Quantum Cryptography

Dylan Evans, Alec Landow, Aaron Ross, Stefan Salanski
Department of Physics
University of Virginia

May 2nd, 2011

Abstract

This paper will explore the subject of quantum cryptography. More specifically, methods of making and breaking QC will be introduced. In addition to a discussion of the theoretical aspects of QC, the technological aspects of the subject will also be presented, including contemporary demonstrations and future projects.

Introduction: The development of quantum cryptography began with an exploration into the idea of mathematically secure cryptosystems, or systems which allow the secure transfer of data across insecure channels. Concepts which do not exist in the classical regime such as quantum entanglement, defined later in the paper, allow one to produce a system in which information can be transmitted in a secure manner. Key to this discussion is the idea that quantum cryptography is more accurately referred to as "quantum key distribution," or QKD. The differences between symmetrical and asymmetrical key distribution will be explained in the context of information theory. We will then discuss the quantum mechanical phenomena necessary to construct these systems, such as entanglement, the no cloning theorem, and Bell's inequality.

After an introduction to this background information, the paper will essentially be divided into two sections: the making and breaking of these quantum cryptosystems. The technological aspects of these systems will be discussed, along with performed and future experiments.

Quantum mechanics background: Perhaps the most important quantum mechanical phenomenon related to quantum key distribution is the no-cloning theorem. The concept, proven in 1982 by Wootters, Zurek and Dieks, says that no outside observer can reproduce perfectly an unknown quantum state without leaving the result of an observer's measurement unchanged[1]. Take the unknown state $|\chi_1\rangle$ and some state $|\phi\rangle$ to which the state will be copied. If cloning were possible, some unitary evolution operator U would act such that $U|\chi_1 \otimes \phi\rangle = |\chi_1 \otimes \chi_1\rangle$. One can then take the inner product $X = \langle\chi_1 \otimes \phi|U^\dagger U|\chi_2 \otimes \phi\rangle$, where $|\chi_2\rangle$ is some other unknown state. This inner product which is known to be zero due to the orthogonality of the states, can be evaluated in two ways:

$$X = \langle\chi_1 \otimes \phi|\chi_2 \otimes \phi\rangle = \langle\chi_1|\chi_2\rangle \tag{1}$$

$$X = \langle\chi_1 \otimes \chi_1|\chi_2 \otimes \chi_2\rangle = \langle\chi_1|\chi_2\rangle^2 \tag{2}$$

This proves that either $|\chi_1\rangle \equiv |\chi_2\rangle$ or $\langle\chi_1|\chi_2\rangle = 0$. Thus, one can either clone the state $|\chi_1\rangle$ or an orthogonal state, but never both [2]. This theorem becomes extremely important in the discussion of QKD protocols, particularly the BB84 protocol discussed later in the paper. It implies that an outside observer, whom we shall call Eve, cannot clone the quantum state without introducing a perturbation into the system. Although perfect cloning is impossible, an unknown state can be cloned approximately to an extent dependent on the system configuration[3]. Another proof of the no-cloning theorem arises out of the impossibility of superluminal information transfer. One must first introduce the concept of quantum entanglement. For the sake of simplified introduction, we consider a bipartite system composed of states from separate Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, with product space given by $\mathcal{H}_A \otimes \mathcal{H}_B$. The states which live in this product space can be considered either pure or entangled; pure states can be written in the form $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, whereas entangled states must be written as a linear combination of other states which live in the product space. More generally, given an appropriate basis, one can decompose any state living in $\mathcal{H}_A \otimes \mathcal{H}_B$ as

$$|\psi_{AB}\rangle = \sum_{i=1}^{M} a_i |e_i\rangle \otimes |f_i\rangle, \tag{3}$$

where M $\leq dim\mathcal{H}_{\mathcal{A}}, dim\mathcal{H}_{\mathcal{B}}$, and $|e_i\rangle, |f_i\rangle$ are orthonormal basis vectors of $\mathcal{H}_{\mathcal{A}}, \mathcal{H}_{\mathcal{B}}$. In the case of the pure state(and appropriate basis), there is only one Schmidt coefficient a_i, whereas in the entangled state, one cannot decompose the state with only one Schmidt coefficient[2]. The most well-known example of an entangled state is the singlet spin state: $\frac{|10\rangle - |01\rangle}{\sqrt{2}}$. These states are described as entangled because a measurement on one state is directly correlated to the state of the other particles. For instance, if one measures an eigenvalue of 0 for state A of the singlet state, state B is forced into the state which yields an eigenvalue of 1. This result leads to a possible violation of the locality required in a physical theory. Locality implies that if two events are spatially separated, ie. $ds^2 > 0$, the systems can not be causally connected. Quantum entanglement seems to violate this requirement. In reality, violation is prevented by the fact that entanglement is analogous to a shared-coin-flip. This coin flip has the same observable outcomes as entanglement, allowing for no information transfer.

Assume first that Alice and Bob share an entangled singlet state. Alice then measures her state, recording which basis the state was measured in. Afterward, Bob, who is equipped with a hypothetical unitary cloning operator, makes an unlimited number of copies of his state. He can then measure these copies in both bases. These measurements depend only on the speed of the copier; thus, if the unitary cloning oeprator did exist, one could transfer information at a superluminal rate[2].

Cryptography background: We now discuss general cryptography systems, specifically symmetric and asymmetric key systems. Although less significant in the study of QKD, mentioning the concept of the asymmetric key system will help illustrate the mechanics of cryptosystems in general. In such a system, two keys exist: a private and public key. A specific implementation of this method is the RSA protocol, developed in 1978 at MIT [4]. The private key N, the product of two large prime numbers p and q, is first chosen. The size of this key N is chosen to be larger than the message block desired to be transmitted. Bob, one agent in the exchange, chooses randomly some integer d which is relatively prime with $(p-1)(q-1)$. The inverse modulo $(p-1)(q-1)$ of d, called e, is then computed, after which p and q are discarded. A public and private key are then produced from this information, allowing Alice to encrypt messages while Bob can decrypt them.[4].

This protocol is worth mentioning because it allows us to analyze the mathematical security of asymmetrical key systems. The security of the RSA protocol depends on the computational difficulty in decomposing integers into their prime factors. Specifically, this problem is believed to live in the class of NP problems. One algorithm, Shor's algorithm, already exists which reduces the complexity of the problem from NP to P. This algorithm can only be implemented using a quantum computer. A successful implementation of this algorithm in factoring large integers will immediately render RSA useless.

On the other hand, symmetric key systems offer a mathematically secure solution to information transfer. This method is commonly referred to as the one-time pad in that it requires a new key during each information exchange. If the channel over which the secret key is distributed can be guaranteed secure, then no method exists through which the encryption can be broken. The message to be sent is first encoded in binary. A secret key of size equal to the message block is then produced randomly. This key is added bitwise modulo 2: $c_i = p_i \oplus k_i$, where c_i is the cypher text, p_i the plaintext and k_i the secret key, where each of these is split up into uniform size blocks. The receiver then uses the secret key which has been distributed over some channel to decrypt the message through the same process: $p_i = c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i$.[1] The essential component of this system is that this secret key can be transmitted over some channel without being determined by an outside observer. This is the point at which quantum key distribution comes into play.

BB84 protocol: The first ideal QKD protocol, the BB84 protocol, is due to Bennett and Brassard(1984). The protocol requires two bases from which there are two quantum states each. In practice, this involves two pairs of orthogonal states are used, horizontal/vertical and two states at $\pm 45°$. Specifically, the alphabet is given by $|0\rangle$ and $|1\rangle$ for the horizontal and vertical polarizations, and $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ for the $\pm 45°$ polarizations. The system utilizes two channels, one quantum and one classical channel. Alice first produces a qubit which she measures in a random basis. Afterward, she assigns the measurement a letter in her "alphabet": composed of $|0\rangle$ or $|+\rangle$ for 0 and $|1\rangle$ or $|-\rangle$ for 1. These qubits are sent to Bob, who then chooses a basis at random to measure these bits, recording which basis he used. At the end of this exchange, Alice and Bob then communicate over a classical channel which basis they used for each measurement. If they agree, the data is kept; if not, the data is thrown away. On average, 50% of the bits will be kept. What is left over is known as the *sifted key*. Although it seems as if information is lost by this process, one must recall that the protocol is a key distribution method. No information

is ever given about the message to be exchanged.

The security of this method arises out of purely quantum mechanical reasons. Imagine an observer known as Eve who wishes to eavesdrop on Alice and Bob's exchange. If she wishes to know the state of the quantum state which is being sent from Alice to Bob, she must first observe this state. One of the basic principles of quantum mechanics states that an observation will disturb a quantum state, perturbing it away from its original state. Not only this, but we now know from the no-cloning theorem that there is no way for Eve to reproduce this quantum state with full fidelity. Many attacks on the BB84 protocol revolve around making approximate copies of states exchanged between Alice and Bob[2]. Alice and Bob can detect whether or not an eavesdropper is intercepting their communcations by comparing statistics on a small set of exchanged data. More specifically, one refers to the quantum bit error rate(QBER), simply the probability that Bob measures the wrong polarization when Alice's basis is known[3]. For a secure transfer of the key, the QBER must be smaller than 11%. Generally, the QBER q equals

$$q_0 = p_f + \frac{p_d n q \Sigma f_r t_l \mu}{2} \tag{4}$$

where p_f, p_d are related to detector problems, n is the number of detections, q is the phase related to the medium, Σ the detector efficiency, f_r the pulse repeat frequency, t_l the transmission rate and μ the attenuation for light pulses [10]. The error rate R is measured on some small subset of the sifted key. If $R < q_0$, then two techniques are applied: *information reconciliation* and *privacy amplification*. Both of these proccesses are classical information techniques. First, the sifted key is divided into blocks of length l. This length l is chosen according to the error rate R previously measured such that only one error occurs per subset on average. For each of these blocks, the parity is calculated: the blocks are split up into binary strings, after which each string b_i is added bitwise modulo 2, $P = b_1 \oplus b_2 \oplus \cdots \oplus b_n$. If the parities differ between Alice and Bob, the block is broken up into smaller subsets until the incorrect bit is found. After each of these checks, the final bit b_n is discarded. At the end of the process, Alice and Bob have the same data set, ie. errors have been corrected.

After information reconciliation, privacy amplification occurs. This process was first mentioned in Bennett, Brassard and Robert(1988) and now has been extended to classical information theory. From the error rate R above, the maximal number of bits k known to Eve is calculated. An arbitary security parameter s is then chosen that determines the amount of information that should be reduced from Eve's knowledge. Alice and Bob then choose at random $n - k - s$ bits from the sifted key, where n is the number of bits in the key. The parities P_i of these subsets become the new sifted key. By choosing s accordingly and with sufficiently large n, the amount of information Eve receives can be kept to a minimum. Eve's observed information is on the order of $1/2^s$. Thus, at the end of the BB84 protocol, Alice and Bob share an identical secret key which can be used as a one-time pad. The protocol eliminates the need for direct transfer of the secret key, which is the only place the symmetric key system can be compromised.

Quantum key distribution is generally susceptible to attack in non-ideal situations, particularly with regards to technological limitations. These hardware limitations will be discussed in the technological aspects section. The BB84 protocol is particularly vulnerable at a few key spots. First, the system requires authentication over the classical channel when Alice and Bob begin to exchange basis data. This process must be bootstrapped with an existing classical secret key. Thus, if Eve is already aware of the initial secret key, she can simply imitate Bob without the need to clone exchanged quantum states. The process through which Alice and Bob start with an initial secret key and develop stronger secret keys is known as *quantum secret growing*.

Many new strategies for breaking BB84 focus on collective and joint attacks [5]. In the collective attack, Eve attaches a probe qubit to each bit that Alice sends, whereupon Eve performs a unitary operation on the product states. Eve then sends Bob the qubit. Once the protocol is finished, Eve measures all of the probe bits together. At this point, a large amount of information has been collected by Eve over the classical channel. This is a multibit but uncorrelated attack, and has been shown to give Eve more information than individual attacks [11]. Instead, the joint attack works by entangling all of the states sent from Alice to Bob first, performing a unitary operation and then sending the states to Bob. After waiting for the protocol to end, she then performs her measurement on her entangled probe states [5]. No matter which attack is used on the ideal BB84 protocol, one rule always applies: the more information one gains about the exchange, the more errors are introduced. Thus, Eve must be sure not to increase the QBER past the point of being recognized by Alice and Bob's error checking techniques. Regardless of these advancements, it has been shown that security is still possible even against the strongest general joint attacks, discussed in Biham [11].

Other protocols are actively being researched. In ad-

dition to BB84, in 1992 Charles Bennett discovered that only two nonorthogonal states are necessary for quantum cryptography. Although the states are theoretically incompatible, they are more easily distinguishable at the cost of some loss [4]. The quantum channel must be monitored for attenuation to ensure that no eavesdropper is on the line. In addition, a protocol exists based around the EPR paradox. The quantum channel between A and B is eliminated and replaced with a source which sends entangled states to A and B. The source can emit the states in the same basis chosen in the same manner as in the BB84 protocol, after which the protocol continues as before. Instead of checking the QBER, Alice and Bob can now test Bell's inequalities, which Ekert argues demonstrates security [6]. These inequalities test the extent to which the states are entangled, rather than being the linear combination of product states which are not entangled.

Technological aspects: The original demonstration of QKD was performed in Bennett's lab at IBM in 1992 at a distance of 30 cm [4]. Contemporary experiments involve two regimes: transmission of quantum information through free space or over optical fiber. Transmission of quantum information through free space utilizes many existing technologies, particularly efficient photon counters at frequencies of approximately 770 nm. Photon polarization is largely unaffected by the atmosphere at this frequency. An advantage of the free space technique is that signal attenuation is much smaller than that of the optical fiber. However, atmospheric conditions can affect transmission, particularly on days without clear weather. Specifically, atmospheric turbulences due to temperature gradients can introduce jitter into the signal on the order of 0.1 seconds. Using reference pulses compensates for these effects [7]. In the experiment performed by Hughes, between 100 and 2000 sifted key bits were transferred per one second quantum transmission both during the day and at night [7].

The other regime, transmitting quantum information over optical fibers, reduces the noise associated with free space transfers. Modern optical fibers have attenutation levels as low as 0.35 dB/km at 1310 nm and 0.2 dB/km at 1550 nm [4]. Singlemode optical fibers are particularly fit for transferring single polarized photons. It is well-known that degenerate polarization modes exist in optical fibers with perfect cylindrical symmetry; problems arise in non-ideal fibers which lack this symmetry. In this case, the polarization of a photon oscillates as it passes down the fiber. This is a major problem when one considers how essential photon polarization is in protocols such as BB84 when establishing a set of nonorthogonal bases.

For optical quantum cryptosystems, methods for producing and detecting single quanta are under intense research. Ideally, a two-level quantum system would exist which only produces one photon at a time. Photon emitters which produce more than one photon during one event introduce vulnerabilities into the system. Multiple photon production can be exploited through beam-splitting techniques [8]. Promising research has been done into single nitrogen-vacancy centers, luminescent defects in diamond. These centers have a high radiative quantum efficiency at room temperature plus a short decay time. Excitation by a 532 nm laser beam causes the diamond to fluoresce at 700 nm, exhibiting photon anti-bunching at room temperature [9].

Conclusion and Outlook: The current state of quantum cryptography is at the frontier of applied and theoretical physics. While much active research has been committed to the implementation of QKD protocols, the limiting factors are largely technological. Innovations such as the single-photon laser and detector will result in nearly perfectly secure QKD systems.

References

[1] G. Benenti, G. Casati and G. Strini, *Principles of Quantum Computation and Information, Volume I: Basic Concepts*, World Scientific, New Jersey, 1st Edition, 2004.

[2] D. Brußand G. Leuchs, *Lectures on Quantum Information*, Wiley-Vch, Weinheim, 1st Edition, 2007.

[3] M. Bellac, *Quantum Information and Quantum Computation*, Cambridge University Press, New York, 1st Edition, 2006.

[4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *submitted to Rev. Mod. Phys.*, Group of Applied Physics, University of Geneva, February 1st, 2008.

[5] R. Gelles, *Security of Quantum Key Distribution Against Collective Attacks*, Technion IIT, September 8th, 2005.

[6] Ekert. A, Phys. Rev. Lett. 67, 661-663 (1991).

[7] R. Hughes, J. Nordholt, D. Derkacs and C. Peterson, *Practical free-space quantum key distribution over 10 km in daylight and at night*, Los Alamos Physics Division.

[8] M. Dusek, O. Haderka and M. Hendrych, *Generalized beam-splitting attack in quantum cryptography with dim coherent states*, Optics Comm., October 1999.

[9] Kurtsiefer, C. Phys. Rev. Lett. 85, 290293 (2000).

[10] BB84 and Ekert91 Protocols, *http://www.quantiki.org/wiki/BB84_and_Ekert91_protocols*, Quantiki.

[11] E. Biham, M. Boyer, P. Boykin, T. Mor, V. Roychowdhury, J. Cryptology (2006) 19: 381439.