A Solution for Post Quantum Security Using Existing Communications Infrastructures

Freya Louise Wilson

University of Leeds

School of Physics and Astronomy

Submitted in Accordance With the Requirements for the Degree of

Doctor of Philosophy

December 2017

Declaration

The candidate confirms that the work submitted is their 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.

Chapters 3,4,5,6 and 7 contain work in publications that are either in submission or preparation.

Chapter 7 contains work in submission with an MoD specific journal (As main author, with B. Varcoe) titled “Leakage from Shielded Rooms Using the Vector Potential”. The work in this is attributable to the Author under the guidance and supervision of B. Varcoe.

Chapters 3-6 contain work in 3 serparate papers in preparation. These are titled “Properties of Randomness as a Resource for Post-Quantum Key Distribution”, “Security Boundaries for CVQKD”, and “Characterisation of Microwaves for Quantum-Safe Key Distribution”.

Chapters 4 and 5 contain some work which features in a paper in submission, co-authored with B. Varce and A. Ghesquire entitled “Quantum Secrecy in Thermal States”. The work attributable to the Author of this thesis is the analysis of thermal states, correlations and fluctuations.

Furthermore, chapters 3-6 contain material featuring in posters and talks presented at QCrypt ’17, Photon ’16, QIPC ’15, and QCN ’14.

For my Grandad, Albert Pickett. He always believes in me, is always proud of me, and always supports me in whatever I choose to do.

Acknowledgements

First and foremost my thanks go to my supervisor, Ben Varcoe, whose relentless enthusiasm, wisdom and faith in me was invaluable over the last five years. I first became his student during a particularly interesting summer project as an undergraduate which then led on to an MPhys project and then a PhD. His support through these years has been unrelenting and he has been a constant source of inspiration and motivation. I owe him, not only this PhD, but my sanity. The atmosphere that he fosters in the lab is one that makes it a pleasure to do my work.

The other members of QIX lab I would be lost without. Especially to Shima Ghasemi(who always puts a smile on my face), Beth Newton (whose sacrifices to the laser Gods kept my experiments running smoothly), Joe Wilson (for the wit) and Anne Ghesquiere (from whom I have learnt a lot, and with whom I have passed many entertaining hours!). It would be remiss of me to mention QIX without also mentioning Matt Everitt. I am supremely grateful to Matt for always having a snide remark, and for having the most impressive programming skills! He is wiser than he knows and my PhD wouldn't have been half as enjoyable if it wasn't for him. When he left QIX it wasn't the same and he is - to me - truly the heart of the lab. Thank you also to Matt for many fruitful discussions over the years which helped guide my research.

I am also grateful to the physics coffee group - Rachel Thompson, Amanda McDonnell, Joe Hooper, Matt Everitt, and Chris Symonds. These friends have kept me sane, made life bearable during the sticky parts, and have provided endless support. Tuesday mornings were

a time of great sanctuary and comfort. In particular, their support whilst I have been writing this thesis has been incredible and some days I have no idea where I would be without them! I would especially like to thank Chris for dragging me in to work with him, and then home again, and for having sleeping patterns that mean he is always there for middle-of-the-night panics!

I would like to thank my friends - Hannah Buckley, Sophie Mann, Alex Bisby, Ollie O'Doherty, Mike Forrester, and Jon Mozley - for always being there for me through thick and thin. They have put up with me when I have been stressed and for celebrated with me through the good times.

I owe a special thank you to Maddie Lawrance-Thorne for being my personal grammar assistant; thank you for teaching me the difference between less and fewer, how to use 'effect' and 'affect' to the greatest effect, and felicitous use of semi-colons.

Of course these acknowledgements would be incomplete without mentioning my funders, the EPSRC, the MoD and Airbus Defence and Space - the funding from whom made this work possible. The latter provided me with equipment and much guidance on the topic of signals communications. Specifically, Martin Moseley, Gari Owen and Andrew Powell have been involved in many discussions and provided much insight into the research in this thesis, especially providing assistance with understanding the workings of telecommunications infrastructures.

Last but definitely not least, I owe my family a huge thank you. Thank you for supporting me in whatever I choose to do, thank you for looking after me when I need it, thank you for encouraging me, and thank you for listening to me waffle on about physics. Thank you to my Gran and Grandad for always being proud of me, loving me and believing in me. Thank you to my late Grandma for being the most wonderful influence. Thank you to my Dad for your love, confidence and inspiration to be the best that I can be.

Above all, thank you to my Mum. She has been there for me at every turn, she has had words of reassurance and optimism when I've needed them the most, she has listened to me whinge and listened to me celebrate, she has looked after me when I've been at my worst and she has picked me up and dusted me off when I've stumbled. More than anything she has never let me believe, for a second, that I can't achieve anything I put my mind to.

Lots of people working in cryptography have no deep concern with real application issues. They are trying to discover things clever enough to write papers about.

– Whitfield Diffie, *1992*

Abstract

The application of quantum cryptographic methods to existing communications infrastructures can be extremely difficult owing to the complex nature of quantum transmission methods. The premise of this thesis is an examination of methods to combine quantum-safe security with standard protocols, such as phase shift keying. Use is made of an algorithm previously presented by Ueli Maurer which allows for the distillation of a mutual symmetric cryptographic key from some shared secret information (Maurer, 1993). This algorithm is examined extensively and incorporated into a complete protocol which can be applied to pre-existing communications using phase shift keying. Primarily, one must consider the theoretical noise capabilities. In order to ensure the security of these communications the properties of microwaves are characterised and established as quantum-limited coherent states with a fractional excess noise on measurement.

Side channel attacks are more prolific when one considers the quantum measurement attack vector, especially when one considers that the full extent of these attacks in not yet known. If the same security could be extracted from the distillation algorithm, without relying upon quantum mechanics as the resource, then a universal standard for widespread implementation could be produced. The properties of random numbers are shown to be a sufficent resource for the advantage distillation algorithm which provides a strong candidate for a possible post-quantum secure universal standard.

The security of this (and various other protocols), however, relies upon the presence of an 'impenetrable' safe-house for trusted parties to prepare their cryptogrpahic resource (whether it be quantum or random

numbers). A side channel attack is examined which is based on the possibility of signal leakage from a shielded room. The use of the vector potential elucidates a possible method for signals to be detected outside a Faraday shielded enclosure - methods for performing this detection are examined and a characterisation of the properties of the leakage is performed. Leakage is detected from a shielded room at the National Authority for Counter Eavesdropping. It is concluded that a threat exists from this. However, there are possibilities for counteracting this using certain dielectric materials which need to be explored further.

Overall, it is established that advances have been made towards developing a post-quantum secure cryptographic method, which can be straight forwardly implemented in a variety of existing infrastructures using phase shift keying protocols, and even in a universal implementation using random numbers as a secure resource.

Abbreviations

AD	Advantage Distillation
AWGN	Additive White Gaussian Noise
BB84	Bennett and Brassard 1984 protocol
BCH	Bose-Chauhuri-Hocquenghem error correction
BPSK	Binary Phase Shift Keying
COMSOL	COMSOL Multiphysics Modelling Software
CV	Continuous Variable
CVQKD	Continuous Variable Quantum Key Distribution
EM	Electromagnetic
GCHQ	Government Communications Head Quarters
GHz	Gigahertz
HBT	Hanbury-Brown and Twiss
IQ	In-phase and Quadrature
LO	Local Oscillator
Long	Longitudinal
MHz	Megahertz
NACE	National Authority for Counter Eavesdropping
NCSC	National Cyber Secruity Centre
NI	National Instruments
NIST	National Institue of Standards and Technology
NP	Non-deterministic Polynomial Time
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QKD	Quantum Key Distribution
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
Rx	Receiving
SNR	Signal to Noise Ratio
TV	Transverse
Tx	Transmitting
UD	Uni Dimensional
USRP	Universal Software Defined Radio

List of Symbols

I(...)	Mutual Information
A	Alice, Legitimate Communicator
B	Bob, Legitimate Communicator
E	Eve, Eavesdropper
S(...)	Secrecy Capacity
$\mathrm{H}(\cdot)$	Information Entropy
$p(x)$	Continuous Probability Distribution
σ	Standard Deviation
μ	Mean
$\mathrm{C}(\cdot)$	Channel Capacity
τ	Time Period
M	Message
C	Ciphertext
K	Key
$\mathrm{h}(\cdot)$	Binary Entropic Function
ϕ^{-1}	Inverse Error Function
α	Noise in Alice
β	Noise in Bob
ε	Noise in Eve
C_S	Channel Capacity of a Broadcast Channel
T	Temperature
f	Frequency
λ	Wavelength
ω	Angular frequency
$\lvert\alpha\rangle$	Coherent State
$\mathbf{B}$	Magnetic Field
$\mathbf{A}$	Magnetic Vector Potential
$\mathbf{E}$	Electric Field
ρ	Electric Charge Density

Contents

List of Figures

1

Introduction

From Caesar to Shor - Keeping the Enemy at Bay

For centuries people have concerned themselves with the problem of securing the information shared between two parties (Singh, 1999), without revealing the information to an untrusted third party. The Romans brought about the Ceaser cipher, the ancient Greeks invented the Polybius square and Hebrew scholars used the Atbash cipher. In later centuries came the Italian Vigenere square, cracked in the 19th century by Charles Babbage, and various advances from Arabic mathematical scholars. The world wars fueled further progress in the topic - Alan Turing's Bombe was designed to crack the Nazi enigma cipher for example. In 1948 the founding father of 'information theory', Claude Shannon, published his seminal works (Shannon, 1948) (Shannon, 1949) treating knowledge as 'information entropy', with the hope of being able to explicitly describe and thus improve communication methods. Modern cryptography was born from these tools and the problem of sharing information became a rigourous field of communication intersecting mathematics, physics, and engineering.

This problem of modern information exchange can be thought of as three distinct, but related, goals;

(a) **Authenticity:** A trusted party can determine, unequivocally, from whom the communication came.

(b) **Integrity:** The trusted parties can identify when communicated information has been tampered with.

(c) **Confidentiality:** Two trusted parties can share information without it leaking to a third party.

A good cryptosystem will address all three. Indeed, there exists a variety of sophisticated cryptographic systems that meet these criteria; in particular, the 'one time pad' method encrypts a message with a unique key shared between trusted parties. The sharing of this key, however, presents a significant problem. The current method, 'public key cryptography', relies upon the complexity of solving certain problems computationally, namely the factorisation of the product of two large prime numbers (Nielsen & Chuang, 2004).

This is an extremely difficult problem for a classical computer to handle. However, various algorithms, for example 'Shor's algorithm', exist for quantum computers which will allow the computation to be handled with ease. The security community is concerned with this rising problem and has called for a 'post-quantum secure' solution (NCSC, 2016b).

Many proposals for quantum safe key distribution rely on the complexities of quantum mechanics for security - quantum key distribution (QKD) became synonymous with entanglement which is very difficult to apply to existing communications infrastructures(Christandl *et al.*, 2008; Ekert, 1991; Ozols *et al.*, 2014). Continuous variable quantum key distribution (CVQKD) solutions have been investigated in an attempt to make QKD more applicable to existing infratrucutres (Assche *et al.*, 2004; Cerf & Grangier, 2007; Filip, 2008; Graosshans & Cerf, 2004; Grosshans, 2005; Grosshans *et al.*, 2003; Horodecki *et al.*, 2008; Leung *et al.*, 2014; Pirandola *et al.*, 2008; Symul *et al.*, 2007; Usenko & Filip, 2010; Weedbrook *et al.*, 2009, 2012), however many protocols rely on optical frequencies (Assche *et al.*, 2004; Grosshans *et al.*, 2003; Lance *et al.*, 2008; Weedbrook *et al.*, 2006) and line-of-sight communication or dedicated optical fibres. One of the most celebrated protocols, however, is the uni-dimensional Usenko-Grosshans protocol which relies upon quantum limited measurements (Usenko & Grosshans, 2015).

A truly scalable, integrated solution has not yet been produced (ETSI, 2015; Lidong Chen, 2016; NCSC, 2016a). This thesis, however, works to bridge the gap between quantum safe key distribution and existing communications infrastructure. In particular, implementation in ubiquitious wireless communications such as mobile phone usage and wi-fi.

Motivation

This work started life when, as a Master's student, the author was studying single photon cavity measurements and the group was approached by a satellite communications company, Airbus Defence and Space, who wished to determine if QKD was possible in a pre-existing system. This instigated a more novel top-down approach to quantum safe cryptography.

Noise as a Resource

A conundrum which has prevented QKD and CVQKD from successful microwave implementations has been the presence of noise. Thermal noise in particular is thought to obfuscate the microwaves states and make entanglement especially difficult. A protocol presented by Maurer and Wolf (Bennett *et al.*, 1995; Maurer, 1993; Maurer & Wolf, 1999) called advantage distillation (AD), however, relies on noise as a resource for secrecy. The presence of noise clouds the communication from a potential eavesdropper and the two trusted parties can distill a mutual key from the noise. A further advantage of this protocol is that it can interact directly with phase shift keying protocols and therefore existing telecommunications systems.

Moreover, noise is not merely a product of a physical state. Stochastic noise is produced in random number generation. Harnessing this to power a noise-based distillation would allow for a channel independent protocol - the gold standard of modern cryptography goals.

To briefly review information theory, mutual information in the context of a shared key between two parties, say, Alice and Bob, means that the overlap in an information Venn diagram must be greater than zero.

$$I(A:B) > 0 \tag{1.1}$$

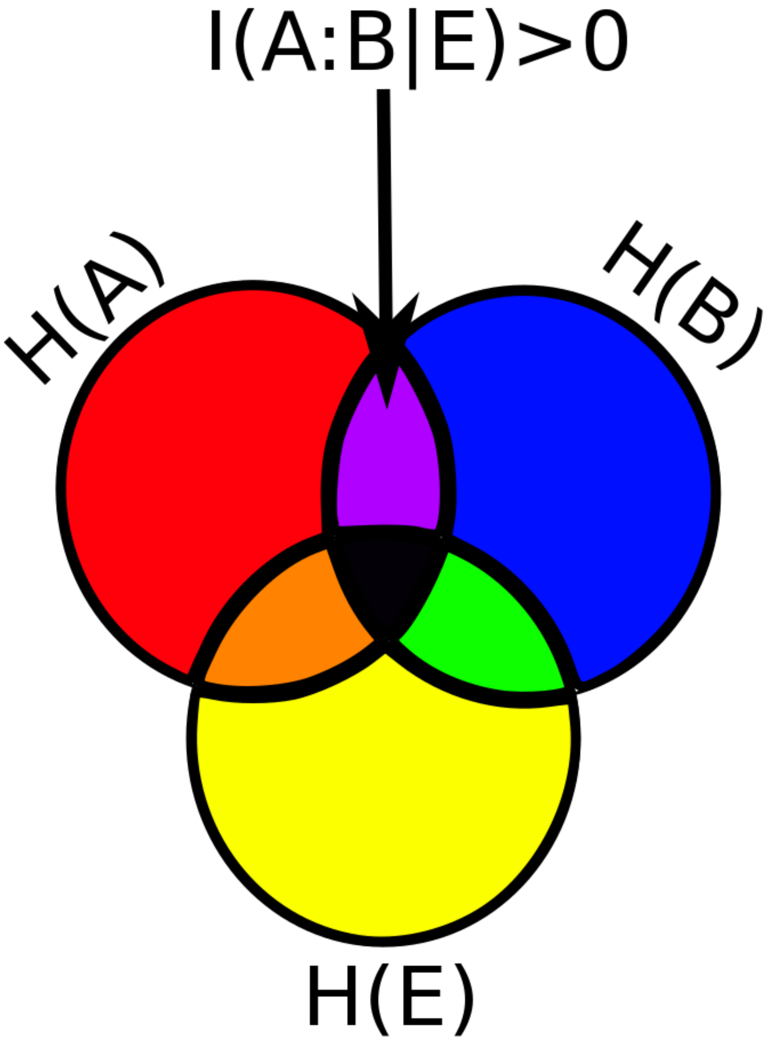


Figure 1.1: This Venn diagram shows the information entropies between the three parties. Mutual information exists in all overlapping areas, however the information which is secret from Eve is highlighted. This is the mutual information between Alice and Bob, independent of Eve. This area of the Venn diagram must be positive for secret key to be exchanged, and then maximised as much as possible for the benefit of efficiency. I denotes information and H denotes information entropy.

In order for this information to be secret, it is required that this mutual information is not known to an eavesdropper (for example, Eve). Mathematically this is represented as:

$$I(A:B|E) > 0 \quad . \tag{1.2}$$

This is demonstrated in figure 1.1. This is the only explicit requirement for secrecy. In fact, it is the definition of secrecy. Information theory then goes on to discuss the concept of 'secrecy capacity', denoted as $S\,(A:B||E)$. This is the ability of any given system (for which equation 1.2 must be valid) to maintain information in secret. It follows that, for a system to have secrecy the following bounds must be honoured:

$$0 < S(A:B||E) \leq I(A:B|E) \quad . \tag{1.3}$$

The Maurer protocol - advantage distillation - elaborates upon the famous BB84 protocol (H. Bennett & Brassard, 1984) and is based upon principles as early as Wyner's wire tap paper in 1975 (Wyner, 1975). Unusually, it is an entirely classical principle with a security proof based purely upon the sharing of some noisy source. The only requirement is that any eavesdropper must have some unavoidable noise. This thesis establishes an interleaving of shot noise limitied measurements and phase shift keying protocols, and furthers the exploration with stochastic noise as a resource for universal implementation.

Novel Contributions

This thesis affords the following additions to the field of post-quantum key distribution:

- The integration of existing telecommunications protocols with an existing key distillation protocol to create a novel method of quantum safe key distribution.

- The analysis of microwave signals to demonstrate that the measurement noise limitations can be used to secure key distribution, contrary to claims made in existing microwave key distrbution literature. (Weedbrook *et al.*, 2012).

- The proposal of using mathematically inherent properties, specifically the properties of random numbers, as an alternative resource for key distribution. This will eradicate the need for shot-noise limited measurements in the physical transmission and enable channel independent key distribution.
- The analysis of an as yet unexplored consideration for signal leakages through a Faraday cage. This work demonstrates the need for concern regarding the use of Faraday cages for security, and a need for further exploration and characterisation.

The summation of the work contained in this thesis outlines an innovative future pathway for effective post-quantum key distribution.

Thesis Structure

- The thesis begins Chapter 2 with an examination of how wireless communications protocols work - specifically phase shift keying - in order to then outline a protocol to incorporate noise based key distribution. The building blocks of this protocol are then examined in more detail.
- The central algorithm is then broken down into component parts in Chapter 3 and a mathematical model is presented leading to a demonstration of security.
- In order to implement this in a wireless system a characterisation of the transmitting medium must first be obtained - performed in chapter 4 and the noise levels are determined along with their suitability for use in the protocol.
- Chapter 5 demonstrates that the system may also be used for the pre-existing unidimensional CVQKD protocol presented by Usenko and Grosshans (Usenko & Grosshans, 2015) with a low level of excess noise.
- Since the goal is to implement post-quantum cryptography universally chapter 6 deals with the analysis of stochastic noise in random numbers as a resource for the advantage distillation protocol.

- A problem that presents itself at this point is the ability for the involved parties to maintain a secure 'housing' so an eavesdropper could not make a direct clone of the random numbers - especially since there is no quantum limited measurement to thwart a cloning attack. Chapter 7 examines the possibility for signal leakage through a Faraday shielded environment.

- Finally Chapter 8 ties these together and identifies the work that must happen next in order to realise the full potential of this post-quantum cryptography proposal.

Following this brief overview, the reader is presented next with a more in depth explanation of the two main concepts required to fully understand later work: information theory and telecommunciations protocols.

2

Background

This chapter reviews the principles that underly the work presented later in this thesis. The concept of Shannon entropy and then how this is used in formulating the quantity 'channel capacity' in the context of the field of information theory is presented first. This chapter will then explain some of the key principles behind wireless communications - essential for considering integration of cryptography with telecommunications infrastrucure.

2.1 Information Theory

This section deals with the classical Shannon blueprints outlined more thoroughly in (Nyquist, 1928; Shannon, 1948, 1949). The concepts covered include infomation entropy, channel capactiy and secrecy, alongside the ways in which these variables relate to each other. These concepts are applied to a simple braodcast channel and the change with the addition of feedback is examined.

2.1.1 Entropy

Shannon entropy is the measure of expected information gain from a message, based on the probabilities of the variables from which it is formed. The way in which the entropy of a channel is calculated is dependent upon the type of channel. The continuous channel can be treated as the general case, with the discrete channel presented as a limiting case of the continuous channel (Nielsen & Chuang, 2004; Shannon, 1948).

Continuous Channels

Any channel can be modelled as continuous by dividing its signals in to an infinite number of regions, each of which are arbitrarily small. Such a continuous channel is defined as one for which the measured output signal x is determined by a continuous probability distribution $p(x)$. Based on this probability distribution the expected information gain can be calculated. This value is designated the Shannon information entropy and is given the symbol H. The information gained from an arbitrarily small signal region is a function only of the probability across that region and is a function of the relationship $p(x) \log p(x)$. This leads to the equation for continuous variable Shannon entropy:

$$H(x) = -\int_{-\infty}^{\infty} p(x) \log p(x) dx \quad . \tag{2.1}$$

Since channels are commonly represented in binary, the basis of the logarithm is commonly taken to be 2, and this is assumed henceforth. It could be the case that the channel has a signal dependent on more than one probability distribution function. This would be a multi-dimensional channel, for which the generalised case of Shannon entropy is

$$H(x) = -\int_{-\infty}^{\infty} ... \int_{-\infty}^{\infty} p(x_1, ..., x_n) \log p(x_1, ..., x_n) dx_1 ... dx_n \quad . \tag{2.2}$$

An important consequence of defining entropy in this manner is that H is relative to the coordinate system and thus is not invariant under coordinate transformation, and additionally, the entropy for a continuous channel can be negative for the case.

Gaussian Channels

A continuous channel which consists of Gaussian modulated signals is a commonly occuring scenario in an application to telecommunications. The probability distribution function $p(x)$ for a one-dimensional Gaussian distribution with standard deviation σ and centred on a mean of 0 is:

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x^2/2\sigma^2)} \quad . \tag{2.3}$$

It follows that the information entropy for this Gaussian variable is given as:

$$H(x) = \log \sigma\sqrt{2\pi e} \quad . \tag{2.4}$$

Discrete Channels

The discrete channel is a specific case of the continuous channel entropy. If, in analyising the probability distribution $p(x)$, there are regions, i, in x which can be generalised as a single probability then one can perform the integral as a summation. Shannon presents the entropy of a channel as

$$H = -\sum_{n} p_i(x_i) \log p_i(x_i) \quad . \tag{2.5}$$

When considering digital logic there is a tendency to discretise models when considering models, for example in (Maurer, 1993). However this does not consider the entirety of the situation when dealing with what is a Gaussian channel in a real physical model, and some important subtleties are lost in the process. Conversely to the continuous case, the discrete information entropy must always be positive as it measures an absolute value of the randomness rather than being dependent upon some coordinate system. A special case of the discrete channel entropy is that of binary probability; if there are two outcomes with probabilities $p(x)$ and $q(x)$ then

$$p(x) = 1 - q(x) \quad . \tag{2.6}$$

and

$$H_{bin}(x) = -p\log(p) - (1-p)\log(1-p) \tag{2.7}$$

This can represent data which has been processed through slicing, where $q(x)$ is the probability of a bit flip error.

2.1.2 Multiple Variables

In communications cases there are frequently two or three variables to be considered[1]. The relationships in entropy between these variables are useful tools. The mutual information, I, between two variables X and Y is defined as:

$$I(X:Y) = \int_Y \int_X p(x,y) \log \left(\frac{p(x,y)}{p(x)p(y)} \right) \mathrm{d}x \, \mathrm{d}y = H(X) + H(Y) - H(X,Y) \quad , \tag{2.8}$$

which for N variables can be generalised to:

$$I(X_1 : X_2 : ... : X_N) = I(X_1 : X_2 : ... : X_{N-1}) - I(X_1 : X_2 : ... : X_{N-1}|X_N) \quad . \tag{2.9}$$

In the classical domain the mutual information is always greater than or equal to zero, in both discrete and continuous cases.

The mutual information can be thought of as the overlap between the entropies of each variable; the opposite of this, the 'independent part' of the entropies, is the conditional entropy:

$$H(X|Y) = H(X,Y) - H(Y) = -\int_x \int_y p(x,y) \log\left(p(x|y)\right) \mathrm{d}(x) \, \mathrm{d}y \quad . \tag{2.10}$$

or in the multivariate case:

$$H(X_1, X_2, ..., X_N) = \sum_N H(X_i|X_1, ...X_{i-1}) \quad . \tag{2.11}$$

2.1.3 Channel Capacity

The treatment of entropy using Shannon guidelines causes a fundamental difference in the channel capacity of a discrete channel compared to a continuous channel. For the case of a discrete channel it is possible for the channel capacity to have a zero value. For a continuous channel it is a requirement of the system to have a positive, non-zero capacity. This difference, while subtle, gives rise to a

[1] It is conventional in communications to consider the interaction between two people who are called Alice and Bob, and denoted A and B respectively. A third, trusted, party is often called Charlie and denoted C, however an eavesdropper is named Eve and denoted E. This thesis follows this convention, however when discussing the general cases the variables 'X,Y,Z' are used.

number of interesting features. The generalised definition of channel capacity for a noisy channel, N, is the maximum possible mutual information of all x between the input, X and output Y, given by

$$C(N) = \max_{p(x)} I(X:Y) \quad , \tag{2.12}$$

and $I(X:Y)$ is the mutual information of the input signal X and the output signal Y, with joint entropy $H(X,Y)$, denoted by the probability distribution $p(x,y)$. Thus for a continuous channel, over a period of time τ, the capacity, C is

$$C = \lim_{\tau \to \infty} \max_{P(x)} \frac{1}{T} \int \int P(x,y) \log \frac{P(x,y)}{P(x)P(y)} \mathrm{d}x \, \mathrm{d}y \quad . \tag{2.13}$$

This is independent of the coordinate system despite using probability distributions which are continuous.

2.1.4 Secrecy

Having outlined the key concepts of information theory, this overview will examine next the application of these to the principles of cryptography.

Consider transmission of a message, M from a sender (Alice) to a receiver (Bob), via a ciphertext C, which is achieved by encryption of M with a key, K. For such a ciphertext to be entirely secure (in which an eavesdropper, Eve, can do no better than guess at random) then M and C must be statistically independent. That is

$$I(M:C) = 0 \quad . \tag{2.14}$$

(Shannon, 1948) One such cipher is one-time pad [1]; however Shannon also identified that the key must be at least as long as the message, i.e.,

$$H(K) \geq H(M) \quad . \tag{2.15}$$

This clearly leads to difficulty in the accessibility of mutual key. Shannon proclaimed this based upon various assumptions. More generally, a requirement for

[1] The one time pad encodes an n bit message string with an n bit private key string, which is used only once. This ensures provable secrecy however the large amount of key required often makes it cumbersome to implement (Nielsen & Chuang, 2004).

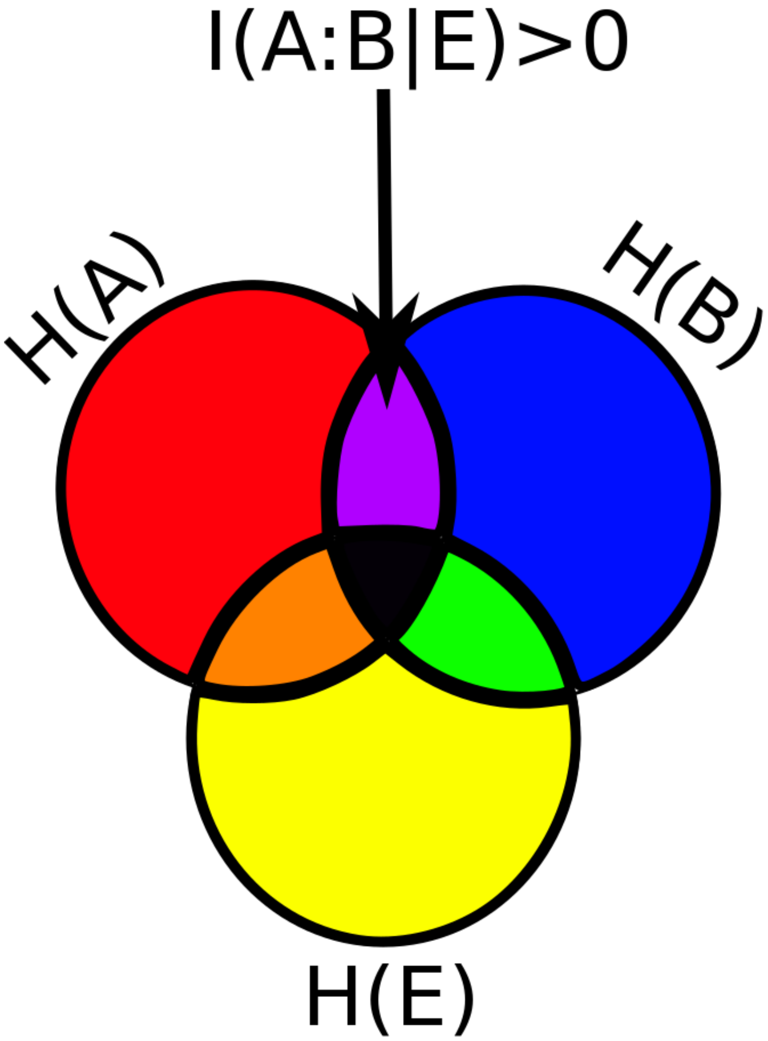


Figure 2.1: *Reproduced from Chapter 1 for ease* This Venn diagram shows the information entropies between the three parties. Mutual information exists in all overlapping areas, however the information which is secret from Eve is highlighted. This is the mutual information between Alice and Bob, independent of Eve. This area of the Venn diagram must be positive for secret key to be exchanged, and then maximised as much as possible for the benefit of efficiency. I denotes information and H denotes information entropy.

secrecy is illustrated in figure 2.1: the mutual information between the sender and receiver, independent of any mutual information with the eavesdropper, must be greater than zero, i.e.,

$$I(A : B|E) > 0 \tag{2.16}$$

where $I(A : B|E) = K$. It is equal to say that Alice and Bob wish Eve's knowledge of K to be fractionally small:

$$I(E : K) < \epsilon \tag{2.17}$$

It is these objectives that a cryptographic method is aspiring to.

2.1.5 Definitions

The key concpets have been introduced, however a few formal definitions regarding communications are required before continuing.

Definition 1: Broadcast Channel

Any broadcast channel between multiple parties can be modeled by some probability distribution $P_{X,Y,Z}$ where X, Y, Z indicates the sequence of bits received by the parties. Whilst this method is applicable to multiple parties this discussion will be restricted to two legitimate parties, Alice and Bob, and one eavesdropper, Eve. X, Y and Z are random variables which take on values from the finite alphabets $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$

Definition 2: Secrecy Rate

The secret key rate between X and Y with respect to Z is denoted as $S(X : Y||Z)$ and is the maximum rate, R at which the parties Alice and Bob can agree on some secret key, S, whilst the rate at which Eve obtains information is arbitrarily small. Hence for every ϵ greater than zero, there is a protocol for a sufficient number of repeats, N, achieving $\frac{1}{N}H(S) \geq R - \epsilon$.

Definition 3: Secrecy Capacity

In a broadcast channel $P_{YZ|X}$ the secrecy capacity $C_s\left(P_{YZ|X}\right)$ is the maximum rate at which Alice can reliably send information to Bob such that the rate at which Eve obtains information is arbitrarily small. C_s is the max bits-per-use of the channel which Alice can send to Bob in secrecy, defined as:

$$C_s = \max R \tag{2.18}$$

It is the maximal rate R for which (for every $\gamma > 0$ and for all sufficiently large N) there exists an encoding function

$$e : \{0,1\}^K \rightarrow \mathcal{X}^N \tag{2.19}$$

where

$$K = \lfloor RN \rfloor \tag{2.20}$$

together with a corresponding decoding function

$$d : \mathcal{Y}^N \rightarrow \{0,1\}^K. \tag{2.21}$$

A deterministic encoding function $e(V)$corresponds to a binary code of length N with 2^K codewords. Where for some $x = e(V)$ and for V uniformly distributed over $\{0,1\}^K$ the following two conditions are satisfied

(a) $P[d(Y) \neq V] < \gamma$, where $X = e(V)$

(b) $H(V|Z^N)/K > 1 - \gamma$

It is equivalent to require the two conditions to hold for all probability distributions. A lower bound in the secrecy capacity can be given by the secret key rate. Logically, the key rate cannot be greater than the capacity of the channel to provide secrecy. An upper bound in the secrecy capacity can be given by the maximal mutual information between Alice and Bob. This could be either $I(X : Y)$ or $I(X : Y|Z)$, whichever is minimal:

$$\max_{P_X} S(X : Y||Z) \leq C_S \leq \min[\max_{P_X} I(X : Y), \max_{P_X} I(X : Y|Z)]. \tag{2.22}$$

[1]

[1] It is possible for $I(X : Y) < I(X : Y|Z)$. the example given in (Maurer, 1993) uses the case where X and Y are independent, binary and symmetric ($P(X = 0) = P(Y = 0) = \frac{1}{2}$) but $Z = X + Y (\mod 2)$. Thus $I(X : Y) = 0$ but $I(X : Y|Z) = H(X) = 1$

2.1.6 Properties of a Simple Broadcast Channel

To understand future protocols it is necessary to understand first the simple broadcast channel. A set-up where a source sends sequences X,Y,Z to Alice, Bob and Eve. This 'discrete memoryless channel' is dealt with by Csiszar and Korner in (Csiszar & Korner, 1978).

The following statement was proved in (Csiszar & Korner, 1978), and is repeated here:

$$C_S = \max_{P_{UX}}[I(U;Y) - I(U;Z)] \tag{2.23}$$

where U is a probability distribution taking on values from some arbitrary set $\mathcal{U}$. Since $U = X$ is a legitimate choice it follows then that

$$C_S(P_{YZ|X}) \geq \max_{P_X}[I(X:Y) - I(X:Z)] = \max_{P_X}[H(X|Z) - H(X|Y)] \quad . \tag{2.24}$$

Clearly C_S is 0 if $I(X:Y) = I(X:Z)$. For secrecy to exist in this situation it is required that there is more mutual information between X and Y than between X and Z.

Further Defining the Broadcast Channel

In this broadcast situation one can now model the channels as binary symmetric and independent of each other. For simplicity this discussion moves away from the central broadcast view and considers the case that there is a channel between the two legitimate parties, and an additional channel between the sender and the illegitimate receiver. The channel from Bob to Alice will have bit error probability ϵ and Eve's channel will have bit error probability δ. In mathematical terms this means that:

$$P_{Y|X}(y|x) = \epsilon \text{ if } x \neq y \tag{2.25}$$

$$P_{Y|X}(y|x) = 1 - \epsilon \text{ if } x = y \quad . \tag{2.26}$$

Without loss of generality it can be assumed that $\epsilon, \delta \leq \frac{1}{2}$. To distinguish this from other probability distributions, and to keep in line with the notation in (Maurer, 1993), let this probability dsitribution be called $D(\epsilon, \delta)$.

Properties of the Binary Symmetric Channel

Since these channels are binary symmetric then the binary entropy function can be applied:

$$h(p) = -\log_2 p - (1-p)\log_2(1-p) \tag{2.27}$$

it follows then, that

$$C_S(D(\epsilon,\delta)) = \begin{cases} h(\delta) - h(\epsilon) & \text{if } \delta > \epsilon \\ 0 & \text{otherwise.} \end{cases} \tag{2.28}$$

The proof for this can be found in (Maurer, 1993).

2.1.7 Broadcast Channel with Feedback

Having defined a simple broadcast channel examine what happens to the properties if public, insecure, error-free feedback is allowed. Eve will be able to observe all messages in the public domain as well as her usual Z outputs. The channel capactiy for this modified situation will be denoted $\hat{C}_S(D(\epsilon,\delta))$.

An Examination of the Channel Capacity

Suppose Alice sends some random bit X over the original broadcast channel, such that $P_X(0) = P_X(1) = 0.5$. The error in the receipt of the bit is independent of P. The error in the bit that Bob receives call E and the error in the bit Eve receives call D. Thus $Y = X + E$ and $Z = X + D$. So far this is identical to the previous channel set up: $P(E = 1) = \epsilon$ and $P(D = 1) = \delta$.

Now suppose that Bob wishes to send some V back to Alice. He sends $W = Y + V = X + E + V$. Alice calculates $W + X = V + E$ (by binary addition) and 'receives' V with E.

Eve now knows: $Z = X + D$, $W = X + E + V$ and, if she tries to extract V then $Z + W = V + E + D$. This is equivalent to a cascaded channel.[1]

The probability that Eve has a bit error in V is given from the probability that only and exactly one of E and D is a bit flip.

$$P(\text{Eve has a flipped bit}) = P(f) = \epsilon(1-\delta) + \delta(1-\epsilon) = \epsilon + \delta - 2\delta\epsilon \tag{2.29}$$

[1] No information is lost by Eve from computing $Z + W$ see (Maurer, 1993) for proof.

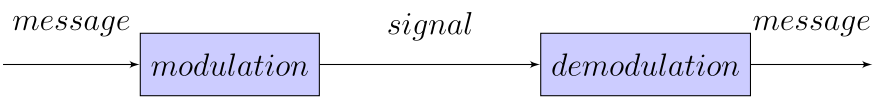


Figure 2.2: Telecommunications protocols must include transformations in to and out of the physical layer. This is done with modulation.

This can be used to transmit key, so this gives a lower limit for $\hat{C_S}$ by calculating $H(Y|Z) - H(Y|X)$:

$$\hat{C_S}(D(\epsilon, \delta)) \geq h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon). \tag{2.30}$$

Since an upper bound on $\hat{C_S}$ can be given by equation 2.22 and $I(X : Y|Z) = H(Y|Z) - H(Y|X, Z) = H(Y|Z) - H(Y|X)$ (where the last equality follows from channel independence). $H(Y|Z) - H(Y|X)$ is maximised for $P_X(0) = P_X(1) = \frac{1}{2}$ giving the result that:

$$I(X : Y|Z) = h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon), \text{ for } P = \frac{1}{2} \quad . \tag{2.31}$$

This is the upper bound, but is also equal to the lower bound from 2.30 so

$$\hat{C_S}(D(\epsilon, \delta) = h(\epsilon + \delta - 2\epsilon\delta) - h(\epsilon). \tag{2.32}$$

given that X and Y are statistically independent, and Z does not uniquely determine X.

Note also, that (for $0 \leq x \leq \frac{1}{2}$) $h(x)$ is monotonically increasing. Thus $h(\epsilon + \delta - 2\epsilon\delta) \geq h(\epsilon)$ with equality if and only if $\delta = 0, 1$ or $\epsilon = \frac{1}{2}$.

2.2 Telecommunications

A typcial telecommunications infrastructure follows the transformations illustrated in figure 2.2. where *modulation* and *demodulation* are in phase space (contrary to the frequency and amplitude modulation of older procotols). This is called phase shift keying ('PSK').

In loose terms, wireless telecommunications devices send information to each other based on creating a 'spot' in IQ space. IQ space is equivalent to phase space with the x-axis as the 'in phase' component and the Q as the 'quadrature' component. Satellite communications happen via modulation in this space. This can be either amplitude modulation (AM), or phase shift keying (PSK). This corresponds to modulation in the radial axis and direction of changing angle in an IQ diagram, respectively. For any given communication, these diagrams can be called 'constellations', and each individual spot indicates the piece of information which is being sent. These are then mapped to a binary label. Examples of these include QPSK which sends a 'spot' in each quadrant, BPSK which is just a binary division between positive and negative I, and QAM which has the same constellation diagram as QPSK.(Heath, 2012). To phase shift, the phase space is categorised into several domains depending upon the desired density of communication - binary and quadrature are common (BPSK and QPSK respectively), but 8- 16- and further PSK is not uncommon.

A diagram depicting the I and Q measurements on respective coordinate axes indicates the phase and amplitude of the signal, and is called a constellation diagram. QPSK can be depicted easily on a constellation diagram as each quadrature is a separate domain.

Each domain is assigned a specific 'Gray coding' for bit relationships as shown for the binary and quadrature distributions in figure 2.3. This can be thought of as a phase modulated signal, sliced in phase and bits assigned accordingly.

Density of slicing can be increased as error rates allow. A noisy signal results in a more spread out received signal in the constellation diagram. Bit flips occur when a signal is received in a domain that it was not sent in. This can happen when the noise in the constellation is high. Many error correction protocols (commonly 'turbo codes') exist to combat this and are very successful to a high degree of attenuation, at around 80 dB two domains of BPSK can still be identified on a satellite modem (loaned to the project courtesy of Airbus Defence and Space) as shown in figure 2.4.

Other common protocols exist including those modulated in amplitude as well as phase (for example, 4QAM and 16QAM). However, these are not practical in satellite communications which is the main focus of this work, as amplitude dependence breaks down at the high losses of satellite signals.

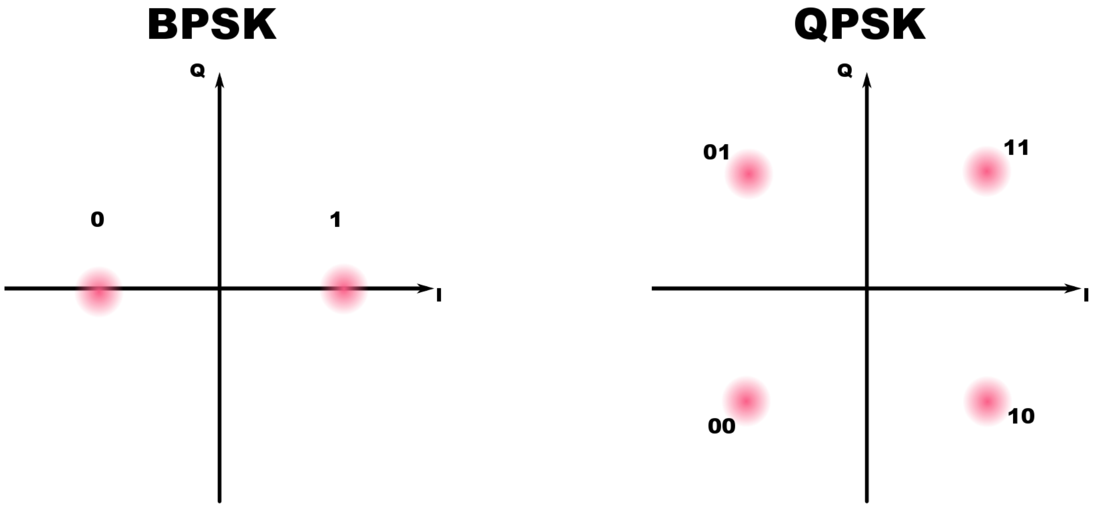


Figure 2.3: An example of BPSK and QPSK. Note that the axis I and Q used in the telecommunications industry are equivalent to the p and q notation common in quantum optics. This is called a constellation diagram

Aside from the actual transmission there is some processing enveloping it. The data to be sent (the source) undergoes compression, channel encoding, symbol mapping, constellation mapping, pulse shaping (filtering the pulse so its distribution over the bandwidth adds maximum tolerance to the system) and digital to analogue conversion. These last four parts formulate modulation. The channel consists of an analogue front end, the propagation channel, and an analogue front end at the receiver. It is in the channel where noise distorts the signal and errors are introduced. The receiver demodulates the signal and makes decisions about the meaning of the signal, decodes the now digital sequence of data, applies decompression and is left with the final data string- the sink. Should post-quantum key distribution work for widepsread application it is in this structure that it would need to fit for maximum efficency.

Simulation

To make things simple this section shall look only at one quadrant of QPSK, the +I, +Q quadrant, equivalent to a {1,1} constallation mapping. Normally in communication a single spot in this quadrant is sent several times, then depending

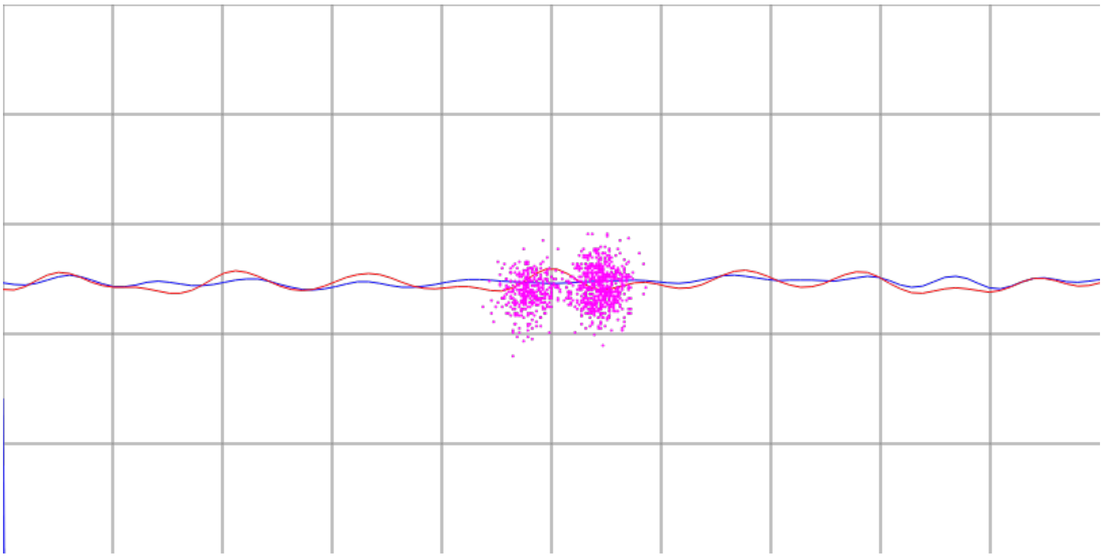


Figure 2.4: This is a raw example of a BPSK protocol, whereby the two domains are close (due to attenuation) but independent domains of phase shifting can be identified at 80 dB loss. This is owing to error correction protocols in the hardware used (provided by Airbus Defence and Space). This diagram is a screen-shot of the software provided with the Airbus modems. The x- and y axes are the normalised in-phase and quadrature-phase measurements of the incoming signal. Upon detection the signal is split in two and a 90° phase transformation applied to one half - the oscilliscope trace of these is imposed on the diagram as the red and blue lines.

upon the noise of the signal ‘spots’ are received in a Gaussian distribution around the original, as the noise increases the uncertainty. However what is actually required is to declare the sending of a particular spot, then have some uncertainty in *what is actually sent*. For a typical transmission Alice sends

$$\alpha(I+Q) \tag{2.33}$$

where $\alpha = 1$ or some constant. If Alice makes α a Gaussian variable centred about a mean $\bar{\alpha} = 1$ she can introduce the uncertainty that she requires into the transmission. A possible way to do this is using the inverse error function, ϕ^{-1}:

For a random number x which is uniform on the interval $[0, 1]$

$$\phi^{-1}(x) = \sqrt{2}\,\mathrm{erf}^{-1}(2x-1) \tag{2.34}$$

The mean of the distribution this produces is centred on 0, so a simple solution is to convert α using this property:

$$\alpha = 1 + \phi^{-1}(x) \tag{2.35}$$

$$\text{where } x = \text{ random number, } 0 \leq x \leq 1$$

After this has been transmitted and received by two seperate receivers, which each add a different Gaussian noise distribution onto the transmission, there are two data sets which will be used for the next stage in simulation.

2.3 Combining Post-Quantum Key Distribution with Telecommunications

Symmetric key creation has the purpose of encrypting messages, so it would become a part of the encryption/decryption segment of the system. However to execute this it in general requires use of other parts of the system. This implies that the simplest way for implementation requires an intial exchange with the receiver before commencing the sending of the intended message. A simplified process, modified from the current standard communication procedure could look like this: Source, channel code, modulation, noisy propagation, demodulation, channel decoding, sink, where source and sink are strings of random numbers.

Error correction is typically turbo code in most current communications systems. At its most basic level turbo code adds redundancy to correct channel errors. More specifically it convolves data with impulse response filters and randomly interleaves the results. This is very different to the cascade system proposed later in this thesis, and the positives and negatives of each type have yet to be considered. Another feature which may benefit from some consideration is pulse shaping. Pulse shaping is to reduce the effects of noise in the system, but noise is actually benefical to the key, so a balance will have to be found.

A particular benefit of the current procedure is the receiver's ability to make either 'hard' or 'soft' decisions. This occurs during the detection of a signal as a point on a symbol map, and the interpretation of what this point represents on that symbol map. A hard decision simply interprets the symbol purely based on its location- if it is in the area designated as {1,1}, for example, then the point is assumed to be 1,1. A soft decision processes the incoming signal and decides the probability of being in the correct location for the symbol it was intended to represent, often by comparing repeated signals. The soft decision mechanism allows for the receiver to get a potentially higher yield for matches when implementing symmetric key distribution.

As a conceptual interpretation of the process for key generation, consider the following. Alice sends a series of symbols. Any individual symbol will be initially represented as a specific point, however during sending, the noise transforms this specific point into a probability distribution over its local region, meaning that it will ultimately be detected as a different exact point. This will be a different exact point for both Eve and Bob. They make a soft decision on where this point is supposed to represent, which will be right for most of the time, but not all of the time. The correct decisions will not be identical for both Bob and Eve due to the randomness of noise. The points with correct decisions can be used to generate the symmetric key.For further consideration of the methods of eavesdropping consider the simplest case of a standard wire tap channel, as that outlined by Wyner in 1975(Wyner, 1975). This set up has the properties that it consists of channels along which continuous signals are sent, which are Gaussian modulated according to the information that is being sent.

2.3.1 Wiretap

One of the most basic hacks of a cryptographic system that can be imagined is a simple 'wiretap' hack.In a wiretap model Alice will create her signal, send it to Bob, who will receive it with the addition of some noise. This will look like:

$$Y^{1,2,...,n} = R^{\otimes n} \oplus \{\beta_i, ..., \beta_{i+n}\} \tag{2.36}$$

in the case of Bob. In the case of the eavesdropper, Eve, it will look like:

$$Z^{1,2,...,n} = R^{\otimes n} \oplus \{\varepsilon, ..., \varepsilon + n\} \tag{2.37}$$

In a continuous Gaussian based wiretap model, Alice is sending a string of random variables, with a probability distribution denoted by equation 2.3. Bob receives this string of random variables where each Y^i has its own Gaussian distribution, $p(y)$ centred on the expected value of the $p(x)$ that Alice sent. Additionally, Eve receives a string of random variables where each Z^i has its own Gaussian distribution, $p(z)$ centred again on the expected value of the $p(x)$. It is important to note that, since $\beta \neq \varepsilon$, then $Z^{1,2,...n} \neq Y^{1,2,...,n} \neq X^{1,2,...,n}$. This basic model has the benefits that Eve has unavoidable noise, and even in the perfect channel limit she has quantum shot noise. An intercept-resend hack is also detectable- the noise added in this process will be distinguishable from β. However, the downfall of this model is that it does not adequately represent the physical systems which one uses realistically. In all experimental situations Alice will have some noise α which she will create from the desired signal input to the generated signal.

3

Protocol

Having outlined some of the key concepts required for integrating cryptography with telecommunications, the next stage is to examine how this integration could be performed. This chapter presents a proposal for integration, and then examines in more detail some of the processes required, ending with some considerations on the character of the wireless signals.

3.1 Novel Contributions

This chapter examines in detail work by Maurer, the 'advantage distillation algorithm', complete with mathematical rigour which highlights a correction to Maurer's work. This algorithm rarely features in the quantum cryptography community, despite the majority of proposed QKD protocols relying upon this work. This chapter also examines a variety of commonly used principles - slicing, information reconcilliation and privacy amplification. However, the novel work in this chapter brings all these components together, along with an understanding of telecommunications protocols, to provide a framework for integrating quantum-safe key distribution with existing infrastructure. This combines two fields of work in an innovative way, and the proposal to combine all these features in novel.

3.2 Proposed Method

The method proposed for integrating key distribution with a telecommunications is based upon a key algorithm - ‘Advantage Distillation’. This algorithm takes some noisy data and extracts from it the parts which are mutual to both the sending and recieving parties. It will be shown that, assuming any eavesdropper has some noise separate to the receiver’s noise, this provides secrecy. Surrounding this implementation, however, the following steps must be executed.

(a) The parties intending to communicate securely, Alice and Bob, authenticate each other’s identity. (The problem of achieving this is not dealt with in this thesis, and it is merely assumed to be possible. One can suppose some trusted certifying authority, or some hashing with a previously agreed i.e. face-to-face key which is then chained forwards in all subsequent communications.)

(b) Alice and Bob communicate with each other using a phase shift keying (PSK) protocol - the phase of the signal is being monitored closely with PSK.

(c) Alice generates a series of random bits which she assigns to some value of Gaussian modulation in amplitude.

(d) Within each domain of PSK that Alice sends, the signal is Gaussian modulated in amplitude according to the bit string Alice generated. This ‘sub-level’ modulation means that key distribution can be performed alongside the general communications.

(e) Bob recieves the PSK and measures the Gaussian modulation in amplitude.

(f) This signal is then discretised by Bob, a process known as slicing.

(g) The resultant bits are used to perform ‘advantage distillation’ between Alice and Bob.

(h) The previous steps have not distilled a perfect key - information reconciliation is performed to correct errors.

(i) The resultant key material is privacy amplified to produce a key.

(j) The key is then used in a one-time pad-like scheme and the key is refreshed accordingly.

3.2.1 Encoding

There are two ways to integrate this with existing communications. One efficient way would be to super impose this with an ongoing communication. For example:

- Alice prepares some arbitrary message for Bob (possibly part of the conversation they are already having), for example, 'Hello World', encoded appropriately to some series of '1's and '0's.
- Alice sends this to Bob according to the standard Gray coding.
- Within each domain of the Gray encoding, Alice sub-modulates the domain in either phase or amplitude.
- The sub-modulation is according to a Gaussian distribution, with the distribution sliced to a density appropriate to the communication parameters.
- The resultant signal is received and sliced by Bob, within the separate domains of Gray encoding
- This is equivalent to super-imposing a standard CVQKD protocol, such as those in (Usenko & Grosshans, 2015; Weedbrook *et al.*, 2010).

Another method of encoding would be to take the PSK protocol and operate it in the limit of near indistinguishability. A standard PSK communication which has been attenuated such that there are significant numbers of errors:

- Alice prepares some random numbers, and encodes them in binary
- Alice sends these with the appropriate Gray coding, but at a high attenuation level, such that the domains overlap and generate errors.
- Bob receives this and the slicing step is equivalent to distinguishing the domains of the Gray encoding.

Semantically speaking, the only difference in these implementations is whether or not the slicing is defined be Gray coding domains, or within the domains by some other sub-divisions, as discussed in the next section. Which encoding is preferred is likely unique to the circumstances of the communication. Further work is required to establish the optimum yield from using each of these encodings in different implementation scenarios.

3.3 Slicing

In order to transform the continuous variable into a series of bits as required for a key, the signals must be digitised. Imagine a 'spot' of a PSK transmission, which has been modulated in amplitude, this already has a Gray coding bit assignment, and this will remain for the purposes of ordinary communications. However one can assign an *additional* bit code for sliced-up sections of the recieved spot itself, which can be simulataneously utilised for key distillation. How this is divided up is outlined in this section. The process of division into bits is called slicing and is crucial to the protocol - it is here that noise will be added to the system, which is imperative in order that an eavesdropper will remain ignorant of the distributed key. Note that the process of slicing outlined here is often referred to as quantisation in the communications community. The term has been avoided here to maintain compatability with the quantum cryptography community's use of the term slicing and to avoid confusion with quantisation - the transition of a classical model to a quantum model.

3.3.1 Method

Consider a continuous variable with a probability distribution $p(x)$. To convert this into a digital, binary describable string, it must be mapped onto one such string in some way. One can use a form of mapping based upon slicing the continuous variable into divisions of two. This is done by defining a limiting point, usually at the mean of the distribution, beyond which any points are assigned a 1 and prior to which any points are assigned a 0. This assigns each data point a binary string of unit length 1. Each side of the limit point of the distribution is a 'slice'. For a longer and more accurate binary string each slice of the distribution can then be split into as many slices as required and each assigned an appropriate binary value (e.g. 00,01,10,11 for 4 slices). This gives a mapping to the integers $[0, ..., 2^n - 1]$ where n is the number of divisions made.

Obviously the greater the number of slices the greater the accuracy in the mapping of the variable to a binary string. Figure 3.1 shows a basic slicing of data points in an exchange between Alice and Bob. The example of a single quadrant of QPSK which has been amplitude modulated has been used for illustrative purposes.

Data points are sliced twice. Once at the point of sending - if Alice intends to send a 000 with the slicing method in figure 3.1 she will send a point with smaller amplitude. Then once at the point of receipt when it is measured by Bob. Alice has a string of Gaussian variables, $X^{(1,2,...,n)}$, which she sends to Bob. Bob recieves a string of Gaussian variables, $Y^{(1,2,...,n)}$, where

$$X^{(1,2,...,n)} + \delta^{(1,2,...n)} = Y^{(1,2,...,n)} \tag{3.1}$$

and δ represents some small amount of noise that has been introduced in the communication channel(Assche *et al.*, 2004). In the process of slicing, each X^i has been mapped to an n bit string (sliced n times) $S_{1,2,...,n}(X^i)$. In the example of figure 3.1 $n = 3$. Clearly, as Bob does the same, dependent upon the value of δ for each point, he will have errors in his bit strings $S_{1,2,...,n}(Y^i)$ with respect to Alice.

An eavesdropper who performs the measurement will also recieve some errors with respect to both Alice and Bob - the eavesdropper will recieve a string of Gaussian variables $Z^{(1,2,...,n)}$ where

$$X^{(1,2,...,n)} + \epsilon^{(1,2,...n)} = Z^{(1,2,...,n)} \tag{3.2}$$

and ϵ represents the noise introduced either from measurement or from the channel.

The probability of recieving a bit error is related to the Helstrom bound - the probability that something sent as one state is recieved as another state based on the indistinguishability of two Gaussian distributions (Helstrom, 1976). An

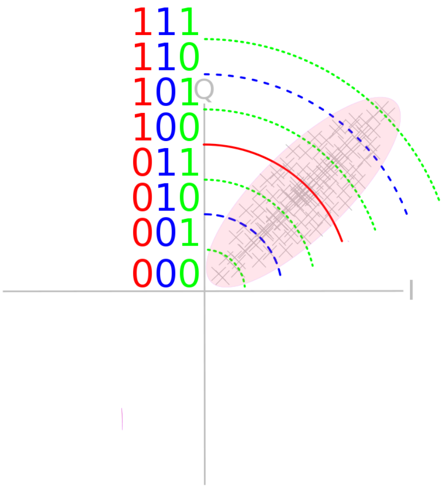


Figure 3.1: The slices of data are labelled as a bit string according to the position of the slice. With the first slice (red), data points either side were labelled as a 0 or 1. This label remains and the next bit in the string was labelled 0 or 1 according to the position in relation to the second, blue slice. This process is then repeated for the third, green slice.

example of this in action can be seen in figure 3.2. As Bob will have some deviation in what he has detected from the sender, then some reconciliation must take place. This is dealt with in future sections.

3.3.2 Practical Notes on Slicing

During the investigations an interesting practical note on data slicing emerged. This applies to any continuous variable broadcast, which must undergo a transition into classical variables.

The simplest method of slicing is to take the mean of all the received values with any above the mean becoming a binary 1 and anything below becoming 0. It is however possible to increase key production rates by instead of dividing the received data in half, divide it into four ‘bins’, slicing more thinly. This requires each bin to be labelled by two digits, 00, 01 etc. This however raises its own set of problems, as the different positioning and labelling of the bins will affect the security of the transmission by different amounts.

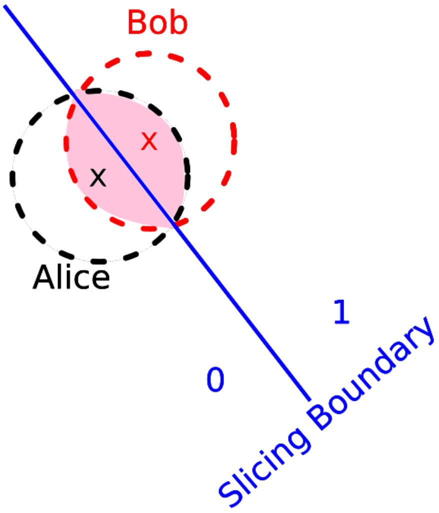


Figure 3.2: Alice sends some point (marked in black as 'x') which has some associated noise (Gaussian distributed), outlined in a black dashed line. It is possible for Bob and Eve to measure this at any point in this black dashed line. For example, Bob may measure at the point 'x' in red. His best guess is to assume that this originally came from anywhere within the red dashed line. The shaded area is the Helstrom bound and it is the point at which any two overlapping Gaussians cannot be distinguished from each other. This instance demonstrates how a point may be incorrectly sliced and given the incorrect bit designation.

If splitting into more than two bins, there are two main methods of bin positioning: using an equal bin width so that the bins are equally spaced on the x-axis; and using an equal bin probability, so that the same number of received points fall into each bin. In the case of Gaussian distributed data, this causes a spatial bunching of bins around the mean. The two main numbering systems are the standard binary system e.g. for four bins 00, 01, 10, 11, and Gray coding where adjacent bin labels differ only by one bit, i.e. for four bins, 00, 01, 11, 10.

For each method, the classical information shared between Alice, Bob and Eve is different, even when derived from the same quantum information. This means that some methods are more secure than others. Unfortunately, the security of each method also changes with channel transmission, with different methods being optimal at different channel transmissions. In general, however, slicing to fewer bins is preferable, as is using Gray coding and bins of equal probability at higher transmissions, as Alice and Bob share a high amount of information these methods cause small errors in transmission to become small errors in the resulting string.

Overall the recieved values have a binomial noise distribution which tends to Gaussian at the high slicing limit.

3.4 Distilling a Key

Having sliced the data into bit strings with some errors, the parties must come to a mutual agreement on the content of the bit strings in order to use them for a key. Using the advantage distillation algorithm is the first step for this. The purpose of advantage distillation is to create data sets which have been refined to minimise errors. The protocol sifts through data to locate areas where Alice and Bob do not agree and modify them without revealing the original data to an eavesdropper. This is enabled by the addition of noise. Consider a random bit, Q, which is randomly chosen by the sender, Alice. Alice sends this to Bob, N times along her channel, A.

$$[Q \oplus X_1, Q \oplus X_2, \cdots, Q \oplus X_N] \tag{3.3}$$

To attempt to recover Q, Bob can then check it with his variable, and see if he recovers an exact match N times.

$$[(Q \oplus X_1) \oplus Y_1, \cdots, (Q \oplus X_N) \oplus Y_N] \tag{3.4}$$

If Bob recieves either $[0, 0, \cdots 0]$ or $[1, 1, \cdots 1]$, he accepts Q, and records his choice. He then tells Alice of his decision, who also accepts it.

The bits, Q_i can then be used to modify a new Q and repeat the process to increase the number of matches, until a key is reached from Q. This, however, can leak information. Alternatively, the bits, Q_i can be saved, and some error correcting protocol implemented to create a key from Q.

This process is post selection by advantage distillation.

Requirements and their Purpose

Before distillation can occur, the participating parties must first have recieved a mutual signal. That is to say that both (or all) legitimate parties share information which differs from each other only by some quantity of noise. This can be in the form of a signal sent from a central source to all parties; alternatively from a party broadcasting their information to the other parties. These two options are semantically the same.

This initial message would be sent out bit by bit, with each bit being transmitted at least twice, or more times according to the desired yield and security. Afterwards all parties will hold a list of bits differing from the original signal by some number of noisy bits. The repeats allow the holders to make an informed guess at the original sent bit.

The Advantage

Since the discarding of the seemingly incorrect bits is within the control of one of the legitimate parties this means that this party gains an advantage over any illegitimate participants. For a large enough starting set the illegitimate participants will have un-identifiable guesses remaining in their bit set after discarding bits according to the matchlist which is sent out publicly.

An Example

Having painted a picture of the set-up, an example is now presented. Say Alice generates some random number set, R. She sends this number set, combined with some noise. For simplicity the XOR function is used to represent this. She sends $R \oplus N_A$ Bob receives this number set combined with his own noise giving $R \oplus N_A \oplus N_B$. Similarly, Eve receives $R \oplus N_A \oplus N_E$. To see why this is useful, examine what happens in an example where $R = \{0, 0, 0, 0\}$ is chosen.

Alice generates $R = \{0, 0, 0, 0\}$. She combines this with some noise, $N_A = \{0, 0, 0, 1\}$, giving $R \oplus N_A = \{0, 0, 0, 1\}$ and sends it to Bob. Bob receives this and combines it, for example, with local signal noise which will also be a noisy version of R. He has three options

(a) $N_B = N_A$

(b) $N_B = \bar{N_A}$ [1]

(c) $N_B \neq N_A, \bar{N_A}$.

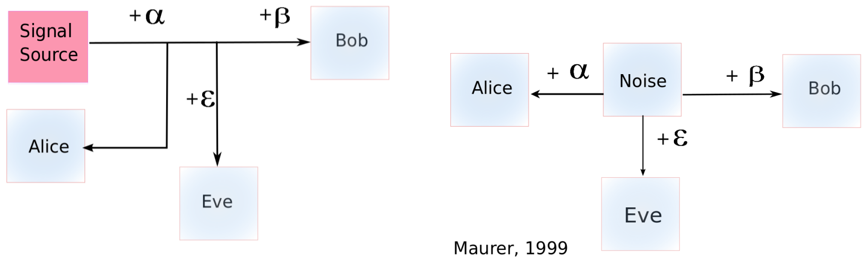
Examine (c) first- choose $N_B = \{1, 0, 1, 0\}$. This gives $R \oplus N_A \oplus N_B = \{1, 0, 1, 1\}$. This result does not give $\{1, 1, 1, 1\}$ or $\{0, 0, 0, 0\}$ so results of this nature are excluded.

Next, examine case (a), $N_B = N_A$. Hence, $N_B = \{0, 0, 0, 1\}$ and $R \oplus N_A \oplus N_B = \{0, 0, 0, 0\}$ this result is not trivial, and Bob has managed to procure the original R, although he knows only that he has R or $\bar{R}$

Similarly, in case (b) $N_B = \{1, 1, 1, 0\}$ yields $R \oplus N_A \oplus N_B = \{1, 1, 1, 1\}$. Again, this result is non trivial and Bob knows he has either R or $\bar{R}$. He computes this value for each element he receives from Alice and alerts her to the components which produced case (c), which they both dispose of.

Variations on this process exist. Firstly, at the end of this first run, Alice and Bob can either repeat the same process to find R more exactly or they can use alternative error correcting protocols. An advantage of running a number of repeats of this advantage distillation process is that it can be mathematically

[1] $\bar{N}$ indicates 'NOT' meaning each 0 is exchanged for a 1 and vice versa



Maurer, 1999

Figure 3.3: A schematic diagram outlining the communication channels between sender (Alice) and receiver (Bob), and a potential eavesdropper (Eve). α, β and ε represent noise. The two schematics are semantically identical, however the ‘mutual reconciliation’ implementation (left) is a more practical implementation of the noisy broadcast theory (right) as found in (Maurer & Wolf, 1999).

modeled and hence simulated key can be found (Maurer & Wolf, 1999), however, this has to be balanced with possible information leakage.

To summarise, Alice and Bob mutually agree a signal that has been derived jointly from R and their local noise. This signal is provably different to R and is therefore unconditionally secret.

3.4.1 The Simulation Process

A pseudo code implementation is provided here for clarity. This involves an 8 bit comparison and uses conventional notation for demonstration[1].

(a) Alice and Bob both create arrays of biased noise. This is in lieu of a shared

[1] The notation $+\leftarrow$ is used to indicate ‘append to array, $\equiv$ denotes that the single bits must have equality, whereas $==$ denotes that the whole string or array must have equality; $=$ has the usual meaning and is used for general cases. ’Random’ indicates a random number generated from a reliable random number source. Currently, pseudo-random number generators will suffice. Each array element is 1 bit long.

signal with noise.

```
while length(Noise_A) and length(Noise_B) < 8L do
    Noise_A + ← Randombit AND Randombit;
    Noise_B + ← Randombit AND Randombit;
end
```

(b) Alice makes an array, $Seed_A$ filled with random numbers:

```
while length(Seed_A) < L do
    Seed_A + ← Randombit;
end
```

(c) $Seed_A$ and $Noise_A$:

```
while length(Transmit) < 8L do
    for Transmit[i] to Transmit[i + 7] do
        Transmit + ←(Noise_A[i] XOR Seed_A[m]);
        j++;
    end
    m++;
end
```

(d) During a simulation the sending takes place via reuse of the 'transmit' array. During active exchange this will be via email, radio, wifi, bluetooth or any other channel

(e) Bob creates a new array for the one he receives by XOR-ing with noise:

```
while length(Seed_B) < 8L do
    Seed_B + ← element of Noise_B XOR element of Transmit ;
end
```

(f) Bob clears his noise array:

$Noise_B == 0;$

(g) Bob makes his comparisons:

```
while $Length(matchlist) < L$ do
    for $a = 0$ to $a = (8L - 8)$ do
        if $Seed_B[a] \equiv Seed_B[a+1] \equiv \ldots \equiv Seed_B[a+7]$ then
            $Noise_B \mathrel{+}\leftarrow Seed_B[\mathrm{a}]$ ;
            $matchlist \mathrel{+}\leftarrow 1$;
            $a = a + 8$;
        end
        else
            $matchlist \mathrel{+}\leftarrow 0$;
            $a = a + 8$;
        end
    end
end
```

(h) Bob ‘sends’ *matchlist* to Alice:

```
begin
    Send matchlist (according to established protocol)
end
```

(i) Alice clears her array of noise:

$Noise_B == 0;$

(j) Alice examines the matchlist she was sent and uses it to distill her original random numbers:

```
for $i=0$ to $i=8L$ do
    if $matchlist[i] \equiv 1$ then
        $Noise_A \mathrel{+}\leftarrow Seed_A[i]$ ;
    end
    i++;
end
```

(k) $Noise_A$ and $Noise_B$ are now approximately equal.

$Noise_A$ and $Noise_B$ can now be fed into the information reconciliation (error correction) stage of the protocol.

3.4.2 Advantage Distillation

In the situation of advantage distillation, Eve has no information about X and Y other than that which she obtains through Z. For all Eve's knowledge of the universe T, then $I(XY : T|Z) = 0$. Alice and Bob share no secret key initially (not including anything for initial authentication). Eve knows the protocol, but cannot insert fraudulent messages or perform an intercept-resend attack without a change in Alice and Bob's probability distributions. The only assumption made is that Eve has some quantity of unavoidable noise on her detection of the channel.

Each message transmission step is C_i. Alice's messages are $C_1, C_3...$ and Bob's are $C_2, C_4....$ After a t step protocol Alice computes a secret key $S = f(X, C^t)$ where C^t is defined as $[C_1, C_2, ..., C_t]$, and Bob computes $S' = f(Y, C^t)$. S and S' are required to agree with very high probability,

$$P[S \neq S'] \leq \alpha \tag{3.5}$$

and Eve to have very little information about either S or S':

$$I(S; C^t, Z) \leq \beta \tag{3.6}$$

where α and β are small.

Examining the Secret Key Rate for One Way Transmission

The secret key rate must be both positive and non-zero which gives the following theorem:

$$S(X : Y||Z) \geq \max[I(Y : X) - I(Z : X), I(X : Y) - I(Z : Y)]. \tag{3.7}$$

To prove this it needs only work for $I(Y : X) - I(Z : X)$ as the other follows by symmetry.

Let the alphabet $\mathcal{X}$ be:

$$\mathcal{X} = \{0, ..., L-1\} \tag{3.8}$$

for some L. Addition on $\mathcal{X}$ is by modulo L. Alice sends some $V \in \mathcal{X}$ and Bob and Eve receive the respective pairs $[Y, V + X]$ and $[Z, V + X]$. Note that X, Y and Z indicate the noisy channel.

Since the secret key rate can be arbitrarily close to the channel capacity: $S(X:Y|Z) \sim C_S$ and, from 2.22, the channel capacity is lower bounded by:

$$C_S(P_{[Y,V+X],[Z,V+X]|V}) \geq \max_{P_V}[H(V|Z,V+X) - H(V|Y,V+X)]. \tag{3.9}$$

Taking the latter part it can be written as:

$$\begin{aligned} H(V|Y,V+X) &= H(V,V+X|Y) - H(V+X|Y) \\ &= H(V|Y) + H(V+X|VY) - H(V+X|Y) \\ &= H(V+X|VY) \\ &= H(X|Y) \end{aligned}$$

Similarly, $H(V|Z,V+X) = H(X|Z)$. Thus, the term to be maximised in 3.9 is equal to $H(X|Z) - H(X|Y) = I(Y:X) - I(Z:X)$.

Examining the Secret Key Rate with Centrally Broadcasted Bits

Advantage distillation requires the generation of a random bit, R, which is sent a pre-agreed number of times. For this case, for ease of calculation, consider the case where a central power transmits signals to all three parties.

That bit is generated acccording to

$$P_R(0) = P_R(1) = \frac{1}{2} \tag{3.10}$$

and sent over the independent binary symmetric channels. C_A, C_B and C_E with error probabilities ϵ_A, ϵ_B and ϵ_E. The probability distribution is defined by

$$P_{XYZ|R} = P_{X|R}P_{Y|R}P_{Z|R} \tag{3.11}$$

where $P_{X|R}(x,r) = 1-\epsilon_A$ if $x = r$ and ϵ_A otherwise; $P_{Y|R}(y,r) = 1-\epsilon_B$ if $y = r$ and ϵ_B otherwise and $P_{Z|R}(z,r) = 1-\epsilon_E$ if $z = r$ and ϵ_E otherwise.

For binary variables a parameter β_{bc} can be defined over C_A, C_B and C_E:

$$\beta_{bc} = P_{XYZ}(0,b,c) \text{ for } b,c \in \{0,1\} \tag{3.12}$$

This gives the error probabilities:

$$\epsilon_E = \frac{1}{2} - \frac{1}{2}\sqrt{1 - 8\frac{\beta_{01} - 2(\beta_{01}+\beta_{10})(\beta_{01}+\beta_{11})}{1-4\beta_{10}-4\beta_{11}}} \tag{3.13}$$

3.4.3 Optimal Hacking

It follows from the above protocol that in order to find out as much information about Q as possible, Eve should simply calculate

$$[(Q \oplus X_1) \oplus Z_1, \cdots, (Q \oplus X_N) \oplus Z_N] \quad . \tag{3.14}$$

If she calculates that a majority of her received set of bits are '0' then she can presume that Q was indeed '0' and vice versa.

This assumes that:

(a) Eve cannot directly identify Y.

(b) Eve cannot clone X.

This assumption is dealt with rigorously later, however, suppose it to be true for this current model.

Eve has a greater error probability than Bob

Maurer goes on to prove how Eve cannot know Q better than Bob and Alice, a summary of which is provided here. This holds for all Eve channels with $\epsilon > 0$.

The bit error probablity of Alice's channel is α, so let $\alpha_{r,s}(r, s \in 0, 1)$ be the probability that $Q = 0$ is sent by Alice, recieved by Bob as $Q = r$ and recieved by Eve as $Q = s$. There are four possibilities: Bob and Eve are both correct ($\alpha_{0,0}$), Bob and Eve are both wrong ($\alpha_{1,1}$), Bob is correct and Eve is wrong ($\alpha_{0,1}$), Bob is wrong and Eve is correct ($\alpha_{1,0}$).

Focussing first on $\alpha_{0,0}$, this situation could have arisen from one of two possible occurances. The first is that Q remains unchanged:

$$\text{A} \boxed{0} \rightarrow (1-\alpha) \rightarrow \boxed{0} \rightarrow (1-\alpha) \rightarrow \boxed{0} \text{ B}$$
$$\text{A} \boxed{0} \rightarrow (1-\alpha) \rightarrow \boxed{0} \rightarrow (1-\epsilon) \rightarrow \boxed{0} \text{ E}$$

This gives the probability contibution:

$$\alpha_{0,0}^{possibility1} = (1-\alpha)(1-\alpha)(1-\epsilon) \tag{3.15}$$

The second way is that Q is changed in each transmission:

$$\text{A} \boxed{0} \rightarrow \alpha \rightarrow \boxed{1} \rightarrow \alpha \rightarrow \boxed{0} \text{ B}$$
$$\text{A} \boxed{0} \rightarrow \alpha \rightarrow \boxed{1} \rightarrow \epsilon \rightarrow \boxed{0} \text{ E}$$

Which gives the second probability contribution:

$$\alpha_{0,0}^{possibility2} = \alpha\alpha\epsilon \tag{3.16}$$

Putting these together, the probability that both Bob and Eve are correct in receiving Q is:

$$\alpha_{0,0} = (1-\alpha)^2(1-\epsilon) + \alpha^2\epsilon \tag{3.17}$$

Using the same method it follows that for the remaining three possible outcomes, the probabilities are:

$$\alpha_{0,1} = (1-\alpha)^2\epsilon + \alpha^2(1-\epsilon) \tag{3.18}$$
$$\alpha_{1,0} = \alpha_{1,1} = \alpha(1-\alpha) \tag{3.19}$$

If $P_{\alpha,N}$ is the probability that Bob accepts the message sent by Alice (recall that a message is accepted if all N received bits are equal), and β_N the probability that Bob has made an error in accepting the message then

$$\beta_N = \frac{1}{P_{\alpha,N}} \cdot (\alpha_{1,0} + \alpha_{1,1})^N \tag{3.20}$$

that is, Bob's error in accepting the message is the probability of getting an error, divided by the probability that he accepts. Accordingly, substitution from equation 3.19 gives

$$\beta_N = \frac{1}{P_{\alpha,N}} \cdot (2\alpha - 2\alpha^2)^N \tag{3.21}$$

Now, let γ_N be the probability that Eve has made an error in accepting the message. Recall that Eve is choosing to assume that $Q = 0$ if a majority of her results match as 0, and vice versa if the majority of her results match as 1. Note that the only errors which matter are those when Bob has received a complete match, as all other values are discarded. Thus γ_N is dependent upon $\alpha_{0,0}$ and $\alpha_{0,1}$. For ease of calculation, suppose that N is even. Since Eve assumes a value of Q based on having the majority of results equal, it is the probabilities based upon the value of $N/2$ which are important (i.e. Eve does not receive a majority). To account for all the permutations of having the majority of results equal, the binomial coeffient for $\binom{N}{N/2}$ is needed. Again, this factor must all be divided by the probability that Bob accepts, $P_{\alpha,N}$.

Maurer initially includes a further factor of $\frac{1}{2}$ to account for Eve making a random, correct, guess, in the case of not having a majority, However, examination shows this is not necessary as the guesses are statistically independent; so even though Eve may be accidentally 'correct' half of the time, this knowledge is useless to her as she cannot determine the location of the 'correct' results.

To summarise, the expression for γ_N is:

$$\gamma_N \geq \cdot \frac{1}{P_{\alpha,N}} \cdot \binom{N}{N/2} \alpha_{0,0}^{N/2} \alpha_{0,1}^{N/2} \tag{3.22}$$

and the inequality is the result of this being an absolute lower limit in the event Eve happens to guess everything else correctly every time.

Analysis of γ_N can be achieved using Stirling's approximation for binomial coefficients. Stirling's formula states that

$$n!/((n/e)^n \cdot \sqrt{2\pi n}) \to 1\,, \quad n \to \infty \tag{3.23}$$

For sufficiently large even N this gives:

$$\binom{N}{N/2} \geq \frac{1}{\sqrt{2\pi N}} \cdot 2^N \quad . \tag{3.24}$$

Thus, the lower bound for γ_N becomes

$$\gamma_N \geq \frac{1}{P_{\alpha,N}} \cdot \frac{1}{\sqrt{2\pi N}} \cdot 2^N \cdot \sqrt{\alpha_{0,0}\alpha_{0,1}}^N \tag{3.25}$$

$$= \frac{K}{\sqrt{N}} \cdot \frac{(2\sqrt{\alpha_{0,0}\alpha_{0,1}})^N}{P_{\alpha,N}} \tag{3.26}$$

for some positive constant K (Charles H. Bennett, 1995).

In order to understand this in terms of α and ϵ so that it can be compared directly to β_N, substituion from equations 3.17 and 3.18 gives

$$\sqrt{\alpha_{0,0}\alpha_{0,1}} = \sqrt{(1 - 2\alpha + \alpha^2 + 2\alpha\epsilon - \epsilon)(\alpha^2 - 2\alpha\epsilon + \epsilon)} \quad . \tag{3.27}$$

Note that for a $\epsilon = 0$ the right hand side of equation 3.27 reduces to $\alpha^2 - \alpha$. Next, note that for all $\epsilon > 0$, the larger factor (left) decreases by the same amount that the smaller factor (right) increases. Given the assumption that Eve always has noise then

$$\sqrt{\alpha_{0,0}\alpha_{0,1}} > \alpha - \alpha^2 \tag{3.28}$$

which is a lower bound on γ_N. To examine whether the probability that Eve makes an error is greater than the probability that Bob makes an error, an upper bound on β_N is determined as follows:

$$P_{\alpha,N} = p_{\text{Bob correct}} + p_{\text{Bob incorrect}} = (2\alpha - 2\alpha^2)^N + (1 - 2\alpha + 2\alpha^2)^N$$
$$(1 - 2\alpha + 2\alpha^2)^N \leq p_{\alpha,N} < 2 \cdot (1 - 2\alpha + 2\alpha^2)^N$$

If the statement

$$(1 - 2\alpha + 2\alpha^2)^N \leq P_{\alpha,N}$$

is substituted into equation 3.20 it follows that

$$\beta_N \leq \left(\frac{2\alpha - 2\alpha^2}{1 - 2\alpha + 2\alpha^2}\right)^N. \tag{3.29}$$

To summarise so far, the probability of Bob's error is $\beta_N \leq b^N$ where

$$b = \frac{2\alpha - 2\alpha^2}{1 - 2\alpha + 2\alpha^2}.$$

To put Eve's error, γ_N, into a comparable format, $\gamma_N \geq c^N$, some manipulation is required:

$$\begin{aligned} \gamma_N &\geq \frac{K}{\sqrt{N}} \cdot \frac{(2\sqrt{\alpha_{0,0}\alpha_{0,1}})^N}{p_{\alpha,N}}, \\ (1 - 2\alpha + 2\alpha^2)^N &\leq p_{\alpha,N} < 2 \cdot (1 - 2\alpha + 2\alpha^2)^N, \\ \gamma_N &\geq \frac{K'}{\sqrt{N}} \cdot \frac{(2\sqrt{\alpha_{0,0}\alpha_{0,1}})^N}{(1 - 2\alpha + 2\alpha^2)^N}. \end{aligned}$$

This allows for

$$c = \frac{2\sqrt{\alpha_{0,0}\alpha_{0,1}}}{(1 - 2\alpha + 2\alpha^2)} - \delta \tag{3.30}$$

where δ can be made arbitrarily small. Finally, given equation (3.28), it is easy to see that $c > b$ provided that δ is sufficently small. Combined, this shows that there exists positive constants, b and c, with $b < c$, such that $\beta_N \leq b^N$ and $\gamma_N \geq c^N$. Thus, Eve clearly has a greater error probability than Bob when she tries to guess Q. However, this is not equivalent to there being secrecy in the channel between Alice and Bob. This is discussed in the following section.

Positive secret key rate

To determine whether the above protocol has a positive secret key rate, i.e.

$$S(X;Y||Z) > 0 \tag{3.31}$$

an inspection of the Shannon entropy and mutual information is executed. Figure 2.1 illustrates the topography of information and the area which is required to be positive in order to prove the existance of secrecy. It is sufficient to show that the mutual information betwen Alice and Bob is greater than the mutual information between Alice and Eve, although it is not a necessary condition, proofs of which can be found in (Charles H. Bennett, 1995; Maurer, 1993; Maurer & Wolf, 1999).

To show this, the random variables of $\hat{X}, \hat{Y}$ and $\hat{Z}$ are introduced. These variables are constructed from X^N, Y^N and Z^N where, if Bob accepts, $\hat{X} = C$ and $\hat{Y} = C'$ and if Bob rejects, $\hat{X} = \hat{Y} =$ "reject". As Eve must collect her informaton over all messages then $\hat{Z} = [Z^N, V]$ where V is the collection of all public messages. Hence, if the inequality

$$I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z}) > 0 \tag{3.32}$$

holds, then a positive secret key rate exists.

The entropy for the bit C conditional on C' can be determined fairly simply using Shannon's rules and the binary entropy function $h(p)$:

$$h(p) = -p\log p - (1-p)\log(1-p) \quad . \tag{3.33}$$

Note that

$$-p\log p \geq -(1-p)\log(1-p) \quad . \tag{3.34}$$

for $p \leq 1/2$, and recall that Jensen's inequality is

$$\sum_{i=1}^{n} p_i f(x_i) \geq f\left(\sum_{i=1}^{n} p_i x_i\right) \tag{3.35}$$

for positive numbers $p_1, \cdots p_N$ which sum to 1, and f a continuous real function which is concave up, such as $h(p)$. Hence, if Bob accepts then

$$H(C|C') = h(b^N) \leq 2b^N \cdot \log(1/b^N) = 2b^N \cdot N \cdot \log(1/b) < c^N. \tag{3.36}$$

Furthermore, examining Eve's side,

$$H(C|\hat{Z}) = \sum_{\hat{z} \in Z^N \times V} P_{\hat{Z}}(\hat{z}) \cdot H(C|\hat{Z} = \hat{z}) \tag{3.37}$$

and given that the probability of Eve guessing C *incorrectly*, with the optimal strategy and $\hat{Z} = \hat{z}$, is $p_{E,\hat{z}}$ then

$$\sum_{\hat{z} \in Z^N \times V} P_{\hat{Z}}(\hat{z}) \cdot H(C|\hat{Z} = \hat{z}) = E_{\hat{Z}}[h(p_{E,\hat{Z}})] \geq E_{\hat{Z}}[p_{E,\hat{Z}}] = \gamma_N \geq c^N. \tag{3.38}$$

Bob publically rejects which means that there is a zero information entropy for Alice conditional upon Bob and Eve:

$$H(\hat{X}|\hat{Y}) = H(\hat{X}|\hat{Z}) = H(\hat{X}|V) = 0 \tag{3.39}$$

Finally, recall that the probability that Bob accepts the message sent by Alice, $p_{\alpha,N} > 0$, it follows that

$$I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z}) > 0 \tag{3.40}$$

and thus there is security in the model.

3.5 Information Reconciliation

Using the simulated satellite setup provided by Airbus Defence and Space some calculations were performed to investigate the key exchange rate. That is, the bits-per-bit required to produce key, and identify the redundancy of the protocol.

In particular, this process highlighted the need for a carefully chosen error correction. Without error correction $I(A:B) < I(A:E)$, further rounds of advantage distillation creates $I(A:B') > I(A:B)$. But this also improves Eve's information as well. Thus, an error correction code which reveals positional information and does not create an additional advantage for Alice and Bob is required. This eliminates the use of Bose–Chaudhuri–Hocquenghem (BCH) and other forward error correction protocols, such as Hamming codes.

A Hamming($n+p, n$) code will convert an n bit string into a $n+p$ bit string, where p bits are parity indicators for a subset of the n bits. This subset is defined in such a way that any bit flip errors in either the parity or message bits can be identified and corrected.

To illustrate the flaws in forward error correction consider the straightforward example of a Hamming(7,4) code. Say Alice wishes to send (0000). With Hamming code this is (0000000). Assume that Bob has received a bit error and receives (0010), similarly Eve receives (1000). Without the Hamming code Bob, Alice and Eve would receive different data different from each other, without any realising they had an error themselves, or realising that each other had received different data. With the Hamming code Bob and Eve would realise their bit errors and both correct them so they both receive the same as Alice. The target situation is one where both Bob and Eve have errors compared to Alice, and Bob and Alice can isolate a section in which they have matching data and Eve does not. If Eve has the opportunity to correct as equally as Bob then this will not be beneficial.

Cascade

In order to combat the flaws with typical forward error correction a protocol called cascade has been chosen. This was first establisched by Brassard and Salvail in 1994 and is designed to leak the minimum amount of information to an eavesdropper (Brassard & Salvail, 1994). It consists of two algorithms: BINARY and a randomising function affectionately called JIGGLE. First, a binary search is performed on both data sets to locate an error. This involves splitting the data set in to two parts and comparing the parity of each part. Then, if the parity of part one in Alice's set does not match the parity of part one in Bob's set, part one is split further in to two to narrow down the location of the parity discrepency further. When the error has been located it can either be corrected, or simply discarded. Clearly this will only locate one error out of a possible many. Therefore, to increase the coverage, the next step is to use the JIGGLE function. JIGGLE randomises the data string so that the errors are redistributed and another one can be found using BINARY. Similar protocols exist such as Shell, which uses a random subset of data rather than the entire string.(Brassard & Salvail, 1994; Nakassis *et al.*, Pre-print)

Cascade Example

To illustrate the Cascade protocol a simplified example is presented. Suppose that Alice is trying to send a sequence:

$$\text{Alice} = \{0,0,0,0\ \ 1,1,1,1\ \ 0,1,0,1\ \ 0,0,0,0\} \tag{3.41}$$

Bob has received the sequence with a two bit error:

$$\text{Bob} = \{0,1,0,0\ \ 1,1,1,1\ \ 0,1,0,1\ \ 0,0,0,1\} \tag{3.42}$$

And Eve has also received the sequence but with a single bit error:

$$\text{Eve} = \{0,0,0,0\ \ 1,0,1,1\ \ 0,1,0,1\ \ 0,0,0,0\} \tag{3.43}$$

Alice and Bob split their data into two and compare parities:

$$\text{Alice} = \{0,0,0,0\ \ 1,1,1,1\}\text{parity} = 0; \{0,1,0,1\ \ 0,0,0,0\}\text{parity} = 0 \tag{3.44}$$

$$\text{Bob} = \{0,\mathbf{1},0,0\ \ 1,1,1,1\}\text{parity} = 1; \{0,1,0,1\ \ 0,0,0,\mathbf{1}\}\text{parity} = 1 \tag{3.45}$$

$$\text{Eve} = \{0,0,0,0\ \ 1,\mathbf{0},1,1\}\text{parity} = 1; \{0,1,0,1\ \ 0,0,0,0\}\text{parity} = 0 \tag{3.46}$$

Taking side 2 to begin with, Alice and Bob split into two and identify the side in which the error lies:

$$\text{Alice} = \{0,1,0,1\}\text{parity} = 0; \{0,0,0,0\}\text{parity} = 0 \tag{3.47}$$

$$\text{Bob} = \{0,1,0,1\}\text{parity} = 0; \{0,0,0,\mathbf{1}\}\text{parity} = 1 \tag{3.48}$$

Thus it has been narrowed down to the last four bits. Repeating this dividing and parity checking again reveals that the problem bit is the final one;

$$Alice = \{0\}p = 0; \{0\}p = 0; \tag{3.49}$$

$$Bob = \{0\}p = 0; \{1\}p = 1; \tag{3.50}$$

Bob adjusts it and the parity checks now look like this:

$$Alice = \{0,0,0,0\ \ 1,1,1,1\} parity = 0; \{0,1,0,1\ \ 0,0,0,0\} parity = 0 \tag{3.51}$$

$$Bob = \{0,\mathbf{1},0,0\ \ 1,1,1,1\} parity = 1; \{0,1,0,1\ \ 0,0,0,0\} parity = 0 \tag{3.52}$$

$$Eve = \{0,0,0,0\ \ 1,\mathbf{0},1,1\} parity = 1; \{0,1,0,1\ \ 0,0,0,0\} parity = 0 \tag{3.53}$$

Thus far, Eve has learnt very little. She knows two bits exactly, but the ones which were ignored in the binary search she does not. If Eve had the following sequence in her second half, she would still have errors and be unable to do anything about them:

$$Eve = \{1,0,1,0\ \ 0,0,0,0\} parity = 0 \tag{3.54}$$

Now turn attention to the first half where both Bob and Eve have an error. These 8 bits are split into two and the parity of each side checked:

$$Alice = \{0,0,0,0\} p = 0; \{1,1,1,1\} p = 0 \tag{3.55}$$

$$Bob = \{0,\mathbf{1},0,0\} p = 1; \{1,1,1,1\} p = 0 \tag{3.56}$$

$$Eve = \{0,0,0,0\} p = 0; \{1,\mathbf{0},1,1\} p = 1 \tag{3.57}$$

The first four bits are then further searched and the error found and corrected so both Alice and Bob now match. However Eve is still left with an error in the second four bits which are not addressed. Alice and Bob's mutual information has now been maximised in a way which also minimizes the mutual information with Eve, the next stage is to amplify the privacy this gives them, as outlined in the following section.

3.5.1 Monte-Carlo simulations of AD and Cascade

Advantage distillation and cascade have been shown to be mathematically secure as standalone elements of a key distribution scheme. Monte Carlo simulations were written by another student, Liam Hunter[1], a summary of which is included here for completeness. The simulations implemented an eavesdropping scheme whereby in certain conditions it was possible to recover some of the key distilled

[1] Under the instruction and part-supervision of the author.

by Alice and Bob. Eve listened to the exchanges between Alice and Bob and adapted her key distillation technique. In advantage distillation a value is added to Alice and Bob's keys when they both agree that their N-bit repeat codes match after XOR with a randomly generated number. Eve's strategy makes a reasonable guess as to what the value will be depending on her interpretation of the N-bit code. If she is confident that her code is all 0's or all 1's she can add this to her key, however, if she calculates the code and receives, for example, $\{0, 1, 1, 0\}$ she must make a decision. Randomly guessing if the value is 0 or 1 will not be advantageous to Eve therefore she must adopt a different strategy. The key value is highlighted (labelled with a question mark) and its position noted to distinguish it from a regular key value and make it traceable.

At the end of the advantage distillation Alice and Bob now both share a key that is mostly correct. Eve has a key that has slightly more error and highlighted, question marked, values where the true value is not known. Eve can then listen to the Cascade protocol communications in order to attempt to correct these errors. In Cascade, the only information exchanged between Alice and Bob is a parity value for the current block being worked on. This block size reduces until the source of a single error is determined. Once found, the correct key value is revealed by one party which can be captured by Eve. Now Eve has more information than simply the revealed value as she also has parity information for each of the blocks analysed by Alice and Bob. If Eve can find a block containing one unknown value and she knows the parity then that unknown value becomes known.

During simulations, positions of the unknown values were tracked, as well as when parity bits occurred. This was then used to determine if it was possible for Eve to completely correct her key in order to match with Alice and Bob. Simulations were run using different levels of error for each party to see how this changed the number of unknown values remaining at the end of the Cascade protocol. At low error levels (2-6%) Eve was able to recover the whole key most of the time. However, once error levels started to rise into the region of 10-12%, there were only a very few number of occasions where Eve was able to arrive at the same key as Alice and Bob. For a key of length 1024, it was possible to leave the cascade process after 4 iterations with matching keys between Alice and Bob with Eve not knowing up to 300 of the key values. This showed that in an intelligent tracking eavesdrop, it is still possible to maintain secrecy using advantage distillation and cascade.

3.6 Privacy Amplification

The final part to consider in the process of producing a symmetric key is the amplification of privacy to further reduce the knowledge of an eavesdropper. This is commonly used in many current classical crytpographic protocols (Nielsen & Chuang, 2004). A large data string is mapped onto a smaller data string using a matrix mapping, this is commonly called hashing. A universal hash function is used to shorten the key by a prespecified amount. The hash function has the following two properties: (a) it is computationally infeasible to find the original data which mapped to the resultant string (irreversibility) and (b) no two data strings will produce the resultant string (collision free). This ensures that an eavesdropper knows the minimum amount of information about the key from the hashed string which is produced.(Bennett *et al.*, 1995; Cachin & Maurer, 1995; Stallings, 2014)

Method

For the purposes of clarity, call each matching data string, produced by Alice and Bob after error correction, M. M is a data block which can be of variable length. Privacy amplification uses a hash function, H, to map M on to some smaller number of bits:

$$h = H(M) \quad . \tag{3.58}$$

Hash functions use matrix multiplication functions, which have no inverse. This means that for the result, h, the initial data set, M, cannot be explicitly identified. To illustrate this, the example of a considerably simplfied matrix multiplication is used:

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \end{pmatrix} \quad . \tag{3.59}$$

The resultant matrix could have been created by any number of matrix multiplications. In reducing the size of the key the amount of information an eavesdropper knows about, the key has been reduced to an arbitrarily small amount. To understand why, consider the example that an eavesdropper, Eve, knows for certain any 4 bits from M. She may even know H. The resultant, h, is dependent upon every bit of M, including some bits of which Eve has definitely no information. Therefore Eve cannot produce an accurate h and all of her knowledge of the key is reduced. An extended disussion of privacy amplifacation for an imperfect private channel where partial information is leaked to Eve can be found in (Bennett *et al.*, 1988) and (Cachin & Maurer, 1995)

3.7 Integration

In order to adapt a protocol for microwave communications it must integrate with the following factors:

(a) high loss

(b) noise properties of microwaves

(c) possible side channel attacks

(d) modulation in phase and amplitude

(e) standardised error correction present in current telecommunications protocols

(f) detector independence

Combining the above protocols within a PSK type, communication is affected by those needs in the following ways:

(a) The protocol relies on the presence of noise, provided there is some mutual information between Alice and Bob to begin with. The signal must be detectable beyond mere noise.

(b) In order for a cloning attack to remain both detectable and for the no-cloning theorem to apply, the noise properties of microwaves must be quantum limited.

(c) Known hacks such as an 'intercept resend' will affect the signal recieved by Bob and be detectable.

(d) The protocol is actively incorporated with the phase and amplitude modulation.

(e) Standard error correction (such as turbo coding) may not be suitable for this. However, implementing the proposed error correction mechanism solely for key distribution in parallel with (and independently of) exisiting correction for the overall signal is straightforward.

(f) The protocol is independent of detection mechanisms.

The predominant issue is the variety of noise in microwaves. A general transmission will have the following predominant sources of noise; sending mechanism, thermal noise in the channel (additive white gaussian noise- AWGN), shot noise, detection noise. If the thermal noise dominates, an eavesdropper may be able to gain more information by performing a 'freezing attack' - measuring the signal from within a cooled cryostat to remove thermal noise.

However, thermal noise on its own can be used in the same manner. Thermal noise exhibits Hanbury-Brown Twiss correlations. This means that a signal has some correlation but with noise added. This in itself fulfills the requirements for sucessful key distillation. The proof that this is acceptable, however, lies beyond the confines of this thesis and is the subject of future work.

The next stage in applying this protocol is to examine and fully characterise the noise properties of signal microwaves performing PSK. This is dealt with in the next two chapters.

4

Security Boundaries

It is interesting to consider whether the thermal properties of microwaves will dominate beyond the shot noise properties, and the subsequent implications of this on the likelihood of secrecy. To prevent a ‘freezing attack’, one must be able to measure in the shot noise limit. This chapter examines some of the theory behind the profiles of noise in the frequency domain.

4.1 Novel Contributions

Some members of the quantum cryptography community (Weedbrook *et al.*, 2010, 2012), have focussed much of their attention on the inflexibility of CVQKD protocols with thermal states. This has meant that microwaves have repeatedly been dismissed as an adequate medium for CVQKD, on the understanding that the single mode field has thermal noise dominating for the microwave frequency range. This chapter draws on background physics to consider if microwaves can be considered as a valid region for fresh examination.

4.2 Introduction

In order to communicate securely for a variety of CVQKD protocols, the noise levels of the signals must meet certain limits. There has been some discussion over which frequency domains provide security, for example the Usenko unidimensional protocol (Usenko & Grosshans, 2015), and Weedbrook (Weedbrook

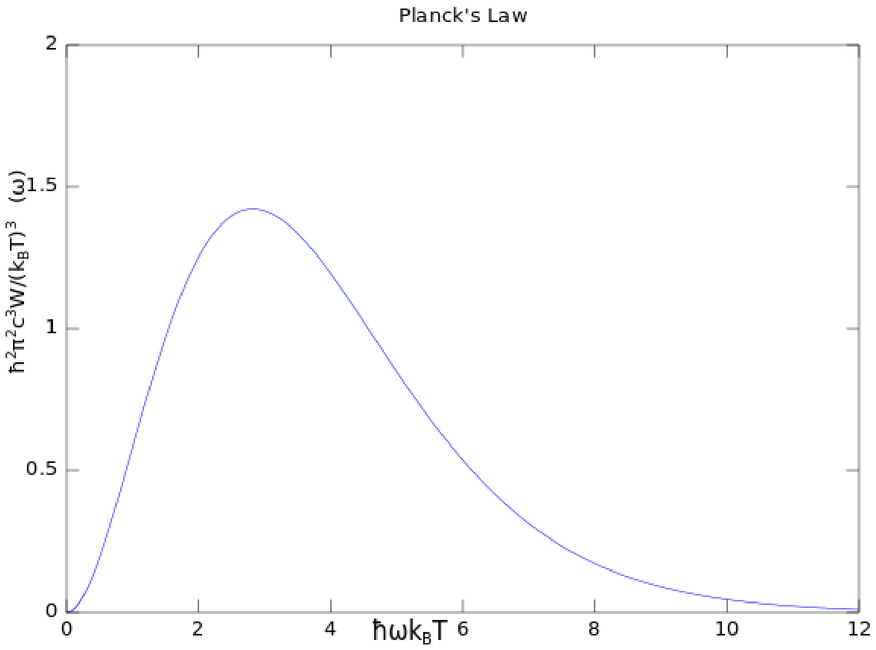


Figure 4.1: Planck's Law shown as in (Loudon, 2000), the energy density, W, varying with frequency, ω with units of $\hbar/k_BT$.

et al., 2010). The basic principle in having a secure region is that the thermal (non-quantum) noise is less than the quantum shot-noise, allowing for a small margin of error dependent upon the protocol. For example, thermal noise can be eliminated with a freezing attack and if thermal noise is dominating significantly beyond the levels allowed by the protocol then the communication is no longer secure.

Since the signals involved are multimodal then analysis cannot be restricted to a single mode perspective. One way to manage this is to examine the average energy for the density of modes. The minimum level of noise for a measurement is dictated by the vacuum energy. A state which has thermal noise is a thermal state, or a coherent state with thermal noise is a displaced thermal state.

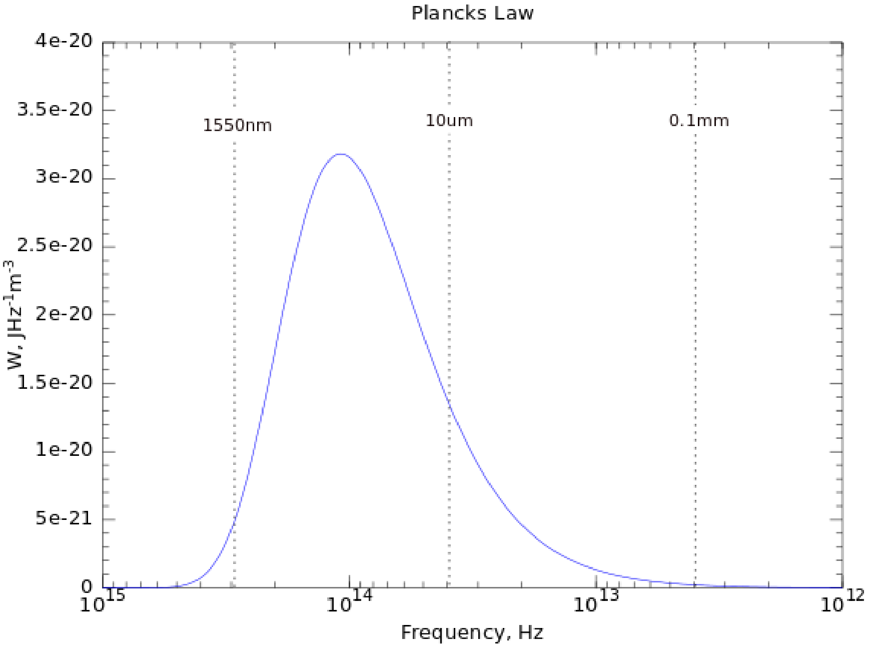


Figure 4.2: Planck's law showing energy density in thermal modes, W, response with frequency. 1550 nm - a popular communications frequency has been labelled for reference. Other sample wavelengths are included and it can clearly be seen that (at room temperature) thermal energy peaks in the infrared region.

4.3 Security in CVQKD

When analysing the thermal noise present in any general multimode field first recall (from (Loudon, 2000)) that the mean number of photons excited at a temperature T is

$$\langle n \rangle = \frac{1}{\exp(\hbar\omega/k_B T) - 1} \quad . \tag{4.1}$$

The mean energy (at some temperature T) of these photons is therefore

$$\langle n \rangle \hbar\omega \quad . \tag{4.2}$$

The density of field modes:

$$\rho(\omega)\,\mathrm{d}\omega = \omega^2\,\mathrm{d}\omega/\pi^2 c^3 \tag{4.3}$$

outlines the number of field modes (per unit volume) with frequencies ω to $\omega+\mathrm{d}\omega$. These have a mean energy as outlined by equation 4.2. Combining 4.1 and 4.2 gives the mean energy density of radiation in modes ω (at temperature, T):

$$\langle W_T(\omega) \rangle\,\mathrm{d}\omega = \langle n \rangle \hbar\omega\rho(\omega)\,\mathrm{d}\omega = \frac{\hbar\omega^3}{\pi^2 c^3}\frac{\mathrm{d}\omega}{\exp(\hbar\omega/k_B T) - 1} \quad . \tag{4.4}$$

$\langle W_T(\omega) \rangle$ is the black-body thermal energy per unit volume per unit angular frequency. This is plotted, for room temperature, in Figure 4.1 in normalised units. It is more useful for the understanding of security regions to see this in terms of frequency. This is shown in Figure 4.2 in SI units (also assuming room temperature). It can be seen from these plots that frequency regions at threat from thermal noise domination at room temperature lie somewhere in the Terahertz region.

To compare the dominance of thermal photons with shot noise limited signals, one can consider how many thermal photons would be measured from the cavity. 4.4 can be considered as a power spectral density in a cavity which is the size of a chosen wavelength:

$$P = \frac{\hbar\omega_0\mathrm{d}\omega}{\exp\left(\frac{\hbar\omega}{k_B T}\right) - 1} \quad . \tag{4.5}$$

The collected power of a measurement would be given by this value multiplied by the bandwidth of the measuring filter, and multiplied by some measurement time, T_0. By taking the bandwidth of the filter to be $\frac{1}{T_0}$ the collected thermal power for any given frequency, ω_0, is:

$$P_{Collected} = \hbar\omega_0 \frac{1}{\exp\left(\frac{\hbar\omega_0}{k_B T}\right) - 1} \tag{4.6}$$

with photon number given by

$$n = \frac{1}{\exp\left(\frac{\hbar\omega_0}{k_B T}\right) - 1} \tag{4.7}$$

The behaviour of this function can be seen in figure 4.3. If the value for this is compared with the strength of the signal it will indicate the number of thermal photons in any one measurement. In particular, frequencies of less than approximately $10^{13} Hz$ would not be suitable for single photon signal detection. However, the ability to use a larger signal strength would improve upon this.

4.4 Conclusions

This Chapter outlines how thermal energy is distributed in multimode signals - the photon number may be significant for the microwave region, however, there are fewer modes meaning that the total energy is smaller. Hence the peak of thermal energy is in the infrared region - this is seen in Figure 4.2. The number of thermal photons which one would expect to be measured can be seen in Figure 4.3. For a protocol which requires single photons there is a clear limit which prevents microwaves from being used - when the expected number of detected thermal photons becomes greater than one. Alternatively, if one requires a shot noise limited signal only, then an increase in the power of the overall signal would dominate the thermal photon presence. It would be interesting to consider how temperature for satellite communications would affect the number of thermal photons and the implications that might have for single photon protocols and shot noise limited only protocols.

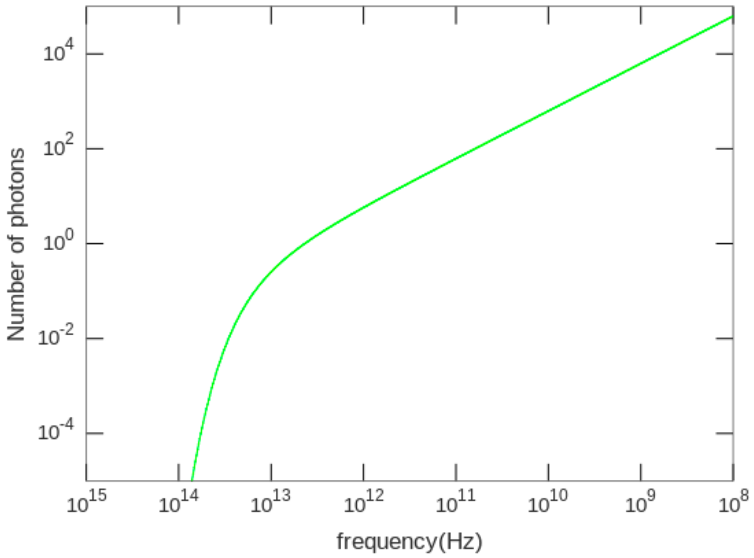


Figure 4.3: The number of thermal background photons which one would expect to measure for a cavity the length, depth, and width of the given wavelength at room temperature can be seen here. If one were to use a signal which was significantly larger than the number of thermal photons then the measurement would be dominated by shot noise. Frequencies less than at least $\approx 10^{13}$ would not be suitable if one were interested in single photon measurements

5

Microwave Characterisation

In order to determine if shot noise limits are achievable using typical PSK microwave signals, a characterisation of the noise must be performed. This Chapter examines the properties of the signals using collective measurement to perform quantum state tomography and reconstruction using homodyne detection. The characteristic behaviour of this can be used to identify if the state is coherent, and therefore quantum limited, or if it is a displaced thermal state. If it is the former, then microwaves may well be suitable for use in both CVQKD protocols and the post-quantum security protocol outlined in Chapter 3. However, if the signals are displaced thermal states then a thermal protocol may have to be implemented, or alternatively considering a post-quantum protocol based on Hanbury-Brown Twiss correlations to produce the biased random noise required as a resource for advantage distillation. this chapter shows that the signals used are coherent, however further calibration may be required to reach the limits for the Usenko protocol.

5.1 Novel Contributions

It has not before been demonstrated that the standard equipment engineered for telecommunications is not dominated by thermal noise measurements for the benefit of key distribution protocols. The signals in question are dominated by shot noise measurements and therefore are suitable for use in CVQKD protocols.

Previous to this work, the microwave region was dismissed and declared unsuitable for CVQKD implementations on the basis that microwaves are thought to be thermal.

5.2 Introduction

Translation of CVQKD into the microwave region is not straightforward. The transition presents a number of challenges, specifically, additional noise, distance factors and a many photon signal. Characterising noise is a crucial step in implementation of post-quantum cryptography or CVQKD in wireless communications.

CVQKD is a possible method for implementing security across networks. The current successful achievements have been in the optical range. A microwave implementation, if possible, would enable quantum security in a range of wireless devices, without need for difficult and time consuming spatial callibrations. The Usenko-Grosshans implementation (Usenko & Grosshans, 2015) sets stringent limits on excess noise.

Usenko et al. base their proof of security on a uni-dimensional protocol of the following form:

(a) Alice produces coherent states.

(b) Alice Gaussian modulates these states in one quadrature.

(c) The resultant states are sent to Bob.

(d) Bob performs a homodyne detection mostly in one. quadrature, and monitors the second quadrature (e.g. through basis switching).

A PSK signal meets the latter three requirements - a modulation in one quadrature could easily be performed by Alice with homodyne detection in two quadratures by Bob. It is interesting to characterise the signals for use in this protocol. As well as performing quantum state tomography to judge suitability for the protocol outlined in chapter 3, it is interesting to characterise the signals for use in this protocol also.

5.3 Quantum State Reconstruction

5.3.1 Background

If one measures the states of a wireless communications system, one can identify their properties and classify the states as either thermal or shot noise limited. If the states are shot noise limited, they will be coherent. Alternatively they will be thermal states, or some mix of the two. Suppose that the states of a typical wireless communications system are coherent states, the properties would resemble the following (as can be found in (Glauber, 2007)).

Consider some state, $|\alpha\rangle$, for which

$$a\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{5.1}$$

meaning that coherent states are eigenstates of the annihilation operator, a. This can be written in terms of the Fock basis as

$$|\alpha\rangle = \sum_{n=0}^{\infty} c_n\,|n\rangle \quad , \tag{5.2}$$

and therefore the annihilation operator applied to this is

$$a\,|\alpha\rangle = \sum_{n=0}^{\infty} c_n\sqrt{n}\,|n-1\rangle = \alpha\sum_{n=0}^{\infty} c_n\,|n\rangle \quad . \tag{5.3}$$

To find the c_n, one can follow the recursion relation given by the definition of the annihilation operator, giving yielding

$$c_n = \frac{\alpha}{\sqrt{n!}}c_0 \quad , \tag{5.4}$$

which then gives the state $|\alpha\rangle$ as

$$|\alpha\rangle = \sum_{n=0}^{\infty} \frac{\alpha}{\sqrt{n!}}c_0\,|n\rangle \quad . \tag{5.5}$$

In order to find c_0 normalise so that the inner product of a state must equal one:

$$\langle\alpha|\,\alpha\rangle = 1 = |c_0|^2 \sum_{n=0}^{\infty} \frac{\alpha^{2n}}{n!}\,\langle n|\,n\rangle \quad . \tag{5.6}$$

Given that the inner product of the number states must also equal 1, and the coefficient $\sum_{n}^{\infty} \frac{\alpha^{2}n}{n!}$ is $e^{|\alpha|^2}$ according to the Taylor expansion. Then, accordingly

$$c_0 = e^{\frac{-|\alpha|^2}{2}} \quad . \tag{5.7}$$

This gives the coherent state in terms of the Fock basis as

$$|\alpha\rangle = e^{\frac{-\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad . \tag{5.8}$$

Similarly, one can look at the relationship with the creation operator $a^\dagger$. For the Fock basis:

$$|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}} |0\rangle \quad , \tag{5.9}$$

and so, for a coherent state

$$|\alpha\rangle = e^{\frac{-\alpha^2}{2}} \sum_{n} \frac{\left(\alpha a^\dagger\right)^n}{n!} |0\rangle \quad . \tag{5.10}$$

Again, using the Taylor expansion, this can be written

$$|\alpha\rangle = e^{\alpha a^\dagger - \frac{|\alpha|^2}{2}} |0\rangle \quad . \tag{5.11}$$

Given that the annihilation operator acting on the vacuum state will just give the vacuum state, then the state can be manipulated to read

$$|\alpha\rangle = e^{\alpha a^\dagger - \frac{|\alpha|^2}{2} - \alpha^* a} |0\rangle \quad . \tag{5.12}$$

Here the following identity and can be used to simplify this further:

$$e^{A+B} = e^{\frac{-[A,B]}{2}} e^A e^B \quad . \tag{5.13}$$

This can now give a coherent state in terms of the vacuum state:

$$|\alpha\rangle = e^{\alpha a^\dagger - \alpha^* a} |0\rangle = D\left(\alpha\right) |0\rangle \quad . \tag{5.14}$$

Therefore, the quantum state reconstruction of a coherent state will be a displaced vacuum state with the amplitude of displacement given by the average photon number.

The statistics of photons in the coherent state can also be outlined. The calculation of the expectation value for the mean number of photons in the coherent state is taken by the application of the number operator, $\hat{N} = \hat{a}^\dagger\hat{a}$ to the state:

$$\langle n \rangle = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^2 \quad , \tag{5.15}$$

the same can be done for the operator $\hat{N}^2$:

$$\langle n^2 \rangle = \langle \alpha | \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^4 + |\alpha|^2 \quad . \tag{5.16}$$

Together equations 5.15 and 5.16 reveal the dispersion of the state:

$$(\Delta n)^2 = |\alpha|^2 = \langle n \rangle \quad , \tag{5.17}$$

meaning that the uncertainty of the state goes as the square root of the number of photons in the state. The amplitude of the state in phase space is given by

$$|\alpha| = \langle n \rangle^{\frac{1}{2}} \quad . \tag{5.18}$$

The quadrature operators, $\hat{x} = \frac{1}{2}\left(\hat{a}^\dagger + \hat{a}\right)$ and $\hat{p} = \frac{i}{2}\left(\hat{a}^\dagger - \hat{a}\right)$ (for which the commuation relation is $[\hat{x}, \hat{p}] = \frac{i\hbar}{2}$), can also be applied to the coherent states to give the real and imaginary parts of the complex amplitude:

$$\langle \alpha | \hat{x} | \alpha \rangle = \frac{1}{2} \langle \alpha | \hat{a}^\dagger + \hat{a} | \alpha \rangle = \left(\frac{\hbar}{2\omega}\right)^{\frac{1}{2}} (\alpha + \alpha *) \tag{5.19}$$

and

$$\langle \alpha | \hat{p} | \alpha \rangle = \frac{i}{2} \langle \alpha | \hat{a}^\dagger - \hat{a} | \alpha \rangle = i \left(\frac{\hbar\omega}{2}\right)^{\frac{1}{2}} (\alpha - \alpha *) \tag{5.20}$$

with the squared operators given by

$$\langle \hat{x}^2 \rangle = \frac{\hbar}{2\omega} \left(\alpha^2 + 2\alpha * \alpha + 1 + \alpha *^2\right) \tag{5.21}$$

and

$$\langle \hat{p}^2 \rangle = \frac{-\hbar\omega}{2} \left(\alpha^2 - 2\alpha * \alpha - 1 + \alpha *^2\right) \quad . \tag{5.22}$$

The variance in the quadrature operators can therefore be expressed as:

$$(\Delta x)^2 = (\Delta p)^2 = \frac{\hbar}{2} \quad . \tag{5.23}$$

The uncertainty relation is given by the inequality $\Delta a \Delta b \geq \frac{1}{2}\left|\left\langle\left[\hat{a},\hat{b}\right]\right\rangle\right|$. It can be seen that this is satisfied:

$$\Delta x \Delta p = \frac{\hbar}{4} = \frac{1}{2}\left|\frac{i\hbar}{2}\right| \quad . \tag{5.24}$$

This means that the combined uncertainty in the quadrature basis of the coherent state must be dominated by the uncertainty principle, and therefore be shot noise limited.

The measurement of the states can be seen by the action of the electric field operator, $\hat{E}$, which can be given in terms of the quadrature operators:

$$\hat{E} = \hat{X}\cos\phi - \hat{Y}\sin\phi \quad , \tag{5.25}$$

the expectation value for which is

$$\left\langle \hat{E} \right\rangle = \langle\alpha|\,\hat{E}\,|\alpha\rangle = \frac{1}{2}\langle\alpha|\,\hat{a}^{\dagger}e^{-i\phi} + e^{i\phi}\hat{a}\,|\alpha\rangle = |\alpha|\cos\left(\phi+\Theta\right) \quad . \tag{5.26}$$

The field variance, $(\Delta E)^2$, is the minimum uncertainty state and is independent of average photon number and phase angle. The two phase angles, ϕ and Θ can be thought of as the measurement phase angle and the phase of the excitation of the field in which the measurement is performed.

It also follows that the photon number and phase obey the uncertainty relation $\Delta n \Delta \phi = \frac{1}{2}$ and so a coherent state is a circle in phase space similar to that in Figure 5.1. In order to examine how this noise is distributed, one can examine the probability distribution of the states along the amplitude axis. Take the probability distribution from the projection of the coherent state into the Fock basis:

$$P(n) = |\langle n|\,\alpha\rangle|^2 = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!} = e^{-\langle n\rangle}\frac{\langle n\rangle^n}{N!} \tag{5.27}$$

which is a Poissonian distribution and can be approximated for large numbers of n by the Gaussian distribution

$$P(n) \approx \frac{1}{\sqrt{2\pi\langle n\rangle}}e^{-\frac{(n-\langle n\rangle)^2}{2\langle n\rangle}} \quad . \tag{5.28}$$

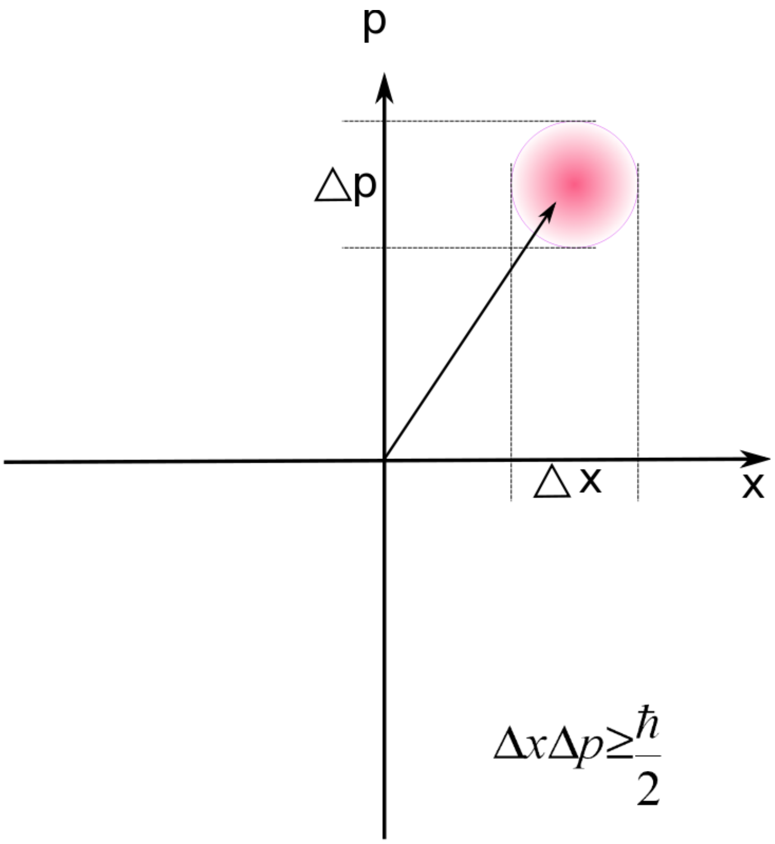


Figure 5.1: An illustration of the uncertainty of a coherent state in phase space.

Given the uncertainty relation between phase and number, it follows that the phase probability distribution is also Gaussian:

$$P(\phi) = \frac{1}{2\pi} \left| \sum_n e^{\frac{1}{2}|\alpha|^2} \frac{|\alpha|^n}{(n!)^{\frac{1}{2}}} e^{in(\theta-\phi)} \right|^2 \quad . \tag{5.29}$$

Now that the coherent state has been completely defined, it remains to outline how one can perform a reconstruction. Quantum state reconstruction methods typically use the Wigner function such as (Leonhardt, 1996; Rundle *et al.*, 2017). The Wigner function is a quasi probability distribution which can be composed for a state, first identifited by Wigner in 1932 (Wigner, 1932). If the probability distribution can be found for a given real state, then it can be compared with the Wigner function. The Wigner function is given as a function of the density matrix. The density matrix for coherent states is given by

$$\rho = \int P(\alpha) \left|\alpha\right\rangle \left\langle\alpha\right| \mathrm{d}^2\alpha \quad , \tag{5.30}$$

where the function $P(\alpha)$ gives real valued coefficients for the coherent state which are analagous to a probability density. This is called the $P-$ representation. The density matrix in the P representation also obeys the normalization condition:

$$\mathrm{Tr}\rho = \int P(\alpha)\mathrm{d}^2\alpha = 1 \quad . \tag{5.31}$$

If it is supposed that the states are modelled by a Gaussian distribution [1] the weight funciton can be written as:

$$P(\alpha) = \frac{1}{\pi \left\langle n\right\rangle} e^{-|\alpha|^2/\langle n\rangle} \tag{5.32}$$

and the density operator then becomes

$$\rho = \frac{1}{\pi \left\langle n\right\rangle} \int e^{-|\alpha|^2/\langle n\rangle} \left|\alpha\right\rangle \left\langle\alpha\right| \mathrm{d}^2\alpha \quad . \tag{5.33}$$

The Wigner function is given by

$$W(q,p) = \frac{1}{2\pi\hbar} \int \rho(q - \frac{x}{2}, q + \frac{x}{2}) e^{\frac{ipx}{\hbar}} \mathrm{d}x \tag{5.34}$$

[1] A proof of this can be found in (Glauber, 2007)

$$W(\alpha) = \frac{1}{\pi^2}\int \mathrm{d}^2\eta e^{\eta*\alpha-\eta\alpha*}\mathrm{Tr}\rho e^{\eta a^\dagger-\eta*a} \quad . \tag{5.35}$$

For a coherent state given by $|\alpha\rangle = |\mathrm{X} + i\mathrm{Y}\rangle$ this is

$$W(X,Y) = \frac{1}{2\pi}e^{-((X-x_0)^2+(Y-y_0)^2)} \tag{5.36}$$

which is a Gaussian centred on (x_0, y_0) is phase space.

A sample probability distribution from the Wigner function for a coherent state centred on $(0.69, 0.69)$ can be seen in Figure 5.4.

5.3.2 Photodetection

In order to see the comparison between detected photocounts and the photons of the original coherent state consider the following explantion.

The photons arriving at a detector during some integration time T can be measured as the following:

$$\hat{M}(t,T) = \int_t^{t+T} \mathrm{d}t\hat{f}(t') = \int_t^{t+T} \mathrm{d}t'\hat{a}^\dagger(t')\hat{a}(t') \quad . \tag{5.37}$$

An inefficient detector can be modelled as a combination of an inefficient beam-splitter and a perfect detector where the beam splitter has reflection and transmission coefficients: $R = i(1-\eta)^{1/2}$ and $T = \eta^{1/2}$. The output which falls on the detector is:

$$\hat{d}(t) = \eta^{1/2}\hat{a}(t) + i(1-\eta)^{1/2}\hat{v}(t) \tag{5.38}$$

where $\hat{a}$ is the input and $\hat{v}$ is the second field input to the beam splitter.

The photocount operator can then become:

$$\hat{M}_D(t,T) = \int_t^{t+T} \mathrm{d}t'\hat{d}^\dagger(t')\hat{d}(t') \quad . \tag{5.39}$$

The mean photocount is:

$$\langle m\rangle = \langle\hat{M}_D(t,T)\rangle = \eta\langle\hat{M}(t,T)\rangle \tag{5.40}$$

and it can be assumed that the standard vacuum state is being used for $\hat{v}(t)$. The second factorial moment is given by:

$$\begin{aligned} \langle m(m-1)\rangle &= \int_t^{t+T} \mathrm{d}t' \int_t^{t+T} \mathrm{d}(t'')\langle \hat{d}^\dagger(t')\hat{d}^\dagger(t'')\hat{d}(t'')\hat{d}(t')\rangle & (5.41)\\ &= \eta^2\langle \hat{M}(t,T)[\hat{M}(t,T)-1]\rangle \quad . & (5.42)\end{aligned}$$

The variance of the photocount is then given by

$$(\Delta m)^2 = \eta^2\langle[\Delta\hat{M}(t,T)]^2\rangle + \eta(1-\eta)\langle\hat{M}(t,T)\rangle \tag{5.43}$$

where the right hand contribution is the variance of the integrated photon number of the light beam (as would be present in a perfect detector). The left hand contribution results from the random selection of incident photons due to imperfect detection.

The value of second order coherence (for zero time delay) is given in terms of photocount averages as:

$$g_D^{(2)}(0) = \frac{\langle m(m-1)\rangle}{\langle m\rangle^2} = \frac{\langle\hat{M}(t,T)[\hat{M}(t,T)-1]\rangle}{\langle\hat{M}(t,T)\rangle^2} \quad . \tag{5.44}$$

The Mandel Q parameter is:

$$Q_D = \frac{(\Delta m)^2 - \langle m\rangle}{\langle m\rangle} = \eta\frac{\langle[\Delta\hat{M}(t,T)]^2 > -\langle\hat{M}(t,T)\rangle}{\langle\hat{M}(t,T)\rangle} \quad . \tag{5.45}$$

The mean photocount is

$$\langle m\rangle = \eta n \int_t^{t+T} \mathrm{d}t'|\xi(t')|^2 \tag{5.46}$$

and

$$\langle m(m-1)\rangle = \eta^2 n(n-1)\left[\int_t^{t+T} \mathrm{d}t'|\xi(t')|^2\right]^2 \tag{5.47}$$

with photocount variance:

$$(\Delta m)^2 = \langle m\rangle - \eta^2 n\left[\int_t^{t+T} \mathrm{d}t'|\xi(t')|^2\right]^2 \quad . \tag{5.48}$$

In homodyne detection, the reflection and transmission coeffients of the beam splitter (separate to an imperfect detector splitter) are:

$$|R| = |T| = 1/\sqrt{2} \quad \text{and} \quad \phi_R - \phi_T = \pi/2 \quad . \tag{5.49}$$

in balanced homodyne detection the measured value is actually the difference between the two arms of the beamsplitter, for which the operator for perfect detection becomes:

$$\hat{M}_{-}(t,T) = i\int_{t}^{t+T} \mathrm{d}t' \left[\hat{a}^{\dagger}(t')\hat{a}_L(t') - \hat{a}_L^{\dagger}(t')\hat{a}(t')\right] \tag{5.50}$$

and for imperfect detection:

$$\hat{M}_{H}(t,T) = \int_{t}^{t+T} \mathrm{d}(t') \left[\hat{d}_3^{\dagger}(t')\hat{d}_3(t') - \hat{d}_4^{\dagger}(t')\hat{d}_4(t')\right] \quad . \tag{5.51}$$

The signal to noise ratio is defined as:

$$SNR = \frac{\langle\hat{E}\rangle^2}{(\Delta\hat{E})^2} \tag{5.52}$$

where the expectation of the field operator is the signal. For a single mode coherent state, $\alpha\,(t)$, given as:

$$\alpha(t) = F^{1/2}exp(-i\omega_L t + i\theta) \tag{5.53}$$

and the coherent signal field of

$$S = \langle\hat{E}_H(\chi,t,T)\rangle = (FT)^{1/2}cos(\chi-\theta) \quad . \tag{5.54}$$

Then the variance of the homodyne field operator is:

$$N = \langle\left[\Delta\hat{E}_H(\chi,t,T)\right]^2\rangle = \frac{1}{4} \quad , \tag{5.55}$$

giving a signal to noise ratio of:

$$SNR = 4FT\cos^2(\chi-\theta) \quad . \tag{5.56}$$

This is comparable to the coherent signal of:

$$S = \langle\alpha|\hat{E}(\chi)|\alpha\rangle = |\alpha|\cos(\chi-\theta) \quad , \tag{5.57}$$

with the field variance of

$$N = (\Delta E(\chi))^2 = \frac{1}{4} \tag{5.58}$$

and signal to noise ratio:

$$SNR = 4\langle n\rangle cos^2(\chi-\theta) \quad . \tag{5.59}$$

5.3.3 Basis Swapping

Much of the background has been considered in terms of the x and p basis. A conversion into the p and q basis is required since the resultant waveform is to be considered in terms of its real and imaginary parts, equivalent to p and q. In order to translate from the x, p basis to the quadrature, p, q basis, one must consider the projection of the x basis onto the p, q basis which goes as the following:

$$\langle x|\, qp\rangle = \left(\frac{\omega}{\pi\hbar}\right)^{1/4} \exp\left(\frac{-\omega}{2\hbar}\left(x-q\right)^2 + \frac{i}{\hbar}p\left(x-q\right)\right) \quad . \tag{5.60}$$

It is clear that this has no effect on the properties described earlier.

5.3.4 Expected Distributions

If thermal noise dominated measurements of a signal then one would expect to see non-poissonian statistics. In particular, consider the following equation for the average number of thermal photons, $\langle n\rangle$:

$$\langle n\rangle = \frac{1}{\exp^{\frac{\hbar\omega}{k_B T}} - 1} \quad , \tag{5.61}$$

which can be rearranged as:

$$\exp^{\frac{-\hbar\omega}{k_B T}} - 1 = \frac{\langle n\rangle}{1+\langle n\rangle} = U \quad . \tag{5.62}$$

In turn, this gives the probability distribution for a thermal state of:

$$P\left(n\right) = \frac{U^n}{\sum_{\infty} U^n} = \frac{\langle n\rangle^n}{\left(1+\langle n\rangle\right)^{1+n}} \quad . \tag{5.63}$$

The variance can be found from this using the following relationship

$$\left(\Delta n\right)^2 = \sum_n \left(n - \langle n\rangle)^2\right) P\left(n\right) \quad . \tag{5.64}$$

Given that

$$\langle n\left(n-1\right)\rangle = 2\langle n\rangle^2 \quad , \tag{5.65}$$

then it can be surmised that

$$\left(\Delta n\right)^2 = \langle n\rangle^2 + \langle n\rangle \quad . \tag{5.66}$$

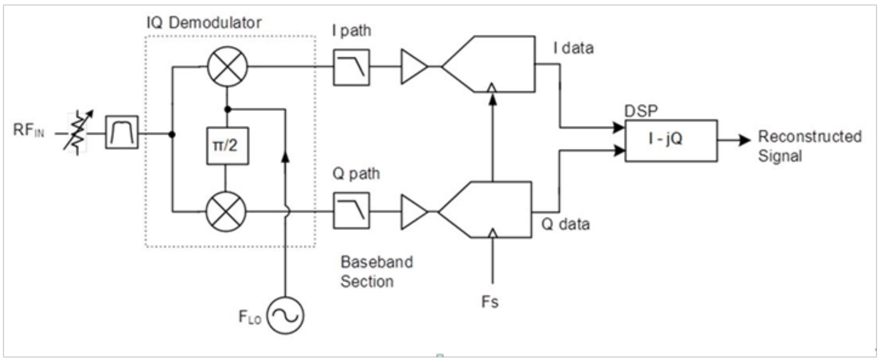


Figure 5.2: The detection mechanism of a QPSK signal includes the detection through a high pass filter, splitting it and comparing each signal to a different phase.

Thus, if the distribution is indeed dominated by thermal noise then the square of the variance will have a squared component. Compare this to 5.48 which shows the expected distribution for a coherent state, or a displaced coherent state which is not dominated by thermal noise. It is possible that other states will have either of these distributions, however, if a possible thermal noise measurement is dominating, then the applicability of many CVQKD protocols, according to (Weedbrook *et al.*, 2010, 2012) fails, or at least becomes significantly more complex.

5.4 Method

Outlined here is the method for quantum state reconstruction using homodyne detection of the output from a software defined radio (commonly used to simulate wi-fi and satellite signals) and compare the results to the expectation for a quantum coherent state as is assumed for the analysis in Section 5.3.1.

Telecommunications protocols use an 'IQ' modulation system. This is equivalent to modulation in phase (I) and out of phase (Q) resulting in a phase shift keying diagram. For example, a four-way modulation would be called 'QPSK' and have a phase diagram of the form shown in figure 5.3.

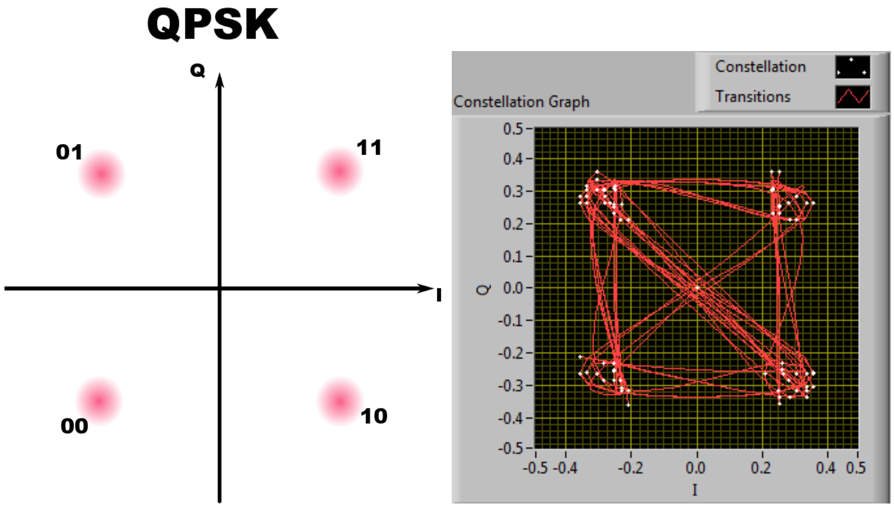


Figure 5.3: QPSK with Gray coding, and a real example from a software defined radio.

This is equivalent to a quadrature phase diagram, with some normalisation. By taking multiple repeated measurements of the signal in 'I' and 'Q' (or in the real and imaginary components of the incoming waveform) a reconstructed approximation of the Wigner function for the state received can be made.

Homodyne detection was performed using the receiver and IQ demodulator of the National Instruments Universal Software Radio Peripheral. The USRP IQ detection goes as follows: An RF signal is passed through a variable resistor and an Intermediate Frequency filter, and passes through a low-noise amplifier. It is then beam-split into two parts. Each part is mixed with a local oscillator signal close to the frequency of the incoming signal (homodyne detection) and a 90 degree phase shift of the LO signal, respectively. These are now the I and Q paths respectively. Each path goes through a filter before meeting the analogue to digital convertor where it is sampled at some sampling frequency. Digital down converting and other digital signals processing is applied before receiving a reconstructed signal. The incoming signal is compared with the LO and the resultant phase difference is found. This allows for observations of phase sensitivity, lending itself to phase space detection. This is illustrated in Figure 5.2.

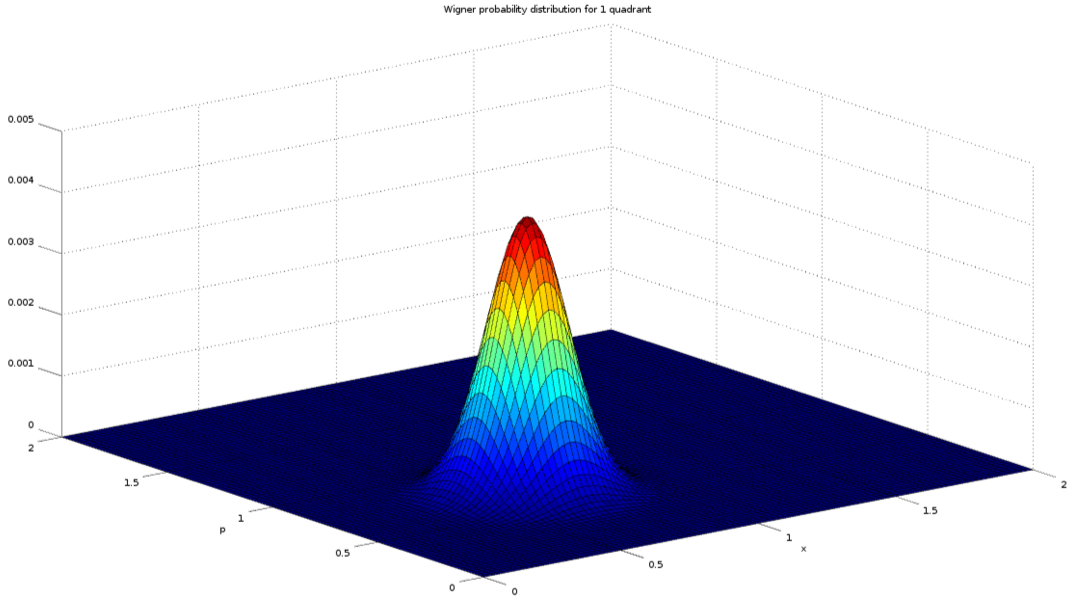


Figure 5.4: This is the Wigner quasi-probability distribution function for a coherent state, with parameters equivalent to the first quadrant of a QPSK

Since an IQ constellation is essentially a map of phase space the coordinates used for this can be extracted and one can record how frequently state measurements are made in each part of phase space, thus allowing for a statistical reconstruction of the Wigner quasiprobability function. Measurement of the mean and variance of the marginal probability distributions can subsequently confirm the statistical distributions.

This was performed at 51 MHz with varying power ranging from 10^{12} to 10^{17} average photon numbers. This means that a relationship between $|\alpha|^2$ and $\langle n\rangle$ can be seen and also between $(\Delta\alpha)^2$ and $\langle n\rangle$ evidencing the signals as either coherent or displaced thermal states.

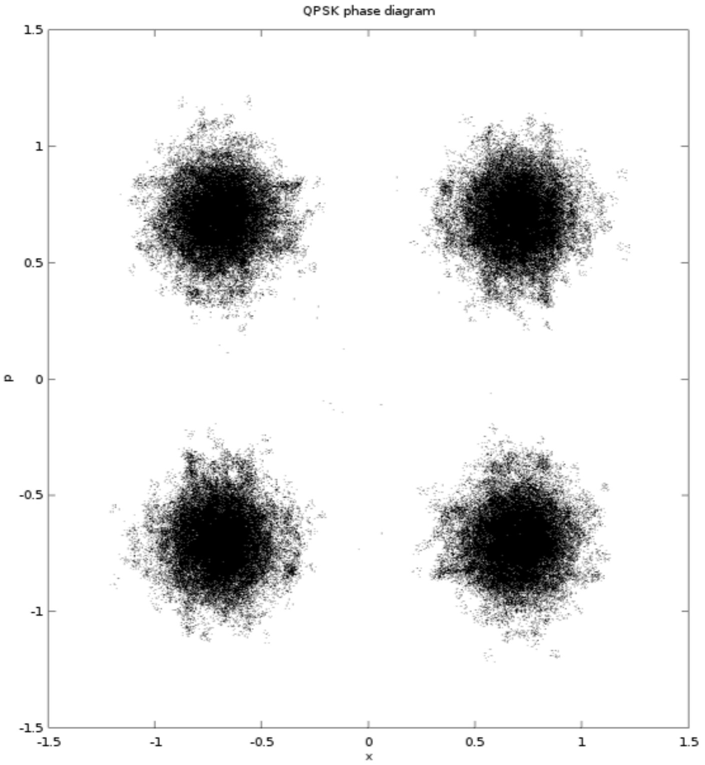


Figure 5.5: Detected QPSK states represented in a phase diagram.

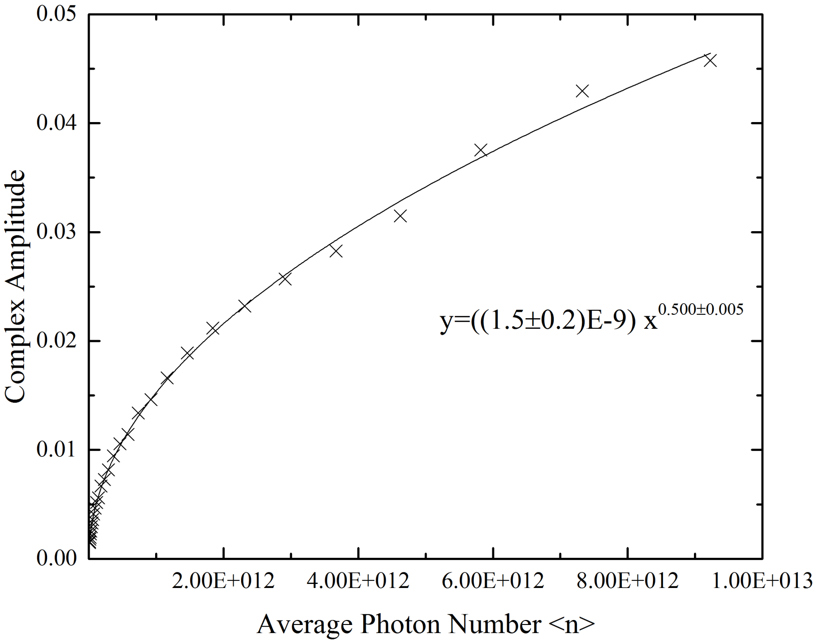


Figure 5.6: There is clearly a positive correlation between the complex amplitude of the state and the photon number. Furthermore, this is proportional to the square root of the photon number giving evidence of coherent states.

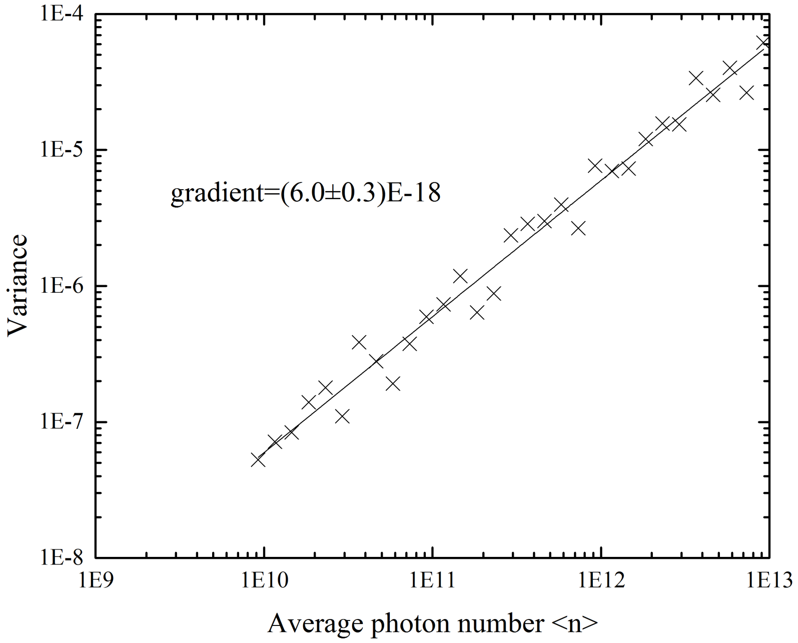


Figure 5.7: The variance of the complex amplitude is directly proportional to the detection of the average photocount. This is indicative of coherent states, whereas thermal states would exhibit a quadratic feature.

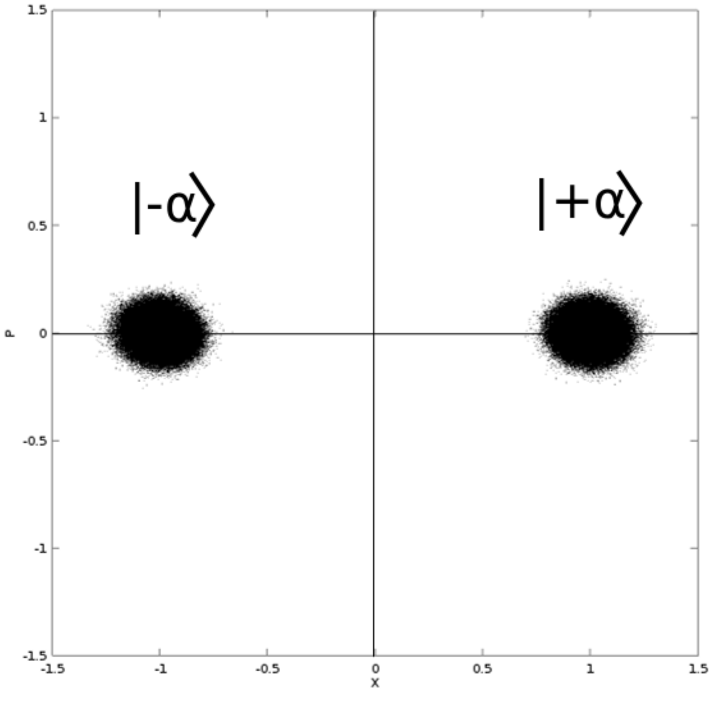


Figure 5.8: A collective measurement of a BPSK signal reveals the $\pm|\alpha\rangle$.

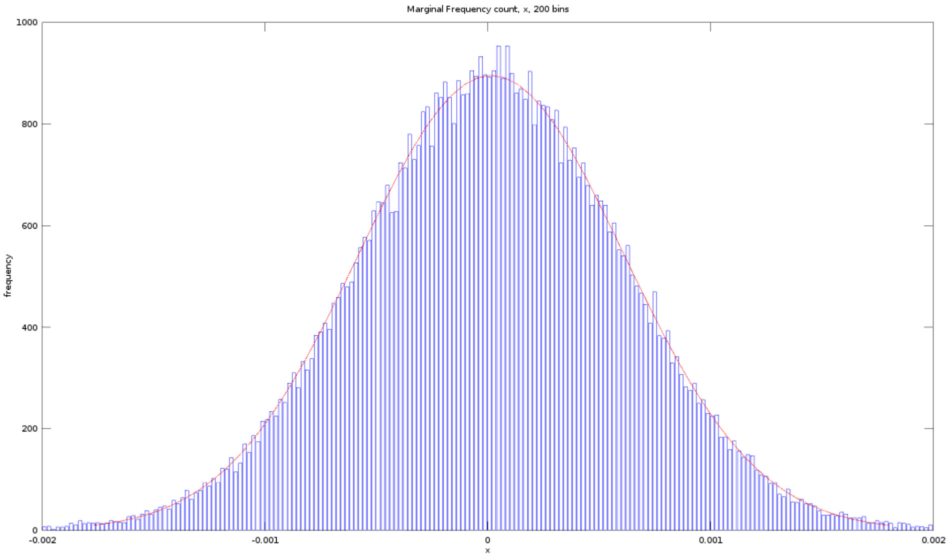


Figure 5.9: The projection of the state onto one basis gives the marginal probability. This is fitted comfortably to a Gaussian.

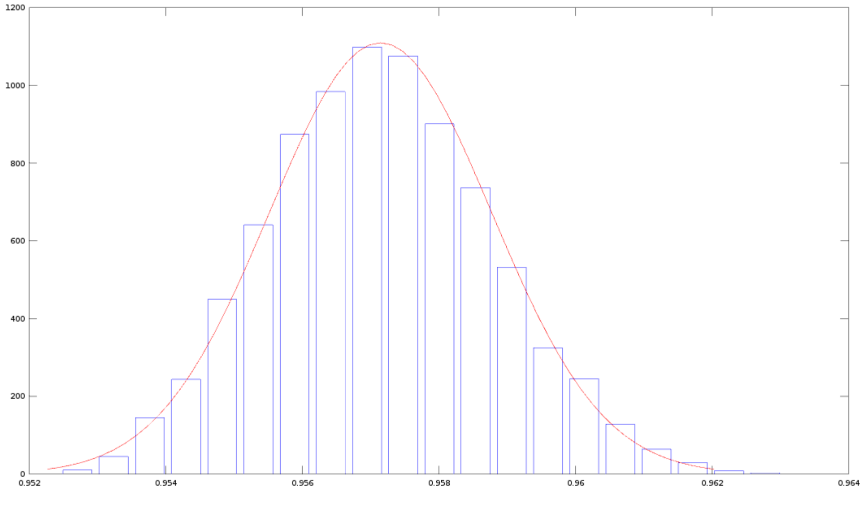


Figure 5.10: The projection of the state onto the other basis, taking only one of the modulations similarly reveals a marginal probability which can be fitted to a Gaussian.

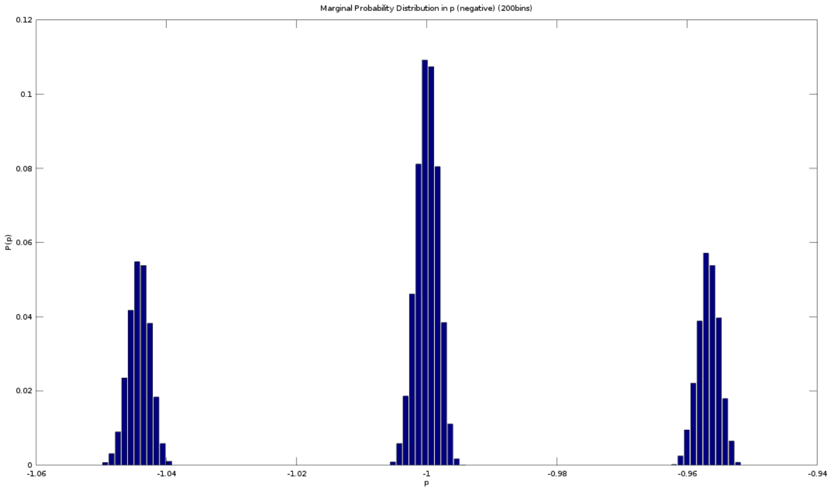


Figure 5.11: The signal's sub-modulation in this basis can be seen. This is a typical feature of PSK communications.

5.5 Results

Firstly, consider the scatter density for collective measurements in both a QPSK and BPSK signal in Figures 5.5 and 5.8. This demonstrates how the PSK signal can be distinguished into distinct states. Next, consider how a QPSK signal is formulated in phase space as shown in Figure 5.14. The signal in each of the four quarters is a sharp Gaussian peak. This can be seen in a BPSK signal also. This signal has been created with some sub-modulation in the 'Q' basis which generates three smaller peaks - as shown in Figure 5.11. The projection of this signal onto the 'p' and 'q' basis can be seen in Figures 5.9 and 5.10 respectively. The sub-modulation is Gaussian also, this can be seen in Figure 5.12. Furthermore the contour plot of one of the BPSK domains can be seen in Figure 5.13.

The marginal probabilities are clearly Gaussian, as shown in Figures 5.9 and 5.10. This is indicitave of either coherent or displaced thermal states compared with the Wigner function. It can therefore be surmised that there is more than a mere thermal chaotic signal, or that other excess noise sources with different relationships dominate.

Furthermore, consider how the complex amplitude compares to the average

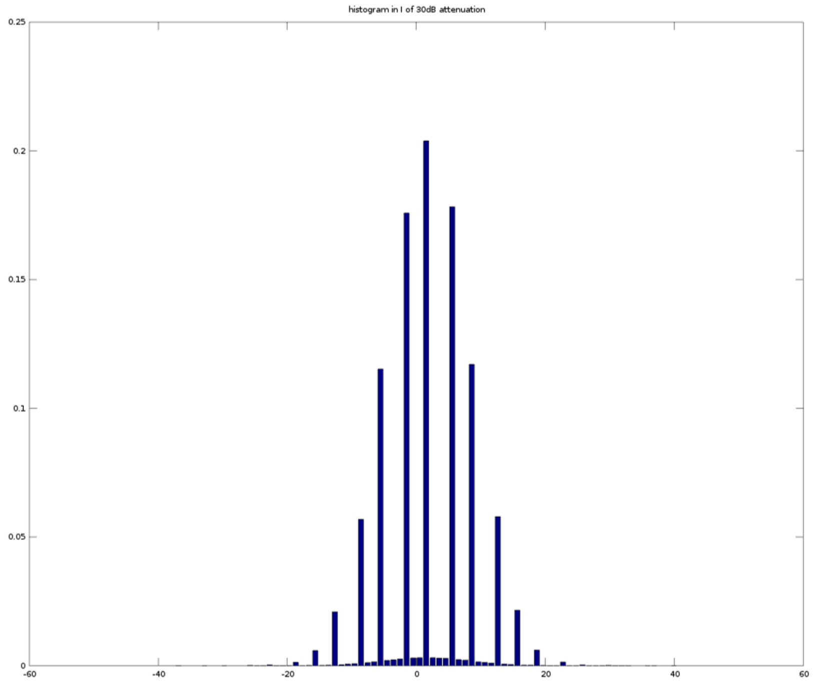


Figure 5.12: The overall Gaussian properties of the sub-modulation can be seen more clearly here.

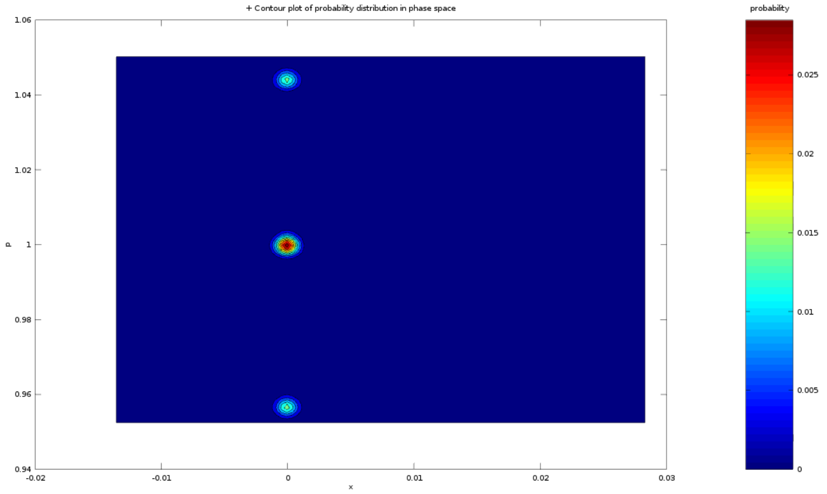


Figure 5.13: This shows the three states sent in a single domain of BPSK. The three states are a result of sub-modulation.

photocount number. A coherent state would reveal a square-root relationship. This is shown in Figure 5.6. A fitting algorithm gives a very strong power relationship of 0.500 ± 0.005. Finally, consider the relationship with the variance in figure 5.7. This, crucially, has only a linear realtionship. Displaced thermal states would have a quadratic component which cannot be distinguished here. Examination of the residuals reveals that there is no further structure and algorithmic fitting forcing a quadratic relationship reveals a negligible quadratic component on the order of 10^{-14}. This evidences the assertion that microwave signals are not dominated by thermal noise, and adds weight to the predication that microwave signals used in existing telecommunications infrastructure can be shot noise limited. It is perhaps possible that other states and nosie sources could lead to this distribution, however, given the knowledge of how the states were prepared there displaced coherent states with shot noise limitations appear the most likely candidate at this stage. This outcome is not unsurprising given the calculations of background thermal noise in multimode states given in Chapter 4.

Unfortunately, the linear fitting in this latter relationship reveals a variance which is greater than that required for the Usenko Grosshans protocol. However,

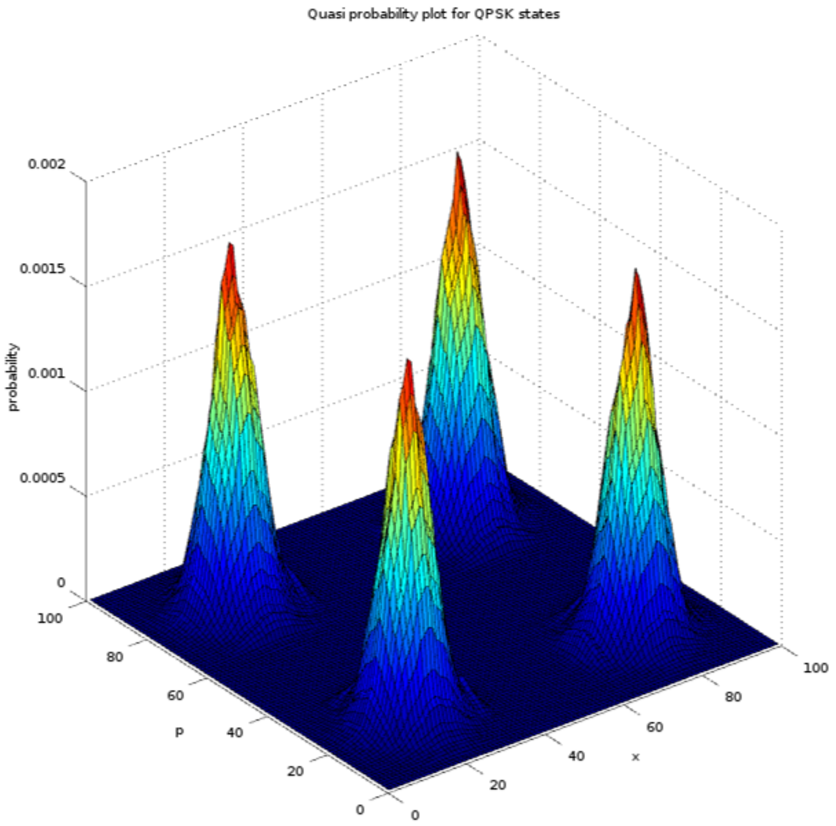


Figure 5.14: This is the reconstructed probability distribution for a QPSK state showing 4 Gaussian peaks in each of the domains.

some further calibration of the measurement system could likely improve this.

5.6 Conclusions

Microwave signals produced in a typical PSK protocol have been shown to not be dominated by thermal noise. Consequently the noise is not subject to a cooling attack and the apparent quantum limited features affirm these signals as a suitable candidate for the post quantum secure protocol outlined in Chapter 3. However, further calibration may be needed to achieve the limits of excess noise given in (Usenko & Grosshans, 2015).

6

Random Numbers as a Resource for Channel Independent Key Distribution

This chapter outlines a thought experiment which validates the existence of a completely channel independent secure quantum-safe communication theory. First, the building blocks of communication theory are outlined. Then various examples are examined in depth by considering the probability distributions upon which they depend. These are scrutinized with respect to potential attacks. Finally, it is concluded that it is possible to generate symmetric key extemporaneously, which is secure against the classical and quantum attacks considered here.

6.1 Novel Contributions

This section takes standard understandings of random numbers and demonstrates that random numbers meet the requirements for quantum-safe key distribution. The concept of using random numbers as a resource for the advantage distillation protocol is entirely novel.

6.2 Background and Motivation

Current widely used cryptographic techniques are based on security from 'computationally hard' problems. In particular, factorising large numbers into primes. Such problems are considered 'NP complete'. However the introduction of quantum computers may void this security. For instance, Shor's algorithm solves prime factorisation in a time several orders of magnitude shorter than all known classical algorithms.

The most advanced quantum computer currently has only the ability factorise numbers as large as 21 and the computer structure is extremely large(Martín-López, Enrique, 2012); but with a focus on building bigger, better, and faster architectures one can imagine a quantum revolution similar to that of classical computing progression from the 1950's to now.

Given the large investment of international governments into the persual of quantum computers, it is prudent to assume that there will bea significant threat to our security systems in the decades to come. This is evident through a push to investigate other methods of cryptography - the UK government funded Quantum Communications Hub for example.

Using quantum cryptography to defeat a quantum problem is a satisfying resolution. However it would be narrow-minded to look only at quantum solutions, especially since these are frequently poorly understood and involve complex implementations which leave more room for mistakes or side channel attacks. This is recognised in the increased focus on "post-quantum cryprography". This has largely been directed by a GCHQ white paper - seeking methods that do not necessarily require a quantum based implementation so long as the solution is secure against all possible quantum attacks (NCSC, 2016b).

As yet, the full extent of all possible quantum algorithms is not known. Seeking a solution based on an inherent property of mathematics rather than on the difficulty of the problem circumvents this issue. In a way, the principle of quantum cryptography seeks to create a solution based on the inherent properties of the mathematics of quantum systems, however it would be more convenient to use better understood mathematical principles.

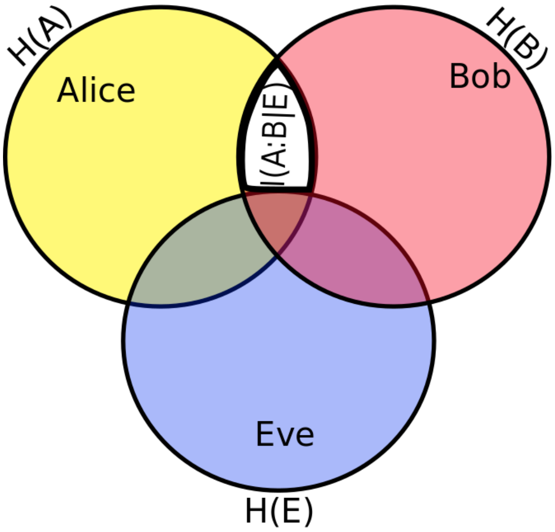


Figure 6.1: This exploration is concerned with looking for a positive $I(X : Y|Z)$. This means maximising the highlighted (white) part. So long as this is positive, the size of I(X:Y:Z) (the knowledge an eavesdropper has of the communication) is inconsequential.

In this chapter the properties of random numbers are examined with the view of seeking an inherent property which may be exploitable.

To thwart an eavesdropper, there must be some information shared between Alice and Bob (two hypothetical parties) that is not shared by some eavesdropper (who shall be named Eve). Consider the Venn diagram in Figure 6.1. The highlighted part must be strictly greater than zero. The algorithm discussed in chapter 3 takes some positive $I(X : Y|Z)$ and outputs useable secrecy capactiy. Thus, the focus of this chapter will be purely upon identifying a positive $I(X : Y|Z)$.

The following exploration will look at the entropy between Alice and Bob, which is directly linked to the 'randomness' of the data that Alice and Bob hold and an examination of the properties of random numbers is a logical place to start looking for exploitable inherent properties of random numbers.

6.3 Probabilities of Random Numbers

Consider a rudimentary random number generator- for instance, the flips of an unbiased coin. One flip of the coin gives the choices of $H = Heads$ and $T = Tails$. Two flips gives the combinations HH, HT, TH, and TT. Three flips gives 8 different possible combinations and so on, with 2^n combinations of outcomes for n flips. The tree describing this can be seen in figure 6.3. Naturally, the binary tree formulates a binomial probability density function. For example, a fair coin flipped with thirty trials has a distribution seen in Figure 6.4. For comparison, one can see the distribution for an unfair coin in Figure 6.5.

Suppose the experiment (e.g. coin flips) is repeated a large number of times. The central limit theorem predicts that the probability density function tends to a Gaussian. This result can be seen in Figure 6.6 and compared to the Gaussian in Figure 6.7 with a cumulative distribution function shown is Figure 6.8.

For a large number of repeated coin flips, the expectation for the combination of H's or T's produced is that half will be H and half will be Ts. For example, $HTHHTTHTTTHH$... etc. A true unbiased coin is expected to give the result that it does not tend to either outcome.

Consider next the probability, for a large number of experiment repeats, of getting some specific x_i combination of N_H (number of heads) and N_T (number of tails). Monte Carlo simulations give a probability density function shown in Figure 6.9 (where each combination has been mapped to a decimal number[1]). This is a uniform distribution; for exactly 50% chance of a head or a tail all the resultant paths are equally likely, but the mean outcome of *numbers* of heads and tails is 50% - if examining specifically the number of heads (or tails) produced in total then the distribution looks very different as seen in Figure 6.10. This is a Gaussian with a mean at $N \times P(H)$ where N is the number of trials and $P(H)$ is the probability of getting 'heads'.

If considering the case where the ordering of each set of outcomes is important, then the probability of getting any one of those outcomes is

$$P(X = x_i) = \frac{1}{2^N} \tag{6.1}$$

[1] For example $HH = 1$, $HT = 2$, $TH = 3$, $TT = 4$

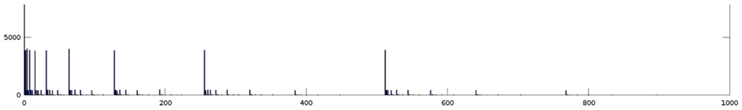


Figure 6.2: This shows the probability distribution for $P = 0.9$. It is more complex than for $P = 0.5$ as certain outcomes are more heavily weighted.

for N trials, assuming that the probability of each flip is 0.5. This can be seen easily in Figure 6.11. For other probabilities the outcome is more complex, consider the outcome for $P = 0.9$ in figure 6.2.

It can be seen how this extrapolates for higher N in Figure 6.12 - if 128 random flips were generated, the probability of getting any one combination would be 2.9×10^{-39}. Clearly, as N tends to infinity, the probability of getting some combination of outcomes tends to zero. Even if considering just the number of heads produced, the probability of receiving a number of heads will still tend to zero for large$N$. The probability of receiving the mean is given by

$$\frac{1}{2^N}\binom{N}{N/2} = \frac{1}{2^N}\frac{N!}{(N-1)!\left(\frac{N}{2}\right)!} \tag{6.2}$$

evaluating this for $\lim N \to \infty$ gives 0.

This shape can be derived from the Gaussian also. Consider the equation for a Gaussian distribution:

$$\frac{\exp(\frac{(x-\bar{x})^2}{2\sigma^2})}{\sqrt{2\pi}\sigma} \quad . \tag{6.3}$$

Evaluating this at $x = \bar{x}$ gives:

$$\frac{1}{\sigma\sqrt{2\pi}} \quad , \tag{6.4}$$

so this is the probability that some distribution has the expectation value. Recall that for counting statistics $\sigma = \frac{\sqrt{n}}{2}$ and as such, equation 6.4 becomes

$$\frac{1}{\sqrt{\pi n}} \quad . \tag{6.5}$$

If this is studied as n becomes large the following relationship can be seen:

$$\lim_{n\to\infty}\left(\frac{1}{\sqrt{\pi n}}\right) = 0 \quad . \tag{6.6}$$

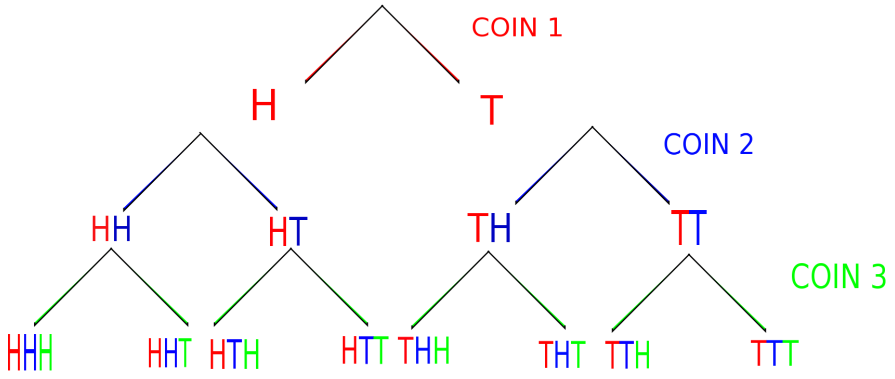


Figure 6.3: This is the binomial tree showing the possible combinations of outcomes for three flips of a coin.

Note that this applies for all x_i, where the distribution evaluates to:

$$\frac{\exp\left(\frac{-(x_i-\frac{n}{2})^2}{n}\right)}{\sqrt{n\pi}} \tag{6.7}$$

with the limit:

$$\lim_{n\to\infty}\left(\frac{\exp\left(\frac{-(x_i-\frac{n}{2})^2}{n}\right)}{\sqrt{n\pi}}\right) = 0 \quad . \tag{6.8}$$

So that $P(X = x_i) = 0$ for large n, for all x_i Thus, for a large enough number of experiments the probability of getting any one set of outcomes is 0. It is counterintuitive, but this works for $x_i = \bar{x}$ also, as seen above.

This result means that for a very large number of experiments, the chances of getting any one distribution (where that one distribution could even be the expected value), is zero.

6.4 Implications

For an infinite number of coin flips the probability of getting any specific combination tends to zero, as does the probability of getting any one number of Heads, or indeed, the mean number of Heads, despite this seeming unintuitive.

In standard counting statistics the standard deviation is approximately equal

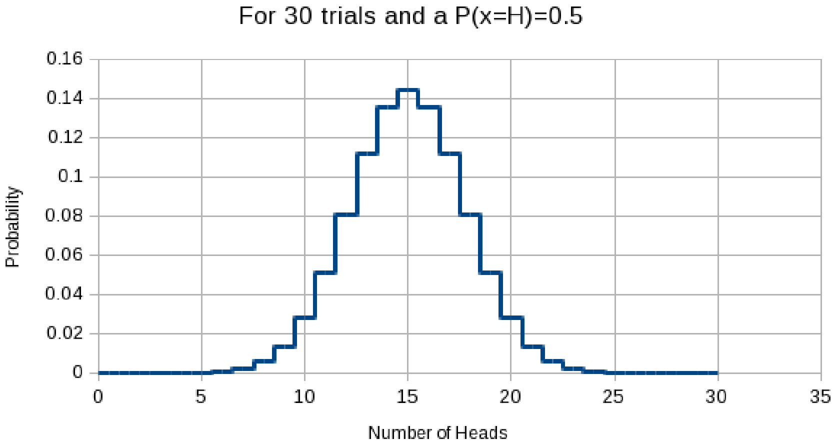


Figure 6.4: This binomial distribution shows the probability that the end combination contains n Heads, after 30 trials of a fair coin. It is clear to see that this is not dissimilar from the shape of a Gaussian, however it is stepped and not smooth as one would expect of a Gaussian.

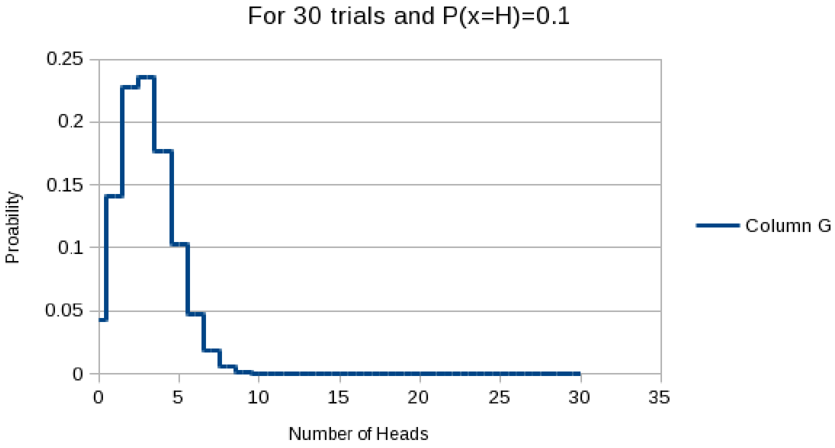


Figure 6.5: This binomial distribution, in contrast to Figure 6.4 shows how the distribution might be affected for a biased coin. In this instance, the probability of getting heads is 0.1.

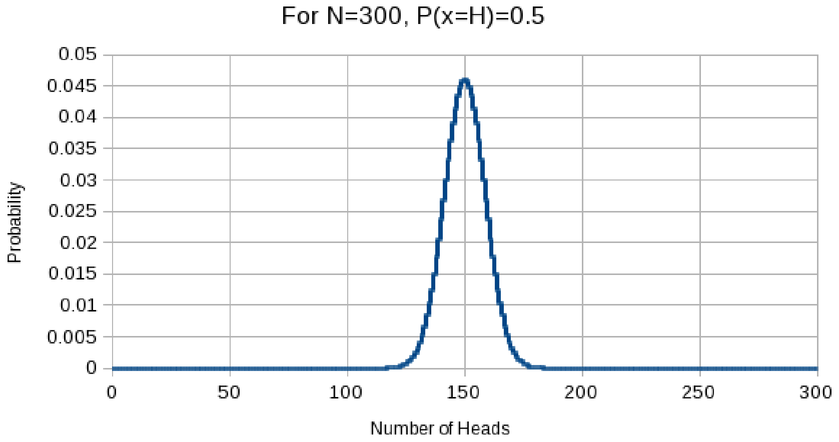


Figure 6.6: This binomial distribution shows the probability that the end combination contains n Heads, after 300 trials of a fair coin. In contrast to $N = 30$, it is possible to see how this approaches a Gaussian distribution with a mean around 150.

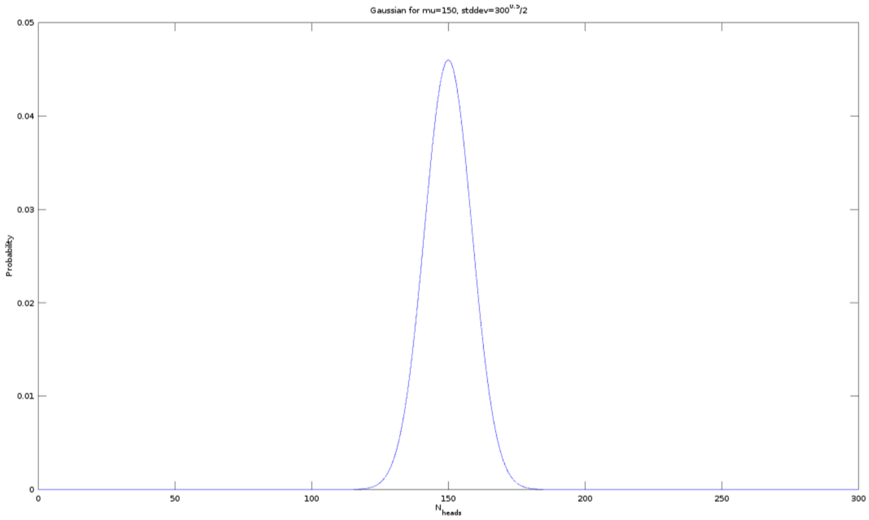


Figure 6.7: This is the Gaussian distribution for a mean of 150 and a standard deviation of $\frac{\sqrt{300}}{2}$. This is almost identical to the binomial distribution for the same figures. This is due to the central limit theorem.

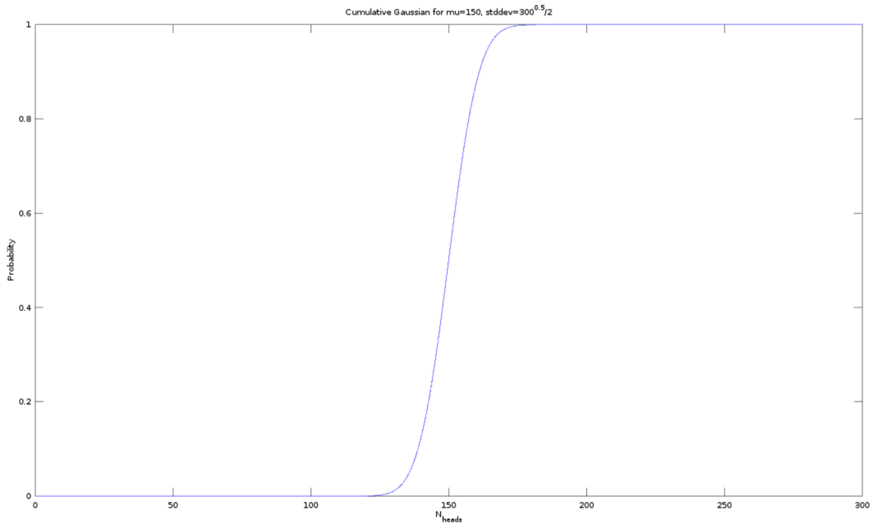


Figure 6.8: This is the cumulative probability distribution for a Gaussian with a mean of 150 and a standard deviation of $\frac{\sqrt{300}}{2}$.

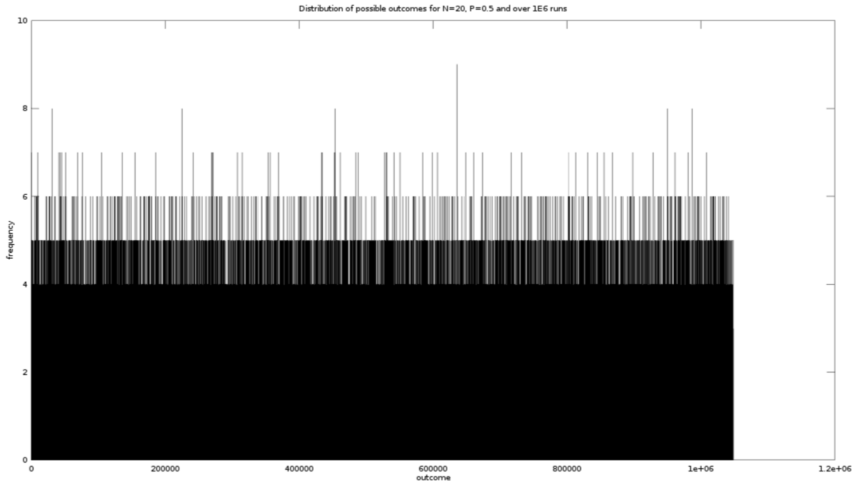


Figure 6.9: This is the probability distribution calculated through Monte Carlo simulations, for any ordered combination x_i of heads and tails where each possible ordered outcome has been mapped to a decimal number. Note that it is a uniform distribution.

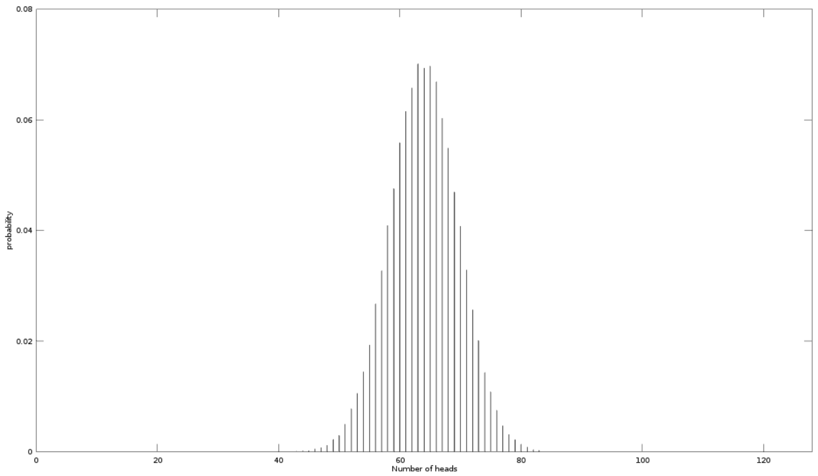


Figure 6.10: For N flips, this shows the probability of getting a number of heads, regardless of ordering. It is clearly Gaussian.

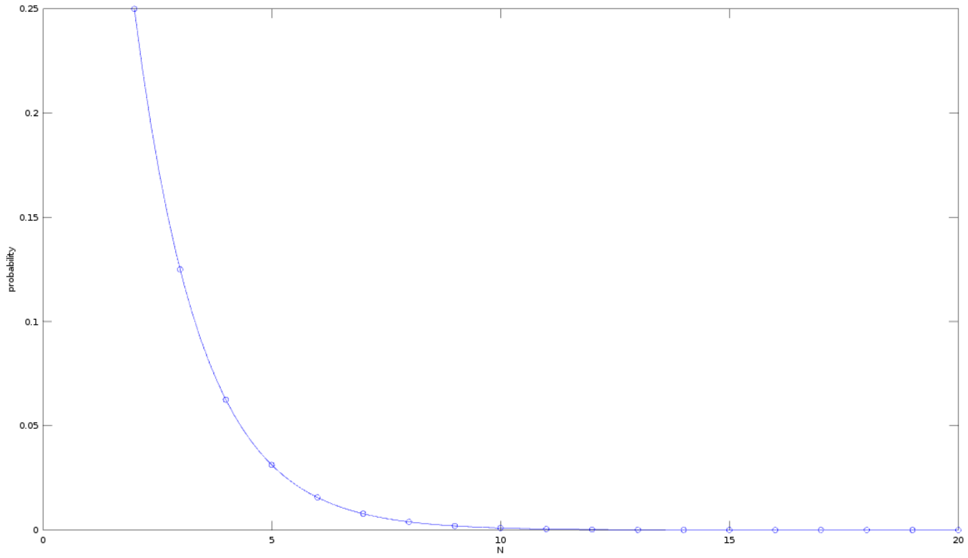


Figure 6.11: The Monte Carlo simulated probabilities for N flips are shown as circles, this is then fitted to $1/2^N$, showing how the probability of any outcome drops exponentially with number of flips.

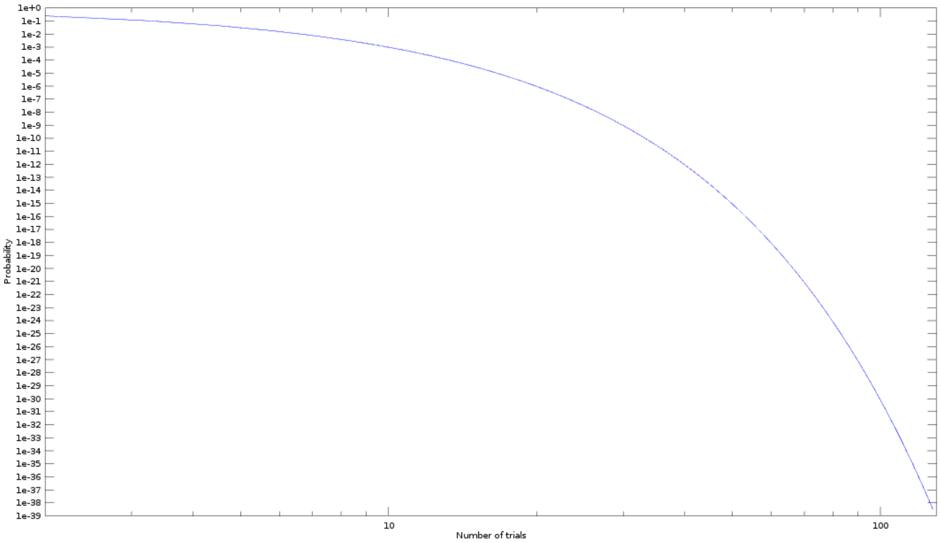


Figure 6.12: Following Figure 6.11 the probability distribution is extrapolated to 128 flips - it can be seen that the probability of getting any one outcome is 1×10^{-39}

to the square root of the number of counts:

$$\sigma_x \approx \frac{\sqrt{N}}{2} \tag{6.9}$$

and so the relative error is given by

$$\epsilon = \frac{\sigma_x}{N} \tag{6.10}$$

which gives 5% for 100, 0.5% for 1000 and so on. This means that the relative error also tends to zero as N tends to infinity and the result number of heads will close in on the mean value, however, for some value of N which is large but isn't actually infinite, then the resultant distribution will not be $\frac{N}{2}$.

Suppose that $P(x = H) = 0.5$ and there are 10^{12} experiments. It is expected that $N_H = 0.5 \times 10^{12}$ however the probability of getting exactly $\frac{N_H}{N_H + N_T} = \frac{1}{2}$ tends to zero for large N.

If two sets are generated, where one is generated by Alice, and the other by Bob, then, if using the expected values, one might expect a joint probability mass function to look something like this:

		Alice	
		H	T
Bob	H	0.25	0.25
	T	0.25	0.25

However it is already known that the outcomes will differ from this for a large N. To see how this impacts the statistical properties consider the following example. A typical joint probability mass function might look like this[1]:

		Alice		
		H	T	
Bob	H	0.245	0.238	$= 0.483$
	T	0.271	0.246	$= 0.517$
		$= 0.516$	$= 0.484$	

The covariance of (X, Y) for discrete X, Y is

$$\begin{aligned} \operatorname{cov}(X,Y) &= E(XY) - E(X)E(Y) && (6.11a) \\ &= E[(X - E[X])(Y - E[Y])] && (6.11b) \\ &= \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\left(x_i - E\left(X\right)\right)\left(y_j - E\left(Y\right)\right) && (6.11c) \end{aligned}$$

which comes out to be ≈ -0.0042. The covariance can be normalised by the standard deviations in X and Y (0.49999 and 0.49996 respectively for the example case) to give the correlation, in this case the correlation is -0.016914. This is non-zero, and indicates a (very small) amount of anti-correlation.

Recall that for statistical independence the following conditions must be met:

$$\begin{aligned} P(A \cap B) &= P(A) \cdot P(B) && (6.12a) \\ P(A|B) &= P(A) && (6.12b) \\ P(B|A) &= P(B) && (6.12c) \end{aligned}$$

[1] This example was generated from a simulated 1000 fair coin flips.

A non-zero covariance means that

$$\begin{aligned} E(XY) - E(X)E(Y) &\neq 0 \qquad (6.13a)\\ \implies \sum\sum XYP(XY) - \sum XP(X)\sum YP(Y) &\neq 0 \qquad (6.13b)\\ \implies \sum\sum XYP(XY) - \sum\sum XYP(X)P(Y) &\neq 0 \qquad (6.13c)\\ \implies \sum\sum XY(P(XY) - P(X)P(Y)) &\neq 0 \qquad (6.13d)\\ \implies P(XY) - P(X)P(Y) &\neq 0 \qquad (6.13e) \end{aligned}$$

which directly violates equation (6.12a) and thus the probability of being truly statistically independent decreases with N. For N large enough that the probability of getting exactly $N/2$ heads is zero, then any two sets of trials will have some small statistical dependence with each other and some bias towards correlation or anti-correlation.

One might expect that the chances of being correlated or anti-correlated are also equally likely. I.e. for K generations of large N sets by Alice and Bob one might expect that correlation would occur half the time and anti-correlation would occur half the time. However this is also beholden to the same probability statistics and thus the outcomes are biased towards either correlated or anti-correlated.

6.5 Relationship with Entropy

The mutual information between Alice and Bob can be given in terms of probabilities as

$$I(A:B) = \sum_a \sum_b P(A,B) \log \frac{P(A,B)}{P(A)P(B)} \quad . \qquad (6.14)$$

Given the definition (6.12a) for statistical independence, that sets of numbers with a non-zero covariance are statistically dependent and equation (6.13e) which shows that

$$\frac{P(X,Y)}{P(X)P(Y)} \neq 1 \qquad (6.15)$$

then $\log \frac{P(X,Y)}{P(X)P(Y)}$ is non zero. This results in positive mutual information between Alice and Bob, given that they generate two sets of random numbers, with large

N. Given that $P(x = 0.5)$ is not *quite* zero, there will be the rare instance when Alice and Bob generate sets where at least one has the 'expected' distribution of numbers (i.e. equal heads and tails) [1].

For all possible N, the mutual information is:

$$I(A_N : B_N) \geq 0 \qquad \forall N \quad , \tag{6.16}$$

where

$$B_N, A_N = \{0,1\}^N \quad . \tag{6.17}$$

However, since $I(A : B) > 0$ for $N \to \infty$, if this is repeated this several times, over, say K experiments (choosing K sets of N numbers) then:

$$\bar{I} = \frac{1}{N} \sum_i I_i(A_N : B_N) \tag{6.18}$$

where either

$$I_i = 0, \text{ or } I_i > 0 \quad , \tag{6.19}$$

then

$$\bar{I} > 0 \text{ for big enough } K \quad . \tag{6.20}$$

This is the same effect as Brownian motion i.e. there is a net movement owing to averages. There is also an entropic argument for this result; having a set of random numbers with zero correlation can be considered to be infinitely ordered for an infinitely big set, a set with zero entropy and zero information entropy.

6.6 Relationship with a Third Set of Numbers

So far it has been demonstrated that there is positive mutual information between Alice and Bob. The impact of a third person (who shall be called Eve) on the mutual information has not yet been considered, however.

Suppose now that three sets of random numbers (which shall again model be modelled as 'perfect' coin flips) are generated - sets that shall be designated Alice, Bob and Eve respectively.

[1] This can be combated however if Alice and Bob produce numbers with an odd N, or indeed by doing a brief check and rejecting any sets whose distributions are equal to the expectation value.

The interesting quantity is

$$I(X:Y|Z) = \sum_z \sum_y \sum_x P(X,Y,Z) \log \frac{P(Z)P(X,Y,Z)}{P(X,Z)P(Y,Z)} \tag{6.21}$$

which can be rewritten in terms of the chain rule for mutual information

$$I(X:Y|Z) = I(X:Y,Z) - I(X:Z) \quad . \tag{6.22}$$

If the quantity $I(X:Z)$ is less than $I(X:Y,Z)$ then $I(X:Y|Z)$ must be nonzero. The relationship between Eve and Bob and Eve and Alice will be the same as the relationship between Alice and Bob.

$$P(A,E) - P(A)P(E) \neq 0 \tag{6.23a}$$

$$P(B,E) - P(B)P(E) \neq 0 \tag{6.23b}$$

It can be deduced that $I(A:E)$ is non-zero. Similarly it can also be deduced that $P(X,Y,Z) - P(X)P(Y)P(Z) \neq 0$. Suppose the following:

$$P(X,Y) - P(X)P(Y) = \delta \tag{6.24a}$$

$$P(Y,Z) - P(Y)P(Z) = \epsilon \tag{6.24b}$$

$$P(X,Z) - P(X)P(Z) = \gamma \tag{6.24c}$$

$$P(X,Y,Z) - P(X)P(Y)P(Z) = \alpha \tag{6.24d}$$

This can be inserted into $\frac{P(Z)P(X,Y,Z)}{P(X,Y)P(Y,Z)}$ to obtain:

$$\frac{P(Z)(\alpha + P(X)P(Y)P(Z))}{(\gamma + P(X)P(Z))(\epsilon + P(Y)P(Z)} \quad . \tag{6.25}$$

Then

$$\frac{P(Z)\alpha + P(X)P(Y)P(Z)P(Z)}{\gamma\epsilon + \gamma P(Y)P(Z) + \epsilon P(X)P(Z) + P(X)P(Y)P(Z)P(Z)} \tag{6.26}$$

which, if this quantity evaluates to a value besides one, means that $I(A:B|E) > 0$. In order to check this, equate the two, and add some constant, Δ, which, for $\Delta = 0$ indicates no conditional mutual information, and conditional mutual information otherwise.

$$\begin{aligned} &P(Z)\alpha + P(X)P(Y)P(Z)^2 \\ &\qquad = \Delta + \gamma\epsilon + \gamma P(Y)P(Z) + \epsilon P(X)P(Z) + P(X)P(Y)P(Z)P(Z) \end{aligned} \tag{6.27}$$

rearranges to give

$$\Delta = P(Z)\alpha - \gamma\epsilon - \gamma P(Y)P(Z) - \epsilon P(X)P(Z) \quad . \tag{6.28}$$

Δ will only be equal to zero in the strict circumstances that the modifiers are zero, or, some exact combination which, since they vary will only be the case with a very small probability. This is the same scenario as seen previously:

$$I(X:Y|Z) = \frac{1}{N}\sum_i I_i(X:Y|Z) \tag{6.29}$$

where either

$$I_i(X:Y|Z) = 0\,,\text{or}\, I_i(X:Y|Z) > 0 \quad . \tag{6.30}$$

Over some large number of experiements this means that

$$I(A:B|E) > 0 \tag{6.31}$$

for a large enough K experiments. This results in some non-zero value in all parts of the Venn diagram. Note that this only holds if Eve does not have an exact copy of either Alice or Bob. Crucially, however, by pure guessing, the chances of replication of either Alice or Bob is $1/2^N$. If N is large, the number of repetitions required to get an exact copy is 2^N and as a result, a brute force attack is unreasonable.

The random numbers generated by Alice and Bob with these properties can be input into an algorithm such as advantage distillation discussed in Chapter 3. However, whilst Alice and Bob do not publish their number sets using the advantage distillation algorithm, Alice and Bob must be within a trusted environment when these numbers are produced - such as a shielded room.

6.7 Efficiency

Simulation of random numbers as a resource reveals that there is a baseline efficiency of 0.06%. For the bits sent between Alice and Bob, 0.06% will end up as a final key. Some bits will be required for authentication for each transmission. For n bits required per round for authentication, the starting number set will have to be of length $0.06\% \cdot n = 1667 \cdot n$ per transmission. For x rounds of transmission, the initial number set would have to be of length $1667 \cdot n \cdot x$ Assuming a 256 bit authentication per transmission, 4266667 bits per round will be required to meet the minimum level for efficency. The number of rounds of CASCADE required for this length of key varies dependent upon the bias in the random numbers. However, in the event that the bias in the random numbers is low enough that the number of rounds of CASCADE required is too beyond a certain limit, then the sets can be discarded and new sets generated. There is considerably more work to be done to find the optimum maximum rounds of CASCADE compared to the length of the keys and the bias between the two sets.

6.8 Conclusion

This chapter looked to the properties of random numbers as a potential resource for symmetric key creation using advantage distillation. To demonstrate suitability as a resource this chapter showed that there exists a positive mutual information $I(A : B|E) > 0$. This results from a natural bias inherent in a set of random numbers, despite the expectation that any set of true random numbers has equal quantities of all possible values. Since these numbers are randomly generated, then attacks from an eavesdropper are limited to attacks on the advantage distillation protocol, dealt with in Chapter 3. This shows that random numbers are a potential suitable resource for post quantum symmetric key distribution. One of the potential difficulties with this method is the large amount of redundancy within the production of a key. The number of bits required to exchange a 256 bit key would vary dependent upon the combination of protocols used to produce the key. This requires further examination to determine the efficiency of the protocol. The caveat to using random numbers as a resource is that they can be produced without any possibility of eavesdropping, for example, preparation in a shielded room. The assumption that a shielded room prevents eavesdropping is looked at more thoroughly in the next chapter.

7

A Side-Channel Attack Arising from Barrier Leakage

7.1 Novel Contributions

The only work which previously considers the vector potential as a mechanism for leakage through Faraday cages is (Gelinas, 1984; Kawakami & Yamashita, 1999; Konopinski, 1978; Puthoff, 1998; Zimmerman, 2011, 2013). None of these have experimentally examined this mechanism, or considered its viability as a vulnerabilty in security contexts. This work draws on basic knowledge of electromagnetism (specifically the formulation of the vector potential) and presents experimental work based on this in the context of Faraday cages as secure rooms.

7.2 Introduction

Shielded rooms and Faraday cages have been used for decades in the fight for cybersecurity, both commercially and within government. TEMPEST [1] attacks and eavesdropping are a significant threat to defence and containing signals within a shielded room is thought to eliminate this risk. This is based on the principle that electromagnetic signal leakage cannot occur though a Faraday cage (or

[1] TEMPEST is the American National Security Agency code name for the process of taking advantage of information from stray signals, as in (Marquardt *et al.*, 2011). It covers defensive emission security as well as offensive eavesdropping.

shield) owing to the properties of conventional transverse waves. However, it has come to light in recent times that some signal types may be able to penetrate Faraday cage type shielding possibly using the Aharanov-Bohm mechanism (Gelinas, 1984; Puthoff, 1998; Zimmerman, 2011, 2013). In this Chapter it is shown that these signals demonstrate a leakage risk. Longitudinal signals emitting within a shielded box are detected from outside the box, the extent is such that text based conversations can be held with simple off-the-shelf software defined radios.

7.2.1 Motivations

Various protocols for Continuous Variable Quantum Key Distribution (CVQKD) require that participating parties have a private and secure space to prepare states. Many CVQKD protocols assume this can be created by simply using a Faraday shielded box, and continue the protocol proof without further consideration. However literature (Gelinas, 1984; Kawakami & Yamashita, 1999; Konopinski, 1978; Puthoff, 1998; Zimmerman, 2011, 2013) has surfaced which indicates that this aspect deserves some scrutiny. In order to be assured of the secure implementation of the proposed protocol, one must first examine the realism of the assumption that a secure space can be created.

7.2.2 Typical Assumptions

A secure space could normally be assumed on the understanding that a shielded room and Faraday cage combination will provide the required security. Shielded rooms and Faraday cages have been used to secure and protect against eavesdropping and TEMPEST attacks for a number of years (Agrawal *et al.*, 2003). The principle is simple. Contain all electromagnetic emissions within a single room (where no signals can escape, leak, or be observed by an adversary), using the ability of a Faraday cage to 'neutralise' an internal electric field resulting in zero electric field externally. This ability certainly holds true for conventional, transverse signals. However, some research suggests that a property of the signal called the vector potential, and therefore information about the signal, can leak through a Faraday cage (Gelinas, 1984; Kawakami & Yamashita, 1999; Puthoff, 1998). This Chapter describes a quantum eavesdropping method, detecting the vector potential by using the Aharanov-Bohm effect for a possible side-channel attack on various CVQKD protocols.

7.2.3 Implications

Clearly, if such an eavesdropping method is possible there is a significant question regarding the security of Faraday cages and shielded rooms. This has the consequence of voiding the security of many existing protocols (especially CVQKD protocols) and current TEMPEST defences until a solution to this side-channel attack can be found. This presents a dilemma to governments and other organisations currently relying upon Faraday cages and shielded rooms to secure their communications. Furthermore, some researchers may rely on Faraday shielding to perform experiments in an EM-free zone.

7.2.4 Chapter Outline

This Chapter outlines the possibilities for vector potential leakage, including an investigation of the signal propagation through various shielding barriers. It starts with a presentation of the theory behind such effects, a look at pre-existing literature, and preliminary simulations of signals using the COMSOL simulation software package. The Chapter then moves on to present experimental findings and summarise the possibility of risk to eavesdropping in shielding scenarios.

7.3 Background

7.3.1 Shielding Methods

There are two principal mechanisms through which leakage is prevented - Faraday shielding and attenuation. The former requires a continuous metal barrier, or cage, which may have holes provided their size is small compared to the wavelength being blocked. As the metal barrier is conductive the charge which builds up (as a result of the electric field) is allowed to neutralise through movement of charge carriers along the metal. This is, however, not entirely fool-proof; some residual fields can leak through depending on the conductivity of the Faraday cage, the size of holes and the continuity quality. Attenuation is used to dampen these stray signals, a thickness of field-dampening material is added so that the field strength through the barrier decreases exponentially with thickness until it can be considered to be negligible and 'undetectable'. These are particularly designed with a focus towards transverse signal types and work very effectively in blocking this type of signal, thanks to years of engineering efforts.

7.3.2 The Vector Potential

The eavesdropping mechanisms outlined in (Gelinas, 1984; Kawakami & Yamashita, 1999; Konopinski, 1978; Puthoff, 1998; Zimmerman, 2011, 2013) are based on the use of the vector potential and the Aharonov-Bohm effect[1]. What follows is a study of significant features of the magnetic vector potential so that it may be further understood in the context of these mechanisms.[2]

The explanation commences with a complete description of the electric ($\mathbf{E}$) and magnetic ($\mathbf{B}$) fields in the form of the differential Maxwell equations.

Gauss' law states

$$\boldsymbol{\nabla} \cdot \mathbf{E} = \frac{\rho}{\varepsilon_0} \tag{7.1}$$

where ρ is the electric charge density and ε_0 is the physical constant of vacuum permittivity. Gauss' law for magnetism states

$$\boldsymbol{\nabla} \cdot \mathbf{B} = 0 \tag{7.2}$$

and together the Gauss laws define the fundamental fields. The following two laws link the two fields. Faraday's law of magnetic induction is

$$\boldsymbol{\nabla} \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \quad , \tag{7.3}$$

[1] Technically the Aharanov-Bohm effect is specifically the phase effect of the vector potential presence; in this instance it is a reference to the physicaly observable effect of a non-zero vector potential

[2] This treatment of the vector potential approximately follows the method of that in (Townsend, 2000), which should be sought for further details. Similarly, (Barbieri *et al.*, 2013) provides a transparent explanation of the physical effects of the vector potential.

defining the electric field as a spatial response to a time variant magnetic field. Finally, Ampere's law is

$$\boldsymbol{\nabla} \times \mathbf{B} = \mu_0 \mathbf{j} + \mu_0 \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t} \quad , \tag{7.4}$$

where μ_0 is the magnetic permeability and the $\mathbf{j}$ term referes to charges moving through the fields which is zero in the case that there are no additional charges present. Together these four laws provide a complete description of the EM fields.

The vector calculus identity stating that the divergence of a curl is zero

$$\boldsymbol{\nabla} \cdot \boldsymbol{\nabla} \times \mathbf{f} = 0 \tag{7.5}$$

can be used with Gauss' law (7.2) so that the magnetic field $\mathbf{B}$ can be written in terms of a hypothetical quantity that is called the 'vector potential':

$$\mathbf{B} = \boldsymbol{\nabla} \times \mathbf{A}. \tag{7.6}$$

It is easy to see that (7.2) holds given (7.5). However Faraday's law (7.3) becomes:

$$\boldsymbol{\nabla} \times \left(\mathbf{E} + \frac{1}{c} \frac{\partial \mathbf{A}}{\partial t} \right) = 0, \tag{7.7}$$

and using the vector calculus identity that the curl of the gradient is zero:

$$\boldsymbol{\nabla} \times \boldsymbol{\nabla} f = 0, \tag{7.8}$$

then there is the possibility that

$$\mathbf{E} + \frac{1}{c} \frac{\partial \mathbf{A}}{\partial t} = -\boldsymbol{\nabla} \varphi. \tag{7.9}$$

where φ is some arbitrary scalar potential. Note that this means the vector potential, $\mathbf{A}$, can be transformed by the addition of some scalar potential function χ:

$$\mathbf{A} \rightarrow \mathbf{A} + \boldsymbol{\nabla} \chi; \tag{7.10}$$

as long as the scalar potential is also transformed by

$$\varphi \rightarrow \varphi - \frac{1}{c} \frac{\partial \chi}{\partial t}. \tag{7.11}$$

This is a gauge transformation - the potentials $\mathbf{A}$ and φ are altered but the physicality of the fields $\mathbf{E}$ and $\mathbf{B}$ remain unchanged; this is known as gauge invariance.

7.3.3 The Aharonov-Bohm Effect

To see how the role of the vector potential can influence the detection of a field, despite the field remaining gauge invariant, one can consider the Aharanov-Bohm effect, first derived in (Aharonov & Bohm, 1959). [1]

Consider first a scenario in which a magnetic field is confined to the interior of a hollow cylindrical shell (as in figure 7.1), for example a solenoid in the 'long' approximation [2] Taking the vector potential equation (7.6) in the integral form, the flux of the magnetic field through a surface **S** can be written in terms of the vector potential as:

$$\int \mathbf{B} \cdot d\mathbf{S} = \int (\boldsymbol{\nabla} \times \mathbf{A}) \cdot d\mathbf{S}. \tag{7.12}$$

To analyse the left hand side use can be made of Stokes' theorem:

$$\oint \mathbf{A} \cdot \mathrm{d}\mathbf{r} = \int (\boldsymbol{\nabla} \times \mathbf{A}) \cdot \mathrm{d}\mathbf{S}. \tag{7.13}$$

This means that for radii $\rho < R$ then (7.12) becomes:

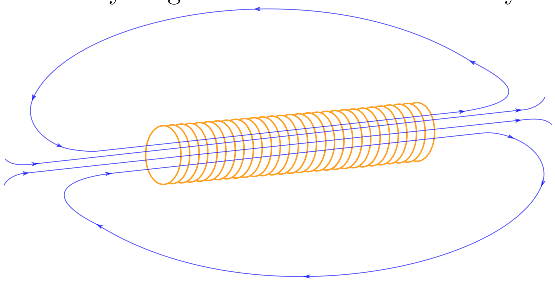
$$\int \mathbf{B} \cdot \mathrm{d}\mathbf{S} = \oint \mathbf{A} \cdot \mathrm{d}\mathbf{r} = |\mathbf{A}|\, 2\pi\rho = B_0 \pi \rho^2 \quad . \tag{7.14}$$

Thus, using the azimuthal symmetric property of the cylinder the vector potential is

$$\mathbf{A} = \left(\frac{B_0 \rho}{2}\right) \hat{\boldsymbol{\varphi}} \qquad \rho < R \tag{7.15}$$

[1] Note that this follows the explanation given in (Townsend, 2000) and (Sakurai & Napolitano, 2011) which provide further detail if required.

[2] For a 'long' solenoid its external fields are considered to be so weak as to be non-present. An infinitely long solenoid would not have any field lines which meet outside the solenoid.



The imagined cylinder has some radius R, and for all radii $\rho > R$, then $\mathbf{B} = 0$. The inside of the cylinder ($\rho < R$) can be considered to have a uniform magnetic field $\mathbf{B} = 0 \cdot \hat{\boldsymbol{\rho}} + 0 \cdot \hat{\boldsymbol{\varphi}} + B_0 \hat{\mathbf{z}}$.

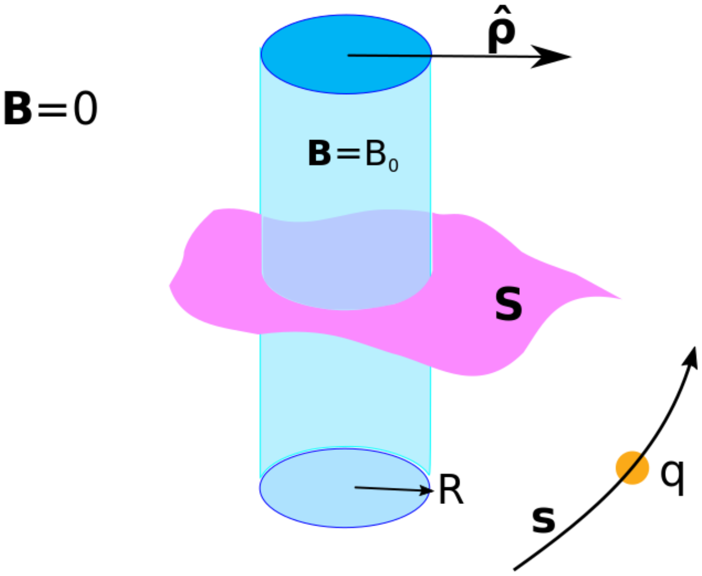


Figure 7.1: A hollow cylinder with a magnetic field, B_0, inside and no magnetic field outside, a surface **S** which it penetrates and in the presence of a charge q moving along the path **s**.

and for all points beyond the cylinder **B** has been defined to zero so using the confined definition of the magnetic field:

$$\mathbf{A} = \left(\frac{B_0 R^2}{2\rho}\right)\hat{\boldsymbol{\varphi}} \qquad \rho > R. \tag{7.16}$$

This can be checked by applying the gradient to the curl of **A** giving B_0 inside the cylinder and 0 outside.

Now that the vector potential for the imagined cylinder has been derived, it is interesting to investigate what happens to a charge, q, travelling at some velocity **v** along some path **s** in its presence. It is useful to consider the modified Lagrangian [1]for this:

$$L = \frac{1}{2}m\mathbf{v}^2 - q\varphi + \frac{q}{c}\mathbf{A}\cdot\mathbf{v} \tag{7.17}$$

For some segement of the path that the charge travels along, between the times t and $t + \delta t$, the change in 'action', S, of the particle[2] can be seen as

$$S_{\text{no }\mathbf{A}\text{ present}} \rightarrow S_{\text{no }\mathbf{A}\text{ present}} + \frac{q}{c}\int_t^{t+\delta t} \mathrm{d}t\,\mathbf{v}\cdot\mathbf{A} \tag{7.18}$$

where the integral can be rewritten with respect to the length of the path, d**s**:

$$\frac{q}{c}\int_t^{t+\delta t} \mathrm{d}t\left(\frac{\mathrm{d}\mathbf{x}}{\mathrm{d}t}\right)\cdot\mathbf{A} = \frac{q}{c}\int_x^{x+\delta x} \mathbf{A}\cdot\mathrm{d}\mathbf{s}. \tag{7.19}$$

Using Feynmann's method of path integrals for all possible quantum paths (as outlined in (Sakurai & Napolitano, 2011; Townsend, 2000)), the path amplitude ψ of a charge q without the presence of the modified vector potential is given by

$$\langle x', t'|\, x_0, t_0\rangle = \int_{x_0}^{x'} \mathcal{D}\left[x(t)\right] e^{\frac{i}{\hbar}S[x(t)]} \tag{7.20}$$

where S is the action from the Lagrangian. and $\mathcal{D}$ is a shorthand notation to represent the infinite number of possible path integrals given by

$$\int_{x_0}^{x'} \mathcal{D}\left[x(t)\right] = \lim_{N\to\infty}\int \mathrm{d}x_1 \ldots \int \mathrm{d}x_{N-1}\left(\frac{m}{2\pi\hbar i\Delta t}\right)^{\frac{N}{2}}. \tag{7.21}$$

[1] The Lagrangian describes the energy of a model, and for a charge without the vector potential present the Lagrangian would be $L = \frac{1}{2}m\mathbf{v}^2 - q\varphi$

[2] The action of a particle is the time integral of the Lagrangian of that particle and describes how the system evolves.

for N path segements, particle mass m and over time interval Δt. The addition of the magnetic vector potential to the Lagrangian calls for the modification of this path amplitude to

$$\langle x', t' |\, x_0, t_0\rangle = \int_{x_0}^{x'} \mathcal{D}\left[x(t)\right] e^{\frac{i}{\hbar}S[x(t)]} e^{\frac{iq}{\hbar c}\int_{x_0}^{x'} \mathbf{A}\cdot\mathbf{ds}} \tag{7.22}$$

There are two paths that require consideration in order to observe the Aharanov-Bohm effect, i.e. the paths going opposite sides of the cylinder. Without the cylinder, these paths are ψ_1 and ψ_2. The modified paths, $\psi_{1,2}$ are then

$$\psi_1' = \psi_1 e^{\frac{iq}{\hbar c}\int\limits_{\text{path1}} \mathbf{A}\cdot\mathbf{ds}} \tag{7.23a}$$

$$\psi_2' = \psi_2 e^{\frac{iq}{\hbar c}\int\limits_{\text{path2}} \mathbf{A}\cdot\mathbf{ds}}. \tag{7.23b}$$

The total path amplitude for the particle to go around the cylinder is then

$$\psi_{total} = \psi_1' + \psi_2' \tag{7.24a}$$

$$= \psi_1 e^{\frac{iq}{\hbar c}\int\limits_{\text{path1}} \mathbf{A}\cdot\mathbf{ds}} + \psi_2 e^{\frac{iq}{\hbar c}\int\limits_{\text{path2}} \mathbf{A}\cdot\mathbf{ds}} \tag{7.24b}$$

$$= e^{\frac{iq}{\hbar c}\int\limits_{\text{path2}} \mathbf{A}\cdot\mathbf{ds}} \left(\psi_1 e^{\frac{iq}{\hbar c}\int\limits_{\text{path1}} \mathbf{A}\cdot\mathbf{ds} - \int\limits_{\text{path2}} \mathbf{A}\cdot\mathbf{ds}} + \psi_2\right) \tag{7.24c}$$

$$= e^{\frac{iq}{\hbar c}\int\limits_{\text{path2}} \mathbf{A}\cdot\mathbf{ds}} \left(\psi_1 e^{\frac{iq}{\hbar c}\oint \mathbf{A}\cdot\mathbf{ds}} + \psi_2\right). \tag{7.24d}$$

It can be seen that there is a change of relative phase $e^{\frac{iq}{\hbar c}\oint \mathbf{A}\cdot\mathbf{ds}}$ between path 1 and path 2 as a result of the vector potential presence. Using Stokes' theorem (7.13) the line integral of the vector potential can be related to the magnetic flux, $\Phi_B = \int \mathbf{B}\cdot d\mathbf{S}$. Consequently, as the magnetic field strength varies the relative phase between the two paths varies by $\left(\frac{q}{\hbar c}\right)\Phi_B$. This has an effect on the interference pattern for the charged particle - the probability of observing the particle in some interference region gains a sinusoidal component given by the period $\frac{2\pi\hbar c}{|q|\Psi_B}$ where even numbered multiples give rise to no evident change in interference pattern, and odd numbered multiples give rise to an 180° out-of-phase pattern - i.e. the exact opposite.

This unusual mathematical implication has been physically observed and verified, for example in (Chambers, 1960; Tonomura, 1982). This is considered on the scale of a ‘long’ solenoid. However, a shielded room can be modelled in a similar way, where the Faraday cage encircling the room is equivalent to the solenoid. A magnetic field is confined to a box from which it may not ‘leak out’ and so it cannot be ‘seen’ by the environment. However, charged particles in the environment can be influenced by the presence of the vector potential eminating from within the box. This effect refers specifically to phase change but, whilst this is a useful tool, it isn’t the only observable - a result of the dynamic vector potential is outlined in the next section and is easier to exploit.

7.3.4 The Dynamic Vector Potential

To further elaborate on the detection of the vector potential one can consider the dynamic electromagnetic field equation - Faraday’s law of induction (7.3). Given the definition of the vector potential, (7.6), (7.3) can be rewritten as

$$\boldsymbol{\nabla} \times \mathbf{E} = -\frac{\partial\left(\boldsymbol{\nabla} \times \mathbf{A}\right)}{\partial t} \tag{7.25}$$

which then reveals the electric field as an observable of an oscillating vector potential:

$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t} - \boldsymbol{\nabla}\Phi \tag{7.26}$$

or equivalently

$$\mathbf{E} = -\frac{1}{c}\frac{\partial \mathbf{A}}{\partial t} \tag{7.27}$$

if choosing the Coulomb gauge (by imposing the condition $\boldsymbol{\nabla} \cdot \mathbf{A} = 0$) and using the Gaussian unit form of the Maxwell equations. It is important to note that signals inside a shielded room are not static- they are dynamic electromagnetic fields. As such there is an oscillating vector potential beyond the confines of the shielded room, regardless of the strength of the shielding.

Further characterisation of this oscillating vector potential field can be achieved upon manipulation of the Maxwell equations. Using the relationship between electric field and vector potential in Faraday’s law of induction (7.4) in Gaussian units then a wave equation for $\mathbf{A}$ is produced:

$$\boldsymbol{\nabla} \times \left(\boldsymbol{\nabla} \times \mathbf{A}\right) - \frac{1}{c}\frac{\partial - \frac{1}{c}\frac{\partial \mathbf{A}}{\partial t}}{\partial t} = \boldsymbol{\nabla}^2\mathbf{A} - \frac{1}{c^2}\frac{\partial^2 \mathbf{A}}{\partial t^2} = 0 \tag{7.28}$$

with a set of 'vector potential' wave solutions written as

$$\mathbf{A}(\mathbf{x},t) = \mathbf{A}(\mathbf{k})e^{\pm i\mathbf{k}\cdot\mathbf{x}}e^{\pm i\omega t} \tag{7.29}$$

with $\omega = |\mathbf{k}|\, c$. Additionally, the Coulomb gauge condition means that

$$\mathbf{k}\cdot\mathbf{A}(\mathbf{k}) = \pm i\mathbf{k}\cdot\mathbf{A}(\mathbf{x},t) = 0 \tag{7.30}$$

revealing that the direction of $\mathbf{A}(\mathbf{x},t)$ is perpendicular to the direction of propagation ($\mathbf{k}$). Consequently it is apparent that the resultant observable static electric field from equation (7.27) should be longitudinal with respect to the source of the signal. It can be argued that longitudinal static electric fields can propagate through a boundary and that the use of the vector potential is unnecessary. An explanation can be found in (Boyer, 2000) and the observation of the 'Maxwell-Lodge' effect - a classical equivalent to the Aharonv-Bohm effect with classical only observables - in (Rousseaux *et al.*, 2008) and (Iencinella & Matteucci, 2004). Furthermore, similar vector potential effects can be seen in the Mercereau effect with superconductors (Jaklevic *et al.*, 1964). This provides overwhelming evidence that the vector potential can provide opportunities for communications security breaches.

7.3.5 Consequencies of the Boundary

An electromagnetic field is attenuated by a conductive boundary, whereas an electric only field is able to move through a conducting boundary. These static fields create a polarization within the conductor and the field is cancelled on the inside of the conductor only. The resultant polarization creates an electric field outside the boundary. However a propagating field can be attenuated as moving charges act to counterbalance the field. It is important to note that the field is 'attenuated' only and not 'stopped'- this is because the field cannot be discontinuous at a boundary. The remaining field can be thought of as an 'evanescent' field at this point. In this way a transverse electric field will be attenuated and the longitudinal vector potential induced electric field will be transmitted at the boundary of a Faraday shield.

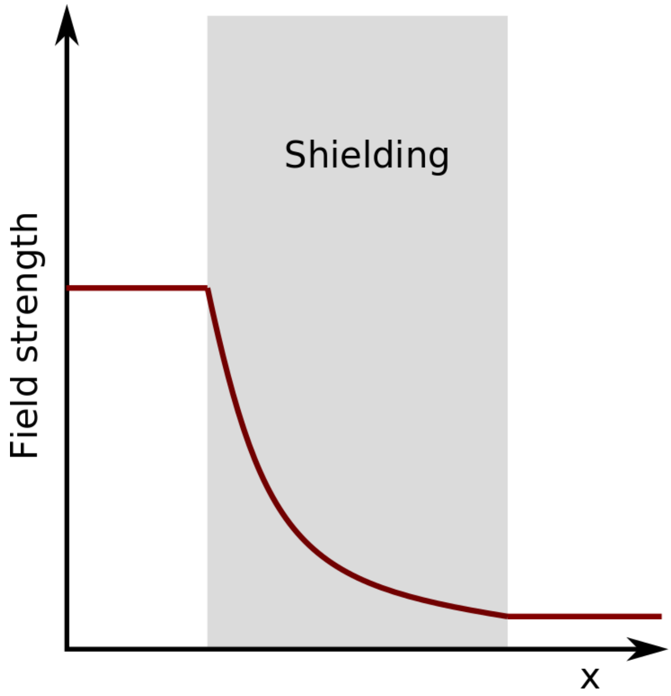


Figure 7.2: A portrayal of barrier tunnelling and evansencent fields.

7.3.6 Evanescent Wave Coupling and Barrier Tunnelling

Evanescent field effects are also referred to frequently as ‘magnetic coupling’ and are a near-field effect only. EM fields are attenuated through Faraday shielding barriers and are the source of the need for a significant thickness of material as outlined in previous sections. The field will decay exponentially along the barrier and then continue through free space at the other end as shown in figure 7.2.This is a tunnelling effect and can be described using similar mechanics to quantum tunnelling.

7.3.7 Characteristics of Barrier Penetration

It has been shown that there are two possible barrier penetration mechanisms to consider: the far-field ‘curl-free’ electic field, and the near-field evanescent effect. They are distinct effects however they are very strongly related. For example in the Goubau transmission line (Goubau, 1954, 1960) surface waves are propagating using the mechanism of the longitudinal electric field described here, but have very similar characteristics to evanescent waves. This is discussed further in (Liu & Lalanne, 2008).

7.3.8 The Zimmerman Discrepancy

The Zimmerman experiments of (Zimmerman, 2011, 2013) use a U-shaped plasma tube for detection of the vector potential field. The results suggest that changing the direction of current flow of the plasma in the tube has an affect on the strength of the observable field. This is the only result not in agreement with the understanding of the vector potential mechanism. However, testing by an undergraduate student revealed that this was a result of asymmetries in the equipment used to supply excitation current and not related to the vector potential(Munroe, 2015).

7.4 Simulations of Barrier Penetration

In order to assess the risk from these mechanisms it is useful to examine some models. As outlined above any risk from the vector potential will manifest as an electric field in a longitudinal direction. The COMSOL multiphysics modelling software package was used to analyse the longitudinal electric fields in various situations considering also the effects of Faraday shielding and grounding.

7.4.1 Capacitor

Why a capacitor?

The most basic formulation of interest is simply a transmitter and receiver of a longitudinal electric field. The transmitter and receiver can be considered as two metal objects, with a dielectric and a longitudinal electric field in between. A simple air gap parallel plate capacitor model provides a starting point for understanding the behaviours of longitudinal fields and how they may behave when interacting with, say, a Faraday shield, by looking at just two metal plates. Simple extensions to this include adding a metal ‘shield’ between the two plates, experimenting with grounding levels, and extending the metal shield into a complete box thereby simulating a Faraday shield.

Parallel Plate Air Gap Capacitor

Two cylindrical metal plates were constructed with SolidWorks and the voltage of one of the plates raised to 1 Volt (the other kept at 0) in COMSOL, generating a static, longitudinal, constant gradient **E** field between the two plates. The electric field was modelled, shown in figure 7.3, giving a region in the airgap with a field as expected. This is consistent with typical knowledge of a capacitor and also the model of a transmitting and receiving **E** field plate model.

Parallel Plate Capacitor with Air Gap Shield

The first natural extension to the parallel plate capacitor model is to consider what happens when a metal shield is placed in the air gap. This is equivalent to examining how the longitudinal electric field may respond to a sheet of metal being placed between transmitting and receiving nodes. The SolidWorks model for this can be seen in figure 7.3. It is clear to see in figure 7.3 that there is almost no effect on the electric field (with the exception of some small edge artifacts). There is no electric field through the metal- this is because electrons neutralise the voltage. However, the surface is then polarized. This is strikingly different to a transverse electric field, which would not penetrate through metal.

Boxed Capacitor

A metal shield is simply not enough for a complete model. A Faraday shield consists of an entirely enclosed metal box. If the metal air gap shield is extended to a box then the model can simulate the effects of a shielded room. A Faraday shield was constructed in SolidWorks as seen in figure 7.4 (note that the incoming wire is not attached to the box). COMSOL then was used to calculate the electric field - shown in figure 7.4. The electric field still penetrates the walls of the box, however this time the entire metal box becomes a source of sorts - charges move to neutralize the fields on both sides, resulting in a polarized surface on the edge of the box. This occurs even if the box is grounded - which is the explicit case shown in figure 7.4.

Conclusions

The model so far has highlighted the ways in which the longitudinal electric field responds with respect to barriers, in ways that would not be expected of transverse electric fields. It can penetrate shields and Faraday cages without any difficulty or attenuation. This is due to the charge response inside the metal, resulting in polarised surfaces.

7.4.2 Zimmerman Aerial and Capacitor

Having established some basic understanding of the longitudinal electric field it is possible to extend the model to look at the radiating dipole antenna. This is similar to that used by Zimmerman in (Zimmerman, 2011). This provides the opportunity to investigate the dynamic effects. Figure 7.5 shows the radiation pattern from a dipole antenna. The capacitor model above was then utilised to elucidate the longitudinal electric field. The expanded region shows the direction of the electric field as longitudinal in the region emanating directly from the end of the antenna. The capacitor can be considered as a capacitive voltage receiver, where the electric field penetrates the conducting boundaries of the receiver.

Conclusions

It can be inferred from this model that a standard radiative dipole antenna does produce longitudinal electric fields as predicted in the theory section of this chapter. However they are produced emanating from the very end of the antenna, not in the typical transverse direction. This means that longitudinal electric fields can possibly be isolated from their transverse counterparts for experimental investigation, by examining the differences between fields emanating from the sides versus the tip.

7.4.3 Toroidal antenna

Toroidal antenna motivation

In order to improve upon the possible isolation of longitudinal from transverse electric fields that can be seen using a dipole antenna, it is possible to develop an antenna which has no transverse radiation. It is possible to draw inspiration from toroidal chokes (such as those commonly found in electrical devices). If one imagines the Poynting vector (the direction of energy flux in an electromagnetic field) of a loop of current carrying wire around a ferrite core, it will be radial towards the center of the core. If several of these are added together, creating a toroid, the overall electron drift is in the direction of the wire turning around the coil and thus the overall Poynting vector of the toroid will also be radial, this time towards the center of the toroid. This means that there will be no overall transverse electromagnetic waves radiating from this construction. However, the vector potential is not cancelled out by the symmetry of the toroid. The radial components of the vector potential will be negated by each other, but the components on the inside and outside diameters will not completely cancel, resulting in a net vector potential in the plane normal to that of the toroid. As such there will be a time varying electric field as a result, without the presence of transverse electromagnetic fields. This offers the possibility of a longitudinal-only producing antenna using a toroidal wound solenoid. An off the shelf toroidal choke would be ideal for this.

Summary

The toroidal model construction from (Everitt, 2015) is summarised here. The SolidWorks model constructed in (Everitt, 2015) is shown in figure 7.6, which is then used in COMSOL multiphysics to model the electric field as a result of the vector potential, shown in figure 7.7. It can clearly be seen that there is a resultant electric field (as a result of the net vector potential) in the direction normal to the plane of the toroid, as predicted. This suggests that using a toroidal solenoid as an antenna in the investigation of leakage will help to isolate the effects that exist as a result of the electric field.

7.4.4 Limitations of COMSOL

Thus far the electric field based model provided by COMSOL has been used. However one can compare this with the RF based model also provided in COMSOL to investigate the strengths and weaknesses of COMSOL as a modelling package. Of particular interest is COMSOL's handling of the vector potential induced electric field, isolated by using the model of a toroidal antenna in the previous section, and observing how this relates to a metal plate (such as one used in the capacitor model). The model set-up is shown in 7.8, importing the toroidal model from (Everitt, 2015). If one examines the strength of the electric field using the RF package, in a direction normal to the toroidal plane one can see that (in figure 7.8) if the path is unimpeded (the red line) the field just attenuates as one would expect through free space. However with the metal plate, there is a discontinuity (blue line) and the field goes to zero immediately. This indicates that the metal is being treated purely as an attenuator rather than the electron plasma that allows for the more unusual effects which could be exploitable. This means that COMSOL modelling cannot be reliable for investigating all the possible effects and real world experimentation is necessary.

7.4.5 Simulation Conclusions

The simulations performed indicate that electric fields arising as a result of a vector potential can pass through Faraday shielding, and that a variety of novel antennas can be used to generate a dynamic electric field resulting from the vector potential. This clarifies that there is a potential risk for information leakage during state preparation in a cryptographic context. An experimental realisation would be the next stage to check if the modelling results are as damning as they appear.

7.5 Analysing the Risk of Side Channel Attacks

Recall that the motivation for this investigation comes from the risk of information leaking uncontrollably from within a completely shielded environment, such

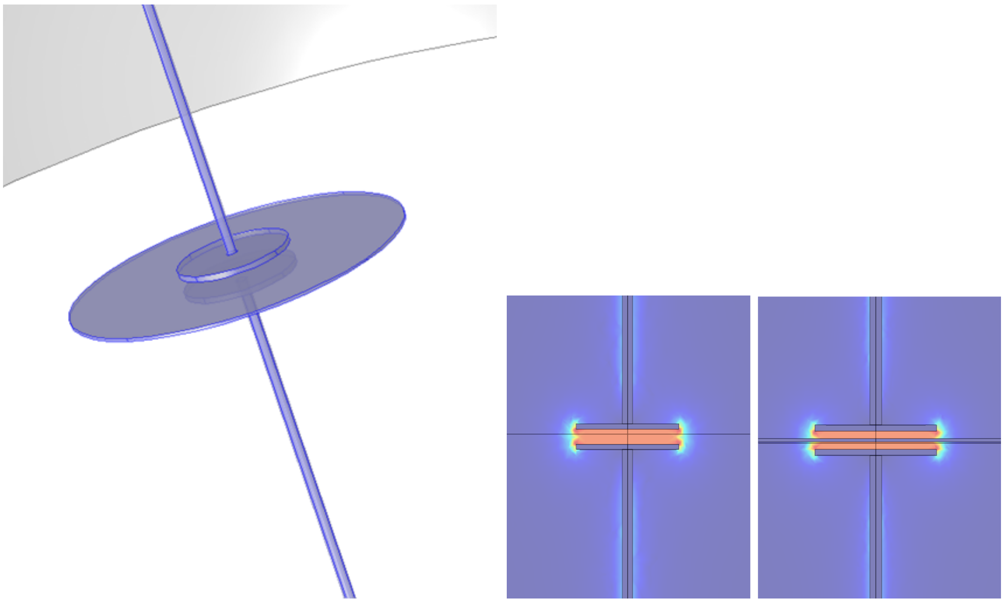


Figure 7.3: A COMSOL model of a parallel plate capacitor with a shield. The model is on the left, and a cross section of the electric fields on the right with and without a grounded shield. The electric field polarizes the metal to remove the electric field from inside of the metal.

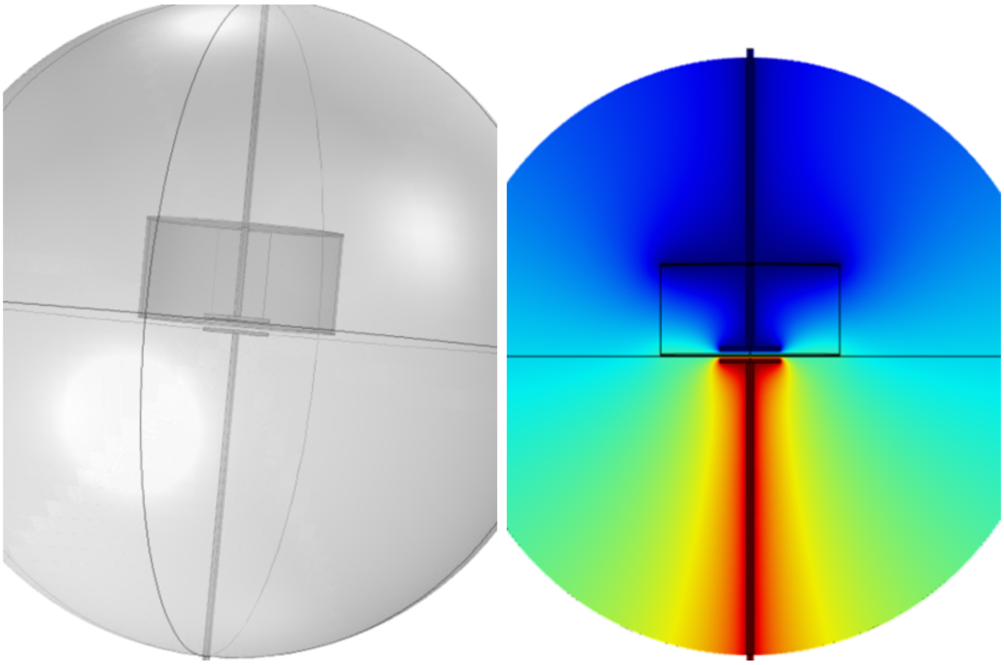


Figure 7.4: A COMSOL model (left) of a parallel plate capacitor with one plate enclosed within a Faraday shield. The electric field (right) still penetrates the walls of the shield.

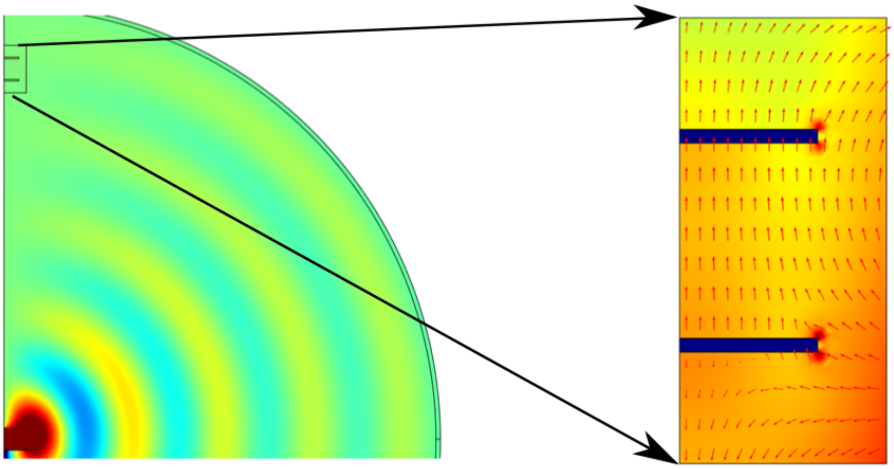


Figure 7.5: A COMSOL model of the Zimmerman aerial and 'field detector' The detector is modeled as two parallel plates with the aim of determining the electric field between the plates. This shows that measurable voltage can be determined.

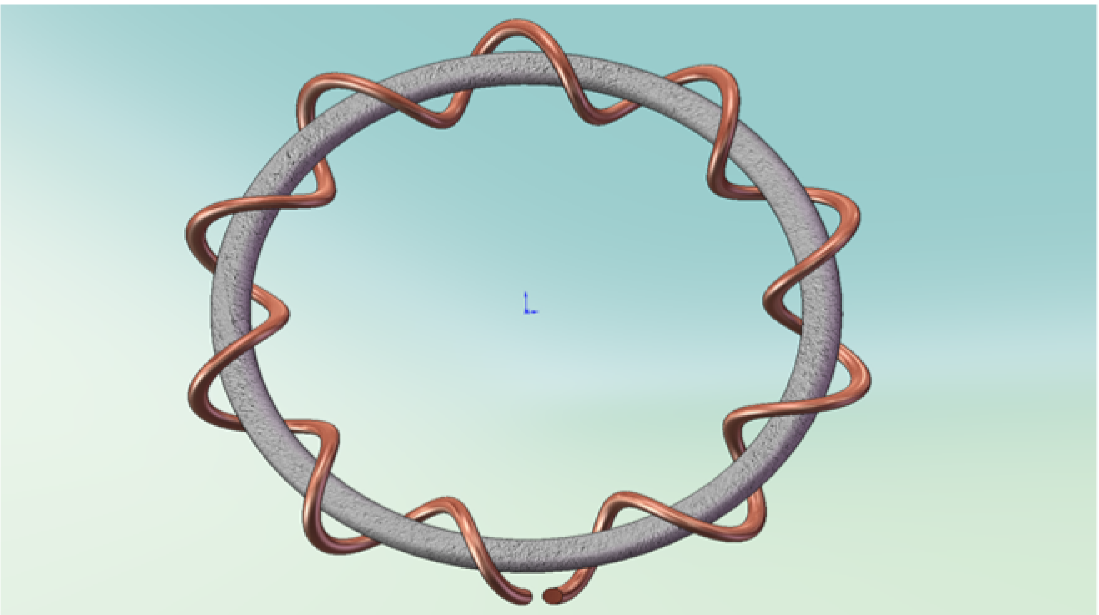


Figure 7.6: A SolidWorks model of toroidal winding around a ferrite core (from (Everitt, 2015)).

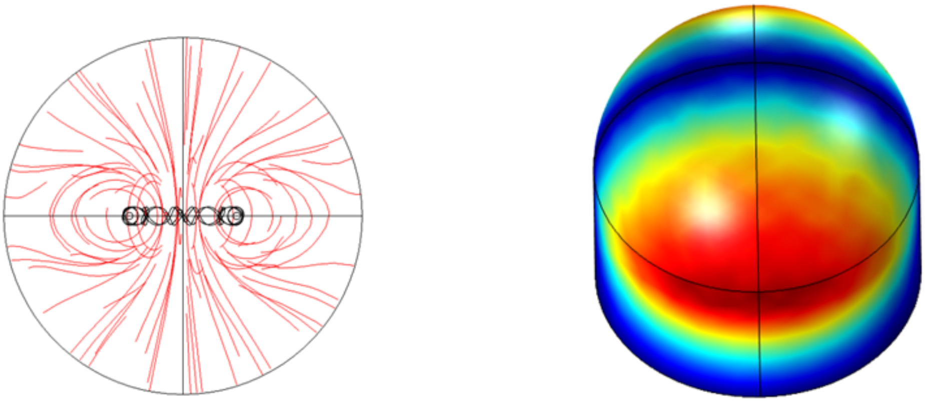


Figure 7.7: The vector potential emitted from the toroidal aerial is shown in terms of the electric field. The longitudinal electric field generated by the toroid is highlighted in red (left). The colour map (right) represents the electric field intensity, where red indicates high intensity and blue indicates low intensity.

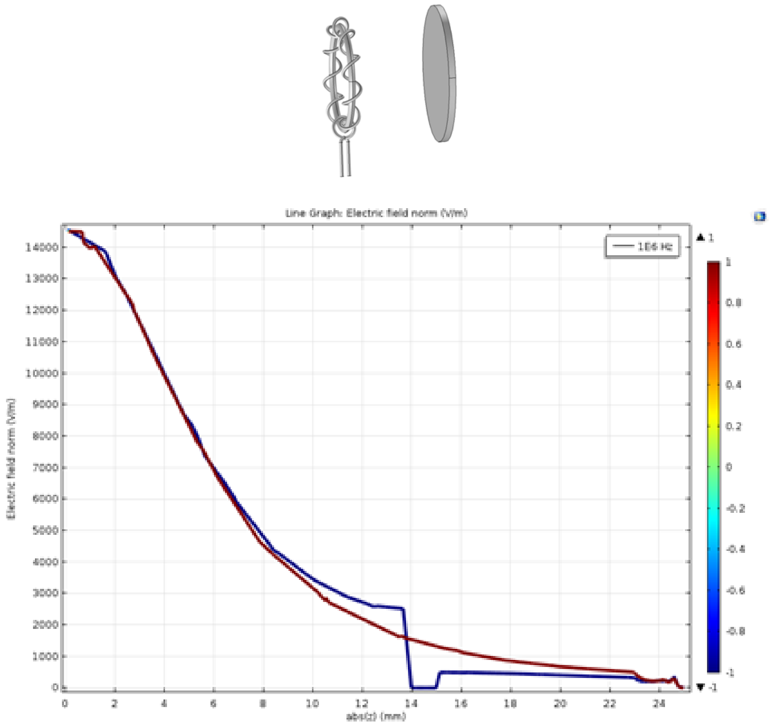


Figure 7.8: This figure shows the COMSOL model 'RF' package equivalent of the static electric field model in figure 7.3 using a toroid in place of a capacitor.

as might be used in the defence industry. In addition, if this effect is palpable it may be exploited for novel communication methods. Previous work in this area, outlined in the previous section, indicates that this type of exploitation may already exist, leaving current security mechanisms vulnerable. To thoroughly investigate this matter there will be two goals, to isolate longitudinal signals and compare their features and performance with conventional signals, and to investigate the possibilities of communicating from within a freestanding shielded box. These have been catalogued in the following methods:

Field Detection In isolating longitudinal signals the purpose was to identify and characterise the existence of non-conventional signal leakage through a shielded box, and aggravating or alleviating factors. In particular, it is enlightening to compare this to conventional leakages for a thorough understanding of the future scope and application of this signal leakage effect.

Attack Simulation In investigating the possibilities of communications through a shielded box the intent was to set up a stand-alone transmitter and receiver with a communications wrapper such that messages could be sent and received from within a shielded box.

7.6 Methods

7.6.1 Suitable Domains

Given the motivation of this experiment it is prudent to look at signals in the microwave and RF regime, specifically around 10-2500 MHz, as these are typical of signals from wi-fi and from the choke coils in common electronics.

Since the purpose of the experiment is to isolate and compare longitudinal signals with conventional signals, a variety of aerial types with different properties were investigated, and free space transmissions were compared to shielded transmissions.

7.6.2 Equipment

Antennas

The aerial types used (as seen in figure 7.12) were as follows:

A conventional whip antenna aligned vertically: The radiation pattern of such an antenna emits conventionally in a direction radial around the whip, but longitudinally in the direction of the whip; vertical alignements will couple transversely. This antenna optimally operates at 900 MHz. The radiation pattern for this can be see in figure 7.5.

A conventional whip antenna aligned horizontally: The change in alignment allows for investigation of the properties of the longitudinal components, as outlined in the 'background' section.

A toroidal choke: This emits longitudinal components only in a direction normal to the plane of the toroid. This antenna optimally operates around 90 MHz. An example radiation pattern can be observed in figure 7.7.

Shielding

The shielding used was 'Eccosorb AN-79' – 11.4 cm thick carbon treated polyurethane foam, backed on a metal coating for best performance, as recommended in (Technologies, 2015). The sheets are 61 cm^2. For frequencies greater than 600 MHz, Eccosorb AN-79 will attenuate a signal by a minimum of 17 dB with a ceiling frequency of at least 18 GHz. The performance with respect to frequency can be seen in (Technologies, 2015) which also shows that Eccosorb AN-79 attenuates far below 600 MHz to at least 100 MHz. Several sheets of this were arranged to form a cuboid box, housing the emitter, with no gaps (which would have allowed for leakage at the edges). The metal coating forms a shielded box with the carbon treated foam providing additional attenuation.

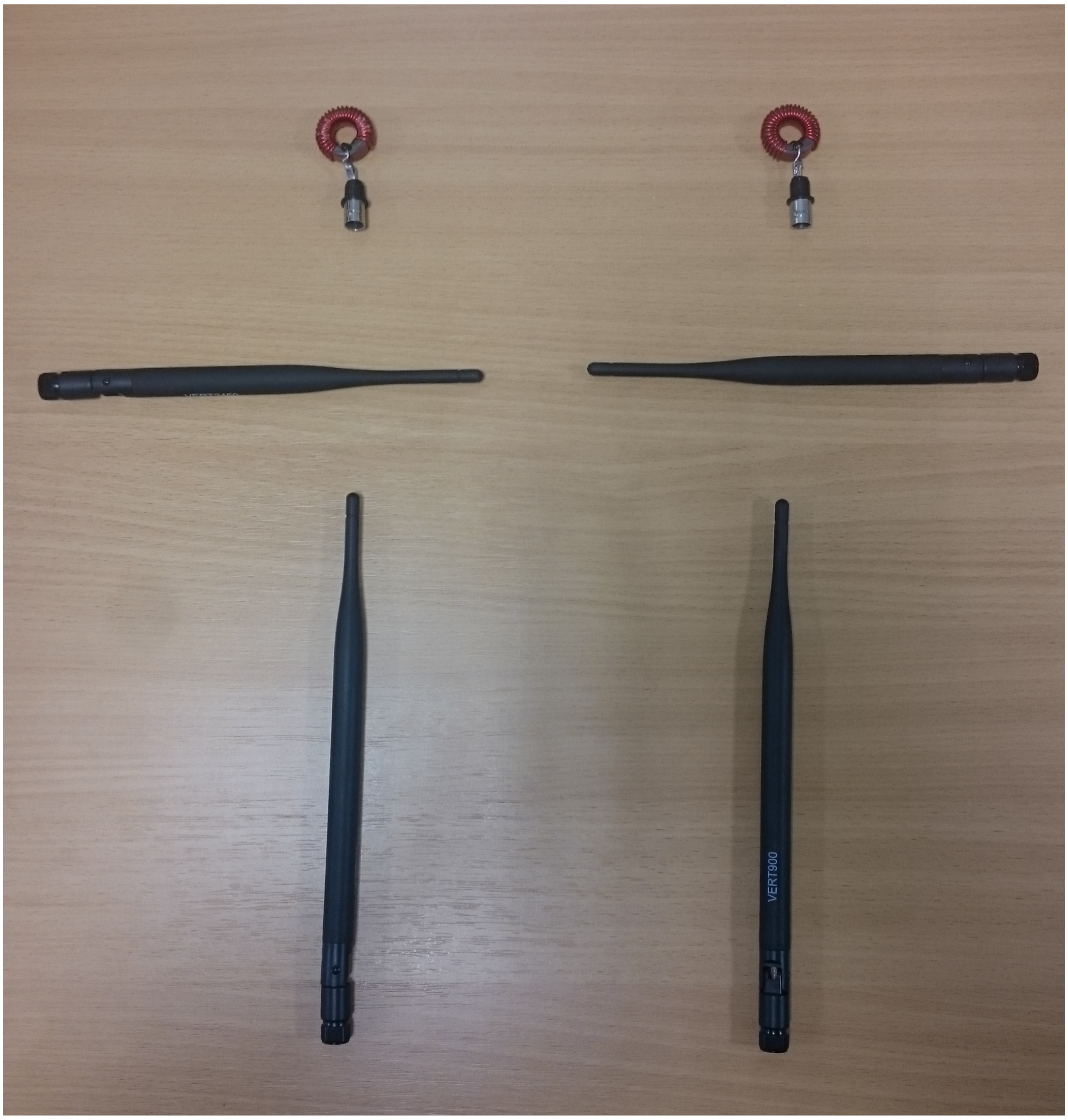


Figure 7.9: These are the three main antenna configurations used. From top to bottom: The toroidal choke coils; the whip antennas in 'horizontal' point-to-point transmission (longitudinal); the whip antennas in 'vertical' parallel transmission, this is optimal and is used for conventional signal transmission.

7.6.3 Setup

Field Detection To investigate if fields could be detected a signal was generated with a TTi TGR 2050 synthesised RF generator, and detected with a Rohde and Schwarz FS315 spectrum analyzer, as shown in figure 7.10. All three aerial types were used as transmitters and receivers. This gave a matrix of 9 scenarios which could then be compared. The transmission strengths were recorded with no shielding, and then with 1 sheet of Eccosorb. A distance of 12 cm was maintained throughout and the signals were transmitted with a consistent power of +7 dBm. The transmission frequencies used were 900 MHz for whip antennas and 100 MHz for toroidal aerials in accordance with their optimal operation. Further additions of Eccosorb had little reliably determinable impact upon the results of the experiment and (Technologies, 2015) recommends against it[1].

Attack Simulation To simulate an attack a signal was generated and received with two NI USRP-2901 software defined radios; the set up can be seen in figures 7.9, 7.13 and 7.14. A simple communications wrapper was added which allowed text to be sent and received using typical protocols (quadrature phase shift keying - QPSK) [2]and with some standard error correction. An example can be seen in table 7.1. This was a stand-alone battery operated solution such that the inside of the shielded box was fully sealed and transmitting to the outside. This is shown in figure 7.13. 900 MHz aerials were used, driven at 100 MHz, so that the signal was weak enough that conventional radiation would be attenuated by the Eccosorb, to a degree sufficient to minimise the effect on the detector, leaving just longitudinal signals. The transmitting antenna was connected to the USRP and the USRP programmed, via a battery operated laptop, to transmit many lines of text from completely within the shielded box. The receiving antenna was connected to a USRP and programmed to receive the text. This antenna was then aligned at various points and positions around the shielded box and the receipt, or not, of a transmission recorded, as seen in table 7.1. Use of the toroidal choke antennas in both receiving and transmission parts, driven at 100 MHz, then confirmed observations.

[1] This is consistent with the shielding mechanism outlined in 7.3.1

[2] as seen in the circuit diagram in figure 7.11

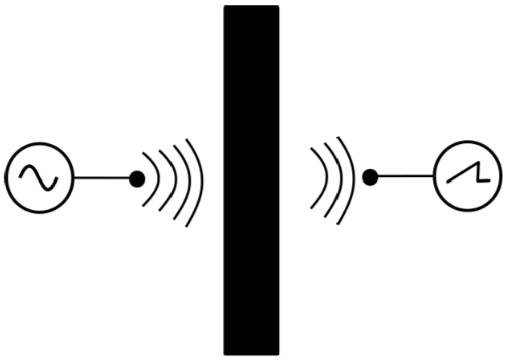


Figure 7.10: This shows more clearly the setup with electric field being detected either side of a shield

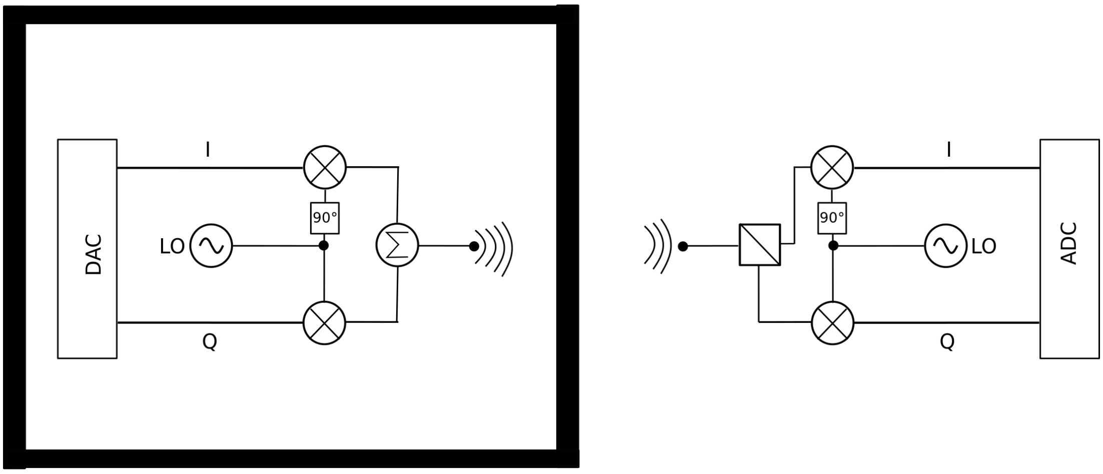


Figure 7.11: The circuit diagram for an attack simulation, including phase modulation for QPSK.

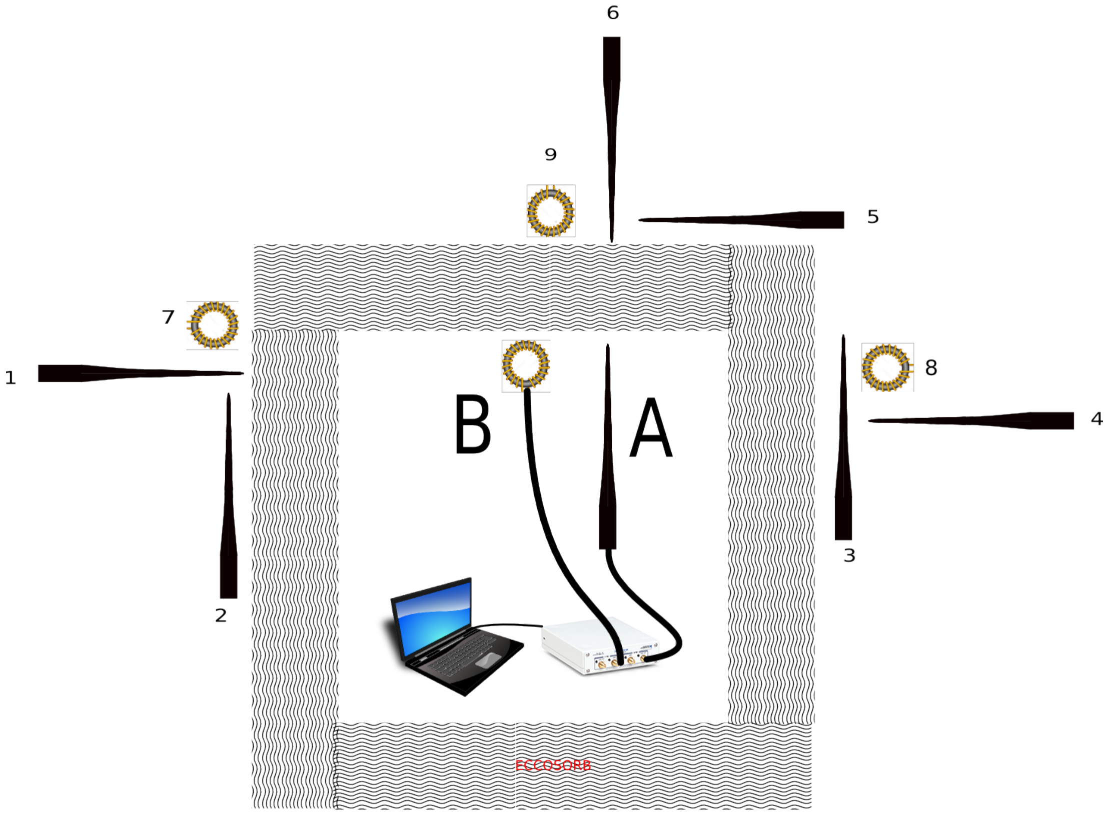


Figure 7.12: This shows the alignment and positions of the various aerials for attack simulation. The signal can be transmitted using either aerial A (900 MHz whip) or B (toroidal choke) and the signal can be received in any one of the 9 configurations.

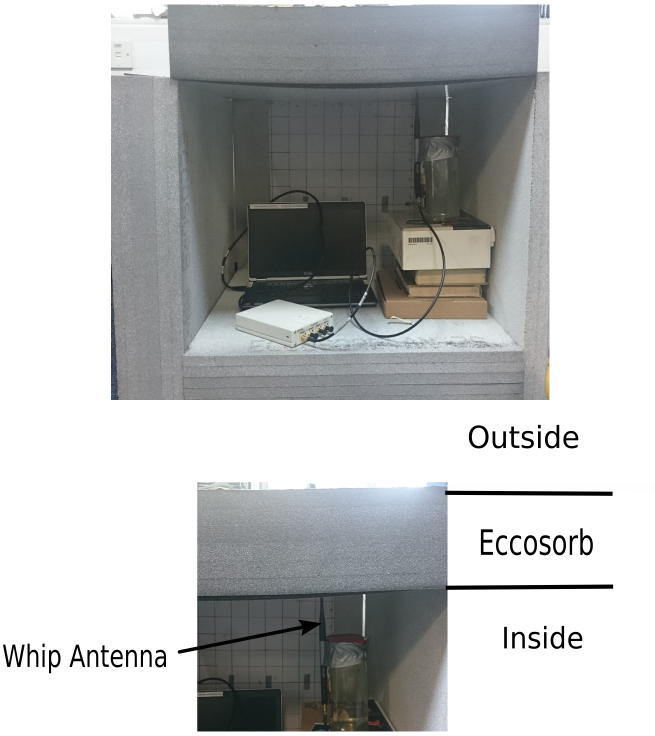


Figure 7.13: The setup for attack simulation- a shielded box with a transmitting antenna inside. A sheet of Eccosorb covers the front but has been removed for ease of observation. The bottom image shows this in more detail.

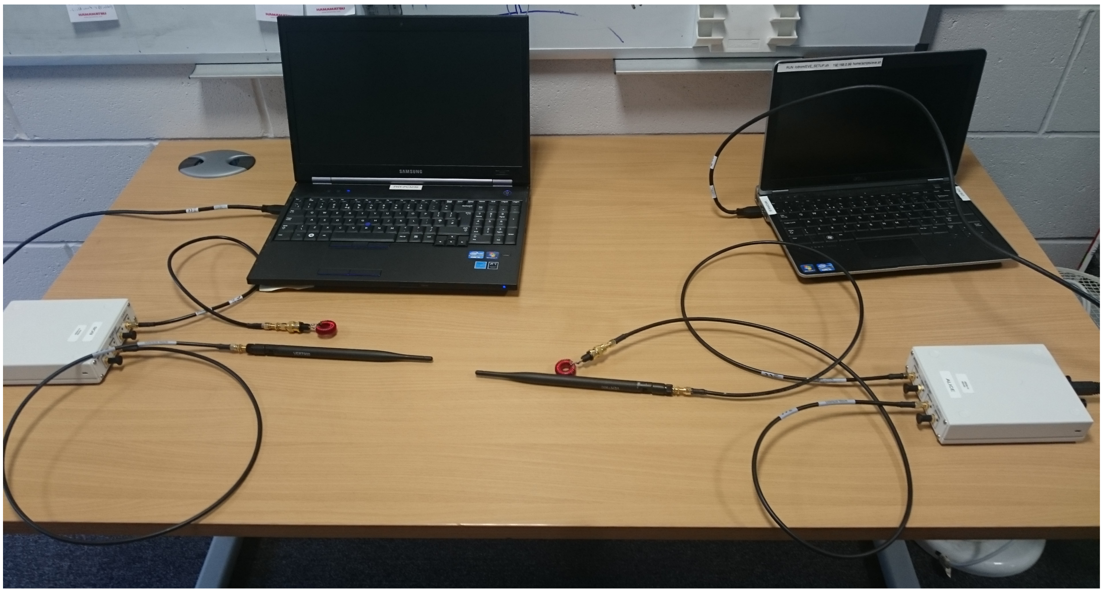
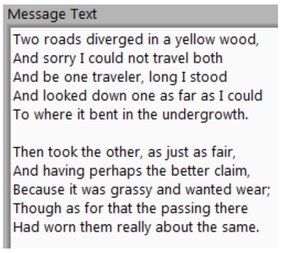
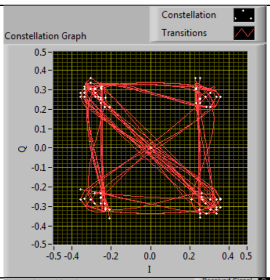
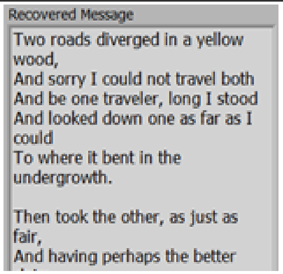
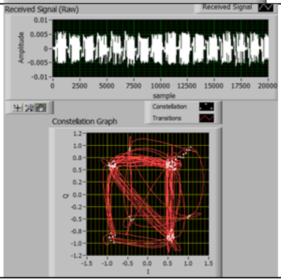
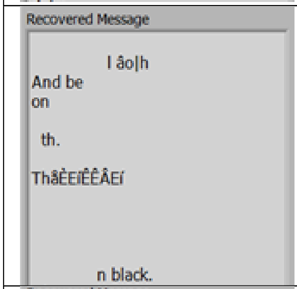
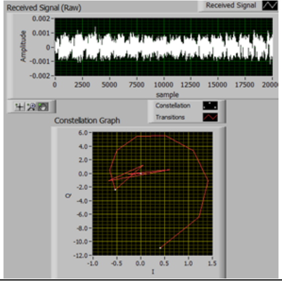
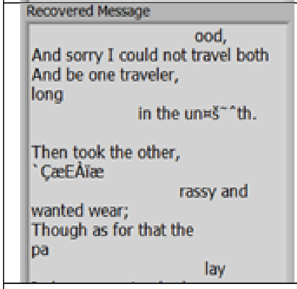
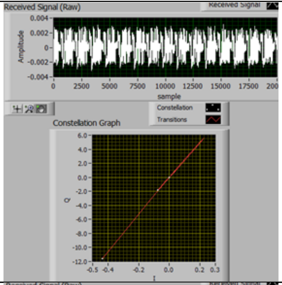
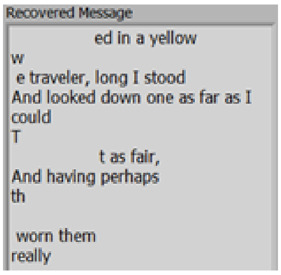
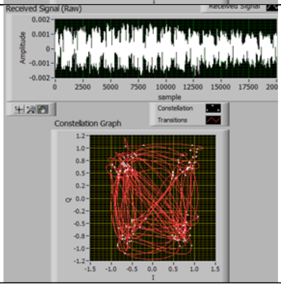
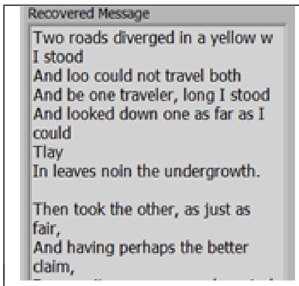
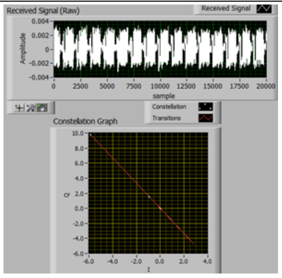


Figure 7.14: This shows, without the addition of the shielding, the basic set-up of the laptop-to-laptop equipment for attack simulation. Each half consists of the laptop with software, connected to the USRP (in white) which is connected to one of the two aerials.

Table 7.1: Examples of transmission quality in text communication.

Example Text	Example Graph	Description
 Message Text Two roads diverged in a yellow wood, And sorry I could not travel both And be one traveler, long I stood And looked down one as far as I could To where it bent in the undergrowth. Then took the other, as just as fair, And having perhaps the better claim, Because it was grassy and wanted wear; Though as for that the passing there Had worn them really about the same.		Transmission
 Recovered Message Two roads diverged in a yellow wood, And sorry I could not travel both And be one traveler, long I stood And looked down one as far as I could To where it bent in the undergrowth. Then took the other, as just as fair, And having perhaps the better		Perfect, complete reception.
 Recovered Message I âo|h And be on th. ThåÈEíÊÊÂEí n black.		Very poor. Almost no reception: very little text has been received, the QPSK diagram includes spiral artifacts, and parsing of the bit modulation is extremely poor.
 Recovered Message ood, And sorry I could not travel both And be one traveler, long in the un¤ʓˉˆth. Then took the other, ˋÇæEÅÏæ rassy and wanted wear; Though as for that the pa lay		Medium to poor transmission - some text received, low quality QPSK diagram and low quality bit modulation.
 Recovered Message ed in a yellow w e traveler, long I stood And looked down one as far as I could T t as fair, And having perhaps th worn them really		Medium to good transmission – high quality QPSK diagram, clear bit modulation, a few additional seconds of receipt would usually resolve this to a complete text.

 Recovered Message Two roads diverged in a yellow w I stood And loo could not travel both And be one traveler, long I stood And looked down one as far as I could Tlay In leaves noln the undergrowth. Then took the other, as just as fair, And having perhaps the better claim,	 Received Signal (Raw) Received Signal 0.004 0.002 0 -0.002 -0.004 Amplitude 0 2500 5000 7500 10000 12500 15000 17500 20000 sample Constellation Transitions Constellation Graph 10.0 8.0 6.0 4.0 2.0 0.0 -2.0 -4.0 -6.0 Q -6.0 -4.0 -2.0 0.0 2.0 4.0 I	Very high quality, almost full transmission. Lacking in QPSK diagram but this is due to software discrepancies displaying only the last parsed bit after transmission.

7.7 Results

7.7.1 Field Detection

Recall that the purpose of field detection was to compare longitudinal and conventional signals and the effects of shielding on the strength of transmission. The results of the transmissions between the three antennas configurations are tabulated in table 7.2. It is clear to see that shielding made little difference in coil to coil transmissions and horizontal to horizontal whip transmissions but a 20 dB loss occurred for whip antennas in conventional arrangements. Horizontal to vertical transmissions are almost undetectable. However coil to vertical transmissions do occur and are attenuated at a similar amount to that of vertical to vertical, suggesting some transverse signals leak from the toroid.

7.7.2 Attack Simulation

Recall that for attack simulation the purpose was to identify whether complete text could be communicated to outside a shielded box, from within it. The Rx whip antenna was placed at various points with respect to the internal Tx whip antenna and the result of a transmission recorded as either present or unobtainable. This was repeated for coil antennas in the parallel position. The results are recorded in table 7.3. Transmission was possible only when the whip antennas were aligned end-to-end - a position akin to the 'horizontal' alignment in 'field detection', and with the coils.

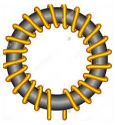
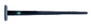
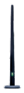
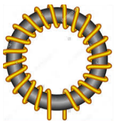
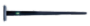
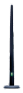
Transmit Tx Receive Rx			
	Free standing: -40 dBm Shielded: -50 dBm	Free standing: -59 dBm Shielded: -57 dBm	Free standing: -40 dBm Shielded: -70 dBm
	Free standing: -48 dBm Shielded: -45 dBm	Free standing: -40 dBm Shielded: -37 dBm	Free standing: -40 dBm Shielded: -55 dBm
	Free standing: -50 dBm Shielded: -75Bm	Free standing: -40 dBm Shielded: -55 dBm	Free standing: -20 dBm Shielded: -40 dBm

Table 7.2: The three antennas types were used as both transmitter and receiver (Tx and Rx) in field detection. Here the corresponding strengths with and without shielding are shown. Note that the results are almost symmetrical for Tx and Rx.

Position	Tx/Rx	Transmission?	Implication
Side (A4,A1)	TV/ Long	None	Blocked signal
Side (A3,A2)	TV/ TV	None to poor	Signal attenuated
Top (A5)	Long/ TV	None	Blocked signal
Top (A6)	Long/ Long	Complete	Signal free
Side (B7,B8)	Long/ Long	Medium to good	Attenuation is in space only
Top (B9)	Long/ Long	Complete	Signal free

Table 7.3: This table shows the transmission record for various positions of receiving antenna, as outlined for attack simulation. The code in brackets (under 'position') refers to the position matrix outlined in figure 7.12. Examples of quality of transmission can be seen in table 7.1 TV here indicates transverse signals and long indicates longitudinal signals.

.

7.7.3 Limitations

Preliminary experiments highlighted that the signals were extremely sensitive to subtle changes in the environment which limits the usefulness of possible extensions to this experiment such as finding the emission patterns by performing raster-type measurements. In addition it limits the usefulness of direct comparisons between two different aerial set types, although the signals were consistent within the time period required to add or remove the Eccosorb. All the recordings made with the spectrum analyser were fluctuating by around 2 dB and as such results showing a change of less than this should not be considered significant. The noise floor of the spectrum analyser was around -80 to -90 dBm. The signals were highly distance dependent. It is also possible that if the toroidal antennas are not completely symmetrical there may be some very small residual amount of transverse radiation, with the Poynting vector not quite aligned to the center.

7.7.4 Leakage

It could be argued that since the Faraday shielding is not completely sealed there is a possibility that transverse electromagnetic waves could be leaking around the edges, including any possible residual transverse leakage from the toroidal antennas. However, looking at the results from the field detection part of the experiment in table 7.2 it can be seen that transverse radiation is typically attenuated by approximately 20dB. Since the attenuation of any of the longitudinal set-ups do not include a 20dB drop it can be assumed that this is a distinct form of radiation that is being detected.

7.8 Threat Analysis

7.8.1 Use in a Real Shielded Room

A further extension to this involved access to a real shielded room at the National Authority for Counter Eavesdropping. The shielded room consisted of two layers of metal Faraday shielding with some concrete gap in the middle, excepting the door which was a thick layer of metal. Preliminary results here indicated that longitudinal radiation leaked through the door but not through the sides, with the exception of some small residual amount that could be seen as tunnelling. This indicates that the doors of shielded rooms are a possible threat, but also that the concrete plays some sort of role in attenuating the signal. Since the use of concrete in this particular room was completely coincidental, and not included as standard in shielded rooms it is important that this is noted. Further investigation is needed to characterise this as a blocking method. Alternatively, the size of the room proportional to the wavelengths used could be influencing the conductivity, or the size of the room proportional to the energy in the signal - where the energy is dissipated through the entire surface area of the metal resulting in only a very weak almost undetectable signal emitting.

7.9 Conclusions

7.9.1 Field Detection

It is clear that for antennas transmitting and receiving conventional radiation (that is- the whip antennas in vertical positions) the Eccosorb attenuates the signal by around 20dB. This is in accordance with the published values in (Technologies, 2015) and what would be expected according to convention. For aerials transmitting unconventional longitudinal radiation there was very little change in signal strength. This is seen in the horizontal to horizontal, the coil to horizontal, and the coil to coil arrangements. Mysteriously, the converse is true- there is some small increase in the signal strength, this may be related to the limitations in signal fluctuations however it is somewhat consistently an increase. This gives some credence to the idea that the transmissions may in fact use intervening material as a waveguide and may be indicative of a tunneling effect. Overall, despite their relative lack of strength, it is clear that unconventional, longitudinal signals are insensitive to standard shielding attempts.

7.9.2 Attack Simulation

In the arrangements which were optimal for the transmission there were no recorded transmissions; that is to say where the aerials were parallel (akin to the 'vertical' arrangements of part 1). In the arrangements allowing for longitudinal transmissions only (coil to coil and end to end - akin to 'horizontal' arrangements in mode 1) there were clear transmissions. This demonstrates that communication through shielded walls is possible.

7.9.3 Summary

It is clear that there is a significant cause for concern regarding the potential for eavesdropping through shielded rooms. Further work is required to establish the extent of this threat and the designs of boxes which increase or decrease the amount of signal leakage.

7.9.4 Future Work

In order to truly identify the strength of this threat further work must be done on testing in ‘real-life’ shielded rooms. This includes the comparison or a concrete filled wall versus a pure metal cage. Additionally, some observations on concrete specifically would help to identify how this may be utilised as a blocking material. Furthermore, expanding the equipment to investigate other wavelengths compared to the size of the room may be useful to see if this has some effect. Ideally, investigating different sizes of room with different intensities of signal will help to discover if the signal is in some way being dissipated around the surface area of the shielding, resulting in a negligible signal transmitted.

8

Conclusions and Future Work

The aim of this thesis was to examine the possibilities for security in implementing post-quantum key distribution in pre-existing telecommunications systems. In particular, it was concerned with the implementation of a particular algorithm, the security constraints set by other authors, and the adherence of signals in the microwave regime to the necessary characteristics. An alternative source of noise, stochastic noise from random numbers, was also considered which would allow application in a wider range of circumstances. Furthermore, this work was concerned with a possible side channel attack which could hinder its use in practical implementation.

The post-quantum protocol for implentation in phase shift keyed communications systems is considered in Chapter 3. The security is analysed, following that given by Maurer, with some mistakes corrected. It states that provided an eavesdropper has some unavoidable noise on measurement of the message then it will be secure. The subject of the noise is then considered in the following Chapters.

Chapter 4 examines how the presence of thermal noise affects the signal measured. Theoretical analysis of multi-mode signals such as those found in a typical wireless communications system indicates that the energy density peaks in the infrared region. The number of thermal photons which one detects is considered and shows that single photon protocols would not be suitable beyond a limit (which varies according to temperature). However, this would not affect protocols which require only a shot noise limited signal, as this cacn be mitigated by sending a stronger signal.

Chapter 5 goes some way towards justifiying the claims in Chapter 4 that telecommunications protocols in the microwave region are secure for implementing the CVQKD protocols that are outlined in (Usenko & Grosshans, 2015; Weedbrook *et al.*, 2010). It can be seen that mixed binary coherent states can be resolved in phase space with shot noise characteristics. This quantum limited noise measurement means that the excess noise from thermal background does not dominate and remains below the levels indicated in Chapter 4.

The prospects for implementing a post-quantum cryptographic solution which relies purely on the properties of mathematics rather than the physical manifestations of quantum physics are examined in Chapter 6. A thought experiment reveals properties of random numbers on the large scale which give some small amount of correlation or anti-correlation. This correlation or anti-correlation is also attributed to the trusted and untrusted parties, however, in different places. This results in a positive $I(A : B|E)$ over a large enough number of runs. The outcomes can be fed into an algorithm such as advantage distillation, giving a secure key, but with a large amount of losses. Chapter 3 deals with the security of advantage distillation and Chapter 6 demonstrates that random numbers could be a resource for this algorithm. This is impenetrable to quantum attacks as the key distribution is completely independent of the channel and the security comes from the randomness of numbers. The quality of it is such that it could be a proposal for a universal cryptographic standard. It is implementable on an algorithmic basis only and not dependent upon line of sight communications, fibers, shot noise limited signals, or other transmission medium properties. The main caveat is that if an eavesdropper was able to clone something on the 'private' and non-disclosed side of the trusted parties then said eavesdropper would be able to extract the key. However, this can be prevented if the trusted parties are held within a secure box, for example a shielded room.

In order to implement a quantum secure key distribution scheme in a realistic microwave communications structure one must consider the realism of the assumptions made for the security of CVQKD, and whether these could reveal a side channel attack in an authentic application. Chapter 7 discusses a potential side channel attack arising from the assumption that a secure housing can be created for the parties to prepare their states before transmission. This assumption is typically justified on the basis that a Faraday shielded structure will prevent leakage of EM fields. However, Chapter 7 outlines a method of field leakage through Faraday shielding based on a longitudinal field component, elucidated through use of the magnetic vector potential mechanism. Tests reveal leakage in longitudinally directed fields in mock-up shielded boxes; longitudinal fields are not attenuated by the presence of the shielding and typical transverse fields are. Further testing in an authentic shielded room at the National Authority for Counter Eavesdropping indicates this leakage exists in these rooms also with the indication that there is a possibility that the fields are dampened by materials such as concrete owing to the leakage through the door and much weaker leakage throught the sides (which could be attributable to tunnelling). This leakage has wider implications than the security of CVQKD and could cause problems for the defence industry regarding TEMPEST security and for those who may use shielded rooms for experimental purposes.

8.1 Future Work

The security boundaries identified in Chapter 4 have been determined theoretically making use of the foundations provided in Loudon (Loudon, 2000). It would be useful to perform an experimental analysis on all wavelengths in the optical to microwave range to identify whether shot noise limited signals could be extracted from the entire range of frequencies, and how this is influenced by temperature, and the temperature of the measuring equipment. In particular, looking at a typical temperature profile of signals sent through a satellite system. This could be by performing some signal analysis or by using cooling detection techniques. It would also be useful to compare a quantum state reconstruction of states sent at these different wavelengths with those in Chapter 5 to see how the mixed thermal and coherent state would perform.

The characterisation of microwaves in PSK systems with quantum state reconstruction can be seen in Chapter 5, however it would be useful to extend this to observing how distance dependence is affected based upon the strength of the detection sytem. Susbsequently it would be useful to see how the key rate is affected by this.

Since the examination of a key distillation protocol from Chapter 3, and the proposal in Chapter 6 of using random numbers as a resource rather than a quantum property to create post-quantum security, the question remains on how 'random' the random numbers must be. The American National Institute of Standards and Technology (Kelsey & Barker, 2017) outlines some requirements for the randomness of a random bit generator. It is unclear at this stage to what extent the numbers must exhibit 'true randomness'. It is also possible that other side channel attacks exist which have not yet been considered.

The work outlined in Chapter 7 reveals some open questions regarding the security and countermeasures for the use of shielded rooms. In particular further work is needed to determine which properties of an authentic shielded room make the longitudinal signals harder to detect. It would be useful to test longitudinal signals travelling through a variety of materials with different dielectric constants, including concrete, with a view to settling upon the optimum combination. Furthermore, it would be interesting to see if the size of the room, or the ratio of the size of the room to the wavelength or the energy density of propagating signals has an effect on the leakage of longitudinal signals. It would be useful to accurately characterise the weak leakage detected through the concrete sided walls to determine if this was a barrier tunnelling mechanism or longitudinal penetration mechanism. This could possibly be implemented using a range of thicknesses and determining if the signal was exponentially depleted.

Appendix A

Key Distillation Code

The following is the code used to simulate a noisy exchange with key extraction, using advantage distillation.

```
/*Symmetric key agreement with varied inputs to examine the influence on the key output*/

#include <stdio.h>
#include <time.h>
#include <stdlib.h>
#include <math.h>

#define Mask 1                  /*Used as an identifier later*/

typedef unsigned char uint8;  /*A variable type 8 bits only in length (+ numbers only) */

typedef signed char int8;     /*A variable type 9 bits in length where 1 bit signifies + or -*/

/*This function checks that the key output matches and is symmetric*/

int MatchCheck(uint8 i, uint8 Array1[i], uint8 Array2[i]){
      int j=0;
      while(Array1[j]==Array2[j]){
          j++;
          if(j==(i-1)){
              return 1;
          }
      }
      return 0;
  }



void main() {

  srand(time(NULL));

  uint8 C_A[512]={0}, Transmit_1[512]={0}, Transmit_2[512]={0}, C_B_1[512]={0}, C_B_2[512]={0}, Matchlist
[512]={0}, sendMatches[512]={0}, BobNoise[512]={0}, AliceNoise[512]={0};
  int j=0, bytecount=0, bitcount=0, i=0, DONE=0;
  int DistilledSize = 255;

  /* Alice and Bob start off with some biased random noise*/


  for(i=0;i<512;i++){

    AliceNoise[i]=rand()&rand();
    BobNoise[i]=rand()&rand();

  }

  while(DONE!=1){

    /*ALICE*/

    /*Alice gets random numbers*/

    for(i=0;i<DistilledSize;i++){

      C_A[i]=rand();

    }

    /*Alice XOR's these twice with independent noise*/

    for(i=0;i<DistilledSize;++i){

      Transmit_1[i]=AliceNoise[2*i]^C_A[i];
      Transmit_2[i]=AliceNoise[(2*i)+1]^C_A[i];

    }
  /*Transmit_1 and Transmit_2 are sent to Bob*/

  /*BOB*/

  /*Bob receives Transmit_1 and Transmit_2 from Alice and XOR's them with his own noise*/

  for(i=0;i<DistilledSize;i++){

    C_B_1[i]=BobNoise[2*i]^Transmit_1[i];
    C_B_2[i]=BobNoise[(2*i)+1]^Transmit_2[i];

  }

  /*Bob clears his noise so it can be repopulated later*/

  for(i=0;i<512;i++){
    BobNoise[i]=0;
  }

  /*Ensure the counters are set to zero before commencing*/

  bitcount=0;
  bytecount=0;

  for(i=0;i<DistilledSize;i++){   /*For every array element (byte)*/


   for(j=7;j>=0;j--){            /* and for every bit within that array element*/

    if( (C_B_1[i]>>(j) & Mask) == ( (C_B_2[i]>>(j)) & Mask) ){  /*compare the two arrays*/

     BobNoise[bytecount]=(BobNoise[bytecount]<<1)+((C_B_1[i]>>(j) & Mask));
                                                                   /*If they match then save this bit
into the noise array to be used as noise later*/
     bitcount++;
                                                                  /*Keeping track of how many bits have
been saved so that the next array element (byte) can be started when appropriate*/
     if(bitcount==8){                                   /*-Start a new byte after every 8 bits*/

      bitcount=0;
      bytecount++;

     }                                  /*Save this into a matchlist as a '1'*/

     Matchlist[i]=(Matchlist[i]<<1)+1;

    }
                          /*otherwise- save this bit into the matchlist as a '0'*/
    else {

     Matchlist[i]=Matchlist[i]<<1;

    }
   }
  }

  /*Keep track of the results on the output screen*/

  printf("\nBob's results(C_new_B): \n");

  for(i=0;i<DistilledSize;i++){

    sendMatches[i]=Matchlist[i];  /*and 'send' the matchlist over to Alice*/

    printf("%d\t",BobNoise[i]);
  }


  /*Alice clears her noise to it can be repopulated later*/

  for(i=0;i<512;i++){
   AliceNoise[i]=0;
  }

  /*Ensure the counters are set to zero before commencing*/

  bytecount=0;
  bitcount=0;

  for(i=0;i<DistilledSize;i++){ /*For every array element (byte)*/

    for(j=7;j>=0;j--){          /* and for every bit within that array element*/

      if( (sendMatches[i]>>j) & Mask) { /*search the matchlist for '1' values (ignoring '0' values*/
                                         /*save into the noise array the random bit that corresponds to
that placeholder on the matchlist*/
        AliceNoise[bytecount] = (AliceNoise[bytecount]<<1)+((C_A[i]>>j) & Mask);
        bitcount++;
                            /*keeping tabs on the number of bits so that the next byte can be filled when
necessary*/
        if(bitcount==8){

          bitcount=0;
          bytecount++;


        }
      }
    }
  }

  /*Keep track of the results on the output screen*/

  printf("\nAlice's C_new_A:\n");

  for(i=0;i<DistilledSize;i++){

    printf("%d\t",AliceNoise[i]);

  }

  /*We have halved the amount of noise by comparing two bits at a time. Hence on the next repeat we need
only look at half the size*/

  DistilledSize=(bytecount/2);

  /*Since this is a simulation, we will repeat it until a matching key is produced*/

  DONE=MatchCheck(DistilledSize,AliceNoise,BobNoise);

  /*In the case where there is no key produced, we will add a break from the program*/

  if(bytecount==0){

    break;

  }

 }
 printf("\n");
}
```

References

Agrawal, D., Archambeault, B., Rao, J.R. & Rohatgi, P. (2003). The EM Side-Channel(s). In *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, 29–45, Springer-Verlag, London, UK, UK. 106

Aharonov, Y. & Bohm, D. (1959). Significance of Electromagnetic Potentials in the Quantum Theory. *Phys. Rev.*, **115**, 485–491. 110

Assche, G., Cardinal, J. & Cerf, N. (2004). Reconcillation of a Quantum-Dsitributed Gaussian Key. *IEEE transactions on information theory*. 2, 31

Barbieri, S., Cavinato, M. & Giliberti, M. (2013). An educational path for the magnetic vector potential and its physical implications. *European Journal of Physics*, **34**. 108

Bennett, C., Brassard, G. & Robert, J.M. (1988). Privacy Amplification by Public Discussion. *SIAM Journal on Computing*, **17**, 210–229. 53

Bennett, C., Brassard, G., Crepeau, C. & Maurer, U. (1995). Generalized Privacy Amplification. *IEEE Transactions in Information Theory*. 3, 52

Boyer, T. (2000). Does the Aharonov–Bohm Effect Exist? *Foundations of Physics*, **30**, 893–905. 115

Brassard, G. & Salvail, L. (1994). Secret-Key Reconcilation by Public Discussion. *Advances in Cryptogology*. 48, 49

Cachin, C. & Maurer, U. (1995). Linking Information Reconciliation and Privacy Amplification. *Journal of Cryptography*. 52, 53

Cerf, N. & Grangier, P. (2007). From quantum cloning to quantum key distribution with continuous variables: a review. *Journal of the Optical Society of America*. 2

Chambers, R. (1960). Shift of an Electron Interference Pattern by Enclosed Magnetic Flux. *Phys. Rev. Lett.*, **5**. 113

Charles H. Bennett, G. (1995). Generalized Privacy Amplification. *IEEE Transactions on Information Theory*, **41**, 1915–1923. 44, 46

Christandl, M., Ekert, A., Horodecki, M., Horodecki, P., Oppenheim, J. & Renner, R. (2008). Unifying classical and quantum key distillation. *arXiv*. 2

Csiszar, I. & Korner, J. (1978). Broadcast Channels with Confidential Messages. *IEEE transactions on information theory*. 17

Ekert, A.K. (1991). Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, **67**, 661–663. 2

ETSI (2015). Quantum Safe Cryptography and Security. Tech. Rep. White Paper 8, ETSI. 2

Everitt, M. (2015). Work by another PhD student. xxiv, 120, 121, 124

Filip, R. (2008). Coninuous-variable quantum key distribution with noisy coherent states. *Physical Review A*, **77**. 2

Gelinas, R. (1984). Apparatus and method for transfer of information by means of a curl-free magnetic vector potential field. Google Patents. 105, 106, 108

Glauber, R. (2007). *Quantum Theory of Optical Coherence*. Wiley. 63, 68

Goubau, G. (1954). Surface wave transmission line. Google Patents. 116

Goubau, G. (1960). Launching and receiving of surface waves. 116

Graosshans, F. & Cerf, N. (2004). Continuous-variable quantum cryptogoraphy is secure against non-gaussian attacks. *Physical Review Letters*, **92**. 2

Grosshans, F. (2005). Collective Attacks and Unconditional Security in Contunuous variable Quantum Key Distribution. *Physical Review Letters*, **94**. 2

Grosshans, F., Assche, G., Wenger, J., Brourl, R., Cerf, N. & Grangier, P. (2003). Quantum key distribution using Gaussian-modulated coherent states. *Nature Letters*, **421**, 238–241. 2

H. Bennett, C. & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing*, **560**, 175–179. 5

Heath, R. (2012). *Digital Communications*. Tom Robbins. 20

Helstrom, C. (1976). *Quantum Detection and Estimation Theory*. Academic Press. 31

Horodecki, K., Horodecki, M., Horodecki, P., Leung, D. & Oppenheim, J. (2008). Unconditional Privacy over Channels which Cannot Convey Quantum Information. *Physical Review Letters*, **100**. 2

Iencinella, D. & Matteucci, G. (2004). An introduction to the vector potential. *Eur. J. Phys.*, **25**, 249–256. 115

Jaklevic, R.C., Lambe, J.J., Silver, A.H. & Mercereau, J.E. (1964). Quantum Interference from a static vector potential in a Field Free Region. *Physical Review Letters*, **12**. 115

Kawakami, M. & Yamashita, O. (1999). A magnetic vector potential based communications system. Google Patents. 105, 106, 108

Kelsey, J. & Barker, E. (2017). Recommendation for Random Bit Generator (RBG) Constructions. 146

KONOPINSKI, E. (1978). What the electromagnetic vector potential describes. *American Journal of Physics*, **46**, 499–502. 105, 106, 108

LANCE, A., SYMUL, T., SHARMA, V., WEEDBROOK, C., RALPH, T. & LAM, P. (2008). No-switching Quantum key distribution using Broadband modulated coherent light. *PrePrint*. 2

LEONHARDT, U. (1996). Discrete Wigner function and quantum-state tomography. *Phys. Rev. A*, **53**, 2998–3013. 68

LEUNG, D., LI, K., SMITH, G. & SMOLIN, J. (2014). Maximal Privacy without Coherence. *Preprint*. 2

LIDONG CHEN, S.Y.D.R.R.D. (2016). Report on Post-Quantum Cryptography. Tech. rep., NIST. 2

LIU, H. & LALANNE, P. (2008). Microscopic theory of the extraordinary optical transmission. *Nature*, **452**, 728–731. 117

LOUDON, R. (2000). *The Quantum Theory of Light*. Oxford. xxi, 56, 58, 145

MARQUARDT, P., VERMA, A., CARTER, H. & TRAYNOR, P. (2011). (Sp)iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11. 105

MARTÍN-LÓPEZ, ENRIQUE, L.L.A.Z.O. (2012). Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, **6**. 88

MAURER, U. (1993). Secret Key Agreement by Public Discussion from Common Information. *IEEE transactions on information theory*, **39**. xi, 3, 11, 16, 17, 18, 46

MAURER, U. & WOLF, S. (1999). Unconditionally Secure Key Agreement and the Intrinsic Conditional Information. *IEEE transactions on information theory*, **45**. xx, 3, 37, 46

Munroe, H. (2015). Private Communications. 117

Nakassis, A., Bienfang, J. & Williams, C. (Pre-print). Expeditious Reconcialiation for Practical Quantum Key Distribution. *Pre-print*. 49

NCSC (2016a). Quantum key distribution. Tech. rep., NCSC. 2

NCSC (2016b). Quantum-safe cryptography. Tech. rep., NCSC. 2, 88

Nielsen, M. & Chuang, I. (2004). *Quantum Computation and Quantum Information*. Cambridge. 2, 10, 13, 52

Nyquist, H. (1928). Certain Topics in Telegraph Transmission Theory. *Transactions of the A.I.E.E.*, **47**. 9

Ozols, M., Smith, G. & Smolin, J. (2014). Bound entangled states with secret key and their classical counterpart. *Preprint*. 2

Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. (2008). Continuous-variable quantum cryptography using two-way quantum communication. *nature physics*, **4**, 726–730. 2

Puthoff, H. (1998). Communication method and apparatus with signals comprising scalar and vector potentials without electromagnetic fields. Google Patents. 105, 106, 108

Rousseaux, G., Kofman, R. & Minazzoli, O. (2008). The Maxwell-Lodge effect: Significance of electromagnetic potentials in the classical theory. *The European Physical Journal D*, **49**, 249–256. 115

Rundle, R.P., Mills, P.W., Tilma, T., Samson, J.H. & Everitt, M.J. (2017). Simple procedure for phase-space measurement and entanglement validation. *Phys. Rev. A*, **96**, 022117. 68

Sakurai, J. & Napolitano, J. (2011). *Modern Quantum Mechanics*. Addison-Wesley, 2nd edn. 110, 112

Shannon, C. (1948). A Mathematical Theory of Cummincation. *The Bell System Technical Journal*. 1, 9, 10, 13

Shannon, C. (1949). Communication in the Presence of Noise. *Proceedings of the IRE*. 1, 9

Singh, S. (1999). *The Code Book*. DoubleDay. 1

Stallings, W. (2014). *Cryptography and Network Security, Principles and Practice*. Pearson. 52

Symul, T., Alton, D., Assad, S., Lance, A., Weedbrook, C., Ralph, T. & Lam, P. (2007). Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Physical Review A*, **76**. 2

Technologies, L. (2015). Eccosorb products website: Eccosorb AN tech bulletin. `http://www.eccosorb.com/Collateral/Documents/English-US/RFP-DS-AN%20081215.pdf`, accessed 2017 Mar 30. 128, 130, 140

Tonomura, A.e.a. (1982). Observation of Aharonov-Bohm Effect by Electron Holography. *Phys. Rev. Lett.*, **48**. 113

Townsend, J. (2000). *A Modern Approach to Quantum Mechanics*. University Science Books. 108, 110, 112

Usenko, V. & Filip, R. (2010). Feasibility of continuous-vairable quantum key distribution with noisy coherent states. *Physical Review A*, **77**. 2

Usenko, V. & Grosshans, F. (2015). Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A*, **92**. 2, 6, 29, 55, 62, 85, 144

Weedbrook, C., Lance, A., Bowen, W., Symul, T., Ralph, T. & Lam, P. (2006). Coherent-state quantum key distribution without random basis switching. *Physical Review A*, **73**. 2

Weedbrook, C., Alton, D., Symul, T., Lam, P. & Ralph, T. (2009). Distinguishability of Gaussian sates in quantum cryptography using postselection. *Physical Review A*, **79**. 2

Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. (2010). Quantum Cryptography Approaching the Classical Limit. *Phys. Rev. Lett.*, **105**. 29, 55, 73, 144

Weedbrook, C., Pirandola, S. & Ralph, T. (2012). Continuous-variable quantum key distribution using thermal states. *Physical Review A*, **86**. 2, 5, 55, 73

Wigner, E. (1932). On the Quantum Correction For Thermodynamic Equilibrium. *Phys. Rev.*, **40**, 749–759. 68

Wyner, A. (1975). The wire-tap channel. *Bell System Technical Journal*, **54**. 5, 24

Zimmerman, R. (2011). Macroscopic Aharanov–Bohm Effect At L-Band Microwave Frequencies. *Modern Physics Letters B*, **25**, 649–662. 105, 106, 108, 117, 119

Zimmerman, R. (2013). Reception of longitudinal vector potential radiation with a plasma antenna. *Journal of Applied Physics*, **114**, 044907. 105, 106, 108, 117