Quantum Encryption: Unconditional Security for the Information Age

Jeffery Lyons
Junior Sophister
Physics

Current encryption methods such as public or asymmetric key encryption utilize the computational difficulty inherent in performing certain types of tasks to make third party decryption computationally impossible. However, the rise of quantum computing, which would render encryption methods such as asymmetric key distribution obsolete, necessitates the development of a new and perfectly secure method of encryption. Quantum encryption or quantum key distribution is a method of encryption which relies on fundamental quantum mechanical properties to ensure the unconditional security of information. Two main protocols have been developed by Bennett, Brassard and Ekert for the implementation of quantum key distribution. The details of these protocols are investigated as well as the practicalities of implementing them.

Introduction

Cryptology is defined as the science of rendering messages sent between two parties unintelligible to any external observers known as adversaries. Encryption refers to the exact process by which this is achieved. Specifically, it is the use of an algorithm to combine the original message with an additional piece of information common to both the sender and receiver, known as the key. The key allows the sender to encrypt the message for communication over unsecure channels assumed accessible to adversaries. The party for which the message was intended,

termed the receiver, can then use the key to decrypt the message. In cryptology the sender and receiver are often referred to as Alice and Bob respectively while any present adversary is known as Eve. This formalism will be used throughout the review.

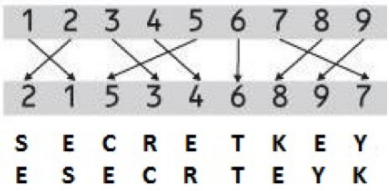

Figure 1. *(Adapted from Skelton, 2015) A transposition cypher. The key used to encrypt the message is the form of the transposition. If the receiver knows how the letters have been transposed the message may be decrypted.*

A cryptographic system where both Alice and Bob are in possession of the same key is known as symmetric key encryption (SKE). SKE is efficient for fast and secure communication of large amounts of information. Alice and Bob can only communicate securely through open channels if they share the same key. This process relies on the successful exchange of the key on which the encryption is based.

Figure 2. *(Adapted from Skelton, 2015) Symmetric key encryption. Both the sender and receiver are in possession of the same key and use this to encrypt and decrypt the message.*

The development of public key encryption and the RSA cryptosystem offers a solution to the problem of key distribution (Rivest *et al*., 1978). As opposed to SKE, public or asymmetric key encryption (AKE) uses two separate keys to construct a secure cipher. If Bob desires to communicate with Alice he chooses a private key which is then distributed throughout the open channels. Any message sent to Bob is then encrypted using his public key. Bob then decrypts the message using his private key. The asymmetry in this system arises from the 'one-way' nature of the public-private key relationship. The public key may be constructed

from the private key; however the reverse process is not computationally feasible. The security which AKE affords is based solely on the idea of computational complexity. A one-way-function is a function computationally feasible to compute given any input but computationally infeasible to invert given an output. The use of such functions ensures that any attempt to reverse the public key production process is computationally infeasible (Rivest *et al*., 1978).

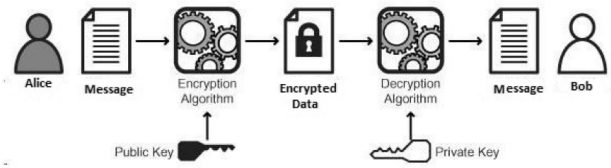

Figure 3. *(Adapted from Skelton, 2015) Public or Asymmetric key encryption. The sender encrypts the message using the receiver's widely available public key. The message may then be decrypted by the receiver using their private key.*

RSA encryption exploits two characteristics of prime products. It is trivial to compute the product of two prime numbers regardless of size. However, it is infeasible to compute the reverse process. This is due to computational time scaling exponentially with the length of the origin primes (Lenstra *et al*., 1992). Therefore, the successful decryption of an RSA cipher in the absence of the correct key would be practically impossible for adversaries. However, it has not been proven that an algorithm capable of completing this task on practical timescales does not exist. The absence of a mathematically rigorous underpinning to RSA asymmetric key encryption means that it is not unconditionally secure (Gisin *et al*., 2015).

Shor's algorithm is one such an algorithm, though it may only be run on a quantum computer (Shor, 1999), a theoretical computing system which makes use of quantum mechanical phenomena to perform operations on data. RSA encryption will be rendered obsolete when a quantum computer capable of running Shor's algorithm is built. A secure method of key distribution must be developed in advance of this eventuality. While quantum computation makes use the characteristics of quantum mechanics to undermine AKE, these same characteristics may provide a provably unconditionally secure method of key distribution known as Quantum Key Distribution (QKD) (Lo *et al*., 2001) (Quan *et al*., 2002).

The unconditional security of QKD arises when the operation of measurement on quantum system is considered. The Heisenberg Uncertainty Principle (HUP) places fundamental limits on the amount of information an observer can have about a quantum system (Heisenberg, 1927).

The HUP states that in performing a measurement on a quantum system only one property out of a pair of conjugate properties can be known with any certainty. It is therefore impossible to have perfect knowledge of the conjugate properties of a system simultaneously (Heisenberg, 1927).

The HUP is utilised by QKD to attain unconditional security. As a consequence of the HUP it is impossible for Eve to make a measurement on a key during distribution without altering it in a detectable way (Wooters *et al*., 2006). Once Bob detects that an adversary has attempted to make a measurement, the key is discarded and a new one is chosen for distribution.

The BB84 protocol

While the concept of QKD as an alternative to traditional key exchange methods was first introduced by Stephen Weisner in 1983, it was not until 1984 that Charles Bennett and Gilles Brassard developed the first practical quantum key exchange protocol.

Alice and Bob are connected by a quantum channel, a channel which preserves quantum states, assumed to be populated by adversaries. Photons are used as message carriers due to their ease of production, detection, and transmittance through optical fibre (Lodewyck, 2005).

The security of the BB84 protocol is based on the HUP. Information is encoded in conjugate states. As per the HUP, a measurement cannot be made on either of these states as this will cause a detectable change in the quantum system.

The BB84 protocol makes use of four non-orthogonal quantum states, which form two conjugate bases to transmit information. The first basis is rectilinear and the states can be represented by ↑ and →. The second basis is diagonal and can be represented by ↗ and ↘. These states correspond to the polarisation direction of the photons. Values are assigned to each state so that results may be tabulated and compared upon detection. The two bases and their corresponding bit values are illustrated in table 1.

To initiate quantum key distribution according to the BB84 protocol an information carrying photon must be prepared by the sender. To prepare a photon for transmission Alice generates a random bit (0 or 1) and randomly chooses a basis to transmit the bit value in (rectilinear or diagonal).

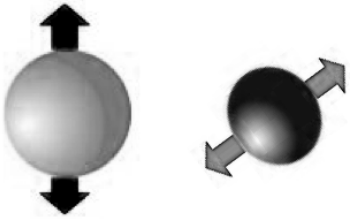

Figure 4. *Photon polarisation directions in the rectilinear and diagonal regimes respectively.*

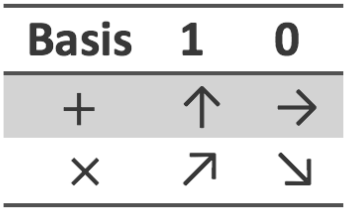

Figure 5. *Photon polarization direction according to chosen basis and bit value.*

Alice then selects a photon with a polarization state that corresponds to both the randomly chosen bit value and basis. The photon is then sent to Bob through a quantum channel assumed to be populated by adversaries. This process is repeated until the key has been exchanged with the details of each photon and the transmission times recorded by Alice.

As Bob has no knowledge of which emission basis Alice transmitted the photons in, he must attempt to detect them using a randomly chosen detection basis of his own. If he measures a vertically polarized photon sent by Alice with a rectilinear basis he will record a bit value of 1. However, on average, 50% of the time Bob will use the wrong measurement basis for the photon resulting in the receipt of a random bit. Since the bases are non-orthogonal, no measurement scheme would be able to effectively distinguish between all four quantum states (Gisin *et al*., 2015). If an observer attempted to measure a diagonally polarized photon with a rectilinear detector, the detector would return a random bit value, with a 50% probability of a 1 or 0.

After transmission and measurement has taken place Alice and Bob communicate openly over an unsecured channel assumed accessible to Eve. They compare the basis they used on each measurement and discard those measurements where Bob chose the conjugate basis to Alice. They do not mention any of the bit values at this point as this would compromise the security of the eventual key. The remaining string of bits is the shared key which is then used to transfer information using SKE.

Table 1. *The exact process by which the encryption key is derived from the transmitted photons is outlined.*

Alice's random bit	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**0**
Alice's random sending basis	+	+	×	+	×	×	+	×
Photon polarization direction	→	↑	↗	→	↘	↘	→	↘
Bob's random measurement basis	+	×	×	×	+	×	+	+
Photon polarization measured by Bob	→	↗	↗	↘	↑	↘	→	↑
Comparison of bases used.								
Shared key.	0	-	1	-	-	0	1	-

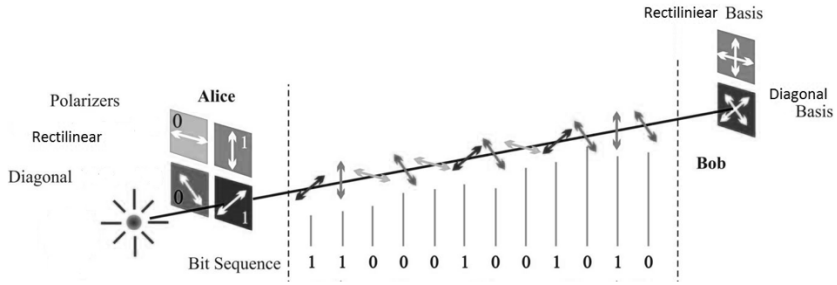

Figure 6. *(Adapted from Swiss Quantum Corp, 2015) The sender randomly chooses an emission basis (rectilinear or diagonal) and a bit value (0 or 1). A photon whose polarisation direction corresponds to the chosen values is sent to the receiver. The receiver then makes measurements using a randomly chosen basis as shown in the diagram.*

To verify the security of the encryption key Alice and Bob now compare a certain subset of the bit string. If they notice a discrepancy in the chosen section of the bit string they abort the key and try again. As a consequence of the HUP, any attempt by Eve to intercept a portion of the key and make a measurement on a certain proportion of the photons will change the nature of the system. Just as making a positional measurement on a quantum particle will cause a change in its momentum, so will a measurement of the photon by Eve cause a change in the photon polarisation received by Bob (Wootters *et al*., 2006). The errors that Eve's measurements introduce into Bob's bit string are easily detectable upon comparison with Alice (Bennett *et al*., 1984).

Through the use of the BB84 protocol, two friendly parties can share an encryption key over unsecured quantum (photon transmission phase) and classical (comparison phase) channels for use with SKE.

The E91 protocol

In 1991 Artur Ekert submitted a new method of QKD for consideration by the scientific community. The theoretical unconditional security of his protocol is entirely underpinned by another set of quantum mechanical phenomena entirely distinct from those utilized by Bennett and Brassard.

The E91 protocol makes use of quantum entanglement to exchange a key in a similar manner to that of the BB84 protocol (Ekert,1991). Instead of Alice sending photons to Bob, a central source creates a pair of entangled photons, sending one to Bob and one to Alice. In a fashion similar to the BB84 protocol, both Alice and Bob choose random bases with which to detect the photons. According to the characteristics of quantum entanglement, for each instance where they both choose the same base, opposite results will be recorded. The results of all measurements are perfectly random. Neither Bob nor Alice can predict whether they will measure horizontal or vertical polarization in the photons provided by the source (Ekert,1991). Both parties then communicate over an open channel and compare the bases chosen for each measurement. When both parties discard the measurements for which opposite bases were chosen, they are left with bit strings that are binary complements of each other. To assemble a private key one party must simply invert the respective bit string.

Any interference by Eve will be immediately detectable upon comparison of the measured polarization directions. A small subset of the key shared by both parties can be compared over unsecure channels. If the strict opposite correlations resulting from the nature of quantum entanglement are not preserved, then Eve has attempted to make a measurement on one of the photons.

Practicalities of implementation

A quantum channel preserves the quantum state of the photons used in the exchange of an encryption key. For both the BB84 and E91 protocols ordinary single mode optical fibre is appropriate as it is widely used and preserves the conjugate quantum states used in BB84 and E91. In practice there will be signal loss which will limit the number of measurable photons arriving at a detector. This directly curtails the key exchange, as the raw key rate is directly proportional to the probability of photon transmission (Hjelme *et al*., 2015). Typical optical fibre transmission loss rates can become problematic over large distances. A typical loss rate for widely used optical fibre is 0.2 dB/km at a wavelength of 1500 nm. At 15 km, a minute distance in the context of modern communication, at least 50% of the photons are lost. This increases to 99% at 100 km (Hjelme *et al*., 2015). Transmission losses of this magnitude limit the practical use of QKD.

Success has been reported with the use of open air as a quantum channel. The longest successful atmospheric transmission of information carrying photons to date is over 144 km between peaks in Gran Canaria (R. Ursin *et al*., 2007).

The practical application of the QKD protocols examined in this paper require reliable single photon sources. In reality single photon detectors represent a significant problem for QKD. Most extant systems rely on faint laser pulsing to produce single photons for transmission. The number of photons present in the pulse is governed by Poisson statistics (Hu *et al*., 2007), which, if examined with regards to the attenuated laser beam, reveal the difficulties inherent in single photon emission. If the beam is attenuated such that there is an average of 0.1 photons per pulse then there is 90% probability that an observer will not measure any photons in the pulse. In addition, there exists a 9% probability that the desired single photon will be observed. A risk is also posed to the security of the key by photon emitters with a high probability of emitting more than a unitary photon. Eve may be able to capture one of the extra photons and wait until the basis information is broadcasted on the open channel (Gisin *et al*., 2007). With knowledge of the sequence of bases used by both parties, Eve may then perform a measurement on the captured photon and reduce the security of the key without possibility of detection.

Single photon detectors are far easier to realise than emitters. Single photon avalanche photodiodes represent the most efficient single photon detection method available for QKD. They operate in a Geiger mode whereby photons entering the detector excite an electron due to impact ionization (Geiger *et al*., 1909). This triggers an avalanche of electrons until the initial excitation is amplified to a level that can be detected as a pulse of electric current by external circuitry.

Conclusions

The central tenet of modern telecommunications is the transfer of information quickly, efficiently and securely. While modern cryptographic methods such as symmetric and asymmetric key encryption currently provide the required security, the prospect of a quantum computer capable of running Shor's algorithm necessitates the development of a new system.

Quantum encryption and QKD promise to provide unconditional security for use with SKE. The quantum physical principles on which these are based cannot be circumvented by a potential attacker and are therefore ideal for use in cryptography. The practical implementation of such systems and the resultant problems constitute the biggest difficulties in the applications of QKD. Such systems are also vulnerable to attack using loopholes in detector design such as the continuous wave illumination attacks.

It is widely believed that these difficulties will be overcome (Jogenfors *et al*., 2015) and a viable QKD system will be built. However, to ensure the security of information, this must occur before RSA encryption is rendered obsolete by quantum computing.

Acknowledgements

The author would like to thank Mr. B. Delaney, Prof. W. Blau and Prof. S. Hutzler for helpful appraisals.

References

RIVEST, R. L., SHAMIR, A., ADLEMAN, L. (1978). 'A method for obtaining digital signatures and public-key cryptosystems', *Communications Of the ACM Commun. ACM*, 21(2), 120–126.

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

HEISENBERG, W. (1984). 'Über den anschaulichen Inhalt der quantenmechanischen Kinematik und Mechanik' (1927). *Die Deutungen Der Quantentheorie*, 53–79.

LENSTRA, H. W., POMERANCE, C. (1992). 'A Rigorous Time Bound for Factoring Integers', *Journal Of the American Mathematical Society*, 5(3), 483.

LO, H.-K. (2001). 'A simple proof of the unconditional security of quantum key distribution', *J. Phys. A: Math. Gen. Journal Of Physics A: Mathematical and General*, 34(35), 6957–6967.

LODEWYCK, J. (2005). 'Quantum key distribution with coherent states at telecom wavelength', *31st European Conference On Optical Communications* (ECOC 2005).

LOEPP, S., WOOTTERS, W. K. (2006). 'Protecting information: from classical error correction to quantum cryptography', *Cambridge: Cambridge University Press.*

LYDERSEN, L., WIECHERS, C., WITTMANN, C., ELSER, D., SKAAR, J., MAKAROV, V. (2010). 'Hacking commercial quantum cryptography systems by tailored bright illumination', *Nature Photonics Nature Photon*, 4(10), 686–689.

MJØLSNES, S. F. (2012). 'A multidisciplinary introduction to information security', *Boca Raton: CRC Press.*

QUAN, Z., CHAOJING, T. (2002). 'Simple proof of the unconditional security of the Bennett 1992 quantum key distribution protocol', *Phys. Rev. A Physical Review A,* 65(6).

SHOR, P. W. (1999). 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', *SIAM Rev. SIAM Review*, 41(2), 303–332.

URSIN, R., TIEFENBACHER, F., SCHMITT-MANDERBACH, T., WEIER, H., SCHEIDL, T., LINDENTHAL, M., BLAUENSTEINER, B., JENNEWEIN, T., PERDIGUES, J., TROJEK, P. AND ÖMER, B. (2007). 'Entanglement-based quantum communication over 144 km', *Nature physics*, 3(7), pp.481-486.

N. GISIN, G. RIBORDY, W. TITTEL, AND H. ZBINDEN.(2002) 'Quantum cryptography', *Reviews of Modern Physics,* 74:145{195}.

JOGENFORS, J., ELHASSAN, A. M., AHRENS, J., BOURENNANE, M., LARSSON, J.-A. (2015). 'Hacking the Bell test using classical light in energy-time entanglementvvv-based quantum key distribution', *Science Advances*, 1(11).

EKERT, A. K. (1991). 'Quantum cryptography based on Bell's theorem'. Phys. Rev. Lett. Physical Review Letters, 67(6), 661–663.
Hjelme, D, Lydersen,L & Makarov, V,(2015). 'Quantum Cryptography', *arXiv.org, arXiv:1108.1718*.

HU, Y., PENG, X., LI, T., GUO, H. (2007). 'On the Poisson approximation to photon distribution for faint lasers', *Physics Letters* A, 367(3), 173–176.

GEIGER, H., MARSDEN, E. (1909). 'On a Diffuse Reflection of the Formula-Particles', *Proceedings Of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 82(557), 495–500.