Quantum Cryptography and Secure Data Transfer

Redefining the Future of Communication Security

Alex Jackson
Mentor: Ming Chow

Abstract

The security of communicating secret messages has needed to be considered since the dawn of writing. Some of the earliest known encryption came with the Caesar cipher, in which each letter in a message is replaced with another one a fixed number down in the alphabet. As technologies developed, so did encryption techniques; with the advent of the classical computer, new encryption methods were invented that rely on problems that are thought to be computationally hard for another computer to solve, such as the factoring of two large prime numbers. As the prospect of quantum computers becomes realized, we enter into a new age of security for data communication. Using quantum cryptographic algorithms, standard decryption problems (or determining the "key" used to reveal the information in an encrypted message) that are thought to be computationally hard can be solved in efficient times. However, while quantum computing could compromise the most widely used encryption standards, it can also offer a method for *unconditionally secure* key distribution. In other words, quantum key distribution (QKD) can guarantee secure key transfer without imposing any restrictions on the power of an eavesdropper. Although the implementation of universal quantum computers capable of breaking the current key encryption protocols are still in the experimental stages, commercial development of QKD systems has already begun.

Introduction

In order to fully understand the implications of quantum computer systems on security, it is necessary to grasp the concepts of quantum mechanics that make these systems so unique. In classical computing, data is represented as long strings bits, which are basic units that take on either the value of 0 or 1. However, quantum computational systems use qubits, or units of data that represent the values of 0 and 1 *at the same time*. This is possible by using the principle of superposition. The specific mechanics of this principle are non-intuitive and are out of the scope of this discussion, but it is enough to understand that superposition stipulates that a particle can exist in two quantum states at once until it is observed, at which point it will *decohere* into a singular value. Thus, a qubit can be represented by any system that has measureable quantum states, such as the spin of an electron, the magnetic moment of a superconducting loop, or the polarization state of a photon. As a result of this strange behavior, a system composed of n qubits can represent 2^n states at one time. This is an incredibly powerful property; with just 22 qubits, a quantum computer can evaluate 2^{22} = 4,194,304 probabilities simultaneously. Certain problems that scale exponentially when using classical algorithms can be addressed efficiently with quantum methods. Take, for example, the problem of factoring; doing so for a 60-digit number may take ~ $3 * 10^{11}$ *years* using a classical computer, but only 10^{-8} seconds on a quantum one. For encryption systems the rely on such problems, quantum computers are a real concern for their security. Where superposition gives a new dimension of computational power to quantum information systems, quantum entanglement is the property that links the system together. Entanglement is a phenomenon that correlates two particles together even when separated by large distances. In the case of quantum computers, if two qubits in states of superposition are

entangled, then measuring the state of one of them will reveal state of the other. By utilizing these quantum mechanical properties when storing and manipulating data, a new world of information processing is opened.

To the Community

Over the past several decades, the development of quantum information systems has improved dramatically. Although a practical universal quantum computer has yet to be created, it is possible that a construction of one will be realized in the near future. Adiabatic quantum computers (less powerful computational systems that use annealing to solve global optimization problems) are commercially available through D-Wave Systems, and quantum key distribution is a commercial service offered through several companies such as ID Quantique and MagiQ Techonlogies. It is only a matter of time before computers capable of performing algorithms that break the most popular encryption standards are created and once that happens, the world must be ready. Although it is unreasonable to expect computer system security professionals to be well-versed in the world of quantum mechanics, it is necessary that they are at least aware of the capabilities associated with quantum technology and what the development of such devices would implicate. There is an opportunity here to protect against a future system vulnerability before it is realized, instead of continuing the cycle of bandaging the problem after it is exploited. Quantum key distribution is important to explore as it theoretically offers one of the only methods of unconditionally secure data transfer. Examining an implementation for one of these protocols is a good security analysis exercise, as it can reveal vulnerabilities in the system's *physical* construction.

Classical Encryption in a Quantum Environment

The concept of quantum cryptography was first introduced by Stephen Wiesner in the 1970s, where he proposed encoding messages in two "conjugate observables" in order to create unforgeable bank notes[1]. However, this idea was largely ignored until 1994 when Peter Shor demonstrated that a universal quantum computer could efficiently factor a large integer[2]. This gave rise to a new computational complexity class, BQP (bounded error quantum polynomial time), which include problems that are thought to scale in polynomial time with a quantum algorithm, and exponentially with a classical algorithm. With this discovery, people started to realize the implications that quantum technologies could have on many modern day security protocols.

In order to communicate data between two parties securely it needs to be encrypted; to decrypt this data, a known decryption key needs to be applied. The most common method used to exchange these secret keys between parties is asymmetric encryption (AKA public key cryptography, where the public key encrypts data and a different, private key decrypts it), and the most utilized protocols are the Diffie-Hellman key exchange, RSA encryption, and Elliptic Curve Cryptography (ECC)[3]. Each of these relies on the fact that it is incredibly hard for classical computers to solve discrete logarithm and integer factorization problems. However, as was just discussed, quantum computers provide a method by which to solve these problems and if a cryptanalyst was given a public key, he could use a quantum algorithm to compute its

[1] Gisin, N. et al. (2002)
[2] Shor, P W. (1997)
[3] Jodoin, E (Aug 2014)

corresponding private key. Obviously, this would compromise all communications that use these security protocols; an attacker could read all encrypted information sent between the two parties, or even impersonate a victim and perform man in the middle attacks.

Perfectly Random Number Generator

It should be noted that using quantum mechanical properties offers an avenue for creating a perfectly random number generator. By sending a weak coherent pulse (WCP) of photons through a 50:50 beam splitter and setting up two single-photon detectors on the outgoing arms to measure the result, the random sequence of 0's and 1's will be generated based on which detector is hit. This is a powerful tool to use for encryption, as many protocols need to generate random numbers during parts of their processes. For example, the first unbreakable code that was documented, the Vernam cipher (aka one-time pad), creates a symmetric key (which is used to both encrypt and decrypt its corresponding data) of completely random values.

QKD

While quantum physics provide methods that break modern day public key cryptography, it also opens up a new realm of distributing secret symmetric keys. Instead of relying on the problems that are *assumed* to be too hard to solve, quantum key distribution relies on quantum physical *laws*. Arising from the quantum mechanical properties that were discussed earlier are a set of negative rules of actions that cannot be done, the most important of which (for quantum key distribution) being:

1. One cannot take a measurement without perturbing the quantum system.

2. One cannot duplicate an unknown quantum state (this rule is often referred to as the "no-cloning theorem")[4].

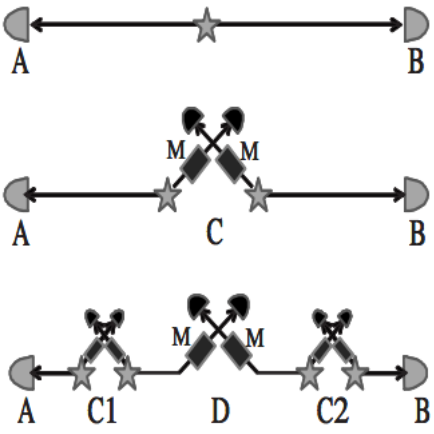
The unconditional security of QKD is entirely dependent on these statements; given a communication between Alice and Bob on quantum channel (the conventional names for a communication system between the sender and receiver, respectively) an eavesdropper, Eve (the conventional name for a third-party adversary), cannot get any information without revealing her presence.

Although quantum information can be represented by many different quantum system states, the only practical implementation of communicating quantum data over macroscopic distances is through the use of photons. Light does not interact easily with matter; thus, quantum states of light can be transmitting to distant locations without fear of decoherence. However, the problem with photon transmission is *losses*: the instance where photons do not arrive at their location. These losses impose bounds on the distance of the quantum communication channel, thus current technologies can only implement these channels to a maximum range of roughly 100 km. There are two viable implementations of such quantum communication systems: fiber optic and free space transmissions. Due to the no-cloning theorem, it is not possible to amplify fiber optic transmissions through classical means (as it would require measuring the data and resending it). Instead, the fiber optic channel uses quantum teleportation to increase the transmission range. Given a quantum channel set between points A-B, n repeaters are set up that create a new link, A-C_1-C_2-...-C_n-B, where each link contains sets of entangled photons to propagate the quantum data from A to B. Each repeater introduces a chance for error, so as the

[4] Jodoin, E (June 2014)

number of links increase, the photon transmission losses increase as well. For a free space quantum channel, the main sources for losses are of geometric and atmospheric nature. Geometric losses result from incompatible configurations of the apertures of the sending and receiving telescopes. Atmospheric losses are due to scattering and scintillation of photons as it travels through the free space. Consequently, the performance and reliability of the free space quantum channel may rely on the weather.

Figure 1: Quantum channel configurations: direct-link, two-link and four-link repeaters (Scarani V., et al. 2009).



Although the fiber optic quantum communication channel is the most common implementation for QKD, free space channels have a higher theoretical cap to the distances they can cover. Experimental development has begun for ground-to-satellite links that could implement a QKD protocol over long distances; the challenge to this is building a device that could operate in a satellite without needing maintenance. Another method for improving the distance of free space quantum channels is to use a system of repeaters similar to that used for the fiber optic channel. However, these repeaters would need to store quantum memory (i.e contain a qubit system). This is currently not practically possible, but would become so upon the advent of a practical universal quantum computer[5].

There are several theorized QKD protocols that have been researched, but only a couple of them are in commercial use at this time. QKD protocols are categorized based on their photon detection schemes, of which there are three main families: discrete-variable, continuous-

[5] Lo, Hoi-Kwong, et al. (2014)

variable, and distributed-phase-reference.[6] The specific details of these detection methods that differentiate different protocols is outside the scope of this paper, but it is enough to know that every commercially used QKD protocol to date uses discrete-variable detection.

BB84 Protocol

The most commonly used QKD protocol was invented by Charles H. Bennett and Gilles Brassard in 1984, and was appropriately named the 'BB84 protocol'. For a sender, Alice, and a receiver, Bob, two independent communication channels, a quantum one and a classical one (like the internet), are set up in order to transfer data. The quantum channel exchanges a random symmetric key between the participating parties, while the classical one uses the resulting key to encrypt and decrypt sensitive data. Note that this classical channel must first be authenticated with a short encryption key; thus, the process can be thought of more as a key *growing* protocol. The symmetric key is transferred with a fiber optic link using the following process:

1. Alice transmits photons through the quantum communication channel to Bob.
2. Both Alice and Bob apply random polarization filters (note that the photon beam splitting technique described earlier can be used to generate the random filters) to the corresponding quantum data.
3. Bob reveals his sequence of filters over the unsecure channel and Alice responds by confirming each case where the polarization was compatible.

[6] Scarani V., et al. (2009)

4. Alice and Bob now have enough information to reconstruct the series of bits that represent the randomly generated symmetric key through a process known as the 'sifting of keys'[7].

When Alice sends a photon and Bob measures it, there are two polarization bases (+ and x) that they may choose from to apply their filter. Because the choice is random for each photon, there will be ~ N/2 cases in which the measurements are compatible. During this stage where quantum data is being transferred, any eavesdropping attempts by Eve would require her to measure the polarization of the photons; by doing so, she would interrupt the quantum indeterminacy and introduce noticeable errors on the sides of both the sender and receiver. It is thus necessary to set a bounded error minimum that would confirm the presence of an eavesdropper if surpassed, at which point Alice and Bob could decide the best action with which to proceed.

E91 Protocol

The E91 protocol is another QKD protocol that uses different aspects of quantum mechanics in order to distill a secure key. Instead of distributing a random symmetric key via correlated polarization states of single photons (like BB84), E91 uses non-local correlations between maximally entangled photon-pairs. The quality of such entanglement can be measured by the degree of violation of a Bell inequality, a set of constraints that describe the relationship between the measurements of an entangled pair and their correlation (where the pair becomes more correlated with *increasing* degrees of violation). Originally, this protocol was restricted as it lacked a mechanism for error correction and unconditional security; however, it was discovered

[7] Scarani V. et al. (2009)

that the degree of violation to the corresponding Bell inequality was related to the error fraction in the generated key.[8] Because the entanglement between two systems decreases when a third party (perhaps an eavesdropper) interacts with the pair, all attempts to sniff the communication would be noticed, given that the Bell-type inequality is properly monitored during communication. The E91 protocol has a couple unique advantages. First, there is no max distance to when entanglement dissipates, thus quantum communication could theoretically be achievable between parties at opposite sides of the Earth. Next, there is no physical channel between the two particles, thus attempts to eavesdrop on the communication become more difficult to accomplish. While this protocol could be a promising standard, it is still in the nascent stages of research.

Methods of Attack

While the theoretical foundation of QKD protocols is impervious to attack, experimental implementations of QKD have developed at a different rate than the theory and often fail to account for all security features. Shortcomings of early QKD constructions were first realized with the discovery of photon-number-splitting (PNS) attacks. For all practical QKD protocol structures, phase-randomized weak coherent pulses (WCPs) are used to simulate photons. These lasers emit average number of photons below 1 with a Poisson distribution. As a result, some pulses may emit 2 or more photons during a single event. When this occurs, Eve may measure one photon in a given basis and gain information about the key, then send the other photon to Bob *without*

[8] Ling, A et al. (2008)

introducing noticeable errors[9]. In order to prevent this, a decoy-state method implementation can be added. Instead of sending signals of equal intensity, Alice chooses an intensity for each photon pulse based on a random set of prescribed values. One given intensity is chosen to be the 'signal state' intensity, while all signals sent at different intensities are 'decoy signals'. After Bob has received and detected all signals, Alice broadcasts the intensities used for each pulse. Even if Eve knew the total number of photons in each pulse, she could not have known the correct intensity with which to send extra photons to Bob (if she intercepted a pulse with > 1 photon). Given that Alice sent a single-photon WCP, the probability of a detection event for a signal or decoy pulse is the same; thus, Alice and Bob can more precisely estimate the fraction of detected events which would arise from a single photon pulse (which cannot be exploited with a PNS attack). As seen with this method of attack, all vulnerabilities with QKD arise from shortcoming in the physical implementations. Often times, these vulnerabilities will be specific to how the system was manufactured. For example, in 2011, security researchers demonstrated that they could break ID Quantique's QKD system by overriding their receiver's ability to detect eavesdropping instances.

Counter Measures

There are three main countermeasures that could be pursued to combat against QKD attacks. First, security patches may be implemented; that is, as vulnerabilities are discovered corresponding countermeasures can easily be developed to match it. However, this is the cycle that is often seen with classical cryptographic technologies and is less than ideal. Another option

[9] Lo, Hoi-Kwong, et al. (2014)

would be to pursue device-independent (DI) QKD systems. In these environments, Alice and Bob treat their devices as black boxes and do not characterize their components. Instead, they rely on the violation of the Bell inequality (e.g E91 protocol). The technology to perform a loophole-free Bell test is still unavailable and until then, practical implementations of these systems cannot be created. Last, MDI-QKD could be developed, a method that allows Alice and Bob to perform QKD with untrusted measurement devices. This process relies on the idea of time reversal to verify the honesty of an untrusted source. Although this would result in a lower secret key rate, it would force attackers to direct their efforts towards the sources and quantum signals rather than the receivers.

Conclusion

As quantum technologies develop, modern communication protocols have to be refactored accordingly. It is imperative that security experts are aware of the capabilities associated with quantum informational systems and design security systems with them in mind. When a practical universal quantum computer is realized, the current standards for public key communication will be compromised. Communication channels that contain incredibly sensitive information must no longer rely on assumptions of classical computing limitations. Fortunately, quantum technology also offers new methods to communicate unconditionally secure data. By relying on quantum physical properties, quantum key distribution opens up a new realm of communication standards. Although ensuring the security for a QKD system is difficult in practice as vulnerabilities may arise for their physical constructions, QKD is at least built on a foundation

of theoretically pure security. For communicating parties that require completely secure data transfer, QKD may offer an elegant solution.

References

Benenti, G., Casati, G., & Strini, G. (2004). *Principles of quantum computation and information.* World Scientific Pub.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography*. Reviews of Modern Physics 74(1), 145-195.*

Jodoin, E. (June 2014). *Straddling the Next Fronteir Part 1: Quantum Computing Primer.* Austin, TX: SANS Institute.

Jodoin, E. (Aug 2014). *Straddling the Next Fronteir Part 2: How Quantum Computing has already impacted the Cyber Security landscape.* Austin, TX: SANS Institute.

Ling, A., Peloso, M., Marcikic, I., Lamas-Linares, A., & Kurtsiefer, C. (2008). Experimental E91 quantum key distribution. *Advanced Optical Concepts in Quantum Computing, Memory, and Communication.*

Lo, Hoi-Kwong, Marcos Curty, and Kiyoshi Tamaki (2014). Secure Quantum Key Distribution*. Nature Photonics, 8(8), 595-604.*

Scarani et al, V. (2009). *The security of practical quantum key distribution.* Geneva, Switzerland: University of Geneva.

Shor, P. W. (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. Siam Journal on Computing, 25(5), 1484-1509.*