University of Kent

Department of Computer Science

CO620 - Individual Research Project

Technical Report

Quantum Cryptography: Security for the Post-Quantum world

Author:

David W. Arnold

University Supervisor:

Dr. Carlos Perez-Delgado

This technical report is submitted for the degree of

BSc Computer Science with a Year in Industry

June 10, 2020

Abstract

The predictions of quantum computing potential puts the world's classical cryptography at risk of exploitation. Cryptographic protocols are used extensively on the World Wide Web. The Rivest–Shamir–Adleman (RSA) protocol is just one public-key cryptosystem at risk, as it derives its security from the computational hardness of factoring a large integer into two primes - a feat now possible in a fraction of the time over classical means using Shor's quantum factoring algorithm. Post-quantum cryptography provides a short-term/cost effective plan to counter quantum attacks, with the goal being to develop cryptographic schemes secure against both quantum and classical computers. Society needs to be pre-emptive, as all the while existing cryptographic protocols are at risk of quantum attacks.

Quantum cryptography is a long-term/more costly option, providing new cryptographic schemes which exploit the principles of quantum mechanics to enable provably secure distribution of private information. This paper will discuss the current quantum cryptographic techniques both available and in development, such as: quantum key distribution (QKD), quantum networks, delegated quantum computing techniques (BQC and QHE) and quantum random number generators (QRNGS), along with a new classical scheme heralded as a classical QKD-like protocol. This paper is aimed at computer scientists and people in industry who concern themselves with the post-quantum era of security and cryptography.

Acknowledgements

I'd like to thank Dr. Carlos Perez-Delgado, my university research project supervisor, for his support in suggesting good reading materials/articles, giving me direction for surveying the field of quantum cryptography and providing invaluable feedback.

I'd like to thank Dr. Carol Wicken-Arnold for her continued support in reviewing my research project materials, drawing my attention to relevant daily news articles and providing feedback from a perspective other than computer science.

Contents

List of Figures

Chapter 1

Introduction

Quantum computers are still in the early stages of development however research institutes and major corporations are investing heavily in their future. In October 2019 Google claimed to have made a breakthrough in the field by achieving "quantum supremacy" when, "its processing chip took 200 seconds to perform a calculation that would have taken a classical supercomputer 10,000 years to complete" (Boland and Zolfagharifard, 2019).

The reason for such wide-spread interest in quantum computers is the potential disruption which they pose to existing classical systems. In particular the implications on cyber security and cryptography used by websites, web browsers and other software applications in our day-to-day life. Quantum computers potentially threaten a global catastrophe of digital privacy infringement and subsequent insurrection were this technology to be used by malicious actors (Majot and Yampolskiy, 2015).

This paper is intended to introduce people in the field of computer science and business personal to the pitfalls of classical cryptography and the potential of future-proof cryptographic techniques in response to quantum computers. It is important to consider the options for the future with regards to our digital security: post-quantum cryptography and quantum cryptography. How the best path forward might be to look into quantum cryptography as a means of authentication and secure communications for our future. The paper will discuss the different types of quantum cryptography, delve into how they work, and help pin-point their potential applications.

The development of quantum computers cannot be stopped, nor should it be, but if we wait until prototypes become fully fault-tolerant and general purpose machines, it will be too late. Only through informing people can we bring about pre-emptive change in cyber security and cryptographic methods to keep communications safe in the future age of quantum computers.

Chapter 2 introduces various background materials relevant to understanding the potential importance of quantum cryptography. Chapter 4 is an introduction to quantum key distribution (QKD) and other general concepts within quantum cryptography. Chapter 5 covers the topic of quantum networks for widespread use of quantum cryptographic methods. Chapter 6 talks about delegated quantum computing, for people who wish to harness quantum computation without owning a quantum computer. Chapter 7 covers quantum random number generator and its usefulness, especially within QKD. Chapter 8 presents some newly theorised classical cryptography with the potential to match existing quantum cryptography.

Chapter 2

Background

2.1 Quantum Computing, Qubits and Quantum Information Processing

Quantum computing is a new and ever growing paradigm in the history of computation. In the 1980s, Richard Feynman discovered that "certain quantum mechanical effects cannot be simulated efficiently on a classical computer" (Rieffel and Polak, 2000), leading to speculation over the efficiency of classical computing and whether computation could be done more efficiently by making use of quantum effects. Quantum computers make use of quantum information processing which involve, "doing information processing using quantum mechanical systems" by, "using quantum mechanics to perform computations, instead of classical physics" (Nielsen and Chuang, 2011; Ornes, 2017).

Rieffel and Polak (2000) suggest that quantum computing offers, "an exponential speed-up" over classical computers in certain cases. However, researchers are certain that, "no conceivable amount of progress in classical computation would be able to overcome the gap between the power of a classical computer and the power of a quantum computer" (Nielsen and Chuang, 2011). Quantum computers also promise to, "efficiently simulate systems that have no known efficient simulation on a classical computer" (Nielsen and Chuang, 2011).

Cusumano (2018) describes quantum computing having uses for mathematical problems that require massive parallel computations such as: optimisation, cryptography and secure communications, pattern matching and big-data analysis, artificial intelligence and machine learning. The main problem is, "quantum computing hardware will likely be more expensive to build than classical hardware" (Moody et al., 2016).

A classical computer works differently to a quantum computer; where a classical computer uses classical bits (in the state 0 or 1), a quantum bit (or qubit, see figure 2.1) can be, "in a superposition state that encodes both 0 and 1" (Rieffel and Polak, 2000; Ornes, 2017). A qubit represents the combination of probabilities for all classical states, wherein measuring a

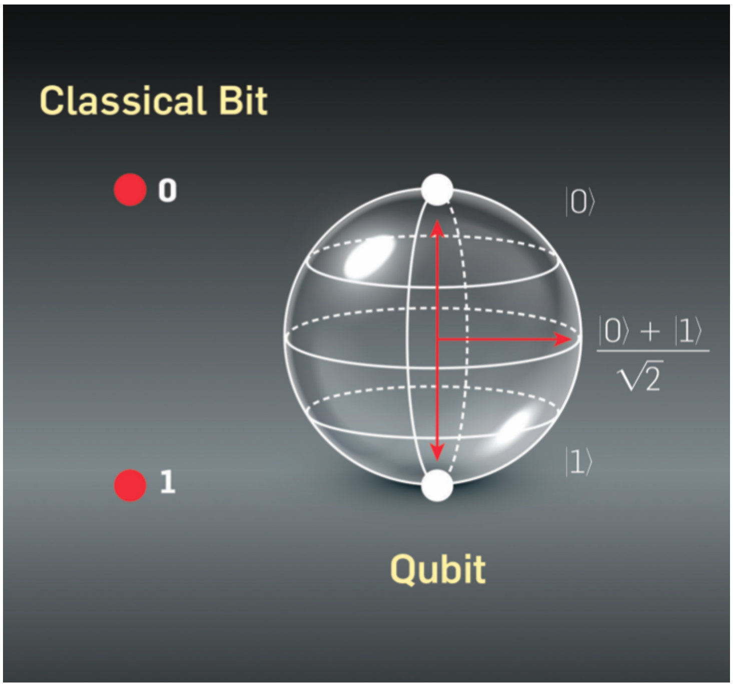


Figure 2.1: Classical Bit vs. Qubit (Monroe, 2018)

qubit randomly yields only one of the values in the superposition (in this case just one classical bit of information, either 0 and 1), while simultaneously destroying all of the other results of the computation (Rieffel and Polak, 2000). If a single qubit can be in a superposition of states 0 and 1, a register of n qubits can be in a superposition of all (2^n) possible input values (Rieffel and Polak, 2000).

A quantum state denotes a group of qubits, and a quantum algorithm performs transformations over quantum states; this transformation changes the probabilities characterising the state of superposition of the qubits (Nielsen and Chuang, 2011). In the time it takes a classical computer to compute the output for a single input state, a quantum computer can compute the values for all input states - known as quantum parallelism. The power of quantum computation derives from, "the exponential state spaces of multiple quantum bits" (Rieffel and Polak, 2000).

It is also important to bare in mind that all quantum state transformations have to be reversible. The classical 'NOT' gate is reversible, though: 'AND', 'OR' and 'NAND' classical gates are not (Rieffel and Polak, 2000). By using various quantum logic gates: controlled-NOT (CNOT) gate and Hadamard gate (Nielsen and Chuang, 2011) in different combinations and orderings, it is possible to carry out all classical computations on quantum mechanical systems.

The power of quantum algorithms derives from taking advantage of quantum parallelism and quantum entanglement where, "desired results will be measured with high probability" (Rieffel and Polak, 2000). Quantum entanglement is defined by Aumasson (2017) as, "two particles can be entangled in such a way that observing the value of either of the two gives you the value of the other particle" and holds true even if the two entangled particles (qubits) are separated by thousands of kilometres Aumasson (2017). Two entangled particles (qubits) are said to be in a Bell state (named after John Bell) and can also be referred to as an Einstein-Podolsky-Rosen (EPR) pair - a concept first discussed in a paper by the three authors concerning, "the strange properties of states like the Bell state" (Nielsen and Chuang, 2011).

The biggest limitation for building a quantum computer is decoherence, "the distortion of the quantum state due to interaction with the environment" (Rieffel and Polak, 2000). This characteristic of physics had researchers believing for a while that quantum computers could not be built, that it would be impossible to isolate quantum states sufficiently from the external environment. The solution to this was in the breakthrough of quantum error correction techniques for multiple qubits (Rieffel and Polak, 2000).

Along side research into the creation of quantum computers, researchers continue to develop theoretical quantum algorithms to evident the practical use of quantum mechanical systems. In 1994, Peter Shor unveiled an algorithm, later known as Shor's algorithm, to tackle two enormously important problems: the factoring of a large integer in order to find the two original prime factors and the discrete logarithm problem (DLP) (Nielsen and Chuang, 2011). Shor's algorithm brings an exponential speed-up for solving not only factoring of a large integer and the DLP, but also elliptic-curve DLP (ECDLP) problems that are widely used in current cryptographic methods (Aumasson, 2017). This sparked widespread interest as these problems were widely believed to be impossible by classical means, leading experts to believe, "the only way to thwart quantum computers is to fight fire with fire, using cryptography that itself relies on quantum mechanics" (Ornes, 2017).

2.2 Cryptography and Cryptosystems

The main chapters of this survey paper discuss quantum cryptography, so it's important to first understand the basics of (classical) cryptography. Cryptography is used to ensure communications between specific parties are kept private by preventing eavesdropping. Cryptography is therefore framed by Nielsen and Chuang (2011) as, "communication or computation involving two or more parties who may not trust one another". The best known cryptographic problem is the transmission of secret messages, such as the communication of payment information to a merchant over the World Wide Web, to prevent a third party intercepting the transaction (Nielsen and Chuang, 2011). This is done using a cryptographic protocol and these can be utilised in two types of cryptosystems: private and public.

Nielsen and Chuang (2011) describe how private-key cryptosystems work by having two parties share a private key, which only they know. Both parties use this key to encrypt communications they wish to send to the other party, then the same private key is used by the recipient for decryption. This is an example of symmetric encryption. Unfortunately, private-key cryptosystems suffer from the basic problem of how to distribute the keys without malicious actors stealing the key and intercepting messages. Public-key cryptosystems solve this by making it unnecessary for two parties to share a private key before communicating.

By contrast public-key cryptosystems work by having each party publish a public key, which is available to the general public. Public-key cryptosystems are most commonly used today for digital signatures and key establishment (Moody et al., 2016), with its security provided by "unproven mathematical assumptions about the difficulty of solving certain problems" (Nielsen and Chuang, 2011). Public-key encryption is an example of asymmetric encryption, it works by having the sender of a message encrypt that message with the recipients public key, so only the correct recipient can decrypt the message using their unique (and secret) private key (Nielsen and Chuang, 2011). Public-key signing (digital signatures), is similar to public-key encryption, wherein a sent message is encrypted by the sender's private key, so any recipient of the message will be able to decrypt the message using the sender's public key (Rivest, Shamir and Adleman, 1983) - this is useful to ensure a message came from a genuine sender.

Aumasson (2017) warns, "quantum computing has been heralded by some as the death of cryptography as we know it". The security of cryptographic protocols, like the widely used Rivest–Shamir–Adleman (RSA) algorithm, rely on the computational hardness of factoring a large integer into its original two prime integers. Shor's algorithm has proven to be effective at factorisation, and so a quantum computer which can implement Shor's algorithms would make RSA obsolete (Rieffel and Polak, 2000; Ornes, 2017). Subsequently, nearly all the public-key cryptography mechanisms currently deployed on the Internet would be broken. The only saving grace is that, in reference to quantum computers, "such machines are still in the early stages of development" and thus, "we should be prepared and understand the real impact of quantum computing on our networks' security" (Aumasson, 2017). There two cryptographic options to consider for our future security: post-quantum cryptography and quantum cryptography.

2.3 Post-Quantum Cryptography

A short-term and relatively cost effective backup plan to prevent a global catastrophe is post-quantum cryptography, also known as quantum-resistant cryptography (Aumasson, 2017). Moody et al. (2016) describe the goal of post-quantum cryptography as developing, "cryptographic systems that are secure against both quantum and classical computers, and can inter-operate with existing communications protocols and networks". It's based on cryptographic protocols that run on classical computers with no known risk from quantum attacks.

Post-quantum cryptography protocols represent a proactive response to predicted future threats, since Moody et al. (2016) caution that, "regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing". This transition to post-quantum cryptography standards brings with it fresh challenges for implementing new cryptographic infrastructures. Therefore it is important for agencies and businesses to focus on "crypto agility" strategies while there is still time (Moody et al., 2016). Public-key cryptosystems are particularly vulnerable, with the construction of large-scale quantum computers rendering them "insecure". By contrast, the impact on symmetric key systems does not seem to "as drastic" (Moody et al., 2016).

Rieffel and Polak (2000) introduce an algorithm developed by Lov Grover, known as Grover's algorithm, intended for unstructured searches in a quantum system. Grover's algorithm provides a quadratic speed-up over classical equivalents for unstructured searches, with an exponential speed-up for search algorithms considered impossible, suggesting that both symmetric algorithms and hash functions should be usable in the era of quantum computing (Moody et al., 2016). This turns the spotlight onto public-key algorithms and which of those currently in use are quantum resistant and, more importantly, those which are not.

Moody et al. (2016) talk about several categories for which post-quantum primitives have been suggested including: lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, hash-based signatures and others which don't fall into the above categories, such as, "evaluating isogenies on supersingular elliptic curves". The National Institute of Standards and Technology (NIST) has started to accept proposals for quantum-resistant public-key encryption, digital signature and key exchange algorithms (Moody et al., 2016). In 2017 they began holding open competitions to encourage the development and ultimately standardisation of post-quantum cryptographic schemes that could be proven unbreakable by quantum computation (Aumasson, 2017). This standardisation drive by NIST has been successful in the past, leading to protocols such as Advanced Encryption Standard (AES), which was developed as a result of co-operation between academia and industry. The effectiveness of the standard has subsequently seen it widely adopted. NIST's standardisation drive into post-quantum cryptography will, "likely provide similar benefits" (Moody et al., 2016), although the agency's current stance is that more research and analysis is needed before proposed post-quantum algorithms can be recommended for widespread deployment.

Post-quantum cryptography is essential for our foreseeable future as part of an overall strategy to, "meet demands for cryptographic usability and flexibility without sacrificing confidence" (Bernstein and Lange, 2017). Aumasson (2017) cautions that it's not clear whether the performance of post-quantum cryptography will be on par with that of quantum-unsafe algorithms in current use. This suggests that there might have to be a trade-off between speed and security. Indeed there are still many conundrums surrounding the future application of post-quantum cryptography.

Moody et al. (2016) suggest that, "most public-key cryptosystems come with a security proof, these proofs are based on unproven assumptions" and thus, "lack of known attacks is used to justify the security of public-key cryptography currently in use". Until systems are tested in earnest by sophisticated quantum attacks in the future there can be no definitive answers. While at this stage, it has to be acknowledged that "current quantum cryptanalysis remains rather limited" (Moody et al., 2016) meaning post-quantum cryptography is so far not known to be insecure.

2.4 Global Catastrophe and Cyber Security Concerns

The impact on society from general-purpose fault-tolerant quantum computers becoming a reality is such that Majot and Yampolskiy (2015) believe, "governments and other organisations would be able to eavesdrop on private citizens with relative ease.'' They predict that this could result in, "a slew of rights violations leading to catastrophe" (Majot and Yampolskiy, 2015).

With the potential to compromise digital certificates by harnessing quantum computation, malicious actors could masquerade as trusted entities. This could threaten the security of digital transactions such as: stock exchanges, personal banking, and software update verification (Majot and Yampolskiy, 2015). Keplinger (2018) believes that, "quantum resistant crypto-currency" would be a necessity for the future, as even block-chain methods could be subject to disruption by quantum computing.

Majot and Yampolskiy (2015) state the necessity for development and maturation of post-quantum cryptographic algorithms, along with new and updated regulations set out by governments and other global institutes. Such new regulations would be required to, "promote the containment and responsible use of quantum computers in order to help alleviate some of the security issues posed by outdated cryptographic systems in a post-quantum environment" (Majot and Yampolskiy, 2015).

The current development of quantum computing is, arguably, reminiscent of conventional computing circa the late 1940s and early 1950s (Cusumano, 2018). However, Moody et al. (2016) stated that researchers working on the building of quantum computers estimated, "a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars". Knowing the risks with current cryptographic protocols, the National Security Agency (NSA) has been transferring to quantum-resistant cryptography since 2015, in preparation for the post-quantum era (Keplinger, 2018).

For all the above reasons, it's vital that post-quantum cryptography avenues continue to be explored. Moody et al. (2016) advise that when standards for quantum-resistant public-key cryptography do become standardised, "NIST will reassess the imminence of the threat of quantum computers to existing standards, and may decide to deprecate or withdraw the affected standards thereafter as a result". It is also important that agencies and businesses be prepared to transition away from any deprecated algorithms in favour of new post-quantum cryptography alternatives as early as 10 years from now (Moody et al., 2016). Just as quantum computation is predicted to be more efficient than classical computation, quantum cryptography could provide a better means of security than standalone post-quantum cryptography.

Chapter 3

Aims

This paper sets out to survey the field of quantum cryptography. Initially providing a background concerning why quantum cryptography could be important and the main body summarising all the different topics within quantum cryptography. The target audience being fellow computer scientists and people in industry who concern themselves with the new era of security and cryptography with regards to the emergence of quantum computing.

Chapter 4

Quantum Cryptography & Quantum Key Distribution (QKD)

4.1 Quantum Cryptography

A long-term and more costly option to help prevent potentially catastrophic breaches of data security in the future is quantum cryptography. Although quantum computing poses a threat to existing public key cryptosystems, it makes sense that new cryptographic schemes should also be developed by exploiting, "the principles of quantum mechanics to enable provably secure distribution of private information" (Nielsen and Chuang, 2011). This leads to the discussion of how quantum mechanics can be used to do key distribution in such a way that security between two parties cannot be compromised, a procedure known as quantum key distribution (QKD).

4.2 What is QKD?

QKD is a quantum-based, provably secure technique by which, "private key bits can be created between two parties over a public channel" (Nielsen and Chuang, 2011). By using properties of quantum mechanics to create a secure communication channel, also known as a quantum channel (Moody et al., 2016; Nielsen and Chuang, 2011), quantum state information/qubits can be shared as part of the key distribution procedure (see figure 4.1) providing, "security and confidentiality by resorting to unbreakable principles of nature" (Pirandola et al., 2019). A requirement for the QKD is that qubits need to be communicated over the quantum channel with an error rate lower than a pre-determined threshold (Nielsen and Chuang, 2011).

The result of QKD being a string of (classical) bits, acting as a private key to be used in a private-key cryptosystem. Recall that with private-key cryptosystems, the difficulty was sharing of a private key between two parties. The security of the resulting private key is, "guaranteed by the properties of quantum information, and thus is conditioned only on fundamental laws of physics being correct" (Nielsen and Chuang, 2011).

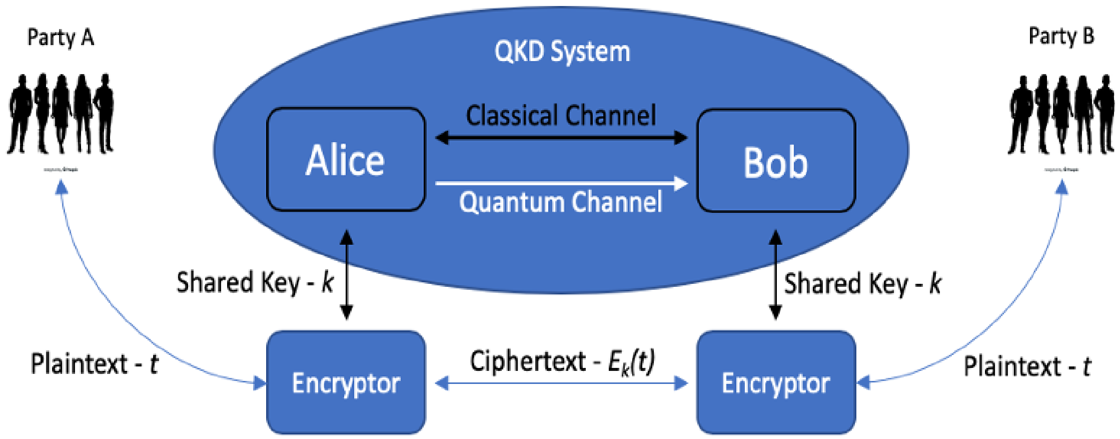


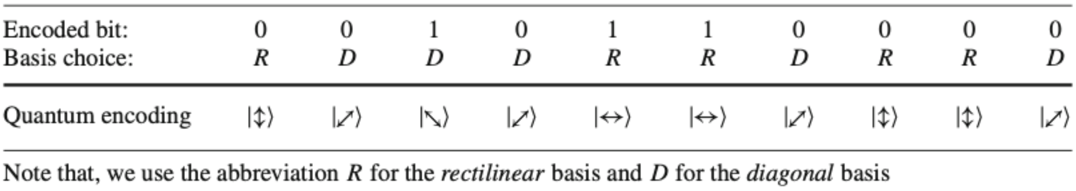
Figure 4.1: Two parties, communicating over a simple quantum network (see chapter 5), which uses a QKD system for key establishment

With QKD, an eavesdropper cannot gain any information through measuring the qubits transmitted between two parties, as this would disturb the state of those qubits - recall how quantum information is inherently susceptible to the act of measurement (see section 2.1). It is therefore possible for two parties conducting QKD to detect whether measurements have been made to a qubit. This property is called "contextuality" (Singh, Bharti and Arvind, 2017) and forms the basis for all QKD, through methods such as conjugate coding (see section 4.3) which make it harder for eavesdroppers to go undetected. Also due to the no-cloning theorem mentioned by Nielsen and Chuang (2011), it is impossible for an eavesdropper to make a copy of a transmitted quantum state (qubit). QKD works very simply in the following way:

1. Alice sends individual particles (e.g. light photons representing qubits) to Bob over a quantum channel.
2. Bob measures the state of the qubits he receives, with each measurement of each qubit resulting in a classical bit (either 0 or 1).
3. Bob and Alice communicate to each other over a classical channel the result of each qubit measurement, and compare each others results.
4. Both Alice and Bob will keep matching bits and use these as a shared (private) key, discarding all non-matching bits.

4.3 Conjugate Coding

Wiesner (1983) introduced the concept of conjugate coding in 1983, also known as quantum coding or quantum multiplexing, based on the principle that one can, "encode classical information into conjugate quantum bases" (Broadbent and Schaffner, 2015). The vast majority of quantum cryptographic protocols exploit conjugate coding in one way or another.



Encoded bit: Basis choice:	0 *R*	0 *D*	1 *D*	0 *D*	1 *R*	1 *R*	0 *D*	0 *R*	0 *R*	0 *D*
Quantum encoding	|↕⟩	|⤢⟩	|⤡⟩	|⤢⟩	|↔⟩	|↔⟩	|⤢⟩	|↕⟩	|↕⟩	|⤢⟩

Note that, we use the abbreviation *R* for the *rectilinear* basis and *D* for the *diagonal* basis

Figure 4.2: Example of Conjugate Coding (Broadbent and Schaffner, 2015)

Broadbent and Schaffner (2015) and Padamvathi, Vardhan and Krishna (2016) state how conjugate coding involves representing a qubit as a light photon, with photon polarisation as a quantum degree of freedom, where photons can be polarised in one of four ways: horizontally (H), vertically (V), diagonally to the left (DL), or diagonally to the right (DR).

Each photon polarisation acts as a quantum property by associating: $H = |0\rangle$, $V = |1\rangle$, $DL = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $DR = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, such that we can apply quantum operations to these states. Using these states, we can define two sets: $R = H, V$ and $D = DL, DR$, the former called the rectilinear basis (R) and the latter called the diagonal basis (D), where R and D are known as "conjugate bases" (Broadbent and Schaffner, 2015; Padamvathi, Vardhan and Krishna, 2016).

Each state within each basis can be associated with a classical bit value (see figure 4.2). The non-orthogonality condition of conjugate bases, "guarantees that an eavesdropper cannot clone or measure the prepared states with perfect fidelity" (Pirandola et al., 2019). Also, with the no-cloning theorem assuring that eavesdroppers cannot replicate a particle of unknown state, any attempt at information retrieval by an eavesdropper, "causes a disturbance on the quantum states that can be detected by the legitimate users" (Pirandola et al., 2019).

4.4 QKD Protocols

There are many QKD protocols in existence today, each take the basic principles of QKD and extend upon it to improve upon security by making it harder for eavesdroppers. Pirandola et al. (2019) summarise the process of generic “prepare and measure” QKD protocols as having two main steps: quantum communication, followed by classical post-processing, which is exactly what most QKD protocols aim to accomplish. Some of the most famous and earliest QKD protocols to be created are the following: BB84, E91 and B92.

4.4.1 BB84 Protocol

BB84 is heralded as the first quantum cryptography (and QKD) protocol, created in 1984 by Charles Bennett and Gilles Brassard (Bennett and Brassard, 1984, 2014). BB84 and many other QKD protocols utilise a concept called conjugate coding (see section 4.3). BB84 in particular was the first QKD protocol to show, "how conjugate coding could be used for an information-theoretically secure key agreement protocol" (Broadbent and Schaffner, 2015), to ensure greater security during the QKD process.

Bennett and Brassard (1984, 2014) and Pirandola et al. (2019) describe how the BB84 protocol works step-by-step, where hypothetical subjects Alice and Bob are trying to securely communicate, and Eve is a potential eavesdropper:

1. Alice sends qubits (or states, each state represented as a light photon) over a quantum channel to Bob, with each qubit encoded in one of two bases (see section 4.3).

2. Bob measures the qubits he received. For each measurement he randomly chooses one of two bases (see section 4.3) to measure each qubit.

3. Alice and Bob both publicly disclose a subset of the data over an (authenticated) classical channel, with Alice announcing which states she sent and Bob announcing which measurement results he obtained.

4. Alice and Bob can now both determine which bits have been transmitted correctly, by identifying those bits for which the sending and receiving bases agree.

5. If any third party had intercepted and measured the qubits, it would change Bob's measurement outcomes and the intrusion would be detected by Alice and Bob.

6. If an intruder is detected, QKD aborts, and repeats at a later stage. If no intruder is detected, the process continues with use privacy amplification and information reconciliation techniques (see section 4.5).

7. After classical post-processing techniques have been applied, Alice and Bob will each have a shared string of bits, known only to them, which can act as private key.

Suppose a malicious actor Eve was to attempt to intercept and measure the state of the qubits initially transmitted by Alice over the quantum channel, then resend new qubits with the measured state. Recall how when a qubit is measured it falls out of superposition yielding a classical bit (either 0 or 1, see section 2.1). If Eve was to try the above she will potentially use the wrong basis for her measurements approximately 50% of the time, and potentially resend a qubit with the wrong basis (Nielsen and Chuang, 2011).

If Bob were to measure a resent qubit with the correct basis there will be a 25% probability that he measures the wrong value. Thus any eavesdropping on the quantum channel is bound to introduce a higher error rate, making it apparent to Alice and Bob that someone is eavesdropping, which can be checked by, "communicating a sufficient number of parity bits of their keys" (Nielsen and Chuang, 2011) over the (authenticated) classical channel. It's also likely that Eve's version of the key would be 25% incorrect anyway.

The BB84 protocol has also been extended in subsequent years from using four states (four qubits sent, two bases used) to use six states with three bases used (Pirandola et al., 2019). This makes it harder for eavesdroppers to guess the correct basis used for measurement, and will result in the eavesdropper producing an even higher rate of error.

4.4.2 E91 & BBM92 Protocol(s)

In 1991, Artur Ekert developed a new approach to QKD, which for the first time exploits entanglement for cryptographic purposes, later called "BBM92" or "EPR scheme" (Pirandola et al., 2019). Consider a pair of entangled particles (an EPR pair in a Bell state), which are then separated and sent to Alice and Bob, each getting one half of each pair. The received particles are measured by Alice and Bob by one of three possible bases. Any intervention from eavesdroppers would subsequently induce, "elements of physical reality which affects the non-locality of quantum mechanics" (Pirandola et al., 2019). The security of the protocol is guaranteed by a Bell-like test to rule out eavesdroppers by relying on the non-local feature of entangled states in quantum physics.

4.4.3 B92 Protocol

In 1992, Charles Bennett showed that it was possible for QKD to be performed using only two (non-orthogonal) states - the bare minimum required to transmit one bit of a cryptographic key in any QKD protocol (Pirandola et al., 2019). The process starts with Alice preparing a qubit in one of two quantum states, with each possible state associated with a classical bit value (the first quantum state as 0, and the second as 1). The state is sent to Bob, who measures it in a suitable basis, to retrieve Alice's bit. If the states were orthogonal, it is always possible for Bob to deterministically recover the bit (Pirandola et al., 2019). Due to its properties of demonstrating the minimum requirements for QKD, the performance of the B92 protocol is not as good as that of the BB84 protocol.

4.5 Privacy Amplification & Information Reconciliation

In terms of the Alice and Bob example above, if no intrusion is detected, two classical pre-processing techniques can be applied to, "systematically increase the correlation between their key strings, while reducing eavesdropper Eve's mutual information about the result, to any desired level of security" (Nielsen and Chuang, 2011). These are privacy amplification and information reconciliation.

Information reconciliation provides a means of doing error-correction conducted over a (classical) public channel, reconciling errors between both parties bit strings (X and Y) to obtain a shared bit string (W), while divulging as little information as possible to Eve (Nielsen and Chuang, 2011).

Privacy amplification involves a string of bits, which is partially known by an adversary, and producing a smaller string of bits out of the original string, for which no external attacker can have any, "statistically significant information" (Herrero-Collantes and Garcia-Escartin, 2017) concerning the new string. Supposing Eve has obtained a random string (Z) which is partially correlated with Alice and Bob's shared key (W), privacy amplification can be used to, "reduce Eve's stolen information to a negligible amount" (Pirandola et al., 2019).

Specifically, Alice and Bob extract from the current shared key (W) a smaller set of bits (S) whose correlation with Eve's obtained information (Z) is below a desired threshold (Nielsen and Chuang, 2011). This smaller set of bits (S) known only to Alice and Bob will have high entropy, and thus make a good private key.

4.6 QKD vs. Public Key Cryptosystems

It's important to reiterate how, "none of the QKD techniques are substitutes for public key encryption schemes" (Nielsen and Chuang, 2011). It stands to reason that public-key (asymmetric) cryptographic schemes will still be favoured going forward as QKD, by itself, cannot compete in aspects such as authentication (Ioannou and Mosca, 2014). This is the main limitation of QKD, in that it can only create a private channel between two parties that can authenticate to each other. Without a separate means of authentication, QKD is susceptible to man-in-the-middle attacks. Since QKD requires an authenticated classic channel to conduct authentication (Zawadzki, 2018), the only means of currently authenticating users over the Internet is by using existing (classical) public-key cryptographic schemes.

4.7 Device-independent Quantum Cryptography

Quantum cryptographic protocols can be said to be device-independent if, "protocols can be run on untrusted devices which have possibly been constructed by the adversary" (Broadbent and Schaffner, 2015), and thus implementations of such protocols need to have measures in place to counter these malicious devices such that the process of the quantum cryptographic protocol (e.g. QKD) is unimpeded.

4.7.1 Measurement-Device-Independent QKD

Measurement-device-independence holds the same definition as 'device-independent', as seen in section 4.7, only it refers specifically to the act of conducting measurements of quantum states. Lo, Curty and Qi (2012) conceived the notion of measurement-device-independent QKD (MDI-QKD), showing that two parties can successfully and efficiently engage in a QKD process using an untrusted relay, as long as Alice and Bob trust the equipment in their own possession. This means that quantum repeaters or relays (used in making up a quantum network, see chapter 5) need not compromise the security of a QKD protocol.

4.8 Position-based Quantum Cryptography

Position-based quantum cryptography is where entities involved in a quantum cryptographic process can use, "geographical position as cryptographic credential" (Broadbent and Schaffner, 2015). This works by exploiting the, "relativistic no-signalling principle" that messages cannot travel faster than the speed of light; this can be used to conduction timely verification (by a 'verifier') concerning whether one is within a certain distance (Broadbent and Schaffner, 2015). Even though currently it seems inapplicable for quantum protocols, for the task of position verification, the possibility of, "position-based quantum cryptography against resource-bounded adversaries remains a tantalising open question" (Broadbent and Schaffner, 2015).

4.9 Quantum Coin Flipping

Bennett and Brassard (1984, 2014) describe quantum coin flipping as a solution to the problem of, "two distrustful parties communicating at a distance without the help of a third party", such that they can agree on a winner and a loser between themselves, with each party having exactly 50% chance of winning. Also, if either party were to bias the outcome, this would be detected by the other party as cheating.

The process is similar to QKD, though the process of quantum coin-flipping is as follows

(Bennett and Brassard, 1984, 2014):

1. Alice randomly chooses one basis and encodes a random a string of bits with that basis before sending the resulting sequence of qubits to Bob.

2. Bob reads each qubits with a random basis, and records the results in two tables, one table for rectilinear received qubits and one of diagonally received qubits.

3. Bob makes his guess as to which basis Alice used, and announces it to Alice. Guessing correctly means he wins, other he loses.

4. Alice reports to Bob whether he won, certifying this information by sending Bob (over a classical channel) her entire original string of bits.

5. Bob can now verify that no cheating has occurred, by comparing Alice's sequence with both of his tables (from step 2), as there should be perfect agreement with the table corresponding to Alice's reported basis and no correlation with the other table.

4.10 Quantum Money

Quantum money, was a concept thought up in the 1960s by Wiesner (1983) and uses conjugate coding (see section 4.3) techniques in the construction of "physically unforgeable" (Broadbent and Schaffner, 2015) money, which relies on the properties of quantum mechanics and the no-cloning theorem to prevent counterfeiting. The proposal by Wiesner (1983) consists of quantum banknotes created by encoding quantum particles using conjugate coding, with both the classical information and basis choice being chosen as random bit strings. A quantum banknote consists of a sequence of single qubits, chosen randomly from two bases (see section 4.3), with each quantum banknote also having an originator (typically called "the bank") that can verify that a quantum banknote is genuine.

Chapter 5

Quantum Networks

Quantum networks concern the creation of infrastructure for quantum cryptographic techniques (such as QKD) over large distances, through both physical and wireless technologies, boasting "impregnable security" (Ornes, 2017). QKD in particular requires the ability to reliably transmit, receive, and measure single qubits (generally encoded as single light photons), with new challenges arising when trying to implement a QKD network on a global scale.

A quantum network for QKD (known as a nodal QKD network) would be made up of quantum transmitters (Alice's) and quantum receivers (Bob's), inter-connected with (trusted) quantum repeaters or relays, via point-to-point links (Fröhlich et al., 2013). Pirandola et al. (2019) define quantum repeaters or relays as, "any type of middle node between Alice and Bob which helps their quantum communication by breaking down their original quantum channel into sub-channels".

Fröhlich et al. (2013) mention how point-to-point links in a quantum network could be realised using long-distance 'lit' optical fibres (in contrast to 'dark' optical fibre, 'lit' optical fibre is simultaneously being used for other applications), and in the future, potentially ground-to-satellite communication. Ornes (2017) mentions how some experts are interested in building, "a global quantum Internet in which computers would communicate securely using the quantum mechanical properties of particles of light", harnessing networks both on the ground using existing fibre-optic cables and in space using satellites capable of exchanging light photons.

Fröhlich et al. (2013) mention how several field tests of QKD have proven it to be a, "reliable technology for cryptographic key exchange" though currently we are unable to extend the scope of QKD beyond, "niche applications in dedicated high security networks". Even though both fibre and satellite technologies would be great for the longer distance point-to-point links, they would be less suitable in providing a multitude of individual users access (e.g. the last-mile service) to this QKD infrastructure (Fröhlich et al., 2013). Also, though 'lit' optical fibre is in principle able to perform QKD over commercial fibre-optical networks, elements of existing networks may be incompatible with QKD at present. Background noise from commercial implementations would also be worse than in dedicated fibre.

Garcia-Escartin and Chamorro-Posada (2007) mention how future quantum networks, intended primarily for communication, will involve multiple users sharing limited resources. Whereby in order to allow for multiple simultaneous communications, multiplexing techniques will also need to be considered.

It has been shown that quantum networks using primarily satellite communication may be much more efficient due to the vacuum of space (Yin et al., 2017). QKD over 'lit' optical fibre has been shown to reach around 100 km (greater than 300 km on dedicated fibre), though a satellite link can reach as far as 1200 km.

Quantum networks still have a long way to go, with the need to develop and implement more robust (QKD) protocols able to achieve long distances while upholding a reasonably high data rate. These would also need to support concepts such as MDI-QKD (see section 4.7), wherein middle nodes (quantum repeaters or relays) may generally be unreliable and untrusted.

5.1 Network-centric Quantum Communications (NQC)

Hughes et al. (2013) mention how trusted QKD networks using point-to-point links: lack scalability, perform optimally on dedicated optical fibre, are expensive and lack incentive for mass production, and only provide one of the cryptographic functions (QKD) needed for secure communications, such that they have received limited practical interest.

As quantum networks could see implementation on optical fibre, and so topics such as network-centric quantum communications (NQC) for, "light weight encryption, authentication and digital signatures" (Hughes et al., 2013) over fibre-optics are vital. NQC offers, "a scalable form of quantum cryptography providing key management with forward secrecy" (Hughes et al., 2013).

Chapter 6

Delegated Quantum Computation

Since quantum computers are very expensive, and thus not everyone will be able to afford one, it is likely for standalone users in the future (without physical access to a quantum computer) to harness the power of quantum computation through cloud-based quantum computing services, in which a client's computation is delegated to a remote quantum computing server. Delegated (classical) computation is currently widespread, in the form of cloud computing (Fitzsimons, 2017), with security of cloud computing (in particular for cloud quantum computer) potentially becoming a serious issue in the future (Pirandola et al., 2019). There are two prevalent types of delegated quantum computation: blind quantum computation (BQC) and quantum homomorphic encryption (QHE).

6.1 Blind Quantum Computation (BQC)

BQC addresses the task of a client with limited quantum capabilities interacting with a remote quantum computer to, "perform an arbitrary quantum computation, while keeping the description of that computation hidden from the remote quantum computer" (Mantri, Perez-Delgado and Fitzsimons, 2013), wherein a client sends a quantum state to the quantum server, with such state encoding both the chosen algorithm and the input (Pirandola et al., 2019).

BQC expects a client to at least be able to create, measure, send and/or receive very simple single qubit states. BQC allows a client to execute a quantum algorithm by using one or more remote quantum computers, while allowing the client to verify that the server is correctly performing the delegated computation and at the same time keep the results of the computation hidden (Pirandola et al., 2019). Fitzsimons (2017) explains how a client is able to verify the the correctness of the computation performed by the remote quantum server by embedding hidden tests within the computation. During BQC, it is key that the server does not learn the input, output, or even track the computation performed on behalf of the client, and thus by ensuring anonymity from the server, it allows one to counteract the threat posed by a compromised or malicious server (Fitzsimons, 2017).

Broadbent, Fitzsimons and Kashefi (2009) describe a fault-tolerant universal BQC (UBQC) protocol, known as the BFK protocol, which can detect cheating by the quantum server and does not require any quantum computation by the client. The only requirement of the client is that they can prepare single qubits randomly chosen from a finite set and send them to the quantum server (Broadbent, Fitzsimons and Kashefi, 2009). The protocol works in two steps: preparation and computation.

- Preparation: Alice (client) prepares single qubits chosen randomly and sends them to Bob (server), wherein Bob entangles these received qubits in accordance with a, "brickwork state" (Broadbent, Fitzsimons and Kashefi, 2009), which results in Bob unavoidably learning the maximum length of input and depth of the computation - though no specific information regarding Alice's computation is revealed.

- Computation: Alice and Bob interact using two-way classical communication: Alice is able to drive the computation, by giving Bob single-qubit measurement instructions based on previous measurement outcomes communicated by Bob to Alice.

In terms of how the properties of BQC are enforced, Fitzsimons (2017) states that, "encryption can be used to hide communication between the client and the server from eavesdroppers, while authentication codes can be used to detect any attempt to modify these messages". The most desirable setting for BQC application would be, "a verifiable BQC protocol which could be performed between a client without any quantum capabilities and a single quantum server" Fitzsimons (2017). Potential future implementations of BQC would be to use satellite quantum communication methods in order to, "send quantum states from a satellite to ground servers" (Pirandola et al., 2019).

6.2 Quantum Homomorphic Encryption (QHE)

Yu (2018) and colleagues (Yu, Perez-Delgado and Fitzsimons, 2014) describe (classical) homomorphic encryption (HE) as an encryption scheme that allows computation to be performed on data encrypted in such a way that certain operations can be performed on that data without decryption. This allows the potential for a user to provide encrypted data to a remote server for processing without having to reveal the plaintext. An HE scheme can be said to be 'fully homomorphic' if it allows for any arbitrary amount of quantum computation to be performed (Ouyang, Tan and Fitzsimons, 2018). An HE scheme that supports quantum computation is a quantum homomorphic encryption (QHE) scheme, and a QHE scheme which is fully-homomorphic is a quantum fully homomorphic encryption (QFHE) scheme (Alagic et al., 2017).

QHE involves performing quantum computation on a party's private (encrypted) data with the program provided by another party, without either party revealing much information (about the data nor the program) to the opposing party (Yu, 2018). QHE gives the certainty that the final computation result is correct, and that the data and the final computation result are known only to the data-provider who, "learns little about the circuit performed beyond what can be deduced from the result of the computation itself" (Yu, 2018).

Though BQC and QHE have the same goal of carrying out a computation on encrypted data (Mahadev, 2018), QHE differs from BQC in that, with QHE, "the party with the program does not know the output" (Yu, 2018). Wherein BQC, "the computation to be performed forms part of the secret, QHE schemes do not have secret circuit evaluations" (Ouyang, Tan and Fitzsimons, 2018) meaning they serve only to obscure the information that is intended for processing. Also, where BQC allows multiple rounds of interaction between the client and server, QHE allows only one round of interaction (Mahadev, 2018).

Ouyang, Tan and Fitzsimons (2018), Yu, Perez-Delgado and Fitzsimons (2014) and Tan et al. (2016) describe how HE and QHE schemes comprise four components: key generation, encryption, evaluation, and decryption.

- Key Generation: conducted by a key generation protocol, producing a quantum state used as a key for encryption.

- Encryption: an encryption unitary operator/algorithm encrypts the data (input state) using the generated encryption key (and potentially making use of some ancilla system). This process results in a decryption key being produced.

- Decryption: a decryption unitary operator/algorithm decrypts the encrypted state using the decryption key.

- Evaluation: conducted by a set of evaluation unitary operators/an evaluation algorithm, used to process the data without decryption such that, "after decrypting the output the net effect is equivalent to applying a quantum circuit directly to the initial input state" (Yu, Perez-Delgado and Fitzsimons, 2014).

QFHE discussed by Ouyang, Tan and Fitzsimons (2018) satisfies two properties: correctness and compactness. Correctness occurs when, "the evaluated output on the cipher-state after decryption is equivalent to the output of the direct evaluation on the quantum plaintext" (Ouyang, Tan and Fitzsimons, 2018). Compactness of a scheme is when the complexity of a decryption algorithm, "does not depend on the computation to be evaluated and scales only polynomially in the size of the plaintext" (Ouyang, Tan and Fitzsimons, 2018). This implies that a decryption algorithm used in QFHE schemes cannot in any way depend on the evaluated computation.

QHE has hit a barrier in recent studies with (Yu, Perez-Delgado and Fitzsimons, 2014) revealing that QHE is not able to achieve "perfect information theoretic security" (Tan et al., 2016) while enabling arbitrary processing of encrypted data, unless the size of the encoding grows exponentially.

Chapter 7

Quantum Random Number Generators (QRNGs)

Random numbers are essential in cryptographic practices and protocols, used in: nonces (numbers that must be used only once), initialisation vectors, sequence numbers (the starting number in a sequence), digital signatures, interactive protocols, and salts (a random sequence that is hashed together with a password) to avoid dictionary attacks in hashed password lists (Herrero-Collantes and Garcia-Escartin, 2017). Herrero-Collantes and Garcia-Escartin (2017) mention two kinds of generating number with random number generators (RNGs); "algorithmically generated numbers that mimic the statistics of random distributions and random numbers generated from unpredictable physical events".

Devices which use the former method are known as pseudo-random number generators (PRNGs), they are intend for "random enough number generation, even if it produces a predictable sequence" (Herrero-Collantes and Garcia-Escartin, 2017) and thus cannot be consider truly random number generation.

Devices which use the latter method of number generation are known as true random number generators (TRNGs), used heavily in applications that require outputs that are not so easily guessed by using a physical process which is, "unpredictable or, at least, difficult to predict" (Herrero-Collantes and Garcia-Escartin, 2017). Ma et al. (2016) suggest that generation of true randomness is generally considered impossible by classical means.

Quantum cryptography also needs a reliable source of randomness and QRNGs could be the answer. QRNGs can, "significantly improve the security of cryptographic protocols by ensuring that generated keys cannot be predicted" (Sanguinetti et al., 2014) as QRNGs use quantum mechanical effects to produce random numbers - they are a particular type of TRNGs (Herrero-Collantes and Garcia-Escartin, 2017; Ma et al., 2016). Ma et al. (2016) state how, "true randomness can only be obtained via processes involving inherent randomness", and due to the randomness at the core of quantum mechanics, it makes a perfect source of entropy with the potential of "true randomness" while achieving fast generation rates - even on untrusted hardware using device-independent generation protocols (Herrero-Collantes and Garcia-Escartin, 2017).

Ma et al. (2016) mention how true randomness can be achieved from the measurement of a quantum system (for example, measuring a single qubit). Herrero-Collantes and Garcia-Escartin (2017) indicate that there are various methods used in QRNGs: radioactive decay, electronic noise and analyses, measuring the quantum states of light photons to gather entropy from a quantum origin, non-optical quantum phenomena, and those whose randomness is primarily backed by quantum mechanics. QRNGs are, "faster than alternative TRNGs, produce random numbers of good quality and suppose small deviations from the usual configuration of the equipment" (Herrero-Collantes and Garcia-Escartin, 2017) such that most QRNGs can be built with the same technology and at a relatively low cost (Ma et al., 2016).

(Ma et al., 2016) define three categorises for QRNGs depending on a devices' degree of trustworthiness: trusted device, self-testing and semi-self-testing.

- Trusted device (practical) quantum random number generation, relies on fully trusted and calibrated devices, generating randomness at a high speed by properly modelling the devices.

- Self-testing quantum random number generation, relies on verifiable randomness can be generated without trusting the actual implementation.

- Semi-self-testing quantum random number generation, is an intermediate category, providing a trade-off between the trustworthiness on the device and random number generation speed.

QRNGs are already available as commercial products and online servers, providing quantum random number generation on demand (Herrero-Collantes and Garcia-Escartin, 2017), as up until now, "the cost, size, and power requirements of current QRNGs have prevented them from becoming widespread" (Sanguinetti et al., 2014). Although proposals such as the one made by Sanguinetti et al. (2014) for integrating random number generation into smartphones, using ever-improving camera technology to measure, "light at the few-photon level", would help make the widespread use of quantum random numbers possible.

7.1 QRNGs for QKD

QKD offers a way to generate two secure keys at distant locations, though its security relies on a vast quantity of random numbers (Sanguinetti et al., 2014). Stipcevic (2011) mentions how the BB84 (QKD) protocol would be, "completely insecure if only an eavesdropper could calculate (or predict) either Alice's random numbers or Bob's random numbers or both", meaning RNGs used by BB84 should be TRNGs. Herrero-Collantes and Garcia-Escartin (2017) describes QKD as a, "sophisticated distributed secure random number generator", which includes a physical method to generate entropy and a randomness amplification algorithm (see section 4.5). QKD protocols assume they have access to true randomness, making QRNGs most beneficial for QKD.

Without a means of true randomness for deciding the measurement bases and the states used in the QKD process, practical QKD protocols such as BB84 protocol could be vulnerable to attacks/hacks due to imperfect state preparation and measurement (Herrero-Collantes and Garcia-Escartin, 2017; Xavier et al., 2009; Li et al., 2015). So long as both sender and receiver (Alice and Bob) involved in a QKD process use a hardware-based true QRNG, the QKD process will benefit from, "truly random and independent choices" instead of relying on (classical) software RNGs which generate pseudo-random sequences (Xavier et al., 2009).

Chapter 8

Perfect Secrecy Cryptography

The future could see classical alternatives to quantum cryptography coming to light, as even though quantum cryptography is unclonable, it requires quantum installations that are more expensive, slower, and less scalable than classical optical networks (Di Falco et al., 2019).

A simple yet effective private key cryptosystem is the Vernam cipher, also known as a one time pad (OTP) (Nielsen and Chuang, 2011), is an example of perfect forward secrecy cryptography; also known as perfect secrecy cryptography (Ornes, 2017). OTP involves encoding a message via a bitwise XOR operation with a random key (string of bits); it is secure only as long as, "the number of key bits is at least as large as the size of the message being encoded" (Nielsen and Chuang, 2011). By never reusing the random key in whole or in part, it reduces the threat of attack through cryptanalysis techniques (Ornes, 2017). As long as the random key used for OTP remains secret, it said to be "provably secure" (Nielsen and Chuang, 2011). Even though OTP is sophisticated enough to divulge no information other than the maximum length of the message, it has not seen wide adoption due to lack of a practical and secure way for users to exchange the key (Ornes, 2017).

Di Falco et al. (2019) have recently introduced a means of perfect secrecy cryptography intended for classical optical channels (see figure 8.1). The system they propose exploits correlated (chaotic) wave-packets, mixed in inexpensive (CMOS-compatible) silicon chips, with each chip generating, "0.1 Tbit of different keys for every mm of length of the input channel, and require the transmission of an amount of data that can be as small as 1/1000 of the message's length" (Di Falco et al., 2019).

Though the security of this proposed system is not of a quantum nature, the security is enforced by, "the second law of thermodynamics and the exponential sensitivity of chaos" such that the process is near irreversible/impossible to replicate, as a result it prevents attackers from getting any information on the exchanged key (Di Falco et al., 2019).

There are upward scalablity issues with current quantum networks technologies for global scale. Data transfer speed exhibited on prototype quantum networks are considerably slower than

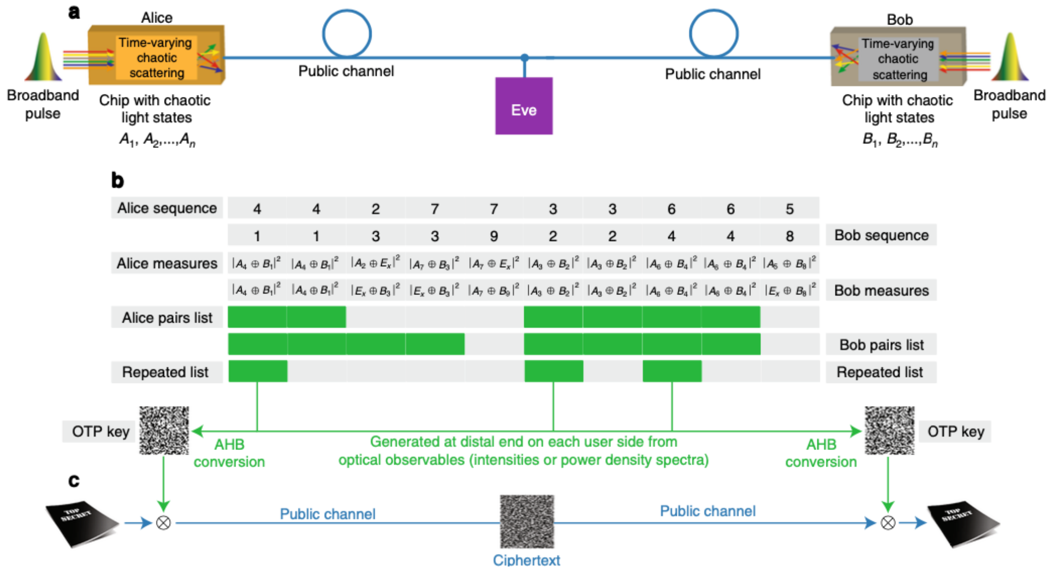

a
Alice
Time-varying chaotic scattering
Broadband pulse
Chip with chaotic light states
$A_1, A_2, \ldots, A_n$
Public channel
Eve
Public channel
Bob
Time-varying chaotic scattering
Chip with chaotic light states
$B_1, B_2, \ldots, B_n$
Broadband pulse
b
Alice sequence 4 4 2 7 7 3 3 6 6 5
1 1 3 3 9 2 2 4 4 8 Bob sequence
Alice measures $|A_4 \oplus B_1|^2$ $|A_4 \oplus B_1|^2$ $|A_2 \oplus E_x|^2$ $|A_7 \oplus B_3|^2$ $|A_7 \oplus E_x|^2$ $|A_3 \oplus B_2|^2$ $|A_3 \oplus B_2|^2$ $|A_6 \oplus B_4|^2$ $|A_6 \oplus B_4|^2$ $|A_5 \oplus B_8|^2$
$|A_4 \oplus B_1|^2$ $|A_4 \oplus B_1|^2$ $|E_x \oplus B_3|^2$ $|E_x \oplus B_3|^2$ $|A_7 \oplus B_9|^2$ $|A_3 \oplus B_2|^2$ $|A_3 \oplus B_2|^2$ $|A_6 \oplus B_4|^2$ $|A_6 \oplus B_4|^2$ $|E_x \oplus B_8|^2$ Bob measures
Alice pairs list
Bob pairs list
Repeated list
Repeated list
OTP key
AHB conversion
Generated at distal end on each user side from optical observables (intensities or power density spectra)
AHB conversion
OTP key
c
Public channel
Public channel
Ciphertext

Figure 8.1: The Di Falco et al. (2019) protocol scheme for perfect secrecy key generation on classical channels. (Step a) Communication setup on a classical public channel with the users (Alice and Bob) and attacker (Eve). (Step b) Communication and key generation steps: Alice and Bob launch broadband pulses from their sides and transmit different chaotic states (A_n and $B_{n'}$), always measuring correlated mixed chaotic states when Eve does not actively interfere on the channel with additional states E_x. At the end of the transmission, Alice and Bob generate new keys. (Step c) Encryption and decryption scheme via bitwise XOR between the text and the generated key.

classical optical communications (Ornes, 2017). Advantages of this scheme by Di Falco et al. (2019) include: the compatibility to make use of existing optical fibre networks and network technologies, while providing a classical means of perfect forward secrecy.

The system works by exploiting the property of 'chaos' to generate, "time varying signals that are mathematically unpredictable" in order to support a, "bidirectional communication channel for securely exchanging random keys of arbitrary length" (Di Falco et al., 2019). If two users (Alice and Bob) each possess a proposed chip, they can generate chaotic light states from the, "chaotic scattering of broadband pulses with different frequencies and diverse input conditions" such that each light state is, "a random superposition of optical waves at different frequencies" for transmission over a public (classical) optical channel (Di Falco et al., 2019).

Di Falco et al. (2019) assure that the system/protocol is fully compatible with existing supporting techniques for QKD, such as privacy amplification and information reconciliation (see section 4.5). It only requires initial communication when authenticating the users; thus this system can be seen as a classical alternative to QKD. Another decisive pro for the adoption of this protocol by Di Falco et al. (2019) is that it does not require, "electronic databases, private keys, or confidential communications", such that when combined with existing network capabilities on a globalised scale, to keep costs down, perfect secrecy cryptography will be still achievable.

Chapter 9

Conclusion

In conclusion, quantum computing is on the horizon and it is clear that a lot of cryptographic schemes and protocols in use today are vulnerable. Post-quantum cryptography is only a short-term solution in preventing a global catastrophe, which could result if there is not sufficient investment in the development of cryptographic standards capable of withstanding quantum attacks. A long-term and costly option, though likely more prevalent and future-proof, is quantum cryptography.

As previously discussed quantum cryptography has many fields of study. The possible implementation of QKD and other quantum cryptographic schemes (such as quantum coin flipping) on global scale quantum networks will only be feasible for large companies and institutes with the financial means to fund such projects. Though thanks to delegated quantum computing techniques, owners of this new quantum network hardware could provide cloud-based solutions for everyone to be able to harness quantum computation through both BQC and QHE methods.

QRNGs will likely see their usefulness increase, for providing a form of true randomness, especially since hardware for such devices are low cost and can feasibly start to be integrated into handheld devices such as smartphones for day-to-day usage. The concept of quantum money, though currently hypothetical, could also be the answer to a future alternative for (classical) block chain methods.

There also exist new concepts of classical cryptography which could match the level of security found from existing quantum cryptographic schemes. One potential scheme, heralded a classical BB84 protocol, implements a OTP type scheme by exploiting correlated (chaotic) wave-packets, mixed in inexpensive (CMOS-compatible) silicon chips. This has the potential for implementation in personal computers and laptops at a fraction of the cost of quantum cryptographic hardware, making perfect forward secrecy accessible for everyone.

This project has surveyed and summarised the field of quantum cryptography and other similar theories; with the intention to make readers of this paper aware of both old and existing discussions. This will hopefully encourage more people to take an early interest in the future of cryptography when considering the very real concern of quantum computation.

For anyone with an interest in the future of cryptographic standards and technologies, who would perhaps like to know more than that which is presented in this entry-level survey paper, the topics outlined in chapters 4, 5, 6, 7 and 8 can be further explored. There needs to be a proactive response to the potential of quantum computing, rather than 'reactive'. With the goal being to make the world's security more stable and assured during a time of great innovation for quantum computing.

Bibliography

Alagic, G., Dulek, Y., Schaffner, C. and Speelman, F. (2017). Quantum fully homomorphic encryption with verification. *Lecture Notes in Computer Science*, p. 438–467.

Aumasson, J.-P. (2017). The impact of quantum computing on cryptography. *Computer Fraud & Security*, 2017(6), pp. 8 – 11.

Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, India, p. 175.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, p. 7–11.

Bernstein, D. J. and Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), pp. 188–194.

Boland, H. and Zolfagharifard, E. (2019). Google ushers in era of 'quantum supremacy': Here's what that means. https://www.telegraph.co.uk/technology/2019/10/23/google-researchers-achieve-quantum-supremacy/, accessed: 24 October 2019.

Broadbent, A., Fitzsimons, J. and Kashefi, E. (2009). Universal blind quantum computation. *2009 50th Annual IEEE Symposium on Foundations of Computer Science*.

Broadbent, A. and Schaffner, C. (2015). Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1), p. 351–382.

Cusumano, M. A. (2018). The business of quantum computing. *Commun ACM*, 61(10), pp. 20–22.

Di Falco, A., Mazzone, V., Cruz, A. and Fratalocchi, A. (2019). Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips. *Nature Communications*, 10(1), p. 5827.

Fitzsimons, J. F. (2017). Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1), p. 23.

Fröhlich, B., Dynes, J., Lucamarini, M., Sharpe, A., Yuan, Z. and Shields, A. (2013). A quantum access network. *Nature*, 501, pp. 69–72.

Garcia-Escartin, J. C. and Chamorro-Posada, P. (2007). Quantum multiplexing for quantum computer networks.

Herrero-Collantes, M. and Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics*, 89(1).

Hughes, R., Nordholt, J., Mccabe, K., Newell, R., Peterson, C. and Somma, R. (2013). Network-centric quantum communications with application to critical infrastructure protection.

Ioannou, L. M. and Mosca, M. (2014). Public-key cryptography based on bounded quantum reference frames. *Theor Comput Sci*, 560, pp. 33–45.

Keplinger, K. (2018). Is quantum computing becoming relevant to cyber-security? *Network Security*, 2018(9), pp. 16 – 19.

Li, H.-W., Yin, Z.-Q., Wang, S., Qian, Y.-J., Chen, W., Guo, G.-C. and Han, Z.-F. (2015). Randomness determines practical security of bb84 quantum key distribution. 1508.06396.

Lo, H.-K., Curty, M. and Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13).

Ma, X., Yuan, X., Cao, Z., Qi, B. and Zhang, Z. (2016). Quantum random number generation. *npj Quantum Information*, 2(1).

Mahadev, U. (2018). Classical homomorphic encryption for quantum circuits. In M. Thorup, ed., *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, IEEE Computer Society, pp. 332–338.

Majot, A. and Yampolskiy, R. (2015). Global catastrophic risk and security implications of quantum computers. *Futures*, 72, pp. 17 – 26, confronting Future Catastrophic Threats To Humanity.

Mantri, A., Perez-Delgado, C. A. and Fitzsimons, J. F. (2013). Optimal blind quantum computation. *Physical Review Letters*, 111(23).

Monroe, D. (2018). Quantum leap. *Commun ACM*, 62(1), p. 10–12.

Moody, D., Chen, L., Jordan, S., Liu, Y.-K., Smith, D., Perlner, R. and Peralta, R. (2016). Nist report on post-quantum cryptography.

Nielsen, M. A. and Chuang, I. L. (2011). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. New York, NY, USA: Cambridge University Press, 10th edn.

Ornes, S. (2017). Code wars: Quantum cryptography gears up to fight code-breaking quantum computers. will the approach bolster security in the future, or is it fatally flawed? *Proceedings of the National Academy of Sciences of the United States of America*, 114(11), pp. 2784–2787.

Ouyang, Y., Tan, S.-H. and Fitzsimons, J. F. (2018). Quantum homomorphic encryption from quantum codes. *Physical Review A*, 98(4).

Padamvathi, V., Vardhan, B. V. and Krishna, A. V. N. (2016). Quantum cryptography and quantum key distribution protocols: A survey. In *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, pp. 556–562.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. and Wallden, P. (2019). Advances in quantum cryptography. `1906.01645`.

Rieffel, E. and Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Comput Surv*, 32(3), pp. 300–335.

Rivest, R. L., Shamir, A. and Adleman, L. (1983). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 26(1), pp. 96–99.

Sanguinetti, B., Martin, A., Zbinden, H. and Gisin, N. (2014). Quantum random number generation on a mobile phone. *Physical Review X*, 4(3).

Singh, J., Bharti, K. and Arvind (2017). Quantum key distribution protocol based on contextuality monogamy. *Physical Review A*, 95(6).

Stipcevic, M. (2011). Quantum random number generators and their use in cryptography. In *2011 Proceedings of the 34th International Convention MIPRO*, pp. 1474–1479.

Tan, S.-H., Kettlewell, J. A., Ouyang, Y., Chen, L. and Fitzsimons, J. F. (2016). A quantum approach to homomorphic encryption. *Scientific Reports*, 6(1), p. 33467.

Wiesner, S. (1983). Conjugate coding. *SIGACT News*, 15(1), p. 78–88.

Xavier, G., Silva, T., de Faria, G., Temporão, G. and von der Weid, J. P. (2009). Practical random number generation protocol for entanglement-based quantum key distribution.

Quantum information & computation, 9, pp. 683–692.

Yin, J., Cao, Y., Li, Y.-H., Liao, S.-K., Zhang, L., Ren, J.-G., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H. et al. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343), pp. 1140–1144.

Yu, L. (2018). A quantum homomorphic encryption scheme for polynomial-sized circuits. *ArXiv*, abs/1810.01166.

Yu, L., Perez-Delgado, C. A. and Fitzsimons, J. F. (2014). Limitations on information-theoretically-secure quantum homomorphic encryption. *Physical Review A*, 90(5).

Zawadzki, P. (2018). Quantum identity authentication without entanglement. *Quantum Information Processing*, 18(1), p. 7.