Quantum Cryptography

Rishad Rahman
Massachusetts Institute of Technology
(Dated: May 5, 2015)

This paper is intended to develop and analyze cryptographic tools which rely on the postulates of quantum mechanics. For a while employing provably secure communication just existed in theory because of the key distribution problem. As a result public key cryptography was invented so that parties would not need to worry about the privacy of their keys but rather the unproven difficulty of breaking certain cryptosystems. We shall see that the Quantum Key Distribution bridges the gap between the two by allowing parties to be confident in the privacy of their keys hence allowing provably secure communication via private key cryptography.

I. INTRODUCTION

A. Quantum Measurement

Before diving into the world of Alice and Bob, we must first take a step a back and question what led to the study of quantum cryptography: quantum information. Information in the quantum perspective is measured using states rather than bits. In the language of quantum information, a qubit is any normalized state of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|0\rangle, |1\rangle$ are orthogonal vectors of a 2-dimensional vector space. The state $|\psi\rangle$ represents the ensemble of bits $I = \{0 : |\alpha|^2, 1 : |\beta|^2\}$. Note that another relevant basis is the rotated basis $\{|+\rangle, |-\rangle\} = \left\{\frac{|0\rangle-|1\rangle}{\sqrt{2}}, \frac{|0\rangle+|1\rangle}{\sqrt{2}}\right\}$. If we want to increase the amount of information represented, then we naturally extend this using quantum mechanics by using tensor products of individual qubits to get the probability distribution of the whole multi-particle state. Mathematically for n qubits this is represented as

$$|\psi\rangle = \sum_{c_{n-1}=0}^{1} ... \sum_{c_1=0}^{1} \gamma_{c_{n-1}c_{n-2}...c_0} |c_{n-1}c_{n-2}....c_0\rangle \quad (1)$$

where we use the convention $|00\rangle = |0\rangle \otimes |0\rangle$. We can interpret $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ as the ensemble of bits $I = \{00 : |\alpha_{00}|^2, 01 : |\alpha_{01}|^2, 10 : |\alpha_{10}|^2, 11 : |\alpha_{11}|^2\}$. Hopefully by now you can see that quantum information is going to be a probabilistic model. However at this point one might wonder how that might be useful, representing an ensemble of information using particles. The key here is the core of quantum mechanics: measurement. Let us review quantum teleportation, a famous example where the rules regarding measurement enable one party to send a quantum state to another, completely intact. Alice starts off with a qubit, $|\psi\rangle$, which she wants to transmit to Bob. First of all Alice may know nothing about the state, but even if she did it could be very difficult Bob to recreate the state. Instead we assume Alice and Bob each of whom start off with half of an EPR pair $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ which will assist in the "teleportation". The full analysis is performed in most introductory textbooks[1], but in brief Alice interacts her particle with $|\psi\rangle$ which creates the state $|\psi\rangle \otimes |\Psi\rangle$. Then Alice performs a measurement of her two particle system that uniquely determines Bob's state, as a result of entanglement, which in turn Bob can transform into $|\psi\rangle$ as long as he knows the result of the measurement. No matter what measurement Alice makes, Bob always has a way of retrieving $|\psi\rangle$ although at the expense of Alice losing the state. The crucial point to get away with here is that entanglement and measurement here both played a role in the teleportation scheme which was successful as a result of quantum mechanical postulates and we will see later how this applies to cryptographic schemes as well. Now let us have our first taste of cryptography in the quantum mechanical sense. Suppose Alice has a state $|\psi\rangle$ which she might use for certain purposes i.e. communicating with Bob. The no-cloning theorem states that another person Eve cannot create a copy of $|\psi\rangle$. Mathematically this means that Eve cannot find a unitary transformation U such that $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$ but physically this means that there is no way for Eve to run away with the state's information without letting Alice know i.e. she either steals the particle or performs a measurement. Keep this idea in mind when we discuss the Quantum Key Distribution, which states something very similar: Eve cannot eavesdrop on communication between Alice and Bob without disturbing the system and hence making her presence known. This is about all the background we need to at least be comfortable with the intuition behind Quantum Cryptography but more reading on the theory of quantum computing and information is suggested since there are still many things this paper will not discuss. One particularly interesting example is the entropy associated with a system using qubits and how this relates to how much information can be leaked which is actually used in the analysis of a lot of cryptographic protocols.

B. Cryptography

The most intuitive form of cryptographic communication adopts the following protocol: Alice applies a transformation to the message she wants to send $m \to f(m)$, transmits the encrypted message to Bob who then decrypts it using the inverse transformation f^{-1}. Indeed many historic forms of communication, e.g. SCYTALE

and the Caesar cipher, do adopt this scheme whose security depends on whether or not f, the method of communication, is secret. Instead most modern cryptosystems uses protocols which are pubic but also dependent on *keys* i.e. the transformation is f_k and the inverse is $f_k^{-1} = g_{k'}$ where k is the encryption key and k' is the decryption key. This can be done in one of two ways: *public* or *private* key cryptography. In the former, encryption is done via a public key and decryption via a private key while in the latter both are done via private keys. The key difference between the two is that public key systems rely on the *computational difficulty* of finding k' given k e.g. this requires factoring large numbers in RSA, while private key systems rely on a secure method of generating keys i.e. a *key distribution*. The problem with the former is that many problems critical to cryptography such as factoring have yet to be proven substantially hard i.e. no polynomial time algorithm exists, and that the implementation of quantum computers may break the computational barrier as well. On the other hand in a private key cryptosystem, Alice and Bob need to determine a set of keys before communication begins either in person or via a channel which they are certain will not be tempered with. As one can imagine, this is very difficult to maintain as Alice and Bob would have to devise a scheme that will inform them of any kind of interference that may occur. The Quantum Key Distribution patches this hole by using qubits to generate the keys and then use the laws of quantum mechanics to argue the security of the protocol since Eve cannot break quantum mechanics. Before we move on to the discussion of QKD, let us verify that secure communication is possible after the generating the keys. A well-known simple protocol for private-key cryptography is the Vernam cipher: if the message is in base b, encrypt the ith bit by computing $m_i' = (m_i + k_i) \bmod b$ then decrypt by $(m_i' - k_i) \bmod b = m_i$. It can be shown that if the keys are chosen randomly, fit the length of the message, and are not repeated then the Vernam cipher is *perfectly secure*[2] in the sense that it is impossible to obtain the original message. Thus if QKD works, our keys are secure so we will never have to worry about our messages being exposed.

II. QUANTUM KEY DISTRIBUTION (QKD)

Informally, the purpose of the Quantum Key Distribution is to prevent eavesdropping. To be a bit more precise, QKD is a protocol which allows Alice and Bob to generate private keys over a public quantum channel. It is *provably secure* in the sense that any attempt at obtaining information from the channel will be rendered useless as the two parties will not use the key bit generated from such an instance with high probability. We already noted that the difference between QKD and familiar classical encryption schemes such as RSA is that the latter can be broken with great computational difficulty while the former uses the laws of quantum mechanics to generate private keys with high probability. We first note that Eve cannot gain information from the channel between Alice and Bob unless she disturbs it. The statement is similar to the no-cloning theorem and we will present it mathematically. Because Eve is trying to obtain information from a state $|\psi\rangle$ without measurement, she will need to interact her own state, $|u\rangle$ with it and since she doesn't want disturbance we have the condition

$$U(|\psi\rangle \otimes |u\rangle) = |\psi\rangle \otimes |v\rangle \tag{2}$$

Of course Eve wants this transformation to work for any state and since she wants to discern states based on the information she receives, there must exist $|\phi\rangle$ such that

$$U(|\phi\rangle \otimes |u\rangle) = |\phi\rangle \otimes |v'\rangle \tag{3}$$

where $|v\rangle \neq |v'\rangle$. Taking the inner product between (3) and (4) tells us immediately that $\langle v|v'\rangle = 1$ unless $|\psi\rangle$ and $|\phi\rangle$ are orthogonal. Even if two orthogonal states were sent, Eve has no way of knowing if the states are kept private during transmission so she cannot guarantee not disturbing the state. We will present two common protocols, BB84 and E91 by first stating the protocol and then analyzing the importance of each step in an effort to realize at the end why the channel is secure under some basis measurement by Eve. Note that secure in the informational sense implies that Eve will have a "hard" time getting the information that she wants. We will see that obtaining information in QKD protocols is made hard by using the laws of quantum mechanics to control the likelihood of Eve obtaining information without detection. Also note that two additional measures taken at the final stages of QKD protocols which we will not discuss are *information reconciliation* and *privacy amplification*. The former corrects the error between Alice's key bits and the ones Bob receives while the latter increases the uncertainty that Eve has about the shared key while losing an acceptable amount of data, so it is easy to see why they are important in communication and can only help QKD.

A. Protocol BB84

We borrow the description of the protocol from [1]:

1. Alice chooses $(4 + \delta)n$ random data bits.
2. Alice chooses a random $(4+\delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
3. Alice sends the resulting state to Bob.
4. Bob receives the $(4 + \delta)n$ qubits, announces this fact, and measures each qubit in the $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis at random.
5. Alice announces b.
6. Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not,

abort the protocol and try again). They keep $2n$ bits.

7. Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8. Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.

If Alice wants to encode a, then b decides what state $|a\rangle$ Alice will send. As a result Bob will receive some state $\mathcal{E}|a\rangle$ where $\mathcal{E}$ is a result of interference, whether from Eve or the environment. Note that neither Bob nor Eve has any idea what the state is since thus far only Alice knows what b is. If Eve were to interfere, it would have to be before Bob receives $|a\rangle$. Note that at step 4 that Bob is in a sense, reverse-engineering as accurately as possible Alice's encryption. Once b is announced, Alice and Bob can figure out which of Bob's measurements aligned with Alice's encoding and this happens for at least $2n$ bits with at least $1 - e^{-\frac{1}{2}\frac{n\delta}{\delta+4}}$ probability[5]. At this point, if transmission was intact then the remaining $2n$ bits that Alice and Bob have match up perfectly and steps 7-8 serve to check whether there was any interference at all. It may be due to a noisy channel but the effect due to eavesdropping is much larger. Eve must make measurements using a random basis and if she chooses from $Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$, she will be correct $1/2$ of the time and incorrect the other $1/2$. When Eve is incorrect Bob keeps the state with probability $1/2$ as well so that the expected amount of error is a non-trivial 25 percent. Alice has control on n and δ so she can make the probability of undetected eavesdropping extremely small hence BB84 is secure from this method of measurement. Of course Eve may try a different set of basis and also alter the number of bases she chooses from but it is relatively easy to show that the Z, X basis achieves a maximum correct measurement probability of $1/2$. We can now see theoretically why QKD is significant in the world of cryptography and not very contrived as long as one holds quantum mechanics very dearly. Not only that, but the BB84 protocol has been realized with relative ease which makes it even more astonishing! A schematic can be found in [1] but essentially what the setup does is prepare photon states from a laser which Alice then polarizes to prepare $|0\rangle$ and $|1\rangle$. Bob then has a device which can analyze the polarization so he can make his measurements. Other than that, only a few other precautions have to be taken so that the sensitivity of the setup doesn't interfere with the experiment. QKD has been realized for distances exceeding 40 km thus far but who knows where it will take us in the future.

B. Ekert/EPR/E91 Protocol

The idea behind the "EPR" protocol follows from the use of the entangled EPR States and the EPR definition of reality which states that that if an observable can be measured without disturbing a system, then there exists an element of physical reality which corresponds to the observable. This would imply that Eve would have other methods of obtaining information about a system without disturbing it. Fortunately for Alice and Bob, quantum mechanics has held experimentally thus far and so under the guidance of Bell's Inequality they can take advantage of entangled states for the following extraordinary application of non-locality which we adapt from [2].

1. Within the channel, a source of states $|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ emits the first set of particles to Alice and the second set to Bob.

2. Alice performs measurements in either the Z_0, $Z_{\frac{\pi}{4}}$, or $Z_{\frac{\pi}{2}}$ basis where Z_θ is the Z-basis $\{|0\rangle, |1\rangle\}$ rotated by θ degrees[4].

3. Bob performs measurements in either the Z_0, $Z_{-\frac{\pi}{4}}$, or $Z_{\frac{\pi}{4}}$ basis.

4. After the measurements, they publicly announce the basis they used at each step.

5. They divide the measurements into two groups: the first of which was done under the same basis and the second all others.

6. Using the measurements in the second group, Alice and Bob estimate the correlation coefficient for each pairs of angles θ_i, θ_j:

$$E(Z_{\theta_i^A}, Z_{\theta_j^B}) = [P_{++} + P_{--} - P_{+-} - P_{--}](Z_{\theta_i^A}, Z_{\theta_j^B}) \tag{4}$$

   using the number of measurements

$$P_{\pm\pm} \to \frac{N_{\pm\pm}}{N_{++} + N_{+-} + N_{-+} + N_{--}}$$

7. Using $\{\phi_1^A, \phi_2^A, \phi_3^A\} = \{0, \frac{1}{2}\pi, \frac{1}{4}\pi\}$ and $\{\phi_1^B, \phi_2^B, \phi_3^B\} = \{0, -\frac{1}{4}\pi, \frac{1}{4}\pi\}$ they compute

$$S = E(Z_{\theta_1^A}, Z_{\theta_3^B}) + E(Z_{\theta_1^A}, Z_{\theta_2^B}) + E(Z_{\theta_2^A}, Z_{\theta_3^B}) - E(Z_{\theta_2^A}, Z_{\theta_2^B}) \tag{5}$$

8. If $S \approx -2\sqrt{2}$, with the offset depending on how secure Alice and Bob want to be, Alice and Bob can start creating keys using the first group of particles formulated in step 5 which are anti-correlated.

One may notice that the calculation of S using the correlation coefficients is vaguely similar to that seen in a discussion of Bell's Inequality so we will briefly perform

the expected calculation below where we implicitly ignore Z:

$$\begin{aligned}
&\left[\left|\theta_+^A\right\rangle\left\langle\theta_+^A\right| \otimes \left|\theta_+^B\right\rangle\left\langle\theta_+^B\right|\right]|\psi\rangle = \\
&\left[\cos\left(\frac{\theta^A}{2}\right)\sin\left(\frac{\theta^B}{2}\right) - \sin\left(\frac{\theta^A}{2}\right)\cos\left(\frac{\theta^B}{2}\right)\right]\left|\theta_+^A\right\rangle\otimes\left|\theta_+^B\right\rangle \\
&= \sin\left(\frac{\theta^B-\theta^A}{2}\right)\left|\theta_+^A\right\rangle \otimes \left|\theta_+^B\right\rangle \\
&\Rightarrow P_{++} = \frac{1}{2}\sin^2\left(\frac{\theta^B-\theta^A}{2}\right) \quad (6)
\end{aligned}$$

Through similar calculations we get

$$P_{+-} = P_{-+} = \frac{1}{2}\cos^2\left(\frac{\theta^B-\theta^A}{2}\right) \quad (7)$$

$$P_{--} = \frac{1}{2}\sin^2\left(\frac{\theta^B-\theta^A}{2}\right) \quad (8)$$

$$E(\theta^A,\theta^B) = -\cos(\theta^B-\theta^A) \quad (9)$$

$$\begin{aligned}
S &= -3\cos(\frac{\pi}{4}) + \cos(\frac{3\pi}{4}) \\
&= -2\sqrt{2} \quad (10)
\end{aligned}$$

However the CHSH inequality (generalized Bell's) states that if there were local hidden variables then $-2 \leq S \leq 2$. We can relate this to interference from Eve from the fact that $|\psi\rangle$ is a maximally entangled state in the sense that it maximizes $|S|$. Therefore we can see that Alice and Bob are clearly at an advantage here since they decide which states to measure and at random. Eve cannot elicit any information before the measurements take place so her only option is to guess the bases Alice and Bob decide to measure in. However interference introduces physical reality and hence the states will not be maximally entangled anymore so the value of $|S|$ will decrease showing that E91 is secure. This sort of security is slightly more general than what we argued in BB84 since there are fewer restrictions on the types of measurements Eve can make as they will all lead to lowering the physical quantity $|S|$. In the matter of Attack and Security proofs that there are measures Eve can try before making measurements but they are still futile against QKD. Compared to using approximately half of the states in BB84 as key bits, we see that on average out of every 9 measurements Alice and Bob make during E91, 4 are used for calculating S and 2 are used for creating keys which makes it less efficient. On the other hand E91 one can use a single photon source in a communication network while BB84 requires one per pair of communicators so we see that there is an nice tradeoff.

C. Attack and Security Proofs

We may naively think by now that Alice and Bob now have what may seem like an impenetrable defense. All we have shown is that QKD is secure against single qubit measurements but there may be other more intricate attack strategies Eve may be willing to try, some of which we summarize below[3]:

- Entanglement Based Attacks: For the BB84 protocol, Eve can entangle i.e. probe the state Alice sends to Bob with an EPR state and then wait until Alice publicly announces her basis choice to start making measurements using the probe.
- Photon Number Splitting: Practical applications of QKD use lasers which emit coherent pulses that occasionally emit multi-photon states. When this happens Eve takes one of the photons, lets the rest go to Bob and proceeds to measure once Alice announces the basis.
- Trojan Horse: Eve interferes with the Alice's and Bob's apparatus directly by sending light pulses to them and then uses the reflected pulse to find out their basis choices.

Separate arguments can be made against each kind of attack but a proof does exist which shows BB84 is secure against an attack using any series of quantum mechanical operations as long as certain conditions, such as using an approximately single-photon source, apply[6]. Practical apparatuses use weak-coherent lasers though so attacks such as the Trojan Horse leave BB84 susceptible unless improvements are made in its realization in the future.

III. DISCUSSION

We have now completed our brief dive into the quantum aspect of modern cryptography and so we summarize the most significant parts to take away without the complete analysis below:

- Some of the more common classical cryptographic schemes are either secure under certain computational assumptions in public key cryptography or flaky in the matter of key distribution in private key cryptography.
- The Quantum Key Distribution solves the key distribution problem by using qubits to generate keys and so Eve must abide by the rules of quantum mechanics when trying to gather information. As a result there are limitations to her plan of attack since Alice and Bob control which qubits to communicate with.
- QKD protocols such as BB84 and E91 exploit the above by noticing significant differences in measurable quantities when interference is involved. BB84 is simpler in the sense that it is easy to implement, while E91 is more interesting in the sense that it exploits the invalidity of physical reality in quantum mechanics. However the intuition behind the security for both protocols are very similar in the sense

that Eve is either forced to make random measurements or interfere with the protocol through more intricate means.

- There exist security proofs for general attacks against QKD protocols such as BB84 but the limitations of equipment today prevent us from taking hand of the full security promised by them.

Although quantum cryptography has made many significant developments, a lot of attention in present time has revolved around the implications of quantum computing. A quantum computer can break many classical and widely used public key schemes such as RSA since the computational power of a quantum computation is greater than that of classical computation. However this does not mean all hope is lost; breaking one scheme does not imply breaking all schemes nor cryptography. Indeed there is an entire subject matter devoted to the study of cryptography algorithms after quantum computers called post-quantum cryptography[7]. Cryptographers have already developed systems in which there are currently no known attacks by a quantum algorithm and we can only hope for a good justification of their security in the future. From this and the discussion of QKD we see that cryptography is still a blooming field and that we must always remember both the implications and limitations of quantum mechanics in such an area.

---

[1] I. L. Chuang and M.A. Nielsen, *Quantum Computation and Quantum Information, 10th Ed.* (Cambridge University Press, Cambridge, UK, 2010) Ch 12.6

[2] D. Bowmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information* (Springer-Verlag, Berlin, 2000), Ch 2.

[3] C. Kollmitzer and M. Pivk, *Applied Quantum Cryptography* (Springer-Verlag, Berlin,2000), Ch 5.

[4] For simplicity we assume the source are entangled electron states but for practical use, a photon source is used which is of spin 1 and as a result the angle of rotations would be halved as a result, see [2] for reference.

[5] Follows from Chernoff Bound.

[6] P. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol* (2008).

[7] D. Bernstein, J. Buchmann, and M. Pivk, *Post-Quantum Cryptography* (Springer-Verlag, Berlin,2008).