Quantum Key Distribution Protocols and Applications

Sheila Cobourne

Technical Report
RHUL–MA–2011–05
8th March 2011

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

Title: Quantum Key Distribution – Protocols and Applications

Name: Sheila Cobourne

Student Number: 100627811

Supervisor: Carlos Cid

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature:

Date:

Acknowledgements

I would like to thank Carlos Cid for his helpful suggestions and guidance during this project. Also, I would like to express my appreciation to the lecturers at Royal Holloway who have increased my understanding of Information Security immensely over the course of the MSc, without which this project would not have been possible.

Contents

Table of Figures

Executive Summary

Quantum Cryptography uses the laws of Quantum Mechanics to create new cryptographic primitives. Most of these primitives are still theoretical, as they rely on quantum computer processing techniques which are not possible with today's technology. However, one primitive -Quantum Key Distribution (QKD) - is achievable today, and can provide unconditionally secure communications. Despite this, QKD has met with mixed reactions within the cryptographic community, and has not yet been widely adopted.

This paper considers the reasons for this: relevant QKD protocols are described, and their strengths and weaknesses are examined to see where the competing claims for its security and applicability arise. This is followed by a brief overview of practical QKD research work: the EU-funded SECOQC quantum network project, and low-cost free space QKD technology. This then enables the commercial potential of QKD systems to be explored.

The conclusion from this study is somewhat mixed. There is a basic problem facing QKD: there are tried and tested "classical" solutions in all the application areas where it could be used. An extensive infrastructure is needed to support QKD implementations, so any security enhancements from QKD systems may be prohibitively expensive. But there are areas where it could provide a real benefit by addressing weaknesses in classical applications.

Commercial success will depend on the *perceived* benefits of installing security "based on the laws of physics alone", rather than security levels per se, and on how acceptable the general public and business find the technology. There will be a place for QKD in the cryptographers' toolbox, but it may only be a small niche with very specific application requirements.

Chapter 1 Introduction

1.1 Background

Quantum Cryptography is a relatively recent arrival in the Information Security world. It harnesses the laws of Quantum Mechanics to create new cryptographic primitives that offer features either not achievable with 'classical' methods, or which improve on existing techniques. New quantum primitives include quantum coin tossing [BB84] [GB09], quantum money [MM09] [SA09], quantum copy protection [SA09], quantum private channels [MM08], blind quantum computation [AB09] and quantum public key encryption [TK07]. Currently these are theoretical only: they have a pre-requirement for a fully functioning quantum computer to allow their implementation, and quantum computing is still in its infancy. Once the relevant technological hurdles have been jumped and quantum computing enters the mainstream, these primitives can be used to build security services. As quantum computing will also have a radical effect on the usability of some of the algorithms employed today, it is a worthwhile theoretical area to study.

There is, however, one quantum cryptographic primitive which is achievable with today's technology – Quantum Key Distribution (QKD) – which is the focus of this report. At first glance, it would appear to be the Holy Grail of cryptography: in the words of Peev et al [MP08], Quantum Key Distribution

> *"holds the potential of absolutely secure communication that cannot be compromised by any eavesdropping technique"*

By using the quantum properties of light, current lasers, fibre-optics and free-space transmission technology can be used for QKD, so that many observers claim security can be based on the laws of quantum physics only (for example, [SQ10], [IQ10a]). Practical commercial QKD implementations have been implemented, such as the SECOQC network [RA07a] and the DARPA quantum network [CE06].

As Stebila et al [DS09] point out, QKD is a tool which can be used in systems to gain new security properties. It doesn't lessen the need for other cryptographic primitives such as authentication in system-wide security: QKD is simply another weapon in the cryptographer's arsenal, albeit a potentially powerful one.

But QKD has also been the subject of some fairly extravagant claims, notably in the SECOQC Business White Paper [SGH08]: it will (apparently)

- *"change the actual network security paradigm"*
- *give "a real competitive advantage"*
- *"prevent several types of existing attacks. The stability of the laws of physics gives* ***highest guarantees*** *to obviate all dangers related to technology evolution"*
- *"satisfy legal compliance to protect informational assets in the best way"*

On the other hand, some analysts have not supported an all-systems-go approach [KP09] [BS08a], as QKD will have to fit into existing systems which are currently secure enough. Strengthening one part of a system does not necessarily improve overall security – as Bruce Schneier remarks, "technology causes security imbalances" because technological advances can make certain attacks easier, or enable better defences [BS08b]. Bruce Schneier has also famously given an interview entitled "Quantum Cryptography: As Awesome as It Is Pointless" [BS08a], so there is crystal clarity where he stands on the issue!

1.2 Objective of the Report

This study aims to examine these competing views, and to investigate why the idea of quantum key distribution gives rise to such diametrically opposed opinions. On the one hand, QKD will provide the ultimate in security; on the other it's practically useless in today's cryptographic environment. Security issues and commercial applications are the two areas which will decide where QKD lies on this wide security spectrum, and this report will investigate both. But before this can be done, the theoretical background to QKD protocols needs to be explained, followed by descriptions of practical and potential implementations.

1.3 Structure of the Report

The above objectives will be achieved through the following report structure:

- In Chapter 2 a brief introduction to some security concepts necessary for the understanding of the topics covered in the body of the work will pave the way for an exposition of the quantum phenomena which underlie the security of QKD in Chapter 3.
- The most common QKD protocols and their security issues are dealt with in Chapter 4. The emphasis here is on the earliest and most widely known protocol, “BB84”, as it is the most commonly used in practical implementations.
- Chapter 5 is the crux of the report: it examines the strengths and weaknesses of the various protocols, and the resulting competing claims for and against QKD
- A technical discussion of quantum networks and a practical realisation of a QKD network (the SECOQC network) follow in Chapter 6 and Chapter 7.
- An interesting area of research, low cost free space quantum optics, is detailed in Chapter 8. This technology could provide a particularly user-friendly method of using QKD and if a suitable infrastructure is in place could have much commercial potential.
- Once all theoretical and technical matters have been covered, potential commercial applications are suggested in Chapter 9. A comparison with their so-called “classical” equivalents and identification of any specific QKD benefits lead into an assessment of QKD’s future commercial success.
- All the issues covered are drawn together in a final conclusion in Chapter 10

Chapter 2 Some Security Concepts

2.1 Cryptographic Theory and Practice

Quantum theory has some interesting properties which can be harnessed in developing cryptographic systems: however, before launching into the wonders of the quantum world, it is necessary to take a brief detour via some cryptographic theory and practice which underpins many of the areas to be addressed in this report. This standard cryptographic theory can be found in many texts: for example, Menezes, van Oorschot and Vanstone's work [AM01] covers these topics in some detail.

The quantum journey will commence in Chapter 3.

2.2 Symmetric and Asymmetric Cryptographic Keys

Cryptography comes in two distinct "flavours", to be used when there are different trust models in the cryptosystem, and their associated cryptographic keys are treated very differently.

2.2.1 Symmetric Cryptography

This is used where the two communicating parties (usually referred to as Alice and Bob) share a key before any encryption and decryption is done. Alice and Bob have to trust each other to keep the key secret. The decryption key can be easily calculated from the encryption key, or may be identical. Quantum key distribution deals with symmetric keys shared between Alice and Bob.

2.2.2 Asymmetric or "Public Key" Cryptography

Here, different keys are used for encryption and decryption, chosen so that it is extremely difficult for the decryption key to be derived from the encryption key. This allows encryption keys to be publicly available (hence the name) so that anyone can encrypt a message for the recipient, without having to share a key first. The parties involved do not need to trust one another at all. Only the genuine recipient is in possession of the secret decryption key, so only they can extract the plaintext from the ciphertext.

2.3 Types of Security

There are two types of cryptographic security which will be relevant in this report: computational security and information-theoretic security (also termed unconditional or perfect security).

2.3.1 Computational Security

This describes a crypto-system which is theoretically breakable (by trying every possible key – the brute-force attack) but the computational effort required to do so is so time consuming and expensive that it is not economically viable for an attacker to consider (i.e. *computationally infeasible*).

2.3.2 Information-theoretic Security

This describes cases when, even if an attacker has infinite resources at their disposal, the crypto-system simply cannot be broken. This is clearly much stronger than computational security, but is not necessarily practically achievable. The founding father of Information Theory, Claude Shannon [CS49], proved that unconditional security was possible if the secret key was the same length as the plaintext message to be encrypted. Information Theory has various uses in cryptography: it can be used to prove the unconditional security of systems, determine the achievability of unconditional security within upper and lower bounds, or reduce the task of breaking a crypto-system down to the equivalence of breaking one of its underlying cryptographic primitives (e.g. a one-way function), which may be an altogether easier task. (Maurer [UM99] gives examples of Information-theoretic security in cryptography).

2.4 The One Time Pad and the Vernam Cipher

In his proof, Shannon used a special case of symmetric encryption to provide unconditional security: the One Time Pad (OTP), invented in 1926 by Vernam and Mauborgne [GV26].

There are fundamental requirements for using the OTP:

- The key is random and non-repeating
- The key is as long as the message
- The key is used only once and then discarded – never reused

If these conditions are met, then a simple encryption operation (such as a logical XOR) will produce unbreakable ciphertext. Even if an attacker has infinite computing power, they will not be able to derive any information from an intercepted ciphertext.

However appealing they sound in theory, OTPs have immense practical difficulties: generating long, truly random keys is problematic, distributing the keys to recipients is a logistical nightmare, sender and receiver have to be totally synchronized to make sure that the same keys are used for the same message, and ensuring keys are never reused is a challenging task. For this reason, OTPs are currently seldom used in practice, but in later sections of this report, it will be shown that they become a much more attractive prospect when used in conjunction with QKD protocols.

2.5 Kerckhoff's Principle

Cryptosystems are designed to cope with the worst case scenario: a malefactor has infinite computing resources, can gain access to plaintext/ciphertext pairs (and thus could study the relationship between each pair) and knows the encryption and decryption algorithms, so can choose plaintext or ciphertext values at will. The only element not accessible to this adversary is the secret key, and thus the security of a cryptosystem depends solely on the security of the key. This is a long-standing design philosophy first enunciated by Auguste Kerckhoff in 1883: Kerckhoff's Principle [AK83a, AK83b] states:

> *"The security of a cryptosystem must not depend on keeping secret the crypto-algorithm. The security depends only on keeping secret the key"*

This is sometimes referred to as Shannon's Maxim – 'the enemy knows the system'. It follows, therefore, that keeping key material away from adversaries is a fundamental requirement of any cryptosystem, be it classical or quantum.

2.6 Key Establishment Protocols

The success of cryptographic processing is ultimately dependent on the quality and security of the key material used. This raises the question: where does this key come from? The answer to this lies in some tried and tested key establishment protocols, which are described extensively in standard cryptography texts [AM01 Ch. 12 for example]. The objective of a key establishment protocol is to provide the communicating parties with a shared secret, and this can be done in one of two ways. In the first method, one party generates a key which is securely delivered to the other party via a ***key transport*** protocol. The second method results in a shared secret derived from information passed openly between the two parties, in such a way that no-one (especially an attacker) can guess the resulting value from the information sent. This is a ***key agreement*** protocol.

There are a number of these protocols in existence, but the most widely known is the Diffie Hellman key agreement scheme. This (and others) is described in detail in Appendix 1 . Technically, QKD is actually a key establishment protocol, but as all the reference literature refers to it as a key distribution method, that terminology is retained in this report for consistency.

2.7 Key Distribution

Key establishment protocols work very effectively: indeed, cryptography itself would probably vanish without trace if keys could not be produced successfully. However, there is another problem regarding keys which isn't so well handled – the so-called "quadratic curse". When a symmetric cryptosystem is in place for a network of users, every pair of users who wish to communicate securely will need to pre-share a distinct key. So theoretically, each party in a network of N users will need to hold (N-1) secret keys: the total number of keys in the system is N(N-1)/2 i.e. proportional to N^2. As the number of users on the network gets bigger, this quickly becomes an unworkably large number of keys to deal with effectively. Protocols and network architectures therefore have to be designed to minimize the number of keys wherever possible. [AM01 Ch. 13]

2.8 Where Does Quantum Key Distribution Fit In?

Quantum key distribution is a key establishment protocol which creates symmetric key material by using quantum properties of light to transfer information from Alice to Bob in a manner which, through the incontrovertible results of quantum mechanics, will highlight any eavesdropping by an adversary. This can be used to derive a key, and the resultant key material can then be used to encrypt plaintext using a one time pad encryption via a Vernam Cipher to provide unconditional security, safe in the knowledge that the key is secret. The N^2 key distribution problem is not easily solved by QKD per se, but a network architecture which addresses this is described later (in Chapter 7).

With these security considerations in mind, an exploration of the quantum phenomena supporting QKD protocols follows. Security based on "the laws of physics alone" becomes a reality.

Chapter 3 The Quantum World

3.1 Quantum Theory Historical Background

Quantum Theory was developed at the beginning of the 20th century, when it was becoming apparent that classical (Newtonian) physics could not explain some puzzling experimental results. In particular, experimental studies of black body radiation –a black body is an object which absorbs all the radiation it is exposed to and then re-emits it – had shown that the emitted radiation depended only on the temperature of the black body, but classical calculations predicted that an infinite amount of radiation at very high frequencies should be observed, irrespective of temperature. This was known as the 'ultra-violet catastrophe', and led a Professor of Physics at Berlin University, Max Planck, to propose the existence of 'quanta' (singular: quantum) on 14th December 1900 at a meeting of the German Physical Society in Berlin [RH99] [MP01].

A quantum is a discrete packet of energy that can be absorbed or emitted; i.e. only certain energy values are permitted as opposed to a continuous range. Marcus Chown [MC04] describes a quantum as "a fundamental chunk" of energy. Bernstein likens quanta to beer being served in multiples of pints only! [JB09 Ch 5] The concept of quanta was then used to explain, amongst others, the photoelectric effect [AE05] and the structure of the atom [NB13], before leading Erwin Schrodinger [ES26] and Paul Dirac [PD28] to lay the foundations of Quantum Mechanics as we know it today.

3.2 Quantum Properties

The quantum world is bizarre, to say the least: even the world famous physicist Richard Feynmann has been quoted as saying "I think I can safely say that no one understands quantum mechanics" [JP02]. The strange properties of quantum superposition and quantum entanglement have direct consequences for the field of cryptography and will now be discussed.

3.2.1 Quantum Superposition

A quantum is described by a probabilistic wave function (the Schrodinger equation) which gives the *likelihood* of finding the quantum at any particular position, but not its *actual* position. A quantum can have many possible states, but it exists in all of them simultaneously in the absence of an observer: this is quantum superposition. Once an observer measures the quantum, the wave function collapses (or as Bernstein puts it, the wave function is "decapitated" [JB09]) and one of the previously superposed states is chosen according to the probability inherent in the wave function. This counter-intuitive property is usually illustrated by the "Schrodinger's Cat" thought experiment shown in Figure 1 and described in detail by Singh [SS99].

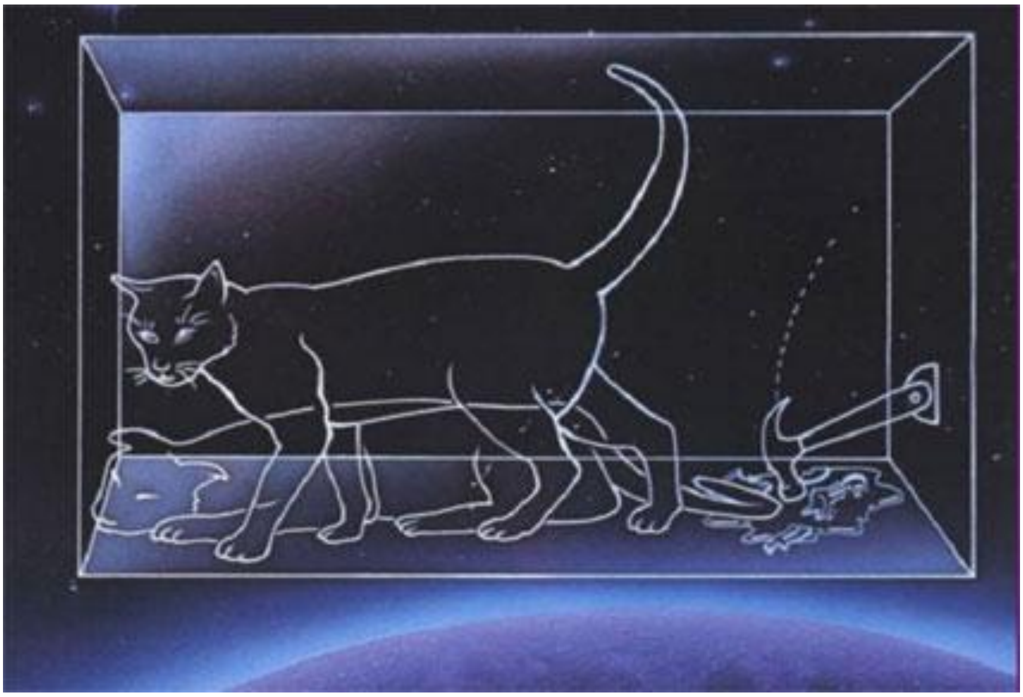


FIGURE 1 SCHRODINGER'S CAT THOUGHT EXPERIMENT

SOURCE [NI05]

A (quantum!) cat is locked in a box with a phial of cyanide which can be broken by some random mechanism – maybe a particle emitted from a radioactive source sets off a trigger – which will have predictably appalling consequences for the unfortunate feline if it is activated. There is no way of telling whether the cyanide has been released until the box is opened. A classical interpretation of this (thankfully hypothetical) experiment is that the cat is alive OR dead in the box irrespective of when it is opened. However, the quantum interpretation is that the cat is both alive AND dead at the same time, and it is only the act of opening the box (i.e. measurement) which collapses the cat wave function into one or other of its possible states.

So, it is the very act of observation that destroys the wave function and determines the final state of the system. [MK06, Ch 6]

3.2.2 Heisenberg's Uncertainty Principle

There is a further complication to quantum observations: when you measure the position of a quantum, be it a photon, electron or whatever, you *cannot* know its velocity exactly, and vice versa: measure the velocity, and the position is unclear. (Strictly speaking, it is the momentum which is the property under consideration here.) This is the Heisenberg Uncertainty Principle, and according to Chown [MC07] and Feynmann [RF95] the uncertainty principle exists to *protect* quantum theory. Too accurate measurements would destroy the wave-like properties of quanta, and instantly quantum interference and superposition would disappear. The Uncertainty Principle is not confined to position and momentum: it affects any conjugate pair of states. These are states where measurements are not commutative, so measuring A then B does not give the same answer as measuring B then A. Polkinghorne [JP02] states "observables come in pairs that epistemologically exclude each other", and this "demi-knowledge is a quantum characteristic". The Uncertainty Principle is therefore the basis of many effects of the quantum world.
A very clear explanation and animation of this principle can be found at [AT07].

3.2.3 Quantum Entanglement

A weird quantum property of relevance to QKD is that of quantum entanglement, a phenomenon that Einstein disliked intensely, and referred to dismissively as "spooky action at a distance" [AE47]. Pairs of quanta can be produced which behave as if they are a single entity, so called EPR pairs following the work of Einstein, Podolsky and Rosen on the phenomenon. [AE35]. For example, quanta possess a property called "spin": one quantum could have spin up, one spin down, so that the total spin is zero but until a measurement is made it is not clear which is which of the pair. If the pair is separated, measuring one causes the other's wave function to collapse into the opposite state. It appears to know instantaneously that its partner has been measured, apparently contradicting Einstein's finding that nothing can travel faster than light. This is known as the EPR paradox, which wasn't resolved until 1965 by John Bell [JB64] [JB09]. It has been speculated that this strange quantum behaviour could be used in Star-Trek style teleportation, but with the slightly unfortunate side effect that the original object is destroyed! [MK08] It is the *information* which travels faster than light, not the quantum itself.

3.2.4 Bell's Theorem

[JP02] [AT07] [RP05] Bell investigated the properties of an entangled system in the case of 'strict locality' i.e. what happens to one particle depends only on events at its location and a different particle should only be affected by events at its (different) location. He showed that in this case, there are measurable effects which quantum physics showed would be violated when certain conditions were met. These are called Bell's inequalities, and experimental results demonstrated that 'strict locality' was not correct and quantum entanglements hold even when the two component particles are separated physically.

3.3 Quantum Computers

Quantum superposition is the basis which underlies the processing capabilities of a quantum computer. Information is stored in quantum bits (qubits) rather than the classical binary digits (bits). A bit has two values, 0 or 1, i.e. on or off, one or the other: a qubit can use the superposition of all available states to store information, allowing a quantum computer to operate on all possible values at once, speeding up calculations and employing different kinds of algorithm not feasible on classical computers.

Quantum computers were first envisaged by Paul Benioff in 1980 [PB80a], [PB80b]: this work was developed further by Richard Feynmann [RF82] and in 1985 David Deutsch proposed a universal quantum computer design [DD85]. In addition to their prodigious processing power, quantum computers, by their very nature, are not subject to the restrictions of Moore's Law [GM65]. This states that the number of components that can be fitted on to a semiconductor chip doubles every 18 months: eventually, the components will become so small that it is physically impossible to fit any more onto a chip and the recent explosive growth in computing power will come to an abrupt halt.
Quantum computing, if it ever becomes a practical reality, will be a new way forward.

Quantum computers are particularly efficient at finding hidden cyclic subgroups in key spaces, using Shor's algorithm [PS97] and this significantly reduces the time taken to factor large numbers, for example. The enhanced parallel processing potential and the ability to use "quantum methods" will reduce the time needed to solve the hard mathematical problems underlying the security of RSA, ElGamal algorithms, and their equivalent Elliptic Curve versions. Asymmetric cryptography as we know it now will be no more, and different asymmetric schemes will have to be devised. Symmetric cryptography will need to use keys which are twice as long as now, to achieve the same level of security (thanks to a "square root speed-up" algorithm for quantum computers devised by Grover [LG97]). Quantum computers therefore force cryptography into a new age.

3.4 Quantum Decoherence

Inevitably, quanta interact with their environment, and in the process their "quantumness" is eroded through the collapse of their wave functions, so they become classical objects not subject to quantum laws any more - the microscopic becomes macroscopic. This is known as quantum decoherence, and whilst quantum physicists may debate the implications and the mechanisms of this phenomenon, it is the reason why strange quantum effects are not seen in everyday life. Minimising decoherence is one of the major technical challenges in the development of quantum computers. For a clear description of decoherence, see [AT07].

3.5 Quantum Channels

Quantum states can be used to transmit information between two authorised parties, conventionally named Alice and Bob. Theoretically, it will make no difference whether atoms, ions, molecules, electrons or any other quantized particles are involved in the exchange. From a practical perspective, however, it is the quantum of light – the photon – which is the preferred option, because photon quantum states can be transmitted over longer distances without decoherence than the other quantum candidates. There are losses due to scattering, but provided they are accounted for and dealt with effectively they do not affect the overall security of a QKD protocol. Any medium which allows light to propagate will henceforth be referred to as a 'quantum channel'. (Examples are line-of-sight free space or optical fibres.) [VS09a]. The channel itself is not quantum, it merely carries quantum information.

3.6 Photon Polarisation

[SV02] Electromagnetic waves such as light have an electric field associated with them, which vibrates as the wave travels. The direction of this vibration is known as polarisation, and polarised photons can be created by passing a normal beam of light (which contains photons of many differing polarisations) through a filter set for a specific angle of polarisation. Light impinging on a filter will either go through and emerge polarised to the angle of the filter regardless of its original polarisation, or will be blocked. The probability of each result depends on the difference between the polarisation angles of the filter and the incoming photon. For example, if vertically polarised photons are sent through a filter set at an angle θ to the vertical, the probability of passing through the filter decreases as θ increases: when θ is 90°, i.e. when the second filter is horizontal, the photon will not pass through. When θ is 45°, this probability is precisely one half, so the output from the second filter in this case is exactly the same as it would have been had a randomly polarised stream of photons been passed through it – it has been *randomized.*

Orthogonal (i.e. perpendicular, such as vertical/horizontal) polarisation states are referred to as a polarisation *basis (plural: bases)*. Two bases are conjugate if the measurement of the polarisation of one randomizes the other, and thus are subject to the Heisenberg Uncertainty Principle –measuring one affects the value of the other, so you cannot know both values simultaneously. So, for example, filters set at 0° and 90° form one basis, and its conjugate basis has filters set at 45° and 135°. See Figure 2 for an illustration. Photons passing through the first will emerge with vertical or horizontal polarisation, which will then be changed to diagonal polarisation once they have been filtered by the conjugate basis, but 45° or 135° polarisations will occur with random probability of ½.

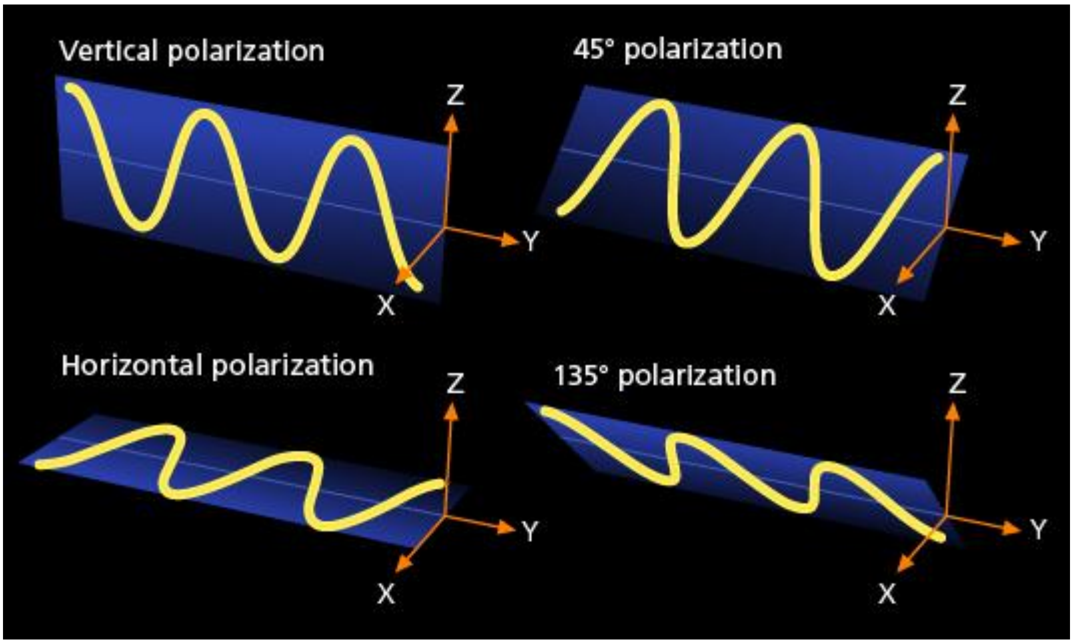


FIGURE 2 CONJUGATE PHOTON POLARISATION DIRECTIONS

SOURCE [NI10]

3.7 Quantum No-Cloning

As its name implies, the Quantum No-Cloning Theorem specifically prevents copies of an unknown quantum state from being created, and was first identified by Wooters, Zurek and Dieks [WW82]. It is another ‘protection’ mechanism for quantum theory, in that copying unknown quantum states would enable an observer to measure the copies exactly, and avoid the restrictions of Heisenberg’s Uncertainty Principle. So, backup copies of quantum states cannot be taken and used in quantum computing error correction routines, and an eavesdropper cannot create copies of quantum information sent along a quantum channel. It also means that a quantum signal cannot be amplified along a quantum channel.

3.8 Quantum Theory and Quantum Key Distribution

Quantum key distribution uses basic quantum properties to detect eavesdroppers in one of two ways: either by relying on the Heisenberg Uncertainty Principle or by the violation of Bell’s Inequalities in entanglement based schemes.

Heisenberg - based protocols use the fact that measuring a quantum state changes it: the eavesdropper will introduce errors into the information transfer along a quantum channel which should always be detected by the protocol.

Entanglement - based protocols do not have any information to eavesdrop! Information only springs into existence when the entangled quanta are measured: the eavesdropper’s only potential ploy is to attempt to inject extra quanta into the protocol. The extra quanta violate Bell’s inequalities, and so the eavesdropper will also be detected in this case.

Quantum no-cloning further ties the eavesdropper’s hands, as no copies of quanta can be taken for processing later.

Life looks bleak indeed for the quantum eavesdropping community!

Chapter 4 Quantum Key Distribution Protocols

4.1 General methodology for QKD

So, quantum mechanical effects can be used to transfer information from Alice to Bob, and any attempted eavesdropping by Eve will always be detectable. But how can this be turned into a working cryptographic key distribution protocol? A combination of quantum processing and well established classical procedures is needed. Three distinct phases are needed: raw key exchange, key sifting and key distillation, with the option to discard the secret key at any of the stages if it is deemed that not enough security could be obtained from it. A clear description of these phases can be found on the swissquantum website [SW10], and is illustrated in Figure 3, where the stages shown with double lines indicate classical authentication is needed.

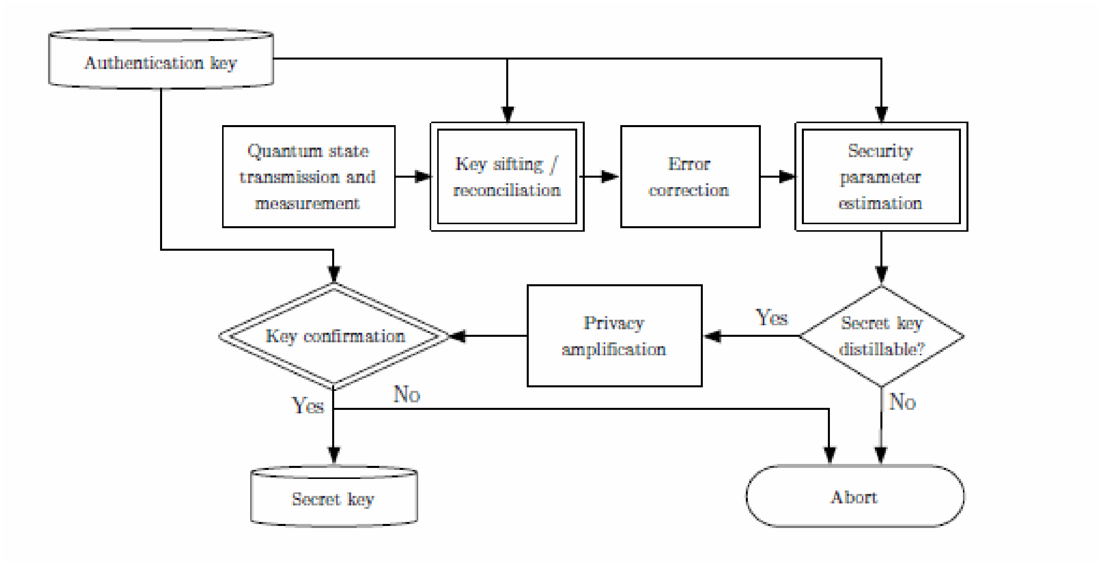


FIGURE 3 FLOWCHART OF QKD PROTOCOL

SOURCE [DS09]

4.1.1 Raw Key Exchange

This is the only quantum part of Quantum Key Distribution! Alice and Bob exchange ‘some quantum states’ [DS09] – it actually doesn’t matter what type of quantum state or technology is used – so quantum information is passed along a quantum channel from Alice to be measured by Bob, with or without the presence of Eve, the eavesdropper.

In all subsequent exchanges in a protocol, only a secure classical channel will be used. This is known as ‘classical post-processing’.

4.1.2 Key Sifting

Alice and Bob decide (classically) between them which of the measurements will be used for the secret key. The decision making rules depend on which protocol is being used, and some measurements will be discarded e.g. if the settings used by Alice and Bob did not match.

4.1.3 Key Distillation

The need for further processing after the key sifting stage was determined by Bennett et al [CB92a] when reviewing experimental results (practical channels are lossy, and the protocol needs to be workable even in the presence of transmission errors) and in previous work [CB88] on how the use of an authenticated public channel could repair the information losses from an imperfect private channel. Thus **error correction** and **privacy amplification** are required, which are the first two steps in the key distillation phase of the classical post-processing of the remaining secret key bits. The third (and arguably most important!) final process is authentication, which counteracts man-in-the-middle attacks (MITM).

- ***Error Correction***

  A classical error-correction protocol estimates the actual error rate of the transmission, known as the Quantum Bit Error Rate (QBER). Errors occur either through noise on the quantum channel, or the presence of an eavesdropper, but for security reasons, it is assumed that *all* errors are due to eavesdropping. If the QBER is less than a pre-determined maximum value, then the secret key is passed on to the next step of key distillation. If the QBER is greater than this value, then the conclusion is drawn that the amount of information lost to an eavesdropper is too great to guarantee the secrecy of the key material, and so the secret key is discarded and a new round of QKD is initiated.

- ***Privacy Amplification***

  This is designed to counteract any knowledge Eve may have acquired on the raw key. Privacy amplification compresses the key material by an appropriate factor, determined by the previously calculated QBER: a high QBER needs more compression, as the purpose is to remove at least the same number of key bits that Eve may have gleaned information about. There are provable privacy amplification processes, based on two-universal hash functions [JC79] [MW81] so the key material is still unconditionally secure. (The output from error correction and privacy amplification is a known fraction of the original secret key, a 'gain'. Gain equations depend on the QBER and the efficiency of Alice and Bob's quantum creation and detection equipment, so can be used to test the security of different QKD implementations, as in the work of Lutkenhaus [NL00])

- ***Authentication***

  As stated previously, probably the most important stage of the whole QKD protocol is this final one: strong classical authentication to ensure that Alice and Bob are not the subjects of a man-in-the-middle (MITM) attack. An adversary poses as Bob to Alice, and Alice to Bob: all traffic between Alice and Bob is therefore redirected through a third party, without them knowing. Unfortunately, quantum processing itself is powerless against such an attack.

  However, QKD does have a property which can be used to strengthen classical authentication procedures. A secret key has to be pre-shared between Alice and Bob, for use in authentication of the very first quantum exchange. But if subsequent sessions use part of the key generated in the previous QKD session to replace the new session's authentication key, then

  > "*if authentication is unbroken during the first round of QKD, even if it is only **computationally secure**, subsequent rounds of QKD will be information-theoretically secure"* [DS09]

  So this means that the initial authentication can be extended to cover all future sessions – with *increased* security levels.

4.1.4 Useable Key Size

As the various stages of a QKD protocol progress, the length of useable key material is reduced. (Figure 4) If, however, there are no errors or eavesdropping, then the raw key and the secret key are identical.

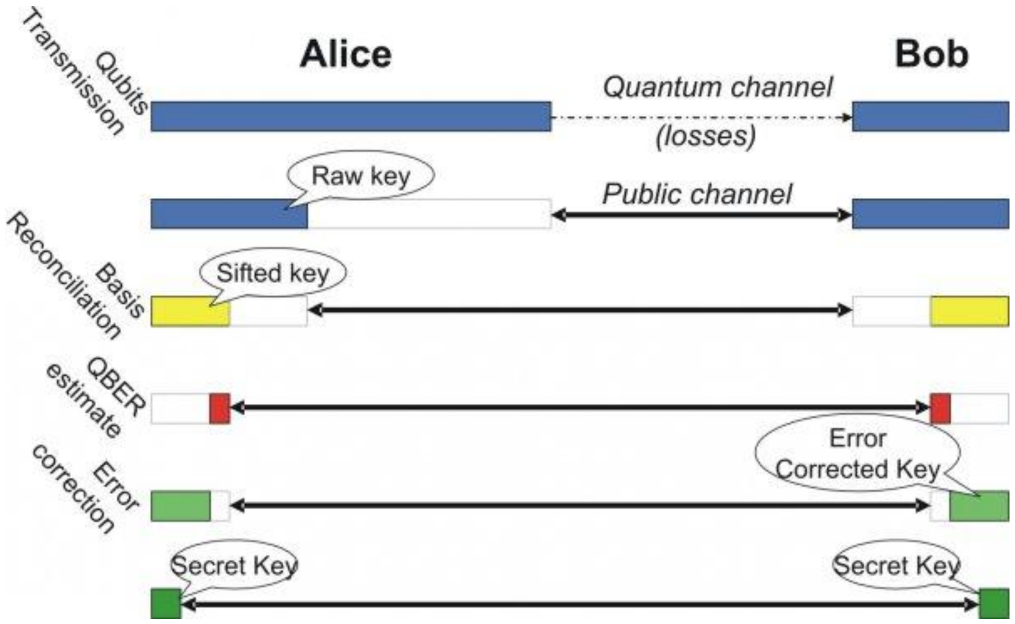


FIGURE 4 REDUCTION IN KEY SIZE AFTER EACH QKD STAGE

SOURCE [SW10A]

QKD is inherently inefficient in its use of generated key material, as many bits are discarded by the end of a protocol run.

4.2 Quantum Security

As explained in Section 3.2.2, measurement of quantum states modifies the quantum system. Eve cannot, therefore, obtain any information about a quantum transmission without being detected. This is true even if Eve had infinite computational resources and time – or even a quantum computer. The laws of physics prevent it. This is cryptographic Nirvana: unconditional security, immune from undetected eavesdropping. Unfortunately, 'unconditional' is a slight misnomer, as there *are* some conditions which need to be met for this to be the case. [VS09a]

- Eve cannot inspect Alice's and Bob's devices to see or affect their creation or detection of photons
- The random number generator Alice and Bob use to set their equipment must be truly random and trusted implicitly
- Classical authentication is done with unconditionally secure Carter Wegman protocols [JC79, MW81]
- Eve must obey the laws of physics!

With these prerequisites in place, specific QKD protocols will now be examined, and relevant security proofs will be identified but not described in detail.

4.3 The BB84 Protocol

The first Quantum Key Distribution protocol was proposed by Bennett and Brassard in 1984 [CB84], and has been described in detail in many works, e.g. Singh [SS99], Vittorio [SV02]. Swissquantum [SW10]).Proofs have been developed showing that its security is unconditional (e.g. Biham et al.[EB06], Mayers [DM98], Shor and Preskill [PS00]).

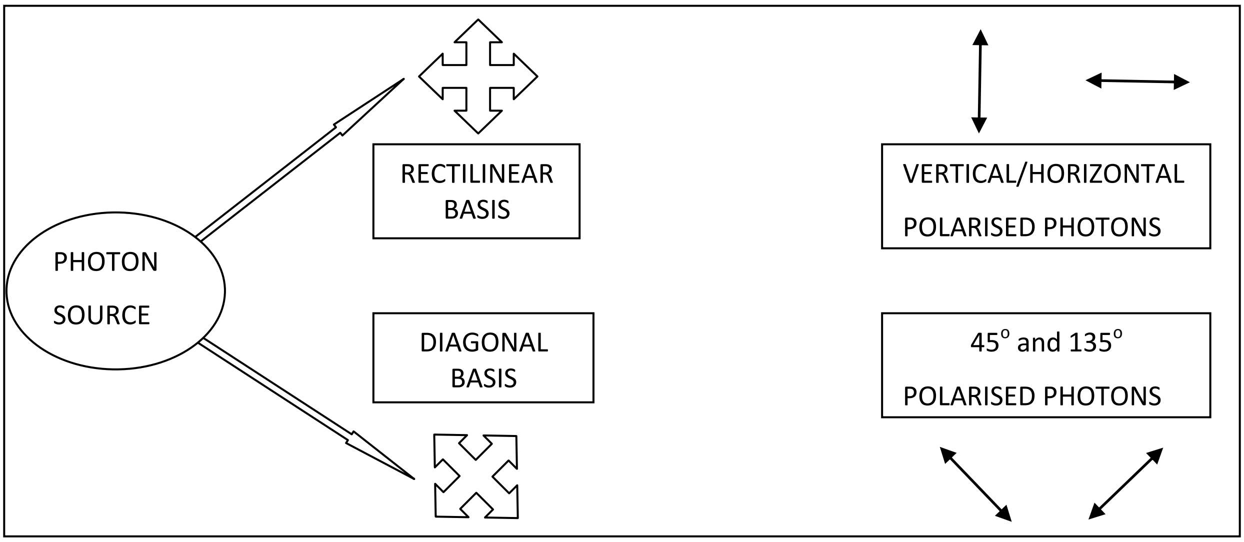

PHOTON
SOURCE
RECTILINEAR BASIS
DIAGONAL BASIS
VERTICAL/HORIZONTAL POLARISED PHOTONS
45° and 135° POLARISED PHOTONS

FIGURE 5 RECTILINEAR AND DIAGONAL POLARISATION BASES

Raw key exchange and key sifting are done as follows:

- Photons are polarised using conjugate bases, either a rectilinear basis (vertical/horizontal polarisations) or a diagonal basis (45^o and 135^o polarisations) as shown in Figure 5.
- These polarised photons can be used to send information if each polarisation generated by a basis is allocated the value '0' or'1' (i.e. one photon can carry one quantum bit (qubit) of information), and these encodings are agreed between Alice and Bob before they attempt to exchange quantum states.
- Alice can produce photons with 4 different polarisations, and (using a trusted random number generator) she chooses the basis for each photon at random and sends a stream of randomly polarised photons to Bob for measurement. This style of protocol is thus termed ***Prepare and Measure (P & M).***

- Bob now has to detect and measure these polarisations. He passes them through filters –potentially changing their original polarisations - and records the results with a photon counter. As Bob does not know which basis Alice has used for each photon, he can only set his receiving bases randomly too. If he chooses correctly, the polarisation is recorded accurately; if he chooses wrongly, then the result is a random polarisation matching his (not Alice's) choice of basis, with all information about the initial photon polarisation lost. This is the *Raw Key Exchange* stage. Figure 6 shows an example of photon sending and receiving in a raw key exchange process.

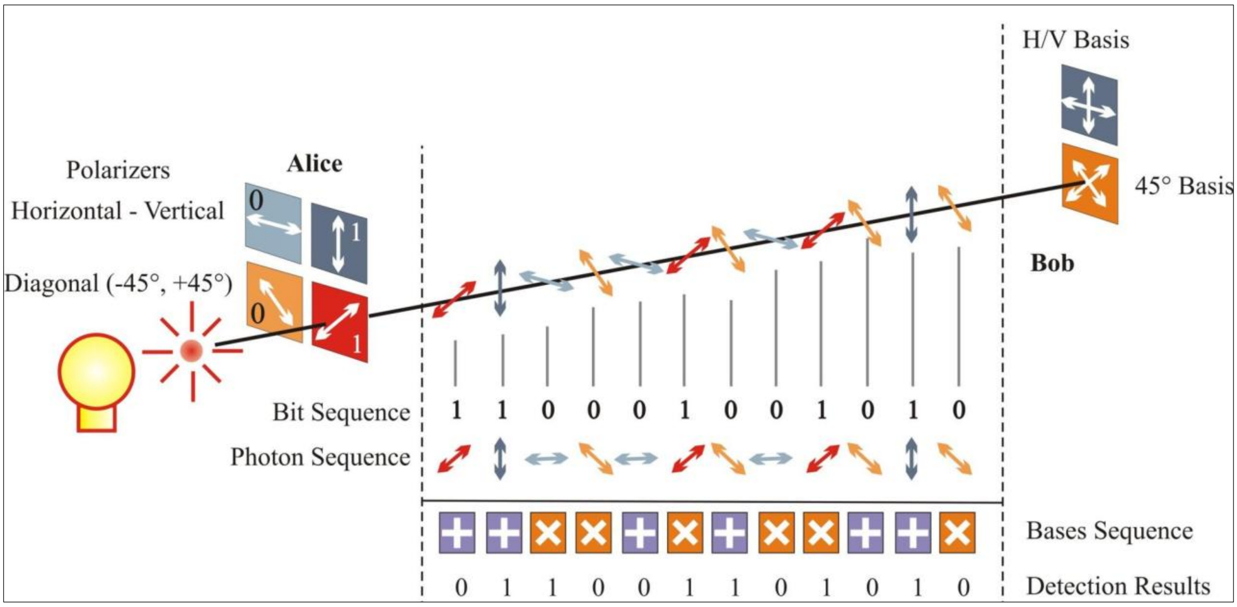
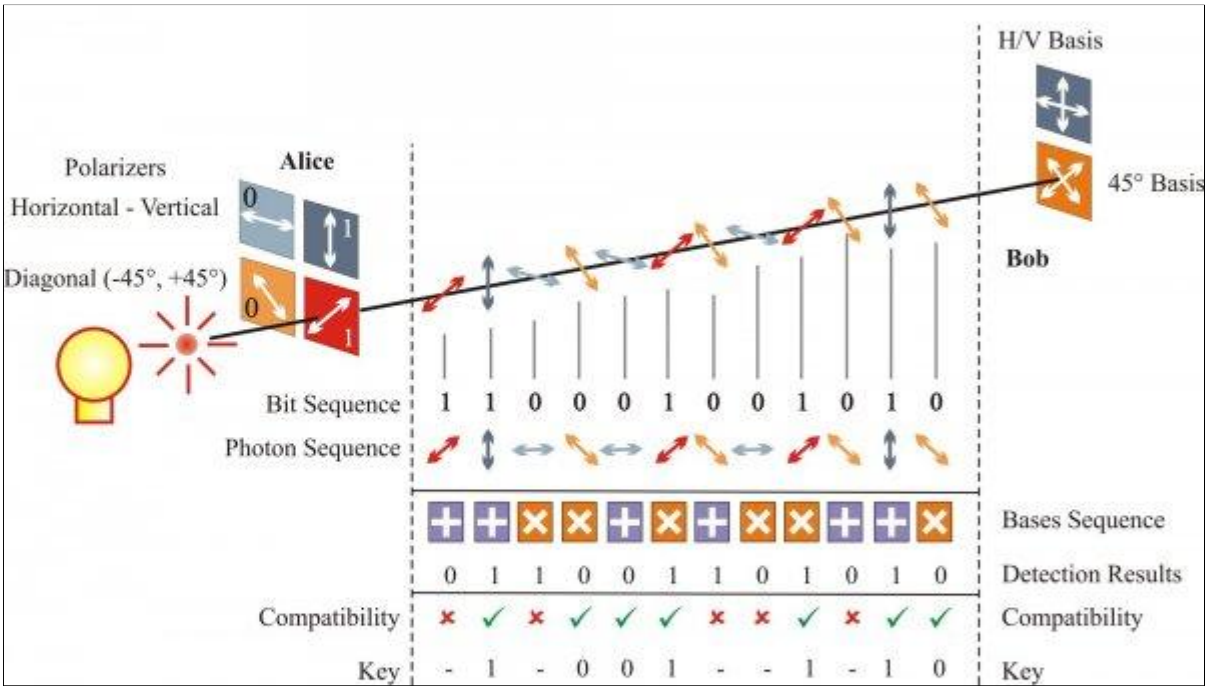


FIGURE 6 ALICE AND BOB USING BB84 PROTOCOL FOR RAW KEY EXCHANGE

SOURCE [SW10B]

- The *Key Sifting* stage is done over a public classical channel, where Alice and Bob each broadcast their choice of basis for each photon. As it is only the basis which is being publicly discussed, no key information can be gained by an eavesdropper at this point. The bases are compared, and any photon which had been processed using non-matching bases is dropped from the raw key material. The sifting process should, on average, leave half of the exchanged qubits still available for use in the final secret key. (See Figure 7)



Bit Sequence	1	1	0	0	0	1	0	0	1	0	1	0
Bases Sequence	+	+	×	×	+	×	+	×	×	+	+	×
Detection Results	0	1	1	0	0	1	1	0	1	0	1	0
Compatibility	×	✓	×	✓	✓	✓	×	×	✓	×	✓	✓
Key	-	1	-	0	0	1	-	-	1	-	1	0

FIGURE 7 BB84 PROTOCOL AFTER KEY SIFTING

[SOURCE SW10C]

4.3.2 Raw Key Exchange in the Presence of Eavesdroppers

Now consider the same set up, but this time when there is an eavesdropper, Eve, who wishes to mount an intercept/resend attack.

As before, Alice chooses her bases randomly, and fires off a stream of randomly polarised photons. Eve intercepts these, but she is in exactly the same position as Bob was previously: she does not know what basis Alice used to generate the polarisations, so her only possible tactic is to set her intercepting bases randomly too. So, like Bob previously, she will have her bases correctly set only half the time, and the incorrect settings will result in random polarisation readings and the destruction of the original polarisation. As a consequence, when she then resends the photons she has intercepted, 50% of them will be wrong.

Bob sets his bases randomly as usual, but in this case, when he sets a base the same as Alice, he only gets a correct result 50% of the time, as Eve has changed the polarisations of the photons he receives in 50% of cases. (See Figure 8). This will be highlighted at the Key Sifting stage, as the QBER will be too high. More stringent privacy amplification procedures can be brought to bear to remove the effects of any information that Eve has extracted.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarisation Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarisation Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×		+
Photon polarisation Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS	+							
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

Figure 8 BB84 key exchange in presence of Eve

source **[WK10]**

4.3.3 *Photon Number Splitting Attacks*

It appears, therefore, that Eve should pack up her eavesdropping kit and retire gracefully: there is no way that she will obtain any useful key information from the BB84 protocol without being spotted. However, the protocol as described has underlying assumptions in addition to the conditions in section 4.2 about the efficiency and capabilities of Alice and Bob’s equipment.

Alice is assumed to possess a perfect single-photon source capable of producing polarised photons on demand. In a practical application, these do not exist: pulses from an attenuated laser, known as Weak Coherent Pulses (WCP) are used, and although single photons are produced, there is a finite probability that multi-photon pulses will be generated. (The number of photons per pulse has a Poissonian distribution.) This practical weakness gives Eve an opportunity to siphon off the surplus photons, keeping one for herself and forwarding the remainder on to Bob untouched. This is the **Photon Number Splitting attack** (PNS) which was first identified by Brassard et al in 2000 [GB00].

Eve’s photon splitting must not destroy the polarisation of the photon or the photon itself, so polarisation-preserving operations and so-called quantum non-demolition (QND) measurements are required, but these are technically possible. Eve then has to wait until the public discussion of the bases happens and then she can measure her stored photons with 100% accuracy. Alice and Bob will be none the wiser, as the original quantum states have been exchanged without errors.

And, to add insult to injury, if the quantum channel between Alice and Bob is noisy i.e. photons are regularly lost in transit, Eve can replace the lossy channel with a perfect quantum channel between herself and Bob. She can then send photons *of her choosing* to Bob, to arrive at his detectors at the same rate he would expect from the original lossy channel. In extreme cases, Eve can block all single photon signals received from Alice, and split and forward only the multi-photon signals; the non-detection of the single photons at Bob's receiver will be attributed to the losses in the quantum channel, not eavesdropping, and Eve will gain complete information on the key, undetected.

It may be that Alice and Bob could find out that a PNS attack was underway by examining the photon number statistics (the Poissonian distribution). But the work of Lutkenhaus [NL02] describes an **Extended Photon Number Splitting** attack, where Eve extracts two or more photons from the multi-photon pulse, and forwards the remaining photons on to Bob following the Poissonian distribution he is expecting. So with Eve cleverly accessing some signals and suppressing others, she can make the results at Bob's detectors look identical to those for a normal lossy channel for given signals from Alice.

4.3.4 Counteracting PNS Attacks

There are two methods which can be used to fight PNS attacks on the BB84 protocol: the use of reference pulses, or by employing a second photon source to create decoy pulses. Reference pulses are stronger signals sent at regular intervals by Alice, containing multiple photons. If a genuine single photon signal is intercepted by Eve, or the reference pulse is used in a PNS attack, Bob records an error and Eve is found out. Reference pulses were first mooted in Brassard et al.'s 1992 paper [CB92b].

Decoy pulses were proposed by Hwang [WH03], and can be used to overcome PNS attacks when the quantum channel is subject to high losses i.e. ideal conditions for an extended PNS attack. Alice used a second photon source to create multi-photon pulses randomly (and intentionally!) On a lossy channel, Bob will only expect to receive a proportion of the original signal, referred to as the *yield* of the signal. If Eve is interfering with the quantum transmission and attempting a PNS attack, she will not be able to distinguish between genuine multi-photon pulses and decoy ones, so will intercept both. If the two photon sources (genuine and decoy) are chosen to have identical characteristics then it is possible to use them for different purposes: one is used to distribute key material, the other is specifically to detect PNS attacks. Bob measures the arriving photons as usual, but the subsequent Key Sifting stage is slightly more elaborate. Alice announces which pulses are decoys, so the total yields of both the key source and the decoy source can be estimated. If the decoy source yield is much higher than the 'genuine' source's yield, then that implies more multi-photon pulses are finding their way through the quantum channel (conversely, more single photon signals are being lost) which points to a PNS attack. The protocol run can then be terminated, rather than risk losing secret key material to Eve. If the total yields of both sources are similar, the protocol continues by estimating the yield of genuine multi-photon pulses from the known characteristics of the decoy pulses. (It has been shown by Hwang that these assumptions can be justified [WH03]). Eve cannot adapt the PNS attack to obtain meaningful information, as she cannot tell which signals are decoys and which genuine.

More sophisticated implementations of this idea involve Alice additionally modulating the intensity of her laser [VS09a].

4.4 The B92 Protocol

The B92 protocol is a variant of the BB84 scheme, still using polarised photons, but this time with non-orthogonal quantum states for encoding information [CB92b] (This paper also included reference pulses in the protocol). Two quantum states are used, instead of the four required in BB84. Alice randomly chooses one or other of these quantum states and sends them to Bob via a quantum channel. Bob has two methods to measure the arriving photons, which will either register "detection" or "no detection". (The actual measurement mechanism is beyond the scope of this paper). During the Key Sifting stage, Bob tells Alice which photons he "detected", but not his actual measurement, and all other photons are discarded. Error correction and privacy amplification continue as normal, to verify that the secret key is the same for both Alice and Bob.

4.5 The SARG04 Protocol

The Photon Number Splitting vulnerability of the BB84 protocol arises because whenever Eve siphons off a photon, she can obtain all the information from it after the public key sifting stage. The SARG04 protocol [VS04] generalizes the BB84 approach (via B92!) to become “robust against PNS attacks” by using four non-orthogonal quantum states for key carrying. The original protocol uses the polarisation of photons to transfer the quantum states from Alice to Bob, but there is also at version which uses entangled photons [CB08].

Alice encodes her bits in one of these four states: Bob randomly selects one of two special filters to measure them, and a key sifting process ensues. At the basic quantum level, this is identical to BB84, but it is the key sifting where the radical change occurs. Instead of discussing which bases were used to generate the photons, Alice reveals “the state she has sent and one of the states which code for the other value of the bit, which are not orthogonal to the first one” [CB08]. Bob will either have guessed correctly or incorrectly, and qubits are discarded accordingly. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key. Errors will be found if

- there are losses on the quantum channel
- the state has been modified en-route by Eve,
- or if there are dark counts at the receiver (i.e. positive results not associated with the quantum transfer, such as background radiation).

Eve is in a tricky position now: if she has retained two photons, for example, in BB84 she would gain full information after the public discussion of the bases. In SARG04, she only finds out that the state is one or other of two non-orthogonal states and she doesn’t know which is which with any degree of certainty. Her best bet to obtain information for certain is to perform operations on three-photon pulses, which will only succeed with probability ½. This severely limits the information available to her.

The SARG04 protocol provides almost identical security to BB84 in a perfect single-photon implementation: if the quantum channel is of a given visibility (i.e. with losses) then the QBER of SARG04 is twice that of BB84, and is more sensitive to losses. However, SARG04 provides more security than BB84 in the presence of PNS attacks, in both the secret key rate and distance the signals can be carried (limiting distance). The conclusion is therefore

> *"Different ways of encoding and decoding the classical information lead to different performances according to the physical characteristics of the set-up"* [CB08]

4.6 The E91 Protocol

In 1991, Ekert proposed a method of harnessing Bell's inequalities to perform key distribution via entangled polarised photons in a quantum channel. [AE91][AE06] These entangled photons can be created by Alice, Bob or a trusted third party (TTP), and each pair is separated in a way that results in Alice and Bob receiving one of each pair. This is arguably a more secure method of using polarised photons, as there is not information to be eavesdropped: it only springs into existence at the moment of measurement.

Alice and Bob both independently and randomly choose from two different orientations of their analysers to measure the polarisations of the photons, and the choice of analyser is the basis for the publicly discussed key sifting stage. A typical physical set-up is shown in Figure 9, using active polarisation rotators (PR), polarising beam-splitters (PBS) and avalanche photodiodes (APD)

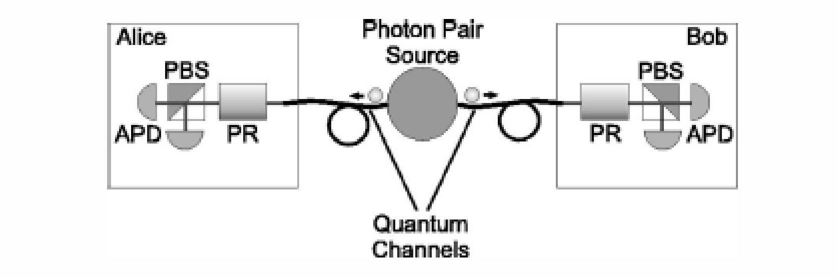


FIGURE 9 A TYPICAL SYSTEM USING ENTANGLED PHOTON PAIRS

SOURCE: [NG02]

The measurements are divided into two groups: the first is when different orientations of the analyser were used, and the second when the same analyser orientation was employed. Any photons which were not registered are discarded. Alice and Bob then reveal the results of the first group only, and check that they correspond to the value expected from Bell's inequality (=-2√2): if this is so, then Alice and Bob can be sure that the results they obtained in the second group are anti-correlated and can be used to produce a secret key string.

Eve cannot obtain any information from the photons when they are in transit, as there is simply no information there! Information is only present once the authorised users perform their analyser measurements and key sifting. Eve's only hope is to inject her own data for Alice and Bob, but as she doesn't know their analyser orientations, she will always be detected (the Bell's inequality value will be too low.)

4.7 The BBM92 Protocol

Shortly after Ekert proposed his entanglement based protocol, Bennett, Brassard and Mermin devised another, the so-called BBM92 protocol [CB92c]. This involves pairs of entangled photons (EPR pairs), and can be regarded as an entanglement-based version of the BB84 protocol. The raw key exchange, key sifting and privacy amplification are essentially the same, with measurement axes being discussed openly, not actual measurements. The only real difference between the schemes (apart from the entanglement aspect) is that in BB84, Alice has to actually choose her polarisations randomly, using a random number generator, whereas in BBM92 the randomness is inherent in the measurement of the EPR pair. This scheme has been proved to have unconditional security [EW02], and it also deals with an apparent weakness of the entangled method, whereby the source of photons could be substituted.

4.8 Other Protocols

There are many other protocols in existence, both prepare-and-measure and entanglement based. Example protocols include: Ping-Pong [KB02]; distributed phase reference; six state; homodyne detection; discrete modulation; coherent one-way (COW). These are all very well described elsewhere [e.g. VS09a] and are beyond the scope of this paper.

Chapter 5 Quantum Key Distribution - The Challenges

5.1 Is QKD Too Good To Be True?

From the descriptions so far, quantum key distribution seems to have many potential benefits, with unconditional security proved and eavesdropper detection guaranteed. It sounds almost too good to be true, and yet there has been no mass stampede to implement QKD on a large scale. This chapter will examine some of the issues which are restricting its appeal to the cryptographic community.

5.2 Basic Issues

There are some inherent problems with using quantum states to transmit information, some to do with quantum theory itself, and some practical ones regarding equipment efficiency which affects the security of protocols.

5.2.1 Point to Point links and Denial of Service

The quantum channel is a specialized piece of equipment, which by its very nature is a point-to-point connection: Alice and Bob have to be at each end of it, with their photon sources and detectors. It is in direct contrast to the loose conglomeration of connections which make up the Internet, where anyone can connect with anyone else on an ad-hoc basis, using a network of computers physically linked by conventional transmission lines. The growth and usage of the internet, with hubs and a distribution pattern for links which follows a 'power-law' pattern is built on "small world" network lines: its aristocratic small world architecture as described by Buchanan [MB02] allows distant regions of the internet to be interconnected with ease. The point-to-point nature of QKD restricts potential growth, and gives rise to the possibility of a denial-of-service attack: if Eve can't obtain key information, then cutting the physical link will mean Alice and Bob can't either, which might serve Eve's purposes just as well.

5.2.2 Photon Sources and Detectors

The quality of photon sources and detectors can have a significant impact on the security of a protocol: as seen in section 4.3.3, less than perfect single photon sources mean polarisation based protocols have to be amended to reflect this to maintain unconditional security levels.

Detectors also have practical issues: for example, there is background activity not related to the QKD signals, known as dark counts, where photons are detected spuriously and have to be eliminated from the final secret key string. [VS09a]; also there is a ‘dead time’ between the detection of a photon and the equipment’s readiness to detect the next, which can be exploited by an attacker. This is due to the fact that there is a substance in the detector which absorbs a photon, then generates an electric current to record the detection event. While an event is being recorded, any photons which arrive at the detector will not be registered.

An ideal photon detector should have the following properties, as detailed in Gisin et al.’s paper [NG02]:

- High efficiency over a large spectral range
- Low probability of generating noise (i.e. low dark count)
- The time between the detection of a photon and the corresponding electrical signal should be as constant as possible
- The dead time after a detection event should be as small as possible to allow for higher data transfer rates

The detection process isn’t 100% accurate, due to imperfections in the detection material – and this is *always* different in different detectors, so there will be a mismatch in the dead times of the rectilinear and diagonal basis measurements. Eve can observe this, and can then work out the exact mismatch between the bases. If she can also control the arrival time of photons at Bob’s detectors, she can choose two delays between signals to give the highest probability of a reading on one detector or another, and hence make a reasonably educated guess as to the value of the qubit, 0 or 1, and hence obtain key information. [YZ08]

Even in the face of an unconditionally secure protocol, Eve can *always* attack the equipment - e.g. in the so-called “Trojan Horse” attack [NG05] Eve shines light onto Alice and Bob’s apparatus, then analyses its backscattering (a process known as reflectometry).

5.2.3 Losses in the Quantum Channel and Limiting Distance

Quantum properties such as polarisation are adversely affected by the distance they travel along a channel. Decoherence, chromatic dispersion, polarisation mode dispersion in fibre optic channels can all result in irreversible loss of quantum state for the photons sent along the link. Free space quantum channels also have atmospheric and equipment dependent geometric losses. Since quantum signals cannot be amplified, eventually the losses on the channel will be so high that readings obtained at detectors will be indistinguishable from dark count rates. Unfortunately, it is impossible to avoid lossy channels: they introduce security weaknesses (see section 4.3.3 for an example) and limit long-distance transmission of information, both challenges to QKD protocols.

5.2.4 Key Distribution Rate

The length of the quantum channel also has an effect on the achievable rate of key distribution. The rate at which key material can be sent decreases exponentially with respect to distance, and is regarded as another limiting factor in the usability of QKD systems [MP09].

5.2.5 Classical Authentication

A strongly authenticated classical channel must be used between Alice and Bob, both for the classical post-processing stages, and to prevent a man-in-the-middle attack. The security of the overall QKD system is reduced to that of the classical algorithm used for authentication, which could be merely computationally secure rather than unconditionally secure. Thus “security based on the laws of physics alone” is not always true for the whole cryptosystem! The use of Carter Wegman algorithms [JC79] [MW81] in the authentication does give unconditionally security, however.

5.2.6 Quantum Physics Itself

On a more fundamental level, as the security of the quantum phase of QKD relies *entirely* on quantum theory, how can we be sure that quantum theory is correct? It is, after all, a general scientific principle that a theory can never be proved per se, just not disproved (yet!) Quantum Theory has been formulated for over a century now, and many experimental results have been found which match its predictions. However, even that may not be convincing enough. Some long standing physics theories are being actively challenged by researchers, notably the Standard Model of particle physics: despite experimental results which are spectacularly accurate, its inelegant and cumbersome equations are forcing researchers to reassess its validity. Kaku [MK08] refers to the Standard Model as “a theory only a mother could love”. No such charge could be laid at

Quantum Theory’s door. The interpretation of quantum phenomena may be under discussion, but its basic premises and predictions are sound. (Even Richard Dawkins – admittedly not a physicist, but he was quoting Richard Feynmann who most definitely was – has been recorded saying the accuracy of quantum theory’s experimental results is like “predicting the width of North America to the accuracy of the width of a human hair” [RD10])

5.2.7 A Security Proof Equals Proven Security?

All security proofs of cryptographic protocols make assumptions: sometimes these are not realistic when practical implementations are undertaken. For example, a proof may assume only certain attacks are possible, when a system may be far more complicated in practice. Or, in extreme cases, the security proof itself may be wrong: this occurred with RSA-OEAP (RSA Optimal Asymmetric Encryption Protocol).

The sad tale of this encryption scheme is told by Koblitz and Menezes [NK06] [NK04]: a security proof was developed by Bellare and Rogaway [MB94] and later amended by Shoup [VS01], leading RSA-OAEP to be widely recommended as totally secure. However, a chosen cipher text attack was found by Manger [JM01] which used a method that was unthought-of when the proof was written. The proof was still “correct”, but the scheme was found to be insecure seven years after the proof was published!

In QKD, the most telling assumptions are about Alice and Bob’s capabilities [VS09b]: they can be over-idealized in a security proof. For example, detector efficiency is not perfect, as illustrated in section 5.2.2, but only a few proofs recognize this [CF09, for example]. Scarani and Kurtseifer list more of Alice and Bob’s potential failings in [VS09a], which may affect the validity of some existing security proofs.

5.2.8 Side Channel Attacks

One aspect of security which rarely gets addressed in security proofs is the possibility of side channel attacks: these occur when it is possible to extract meaningful information from the system indirectly, maybe by inducing faults, or through power analysis of the processor. (The Side Channel Cryptanalysis Lounge [SC10] is awash with research on this topic). QKD technology is still in its infancy, and hasn’t had the benefit of sustained research into this type of information leakage.

A notable example of a side channel problem occurred in the very first practical demonstration of the BB84 protocol [CB92a]. This is, after all, a protocol which has many security proofs, catering for a range of differing assumptions, so should be unconditionally secure. In the experiment, the Bob module had a photon detector which made a different sound when it registered different polarisations, due to a noisy power supply. Brassard himself said of the results [GB06]:

> *"we could literally hear the photons as they flew… [the prototype] was unconditionally secure against any eavesdropper who happened to be deaf!"*

5.2.9 Key Management

Quantum Key Distribution, to be effective, has to form part of an overall key management scheme which deals with key generation, key storage, key maintenance and key destruction over the useful life of the key. This is not an easy task, and will be especially challenging for QKD schemes where the resultant secret key is used in a one time pad (OTP) encryption. OTPs haven't been used widely in the past for exactly this reason: key management is often difficult, as the key must be the same length as the message, completely random and used only once, otherwise security is compromised. Additionally, there is a classical authenticated channel which will need (classical) symmetric keys to be exchanged as part of the initial set-up, and appropriate symmetric session keys when the channel is used for the post-processing key sifting and distillation phase of QKD protocols.

Not only is good key management crucial to the success of any crypto-system, it is also probably the hardest aspect of the whole system, as it has to meet both technical and organizational challenges to ensure the key life-cycle remains secure.

5.3 Is QKD Actually Needed?

Perhaps the thorniest issue of all is whether QKD is actually needed at all - this has divided academics in the cryptographic community. There is a spectrum of views, ranging from a notion that QKD is effectively a solution looking for a problem with no current or future practical use [BS08a] [BS08b][KP09] through to regarding QKD as virtually the saviour of the internet because cryptography as we know it is doomed [SGH08]. Peev et al [MP09] capture the prevailing mood perfectly by stating that there have been

"Psychological restraints and acceptance barriers with experts in mainstream security research"

Within the Information Security world, cryptography is regarded as a success story. Properly implemented cryptography enables sensitive information (such as credit card details) to be transmitted in an insecure (or positively hostile!) environment like the internet, and provides the essential security services of confidentiality, integrity and authentication which form the bedrock of many online business and leisure transactions. The algorithms used mean that it is computationally infeasible for an attacker to try every possible cryptographic key in a brute force attack to gain access to the encrypted information. Thus the security provided by current schemes is computationally secure, but not unconditionally secure. But for practical purposes, however, it is an extremely strong defence mechanism. If a security system fails, it is much more likely to be through poor key management, or human failures – password written on a Post-it stuck to a screen, for example – than by breaking a cryptographic algorithm. (However, so-called rubber-hose cryptanalysis, where the key holder is physically threatened, concentrates the mind wonderfully and is very effective at retrieving secret information.)

Is the promise of unconditional security a big enough business imperative to warrant the expense of specialized equipment and infrastructure? Current cryptographic key distribution protocols provide more than adequate security, so the benefits are really unclear: should pragmatism win over theory?

But introducing quantum key distribution, and in effect upgrading from computational to unconditional security, does not necessarily increase the overall protection of a crypto-system: as Bruce Schneier states "Security is a chain: it's as strong as its weakest link" [BS08a]. By further strengthening the strongest link in the chain, it prompts attackers to look for vulnerabilities elsewhere in the system. This is why Schneier famously calls QKD "as awesome as it is pointless" [BS08a]. There is the added psychological problem that the perceived increase in security could lead to unwanted effects elsewhere in the system, in the same way that people adopted more dangerous driving styles once the wearing of seat belts became compulsory, as their perception of safety was increased so risk compensation activities occurred. It is perfectly possible to build an insecure system from strong algorithms and protocols, whilst believing that the overall security level is commensurate with that of the algorithm.

So, with this in mind, the claims of the pro-QKD corner have to be scrutinized very carefully. Announcements that "cryptography solutions widely used at the moment could be threatened and will definitely become obsolete in the near future" [SGH08] are a little exaggerated, to say the least. Cryptography-killing mathematical advances could happen at any time, not necessarily in the "near future", and even if a fully operational quantum computer was developed today, symmetric algorithms will still cope by simply doubling the length of the key (to negate the effects of Grover's algorithm). Similarly, when Shor's algorithm renders asymmetric schemes unusable – again, not an imminent situation - there are other suitable algorithms under development, such as lattice based systems which are immune to quantum processing advances.

It is tempting to attribute these headline-grabbing sound bites as an attempt to raise funds for quantum research: after all, the more fear instilled into the general public (and a few specialists who should know better) that all their online information will become instantly insecure should result in more resources being made available to develop the QKD solution. It is a dangerous game to play, after all. Over-hyping a new technology can backfire spectacularly with swift and destructive effects. For example, the microblogging site Twitter appears to be on the brink of backlash [BR10] [JF09], potentially falling out of fashion shortly after it becomes popular.

Recently there has been some acknowledgement that perhaps things had gone too far [VS09a] and that both camps should work together to provide security solutions for the pre- and post-quantum computing world. It has been suggested [DS09] that a cryptographic landscape might evolve where QKD and asymmetric tools can combine to provide future proof security, without the need for an entrenched classical/quantum divide.

5.4 When to Use QKD

Doubts notwithstanding, widespread adoption of QKD would certainly become desirable if:

- current cryptographic key exchange schemes are not considered secure enough

- advances in mathematical techniques, such as factoring large numbers, threaten the security of existing algorithms
- a fully functioning quantum computer is practicable

The two latter points are the subject of ongoing research, and although they will affect the desirability of QKD protocols in future, they will not form part of this report.

As mentioned previously, current cryptographic schemes can be extremely strong. How secure does a system need to be to warrant the use of QKD? The most secure method of exchanging keys is not computer based at all – by using a trusted courier to physically transport a key (or part of it) in a tamper proof medium (such as a smart card) to its destination, possibly flanked by police/ armed guards to deter interceptors ultimate high-security exchange can be achieved. Even this can go wrong, though, if the trusted courier turns out to be untrustworthy after all, and substitutes an incorrect key somewhere in transit. No existing protocol is 100% secure: QKD will not be either, but may possibly provide a more cost effective and faster way to achieve a similar level of security to the trusted courier approach, in a controlled and secure environment, with the added benefit that security can be future proofed. [DS09] Future proofing means that even if a cryptographic system is broken at some unspecified future time, previous messages sent through it remain secure.

5.5 The Way Forward

There are three choices open to the embryonic QKD technology: firstly, research can continue to develop more secure protocols and more proofs to reach highest security levels, regardless of their practicality; secondly, take the best of what's available, try and find a competitive niche and exploit it [VS09a]; or thirdly, give up quantum technology and concentrate on improving classical cryptographic methods ready for the post-quantum computer world. Option one is research based, with limited commercial appeal, so on the basis that giving up on QKD is not an option until its potential has been explored fully, this analysis will continue with one eye firmly fixed on that potential niche market.

It is time to look at QKD networks.

Chapter 6 Quantum Networks

6.1 Innate Problems with Quantum Channels

The protocols described so far are well thought out and theoretically sound. However, quantum transmission has two glaring problems not addressed by the protocols, which restrict their practicality in a wider setting: the point-to-point nature and distance limitations of a quantum channel.

Alice and Bob have, of necessity, a fixed link between them, the quantum channel. The point-to-point nature of the connection invokes the "quadratic curse". For use by multiple users, each pair of users needs to pre-share symmetric keys, so N users connected via point-to-point links, require distribution of a number of keys proportional to N^2 (see section 2.7 previously). Clearly this becomes unworkable as the number of users grows larger, so an alternative strategy is needed.

There are limits to the distance a quantum signal can travel along a channel. Figure 10 shows the bit transfer rate from a Weak Coherent Pulse (WCP) plotted against distance travelled along a quantum channel: a steep attenuation of the signal is observed at a critical distance, before the signal disappears at approximately 120 km. Much research is being done in an attempt to extend this distance (For example [DSt09]), but it is a severely limiting factor in the potential deployment of quantum channels.

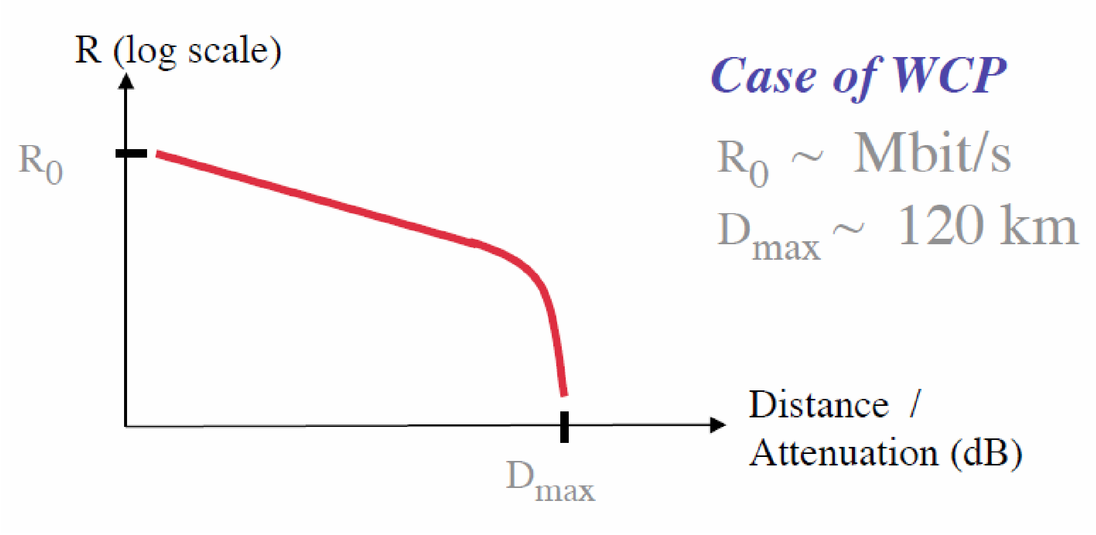


FIGURE 10 SINGLE QKD LINK PERFORMANCE

SOURCE [RA05]

6.2 A Networked Solution

However, the point-to-point nature of quantum links could be removed by joining individual links together in a network. To be suitable, a network design must include sufficient redundancy to cope with failure in one or more of the links, and extend the distance quantum signals can be carried. The network architecture must be chosen so that every potential pair of users of the QKD network can exchange keys with unconditional security, without becoming unworkable. Additionally, the method for joining individual quantum links together (Nodes) has to be compatible with the special properties of quantum optical signals, and must not destroy or alter the key material in a manner which compromises the unconditional security of the transmission.

The various design strategies to deal with these issues will now be examined, and then a practical implementation (the SECOQC network [SQ10]) will be described in detail in Chapter 7.

6.3 Quantum Network Types

The design objectives for a quantum network are that many users can be catered for simultaneously, and that the distance quantum signals can be sent with unconditional security must be significantly longer than that of the individual links. Quantum networks can be split into three distinct types, depending on the technology used at each node connecting individual quantum links. They each have strengths and weaknesses, and varying degrees of practicality - quantum node networks, optical node networks and trusted relay node networks, and all three types are described by Dianati and Alleaume [MD08].

6.3.1 Quantum Node Networks

A quantum node can be used to combat the quantum decoherence of the signal along the quantum channel by actively performing quantum operations on the travelling photons. One way to do this suggested by Cirac et al.[JC98] necessitates the use of quantum entanglement sources, quantum memories and entanglement purifications techniques which result in perfect entangled states subsequently stored in a portion of the quantum channel. These nodes are *Quantum Repeaters*: they chain the stored states together and thus obtain perfect end-to-end entanglement useable over arbitrarily long distances. However, quantum repeaters exist only theoretically: they await the development of fully fledged quantum computing capabilities to become practical. A less elaborate quantum node, the *Quantum Relay* proposed by Collins et al. [DC03] doesn't require a quantum memory, and is hence feasible but technologically difficult. However, quantum relays do not extend the distance over which a quantum signal can be sent so will not be suitable for a practical QKD network.

6.3.2 Optical Node Networks

Optical nodes use classical processes on the quantum signal: beam splitting, multiplexing, de-multiplexing and switching, for example. As this is a classical approach, it is well within the capabilities of existing technology, and can be used to create one-to-many QKD relationships. With the addition of active switching, two QKD nodes can be specifically selected for connection. This multi-user QKD feature was used in the first working QKD network, the BBN DARPA network, which was set up between Boston University, Harvard and BBN [CE06] [CE02]. Optical nodes have no requirement to be trusted, as they merely switch the signal from one quantum channel to another; no processing on the contents of the signal is done. The main disadvantage of this type of network is that it cannot be used to extend the distance the quantum signal travels. In fact, it reduces the maximum signal distance due to optical losses at the node!

6.3.3 Trusted Relay Networks

So the options detailed above both have disadvantages: quantum nodes extend the potential signal distance but aren't achievable with today's technology, and optical nodes enable multi-user operation but reduce the maximum signal distance, thus rendering both less than perfect for a practical implementation. So a third option, trusted relay networking, is a compromise. Using classical technology – and therefore practically possible – a trusted relay does exactly 'what it says on the tin'. A relay node is trusted implicitly to forward on the quantum signal without eavesdropping or tampering with it.

To do this in a QKD network, local keys are generated over QKD links and stored securely in trusted nodes at each end of the links. (The nodes are effectively a mini-Alice and mini-Bob performing their own little QKD protocol run, independently of any other messages being passed through the network.) When a real Alice and real Bob want to do a QKD protocol run, a chain of trusted relays and their intermediate quantum links is created to connect them together: this is a QKD path. Alice and Bob's quantum key is treated as a message, and encrypted via a one time pad using a local key stored at a trusted node: it travels "hop by hop" between each node on the QKD path, and is decrypted and re-encrypted at each node using a new key from the node key store. (And of course, all required unconditionally secure classical authentication procedures are also done at each node using locally stored QKD keys). This is illustrated in Figure 11.

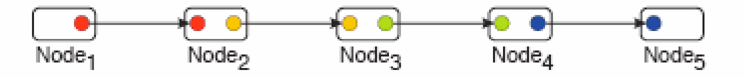


FIGURE 11 HOP BY HOP QKD PATH

SOURCE [RA07B]

This gives end to end unconditionally security provided all the nodes in the QKD path are trusted, since at each node **i**, the message M is related to the cipher text C and the local key $K_{\text{local, i}}$ via the EXCLUSIVE OR (⊕)operation

$$\mathbf{C_{i} = M \oplus K_{local,\, i}}$$

which leaves M appearing in cleartext at each node.

6.4 Practical Quantum Network Implementations

To implement a quantum network using today's technology, therefore, the choice is between optical nodes, or trusted relays: in 2006 the BBN DARPA QKD network used optical nodes [CE06], and the SECOQC Network [SQ10] (to be discussed in the next chapter) was implemented in 2008 on trusted relay principles.

There is a proposal to implement another QKD network, UQCC-10, in Tokyo in October 2010, which will not be covered in this paper. Furthers details of this network can be obtained from the UQCC-10 website [UQ10].

Chapter 7 The SECOQC project

The SECOQC project started in 2004, as a result of an EU-funded initiative to research the development of a Global Network for **SE**cure **CO**mmunication based on **Q**uantum **C**ryptography. [SQ10] A working metropolitan area network (MAN) operated as a field trial in Vienna in October 2008. The main objectives of the project were to investigate and develop hardware and protocols for network operation of QKD. Additionally, relevant standards allowing the technology to be interoperable with classical systems were identified for coordination by the European Telecommunication Standards Institute (ETSI). Example standards cover security assurance, interfaces, security proofs and integration [CE-P09].

The SECOQC design is described in detail by Peev et al. [MP09] and it focussed entirely on information theoretically secure key agreement – not secure communication. The design is modular, and employs a trusted relay philosophy. This enabled both the use of a broad variety of QKD technologies (and hence develop interoperability of the QKD devices), and the development of QKD network-specific protocols. This led to a unique design approach: the network of secrets, which is a classical key management network to support the QKD capability. An overview of the design, architecture, topology, and protocols employed in this network follows.

7.1 Basic Building Blocks

The SECOQC network is formed from access nodes (QAN) and backbone (QBB) nodes, with the assumption that all nodes are trusted. A QAN is essentially a point to point link from an end user into the main quantum backbone network. This is shown in part (a) of Figure 12. These links can be any quantum optical medium.

The QBB building block is more complex: four QBB nodes are connected by 6 quantum channels. Each QBB node can act as an endpoint to a QAN, so in part (b) of Figure 12, information going from Alice to Bob and vice versa has a choice of three separate routes: the paths (L1, L2), (L4,L3) or (L5).

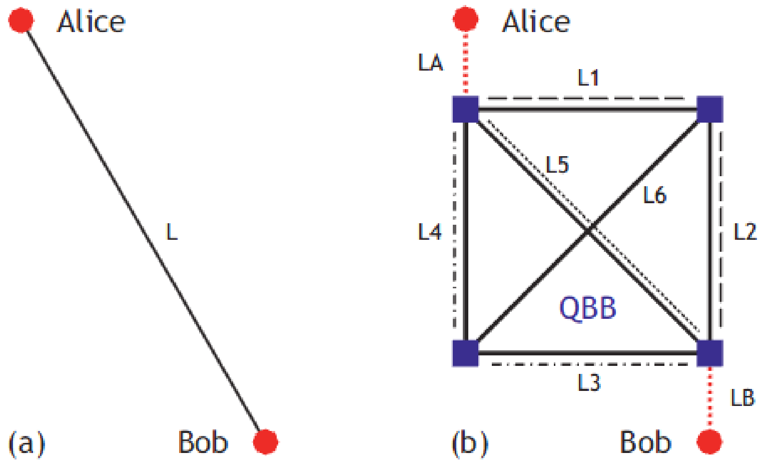


FIGURE 12 QUANTUM ACCESS AND BACKBONE LINKS

SOURCE [AP08]

A modular approach gives a number of advantages: to add an extra user to a pre-existing network, only one new link (QAN) is needed, hooking up to the nearest QBB node. Since all other users are already connected to the QBB network, they can potentially share a symmetric key with the newcomer. If there are N users on the network, this key sharing process increases in proportion to N, not N^2 as in the case of point-to-point networks, which is highly desirable. Additionally, as there are multiple paths between QBB nodes, there is inbuilt redundancy which can weather both technical defects in any one path and active denial of service threats. QBB building blocks can also be easily added to expand the network.

7.2 Hierarchical Network Structures

A hierarchical network breaks down network paths into smaller and more manageable units, which helps with standard network tasks such as routing and planning traffic usage. With this in mind, there is a different network structure for the access nodes and the backbone nodes.

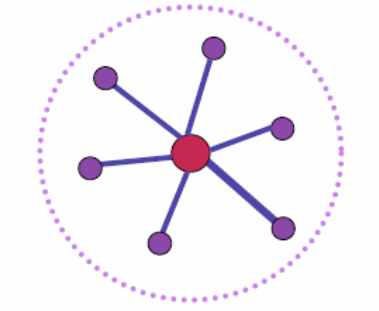


FIGURE 13 STAR NETWORK TOPOLOGY

SOURCE [RA07B]

The QANs are included in a network with a star topology like the one shown in Figure 13, so that many QANs can link to one central QBB.

A meshed topology, as in Figure 14, is more appropriate for the QBB network as it gives high reliability, high connectivity and more efficiency, by providing multiple disjoint paths between any pair of nodes. [LS04][OM05]

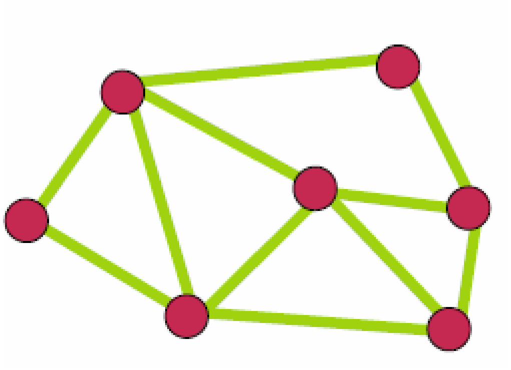


FIGURE 14 MESHED NETWORK TOPOLOGY

SOURCE [RA07B]

Messages through the whole network follow the hierarchical path:

Alice→QAN→QBB→QAN→Bob

7.3 Objective of QBB Links

The quantum backbone is analogous to classical backbone links in the Internet, where a high capacity transmission medium is used to transport information sent to it via smaller branches. Figure 15 shows the structure of a Quantum Backbone link, with its multiple quantum channels between two QBB nodes.

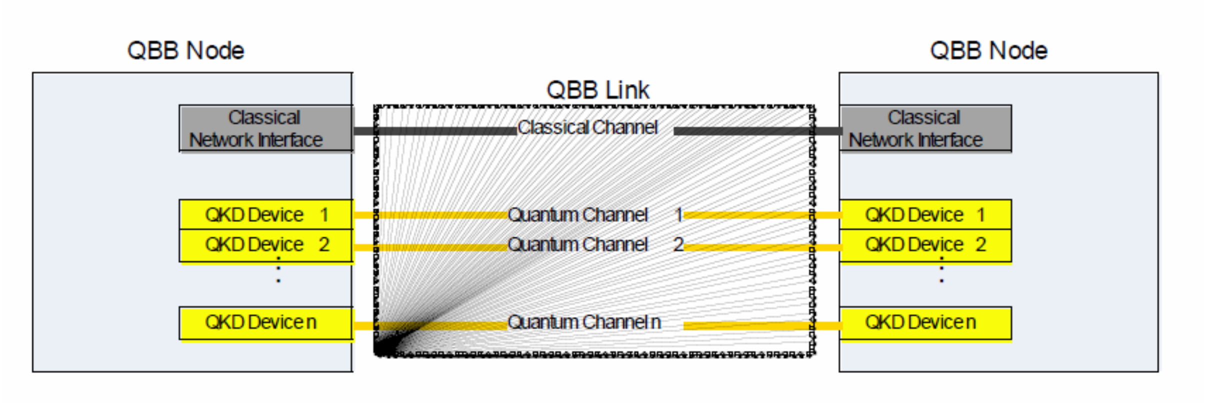


FIGURE 15 QUANTUM BACKBONE LINK

SOURCE [RA07B]

Trusted nodes are effectively key stores for local keys, so the objective of each QBB link is to generate as much key material as possible, and pass it to the node for safekeeping until it is needed. This can be done independently of other traffic on the network. As explained in section 6.3.3, local keys are used to encrypt Alice and Bob's QKD key hop by hop along a QKD network path.

Keys established via the QKD network can then be used in classical cryptographic operations (not necessarily one time pads) over public networks like the Internet. Figure 16 shows how the SECOQC network interacts with other public networks.

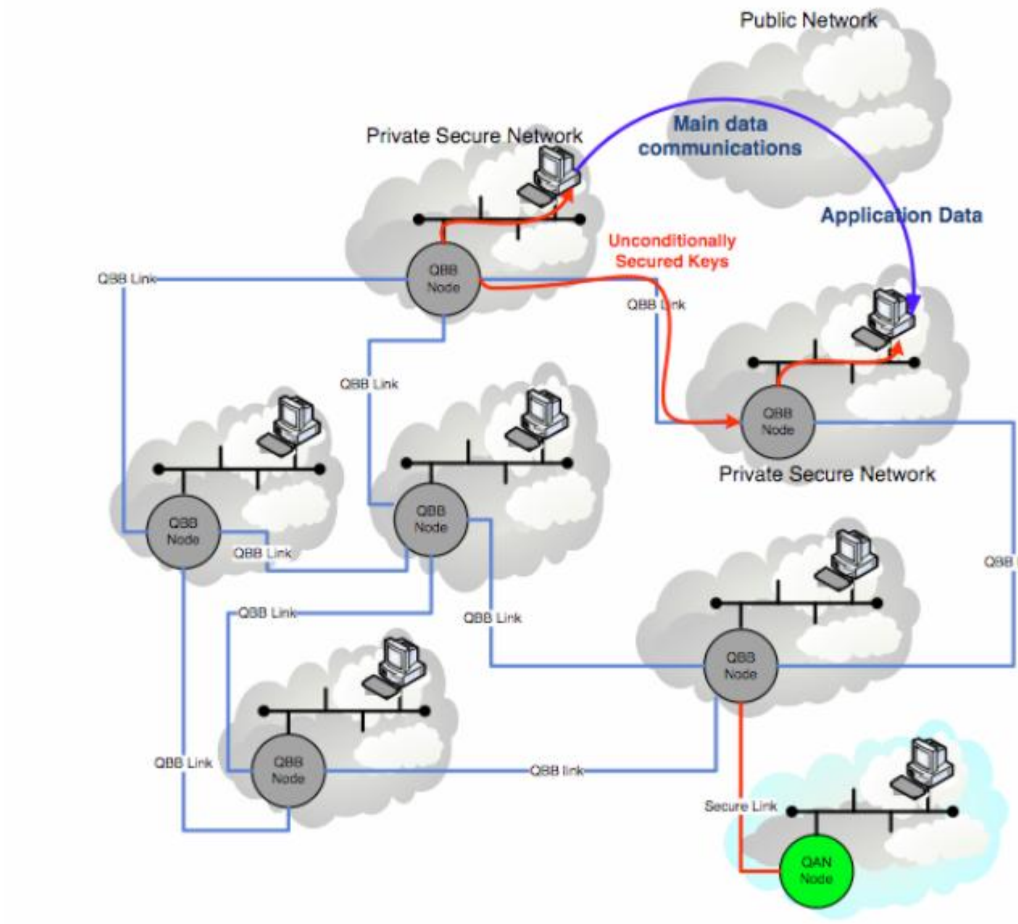


FIGURE 16 THE STRUCTURE OF THE SECOQC NETWORK

SOURCE [MD08]

7.4 The Network of Secrets

The network of secrets is defined by Alleaume [RA07b] as "*a set of trusted key stores sharing extendible pairwise local secrets connected by classical channels*". It is effectively a network for establishing keys with unconditional security, with additional key management features i.e. a dedicated key distribution network infrastructure [RA07a]. It sits between the quantum access network and the quantum backbone network, shown as the middle layer of the network architecture diagram in Figure 17.

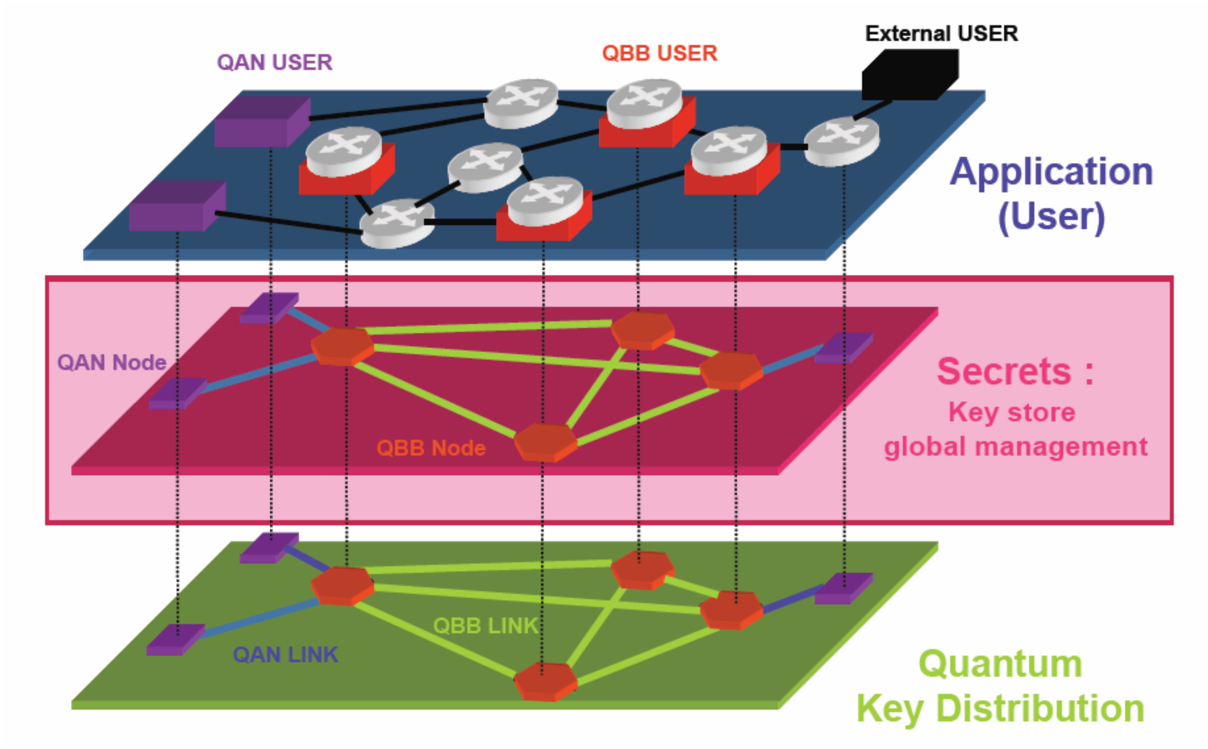


Figure 17 SECOQC network architecture

Source [RA07b]

The main tasks of the network of secrets are to store, forward and manage the key materials generated by QKD. It has dedicated link, network and transport layers (as in the OSI network model) and can be regarded as an independent entity within the overall framework of the SECOQC network. Its key stores are linked by classical channels; using unconditionally secure cryptographic primitives in conjunction with keys derived from local QKD processes ensures that unconditional security can be maintained provided the nodes are trusted. The logical layers are detailed in Figure 18.

Layer 1	Exchange of secure secret key bits
Layer 2	Unconditionally secure transmission of classical payload between adjacent nodes connected by a QKD link
Layer 3	Unconditionally secure transmission of a classical payload between two arbitrary nodes in the QKD network

Figure 18 Logical layers of the network of secrets

Source [RA07b]

7.5 New Protocols

Several different physical devices are used in the SECOQC QBB network (detailed in [AP08]). As a consequence, a common lower layer protocol has been developed to handle their differing characteristics and interfaces – the Quantum Point –to-Point Protocol, or Q3P [MP09].

If Q3P is used to connect a pair of devices, then network protocols can be layered on top of it: unfortunately, the most common one, TCP/IP is not directly compatible with the requirements of QKD, so has been adapted to create a QKD-specific transport layer protocol, known as QKD-TL [MD07]. Also, a routing layer protocol has been developed, based on OSPF (i.e. Open Shortest Path First, a dynamic routing protocol in IP networks), known as QKD-RL. These protocols are described in more detail in [MP09].

7.6 The Implementation

The implementation strategy was to use different types of QKD equipment in different parts of the SECQC network, to maximise the effectiveness of the trial. Each set of devices had to comply with exacting interoperability and performance criteria. (See [MP09] for full details). Specific performance objectives were that QKD links should operate at distances exceeding 25km, and that the key generation rate at this distance should exceed 1 Kbit per second.

Figure 19 shows the geographical implementation of the network: there were six nodes connected by eight QKD links. BREIT, SIE, ERD, FRM and GUD were located in various premises belonging to Siemens, one of the SECOQC partners, and used Siemen's internal fibre optic communications ring. Another node (STP) was a repeater station near St Polten.

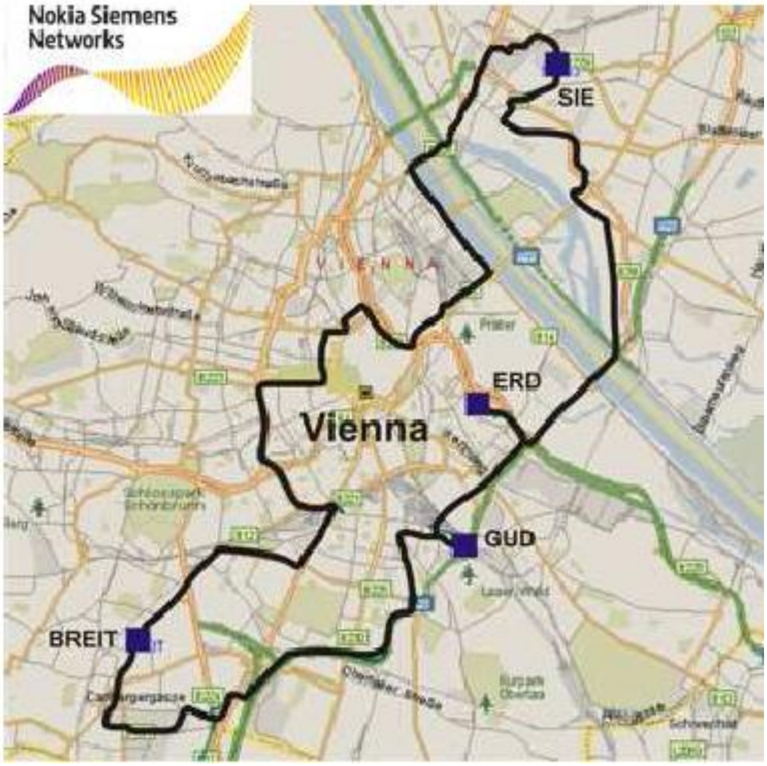


Figure 19 Map of Vienna showing stations SIE, ERD, GUD, and BREIT

source [AP08]

Figure 20 shows the network topology of the SECOQC QKD network prototype. (Solid lines represent quantum communication channels; dotted lines denote classical communication channels). The various QKD technologies are also shown on this diagram:

- STP – BRT used a Coherent One-Way protocol (COW)
- BRT – GUD, BRT – ERD and SIE – GUD used systems developed by idQuantique, known as Plug and Play, which used BB84 and SARG04 (BRT – ERD)
- BRT- SIE used a Toshiba system involving Weak Coherent Pulses plus decoy states in a BB84 protocol
- ERD – FRM used a free space Quantum optical link, via BB84 and decoy states
- SIE – ERD used an entanglement based scheme, in the BBM92 protocol
- GUD – ERD employed a CV system, which is a coherent-state reverse-reconciliated QKD protocol

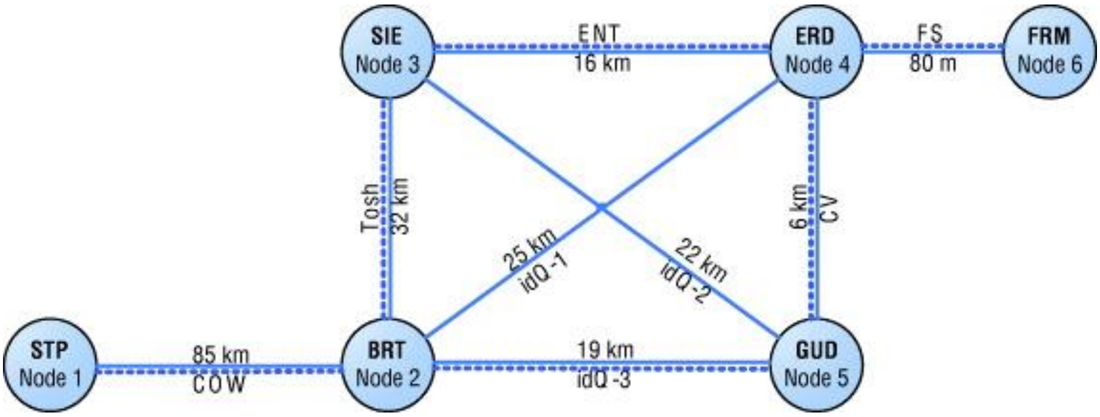


Figure 20 Stations on the SECOQC ring network in Vienna

source [MP09]

7.7 Results of the Trial

With the exception of the free-space link, ERD-FRM, all the devices performed well. (The free space link had some unexpected and unexplained fluctuations in a decoy parameter, which meant that it could only be implemented without the capacity to recognise PNS attacks). Figure 21 summarises the results obtained from the trial, and it can be seen that some technologies were more successful than others. Most exceeded the SECOQC performance objectives.

QKD Technology	Protocol	**Key Generation Rate (Kbits per second)** *SECOQC objective =1kbits^{-1}*	**Distance** *SECOQC objective = 25 km*
idQuantique Plug and Play	BB84 with decoy states and SARG04	27 18 11 5.7 3.1	1 km 10 km 20 km 25 km 33 km
GAP (University of Geneva)	COW	0.6	82 km
Ent QKD (Austrian-Swedish Consortium)	BBM92	2.5	16 km
CV (Thales research, et al)	CV QKD	8	6 km
FS QKD (University of Munich)	BB84 with decoy states	17	80 metres

Figure 21 Summary of key generation rates for SECOQC QKD links

Data taken from [MP09]

Peev at al. [MP09] concluded from these figures (and others not covered in this paper), that the secret transmission capacity of the SECOQC network as implemented is of the order of magnitude of 1 GiB (=2^{30}B) per month: their verdict was

> *"This figure is still very low indeed, but only three to four orders of magnitude away from an adequate transmission capacity. This is not beyond reach!"*

Whether this optimistic view is justified remains to be seen!

7.8 Post SECOQC Technical Developments

Technology continues to improve: for example, recent research by Dixon et al [AD10] has demonstrated that a key generation rate of over 1 Mbit per second is possible by improving the efficiency of the operating frequency of avalanche photodiodes. Also, an electrically driven entangled photon gun [MC10] [CS10] has been created which will improve the usability of entanglement-based protocols.

But, as if to emphasise that information security is an arms race... there has been a phase-remapping attack on idQuantique's Plug And Play system [JL10] [FX10] where an eavesdropper can extract meaningful key information and still stay under the radar, as it were. In this attack, the QBER, which increases in the case of eavesdropping, did not rise above the 20% lower limit set for the system, so the errors were attributed to channel losses, rather than to Eve at her most devious.

7.9 Future Directions for QKD Networks

The SECOQC network (and the BBN DARPA network) proved that QKD networking can be practically viable. Their architectures have, to a certain extent, overcome the innate problems of QKD and been extended over a Metropolitan Area Network (MAN). If, in future, free space quantum optics via satellite (e.g. [PV09]) are used as quantum backbone links, then a wider geographical area can be covered.

The SECOQC design allows for scalability and interoperability of QKD facilities: however, the design is only relevant to the trusted relay regime. Switched or mixed networks, which are more commonly used, do not lend themselves to this type of design. More research needs to be done to incorporate QKD technology into mixed networks, which will widen the implementation opportunities.

Chapter 8 Free Space Quantum Optics Research

8.1 Background

Part of the SECOQC project [SQ10] involved an interesting technology, free-space quantum optics, which is being investigated by Rarity et al [JD06] in conjunction with HP Laboratories, Bristol. Information transfer is done without using fibre-optics, merely through line-of-sight channels, and can be short range (a few cm), medium range as in the SECOQC network or long range via satellite links. All have potential, but this chapter will be dealing solely with short range experiments.

8.2 The Research

Rarity's group has experimented with free space quantum optics as a potential medium for transferring quantum states from Alice to Bob. "Free space" here equates to a line-of-sight path between end points, so that polarised photons travel through the air rather than through a fixed cable, over short distances (around 5cm). The design philosophy of the system is that two modules ("Alice" and "Bob") are constructed from low-cost off-the-shelf components, with "Bob" being responsible for the bulk of the processing effort. A photo of the experimental set up is shown in Figure 22.

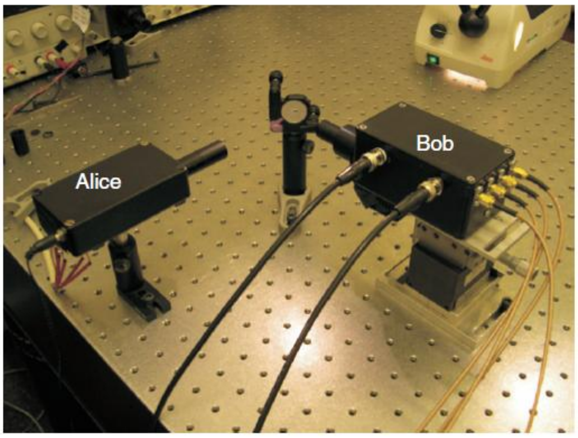


FIGURE 22 QKD EXPERIMENTAL SET UP

SOURCE [JD06]

Polarised photons are used in accordance with the BB84 protocol, along with the mandatory secure classical channel. A diagram of the key exchange method is shown in

Figure 23. Proof of principle has been established, as quantum information has been exchanged, and research efforts continue to improve speed and reliability.

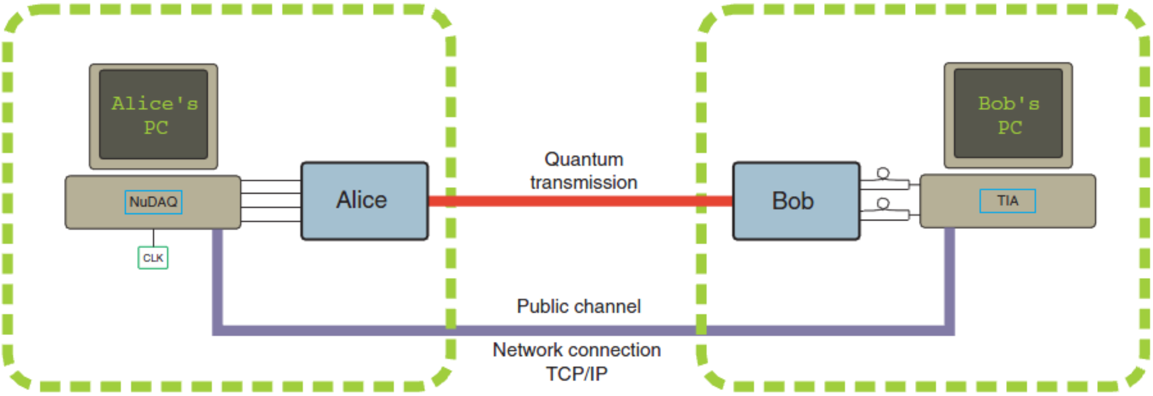


FIGURE 23 EXPERIMENTAL SET UP FOR KEY EXCHANGE

SOURCE [JD06]

Alice is "lightweight", i.e. with minimal processing capabilities; the design lends itself towards a Many-to-One relationship with Bob i.e. many Alices interacting with one heavyweight Bob. This asymmetric design of processing capacity opens up the possibility that Alice can be kept physically small and incorporated into a portable device such as a PDA, SIM or laptop.

This is exciting research: if "Alice" can be freed from the necessity of being in a controlled secure environment, attached to a QKD network with a fixed fibre optic cable, then the implementation possibilities of QKD are expanded dramatically, and could conceivably be relevant to a mass market. In fact, Professor Rarity has been quoted as saying:

> *"People will become as comfortable carrying their own personal quantum key, using it to secure all transactions by encoding their PIN, as they are with lasers in their DVD players" [SD09]*

8.3 Quantum Information as "Consumable"

Central to the thinking behind the statement above is the notion that key material derived through this free space technology should be regarded as a consumable – "quantum secrets" to be used once and discarded. (This is, of course, the exact requirement for a key in a one time pad.) In this case, however, these quantum secrets are designed to be stored on a small portable device or token carried by a user: once the secrets have been used up, a quantum top-up process needs to be undertaken to replenish the secret store (effectively a new QKD run with Bob).

8.4 Quantum ATMs

Figure 24 shows a mock up of the topping up process at a “Quantum ATM”. (In practice the free-space photon transfer is much more likely to be conducted over a shorter distance, but the photo provides a useful illustration of the principle.)

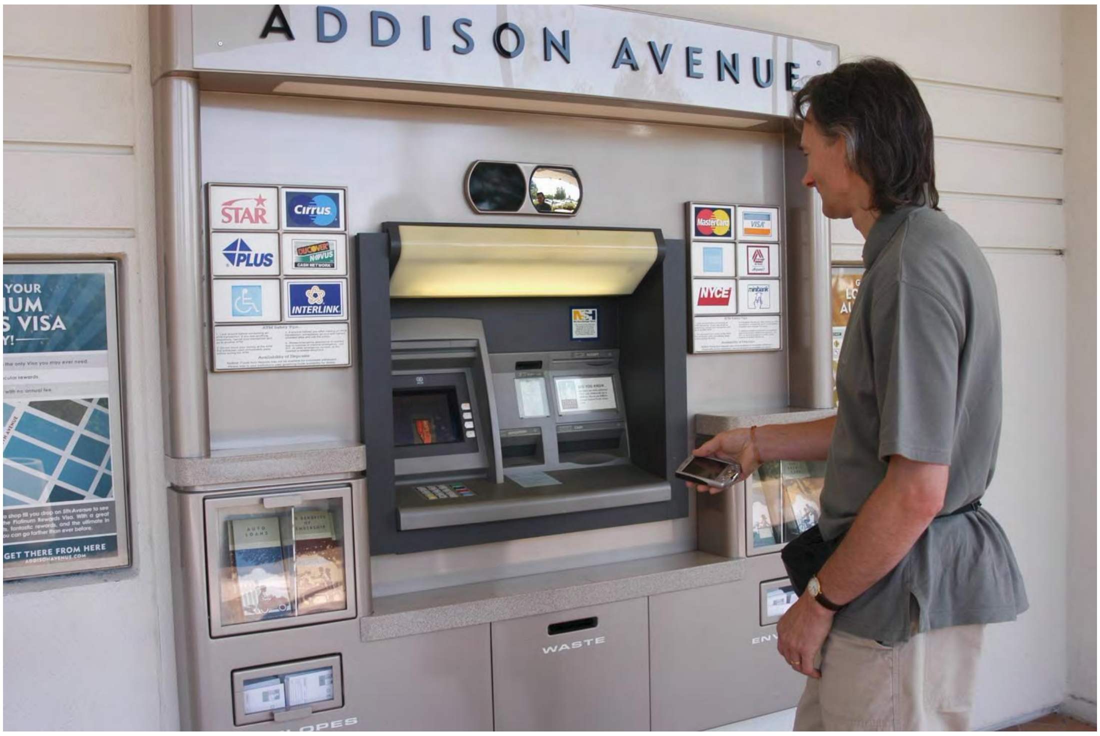


FIGURE 24 QUANTUM TOP UP

SOURCE [BM08]

Alice is the lightweight, portable token; Bob is the quantum ATM equipment. The Alice-Bob QKD link is an Access Node (QAN) to whatever network Bob is connected to, and there will be a requirement for nodes to be easy to use and available in sufficient numbers to minimize the inconvenience of the top-up process. For widespread use by the general public, piggy-backing the quantum equipment onto the existing ATM network has been suggested by the researchers [BM08] [JD06]. This has the advantage that people are generally familiar with the routine of going to an ATM regularly to obtain cash, and the quantum topping-up add-on should introduce an imperceptibly small overhead in the procedure.

8.5 Technical Issues

This quantum technique has great potential, but there are some issues which need to be addressed before the technology could become truly ubiquitous.

The quantum secrets need to be stored in a tamper-resistant component, such as a smart card, so that in the normal course of use, Alice will not be able to lose or damage them. However, with a large enough budget, plenty of time and some specialized equipment, it may be possible to extract some key information forensically.

Also, by its very nature, free space quantum optics interacts with the environment, and is sensitive to changes in the atmosphere. Ambient light levels, temperature and humidity will affect the efficiency of any information transfer. Research is being done in this area [KL09], but will not be discussed in this report.

The technology is at the developmental stage: proof of principle has been obtained, and research efforts are concentrating on reducing the size of the components so that they fit in a mobile device such as a PDA or smart phone.

Chapter 9 Potential Applications for QKD Systems

The preceding chapters have been concerned with the theory and research into quantum key distribution technology, and have shown that both QKD networks and low-cost short range QKD approaches have had some successes at the proof of principle stage of development. Now, in this chapter, it is time for some crystal-ball gazing in order to take a look at the potential of the fully fledged technology. This will be by no means an exhaustive list of applications; just enough areas will be considered to give a general flavour of the implementation options.

In the following discussion of the applications potential of QKD technology, there are some (not insignificant) assumptions to be made, to allow existing solutions to security issues to be directly compared with their putative quantum counterparts.

9.1 Assumptions

The analysis in this chapter will be done using the following assumptions:

- To allow a comparison on a "level playing field", classical solutions are described as they are now, but QKD technology has been fast-forwarded a few years to present a more mature, technically viable QKD environment
- All technical challenges have been overcome, and the performance of a QKD facility is at least as good as the classical equivalent, e.g. in terms of key distribution rates and reliability
- An implementation of QKD can be compared directly with an existing classical technique, and that the choice whether to use one or the other is solely down to security issues , and not necessarily cost
- Any infrastructure requirements are in place: e.g. Alice can top up her token with quantum secrets, and Bob has a quantum ATM.
- Public key cryptography is considered secure in the short to medium term, but not indefinitely: this is a pre-quantum computer world which will be examined

These are, of necessity, huge assumptions: to test whether the end result of QKD research is actually worth pursuing, this strange superposition of a quantum future and classical present provides the best mechanism for assessment. This is, in effect, a thought experiment – just like Schrodinger's Cat!

9.2 Networked Applications

9.2.1 Key Distribution in Classical Networks

The Internet is the biggest, most hostile classical network that cryptographic keys need to be distributed across. Secure key distribution is a challenge, but many protocols have succeeded, using symmetric and asymmetric cryptographic primitives appropriately. There are some examples in Appendix 1; other network-based authentication protocol examples are SSL, where key agreement procedures are negotiated in an initial handshake process between the communicating parties, and Kerberos where long-term keys between a user and Trusted Third parties (TTPs) are used to set up session keys for secure communications.

9.2.2 QKD Networks

The whole raison-d'être of QKD networks is to transfer keys between parties who wish to communicate securely. The networks are essentially "closed", as there are (not insignificant) barriers to joining, in terms of quantum channels, quantum optics equipment, key pre-sharing, and costs. This is in marked contrast to the freely available, "open" network that is the Internet.

The closed nature of QKD networks suggest that they are best suited to high security, controlled environments, where the trust scenario is well defined. So, Military, Intelligence, Government and Finance are areas where QKD could find a place. Transfer of the highest level cryptographic keys between Certification Authorities in a PKI system could also be a potential application arena.

QKD, when combined with OTPs or existing public key cryptography can result in very long term security: organisations which need this include Government and Intelligence agencies (for example, the Government's declassification period for sensitive documents is over 25 years, and advances in cryptanalysis may threaten security within this time period), or businesses with long-term strategic trade secrets which need to be kept confidential. Also, it has been suggested by Stebila et al. [DS09] that ATM networks could benefit from QKD, as it is expensive and time consuming to upgrade each ATM every time a cryptographic protocol is broken or becomes obsolete.

Closed Electronic data Interchange systems (EDI) within an industry, such as SWIFT and CHAPS which are used in high value banking transactions, may also benefit from the added security of QKD. In fact, QKD has already been used to safeguard financial transactions [WK04]: in 2004, money was transferred between Vienna City Hall and Bank Austria Creditanstalt – a donation of €3,000 from the Mayor of Vienna to the University of Vienna – using entangled photons in the cryptographic processing.

9.2.3 What Benefits will QKD bring?

Any super-secret data transfer which needs to be encrypted via a One Time Pad could use QKD generated keys: the specific property of QKD which is useful here is that a relatively short input to the initial authentication process can be used to generate information-theoretically secure key material ever after. This is essentially a key extension service, possible due to the universal composability of the QKD key which allows part of the QKD key output to be reused to authenticate subsequent protocol runs.

The key derived from QKD networks is independent of any inputs to the QKD protocols: this reduces the number of attack points in the system, so can increase security even if a hybrid system (QKD plus classical block ciphers such as AES) is used to encrypt messages.

9.3 Portable Applications and Infrastructure

Low cost free space QKD is arguably the more commercial option. Rather than concentrate on extending the range of QKD networks, by improving the efficiency of the quantum channels, it may make more sense to concentrate on *reducing* the operating distance of QKD! A token containing quantum secrets could be used as an access link to a quantum network like SECOQC, or be the entry point into a classical system: it will carry the benefits of unconditional security and eavesdropper detection into either.

Figure 25 shows an idealized usage pattern for this low-cost approach to QKD [BM08]. It shows the device interacting with an “Authentication Service Provider”, and various commercial transactions that may be enhanced by quantum secrets.

The original research highlighted three areas where QKD could be viewed as a solution to a business problem: anti-skimming; online banking security; and Cardholder Not Present (CNP) fraud. [BM08] .Quantum top-up infrastructure and associated procedures (detailed in section 8.4 previously) are essential here.

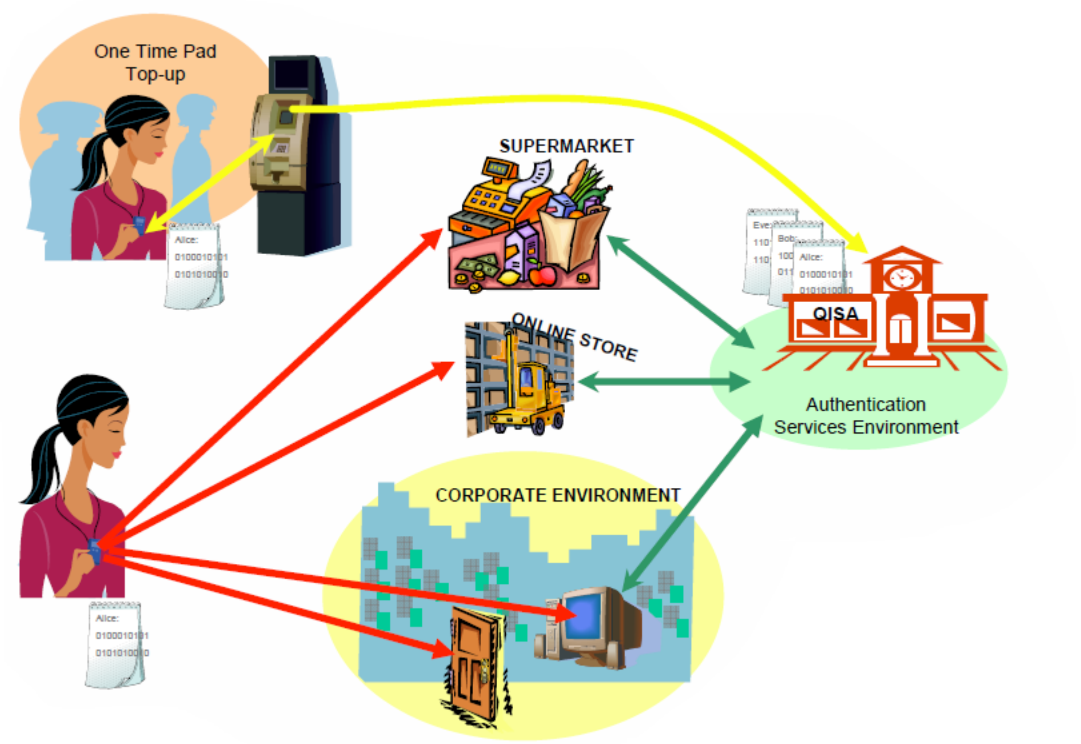


FIGURE 25 QKD AUTHENTICATION AND APPLICATIONS

SOURCE [BM08]

However, a word of warning: not everyone visits ATMs, as cash can be obtained from commercial outlets via cash-back schemes. Incorporating a quantum facility in chip and PIN readers is a much bigger implementation, with associated higher costs. This imposes greater commercial constraints on portable QKD technology.

9.4 Anti-Skimming in ATM Transactions

9.4.1 The Business Security Issue

A "skimming" attack occurs when a malefactor attaches some equipment to an ATM in order to detect and record electronic details from the magnetic stripe of plastic cards as they are used in the machine. Often a small camera is hidden on the ATM somewhere, to observe the PIN being entered. This information is then used to produce fake cards with genuine PINs, which can be used overseas in countries which have yet to upgrade to chip and PIN technology. [CW10]

A graph showing total cash machine fraud statistics is included in Appendix 2. The figures include losses due to card trapping devices (where the plastic card is fraudulently retained in the machine for later use) and shoulder surfing (where a bystander looks over the shoulder of the authorised user when entering a PIN). The losses peaked in 2004, and are now on the rise again, to £47.5 million in 2008. Any attempt to mitigate these losses will have a positive effect on banking profitability.

9.4.1 Classical Solutions

According to The UK Cards Association [CW10] there are some generic initiatives in place to deal with skimming attacks. These include: technology to make ATMs tamper proof, by redesigning the card reader surrounds so that it is difficult to attach malicious devices; encouraging cash machine owners to make regular inspections of the ATMs for evidence of tampering or unusual attachments; consumer advice, via notices and on-screen messages to raise awareness of the security issue; and the use of CCTV to deter attackers.

9.4.1 The QKD Solution

If a QKD link is "bolted on" to existing ATMs in the banking infrastructure, this provides the simplest way for Alice's quantum token to be used in practice. When Alice is physically at the quantum ATM, all the normal financial transactions (e.g. cash withdrawal, bill payment, statements) are available to her. The quantum secrets generated by a previous quantum top-up process are stored on Alice's token, and can be used to encrypt her PIN using a one time pad to allow access to these services, as suggested by the researchers.[BM08] [JD06].

9.4.2 What Benefits will QKD bring?

Skimming will become impossible if QKD processes are used. Eavesdropping of the quantum top-up will be detected, and the transaction aborted. Using a QKD generated quantum secret in a one time pad encryption ensures that the PIN cannot be recovered from intercepted messages later in system procedures.

However, the overall security of the system still relies on the security of the PIN. As mentioned before in this report, security is only as strong as the weakest part of the system [BS08a], so if Alice's storage of the PIN or the quantum secrets is sub-optimal – e.g. if the storage device is damaged, lost or otherwise compromised– then the system is instantly insecure, and no amount of OTP encryption or QKD can ever solve this.

9.5 Online Banking

9.5.1 The Business Security Issue

Online banking fraud is increasing (see Appendix 3 for a graph of the trend), not because bank systems are easy to break into – they are not. Instead, online banking users are targeted to get them to reveal sensitive information. Examples are: "phishing" emails which trick them into revealing secret password details; malware which sits undetected on a user's computer indefinitely, obtaining sensitive information by logging all keystrokes; or active attacks which redirect unsuspecting users to malicious websites which harvest their data.

9.5.2 Classical Solutions

This problem has prompted some banks to implement Two-factor authentication (TFA) schemes. These involve a dedicated card reader, into which the user inserts a (chip and PIN) bank card when prompted during an online banking transaction, and enters a PIN. The reader generates a unique one time password, which the user then enters to provide an extra level of authentication. From the bank's point of view, this ensures that the correct person is online and is making the transaction. [CW10] There are various versions of these authentication devices: for example, RSA's SECUREid [RS10] is a time-based device, which changes the one-time password every 60 seconds.

Another method of authentication (used widely in Germany) is the Transaction Authorisation Number (TAN) scheme. TANs are essentially a printed list of 6 digit numbers issued to bank customers, which are used to authenticate transactions online, in conjunction with a PIN [GE10]. A PIN is no use without a TAN, and vice versa. This system has been extended to an "Indexed" TAN (iTAN), where the bank requests a specific number from the list, and Mobile TAN (mTAN) where the TAN is sent to the customer's mobile phone during the transaction. However, there are security weaknesses in this approach: man-in-the-middle attacks are particularly effective, as are phishing attacks asking for TAN information [JK09a]. Criminals are also paying high prices for old Nokia 1100 mobile phones, which can be re-programmed to use someone else's phone number, and hence receive their mTANs [JK09b].

Banks have also implemented intelligent fraud-detection systems, to highlight unexpected spending patterns (which are thus potentially fraudulent). This enables the bank to contact the customer and verify if a particular transaction is genuine or not.

9.5.3 The QKD Solution

Two-factor authentication procedures can be adapted to add quantum processing to online banking transactions. To supplement the quantum top up procedure, a handheld device capable of reading the stored quantum secrets would need to be issued to every on-line banking customer. (Existing devices could be used if the quantum secrets were stored in the EEPROM area of a smart card, for example). Once the token is communicating with the reader, the next available quantum secret on the token can be used to encrypt the transaction data to give a onetime password. Bob (the bank) can use his knowledge of the quantum secrets and the transaction to perform the same encryption, and check the result against Alice's entry before allowing the transaction to continue.

9.5.4 What Benefits will QKD bring?

The quantum option outlined above would be equivalent to existing TFA systems when using the banking site, with the added advantage that the keys used are truly random. The disadvantage is that the quantum top-up procedure would limit the number of times this could be done without a visit to a bricks-and-mortar bank facility.

However, this use of quantum secrets is an exact equivalent to the TAN system. TAN lists are obtained separately from the bank, independently of the online transaction. By employing a QKD token to store and use quantum secrets in a transaction, this becomes effectively a "Quantum TAN" (qTAN). Encrypting the user's transaction details with this qTAN and a one time pad, will defeat phishing attacks, because even if all the account and PIN details have been inadvertently revealed, and an attacker gets access to the account, they won't actually know what the qTAN is. The user doesn't know what the qTAN is either, as it's securely stored in the quantum token, so it can't be disclosed in a phishing attack. The attacker will therefore be unable to use the other information gained to conduct a fraudulent operation.

9.6 Card Holder Not Present (CNP) Fraud

9.6.1 The Business Security Issue

The Cardholder Not Present (CNP) scenario occurs every time a purchase is made from a supplier over the internet: card holder details are entered online, with the supplementary security code on the back of the physical card (the CVV number), and there is an implicit trust that these sensitive details will be used correctly by the supplier. (Chip and PIN technology cannot help in this model, as the two parties to the transaction are physically separated.)

Cardholder details can be obtained illicitly through many routes: for example, key-loggers recording the keystrokes of the user, phishing sites which entice the unwitting into parting with their sensitive data at an unauthorised and misleading site, social engineering and plain old theft. Once compromised, cardholder numbers and CVVs can be traded wholesale on the black market in so-called "carding" networks and used to obtain goods and services illegally.

The costs of CNP fraud are borne wholly by card providers and financial institutions: in 2008this was £328.4 Million [CW10], an increase of 13% over 2007. Inevitably these costs are passed on to customers indirectly: a workable safeguard against this type of fraud will therefore be beneficial to all.

9.6.2 Classical Solutions

There are schemes in action currently which add a further level of security to online payments: the VISA PIN card [VI08] includes a display panel on the card to show a one-time-password; the "Verified by VISA" scheme [VI10], uses additional security questions to complete a purchase. There are security weaknesses remaining, though – key loggers and phishing are still effective types of attack.

9.6.3 The QKD Solution

Using QKD based quantum secrets in an internet two-factor authentication process is a variation on the online banking scenario. The difference is that the online store does not have access to Alice's quantum secrets, so will have to send encrypted transaction details to Bob (the bank) for authorisation. Alice follows the same process as for online banking, using the transaction data, a QKD reader, and her quantum token/ PIN. Bob (the bank) performs the same calculation in order to send an accept/reject message to the retailer.

This is, of course, not perfect: Alice and Bob may have synchronization issues; Bob may be offline; and error conditions such as Alice running out of secrets or lost messages need careful handling. It does, however, possess the TFA advantage - the credit card information is not enough on its own to complete the transaction.

9.6.4 What Benefits will QKD bring?

Alice and Bob have pre-shared a secret, so have a trust relationship. The token has to be in the Alice's possession (the transaction initiator) in order for the authorization to be successful, thereby rendering the information used by carding communities insufficient for large scale fraud to be perpetrated. There is, of cause still an issue if the quantum token has been physically removed from Alice: anyone with a token in their hand can use it online. That is why the procedures for secure issuing and dealing with lost and stolen cards have to be extremely efficient.

Specific QKD benefits are that the keys are not available to an attacker via phishing or key logging, and the transaction details encrypted via a one time pad cannot be retrieved. The disadvantage is that, again, unlimited card use isn't possible, as a visit to a quantum ATM will be necessary at some stage.

9.7 General Authentication within a Corporate Environment

9.7.1 The Business Security Issue

Online banking and CNP situations are special cases of the generalised problem of authentication. How do you prove that the person/ computer/ entity is the one they claim to be? Authentication is based on "something you know", "something you have" or "something you are". Possession of a quantum token is "something you have", combined with a PIN ("something you know") so are suitable for use in an authentication procedure. (Once authentication is complete, the next stage is authorisation –are the actions being attempted allowable?)

In a corporate environment, authentication needs to be fairly strict: for example it is not good practice to allow unauthorised personnel access to buildings, which can happen if entry and exit points do not have adequate authentication procedures. Lack of authentication can therefore pose severe security problems.

9.7.2 Classical Solutions

There are many existing authentication schemes. Examples are: biometrics for access control; security guards at doors; password log-ins; single-sign-ons; challenge and response tokens (TFA schemes as discussed previously). All are designed to make users demonstrate their credentials before they can be authorised to perform any task. The choice of authentication mechanism depends on the application: it is not appropriate to have a time consuming biometric process at an entrance with a high throughput of personnel, for example.

In all authentication systems, off-line procedures are necessary to deal with lost/forgotten tokens, and off-site working: a basic information security requirement, but often a weak point in the overall security framework.

9.7.3 The QKD Solution

Alice's quantum token could be use to authenticate her, and to provide access control across the organisation, if Bob is used as an authentication server. Quantum topping-up at special access points would ensure that only authorised personnel were furnished with a supply of quantum secrets. These could then be "consumed" in an access control system to limit the employee's access both to information resources and physical areas of the site.

In extremely high security environments, it would be more appropriate to restrict this quantum authentication process to a physically separate quantum network, maybe combined with another authentication factor such as a biometric. Once authenticated, the derived quantum secrets can be used in standard access control procedures.

9.7.4 What Benefits will QKD bring?

QKD topping up adds an extra layer of security into an authorisation procedure: however, there is still the issue of lost, stolen, forgotten or lent tokens to consider. (This is a problem not specific to QKD.) Although, if QKD secrets were used to encrypt biometric data for use as an authentication code (the ultimate in high security access control!), then the authorised user would always have to be present in person to get access privileges and the token could not be lent to another person.

9.8 E-voting

9.8.1 The Business Security Issue

Elections have a number of areas which could be improved: reducing electoral fraud, increasing electoral turnout, improving efficiency in the registration and counting processes to name a few. The Electoral Reform Society [ER10] suggests a number of other changes which could be made to voting systems worldwide: e-voting, where voting can be done by text, internet or digital television (!) is *not* currently one of their recommendations, due to concerns about security, anonymity and authentication of the voter.

9.8.2 Classical Solutions

There have a been many suggestions for e-voting systems, ranging from touch screen voting at a polling station [ER10], to the use of mobile telephony as a suitable infrastructure [YF06], to a cryptographic scheme to ensure votes were counted properly [EN09]. None has been adopted in practice.

9.8.3 The QKD Solution

QKD has already been applied in the e-voting arena in 2007. [EM07] QKD was used in the voting process in Geneva, employing idQuantique's Cerberis product [IQ10c] to protect the voting data once it had been manually counted. Ballot information was encrypted using QKD-generated keys, and sent over a fibre-optic link between the central ballot counting station to the Government data centre. So this is not actual e-voting, merely safeguarding the results. The Geneva State Chancellor, Robert Hensler, said QKD was used

> *"... to provide optimal security conditions for the work of counting the ballots. In this context, the value added by quantum cryptography (sic) concerns not so much protection from outside attempts to interfere as the ability to verify that the data have not been corrupted between entry and storage"*

There is no reason, however, why QKD could not be part of a true e-voting system. For example, using a token which is topped up with quantum keys at a specialised infrastructure point, where other credentials such as a birth certificate are examined, will cut down the opportunities for casual impersonation attacks. Its impact on voter turnout might be undesirable, however, as adding a time consuming process to an election will not encourage participation.

Potentially, QKD derived quantum keys could be used in blind signatures processes common to many e-voting proposals which ensure anonymity of voters.

9.8.4 What Benefits will QKD bring?

E-voting is a contentious area, and it is unwise at this stage to attribute any benefits to QKD systems when classical ones have not reached universal acceptance. Once a recognised standard has been achieved, then QKD may be able to play a part in enhancing security levels.

9.9 Commercial Prospects

For a technology to become successful commercially, it must solve a business problem, save money or make an existing procedure more streamlined. In the words of Sheahan [PS09], these commercial imperatives are “Fast, Good, Cheap... and then add something extra”. “Fast” speaks for itself: both the technology and the service offered by the corporation promoting it must be slick and efficient. “Cheap” really means that the cost of the goods/ services provided *appears* to be good value for the level of quality obtained. The absolute cost value may be higher than a competitor’s equivalent pricing, but here it is the *perception* which is important.

“Good” in the security world is, however, difficult to define. Does it mean cryptographically secure? Or more intuitive so that it will actually be used properly? Future-proof? Easier to implement? What’s “Good” for one environment may be wholly inadequate for another. Even if a technology passes the “Fast, Good, Cheap” test, it must be acceptable to the general public if they are to use it successfully: equally, the business community must deal with any disadvantages it brings. These acceptability issues will now be considered.

9.9.1 Acceptability by General Public

There are parallels between implementing QKD technology on tokens and the roll-out of chip and PIN technology .When chip and PIN was introduced to the general public in 2004, an extensive education programme was necessary to reinforce the need for the user to remember a PIN and keep it secret: the security of the system depends on only the authorised person knowing the PIN. And, as the PIN is only 4 digits, the possibility of a brute force trawl through all potential values is a relatively simple task, so additional measures were added to prevent this (three failed attempts result in the card being locked out). The onus is on the user to use the PIN correctly, so facilities to change the value to a more memorable one minimize the likelihood that the PIN will be forgotten. Special arrangements had to be made for people with disabilities who couldn't use PINs: chip and sign cards are used instead.

As the technology was more widely deployed, and ATMs became more common, attackers targeted the machines to steal PIN information, either by adding bogus equipment to the ATM, or simply looking over the shoulder of an innocent user. The education programme therefore had to be extended to warn people of these dangers. This technology is now so common-place that its usage is second nature to the public: no PIN, no payment. This was helped by the fact that entering a PIN merely replaced another process, which involved adding a signature to the transaction receipt, authorizing the payment manually (which had been open to abuse). The overall transaction time was not significantly lengthened.

Having a 'personal quantum key' introduces a new concept to the general public, in the U.K., at least. Although it could be regarded as on a par with the introduction of chip and PIN technology to secure credit and debit card transactions, it actually represents a culture shift in usage. Instead of regarding a payment card as a fixed and immutable object which can be used at will, the necessity of an intermittent quantum top up process immediately reduces its user-friendliness by adding an extra step in the usage procedure – and one which must be performed at a specialized physical location. It effectively reduces the capabilities of the payment card with quantum key to that of a species of pre-paid card, where a maximum number of transactions can be completed (irrespective of transaction value) before external intervention is required.

The consumer experience in Germany and other countries which use the TAN system of authentication is somewhat different. Here, an extra stage in an online transaction, where a TAN is used from a pre-supplied list from a bank, could be seamlessly replaced by a quantum TAN facility (equipment and infrastructure allowing). As procedures already exist for TANs, the introduction of quantum elements may not be regarded as such an overhead in usage.

Additionally, there must be stringent procedures for the initial set up of a quantum token, the replacement or destruction of lost/stolen/compromised quantum tokens and final deactivation once their useful life is over, which should be no more onerous than current procedures for bank cards.

But, there is always the danger that the general public will vote with their feet if they are presented with an unpalatable technology which makes their day-to-day life more difficult. The quantum top-up process is an added burden on existing transaction procedures: whether the benefits which arise from more secure online banking and internet transactions are perceived to be worth the added chore of extra ATM visits will depend greatly on the education and awareness programme businesses adopt. The added security is of more interest to financial institutions than the general public, so QKD is not a technology that the general public is clamouring for. This is a “push” technology, not a “pull”. If, on its introduction, the supporting procedures are made as simple as possible and explained well, mass market use would be possible - albeit with a fairly intensive investment in infrastructure, equipment and education. It may be that this corporate investment could be better spent developing less radical technologies to fulfil the same business functions.

9.9.2 Possible Usage Issues

There is no technical reason why the ‘personal quantum key’ should be confined to matters financial. If, however its use is extended to act as in some sort of personal identifier, then civil liberties implications will have a marked impact on its acceptability. This could be construed as a centralized ID scheme being introduced by the back door (albeit without ID cards per se). This is anathema to civil libertarians, as a centralized facility could be used to check and track individuals’ actions. Additionally if the token is also used as a dual identity/ financial authorization device then there is a danger that those whose financial affairs are not under control will be denied the identification facility and an underclass of the disadvantaged will be born. Safeguards to prevent the misuse of tokens (e.g. being lent to friends) would have to include a way of tying the token to a person’s identity. Adding biometric data to the quantum token would reduce this problem, but may further diminish the token’s acceptability in civil libertarian terms.

9.9.3 Acceptability by Business

There is no denying that implementing QKD systems will cause businesses to incur extra costs. Infrastructure, quantum equipment, new procedures all add to the financial toll, and ultimately the business decision whether to adopt this new technology will boil down to a cost/benefit analysis.

Costs are measured in hard cash and working hours for personnel: benefits however can be intangible as well as squarely aimed at the balance sheet. Cryptographical issues aside, there may be reputational advantages for an organisation if they adopt QKD technology: implementing the newest, coolest technology makes a business seem "cutting edge", and perception can sometimes outweigh actual facts.

There will be applications where QKD is ideal – replacing trusted couriers, for example – and others where the benefits are not so clear – e.g. CNP and online banking, which need a huge quantum ATM infrastructure to allow it to work, but get added security as a result. Business decisions are never easy!

There is a confidence in the QKD equipment supplier world that there is a market for their goods: Andrew Shields of Toshiba Research Labs, commented on a new photon detector they had developed (which can handle a bit rate of 1Mbit per second over 20km of fibre and thus increase the number of users over that stretch of network) and said it "means we could have 8,000 users and the technology starts to become very useful"[CEP09]. But time will tell if there is a volume market for QKD.

Chapter 10 Conclusion

Every now and then, a technology or invention comes along which changes the face of business: something with un-looked for benefits which experiences explosive commercial growth. Examples of this phenomenon, termed “Black Swan” by Taleb [NT08], are the Internet, mobile phone texting, and Harry Potter (!). Black swans are hard to predict from past events, as they occur so infrequently. Is the technology of QKD a black swan? Will it cause a cataclysmic upheaval in the world of cryptography? On the evidence presented in this report, the answer is probably “No”.

This report has delved into the mysteries of quantum theory in order to understand the claims that QKD protocols give unconditional security based on the laws of physics alone, and analysed the most common protocols in some depth. Potential weaknesses in the protocols have been highlighted, notably the point-to-point nature of the quantum links, the limited distance quantum optic signals can travel along these links, and attacks which target the non-ideal production of the polarised photons which carry the key information. This shows that the technology is still a little fragile. QKD protocols don’t have the testing history of conventional cryptographic primitives – many talented people have examined and attacked DES and AES, for example, without (as yet) finding any significant flaws.

A networked solution, the SECOQC project, was outlined. This uses quantum key distribution within an extensive classical infrastructure, providing an excellent research opportunity to design a new type of network architecture to cater for the demands of quantum key distribution, notably resulting in new network protocols and a dedicated key management system known as the “network of secrets”. This was followed by some interesting research into low-cost QKD, and then an examination of commercial possibilities of networked and low cost QKD was conducted.

The overall conclusions that can be drawn from this study are somewhat mixed.

Commercial success for a technology occurs when the *perceived* benefits of adoption outweigh the costs. Perceived is the operative word here – if an organisation thinks that by using the most up-to-date techniques, whatever the financial cost (or indeed, its effectiveness), they will gain a degree of kudos as an early adopter, this intangible benefit may be seen as a means to competitive advantage. Benefits do not have to be measured in financial, efficiency or even cryptographic terms: this could be seen from the quoted remarks in section 9.8 when QKD was used in the Swiss voting system. The actual processing could have been done just as easily with a classical integrity checking mechanism, but it was somehow seen as “better” because a cutting edge procedure was used.

The main problem QKD faces is that all potential application areas identified for it already have perfectly serviceable “classical” alternative methods of achieving the security levels required. It would be a brave executive indeed who attempts to justify the costs of installing expensive new equipment and changing existing systems so that extremely good security can be upgraded to (claimed) perfect security. Of course, some applications may benefit from the additional security of QKD, especially if their current incarnation has weaknesses – for example, TANs used in German banking – but the commercial imperative may not be there if cheaper classical solutions exist. It is a harsh economic reality that “good enough” is invariably cheaper than “perfect”, and the cost and consequences of adopting one route rather than the other has to be managed as part of an organisation’s overall risk portfolio.

Had QKD been a fully fledged cryptographic primitive when chip and PIN systems were rolled out in February 2006 [CH10] for example, it would have been a relatively easy task to include the quantum technology in the infrastructure by bolting on a module or two in the chip and PIN readers. Conversely, if quantum computers were currently sophisticated enough both to endanger the security levels provided by asymmetric cryptography and to provide quantum relays for quantum networks, this would mean that QKD could provide a seamless transition to post-quantum computing cryptographic key establishment. Unfortunately, neither of these scenarios is in place, leaving QKD in the strangest commercial position. It has arrived in the commercial sphere both too early and too late – a cruel irony for a quantum technology to be placed in such a superposition of commercial alternatives.

However, there is a place for the features QKD offers, co-existing peacefully alongside classical cryptographical methods, not as a replacement. As Stebila et al. [DS09] elegantly state, the cryptographic landscape can change as asymmetric schemes are re-tooled in preparation for the quantum computing era. Even when a fully functioning quantum computer becomes practical, symmetric cryptography will still be useable, albeit with key lengths doubled. It may be that research effort should be redirected away from attempts to extend the maximum length of a quantum channel [VS09a], and wait in the wings until quantum repeaters become available for use in quantum networks. Instead, short range QKD could be developed as a niche market, for consumer applications.

Of course, there are still applications which need the perfect security a one time pad encryption can give, and QKD is especially good at creating long random keys from a short input – key extension functionality which could be invaluable for OTPs.

Although absolute confidence in QKD's security may be slightly misplaced at the moment, it is most certainly an area which merits further research. Bruce Schneier's description - "awesome [but] pointless" – is not 100% true. "***Awesome***"? Definitely. Using fundamental quantum mechanical phenomena to provide unconditional, eavesdropper-proof security is awesome by any standard. "***Pointless***"? Not totally. If QKD is used in carefully selected applications, alongside existing classical cryptography, then there could well be a commercial future for this technology.

The cryptographic world may not be turned upside down by Quantum Key Distribution – it's no black swan – but it should ultimately find its niche amongst the fundamental building blocks of cryptography.

Bibliography

AB09 A. Broadbent, J. Fitzsimons, E.Kashef, ”Universal Blind Quantum Computation”, arXiv: quant-ph/0807.4154v3 ,12 Dec 2009

AD10 A. R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe and A. J. Shields, “Continuous operation of high bit rate quantum key distribution”, *Appl. Phys. Lett. 96*, 161102, 2010

AE05 A. Einstein,” On a Heuristic Viewpoint Concerning the Production and Transformation of Light”*, Annalen der Physik* 17: pp.132–148, 1905

AE06 A. K. Ekert, “Quantum Cryptography”, Chapter 1, Quantum Communications and Cryptography, ed. A.V. Sergienko, Taylor and Francis, 2006

AE35 A. Einstein, B. Podolsky and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete? “, *Phys. Rev*. 47, 777—780, 1935.

AE47 A. Einstein to M. Born, 1947, 'The Born-Einstein Letters' Max Born, translated by Irene Born, Macmillan, 1971

AE91 A. K. Ekert, “Quantum cryptography based on Bell’s Theorem”, *Phys. Rev. Lett*. **67**, 661, 1991.

AK83a A. Kerckhoff: "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan. 1883

AK83b A. Kerckhoff, "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 161–191, Feb. 1883

AM01 A. J. Menezes, P. C .van Oorschot, S.A .Vanstone, “Handbook of Applied Cryptography”, 5th Edition, CRC Press, 2001
Available online at http://www.cacr.math.uwaterloo.ca/hac/

AP08 A. Poppe, M. Peev, O. Maurhart ,”Outline of the SECOQC Quantum Key Distribution network in Vienna”, *International Journal of Quantum information Vol 6 no 2*, arXiv: quant-ph /0804.0122v1, April 2008

AT07 A. Thomas, “What is Reality”, http://www.ipod.org.uk/reality/index.asp, 2007

BM08 B. Munro, J. Duligall, M. Godfrey, K. Harrison, A. Lynch, J. Rarity, T. Spiller, “Consumer QKD, Protecting the future”, Hewlett Packard, University of Bristol, SECOQC, available online at
http://www.brl.ntt.co.jp/tqc/2008/doc/program/consumer.pdf ,March 2010

BR10 http://blogs.reuters.com/commentaries/2009/08/11/twitter-backlash-foretold/
March 2010

BS08a B. Schneier, Interview,
http://www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016 March 2010

BS08b B. Schneier, “Schneier on Security” ,Wiley Publishing Inc, 2008

CB08 C. Branciard, N. Gisin, B. Kraus, V. Scarani, “Security of two quantum cryptography protocols using the same four qubit states”, arXiv: quant-ph/0505035v2 Sept 2005, dated Feb 1st 2008 on report

CB84 C. H. Bennett, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pp. 175-179,1984

CB88 C. Bennett, G. Brassard, J-M. Robert, “Privacy amplification by public discussion”, *SIAM J. Comput.*17 210–29, 1988

CB92a C. Bennett, F. Bessette, G. Brassard, L. Savail, J. Smolin, “Experimental Quantum Cryptography”, *Journal of Cryptology,* vol. 5 no 1, p3-28, 1992

CB92b C. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States”, *Phys. Rev. Lett*. 68 (21) p3121-3124, 1992

CB92c C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography Without Bell's Theorem", *Phys. Rev. Lett.*68, 557-559, 1992

CE02 C. Elliot, ”Building the Quantum Network”, *New J. Phys. 4 (2002) 46. 1-46.12,* 2002

CE06 C. Elliot, “The DARPA Quantum Network”, Chapter 4, Quantum Communications and Cryptography, ed. A.V. Sergienko, Taylor and Francis, 2006

CE-P09 C. Evans-Pughe, “Network of Standards”, *Institute Of Engineering And Technology* , Feb 2009 available online at http://kn.theiet.org/magazine/issues/0903/network-standards-0903.cfm

CF09 C-H.F. Fung, K. Tamaki, B. Qi, H.-K. Lo, X. Ma, “Security proof of quantum key distribution with detection efficiency mismatch” *Quantum Inf. Comput. 9*, 131, 2009

CH10 http://www.chipandpin.co.uk , June 2010

CS10 C. L. Salter, R. M. Stevenson, I. Farrar, C. A. Nicoll, D. A. Ritchie, A. J. Shields “An entangled –light-emitting diode”, *Nature 465*, 594-597, June 2010. Doi:10.1038/nature09078

CS49 C. E. Shannon, “Communication Theory of Secrecy Systems*”, Bell System Technical Journal*, vol. 28, pp 656-715, 1949

CW10 www.cardwatch.org.uk “Fraud the Facts” , 2010

DC03 D. Collins, N. Gisin, H. de Riedmatten, “Quantum Relays for Long Distance Quantum Cryptography”, arXiv :quant-ph/0311101, 2003

DD85 D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer". Proceedings of the Royal Society of London; Series A, Mathematical and Physical Sciences 400 (1818): pp. 97–117, July 1985

DM98 D. Mayers, “Unconditional Security in Quantum Cryptography”, arXiv: quant-ph/9802025, 1998

DS09 D. Stebila, M. Mosca, N. Lutkenhaus, “The case for quantum key distribution”, arXiv: quant-ph/0902.2839, February 2009

DSt09 D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin**,** H. Zbinden, S. Gray, C. R. Towery, S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres” *New J. Phys. 11* 075003, 2009 available online http://iopscience.iop.org/1367-2630/11/7/075003

EB06 E. Biham, M. Boyer, P. Boykin, T.Mor, V Roychowdhury, “A Proof of the Security of Quantum Key Distribution”, *Journal of Cryptology* 19, 381-439, arXiv: quant-ph/0511175v1, 2006

EM07 E. Messmer, Quantum Cryptography to secure ballots in Swiss election, Network world, 2007, available online at http://www.networkworld.com/news/2007/101007-quantum-cryptography-secure-ballots.html

EN09 E. Naone, “First test for election cryptography”, *Technology Review*, November 2009, http://www.technologyreview.com/web/23836/

ER10 http://www.electoral-reform.org.uk/article.php?id=45 June 2010

ES26 E. Schrodinger, "Quantisierung als Eigenwertproblem (tr. “Quantization as an Eigenvalue Problem”), *Annalen der Physik* 79 (6): pp.489-527, 1926

EW02 E. Waks, A. Zeevi, and Y. Yamamoto,” Security of quantum key distribution with entangled photons against individual attacks”, *Phys. Rev. A* 65 052310, 2002

FX10 Feihu Xu, Bing Qi, Hoi-Kwong Lo, “Experimental demonstration of phase-remapping attack in a practical quantum key distribution system” arXiv: quant-ph/1005.237v1, May 2010

GB00 G. Brassard, N. Lutkenhaus, T. Mor, B. Sanders, “Limitations on Practical Quantum Cryptography”, *Phys. Rev. Lett.* 85, p1330-1333, 2000

GB06 G. Brassard, ”Brief History of Quantum Cryptography: A Personal Perspective” based on *Proceedings of the IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security,* Japan Oct 2005, arXiv: quant-ph/0604072v1 April 2006

GB09 G. Berlın, G. Brassard, F. Bussieres, N. Godbout, J. A. Slater, W. Tittel “Flipping quantum coins” arXiv: quant-ph/0904.3946v2 1 May 2009

GE10 Association of German Banks website , June 2010 http://www.german-banks.com/html/19_consumers/consumers_04_2.asp

GM65 G. Moore, “Cramming more components onto Integrated Circuits”, *Electronics*, Volume 38, Number 8, 1965

GV26 G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", *Journal of the IEEE*, Vol 55, pp109-115, 1926

IQ10a http://www.idquantique.com June 2010

IQ10b http://www.idquantique.com/network-encryption/qkd-security.html, May 2010

IQ10c http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html June 2010

JB09 J. Bernstein, “Quantum Leaps”, The Belknap Press of Harvard University Press, 2009

JB64 J. Bell, “On the Einstein Podolsky Rosen Paradox”, *Physics* ***1***, *195-200, 1964*

JC79 J. L. Carter and M. N. Wegman, “Universal hash functions”, *J Comp Syst. Sci* 18, 143-154, 1979

JC98 J. Cirac, P. Zoller, and H. Briegel, “Quantum Repeaters based on Entanglement Purification”, eprint: arXiv :quant-ph/9808065, 1998

JD06 J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, J. G. Rarity, “Low cost and compact quantum key distribution”, *New Journal of Physics* 8 249, 2006

JF09 J. Fenn, M. Raskino, B. Gammage, “Gartner’s Hype Cycle Special Report for 2009” available online http://www.gartner.com/resources/169700/169747/gartners_hype_cycle_special__169747.pdf

JK09a J. Kirk, “German Police: Two-factor authentication failing”, *Network World*, 2009 http://www.networkworld.com/news/2009/032409-german-police-two-factor-authentication.html

JK09b J. Kirk, “Nokia: We don’t know why criminals want our old phones”, 2009 http://www.pcworld.com/businesscenter/article/163515/nokia_we_dont_know_why_criminals_want_our_old_phones.html

JL10 J Leyden, “Quantum crypto boffins in successful backdoor sniff”, The Register, http://www.theregister.co.uk/2010/05/18/quantum_crypto_attack/ May 2010

JM01 J. Manger, “A chosen ciphertext attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as standardized in PKCS #1 v2.0”, *Advances in Cryptology , Crypto 2001,* LNCS 2139, pp. 230-238,Springer-Verlag, 2001

JP02 J. Polkinghorne, “Quantum Theory: A Very Short Introduction”, Oxford University Press, 2002

KB02 K. Bostrom and T. Felbinger ,”Deterministic Secure Direct Communication Using Entanglement”, *Phys. Rev. Lett*. 89 187902, 2002

KL09 K. Lessiak, C. Kollmitzer, S. Shauer, “Statistical Analysis of QKD Networks in Real-Life Environments”, *2009 Third International Conference On Quantum, Nano And Micro Technologies*, IEEE, 2009

KP09 K. G. Paterson, F. Piper and R. Schack, “Quantum cryptography: a practical information security perspective”, arXiv: quant-ph/0406147v2, Aug 2009 (Formerly “Why Quantum cryptography?”, 2004)

LG97 L. Grover, “Quantum Mechanics Helps in Searching for a Needle in A Haystack”, *Phys. Rev. Lett* 79,:p325-328, 1997

LS04 L. Salvail and C. Schaffner, Requirements for security architectures (Rough network architecture for quantum communication applied to basic scenarios), SECOQC Deliverable D-SEC-17, Oct 2004

MB02 M. Buchanan, ”Small World”, Weidenfeld Nicolson, 2002

MB94 M. Bellare, P. Rogaway, “Optimal asymmetric encryption - how to encrypt with RSA”, *Advances in Cryptology – Eurocrypt ’94,* LNCS 950, pp 92-111, Springer-Verlag, 1994

MC04 M. Chown, “Einstein’s Rio requiem”, *New Scientist magazine issue* 2437, March 2004 available online at http://www.newscientist.com/article/mg18124375.900

MC07 M. Chown, “Quantum Theory Cannot Hurt You: A Guide to the Universe”, Faber and Faber, 2007

MC10 M. Chown, “Entangled photons available on tap”, New Scientist , 02 June 2010 http://www.newscientist.com/article/dn18990-entangled-photons-available-on-tap.html

MD07 M. Dianati, R. Alleaume, “Transport Layer Protocols for the SECOQC Quantum Key Distribution (QKD) Network”, *32nd IEEE Conference on Local Computer Networks*, 0742-1303/07, IEEE 2007

MD08 M. Dianati and R. Alleaume , “Architecture of the SECOQC Quantum Key Distribution network”, arXiv: quant-ph/0610202v2 25 Oct 2006, Report dated 1st Feb 2008

MK06 M. Kaku, “Parallel Worlds”, Penguin, 2006

MK08 M. Kaku, “Physics of the Impossible”, Allen Lane, 2008

MM08 M. Mosca, Alain Tapp, R. de Wolf, “Private Quantum Channels and the Cost of Randomizing Quantum Information”, arXiv: quant-ph/0003101v2, March 2000

MM09 M. Mosca, D Stebila, “Quantum Coins” arXiv: quant-ph/0911.1295v1/Nov. 2009

MP01 M. Planck, “Uber das Gesetz der Energieverteilung im Normalspectrum*”,Annalen der Physik* 309 (3), pp.553-563, 1901

MP08 M. Peev, M. Nolle, O. Maurhardt, T. Lorunser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, and A. Zeilinger, “A Novel Protocol-Authentication Algorithm Ruling Out a Man-in-the-Middle Attack in Quantum Cryptography”, arXiv: quant-ph/0407131v1 16 Jul 2004, dated Feb 1st 2008 on report

MP09 M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J .Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shield, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R .Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I .Wimberger, Z. L. Yuan, H. Zbinden, A. Zeilinger,” The SECOQC quantum key distribution network in Vienna”, *New J. Phys. 11* 075001, 2009

MW81 M. Wegman, J. Carter, “New hash functions and their use in authentication and set equality", *Journal of Computer and System Sciences,* Vol.22, pp.265-279, 1981

NB13 N. Bohr, “On the Constitution of Atoms and Molecules part I”, *Philosophical Magazine 26*: pp.1–24, 1913

NG02 N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, “Quantum Cryptography*”, Review of Modern Physics,* Vol 74 No 1, pp145-194, 2002

NG05 N. Gisin, S. Fasel, B.Kraus, H. Zbinden, G. Ribordy, ”Trojan Horse attacks on Quantum Key Distribution systems”, arXiv: quant-ph/0507063v2, 2005

NI05 Originally http://www.nist.gov/public_affairs/colloquia/20050328.htm
Also used on the cover of earlier editions of John Gribbin's Book "In Search Of Schrodinger's Cat", Bantam Books, 1984

NI10 http://www.nikon.com/about/feelnikon/light/chap04/sec01.htm, March 2010

NK04 N. Koblitz, A.J. Menezes, “Another look at provable security” http://eprint.iacr.org/2004/152.pdf , 2004

NK06 N. Koblitz, A.J. Menezes, “Another look at provable security II”, http://eprint.iacr.org/2006/229.pdf , 2006

NL00 N .Lutkenhaus, “Security against individual attacks for realistic quantum key distribution”, *Phys. Rev. A* 61 052304, 2000

NL02 N. Lutkenhaus, M. Jahma, “Quantum key distribution with realistic states: photon-number statistics in the photon number splitting attack”, *New Journal of Physics 4* 44.1-44.9, 2002

NT08 N. N. Taleb, “The Black Swan: The Impact of the Highly Improbable”, Penguin 2008

OM05 O. Maurhart, P. Bellot, M. Riguidel and R. Alléaume, Network Protocols for the QKD Network, SECOQC deliverable D-NET-03, Oct 2005

PB80a P. Benioff, “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines*”, Journal of Statistical Physics 22:* pp.563-591, 1980

PB80b P. Benioff, “Quantum mechanical Hamiltonian models of Turing machines that dissipate no energy”, *Phys. Rev Lett. 48*: pp.1581-1585, 1980

PD28 P. Dirac, "The Quantum Theory of the Electron". Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character 117 (778): 610–624. doi:10.1098/rspa.1928.0023, 1928

PS00 P. W. Shor , J. Preskill, “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, *Phys. Rev. Lett., 85,*441-444, arXiv: quant-ph/0003004, 2000.

PS09 P. Sheahan, “Fl!p”, Harper Collins, 2009

PS97 P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, *SIAM J. Sci.Statist.Comput*. 26 , 484, 1997, arXiv: quant-ph/9508027v2

PV09 P. Villoresi, R.Ursin, A. Zeilinger “Single photons from a satellite: quantum communication in space”, available online at http://spie.org/x33629.xml?pf=true&ArticleID=x33629

RA05 R. Alleaume, F. Roueff, P. Bellot, O. Maurhart, N. Lutkenhaus “Topology, Architecture and Protocols for a Quantum Key Distribution Network”, Workshop on classical and quantum information security Dec 17th 2005 Caltech available online at http://www.cpi.caltech.edu/quantum-security/slides/alleaume.pdf

RA07a R. Alléaume, J. Bouda, C. l. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger., “SECOQC White Paper on Quantum Key Distribution and Cryptography”, arXiv: quant-ph/0701168, 2007

RA07b R. Alleaume, “Quantum key distribution and networks”, QUROPE Winter School on Quantum Information 23 Feb 2007, available online at http://www.qurope.net/ws2007/pdf/Alleaume.pdf

RD10 “R. Dawkins on Quantum Theory”, video clip, http://www.youtube.com/watch?v=NQYGkuHFNuU March 2010

RF82 R. Feynman, "Simulating Physics with Computers", *International Journal of Theoretical Physics 21*: pp.467–488, 1982.

RF95 R. Feynman, “Six Easy Pieces”, Addison Wesley ,1995

RH99 R. Hahn and D. Hoffman, “The Archive of the German Physical Society”, *American Institute of Physics History Newsletter*, Volume XXXI, No 2, Fall 1999. Available online at http://www.aip.org/history/newsletter/fall99/german.htm

RP05 R. Penrose, “The Road to Reality: A Complete Guide to the Laws of the Universe”, Vintage, 2005

RS10 RSA SECUREid, details at http://www.rsa.com/node.aspx?id=1156 June 2010

SA09 S. Aaronson, “Quantum Copy-Protection and Quantum Money”, *24th Annual IEEE Conference on Computational Complexity* , 978-0-7695-3717-7/09 IEEE, 2009

SC10 The Side Channel Cryptanalysis Lounge http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html March 2010

SD09 "Quantum Information: Disentangling a Billion-Dollar Opportunity." Science Daily 21 December 2009, based on information from Institute of Physics, www.sciencedaily.com/releases/2009/12/091220174037.htm

SGH08 S. Ghernaoutie-Helie, I. Tashi, Th. Langer, C. Monyk, “SECOQC Business White Paper”,http://www.secoqc.net/downloads/SECOQC_Business_Whitepaper_01b.pdf, 2008

SQ10 http://www.secoqc.net, June 2010

SS99 S. Singh, “The Code Book: the Secret History of Codes and Code-breaking”, Fourth Estate, London, 1999

SV02 S. Vittorio, “Quantum Cryptography: Privacy though Uncertainty”, CSA Discovery Guides, http://www.csa.com/discoveryguides/crypt/overview.php, October 2002

SW10 http://www.swissquantum.com June 2010

SW10a http://www.swissquantum.com/?Key-Distillation June 2010

SW10b http://www.swissquantum.com/?Key-Sifting June 2010

SW10c http://www.swissquantum.com/?Raw-Key-Exchange June 2010

TK07 Takeshi Koshiba, “Security Notions for Quantum Public-key cryptography”, arXiv: quant-ph/0702183v1 19 Feb 2007

UM99 U. Maurer, “Information-Theoretic Cryptography”, *Advances in Cryptology, CRYPTO 99*, Lecture Notes in Computer Science, Springer Verlag, vol 1666 pp 47-64, August 1999

UQ10 Updating Quantum Cryptography and Communications 2010 website http://www.uqcc2010.org June 2010

VI08 http://www2.visaeurope.com/pressandmedia/newsreleases/press363_pressreleases.jsp June 2010

VI10 http://www2.visaeurope.com/merchant/handlingvisapayments/cardnotpresent/verifiedbyvisa.jsp June 2010

VS01 V. Shoup, “OAEP reconsidered”, *Advances in Cryptology - Crypto 2001*, LNCS 2139, pp. 239-259 Springer-Verlag, 2001

VS04 V. Scarani, A. Acin, G. Ribordy, N. Gisin,” Quantum Cryptographic Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse implementations”, *Phys Rev Lett Vol 92 057901-1*,Feb 2004

VS09a V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf , M. Dusek, N. Lutkenhaus , M. Peev, “The Security of Practical Quantum Key Distribution”, arXiv: quant-ph/0802.4155v3, 30Sept 2009

VS09b V. Scarani, C. Kurtsiefer,” The black paper of quantum cryptography: real implementation problems”, arXiv: quant-ph/0906.4547v1, Jun 2009

WH03 Won-Young Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication*”, Phys. Rev. Lett*. 91 (5) 057901, 2003

WK04 W. Knight, Entangled photons secure money transfer, *New Scientist*, 22 April 2004, available online at http://www.newscientist.com/article/dn4914-entangled-photons-secure-money-transfer.html

WK10 http://en.wikipedia.org/wiki/Quantum_cryptography March 2010

WW82 W. K. Wootters and W. H. Zurek, A Single Quantum Cannot be Cloned, *Nature 299*, pp. 802–803, 1982

YF06 Y. Feng, S.-L. Ng, S. Schwiderski-Grosche, “An Electronic Voting System Using GSM Mobile Technology”, Royal Holloway, University of London Technical Report RHUL-MA-2006-5, 2006 available online at www.rhul.ac.uk/mathematics/techreports

YZ08 Y. Zhao, C-H. F. Fung, B. Qi, C. Chen, H-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems”, *Phys Rev A 78*, 042888, 2008

Appendix 1

Key Agreement Protocols

The following examples of key agreement protocols are based on descriptions from Menezes, van Oorschot and Vanstone [AM01 Ch. 12]

Diffie-Hellman Key Agreement Protocol

Initial Setup.

An appropriate prime **p** and generator **g** are selected and published.

***Protocol messages*.**

Message 1	A to B :	g^x **mod p**
Message 2	B to A :	g^y **mod p**

***Protocol actions*.**

Perform the following steps each time a shared key is required.

(a) A chooses a random secret **x,** where $1 \leq x \leq (p - 2)$**,** and sends B Message 1.

(b) B chooses a random secret **y**, where $1 \leq y \leq (p - 2)$, and sends A Message 2.

(c) B receives g^x, and computes the shared key as $K = (g^x)^y \bmod p$**.**

(d) A receives g^y , and computes the shared key as $K = (g^y)^x \bmod p$**.**

Summary

Alice and Bob have sent each other one message over an open channel, and have agreed on a secret key **K** by the end of the protocol.

Note: This basic version of the protocol has to be supplemented with authentication, as it is vulnerable to man-in-the-middle attacks

ElGamal key agreement Protocol (half-certified Diffie-Hellman)

Initial Setup.

An appropriate prime **p** and generator **g** are selected and published.

Select a random integer **b**, $1 \leq$ **b** $\leq$**(p – 2)**, and compute $\mathbf{g^b}$ **mod p**

B publishes its public key $\mathbf{(p; g; g^b)}$, keeping private key **b** secret.

Protocol messages.

Message 1 A to B : $\mathbf{g^x}$ **mod p**

Protocol actions.

Perform the following steps each time a shared key is required.

(a) A obtains an authentic copy of B’s public key $\mathbf{(p; g; g^b)}$,

(b) A chooses a random integer **x**, where $\mathbf{1 \leq x \leq p - 2}$, and sends B Message 1

(c) A computes the shared key as $\mathbf{K = (g^b)^x}$ **mod p**.

(d) B receives message 1, and computes the shared key as $\mathbf{K = (g^x)^b}$ **mod p.**

Summary

Alice has sent one message over an open channel, and Alice and Bob have agreed on a secret key **K** by the end of the protocol.

Appendix 2

Fraud Losses at UK Cash Machines 1998-2008

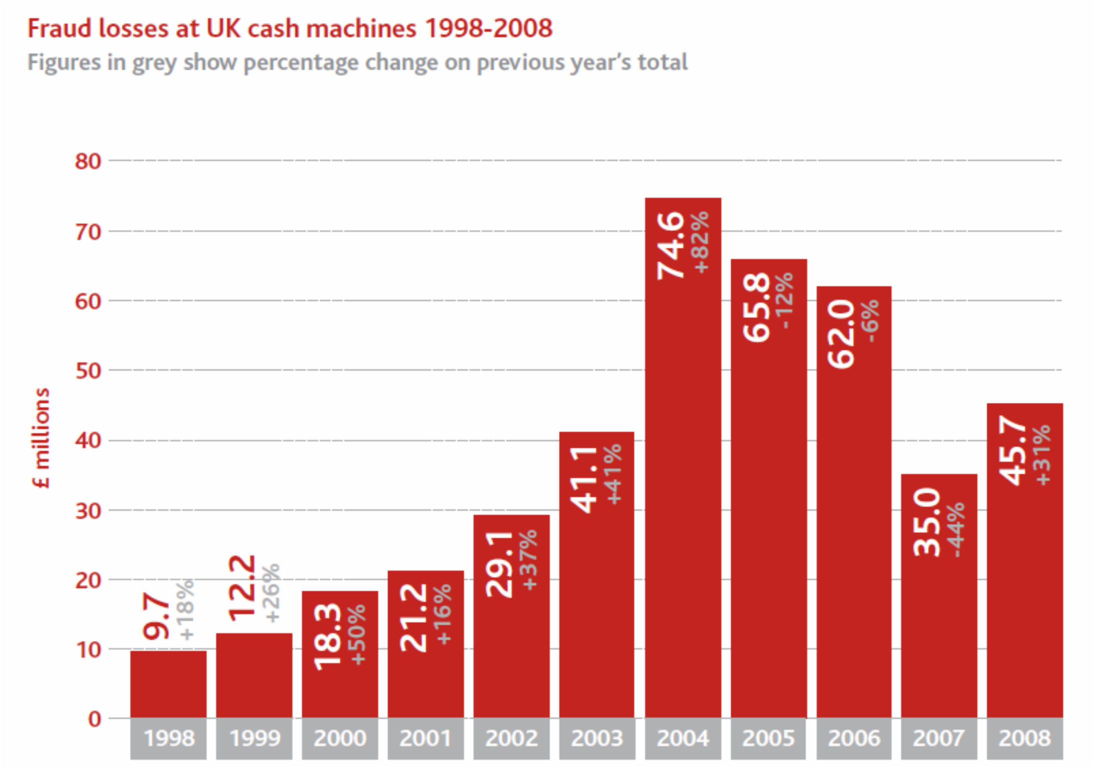


FIGURE 26 FRAUD LOSSES AT UK CASH MACHINES 1998-2008

SOURCE [CW10]

Appendix 3

Online Banking Fraud Losses 2004 -2008

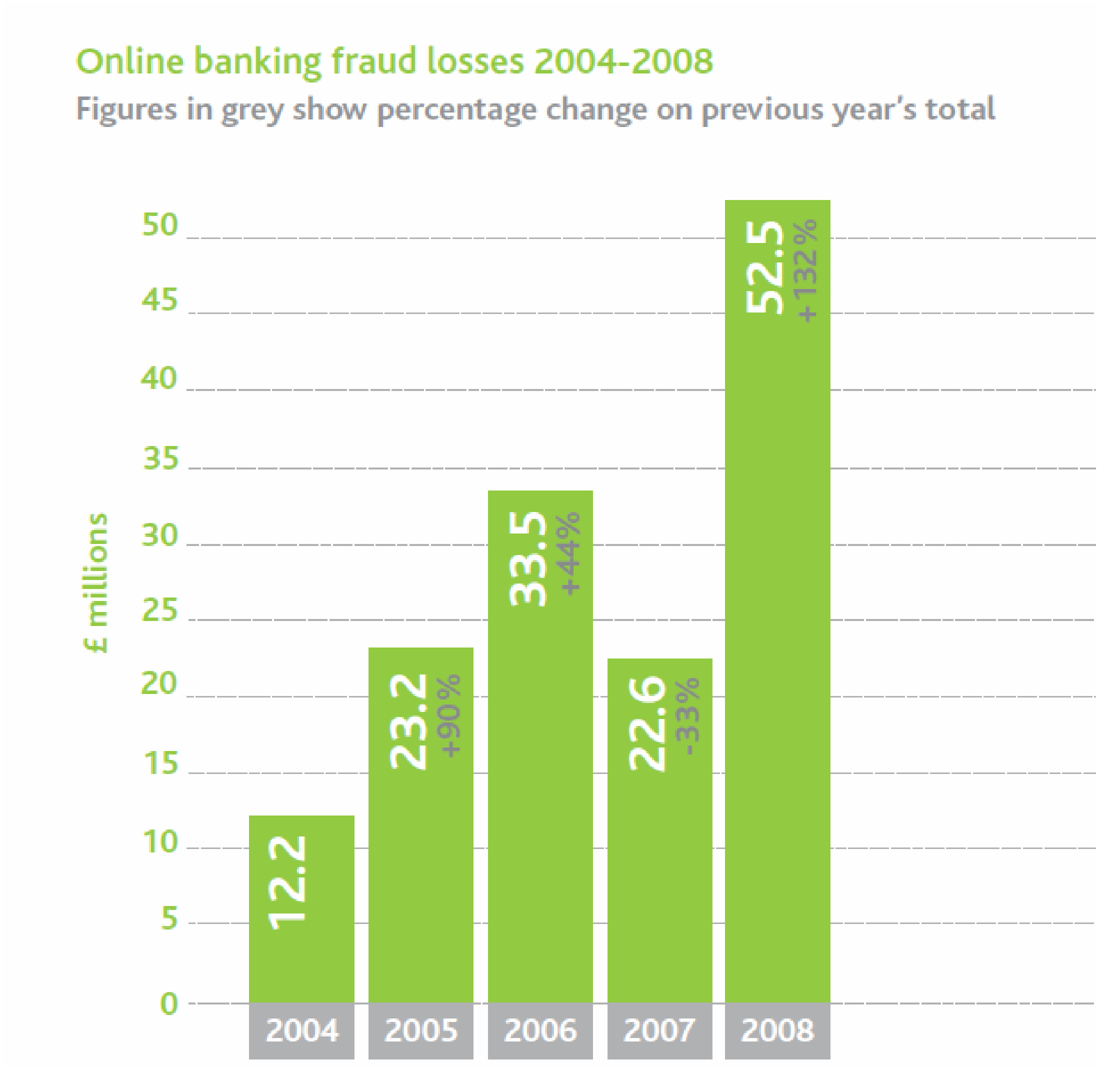


FIGURE 27 ONLINE BANKING FRAUD LOSSES

SOURCE [CW10]

Appendix 4

Card Not Present Fraud Losses on UK-issued Cards 1998 - 2008

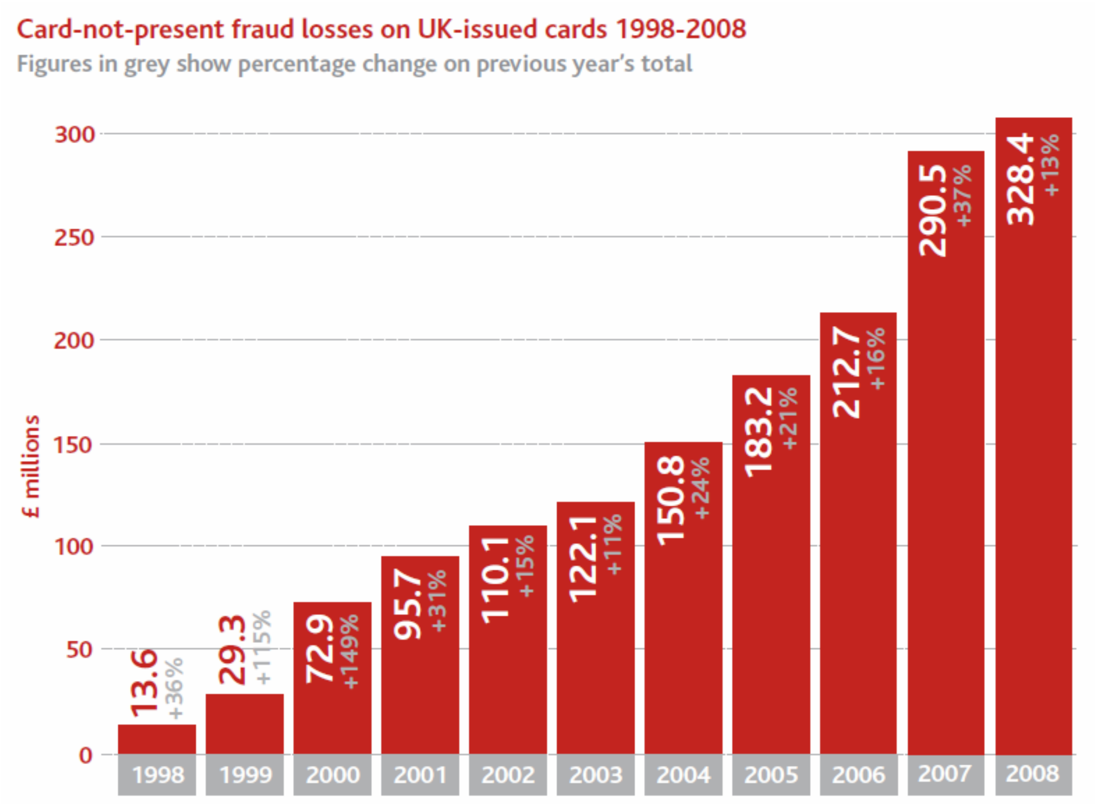


FIGURE 28 CARD NOT PRESENT FRAUD 1998- 2008

SOURCE [CW10]

Appendix 5

List of Abbreviations, Technical Terms and Acronyms

APD	Avalanche Photo Diode
ATM	Automated Teller machine
B92	Quantum key Distribution protocol using polarised photons with non-orthogonal states for encoding information, proposed by C .Bennett
BB84	Quantum key Distribution protocol using polarised photons with orthogonal states for encoding information, proposed by C .Bennett and G. Brassard
BBN	BBN Technologies (originally Bolt, Beranek and Newman) is a high-technology company which provides research and development services.
CNP	Cardholder Not Present
COW	Coherent One Way protocol
CVV	Card Verification Value, used with credit/debit cards for extra authentication
DARPA	Defense Advanced Research Projects Agency
DH	Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read Only Memory
E91	Quantum key Distribution protocol using entangled photons for encoding information, proposed by Ekert
ElGamal	An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange.
EPR paradox	Einstein, Podolsky and Rosen’s thought experiment which attempted to show that Quantum Mechanics was not a complete theory
MAN	Metropolitan Area Network
MITM	Man-in-the-middle, a type of attack on cryptographic protocols where the malefactor intercepts all messages between two parties, and then impersonates them when forwarding the messages on
OSPF	Open Shortest Path First, a dynamic routing protocol in IP networks
OTP	One Time Pad, a type of encryption which is unconditionally secure, provided the key is as long as the message, truly random, and only used once
P & M	Prepare and measure
PBS	Polarising Beam Splitter
PIN	Personal Identification Number

PNS	Photon Number Splitting – an attack on the BB84 protocol when the photon source is not ideal, and produces multi-photon pulses
PR	Polarisation Rotator
Q3P	Quantum Point-to-Point protocol
QAN	Quantum Access Node
QBB	Quantum Backbone
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKD-RL	Quantum Key Distribution –Routing Layer
QKD-TL	Quantum Key Distribution – Transport Layer
QND	Quantum Non-Demolition
RSA	An algorithm for public key cryptography named after Rivest, Shamir and Adleman who first publicly described it
RSA-OEAP	Protocol using RSA encryption, RSA Optimal Asymmetric Encryption Protocol
SARG04	Quantum key Distribution protocol using polarised photons in 4 non-orthogonal states for encoding information, proposed by Scarani, Acin, Ribordy and Gisin
SECOQC	A project for the development of a global network for **SE**cure **CO**mmunication based on **Q**uantum Cryptography
SIM	Subscriber Identity Module
TCP/IP	The Internet Protocol Suite, so named because it uses the Transmission Control Protocol (TCP) and the Internet Protocol (IP)
TTP	Trusted Third party
WCP	Weak Coherent Pulse