variety of different waves, as shown in Figure 2.6.

Using this pair of out-of-phase carrier waves, information can be encoded through varying the amplitudes of the I and Q components between a set of predetermined values. For QAM, this takes the form shown in Figure 2.7, with points arranged in a grid pattern, while Phase-Shift Keying instead uses points evenly spaced around a circle. An example of this performed for four points, referred to as Quadrature Phase-Shift Keying (QPSK) is shown in Figure 2.8. In both of these cases, the amplitudes of the I and Q components of transmitted signals are plotted on the axes.

In both of these cases, information is broadcast by encoding one of the four (16 for 16-QAM) possible binary entries in each of the 4 (16) states being broadcast. It is clear that 4-QAM and QPSK show the same diagram, and are equivalent broadcasts.

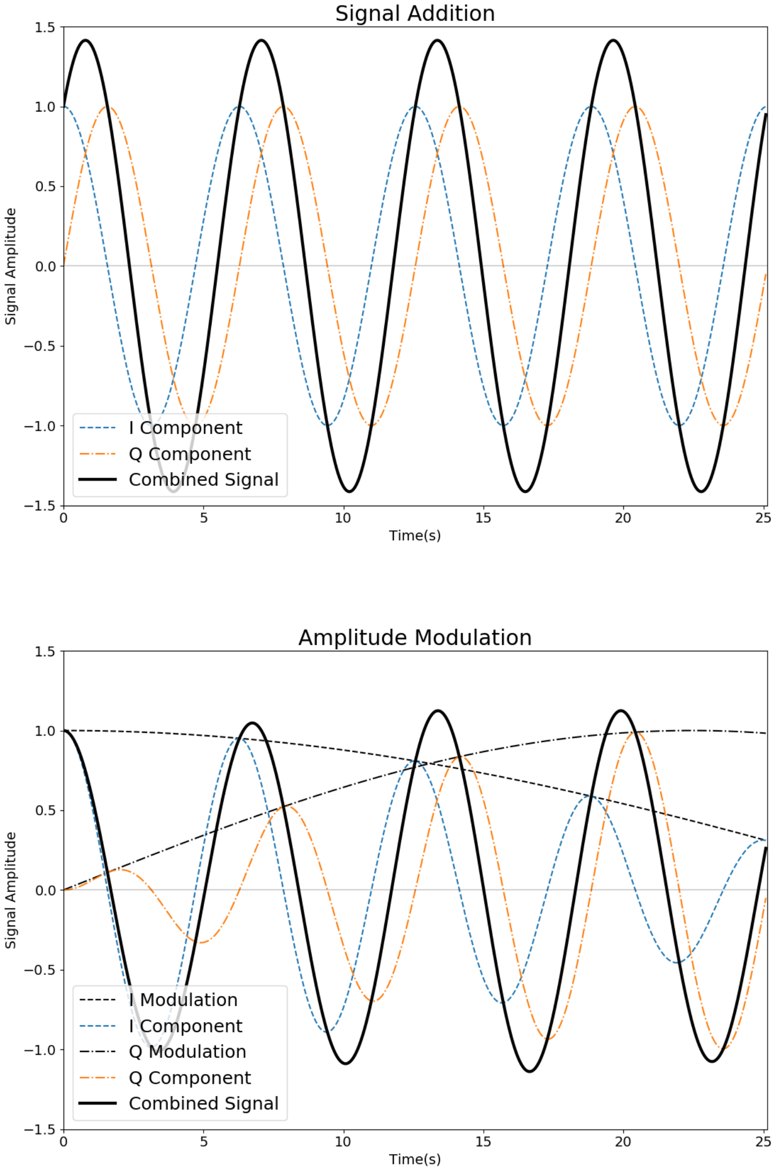


Figure 2.6: **Signal Addition.** A pair of carrier waves summing to create a broadcast signal. Adjusting the amplitudes scaling the I and Q components changes the broadcast signal.

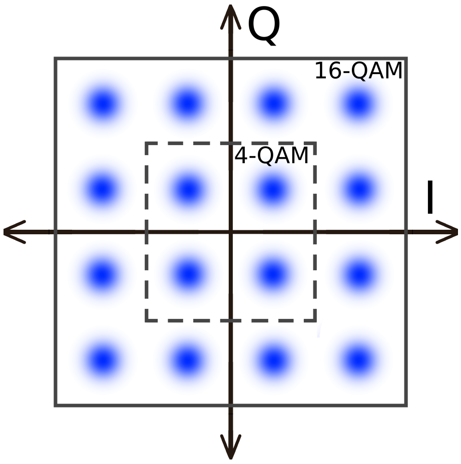


Figure 2.7: **Quadrature Amplitude Modulation.** A phase diagram for 16-QAM. Constraining the diagram to the centre four states gives the phase diagram for 4-QAM.

Also included in Figure 2.8 is a plot of the component signals that make up a QPSK/4-QAM broadcast, being varied over time to produce the four possible broadcasts. However, this is an idealised view. Perfect sinusoidal waves would produce single points at the centre of the clusters in the I/Q plot, whereas in real broadcasts, noise results in imperfect signals, leading to circular clusters of potential signals as seen in the I/Q plots.

In normal Amplitude Modulation, the baseband scaling the carrier amplitude was non-negative. This is not true for these more complex methods which allow for negative quadrature measurements, giving access to broadcasts in all four quadrants of the I/Q graph.

These I/Q diagrams are of similar form to the X/P quadrature graph shown earlier in Figure 2.3, a QPSK broadcast consists of a set of four displaced thermal states, separated by phase.

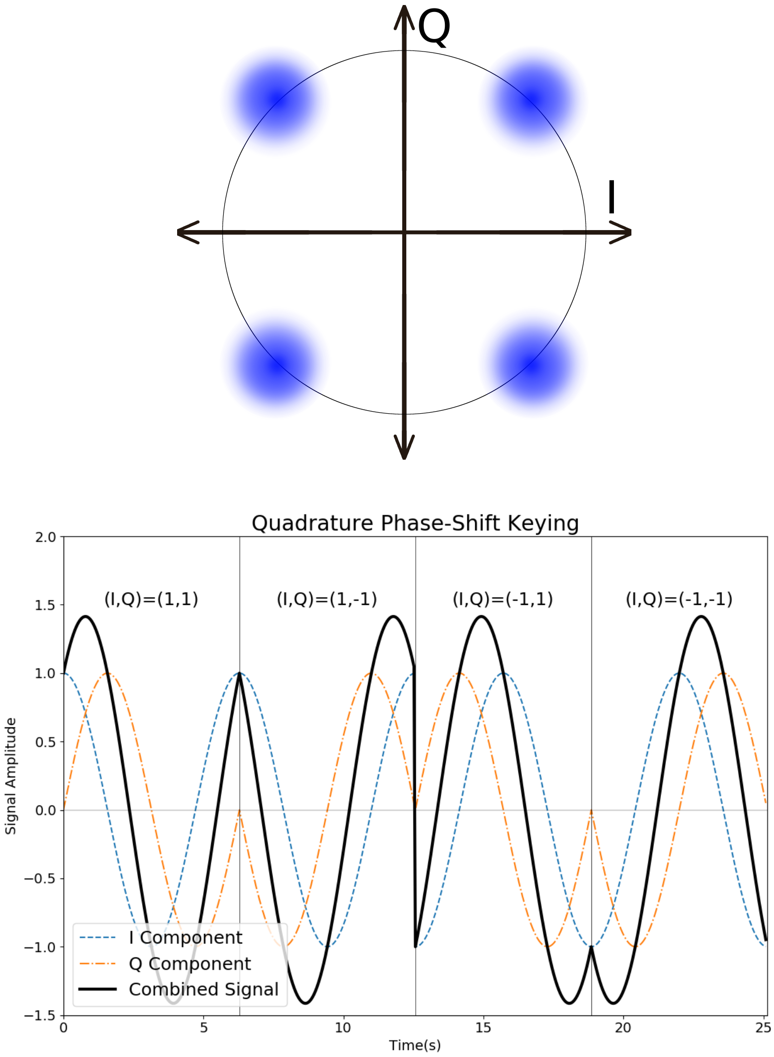


Figure 2.8: **QPSK.** Quadrature Phase-Shift Keying. Four states are equally spaced around a circle, centred on the origin in phase space.

Chapter 3

Introduction to Quantum Key Distribution

While classical methods have so far been useful for security purposes, the assumption that the functions used cannot be reversed in a reasonable time may not be a reliable one. As computers become more powerful, and more algorithms are created, methods of breaking such security may eventually be found. Therefore, it is desirable to create methods of key distribution which do not make assumptions about the level of computing power available to an eavesdropper. Using classical methods, the only available option is to distribute keys through trusted couriers, which is not a practical method of establishing secure channels.

Quantum key distribution enters as a solution to the problem of arbitrarily strong attackers. Instead of basing security on the difficulty of certain mathematical problems, QKD relies on the rules of quantum mechanics, with the aim of allowing secure communication regardless of the attacker's computing power. For such protocols, we assume an eavesdropper may perform any operations on intercepted states broadcast using the quantum channel which are permitted by quantum mechanics. This allows for minimal requirements to be placed on the quantum channel. We also require an authenticated classical channel, through which Alice and Bob can communicate publicly without the ability for the eavesdropper to modify messages. This may be implemented through an authentication protocol which provides the same level of security as QKD, or through short keys distributed previously through methods such as couriers. Due to smaller key lengths required for authentication, couriers are more reasonable for this purpose compared to using couriers to deliver keys for encryption.

There are two common groups for QKD protocols. Prepare-and-Measure protocols, and Entanglement-Based protocols. These are shown in Figure 3.1:

- Prepare and Measure: Alice creates a quantum state which has been used to encode classical information, and sends it to Bob for measurement in order for communication to be established.
- Entanglement-Based: A central source, separate from Alice and Bob, broadcasts entangled states, with each party receiving one part of the state, giving Alice and Bob correlated measurements.

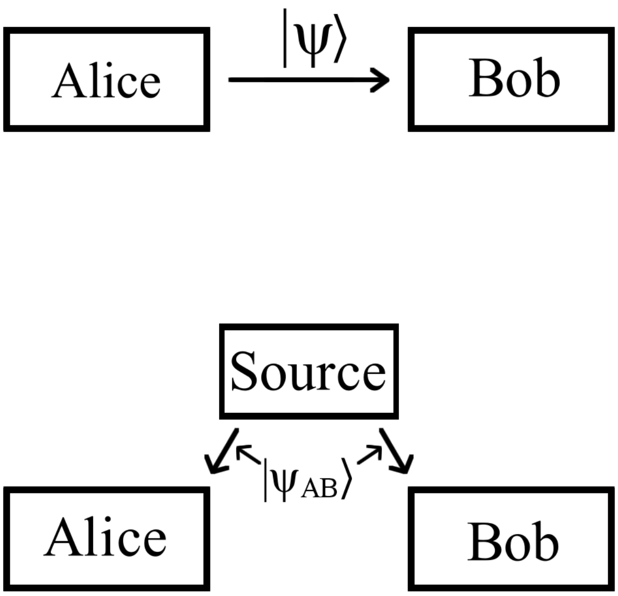


Figure 3.1: **QKD Protocols.** Two general groups of QKD protocols, Prepare-and-Measure (Top), and Entanglement-Based (Bottom).

Regardless of method, the final result is a set of correlated bit strings possessed by Alice and Bob, and potentially an eavesdropper. This matches the outputs of classical key distribution, and at this point refining the bit strings into a key is a classical problem.

3.1 Refining

For public key distribution, the protocol begins with a publicly-shared key and a second, private key, which is kept by the person receiving the message, both of these keys are created by one of the parties involved and do not require the same further processing that symmetric keys require. For symmetric keys, imperfections in the distribution protocols will result in correlated, but not perfectly matching, keys for the involved parties, necessitating additional steps.

This begins with advantage distillation if necessary, which is when Alice and Bob initially share less information than either of them do with Eve. There are multiple protocols to allow Alice and Bob to gain a superior position compared to their eavesdropper, with a well-known example being the bit pair protocol. Alice and Bob split a bit string into pairs and publicly compare the parity of each pair. For pairs where they agree, they both decide on a bit to discard and keep the other, otherwise, both bits are discarded. This produces a shorter bit string which can be used for another attempt at the bit pair protocol.

If advantage distillation is carried out successfully. Alice and Bob will share more information about each other's bit strings than either do with Eve, giving them a superior position. At this point, Alice and Bob go through information reconciliation, the process by which their errors are corrected while attempting to provide minimal information to Eve. A well-studied protocol for attaining this is the Cascade algorithm, which relies on a similar parity-check method to what was described in advantage distillation. Alice and Bob divide their strings into blocks, and compare the parities of each block. Should errors be detected, the block is split in half and parities are checked again. This is repeated until an error is fixed. After this, Bob shuffles the key, and splits the shuffled key into blocks to begin the process again. Telling Alice how the key has been shuffled allows Alice and Bob to continue comparing parities of the correct bits. Correcting errors this way may change parities of previously used blocks, allowing detection of errors that were missed in previous passes. This process keeps repeating for a predetermined number of shuffles or no more errors are detected. Shuffling after each iteration is necessary as comparing block parities can only detect an odd number of errors within the blocks, resulting in false positives in which blocks with any even numbers of errors are stated to have zero errors.

The final step is then privacy amplification, in which Alice and Bob use their now equal keys along with public discussion to minimise Eve's knowledge of the key. This may be carried out through applying a randomly chosen hash function to the key, agreed on by Alice and Bob. These are functions which ideally only produce the same output when given identical inputs, and those outputs then become the final key. Any errors on Eve's part will then prevent discovery of the key, as even applying the same hash function as Alice and Bob would result in Eve having a completely uncorrelated key.

3.2 Discrete QKD

QKD begins with Bennett and Brassard's protocol in 1984 (BB84) [18]. Here, Alice picks a pair of orthogonal bases, separated by a $\pi/4$ angle. Alice and Bob first agree to define horizontally and vertically aligned photons $|0\rangle$ and $|1\rangle$ as 0 and 1 respectively, and doing the same for the diagonal basis:

$$|\phi_{H0}\rangle = |0\rangle\,, \tag{3.1}$$

$$|\phi_{H1}\rangle = |1\rangle\,, \tag{3.2}$$

$$|\phi_{D0}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \tag{3.3}$$

$$|\phi_{D1}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{3.4}$$

These give four possible states for the four choices, $|\phi_{H0}\rangle$ and $|\phi_{H1}\rangle$ describing a 0 or 1 in the horizontal/vertical basis, with $|\phi_{D0}\rangle$ and $|\phi_{D1}\rangle$ filling the same role for the diagonal basis.

After Alice decides on a bit string to send, and which basis to encode each bit in, all of which is done at random, they send photon pulses with the appropriate states encoded to Bob who also randomly decides on which basis to measure each received state in. Here, security arises from the random switching of basis, and Eve's inability to copy the states being sent to Bob.

Bit	1	1	0	0	...	0	1	1
Alice's Basis	→	↗	→	↗	...	↗	→	→
Broadcast State	$\|\phi_{H1}\rangle$	$\|\phi_{D1}\rangle$	$\|\phi_{H0}\rangle$	$\|\phi_{D0}\rangle$	...	$\|\phi_{D0}\rangle$	$\|\phi_{H1}\rangle$	$\|\phi_{H1}\rangle$
Bob's Basis	→	↗	↗	→	...	↗	↗	→
Measurements	1	1	X	X	...	0	X	1

Figure 3.2: **BB84.** Alice randomly selects bits and broadcast bases and sends the resulting state to Bob, who measures in a random basis. Measurements where they picked the same basis may be used to create a key.

As Bob and Eve are unaware of which basis Alice encoded each bit in, they will make an incorrect choice for 50% of bits. This leads to errors where mismatched choices of basis give two possible, equally likely measurement outcomes for Bob and Eve. Should Eve attempt to intercept, perform measurements, then send results to Bob, Eve risks introducing errors. Should Eve for example use the horizontal basis and measure $|\phi_{H0}\rangle$, this could be correct, however the same measurement has a 50% chance of being made should Alice have sent $|\phi_{D1}\rangle$. Should Eve then send $|\phi_{H0}\rangle$ to Bob, Bob will not make the same measurement as Alice even with a correct choice of basis. A comparison of Alice and Bob's measurements would reveal such errors, and Alice and Bob would become aware that an eavesdropper was present. At this point the protocol would be aborted. A sample of some bits and bases are shown in Figure 3.2, with pulses where Alice and Bob picked the same basis producing a shorter, shared bit string for use in creating a key.

Should no issues be found in a comparison of Alice and Bob's measurements in a select set of bits where they chose the same basis, they may proceed to refining the remaining bits into a key. This stage is performed in the same fashion as with classical key distribution, through communication over the authenticated classical channel.

3.3 Improvements to BB84

This does lead to an issue in that perfect single photon sources are difficult to create, and multiple photons will have some probability of being unintentionally broadcast by an imperfect source. This allows Eve to attack by blocking pulses which consist of a single photon, and intercepting multi-photon pulses to keep one photon for measurement, with the remainder continuing to Bob as intended [19].

This problem is averted through the decoy state method. As Eve intercepts multi-photon pulses in order to send all but one photon, while blocking single photon pulses, Bob will observe multi-photons pulses as having a higher chance of being received for measurement. By intentionally broadcasting multi-photon pulses, Alice and Bob can consider the yields of these pulses to verify if unusually high yields are measured due to Eve's attempts to resend pulses.

In the decoy method, Alice uses multiple sources with different average photon numbers, and switches between them at random during the broadcast. Afterwards, Alice reveals which pulses came from which source. If sources which broadcast more multi-photon pulses have a higher chance of being transmitted to Bob, then they can conclude that an eavesdropper is blocking single photon pulses, and that the protocol should be stopped. This method can be implemented with a pair of decoy states, with early work showing little advantage observed in using more decoy states [20].

3.4 Continuous QKD

A diverging field of interest instead focused on encoding data in continuous variables, specifically the quadratures of a coherent state [21, 22]. In this method, Alice creates a series of pairs of random values, and encodes those values as X and P quadratures of a coherent state to be sent to Bob. Bob randomly decides which quadrature to measure when receiving the signal, and switches this choice at random points during the broadcast. With Bob possessing a string of measurements, Alice and Bob decide which quadrature the key will be encoded in. Measurements made on the other quadrature can be publicly compared to check that Alice and Bob are making correlated measurements. This does lead to a weakness in that with a strong enough broadcast, a small proportion may be split off by an eavesdropper for analysis of both quadratures. While measurement of both quadratures is not immediately possible due to the quadrature operators not commuting, measurements of both can be approximated by splitting the beam and measuring different quadratures of both output beams. Employing squeezed states led to improved security, though this initial continuous-variable method was outperformed by discrete-variable QKD.

This was later innovated on with the Gaussian Modulated Coherent State (GMCS) protocol [23]. Here, Alice randomly takes number pairs, x and p from a Gaussian distribution centred at the origin in phase space, and creates a coherent state $|x + ip\rangle$, which is sent to Bob for measurement. For each bit, Bob measures a single quadrature and shares the choice with Alice. This produces a string of correlated measurement values, which can then be converted into a bit string through prearranged methods.

3.5 Practical QKD

Beyond experimental work, devices for QKD have been produced for use by governments, as well as in commercial environments. Construction of quantum networks goes back 20 years, with the DARPA quantum network in 2003. Over 3 years of operation, the network was able to implement the BB84 protocol over 10km, between BBN Technologies and Harvard University but not over their longer, 19km channel. A key generation rate of 1000 bits/second was obtained over the shorter channel [24].

Shortly afterwards (2004-2008), the Secure Communication based on Quantum Cryptography (SECOQC) network was created, consisting of 8 QKD channels connecting 6 nodes over distances between 6-85 km [25]. This network used a variety of protocols, including BB84 as well as SARG04 – a similar protocol that does not require Alice announce which basis was chosen for each pulse. This allowed key distribution to be performed at distances of over 80 km at a rate of 0.6-0.8 kbps, with key rates of 27 kbps possible over 10 km. This network also performed QKD using the previously mentioned GMCS protocol, reaching rates of 8 kbps over a 6 km channel.

This was followed by the Tokyo QKD Network (2010), which showed commercial applications of QKD technology [26]. Here, video conferencing was carried out, which was secured by QKD at a 128 kbps rate over channels of length 24-90 km. This network was also able to detect an photon number splitting attack carried out during the demonstration. Similar efforts on widespread applications of QKD technology in South Korea; headed by ID Quantique and SK Telecomms, aimed to create a large network for use by public and private sectors.

While there have been many implementations of QKD, we see that work still needs to be done to make QKD accessible. This is in part due to current communications infrastructure not being suitable for QKD protocols, requiring specialised equipment. The following protocol, which is the subject of this research, attempts to address this issue. We aim to construct a protocol which can be performed by common communications equipment. In doing this, accessible QKD may become a software problem, with existing hardware already being relevant in the experimental setup.

3.6 Composability and Finite Key Effects

In cryptography, the earlier methods of discussing the level of security afforded by various protocols is not always considered sufficient. When a protocol is used as part of some larger system, it is reasonable to question if security is maintained. If a protocol is said to provide composable security, then it is considered secure even when combined with other protocols [27].

An additional factor to consider when moving away from ideal setups are finite key effects. In realistic scenarios, Alice and Bob are not capable of sending an infinite amount of signals, and have a limited time to perform the protocol for reasonable communication. This reduces the possible key rate and is not always accounted for in older discussions of security.

For the protocol we will be analysing we find that from an outside perspective, most importantly from the view of an eavesdropper, the broadcast sent between Alice and Bob is indistinguishable from those sent in the Gaussian Modulated Coherent State QKD protocol, which has been analysed with each [28, 29] of these effects taken into account. This allows us to proceed under the assumption that the thermal state protocol to be analysed affords the same level of security.

Chapter 4

Thermal State RF Key Distribution

4.1 Thermal Sources

For our work, rather than focus on coherent states, we will instead consider a radio key distribution protocol inspired by quantum methods which will rely on a thermal source. While coherent sources are useful as they have well-known applications involving lasers and fibre optics, thermal sources likewise see regular use in wireless communications, typically in the form of microwaves or radio waves. Mobile phones, Bluetooth, some satellites, and Wi-Fi are all examples of such equipment. Therefore, in order to devise QKD protocols which could be implemented on commonly-used devices, it is useful to focus on microwave sources. While fibre networks also see common use in communications, the cost of burying cables becomes expensive. Working with thermal states potentially allows for transition to wireless, which circumvents this issue.

While optical methods can similarly be implemented wirelessly, even over long distances, such methods require line-of-sight between transmission and detection. This restriction is not shared by thermal broadcasts, as is clearly seen from the uncontrolled environments in which modern communication equipment is expected to operate.

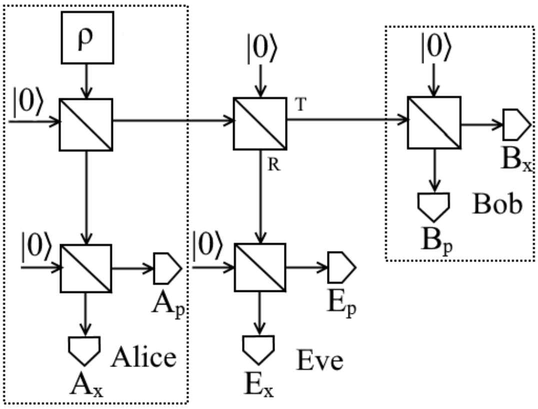


Figure 4.1: **The thermal state protocol.** The central broadcast protocol which will be analysed. This diagram was originally used in "Thermal state quantum key distribution" [1], and is licensed under CC-BY 4.0. [5]

In the central broadcast thermal protocol, a thermal source is incident on a 50:50 beam splitter, the outputs of which are directed to Alice and Bob. If it is assumed each person has control over their own measuring equipment, and the source is held by Alice, this leaves an unsecured channel between the initial beam splitter and Bob, through which interception can occur. Eve intercepts through the use of a beam splitter of unknown reflectance, siphoning off part of the beam directed to Bob before it can be measured. This is all shown in Figure 4.1.

Each person receives their beam and splits it through the use of a 50:50 beam splitter, then employs Heterodyne detection (double homodyne) in order to perform an approximation of simultaneous measurements of the x and p quadratures as shown in Figure 4.2. Additional splitting is needed as the $\hat{x}$ and $\hat{p}$ operators do not commute, and therefore cannot be measured on a single beam. This method of measurement has been employed in other QKD protocols with success [30, 31].

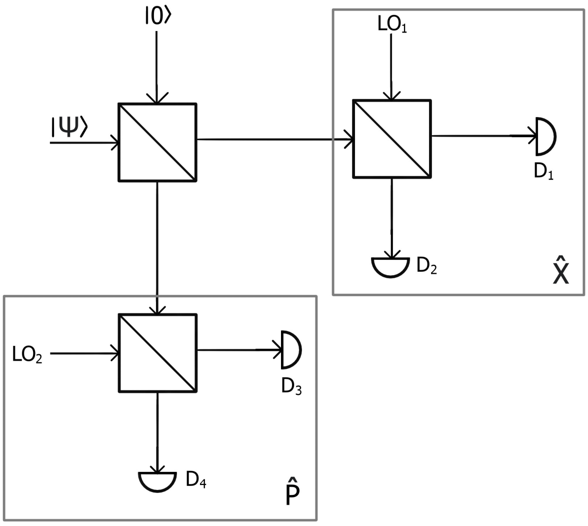


Figure 4.2: **Heterodyne Detection.** The measurement method used in the thermal protocol, in which the incoming beam is split at a 50:50 beam splitter in order to measure the x and p quadratures separately.

After repeatedly measuring quadratures and finding a series of measurement pairs x_i, p_i, each person calculates the Amplitude $z_i = \sqrt{x_i^2 + p_i^2}$ for each pair. The data is converted into bit strings through each person calculating their median z_i values, and recording a binary 0 or 1 for each z_i measurement above or below the median, respectively. As the outputs of a beam splitter with a thermal input are correlated, bit strings derived from measurements of these outputs are likewise correlated. In order to verify this, Alice and Bob may compare results for a subset of measurements. If the results are uncorrelated, Alice and Bob may stop and restart key distribution. A sample of this is shown in Figure 4.3, where any time delay between Alice and Bob's measurements removes all correlation between their amplitude strings, confirming that the original source was thermal.

While these simulations do not account for extra noise added by detectors, this still allows for a method of verifying that a noisy thermal source is responsible for the received measurements rather than detector noise. Even using identical equipment, noise introduced by each party's detectors would have no reason to be correlated. Analysing offsets in real bit strings in a similar manner would also show that Alice and Bob only receive highly correlated amplitudes when they measure the signal from their source at the same time, rather than their results being dominated by the effects of their receivers.

Monte Carlo simulations in Python were used to model the outputs of the protocol, with assistance from QuTiP [32, 33]. As expected, the simulated thermal state gave rise to correlated amplitude measurements by Alice, Bob and Eve. Once each bit string has been derived as described above, we can calculate mutual information to test if the protocol has produced suitable bit strings for key distillation.

4.2 Key distillation

Once each person has their bit string, there are multiple methods of producing a key, depending on the mutual information between each pair of people. Alice and Bob can glean some information about the system through discussion and comparison of parts of their bit strings, provided that any revealed information is discarded.

There are four main relevant concepts.

- Direct reconciliation
- Reverse reconciliation
- Advantage distillation
- Privacy amplification

In direct reconciliation, Alice provides additional information to Bob in order to correct mistakes. As with the initial broadcast, it is assumed Eve has access to communications used to fix errors, allowing both Bob and Eve to act on any information provided by Alice.

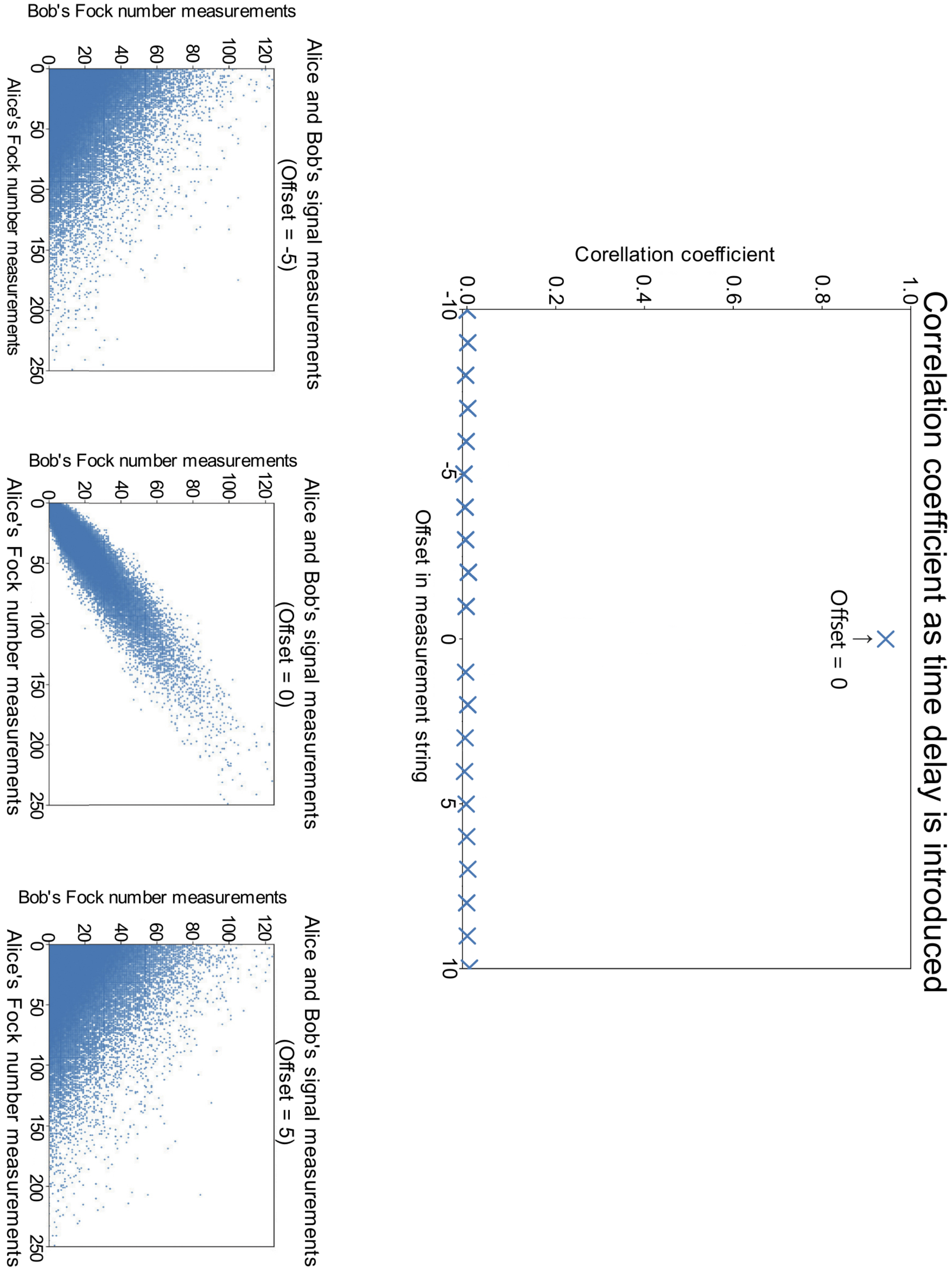


Figure 4.3: **Changes in correlation coefficients.** The effects of time delays on the correlation coefficients of measurement strings using a simulated thermal state ($\hat{n} = 50$). Any time delay produces uncorrelated results, which are clearly visible in the accompanying scatter graphs. This was originally presented in [1].

In order to successfully create a key despite Eve, the original bit strings shared by each party will have varying restrictions. Methods for correcting such errors, such as Cascade, are already known and applied in similar protocols [34]. In this, Alice and Bob reorder their bit strings to an agreed-upon random permutation and divide the new strings into groups with size depending on the estimated error rate. These groups have their parities compared, and if discrepancies are noticed, the groups are spilt further and the check repeated, until an error is found and corrected in Bob's string. Fixing such an error leads to other errors being identified in other groups containing the changed bit due to changes in parity values, allowing additional fixes to the bit string. This process is repeated with more random permutations of the bit string until there is confidence that no errors remain.

In order for this to be successful, Alice and Bob require [35] $H\left(A;B\right) > H\left(A;E\right)$. A clear problem presents itself here however. If Eve intercepts with a 50:50 beam splitter, we would expect $H\left(A;B\right) = H\left(A;E\right)$ due to the symmetry in the protocol setup, with $H\left(A;B\right) < H\left(A;E\right)$ if Eve siphons off more than half of the beam intended for Bob. As Eve is in control of the intercepting beam splitter, this is not an acceptable method of producing a key alone. This is an expected result and is a regular problem with this method of reconciliation.

This process can be inverted, giving reverse reconciliation. Here, Alice instead corrects errors within their bit string instead of Bob, though the reconciliation protocol is otherwise unchanged. To create a key, this requires [35] $H\left(A;B\right) > H\left(B;E\right)$. We will see later that this requirement is attainable using the thermal protocol.

If neither of these methods are available due to Alice and Bob both having higher mutual information with Eve than with each other, advantage distillation is used to give Alice and Bob the superior channel. Methods for this can involve broadcasting code words created from Alice's string, or sharing parity of pairs of bits, and discarding both bits in the case of errors or one element of the pairs when they agree. This only requires $H\left(A;B|E\right) > 0$, and will result in Alice and

Bob's bit strings becoming less correlated with Eve. Finally, privacy amplification is employed. This step takes the key Alice and Bob have created and produces a smaller key, which Eve does not have knowledge of. One possibility for this involves the use of hash functions, which map Alice and Bob's bit strings to their final string. If implemented correctly, any errors between Eve and the legitimate parties at this point will result in Eve having no knowledge of the final key.

From this, we can restrict the boundaries for the key rate K to [36]:

$$H\left(A;B|E\right) \geq K \geq \max\left[H\left(A;B\right) - H\left(A;E\right), H\left(A;B\right) - \left(B;E\right)\right] \tag{4.1}$$

4.3 Shannon entropy measurements

After the simulations are performed, we compare the produced bit strings in order to calculate mutual information between each pair of people, as well as the conditional mutual information. With this, we check if the bit strings are appropriate for conversion into keys by testing if the inequalities in Subsection 4.2 are satisfied.

Additionally, to consider varying levels in interception strength, these initial simulations compared the mutual information values as the transmittance of Eve's beam splitter was adjusted, with the results presented in Figure 4.4.

As expected, $H\left(A;B\right) > H\left(A;E\right)$ is not satisfied if Eve reflects over half of the beam sent to Bob, with equality for a 50:50 beam splitter, therefore, direct reconciliation is not a reliable method for producing a key. However, $H\left(A;B\right) > H\left(B;E\right)$ remains true as long as Bob receives any portion of the beam sent to them, allowing reverse reconciliation as a key distillation method.

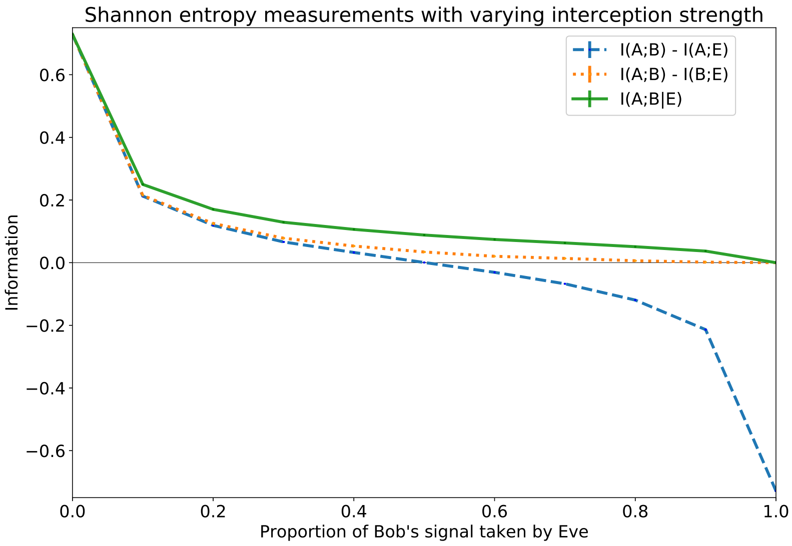


Figure 4.4: **Mutual informations with varying transmittance.** The effects of changing the transmittance of Eve's beam splitter on the mutual information values. This was originally presented in [1].

To confirm these results, we analyse the covariance matrices to calculate von Neumann mutual informations. Fulfilling the above inequalities with von Neumann entropies allows for protection against a wider range of attacks than when only Shannon entropy is considered.

4.4 Von Neumann entropy measurements

We begin with the covariance matrix for a thermal state, γ_0, and a vacuum state, γ_1, as mentioned in Section 2.6:

$$\gamma_0 = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix}. \tag{4.2}$$

$$\gamma_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{4.3}$$

At the initial beam splitter, we have the thermal source and a vacuum source as the two inputs, which have no dependency on each other. This gives the two-mode covariance matrix:

$$\gamma_{01} = \begin{bmatrix} V & 0 & 0 & 0 \\ 0 & V & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.4}$$

To find the final covariance matrix, we apply the transformation for a beam splitter with transmittance and reflectance T and R,

$$B\left(T,R\right) = \begin{bmatrix} T & R \\ R & T \end{bmatrix} \otimes I_{2\times 2}, \tag{4.5}$$

to the appropriate modes, introducing new vacuum modes at the beam splitters as necessary. At the end of the protocol, this gives the final covariance matrix:

$$\gamma_{A_1A_2B_1B_2E_1E_2} = \begin{bmatrix} \gamma_{A_1A_2} & C_{AB} & C_{AE} \\ C_{AB}^T & \gamma_{B_1B_2} & C_{BE} \\ C_{AE}^T & C_{BE}^T & \gamma_{E_1E_2} \end{bmatrix}, \tag{4.6}$$

with sub-matrices given by:

$$\gamma_{A_1A_2} = \frac{1}{4}\begin{bmatrix} (V+3) & -(V-1) \\ -(V-1) & (V+3) \end{bmatrix} \otimes I, \tag{4.7}$$

$$\gamma_{B_1B_2} = \frac{1}{4}\begin{bmatrix} T^2\left(V+1\right)+2\left(1+R^2\right) & -T^2\left(V+1\right)+2\left(1-R^2\right) \\ -T^2\left(V+1\right)+2\left(1-R^2\right) & T^2\left(V+1\right)+2\left(1+R^2\right) \end{bmatrix} \otimes I, \tag{4.8}$$

$$\gamma_{E_1E_2} = \frac{1}{4}\begin{bmatrix} R^2\left(V+1\right)+2\left(1+T^2\right) & -R^2\left(V+1\right)+2\left(1-T^2\right) \\ -R^2\left(V+1\right)+2\left(1-T^2\right) & R^2\left(V+1\right)+2\left(1+T^2\right). \end{bmatrix} \otimes I, \tag{4.9}$$

$$C_{AB} = \frac{T}{4}\begin{bmatrix} (1-V) & -(1-V) \\ -(1-V) & (1-V) \end{bmatrix} \otimes I, \tag{4.10}$$

$$C_{AE} = \frac{R}{4}\begin{bmatrix} -(1-V) & (1-V) \\ (1-V) & -(1-V) \end{bmatrix} \otimes I, \tag{4.11}$$

$$C_{BE} = \frac{TR}{4}\begin{bmatrix} -(V-1) & (V-1) \\ (V-1) & -(V-1) \end{bmatrix} \otimes I. \tag{4.12}$$

Given a covariance matrix γ, the von Neumann entropy is given by [37]

$$S(\gamma) = \sum_{i=0} G\left(\frac{\lambda_i - 1}{2}\right). \tag{4.13}$$

Where λ_i are the symplectic eigenvalues, and

$$G(\lambda) = (\lambda + 1)\log_2(\lambda + 1) - \lambda \log_2 \lambda. \tag{4.14}$$

From this, we can calculate the mutual information, and conditional mutual information. Previously, we compared Shannon mutual information using results from simulations in Figure 4.4. We replicate by using covariance matrix calculations to compare von Neumann mutual information in a similar fashion, with the results plotted in Figure 4.5.

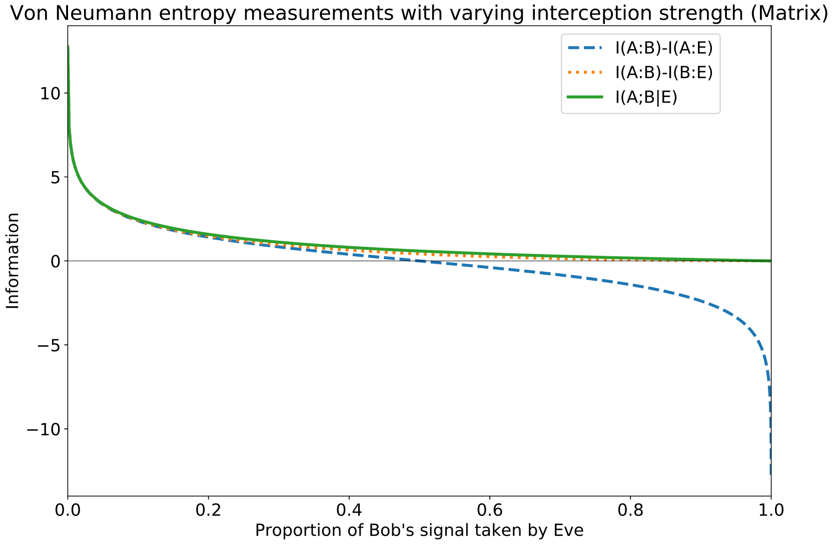


Figure 4.5: **Von Neumann entropy** The effects of varying transmittance of Eve's intercepting beam splitter on von Neumann entropy. This was originally presented in [1].

We see from Figures 4.4 and 4.5 that both methods produce curves with similar behaviour. The von Neumann entropy is of greater magnitude than Shannon; however, this is expected due to discord in the system, which the Shannon entropy does not take into account. As with the simulation, we see that direct reconciliation fails when Eve siphons off 50% or more of Bob's beam, however reverse reconciliation is always available as a possibility.

From this, we have shown that an unmodulated thermal state can be used to produce a usable key for distribution between Alice and Bob. Though as this is only initial theoretical work, further considerations will be needed before we can confirm that this is a viable method. First, we cannot assume that these results transfer over to the modulated signals used in actual thermal broadcasts, and then we will need to confirm that the theory applies in practice with practical testing. The first of these will be explored in the following chapter.

Chapter 5

Introducing Displacement and loss

5.1 Displaced Thermal States

While we have shown that unmodulated thermal states can produce a key, thermal states are typically modulated as described in Section 2.10. In order to mimic the broadcasts typically performed by common microwave communication devices, we move towards analysing displaced thermal states in order to show that the theory analysis in the previous chapter still applies to realistic modulated states that are used in modern communication.

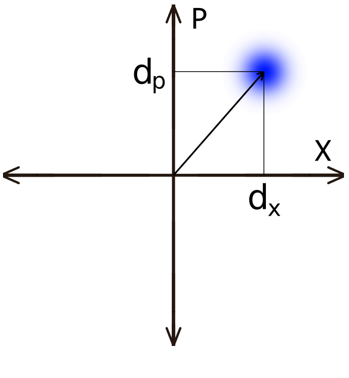


Figure 5.1: **A displaced thermal state.** The state $D^{\dagger}(\alpha)\,\rho_{Th}D(\alpha)$, with d_x and d_p as the quadrature expectation values.

Adjusting the previous covariance matrix analysis to account for displacement, the vector describing the displaced thermal state and the vacuum state entering the initial beam splitter is given by

$$\langle \hat{r} \rangle = \begin{bmatrix} d_x \\ d_p \\ v_{1x} \\ v_{1p} \end{bmatrix}. \tag{5.1}$$

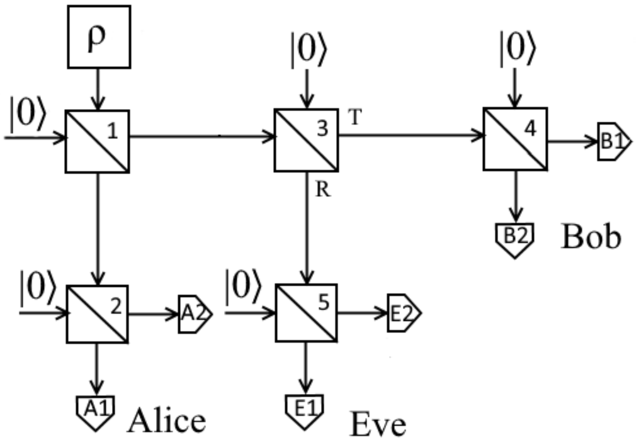


Figure 5.2: **Lossy protocol.** The thermal state protocol with beam splitters labelled for clarity. This was originally presented in [2].

Here, $d_x = \langle \hat{X} \rangle$ and $d_p = \langle \hat{P} \rangle$ describe the quadrature expectation values for the displaced thermal state, as shown in Figure 5.1, while v_{1x} and v_{1p} describe the input noise. Applying the beam splitters to relevant modes, as in Section 4.4, allows the final vector to be found. We model Alice's detector as a beam splitter with transmittance and reflectance t_a and r_a, and do the same for Bob and Eve. Taking v_{2x} through v_{5x} as the vacuum noise at the remaining beam splitters, as shown in Figure 5.2, gives:

$$\langle \hat{r} \rangle_x = \begin{bmatrix} \frac{t_a}{2}\left(d_x + v_{1x}\right) + \frac{t_a}{\sqrt{2}} v_{2x} + r_a v_{A_1} \\ -\frac{t_a}{2}\left(d_x + v_{1x}\right) + \frac{t_a}{\sqrt{2}} v_{2x} + r_a v_{A_2} \\ -\frac{Tt_b}{2}\left(d_x - v_{1x}\right) + \frac{Rt_b}{\sqrt{2}} v_{3x} + \frac{t_b}{\sqrt{2}} v_{4x} + r_b v_{B_1} \\ \frac{Tt_b}{2}\left(d_x - v_{1x}\right) - \frac{t_b R}{\sqrt{2}} v_{3x} + \frac{t_b}{\sqrt{2}} v_{4x} + r_b v_{B_2} \\ \frac{t_e R}{2}\left(d_x - v_{1x}\right) + \frac{Tt_e}{\sqrt{2}} v_{3x} + \frac{t_e}{\sqrt{2}} v_{5x} + r_e v_{E_1} \\ -\frac{t_e R}{2}\left(d_x - v_{1x}\right) - \frac{Tt_e}{\sqrt{2}} v_{3x} + \frac{t_e}{\sqrt{2}} v_{5x} + r_e v_{E_2} \end{bmatrix}, \tag{5.2}$$

with the P quadratures calculated in the same fashion. Taking the noise quadrature expectation values to have mean 0 and variance 1, and the thermal state having variance v, we find the final covariance matrix:

$$\gamma_{A_1A_2B_1B_2E_1E_2} = \begin{bmatrix} \gamma_{A_1A_2} & C_{AB} & C_{AE} \\ C_{AB}^T & \gamma_{B_1B_2} & C_{BE} \\ C_{AE}^T & C_{BE}^T & \gamma_{E_1E_2} \end{bmatrix}, \tag{5.3}$$

where the sub-matrices are given by:

$$\gamma_{A_1A_2} = \begin{bmatrix} \frac{t_a^2}{4}(v+3)+r_a^2 & \frac{t_a^2}{4}(1-v) \\ \frac{t_a^2}{4}(1-v) & \frac{t_a^2}{4}(v+3)+r_a^2 \end{bmatrix} \otimes I \tag{5.4}$$

$$\gamma_{B_1B_2} = \begin{bmatrix} \frac{T^2t_b^2}{4}(v+1)+\frac{t_b^2\left(r^2+1\right)}{2}+r_b^2 & -\frac{T^2t_b^2}{4}(v+1)+\frac{t_b^2\left(1-R^2\right)}{2} \\ -\frac{T^2t_b^2}{4}(v+1)+\frac{t_b^2\left(1-R^2\right)}{2} & \frac{T^2t_b^2}{4}(v+1)+\frac{t_b^2\left(R^2+1\right)}{2}+r_b^2 \end{bmatrix} \otimes I \tag{5.5}$$

$$\gamma_{E_1E_2} = \begin{bmatrix} \frac{t_e^2R^2}{4}(v+1)+\frac{t_e^2\left(T^2+1\right)}{2}+r_e^2 & -\frac{R^2t_e^2}{4}(v+1)+\frac{t_e^2\left(1-T^2\right)}{2} \\ -\frac{R^2t_e^2}{4}(v+1)+\frac{t_e^2\left(1-T^2\right)}{2} & \frac{t_e^2R^2}{4}(v+1)+\frac{t_e^2\left(T^2+1\right)}{2}+r_e^2 \end{bmatrix} \otimes I \tag{5.6}$$

$$C_{AB} = \frac{1}{4}\begin{bmatrix} Tt_at_b(1-v) & Tt_at_b(v-1) \\ Tt_at_b(v-1) & Tt_at_b(1-v) \end{bmatrix} \tag{5.7}$$

$$C_{AE} = \frac{1}{4}\begin{bmatrix} Rt_at_e(v-1) & Rt_at_e(1-v) \\ Rt_at_e(1-v) & Rt_at_e(v-1) \end{bmatrix} \tag{5.8}$$

$$C_{BE} = \frac{1}{4}\begin{bmatrix} TRt_bt_e(1-v) & TRt_bt_e(v-1) \\ TRt_bt_e(v-1) & TRt_bt_e(1-v) \end{bmatrix} \tag{5.9}$$

From Section 4.4, it was noted that von Neumann mutual information can be calculated using elements of the covariance matrix. As the final matrix depends only on the variance, rather than displacement, we deduce from this that displacement also does not affect mutual information. Therefore displaced thermal states, such as those already commonly used in current communication devices, may be usable in QKD through this protocol. While this result may appear unsurprising, verifying this with a more focused analysis was needed to avoid assuming that results for unmodulated states could apply to realistic broadcast states.

5.2 Loss

One of the factors inhibiting the use of thermal states in QKD is the loss at the detectors, or during broadcast. With the covariance matrix from Section 5.1, beam splitters were added to account for detector loss. We use these to calculate the effects of loss on the mutual information. We factor in loss for three cases:

- Loss on Alice's channel. Due to Alice having control over the source, their detector, and the channel between them, it is possible to limit this through a wired connection.
- Loss on Bob's channel, after Eve intercepts.
- Loss on Bob's channel, before Eve can intercept. This is the most relevant scenario for wireless scenarios as Alice's broadcasts may be omnidirectional, in which case most of a broadcast would be lost before any interception takes place.

In each of these scenarios, we maintain the assumption that the channel between Eve's beam splitter and their detectors has no loss. Despite this, Eve is still impacted by loss on Bob's channel before the interception. This assumption is in place to give Eve the most favourable circumstances for interception, to avoid overstating the capabilities of the protocol by unnecessarily reducing an attacker's efficiency without justification.

We use the covariance matrices from Section 5.1 to plot the effects of loss. Beginning with Figure 5.3, we see that loss in Alice's channel quickly results in Eve's

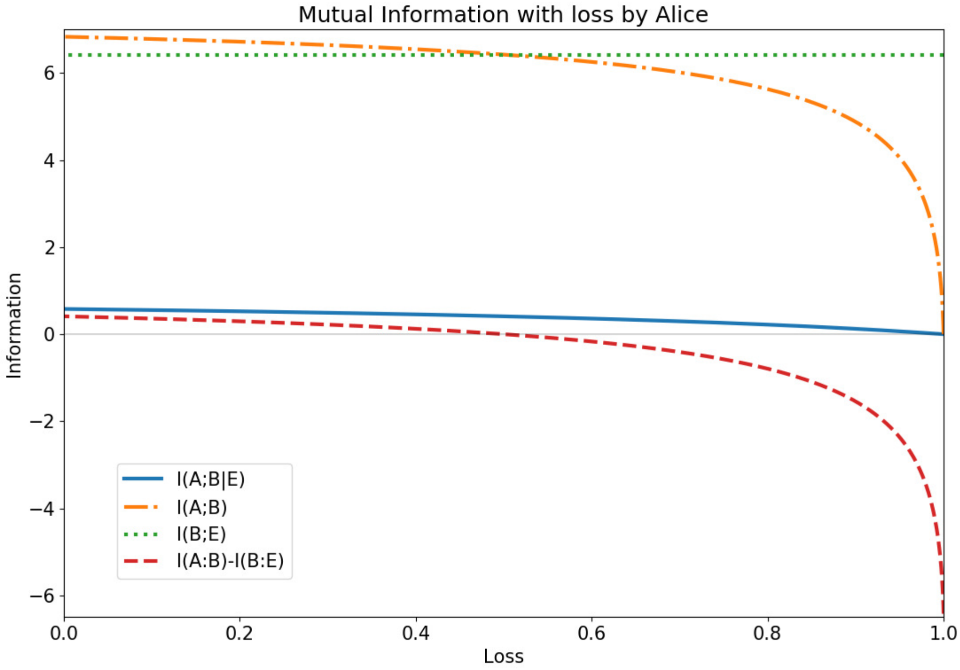


Figure 5.3: **Loss by Alice.** Changes in mutual information as loss is introduced on Alice's channel. This was originally presented in [2].

channel being superior. Due to this, effort should be made to reduce loss before Alice can perform measurement. Alice's access to the source can be used to accomplish this. Ideally, even for wireless communications between Alice and Bob, this segment of the protocol could still be carried out with a wired setup to avoid this becoming a problem. This reduction in key rate with increased loss by Alice is therefore unlikely to cause issues in an appropriately set up protocol.

Next, loss is simulated on Bob's channel, after Eve intercepts. This is shown in Figure 5.4 Unlike in the previous test, Alice and Bob maintain the superior channel provided Bob receives any of the signal sent to them. This is a similar result to the no-loss version, with the main distinction being that loss before Bob can measure was previously attributed to Eve intercepting, rather than channel loss.

While with Alice, loss could be minimised through their full control of the source, their detector, and the channel between them, Bob has no such ability, especially should there be a free space channel between Alice and Bob. Given Bob's inability to restrict loss in the same way as Alice, it is important that the protocol still functions with a perfect Eve despite loss in this segment of the protocol.

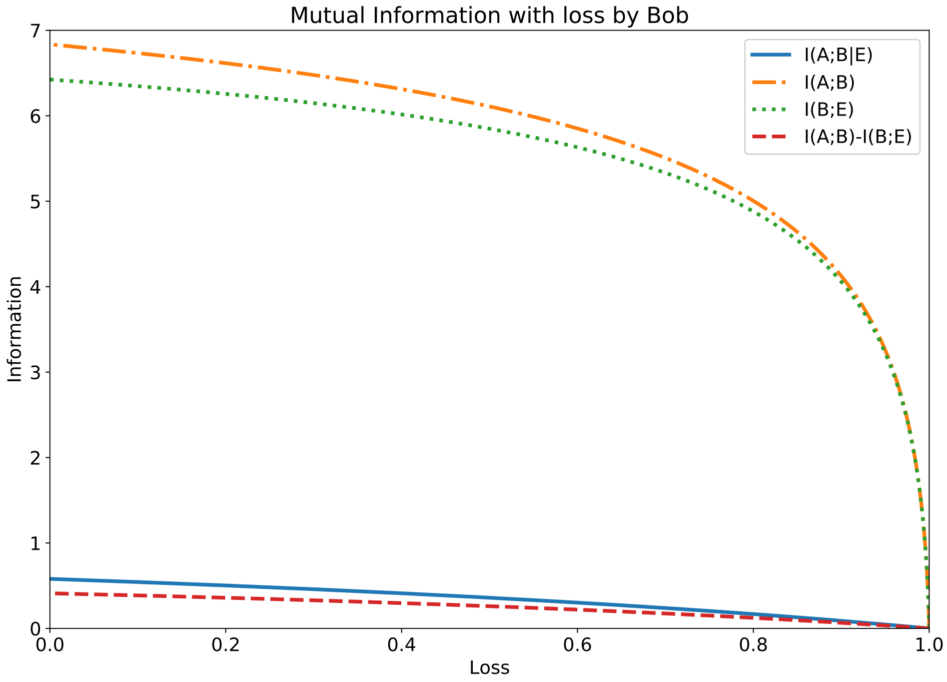


Figure 5.4: **Loss by Bob.** Changes in mutual information as loss is introduced on Bob's channel, after interception. This was originally presented in [2].

Finally, we consider loss on Bob's channel before Eve can intercept. Up until this point, the protocol has been biased unfairly in favour of Eve to avoid potentially understating their capabilities. However, in a realistic wireless scenario, Eve has no way of detecting all of the signal which is not detected by Alice and Bob.

For an omnidirectional broadcast from the initial splitter, such a setup would require Eve to have a detector covering all directions except for where Alice and Bob's detectors are located, which is not a feasible setup. Therefore, large amounts of loss before Eve can intercept is a realistic scenario. In this variant, we likewise see that Alice and Bob continue to have the superior channel as shown in Figure 5.5.

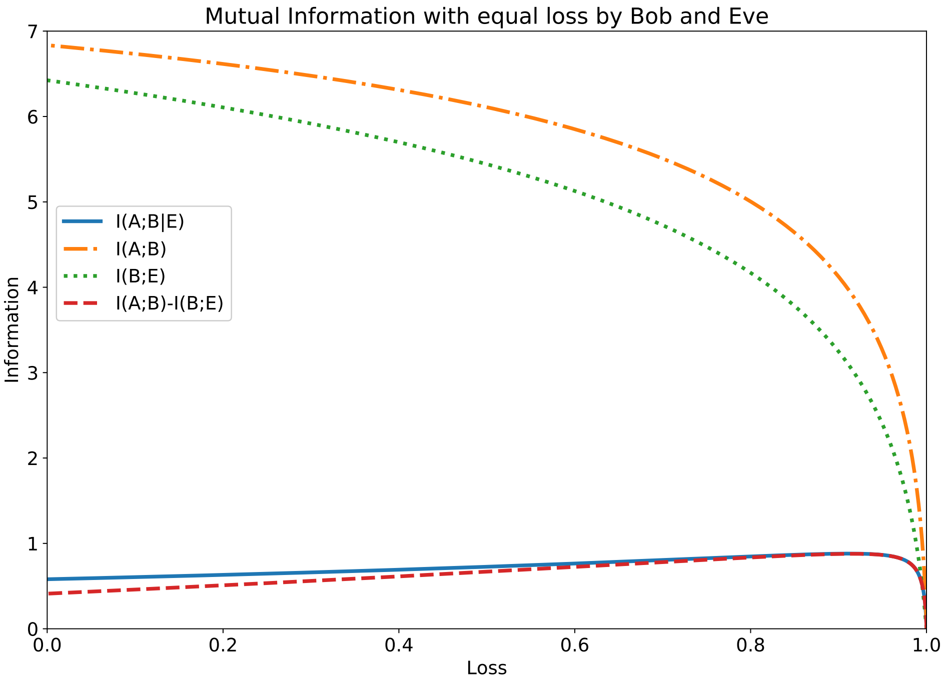


Figure 5.5: **Loss before interception.** Loss on Bob's channel, before Eve is able to intercept. This was originally presented in [2].

To verify this behaviour, we repeat the same scenarios using the Monte Carlo simulations from Section 4.3, calculating Shannon entropy from bit strings. In all cases, Shannon entropy follows the same trend as von Neumann entropies calculated through covariance, as shown in Figure 5.6. Again, von Neumann entropy exceeds Shannon due to presence of discord in the system, which is not accounted for in a classical analysis.

At this point, the thermal state protocol proves able to distribute appropriate bit strings for displaced states in theory, including with realistic loss scenarios. Knowing this, we now proceed to experimental tests of the protocol for both wired, and short range wireless setups.

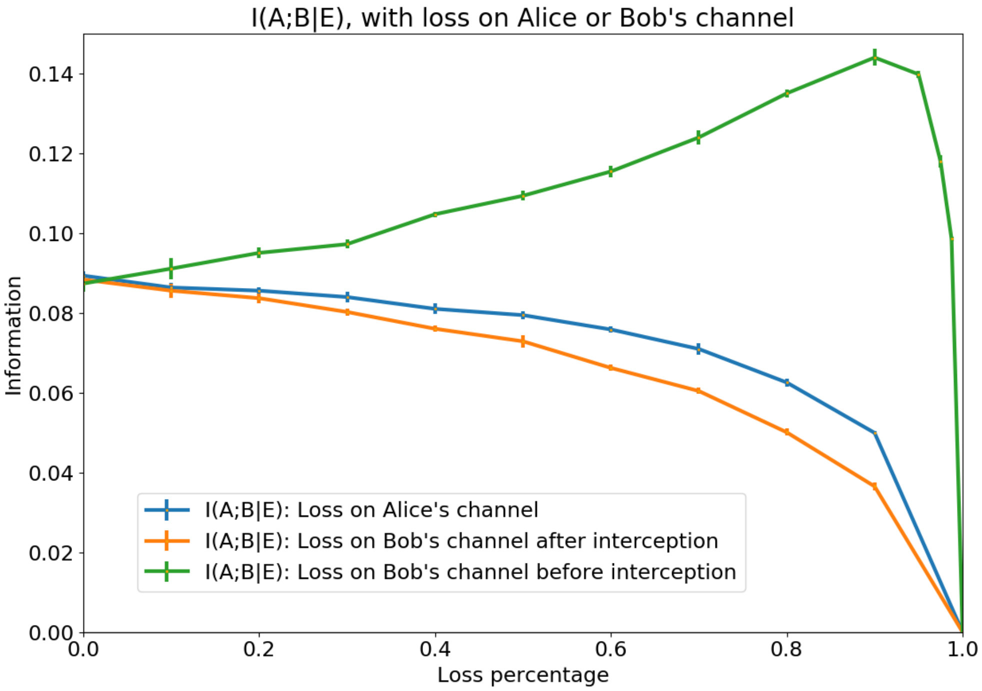


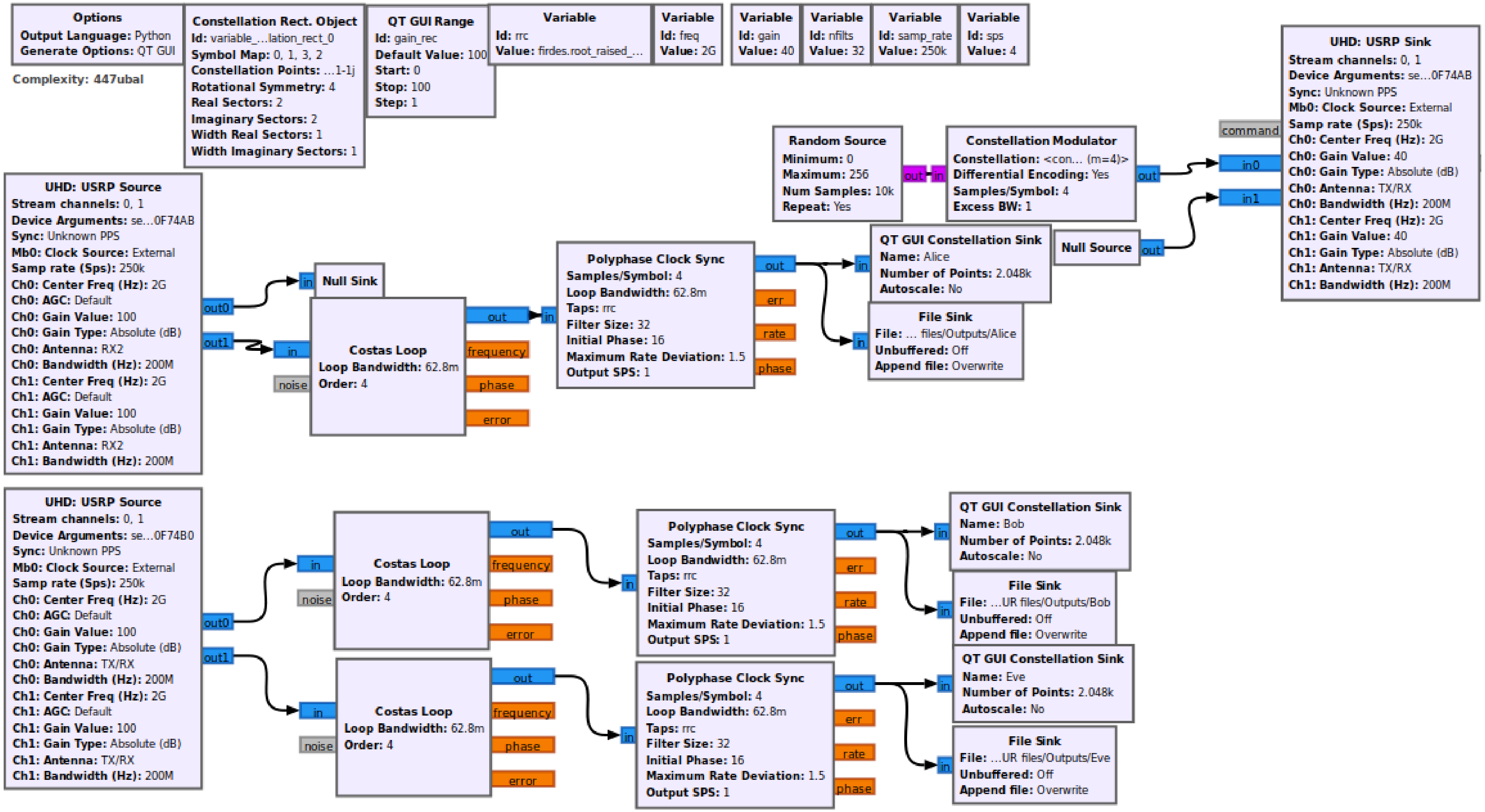
Figure 5.6: **Loss simulations.** The results of Monte Carlo simulations. This was originally presented in [2].

Chapter 6

Performing Key Distribution with Microwave Sources

6.1 Wired Key Distribution

In order to carry out the protocol experimentally we use GNURadio for signal processing, building the flowchart shown in Figure 6.1. A pair of USRP-2901's are used as the radio transceivers, while Costas loops and Polyphase block sync blocks synchronise the timing and phase of the signals. These are commonly used elements in radio broadcasting protocols designed to ensure that different parties involved in communication measure at the appropriate times to recover the intended information from the broadcast, and help radio communications function in uncontrolled environments. Costas loops recover the initial carrier wave from a broadcast, while polyphase blocks ensure that the measurements of the received signals are performed at the correct time.



Options
Output Language: Python
Generate Options: QT GUI
Complexity: 447ubal

Constellation Rect. Object
Id: variable_...lation_rect_0
Symbol Map: 0, 1, 3, 2
Constellation Points: ...1-1j
Rotational Symmetry: 4
Real Sectors: 2
Imaginary Sectors: 2
Width Real Sectors: 1
Width Imaginary Sectors: 1

QT GUI Range
Id: gain_rec
Default Value: 100
Start: 0
Stop: 100
Step: 1

Variable
Id: rrc
Value: firdes.root_raised_...

Variable
Id: freq
Value: 2G

Variable
Id: gain
Value: 40

Variable
Id: nfilts
Value: 32

Variable
Id: samp_rate
Value: 250k

Variable
Id: sps
Value: 4

Random Source
Minimum: 0
Maximum: 256
Num Samples: 10k
Repeat: Yes

Constellation Modulator
Constellation: <con... (m=4)>
Differential Encoding: Yes
Samples/Symbol: 4
Excess BW: 1

Null Source

UHD: USRP Sink
Stream channels: 0, 1
Device Arguments: se...0F74AB
Sync: Unknown PPS
Mb0: Clock Source: External
Samp rate (Sps): 250k
Ch0: Center Freq (Hz): 2G
Ch0: Gain Value: 40
Ch0: Gain Type: Absolute (dB)
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 200M
Ch1: Center Freq (Hz): 2G
Ch1: Gain Value: 40
Ch1: Gain Type: Absolute (dB)
Ch1: Antenna: TX/RX
Ch1: Bandwidth (Hz): 200M

UHD: USRP Source
Stream channels: 0, 1
Device Arguments: se...0F74AB
Sync: Unknown PPS
Mb0: Clock Source: External
Samp rate (Sps): 250k
Ch0: Center Freq (Hz): 2G
Ch0: AGC: Default
Ch0: Gain Value: 100
Ch0: Gain Type: Absolute (dB)
Ch0: Antenna: RX2
Ch0: Bandwidth (Hz): 200M
Ch1: Center Freq (Hz): 2G
Ch1: AGC: Default
Ch1: Gain Value: 100
Ch1: Gain Type: Absolute (dB)
Ch1: Antenna: RX2
Ch1: Bandwidth (Hz): 200M

Null Sink

Costas Loop
Loop Bandwidth: 62.8m
Order: 4

Polyphase Clock Sync
Samples/Symbol: 4
Loop Bandwidth: 62.8m
Taps: rrc
Filter Size: 32
Initial Phase: 16
Maximum Rate Deviation: 1.5
Output SPS: 1

QT GUI Constellation Sink
Name: Alice
Number of Points: 2.048k
Autoscale: No

File Sink
File: ... files/Outputs/Alice
Unbuffered: Off
Append file: Overwrite

UHD: USRP Source
Stream channels: 0, 1
Device Arguments: se...0F74B0
Sync: Unknown PPS
Mb0: Clock Source: External
Samp rate (Sps): 250k
Ch0: Center Freq (Hz): 2G
Ch0: AGC: Default
Ch0: Gain Value: 100
Ch0: Gain Type: Absolute (dB)
Ch0: Antenna: TX/RX
Ch0: Bandwidth (Hz): 200M
Ch1: Center Freq (Hz): 2G
Ch1: AGC: Default
Ch1: Gain Value: 100
Ch1: Gain Type: Absolute (dB)
Ch1: Antenna: TX/RX
Ch1: Bandwidth (Hz): 200M

Costas Loop
Loop Bandwidth: 62.8m
Order: 4

Polyphase Clock Sync
Samples/Symbol: 4
Loop Bandwidth: 62.8m
Taps: rrc
Filter Size: 32
Initial Phase: 16
Maximum Rate Deviation: 1.5
Output SPS: 1

QT GUI Constellation Sink
Name: Bob
Number of Points: 2.048k
Autoscale: No

File Sink
File: ...UR files/Outputs/Bob
Unbuffered: Off
Append file: Overwrite

Costas Loop
Loop Bandwidth: 62.8m
Order: 4

Polyphase Clock Sync
Samples/Symbol: 4
Loop Bandwidth: 62.8m
Taps: rrc
Filter Size: 32
Initial Phase: 16
Maximum Rate Deviation: 1.5
Output SPS: 1

QT GUI Constellation Sink
Name: Eve
Number of Points: 2.048k
Autoscale: No

File Sink
File: ...UR files/Outputs/Eve
Unbuffered: Off
Append file: Overwrite

Figure 6.1: **GNURadio.** The protocol as performed on GNURadio.

A constellation modulator divides a random thermal source into four clusters, giving a distribution matching those shown in the descriptions of QAM and QPSK in Section 2.10. A snapshot of measurements forming the clusters is shown in Figure 6.2. For a wired broadcast, a pair of power splitters direct the signal first between Alice and the broadcast channel, and then from the broadcast channel to Bob and Eve, producing a series of quadrature pair measurements for each person. This allows for calculation of amplitudes as previously described during the theory analysis.

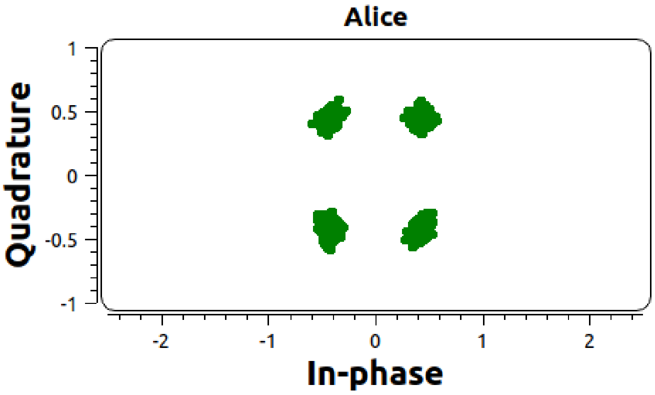


Figure 6.2: **Thermal state clusters.** Four thermal states produced through GNURadio, mirroring the broadcasts used in QPSK. This was originally displayed in [3].

As with the simulations, the amplitude measurements are used to produce correlated bit strings, which will be tested to verify their utility for key distillation. From Figure 6.3, we can see while there is additional noise, correlated measurements are produced, giving similarly correlated bit strings. Meanwhile, we see almost perfect correlation between Bob and Eve in Figure 6.4. This initial testing led to the conclusion that key rates produced through this method are commonly low enough that advantage distillation is required for key production. Repeated testing confirmed that, with the specific experimental setup, we were not able to consistently produce appropriate strings due to Eve's high correlation with Bob. Before performing a more detailed analysis, we first consider the methods available to reduce Eve's performance without impacting the assumptions of the experiment.

While it is still possible to produce keys through this method, the simulations of loss in the previous section suggested that the key rate can be improved by the addition of loss before Bob and Eve can measure. A straightforward way of achieving this is to switch to wireless broadcasting. As the majority of the broadcast signal will not be detected by both Bob and Eve combined, especially if omnidirectional antennae are used, we have a simple way to perform the protocol with loss.

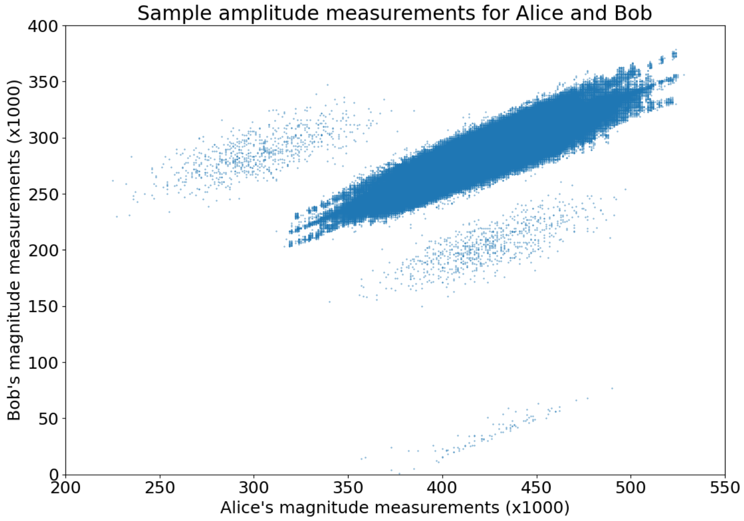


Figure 6.3: **Alice and Bob's wired results.** A scatter graph plotting a set ($n \approx 3000000$) of Alice and Bob's measurement pairs, clearly showing the expected correlations. As we are only concerned with relative measurements, these are presented unitless. This was originally displayed in [3].

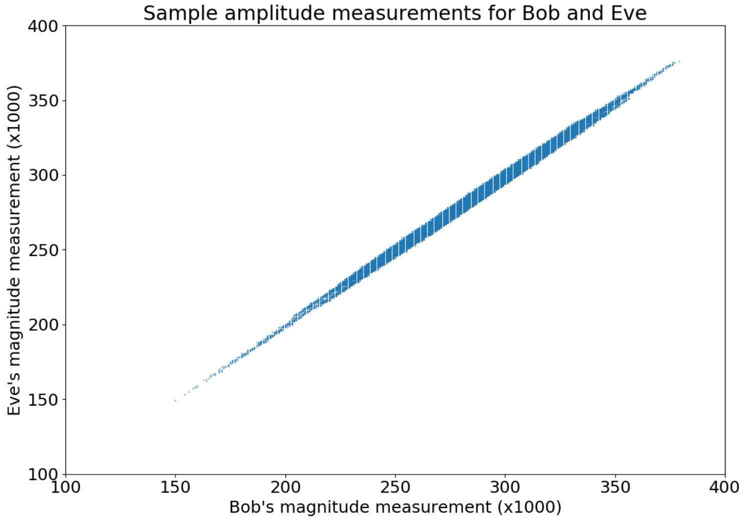


Figure 6.4: **Bob and Eve's wired results.** A scatter graph plotting a set ($n \approx 3000000$) of Bob and Eve's measurement pairs, clearly showing the expected correlations. This was originally displayed in [3].

6.2 Wireless Thermal Key Distribution

Having shown that wired thermal key distribution is possible, we adjust the protocol so that Bob and Eve will receive signals wirelessly, as shown in Figure 6.5. The thermal source retains its wired connection to the initial power splitter, which also is still connected by a wire to Alice. However, the wired channel leading to Bob has been replaced with wireless antennae. This requires Eve alter the method of interception, and causes loss before Eve can measure. This gives a wireless protocol that still maintains our assumptions of Alice having control over the source and the channel up until their own detector.

With a large amount of loss introduced that lies outside of Eve's control, Eve's performance is substantially reduced compared to the wired setup, in which all loss before Bob's measurement was attributed to Eve's interception. As previously mentioned in Section 5.2, this loss is due to the lack of any realistic way for Eve to set up a detector capable of detecting all of the broadcast from an omnidirectional antenna that is not detected by Alice or Bob.

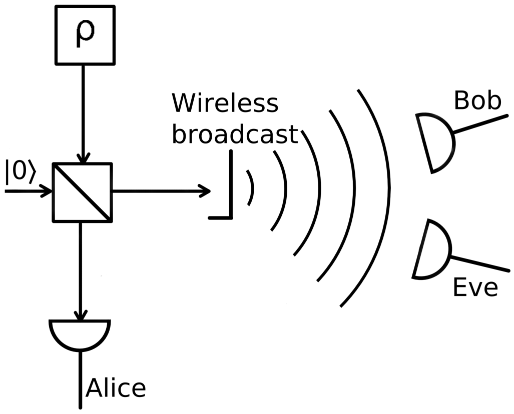


Figure 6.5: **Wireless Key Distribution.** A modified version of the thermal key distribution protocol in which Bob and Eve use wireless receivers. This was originally displayed in [3].

To test this version of the protocol, Bob and Eve were separated from the wireless source by a distance of one metre. From Figures 6.6 - 6.8, it can be seen that Bob and Eve's near-perfect correlation in the wired setup has been severely reduced by the increased loss introduced by the change to a wireless protocol. Despite the lack of error correction code beyond synchronising Alice and Bob's measurement strings, correlated strings suitable for key generation were able to be created over free space in a majority of tests. Given that this is performed using microwave equipment with open-source software, this would suggest that this setup could provide a reasonable, accessible method of performing key distribution inspired by quantum methods without requiring specialist equipment.

While repeated testing did show that the protocol was now more likely than not to produce keys which met the necessary condition of $I(A;B) - I(B;E) > 0$, with the differences between mutual informations given by: $\bar{x} = 0.08157$, $\sigma = 0.06062$, further improvements are still necessary for greater consistency. As in the theory, we do not consider $I(A;B) - I(A;E)$ due to the symmetry in the protocol still being maintained. In order to continue developing this protocol, two immediate areas for improvement are clear.

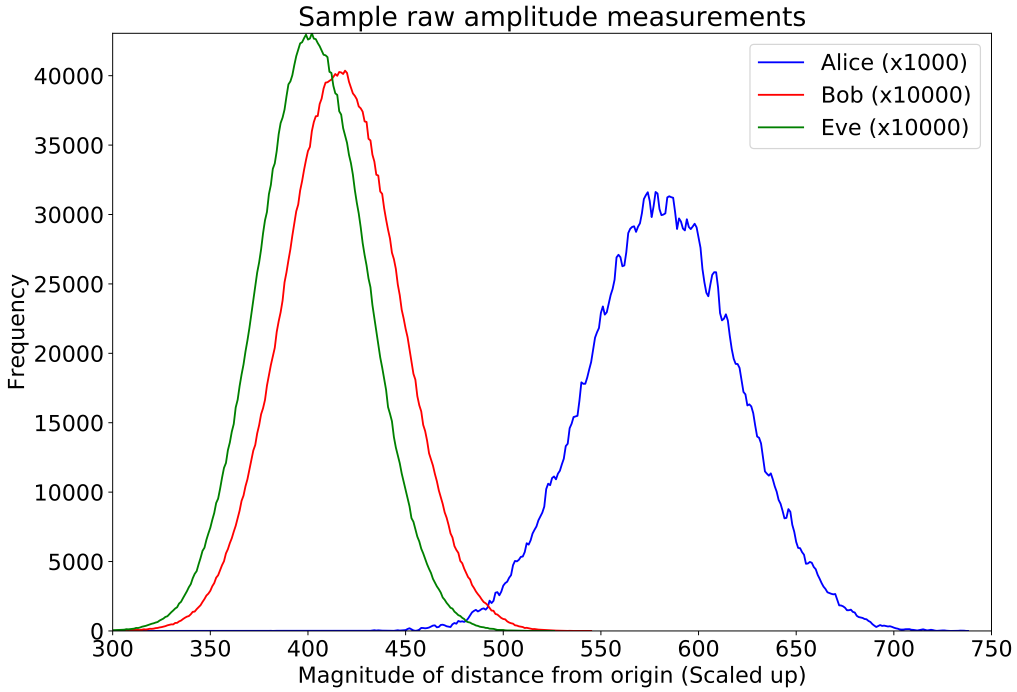


Figure 6.6: **Thermal state amplitude measurements.** A histogram displaying the results of a series of wireless measurements performed over a distance of one meter. This was originally displayed in [3].

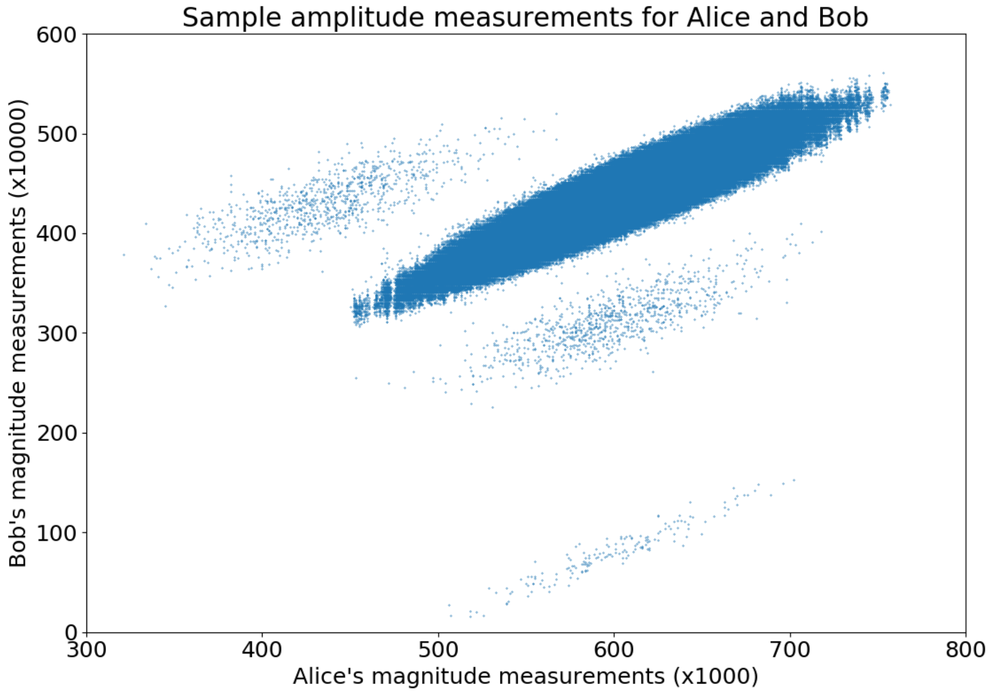


Figure 6.7: **Alice and Bob's wireless results.** A sample set of amplitude measurements produced in one of the wireless tests. What appear to be faint copies of the distribution showing in different locations in the plot are caused by multipath propagation – reflected signals taking different routes to the detector. This was originally displayed in [3]

First, general upgrades to the radios and antennae used in the experiment will allow the broadcast distance to be increased, and reduce the number of attempts needed for successful key exchange. In many cases, errors interrupting key exchange were caused by either a loss of the broadcast or a mistake in timing causing parties to perform measurements at the wrong time, losing correlation and stopping the key exchange. Secondly, the current method does not involve any instance of error correction.

While these problems were not able to be addressed with the equipment and radio knowledge we had access to, these are both issues that need to be dealt with for any form of radio broadcast to function correctly, and we therefore do not foresee any challenges in addressing them which those knowledgeable in communications won't have already dealt with in other radio protocols.

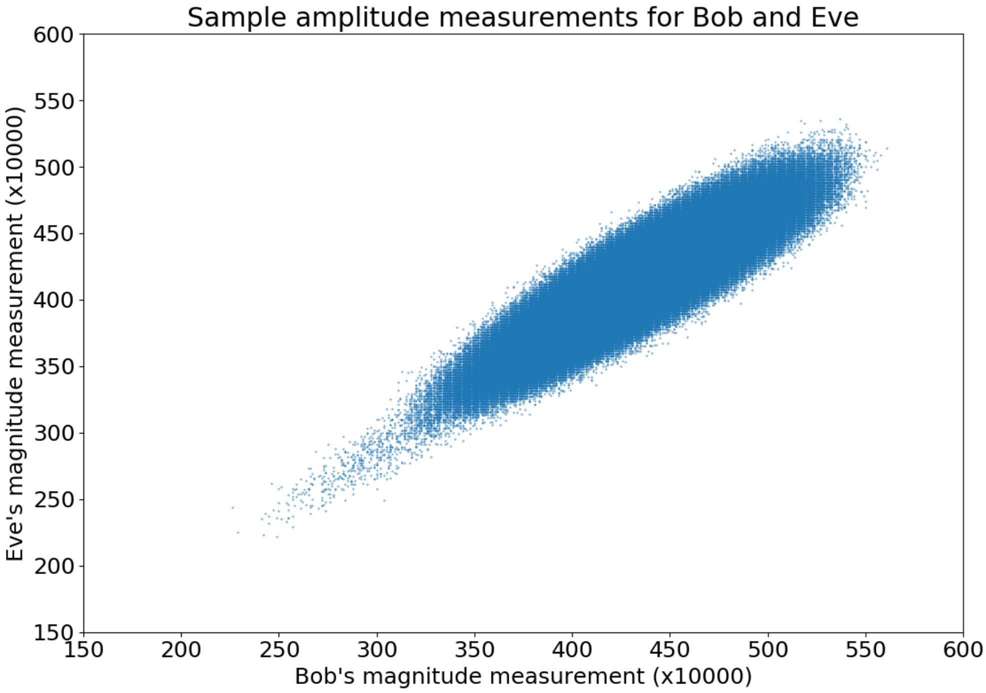


Figure 6.8: **Bob and Eve's wireless results.** A comparison of Bob and Eve's results from the same broadcast. This shows greatly reduced correlation compared to the near-perfect line shown in the wired test in Figure 6.4. This was originally displayed in [3].

With evidence gathered showing the protocol working over short ranges with basic equipment, we conclude this portion of the research. Further work ideally requires support from a group more familiar with radio broadcasting in order to test with superior equipment and error correction that would be available in realistic broadcast scenarios. Given the simplicity of the setup, however, if an appropriate array of equipment were provided then a larger-scale implementation of the protocol could be assembled using the same software. Even with only the basic equipment currently in use however, we have demonstrated an avenue for providing security associated with QKD, without the requirement for specialist equipment.

At this point, we instead consider additional applications of the observations we have made throughout this testing, while still only relying on equipment we currently have access to. In the second part of this writing, we will analyse an effect which was previously considered a broadcast problem to be fixed. Errors in timing caused by using separate imperfect clocks as time references for different radios are typically corrected by software during processing in order to maintain an accurate broadcast. Without such corrections, timing errors will gradually accumulate and result in the broadcast failing due to incorrect measurements by the parties involved.

Instead of fixing this error as is typically required in broadcasting, we will instead consider if the accumulating broadcast errors can be measured. Given that these errors are caused by frequency differences between the clocks being used as time references, it becomes reasonable to believe that measurements of such errors could allow for calculation of frequency differences between the clocks.

In the following section, we will see that analysis of the broadcasts we have been performing will not only allow for calculation of frequency differences between clocks, but will also allow for the correction of such differences to a surprisingly precise degree. This will provide a protocol for wireless frequency distribution using common radio equipment.

Chapter 7

Atomic Clock Phase Synchronisation

7.1 Introduction

In the practical demonstrations up to this point in the writing, a set of four clusters as seen in QPSK broadcasts are transmitted to Alice and Bob from a source separate from each of them. One of the steps required to perform this is to ensure that Alice and Bob first agree on the phase and frequency of the signals they were receiving. To do this, either both parties shared a 10 MHz reference signal from a single atomic clock, or a Costas loop was added to stabilise the phase when Alice and Bob used difference clocks as a reference.

When the experiment is set up this way, the measurements performed by Alice and Bob both form the four clusters that are expected in a QPSK protocol. With the stable frequency and phase ensured by either a shared clock or a Costas loop, these clusters remain centred at the same points in phase space over time. This allows the consistent performance of measurements without phase errors for the duration of a broadcast.

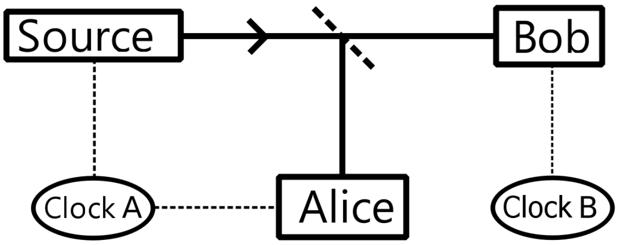


Figure 7.1: **Frequency Distribution.** A frequency comparison setup, in which Alice and a source share a primary clock, while Bob uses a secondary clock. Much like with the key distribution protocol, a signal from a source is split and sent to Alice and Bob for measurement.

Electronic signal processing compensates for differences in timing after a broadcast, though signal processing to recover an original broadcast does not interact with the original source for the timing, and therefore is not a method of clock synchronisation. However, by disabling the elements of signal processing designed to fix such timing errors, we found a new possibility for monitoring and correcting frequency errors.

By disabling these parts of the signal processing chain, the clusters received will not stay in place. If Alice and Bob use separate atomic clocks, as seen in Figure 7.1, any discrepancies in their reference frequencies causes the clusters to rotate, due to a mismatch in frequency manifesting as a change in phase over time. This is displayed in Figure 7.2, and is an unwanted source of error when attempting to analyse a broadcast. This error was observed when using separate clocks for Alice and Bob during initial testing of the key distribution protocol. However, a possible use of it was identified.

If a difference in frequency between reference signals from atomic clocks causes a phase error, leading to cluster rotation, then measurements of this rotation speed allow a difference in frequency to be measured. This would mean that microwave QPSK broadcasts can be used to synchronise two atomic clocks by adjusting the frequency of one clock in response to the errors until the rotation stops.

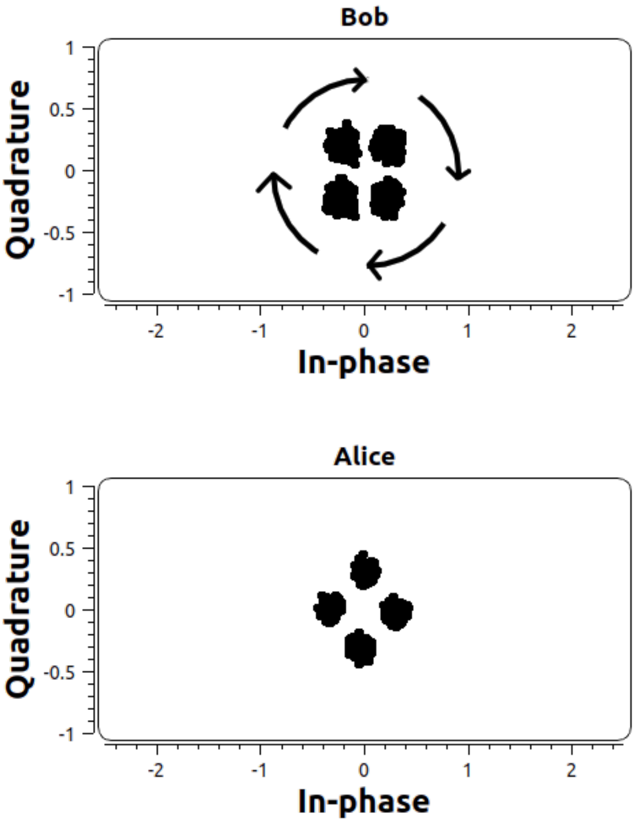


Figure 7.2: **Frequency errors.** A difference in reference frequencies between two clocks leads to Bob's phase changing over time.

During a broadcast, as frequency measures a change in phase over time, we expect an error of 1 Hz in the broadcast frequency to translate to one full rotation of a cluster per second.

This effect has many applications, as frequency distribution is used in a wide variety of areas, such as geodesy [38, 39] and physics beyond the Standard Model [40]. The ability to compare clock frequencies at increasingly higher precision allows for a greater variety of uses, depending on what degree of precision is available through this method.

Currently, time and frequency distribution in the UK is provided by the National Physical Laboratory. This is typically done over fibre when reasonable, or through GPS, radio and the internet when wired frequency distribution is not feasible. Here we devise an alternative method of frequency distribution through phase tracking, attempting to match the frequency of receiving clocks to a primary source through the analysis of observed phase errors. This aims to support the current methods of frequency distribution by covering those scenarios in which optical methods are not feasible. This method employs only one-way communication from a primary clock such that secondary clock can perform frequency adjustments. This is distinct from timing synchronisation protocols which employ two-way communication in order to agree on a definite time [41, 42, 43, 44, 45, 46, 47].

Currently, it is possible to synchronise clock frequency with very high precision in short times through optical methods [48], potentially reaching the region of 10^{-18} to 10^{-20} relative error through optical methods [49, 50]. We will not be attempting to compete with such results, instead comparing to what can be achieved with commonly available equipment currently. The simple setup required to perform our experiment gives clear applications in wireless radio synchronisation, which currently utilises GPS. The target for our experiments is therefore proving the ability to synchronise frequency between a pair of clocks with precision in the region of 10^{-9}-10^{-10} seconds, at which point we could confirm an improvement over the current GPS methods without requiring the use of specialist equipment. With additional improvements to the initial experimental setup, we will see precision of many orders of magnitude smaller than this through a wireless network, with measured Allan Variances in the region of 10^{-15} with averaging times under 10^4 seconds. At extremes, we will see precision in the region of 10^{-16} seconds with averaging times over 10^5 seconds, though broadcasts were not performed long enough for this to be reached in an Allan Variance plot.

7.2 Phase Drift

We perform the protocol by tracking the average phase measurement performed by Bob over time. We broadcast a QPSK signal to Alice and Bob, and split the string of Bob's measurements into blocks in order to track the average of each block.

We employ Alice's measurements to assist in measuring the rate of change of phase. We initially consider the amplitudes of a string of Alice and Bob's measurements, and offset Bob's measurements until we find an area of high correlation ($r > 0.8$). This allows the detection of time delays between Alice and Bob, which are then removed. Given time-synchronised measurements between Alice and Bob, we check which cluster Alice's measurements fall into. These correspond to measurements in each of Bob's clusters, and is a simple method of tracking which of Bob's measurements belong to which cluster. For ease of analysis, as we know which of Bob's measurements belongs to each cluster through the entire measurement period, we apply a rotation of $\pi/2$, π, or $-\pi/2$, to each of Bob's measurements as necessary to condense the four clusters down into a single cluster.

As seen in Figure 7.3, there is a change in average phase over time. Comparing the gradient of this plot to an expected gradient of 2π per 1 Hz difference in clock references gives the difference in frequency.

In plotting this, we see unexpected additional behaviour in the gradient in the form of an oscillation. As the behaviour is very consistent across this broadcast, we add a series in $\cos^2$ to the best fit curve formula, attempting to fit the curve of:

$$\phi\left(t\right) = at + b + c\cos^2\left(dt + e\right) + f\cos^2\left(2dt + g\right)$$

for some choice of constants (a, ..., g).

While this fit is not perfect, we are only interested in the straight line component of the gradient, and this estimate is sufficient to account for most of the oscillations. Additionally, we will see that this additional behaviour does not remain consistent as the frequency is increased. These additional oscillations my be caused by the inherent instability of the clocks, as well as potentially impressing the circular rotation of clusters on a square range of average values. Along with measurement time, these are the limiting factors on uncertainty in these calculations. As clock instability is a hardware problem and inconsistent as frequency changes, we do not try to characterise it.

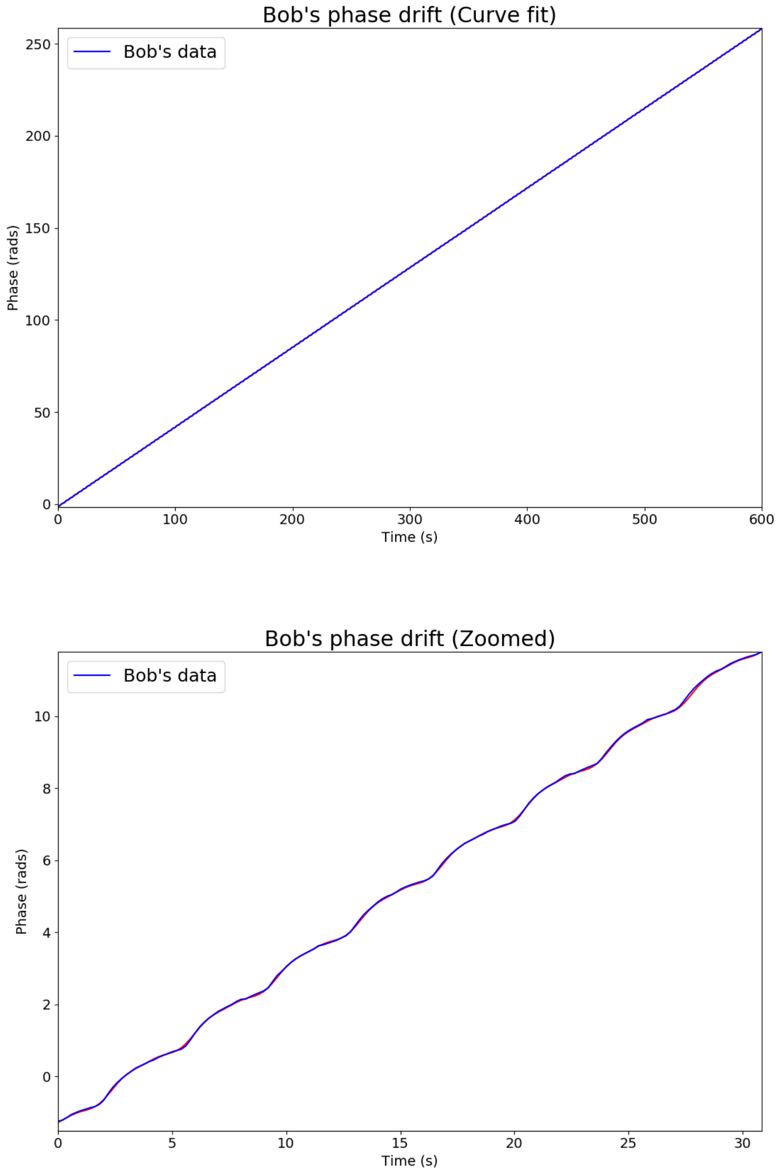


Figure 7.3: **Phase drift.** The average phase of Bob's measurements is observed to increase over time, the rate of change of which will be used to calculate the frequency error. A zoomed view of the first 30 seconds of data makes visible oscillations not clear in the full view. This is caused by the instability of the clocks used for this experiment.

7.3 Uncertainty

To evaluate the usefulness of this protocol, we consider the relative frequency stability, this is the uncertainty in the estimate of the frequency difference as a proportion of the broadcast frequency. For common GPS devices, this relative stability is approximately in the region of 10^{-11} to 10^{-13} relative error after 10 minutes of measurement [51].

For our analysis, we take the covariance matrix of best fit parameters, convert the uncertainty in gradient to hertz, and compare to the broadcast frequency. For the 70 MHz broadcast, this uncertainty was calculated to be less than one part in 10^{14}, showing an improvement over typical GPS-based equipment.

There are several ways to improve on this uncertainty:

- Increase the measurement time
- Increase the broadcast frequency
- Use more stable clocks

For measurement times, there are limits to the improvement possible. Very long measurement times become impractical to carry out in practice, and averaging data over long periods is susceptible to errors caused by gradual changes. Data which appears consistent across a small time frame may have a large variance when measured across its lifetime.

Increasing the broadcast frequency reduces the error as a proportion of the total frequency, reducing our uncertainty. This is limited by the broadcast range of available equipment, with these specific tests using broadcasts limited to a maximum of 4 GHz. Of note is that this covers the 2-2.4 GHz region, which commonly sees use in current broadcasting equipment. For the purposes of testing the limits of this method, it would be useful to test with equipment capable of broadcasting higher frequencies, such as in the region of tens of gigahertz.

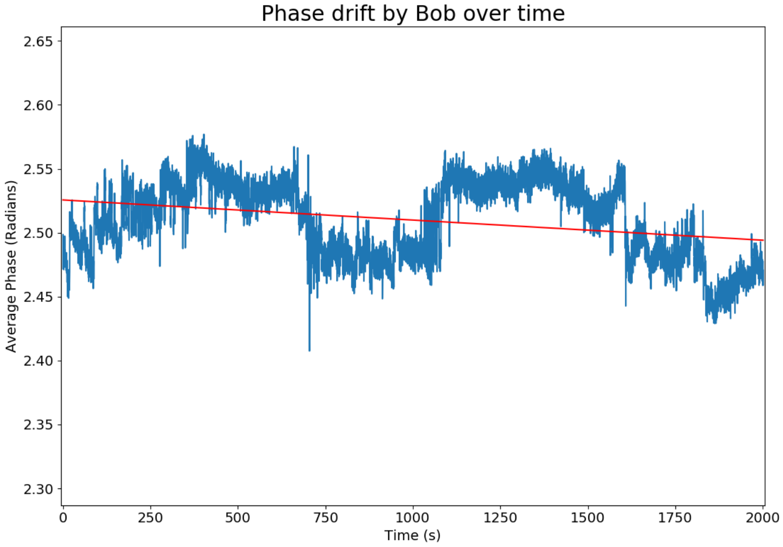


Figure 7.4: **Single Clock.** The frequency distribution protocol performed with a single clock.

Clock stability is a clear avenue for improvement. More stable clocks give more consistent measurements, which leads to reduced uncertainty. We check the stability of the primary clock by splitting the 10 MHz signal from it, and using it as a reference for both Alice and Bob. This is equivalent to setting Clock A and Clock B as identical in Figure 7.1. We see the output of this in Figure 7.4 for a 3 GHz broadcast. While the phase is mostly stable, we do see small shifts over the running time, potentially due to effects introduced in the cables. We also plot the Allan deviation of the same phase measurements in Figure 7.5, a common method of evaluating frequency stability.

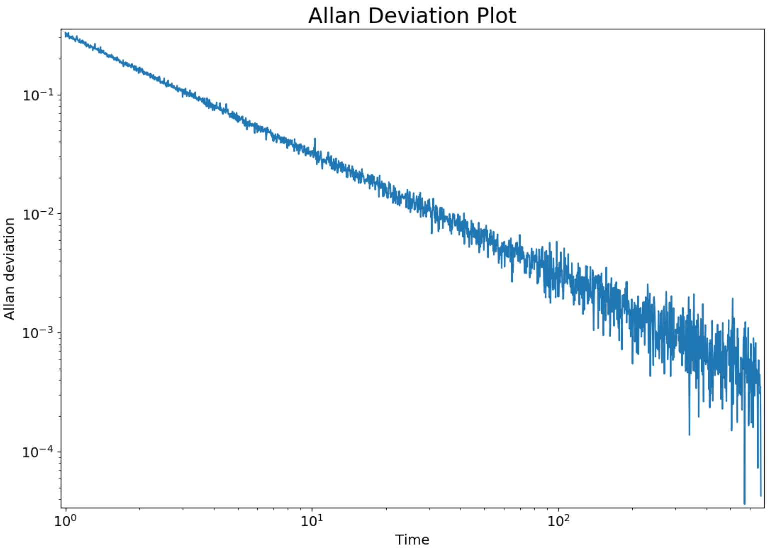


Figure 7.5: **Allan Deviation.** An Allan deviation plot of the raw data used in Figure 7.4.

7.4 Wireless transmissions

As with the experiments on key distribution, a clear next step is to remove the wired channel leading to Bob, allowing for analysis of wireless frequency distribution. Alice remains with a wired connection to the source, allowing for stable phase averages which can again be used to synchronise measurements.

We replace the wired channel to Bob with a pair of antennae 30cm apart on an adjustable platform, and raise the frequency to 3 GHz. Before recording any data, we can already reduce the frequency error between the clocks by watching the clusters rotating in the GNURadio interface, and adjusting the secondary clock's frequency until Bob's clusters appear approximately stationary. We do this as the clusters rotate faster at higher frequencies due to proportionally larger errors, which makes the data more difficult to process.

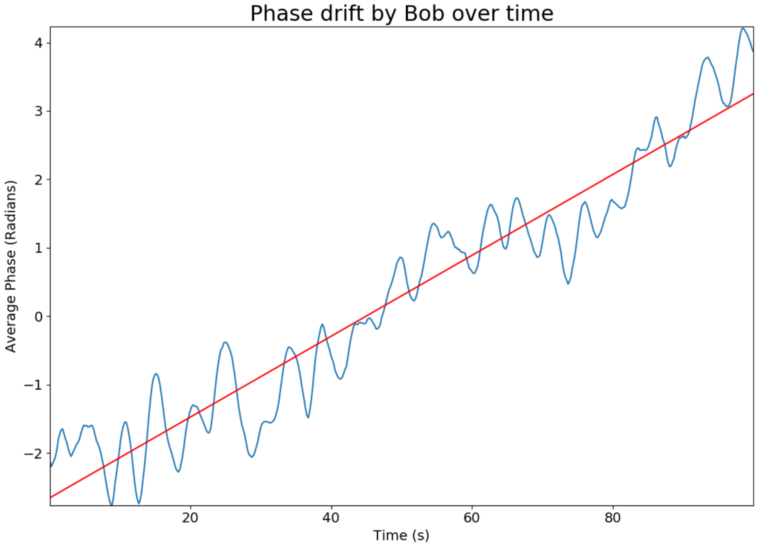


Figure 7.6: **Wireless Synchronisation.** Phase drift observed in a 100 second, 3 GHz wireless broadcast over a 30 cm gap.

Performing the same uncertainty analysis for the 3 GHz broadcast shown in Figure 7.6, we find a relative frequency uncertainty of 4×10^{-14} over 100 seconds. While this test was performed over a relatively small distance, this level of precision remains comparable to the wired versions of the protocol.

7.5 Further Possibilities

Two additional avenues for exploration were noticed while performing the experiments on timing, which require further analysis.

First, Alice and Bob's phase measurements, performed over a small time, are highly correlated. On a plot comparing Alice and Bob's phase measurements, as shown in Figure 7.7, the effects of phase drift caused by errors in Bob's clock manifests as a vertical translation over time.

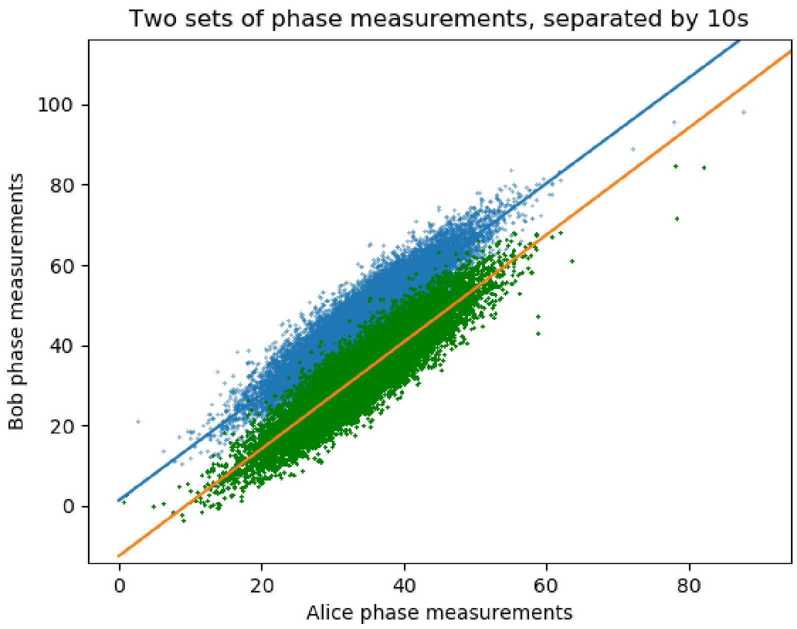


Figure 7.7: **Phase Comparison.** A scatter plot comparing two sets of Alice and Bob's phase measurements in degrees.

When plotted together, Alice and Bob's data forms a line of length equal to the diameter of the clusters, but have a smaller deviation around the line of best fit than the clusters do about their mean value. If this smaller deviation created by phase correlations could be taken advantage of for the purpose of frequency distribution, a considerable increase in precision over the current version of the protocol could be made. Some issues with this method remain to be resolved, most noticeably changes in gradient of the best fit lines over time, which complicates the otherwise simple approach of comparing y-intercepts to measure vertical translation.

An additional application was noticed, which was the potential to measure changes in distance through varying phase measurements. To test this, a moving platform was used to modify the gap over which the QPSK signal was broadcast, first reducing the gap between the antennae by 30 cm before returning to the original position. A single clock with a reference signal split between the source and Bob is used in this initial test, to remove a source of error.

For a 1 GHz broadcast, we expect to see a single full rotation of the clusters as the gap is increased or decreased by 30 centimetres, as this gap is equal to one wavelength. Currently, issues still need to be resolved regarding this method. Reflections of the signal from other surfaces, as well as movement of wires, were both observed sources of errors in the broadcast.

A plot of the measurements obtained in one test of this protocol is shown in Figure 7.8. The broadcast distance began at 55 cm, reducing to a minimum of 25 cm in the centre of the plot, before moving back to 55 cm. While we do not see the exact expected change in magnitude of 2π radians over one wavelength of movement, we do observe the gradient reversing direction as the platform switches from receding from to approaching Bob's antenna halfway through the broadcast. Some external factors, such as reflections from the environment, likely have an effect on readings produced this way.

While this process needs additional refining if the aim is to measure precise distances, it is currently capable of detecting if the broadcast distance is increasing or decreasing. With additional work, this ability could be of interest in quantum illumination/radar, in which case Bob's measurements would be reflections of a signal broadcast towards a target.

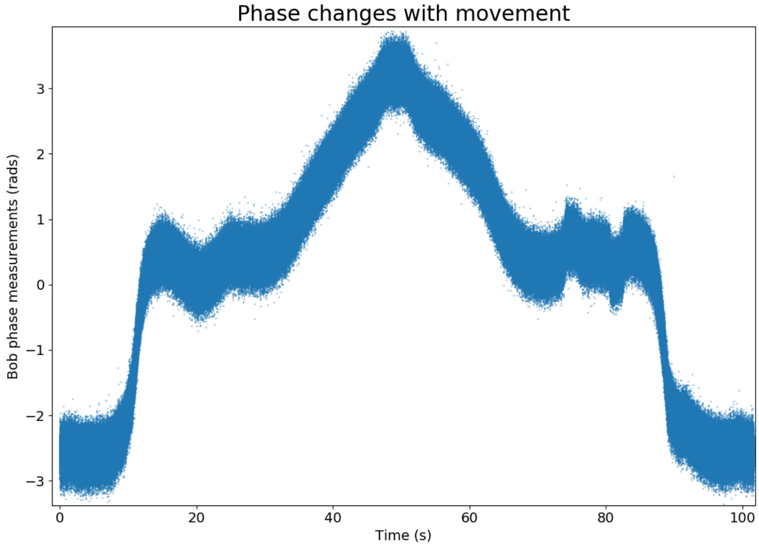


Figure 7.8: **Platform Movement.** A scatter plot showing the change in Bob's phase measurements as the broadcast distance changes. The direction of movement reverses halfway through the plot.

7.6 Synchronisation Through Feedback

While it is interesting to be able to calculate differences in clock frequencies, the ability to use this method to synchronise frequency at high levels of precision would have applications in a wide variety of physics fields, and the relatively straightforward experimental setup would allow for an alternative time frequency distribution method to GPS using equipment already employed in communications equipment. For this, we need a method of using the previous measurements to stabilise a secondary clock using a primary clock.

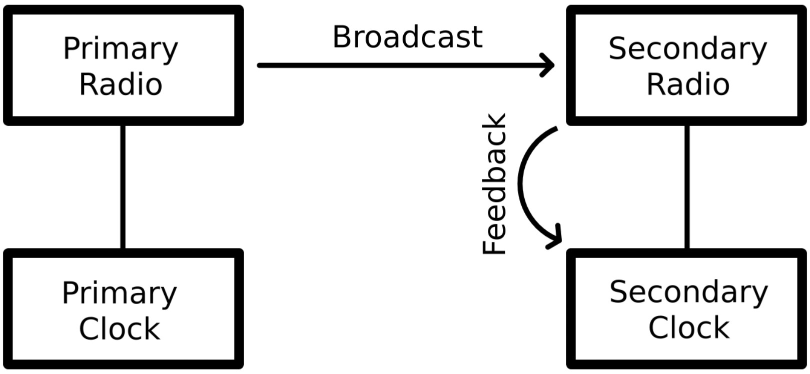


Figure 7.9: **Clock Feedback.** An adjustment to the clock measurement setup which allows for adjustment of a secondary clock.

As shown in Figure 7.9, we alter the experimental setup to allow feedback to the secondary clock. We do this by providing an adjustable voltage from a Raspberry Pi 400 to the secondary clock which controls the clock frequency. A feedback controller measures the errors in phase, and changes the input voltage to remove errors. To simplify the analysis, we switch to analysing a Binary Phase-shift Keying (BPSK) broadcast in which we attempt to keep a pair of measurement clusters centred on the X-axis in phase space. This can be seen in Figure 7.10, with a phase error rotating the clusters from their target position.

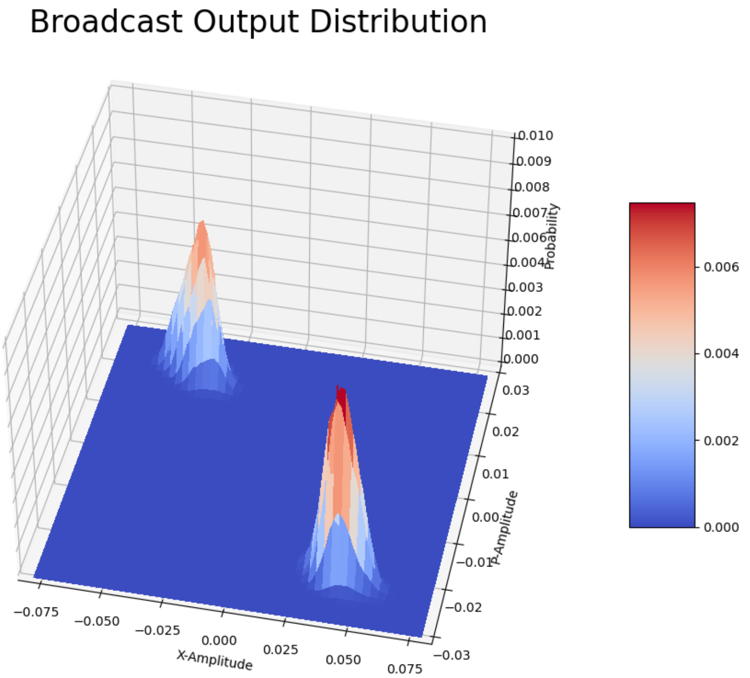


Figure 7.10: **BPSK.** A plot of the probability distribution for a BPSK broadcast, with a clearly visible phase error. This was originally displayed in [4].

This approach is very similar to the previously-mentioned methods used in signal processing for digital communications. In communication, Phase-Locked Loops such as Costas loops fix errors using a phase detector which monitors phase differences between a pair of signals. The output is fed into a low-pass filter to remove noise, before being passed to a voltage-controlled oscillator, which produces a signal with frequency dependent on the input voltage. This output is fed back to the phase detector, which will continue to provide an error voltage. Constant corrections to the frequency in this manner allows for an output and input signal to have a ‘locked’ matching phase, and therefore matching frequency.

We have mimicked this approach with our setup through monitoring of the phase through cluster rotations, which is our version of the Phase-Locked Loop’s phase detector circuit. Averaging the phase of a cluster of measurements before passing the result as an error to a feedback controller which adjusts the clock frequency likewise fills the same role as the low pass filter and the voltage-controlled oscillator, before sending the output signal back for further correction.

Despite being analogous to the common method of fixing frequency errors in digital communications, our intended approach adjusts the speed of the clock used with the receiving radio rather than being a part of signal processing. This gives the desired ability to apply the experiment in clock frequency synchronisation rather than only monitoring differences. Given the high precision required to perform modern communications reliably, this method has the potential for far higher precision than what is currently employed for wireless clock synchronisation through GPS.

Our setup only employs inexpensive, off-the-shelf hardware and free, open-source software, which may be seen as lacking compared to the typical setup for experiments in this field, which commonly involves equipment such as frequency combs for phase comparison, allowing for the highest currently-achievable precision in clock frequency synchronisation. However, regular radio equipment must perform at a very high standard to ensure working communication, regardless of the environment. Figure 7.11 shows the phase diagram for 4096-QAM, which is currently planned for use in the upcoming WiFi standard in 2024 as an upgrade from 1024-QAM. Such protocols require careful control over phase to ensure communication works, especially given that these are protocols to be widely implemented across many devices and demand consistent functionality. Given the high standards required for communication, it seems clear that such equipment can have applications in the precise phase monitoring which may be used for clock synchronisation.

Compared to previous tests, the addition of a feedback controller makes a clear difference to the output. Figure 7.12 shows the average phase of a single cluster during a 70 MHz broadcast with a feedback controller aiming to keep the average phase at zero. The controller is disabled then enabled to verify the controller is working correctly. As expected, the clocks begin to drift apart while the controller is disabled, however at a far lower rate than before the controller was implemented (Figure 7.3).

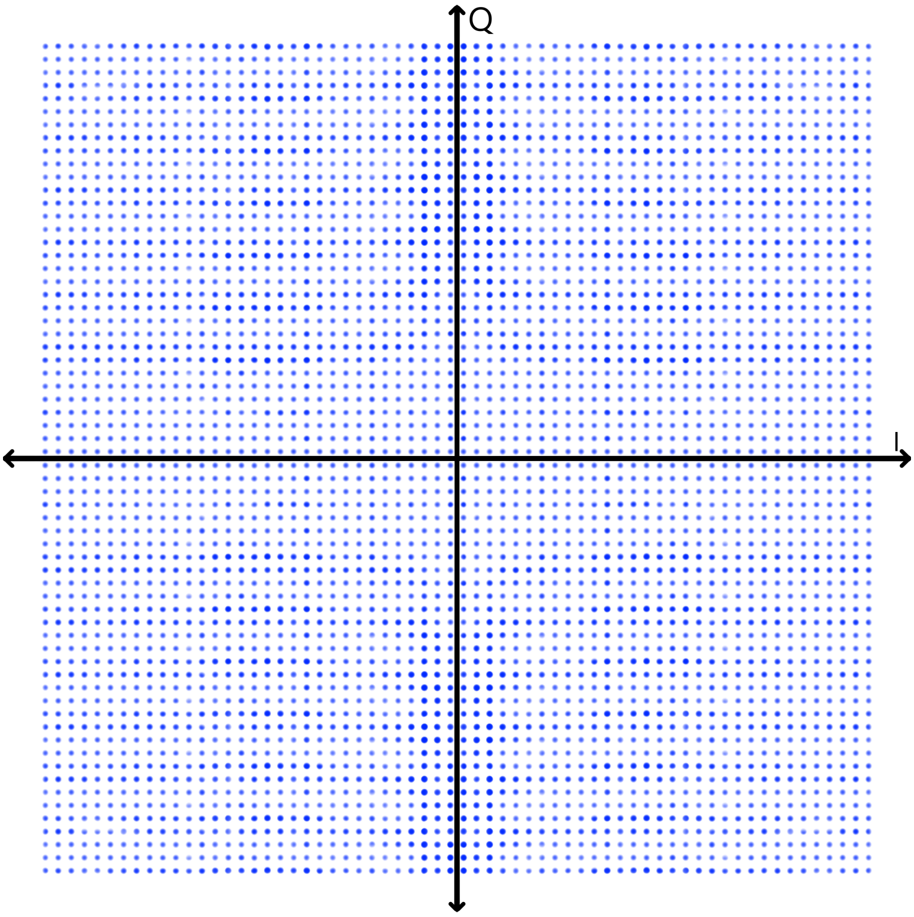


Figure 7.11: **4096-QAM.** A phase diagram for 4096-QAM.

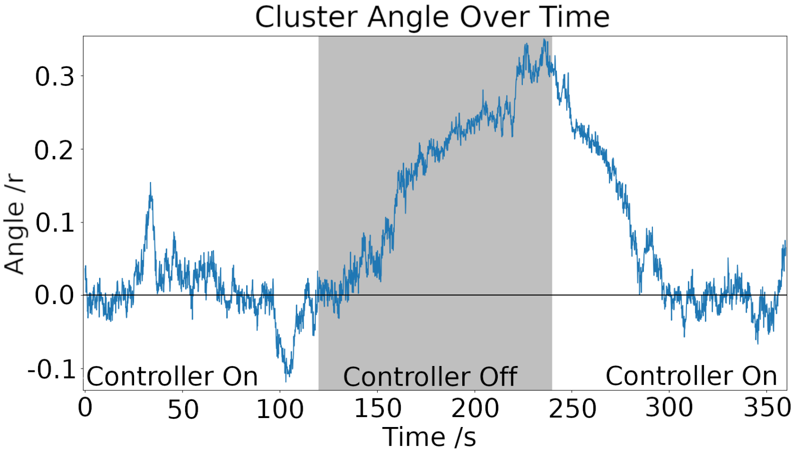


Figure 7.12: **Feedback Control.** Tracking the average phase as a feedback controller is disabled then enabled. This was originally displayed in [4].

To test the precision provided by this method over a long period, we first attempt a 70 MHz wired transmission between two radios with separate clocks as references. The outcome is shown in Figure 7.13. For a 16730 second broadcast, a straight line fit to the data gives a gradient estimate of $2.445 \times 10^{-7} \pm 1.963 \times 10^{-8}$ rads/second over the broadcast. This translates to a frequency error estimate of 38.9 nHz between the two sources. With a 70 MHz broadcast frequency this corresponds to a fractional frequency drift of $\frac{\Delta f}{f} = 5.559 \times 10^{-16}$.

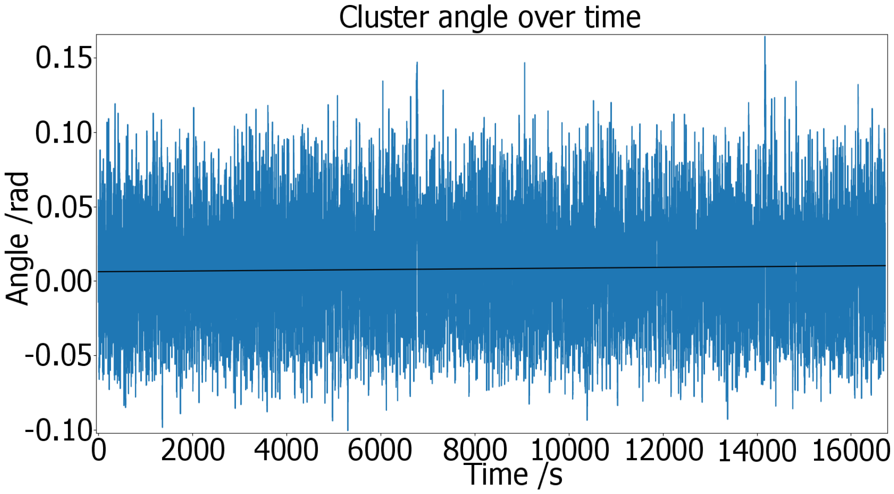


Figure 7.13: **70 MHz.** Tracking the average phase over a long term 70 MHz wired broadcast.

7.7 Wireless Frequency Synchronisation

As this synchronisation method only requires a radio broadcast, it is simple to swap the wired connection between the radios for a wireless broadcast. We test this by using a pair of 900 MHz antennae separated by 2.5 m of free space, and compare the results of the wireless broadcast to the initial 70 MHz wired test in Figure 7.14.

As expected, we see greater instability in phase from the 12.9x increase in frequency, though while sensitivity to errors increases in proportion to the broadcast frequency change, the PID controller prevents the range of results increasing the same amount.

For this wireless broadcast, we find a gradient of $3.609 \times 10^{-06} \pm 1.192 \times 10^{-7}$, which gives a frequency error of $\frac{\Delta f}{f} = 6.382 \times 10^{-16}$ over the 5 hour broadcast.

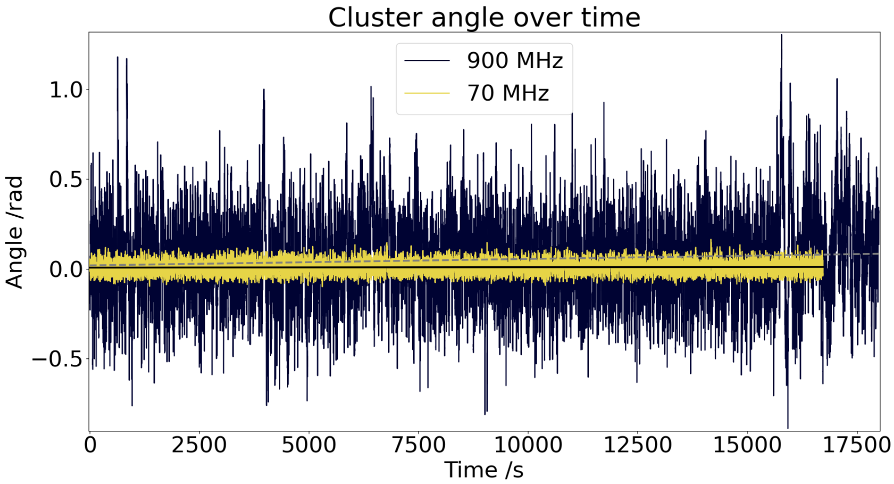


Figure 7.14: **900 MHz wireless.** Tracking the average phase over a 5 hour 900 MHz wired broadcast.

We can also compare Allan variance of both attempts, which provides a more reliable claim for what the protocol is capable of from a single broadcast. We see from Figure 7.15 that transitioning from a wired broadcast to short range wireless does not noticeably impact the Allan variance. Comparing either Allan plot to that provided in the PRS10C datasheet [52], the minimum advertised Allan variance for up to 10^6 seconds never achieves a part in 10^{13}, even at the minimum achieved between 10^3 and 10^4 second averaging times. Both wired and short range wireless display Allan variances approximately 100x smaller than the minimum advertised precision in under 5000 seconds, and evidence of 1000x improvement is seen when averaging across either whole broadcast; however, a longer broadcast is required to confirm this. Longer averaging times will eventually stop providing an improvement in Allan variance, though as we do not see this behaviour for the current plot yet, longer averaging times will be needed to find the limit of precision that can be attained with the current experimental setup.

With short range broadcasts having been demonstrated, access to longer range broadcasting equipment would allow synchronisation across distances already used in broadcasting.

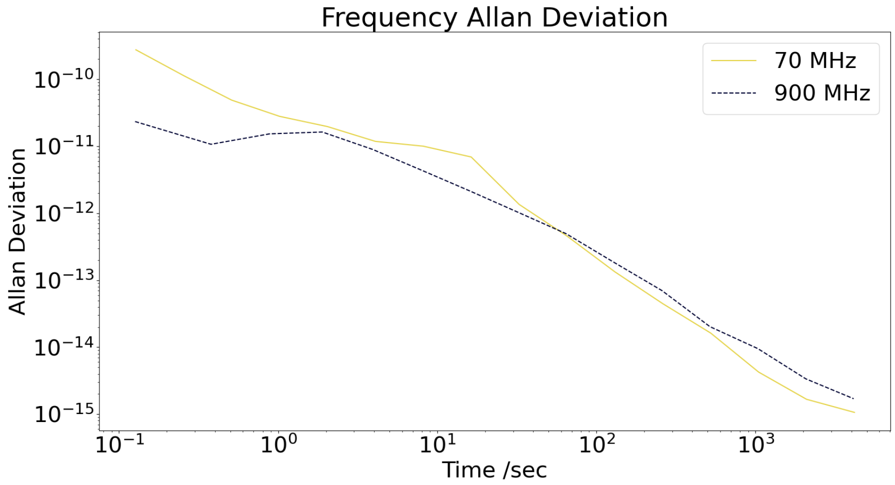


Figure 7.15: **Allan Variance.** The Allan variances of the plots in Figure 7.14.

Given that radio communications equipment already are used over kilometres, this may provide a method of clock synchronisation with greater precision than attainable by current GPS over similar distances, without employing specialised equipment. While the tests performed up to this point fall short of results seen with fiber networks, the use of less precise clocks, ease of setup, and not requiring line of sight due to the use of radio broadcasts provides clear advantages over other methods of synchronisation which currently see use.

In addition, short range broadcasts were later performed outdoors at a nearby farm, as well as at a conference away from the university. This demonstrated the ability to perform the protocol outside of the laboratory without impacting performance. Though the time needed for the atomic clocks to warm up and stabilise means that setup takes 2-3 hours before an experiment can be performed.

Chapter 8

Applications of Phase Tracking

8.1 Distribution across a clock network

A clear way to expand this is the addition of more clocks in order to form a network to synchronise across. It is straightforward to add additional radios to the system using their own clocks as references, allowing for synchronisation to be set up across a network of clocks. Networked synchronised clocks is a known problem in timing, due to the requirements of either fibre connections or line of sight for optical methods, and the lack of precision of common microwave methods. The improved precision of this BPSK method combined with the ease of setup allows for a straightforward method of synchronising many clocks to a single primary clock.

Our setup can be arranged in a similar manner as in the Network Time Protocol (NTP) – employing a primary source as the most stable available time reference connected to a device broadcasting to numerous clients which may not have access to clocks of equal precision. As with NTP, we use a single source connected to a primary client directly, at which point that client may openly broadcast to any number of receivers which pick up the broadcast and adjust their clocks accordingly. Communication can then be arranged between peers in order to improve reliability provided transceivers were used.

Due to the existence of incredibly precise optical methods requiring either line-of-sight or fibre connections, we have more interest in performing this in scenarios in which only radio communications are reasonable to establish, such as when line-of-sight is not available and fibre cables are not feasible. Given the widespread use of current communication methods without fibre we have wide range of possibilities. This provides a clear region of use as a low-cost method of creating a network with common radio equipment, with applications in areas where NTP or the Precision Time Protocol (PTP) are currently in use, focusing on PTP applications as those are areas in which access to increased precision is mostly valued, and optical methods may not be convenient.

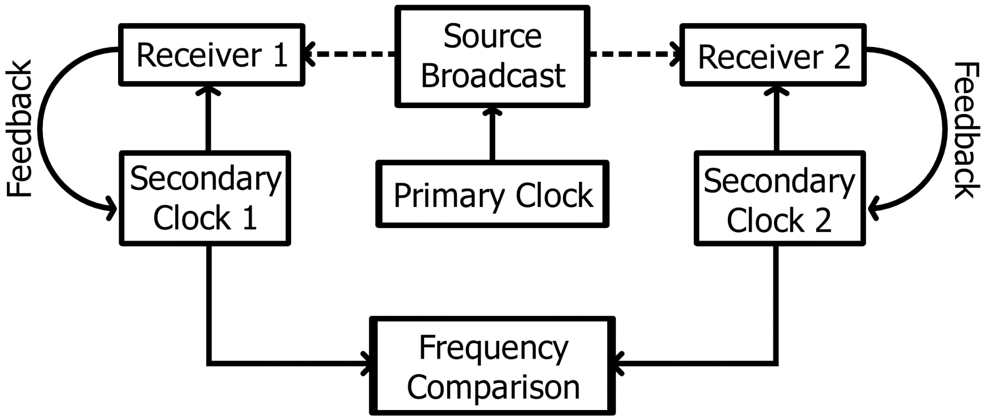


Figure 8.1: **Networked setup.** Scaling up the original frequency distribution setup to allow additional clocks.

To test this network, we adjust the setup by adding an additional receiver and clock in order to carry out the protocol twice simultaneously. With both clocks synchronised, a Moku Go is used to keep track of the phase difference through a direct connection to the clocks. This is due to the Moku offering a more convenient method of performing measurements. The setup for this is shown in Figure 8.1. This provides a simple way to set up a network involving any number of clocks provided that each can receive a signal. Comparing to the NTP setup, this is equivalent to a stratum 0 reference connected to a stratum 1 client, broadcasting to a pair of stratum 2 receivers which are also communicating with each other to compare their received information.

Phase differences are calculated using the Moku's PID controller. As measurements are taking directly from the clocks, the phase errors shown in Figure 8.2 are therefore with respect to a 10 MHz signal. Errors between frequencies provided a constant voltage output, and testing the effects of adding fixed voltages on the phase difference allowed for the conversion between voltage output and magnitude of phase errors to be calculated. This gave a method of calculating phases during the broadcast without tracking clusters as was done during the initial tests.

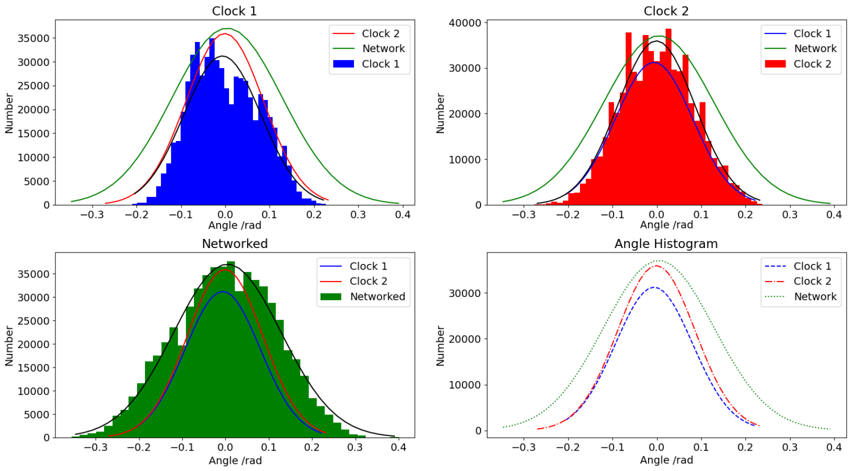


Figure 8.2: **Networked clocks.** The distributions of measured phase for a pair of receiving clocks.

8.2 Acceleration and Height Sensitivity

Given the high sensitivity of measurement of frequency differences provided by this protocol, it was of interest if the difference in clock speed caused by a change in height could be measured.

Gravitational time dilation causes a frequency difference in the region of a part in 10^{16} over a metre change in height, which was at the limit of what was measurable with our setup within the range of averaging times used in our tests. This was tested through comparison of frequency differences between adjacent free running clocks after stabilisation, before moving one clock approximately 30 metres down to check for a change in rotation speed which we could attribute to the height difference.

This was inconclusive due to the requirement of long averaging periods to reach the needed precision over the height difference that was available to us in our building. Further testing with a setup that allowed for a greater height difference between the clocks would give a more reliable opportunity for measurements, though we were limited on the range available to us. Alternatively, clocks with higher short-term stability may also assist by improving the rate at which we reach the level of precision required. While our setup was ultimately not sufficient for this specific test, there are clear avenues for improvement to the setup which could be implemented by a group with appropriate resources, through access to a larger height change or more stable clocks to improve sensitivity.

An unexpected side effect was seen when moving the clock to different heights. While moving the secondary clock between heights, sudden rotations in the clusters were observed. This could clearly not be attributed to the change in height due to the observed drifts being too large. The magnitude of these rotations where clearly visible to real-time observers, while the previous attempts failed to show any measurable differences across height ranges due to limits on precision. Further testing suggested that these changes were caused by either acceleration or velocity of the secondary clock, rather than changes in height. A final possibility considered were that drifts were due to errors introduced by movement of cables which interfered with the broadcast. While the following work to determine the cause of this is only preliminary and provided an unexpected outcome, we believe these initial experiments demonstrate enough to open this up to being a future area of research.

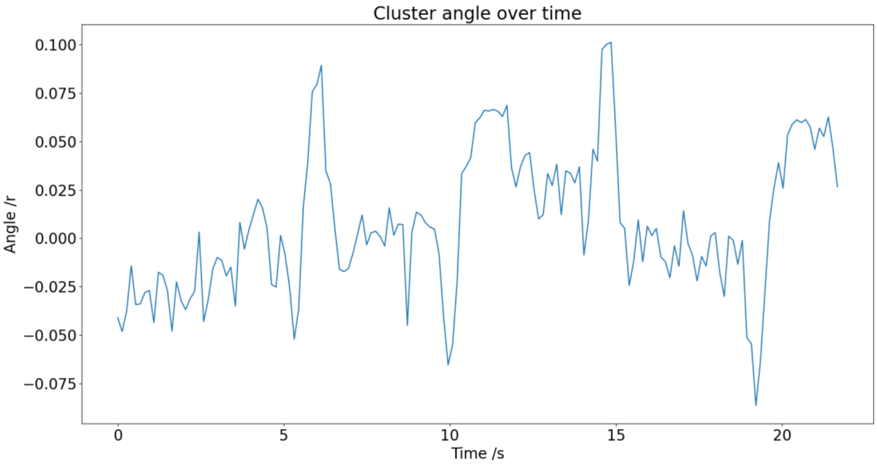


Figure 8.3: **Sudden Oscillations.** Monitoring the average phase of a cluster as a clock undergoes sudden oscillations.

Figure 8.3 shows a broadcast during which the clock was subject to four 30cm oscillations separated by approximately 5 seconds, returning to its initial position each time. These were clearly visible as four spikes in the average phase of a measured cluster.

It was initially unclear what the specific cause of these spikes was. While acceleration seemed possible, the assumption based on the clock principle is that acceleration has no effect on timing [53]. This would have discouraged us from attempting such an experiment had we considered it beforehand, though having already performed the experiments and seen results it was clear that further testing was needed. Under suspicion that is was related to acceleration, the test was repeated with varying oscillation frequencies over a 20cm height. First following pendulum motion for low acceleration, then vertical oscillations at two different rates.

The results of these initial tests are shown in Figure 8.4: in each test the clock was held stationary, before being oscillated, then returning to stationary. It can be seen that the pendulum motion test (top) does not show any significant changes beyond noise which may be attributed to the broadcast. However, the following two tests with increasingly high frequency oscillations show clear changes in average phase as the clock begins to be oscillated.

Given that all these tests involved the same height difference but produced different results, the changes in phase were related to the manner of movement, rather than the distance. The large changes to the phase were observed at the highest changes in acceleration, rather than at the highest velocity or largest height difference. This, coupled with the inability to measure a height difference approximately 100 times larger than these oscillations with stationary clocks, confirmed that the observations are not related to any kind of height change.

For circular motion, high acceleration is known to have no impact on clock measurements from centrifuge testing. This is a side effect of acceleration and velocity being perpendicular and is not the case should the clock be moved differently. Vertical oscillation shows clear and measurable change in phase which, with additional work to convert acceleration measurements into phase shift, could be used to track acceleration. Further testing with accelerometers and closer tracking of phase is needed to make more reliable claims, however later tests in which the clock was fastened to an oscillating platform showed a clear correlation between acceleration and shifts in phase using analogue signal processing methods. This gave two different methods of performing the experiment which gave similar outcomes. Closer examinations of the effects of such acceleration on clock measurements are difficult to find, showing a surprisingly limited amount of research despite the effects having impacts on experiments under motion, with the most clear example being measurements employing atomic clocks performed in vehicles. Most notably in experiments involving flight where stronger accelerations are likely to be experienced.

This may have applications in clock corrections under movement, which currently is difficult to account for. Ideally, accelerometers may be used to estimate clock errors caused by acceleration, which could then be used to correct such errors for experiments involving time measurements while in motion, Though more research is needed to calculate the exact size of the effect of acceleration on these measurements. The impact of similar movement is already known in instances in which atomic clocks are used in moving vehicles, such as aircraft [54]. Here, oscillators in motion and undergoing varied acceleration result in a degrading of precision provided, with

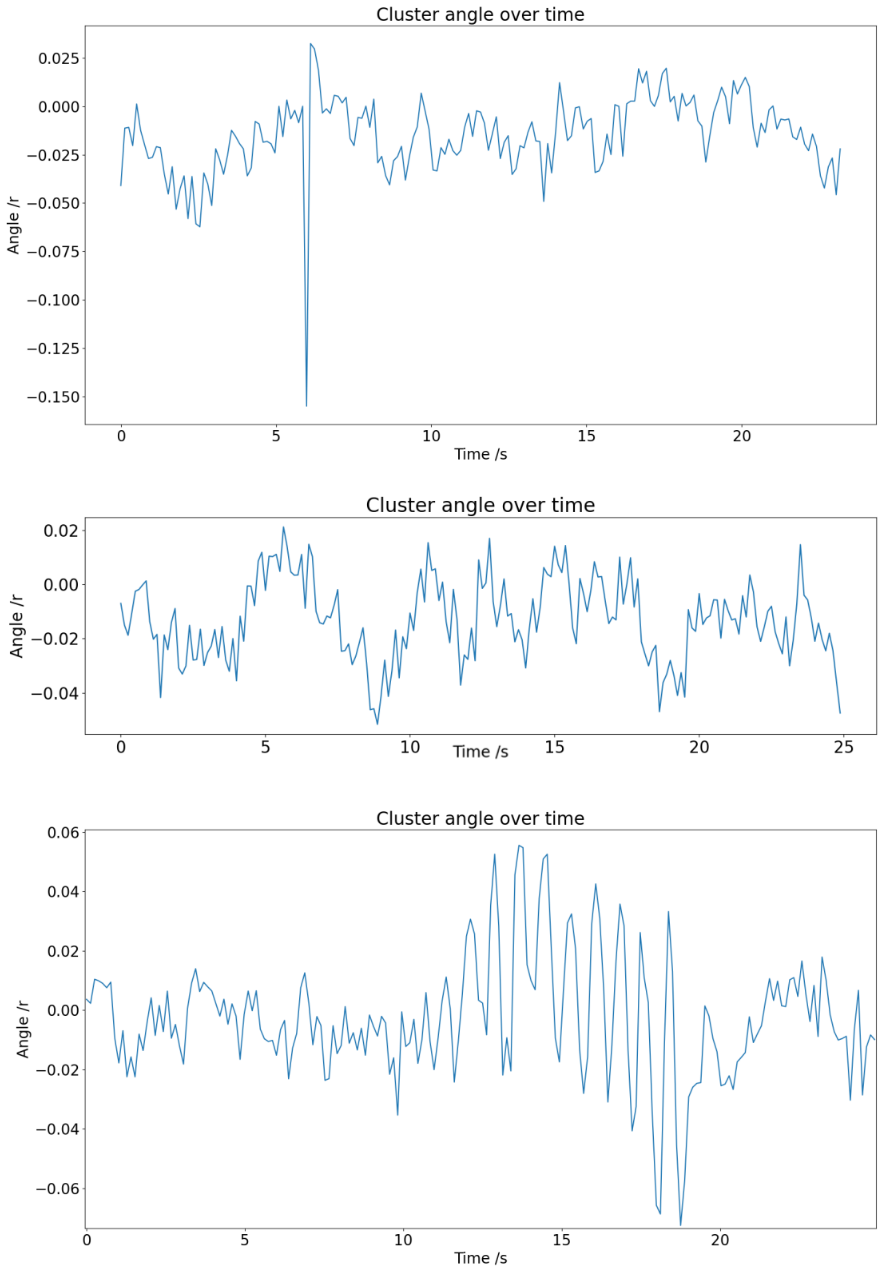


Figure 8.4: **Acceleration.** Monitoring average phase as a clock is oscillated at increasing frequency. The first plot shows a clock slowly undergoing pendulum motion, then oscillating at increasing rates in the following plots. The single spike at approximately 6 seconds in the first plot was caused by a brief loss of the broadcast and should be ignored.

decreases in precision up to two orders of magnitude. Further understanding of this may reduce the scale of such losses, allowing for higher precision despite movement.

While this was initially tested using a digital approach in the same manner as all previous practical tests in this writing, analogue processing appears to provide a more reliable and precise method of analysis, though currently there are too few results to base specific predictions on.

Chapter 9

Conclusions

Key Distribution

In this writing, we analysed a method of radio key distribution using thermal states. We began with a Monte Carlo simulation of the protocol, based off of previous theory. This demonstrated a potential ability to perform the protocol in practice, including with interception from an eavesdropper.

While an important starting point for the research, this initially only showed that unmodulated thermal states could be used for key distribution. This was not relevant for realistic applications, due to such signals not being used in real communication equipment. The next step was to expand on the background theory in order to demonstrate that the key rate had no dependency on displacement of the source states, which was initially not something that could be assumed. This showed that it was reasonable to attempt to perform the protocol using displaced thermal states, which are well known in communications and used in common wireless protocols. At this time, loss was also introduced into the protocol. This first showed that the protocol was still feasible up until total loss, regardless of where in the protocol it was introduced. The most noteworthy part of this was the prediction that loss before Eve could intercept led to an improvement in key rate up to a point, which is the expected scenario in a wireless broadcast. This scenario could only be avoided through an eavesdropper building a detector that picks up everything except for the portion of the signal Bob received, which in the case of a wireless signal being broadcast in all directions would not be possible to build without being noticed. At this point it had become clear that this was a workable protocol, and work should be made on a practical implementation.

With this background theory confirmed, GNURadio was used to broadcast displaced thermal states in the form of a QPSK protocol, which sees regular use in wireless communication. Using this, we were able to perform the protocol using off-the-shelf radio equipment and open-source software. This was done with both wired and wireless setups, up to a distance of 5m without additional error correction. With success in these experiments, we open an avenue for further testing over longer ranges with stronger broadcasting equipment. Given that the main restricting factor with our setup was the broadcast range of the equipment, it is clear that it is reasonable to expect that the protocol should be possible to carry out over standard radio broadcast ranges, and without line-of-sight. The required equipment to perform such an experiment over long ranges is very well understood, and is already reliably in use worldwide with robust error correction in order to carry out communications. Combined with an authentication method of similar security, this could allow a method of establishing secure communication while not requiring any hardware changes.

Clock Synchronisation

The final observations were an unintended side effect of errors introduced during initial testing with Alice and Bob using separate clocks, and is the field in which we are most interested in continuing research. We find that differences in frequency between two imperfect atomic clocks manifest as a phase error in signal measurements which increases over time. When analysing this for a QPSK broadcast, the rate of rotation of clusters can be measured, allowing calculation of the difference in frequency between the clocks to high precision. Over short wireless distances, this method compared favourably to GPS, which is currently used for frequency distribution in places where fibre is not feasible. Given the straightforward experimental setup, it would be simple to set the same experiment up using broadcasting equipment with longer ranges, and more precise clocks. An improvement of approximately a factor of 10^3 over the best advertised precision of the clock was observed, though it remains to be seen how this translates to a clock that is naturally more stable than what we were using. As the stabilisation protocol already handles long-term stability, the priority would be using oscillators which have higher short-term stability, as the responsiveness of the PID controller is a limit on the stability that can be achieved. Less drift over short time periods faster than the controller can respond would remove errors currently reducing the possible precision that can be achieved.

Given that the precision is calculated as a fraction of the broadcast frequency, it is of interest to find the limits of this method with equipment which has a higher maximum frequency and more precise clocks. While typical microwave radio broadcasting involves frequencies up to a few gigahertz, the increased precision at higher frequencies may be of use in laboratories interested in more precise frequency distribution methods. Even at current frequencies however, the clear improvement over what is currently achieved by GPS gives applications for the protocol in any situation where GPS already would see use.

With the current performance, it is difficult to compare the protocol to the highest precision results achieved through optical methods. Optical methods have achieved errors as small as a part in 10^{20} which is far more precise than we have been able to achieve with the current setup. While improvements to the equipment will provide higher precision compared to what we have been able to achieve so far, we do not aim to compete with established optical methods. We would aim to employ this specifically in wireless scenarios in which optical methods are not practical, as it offers a large improvement compared to GPS while using the same equipment.

Similar phase changes are also observed when the distance between Alice and Bob is changed. Initial testing was used to confirm phase changes dependent on the broadcast frequency, with an expected phase change of 2π over one wavelength of path length difference. This showed potential applications in radar, with lower frequencies being preferred in order to avoid needlessly high sensitivity.

Final Thoughts

For both fields, it seems clear that this would benefit strongly from input from people with experience based in radio communications. This may allow an easier transition onto working with more standard radio equipment, as well as possible consideration of error correction, which we do not currently include in our work. Error correction is an important part of keeping consistent communications in uncontrolled environments, which we currently have left out of our protocol due to lack of personal knowledge in the field, though this may become increasingly relevant as either protocol is attempted with longer range broadcasts. Given the simple nature of the equipment needed to perform any of the experiments carried out here, such a transition should be straightforward to carry out and test for people with such experience.

Overall, we have demonstrated uses for radio communications in a pair of fields in which they are currently overlooked. Currently, the most immediately relevant part appears to be the work on clock synchronisation, due to results consistently showing precision far in excess of what is currently achieved through GPS, which would be the main target for our protocol given the similar requirements in equipment, rather than aiming to match the record levels of precision available when optical protocols are feasible. This does currently remain an assumption however, as we have not currently seen or calculated the limit of precision through this method. We are already aware that constant corrections means that precision will tend towards a limit rather than reaching a maximum before decreasing, though we lack a way of calculating this limit.

For this to be relevant in areas in which optical synchronisation is currently possible, the protocol would have to be able to reach precision of approximately 10^5 -

10^6 times greater than what we achieved in our experiments so far. While far more stable clocks exist which could be used as references in order to improve the limit on precision, it is unknown if such a change would be enough to bridge this difference. Fortunately it is not required that the protocol compete with such methods in order to be useful in average synchronisation scenarios that rely on GPS. While this initially seems unlikely to compete with record precision measurements unless upgraded equipment provides a surprisingly large benefit, setting more reasonable expectations still allows for excellent applications in low-cost frequency distribution. Also demonstrated was that the protocol could be easily expanded to a network of clocks without any complications, a process which would have been exponentially more difficult or expensive to implement if specialised equipment were needed.

The final observations on acceleration-induced frequency changes in clocks were an unexpected late development in the work, and require far more research to make more concrete claims concerning it. Currently, we are confident that acceleration is the cause of changes in clock frequency after testing with a pair of different experimental setups. To continue this there should first be calculations carried out and models produced in order to predict the scale of such frequency changes. At such a point if observations were made that were in alignment with predictions, we could more confidently make supported claims about the effects we are seeing. Work is underway on initial attempts at modelling, which currently predicts the frequency changes seen in the experimental results to within an order of magnitude. While these are still preliminary results, it provides a strong starting point to build following research upon.

Bibliography

[1] A Walton, A Ghesquiere, G Brumpton, D Jennings, and B Varcoe. Thermal state quantum key distribution. *J. Phys. B*, 54(18):185501, Sep 2021.

[2] Adam Walton, Anne Ghesquière, David Jennings, and Benjamin Varcoe. Towards quantum key distribution with noisy communication sources, Oct 2022.

[3] Adam Walton, Anne Ghesquière, and Benjamin T. H. Varcoe. Quantum key distribution with displaced thermal states. *Entropy*, 26(6), May 2024.

[4] Adam Walton and Benjamin T. H. Varcoe. Topological state reconstruction for wireless stabilization of distant atomic clocks, Dec 2023.

[5] CC-BY license. https://creativecommons.org/licenses/by/4.0/. Accessed: 11-10-2021.

[6] Aysajan Abidin and Jan-Åke Larsson. Direct proof of security of wegman–carter authentication with partially known key. *Quantum Information Processing*, 13:2155–2170, Oct 2014.

[7] Mark N. Wegman and J.Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, Dec 1981.

[8] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, Jan 1983.

[9] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.

[10] N.C. Jam, S. Khorsandi, and M. Dehghan. Wireless quantum-key distribution in rf and microwave frequencies. In *EUROCON 2005 - The International Conference on "Computer as a Tool"*, volume 2, pages 1822–1825, Nov 2005.

[11] Guillermo Romero, Juan José García-Ripoll, and Enrique Solano. Photodetection of propagating quantum microwaves in circuit qed. *Physica Scripta*, 2009(T137):014004, Dec 2009.

[12] Sankar R. Sathyamoorthy, L. Tornberg, Anton F. Kockum, Ben Q. Baragiola, Joshua Combes, C. M. Wilson, Thomas M. Stace, and G. Johansson. Quantum nondemolition detection of a propagating microwave photon. *Phys. Rev. Lett.*, 112:093601, Mar 2014.

[13] Tasio Gonzalez-Raya. Wireless microwave quantum communication, Jan 2024.

[14] E. Flurin, N. Roch, F. Mallet, M. H. Devoret, and B. Huard. Generating entangled microwave radiation over two transmission lines. *Phys. Rev. Lett.*, 109:183901, Oct 2012.

[15] Ziqing Wang, Robert Malaney, and Jonathan Green. Inter-satellite quantum key distribution at terahertz frequencies. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–7, May 2019.

[16] F. Fesquet, F. Kronowetter, M. Renger, Q. Chen, K. Honasoge, O. Gargiulo, Y. Nojiri, A. Marx, F. Deppe, R. Gross, and K. G. Fedorov. Perspectives of microwave quantum key distribution in the open air. *Phys. Rev. A*, 108:032607, Sep 2023.

[17] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844–1852, Sep 1996.

[18] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, Oct 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[19] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.

[20] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[21] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999.

[22] T. C. Ralph. Security of continuous-variable quantum cryptography. *Phys. Rev. A*, 62:062306, Nov 2000.

[23] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, Jan 2003.

[24] Chip Elliott. The darpa quantum network, Dec 2004.

[25] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, Jul 2009.

[26] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi,

T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[27] Renato Renner and Robert Konig. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Theory of Cryptography*, pages 407–425, Berlin, Heidelberg, Feb 2005. Springer Berlin Heidelberg.

[28] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.*, 110:030502, Jan 2013.

[29] Stefano Pirandola. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Phys. Rev. Res.*, 3:043014, Oct 2021.

[30] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Coherent-state quantum key distribution without random basis switching. *Physical Review A*, 73(2), Feb 2006.

[31] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical Review Letters*, 93(17), Oct 2004.

[32] Jan R. Johansson, Paul D. Nation, and Franco Nori. Qutip 2: A python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 184(4):1234–1240, Apr 2013.

[33] Jan R. Johansson, Paul D. Nation, and Franco Nori. Qutip: An open-source python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 183(8):1760–1772, Aug 2012.

[34] David Elkouss, Anthony Leverrier, Romain Alleaume, and Joseph J. Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *2009 IEEE International Symposium on Information Theory*. IEEE, Jan 2009.

[35] Frederic Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables, Apr 2002.

[36] Ueli Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, Aug 1993.

[37] Jerome Lodewyck, Matthieu Bloch, Raul Garcia-Patron, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76:042305, Oct 2007.

[38] W. F. McGrew, X. Zhang, R. J. Fasano, S. A. Schäffer, K. Beloy, D. Nicolodi, R. C. Brown, N. Hinkley, G. Milani, M. Schioppo, T. H. Yoon, and A. D. Ludlow. Atomic clock performance enabling geodesy below the centimetre level. *Nature*, 564(7734):87–90, Nov 2018.

[39] Jaakko Mäkinen. The permanent tide and the international height reference frame IHRF. *Journal of Geodesy*, 95(9), Sep 2021.

[40] G. Barontini, L. Blackburn, V. Boyer, F. Butuc-Mayer, X. Calmet, J. R. Crespo Lopez-Urrutia, E. A. Curtis, B. Darquie, J. Dunningham, N. J. Fitch, E. M. Forgan, K. Georgiou, P. Gill, R. M. Godun, J. Goldwin, V. Guarrera, A. C. Harwood, I. R. Hill, R. J. Hendricks, M. Jeong, M. Y. H. Johnson, M. Keller, L. P. Kozhiparambil Sajith, F. Kuipers, H. S. Margolis, C. Mayo, P. Newman, A. O. Parsons, L. Prokhorov, B. I. Robertson, J. Rodewald, M. S. Safronova, B. E. Sauer, M. Schioppo, N. Sherrill, Y. V. Stadnik, K. Szymaniec, M. R. Tarbutt, R. C. Thompson, A. Tofful, J. Tunesi, A. Vecchio, Y. Wang, and

S. Worm. Measuring the stability of fundamental constants with a network of clocks. *EPJ Quantum Technology*, 9(1), May 2022.

[41] Jeroen C. J. Koelemeij, Han Dun, Cherif E. V. Diouf, Erik F. Dierikx, Gerard J. M. Janssen, and Christian C. J. M. Tiberius. A hybrid optical–wireless network for decimetre-level terrestrial positioning. *Nature*, 611(7936):473–478, Nov 2022.

[42] J.L. Jespersen, B.E. Blair, and L.E. Gatterer. Characterization and concepts of time-frequency dissemination. *Proceedings of the IEEE*, 60(5):502–521, May 1972.

[43] S. C. Sun, Y. Bai, H. J. Liang, S. G. Wang, and L. J. Wang. Ground-to-satellite time and frequency synchronization link with active carrier phase compensation. *Review of Scientific Instruments*, 90(11):114708, Nov 2019.

[44] J. Miao, B. Wang, Y. Bai, Y. B. Yuan, C. Gao, and L. J. Wang. Portable microwave frequency dissemination in free space and implications on ground-to-satellite synchronization. *Review of Scientific Instruments*, 86(5):054704, May 2015.

[45] Sara Modarres Razavi, Fredrik Gunnarsson, Henrik Rydén, Åke Busin, Xingqin Lin, Xin Zhang, Satyam Dwivedi, Iana Siomina, and Ritesh Shreevastav. Positioning in cellular networks: Past, present, future. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, Apr 2018.

[46] Hui-Jian Liang, Shi-Guang Wang, Yu Bai, Si-Chen Sun, and Li-Jun Wang. Real-time frequency transfer system over ground-to-satellite link based on carrier-phase compensation at 10e16 level. *Chinese Physics B*, 30(8):080601, Aug 2021.

[47] L. Sojdr, J. Cermak, and O. Buzek. Standard frequency dissemination via the digital satellite tv network. In *Proceedings of the 1998 IEEE International Frequency Control Symposium (Cat. No.98CH36165)*, pages 278–283, May 1998.

[48] Ehsan Sooudi, Andrew D. Ellis, and Robert J. Manning. Self starting optical electrical optical homodyne clock recovery for phase-modulated signals. *Opt. Lett.*, 42(17):3486–3489, Sep 2017.

[49] David Gozzard. Clocks synchronized at the quantum limit. *Nature*, 618(7966):680–681, Jun 2023.

[50] Haochen Tian, Youjian Song, Jiahe Yu, Haosen Shi, and Minglie Hu. Optical-optical synchronization between two independent femtosecond yb-fiber lasers with 10^{-20} instability in 10^{5} s. *IEEE Photonics Journal*, 9(5):1–7, Oct 2017.

[51] Michael Lombardi. Evaluating the frequency and time uncertainty of gps disciplined oscillators and clocks. *NCSLI Measure: The Journal of Measurement Science*, 11:30–44, Dec 2016.

[52] Prs10 — rubidium frequency standard with low phase noise. `https://www.thinksrs.com/downloads/pdfs/catalog/PRS10c.pdf`. Accessed: 18/07/23.

[53] J. E. Romain. Time measurements in accelerated frames of reference. *Rev. Mod. Phys.*, 35:376–388, Apr 1963.

[54] Ankit Jain, Thomas Krawinkel, Steffen Schön, and Andreas Bauch. Performance of miniaturized atomic clocks in static laboratory and dynamic flight environments. *GPS Solutions*, 25(1):5, Oct 2020.