A Survey and Simulation of Three Quantum Key Distribution Protocols

Conner Taylor
cotaylor@mines.edu

***Abstract*—Private-key ciphers such as the One Time Pad are the only cryptographic systems with mathematically proven security, even against an adversary using a quantum computer. However, the One Time Pad is rarely used in practice due to the difficulty of secretly generating and distributing the long, random keys it requires. Quantum key distribution algorithms exploit the physical properties of quantum bits to provide a method for two parties to establish a shared key with guaranteed security. This paper will examine three of the most common protocols for quantum key distribution and provide a basic simulation and analysis of each.**

I. Introduction

The infeasibility of large-scale key distribution for private-key cryptography has led to the widespread adoption of public-key ciphers such as RSA, which are not quantum-safe. The most secure public-key ciphers today can be broken in polynomial time by an opponent with sufficient quantum computing ability. Quantum key distribution (hence QKD) protocols attempt to improve the usability of private-key schemes such as the One Time Pad or AES by providing a secure method for generating shared keys over public channels. After the two communicating parties perform classical techniques such as error correction and privacy amplification, the key material can be used in any private-key cipher.

QKD protocols exploit three physical laws governing quantum bits such as polarized photons or spin-$\frac{1}{2}$ particles to achieve guaranteed security:

1) It is impossible to duplicate an unknown quantum state without measuring it
2) Measuring a quantum bit necessarily disturbs its state
3) It is impossible to measure a quantum state in non-compatible bases simultaneously

These properties make it impossible for an eavesdropper to gain information about a quantum key without changing it. We assume two parties, Alice and Bob, wish to establish a shared key while minimizing their mutual information with an eavesdropper, Eve. Even if Eve is allowed to intercept and modify Alice's and Bob's communication over the quantum channel, she will be unable to conceal her measurements and will be detected through classical error analysis. We assume that Eve is also capable of intercepting the classical communication between Alice and Bob, but that she is unable to alter their messages in any way. Therefore, as long as Alice and Bob use an authenticated classical channel and perform error correction and privacy amplification on their keys, Eve will be unable to gain any useful information.

This report will focus on three major protocols for quantum key distribution, namely the BB84 protocol proposed by Bennett and Brassard[1], the B92 protocol proposed by Bennett[2], and the E91 protocol proposed by Ekert[3]. Section II will contain background material on classical cryptography and quantum bits as well as the motivation of this project. Section III will describe the three chosen protocols and compare their strengths and weaknesses. Section IV contains a description of the three simulations, their corresponding unit tests, and results. Section V will discuss the current state of QKD and an alternative six-state protocol. Solutions to selected exercises from Nielsen & Chuang's *Quantum Computation and Quantum Information* as well as the source code for the simulations will be included in the appendix.

II. Background

A. Classical Cryptography

Most electronic communications today are encrypted using a public-key cipher such as RSA[4]. Public-key algorithms are convenient for everyday use because, unlike private-key systems, they do not require a unique shared key for each pair of users who wish to communicate. Instead, each user possesses a private key, which is used for authentication and digital signing, and a public key, which provides confidentiality. As a result, for a system with n users, any pair of whom wish to communicate, a public-key system only requires $n(n-1)$ total keys, $2n$ of which are unique. For comparison, a similar system using private-key cryptography would require $n(n-1)/2$ unique keys (see Appendix A1). For example, a system with 100 users would require 200 unique keys using RSA and 4950 unique keys using a private-key cipher.

However, the limitations of public-key cryptography lie in its reliance on problems which are difficult but not computationally infeasible. The most commonly used public-key cipher, RSA, relies on the difficulty of factoring composite integers[4]. Another type of public-key system, the elliptic curve cipher, relies on the difficulty of computing discrete logarithms[5]. These systems are only considered secure because no polynomial-time algorithm has been

found to solve either of these problems. It has been shown that a network of computers can solve RSA classically in sub-exponential time[6], and the lower bound on time to solve these problems has not been proven. Additionally, n attacker with a sufficiently complex quantum computer can break RSA and elliptic curve ciphers in polynomial time[7]. Although a quantum computer capable of performing Shor's algorithm on 2048-bit RSA keys is not yet practical, advances such as topological quantum computing may render public-key cryptography obsolete in the near future.

Unlike public-key schemes such as RSA, private-key ciphers require the generation of a new key for every pair of communicators. While this requires a much larger amount of key material, the resulting ciphertext is more secure as it does not rely on the infeasibility of solving difficult problems. Instead, the One Time Pad cipher guarantees that the ciphertext is unbreakable through either brute force or cryptanalysis. The One Time Pad is one of the simplest examples of a private-key cipher. It requires a truly random key at least as long as the message to be encrypted. To encrypt, the sender adds the key (modulo 2) bitwise with the message, and as long as the sender and recipient have the same key the recipient can perform the same operation to decrypt. This cipher is perfectly resilient to brute force attacks, since any number of valid plaintext messages can map to the same ciphertext. Unless the attacker learns the key, it is impossible to determine which plaintext is the original message. Other private-key ciphers such as Triple DES and AES use key expansion to reduce the amount of key material required while maintaining nearly perfect security.

In practice, private-key systems are seldom used due to limitations of classical key distribution:

- Keys must be truly random, as defects in pseudo-random number generators can result in low key entropy[8].
- Keys must be exchanged in secret, classically requiring a face-to-face meeting.
- Keys must be guarded until use and destroyed afterwards.

In order for Alice and Bob to regularly exchange encrypted messages, they would have to meet in secret and generate terabytes of key material each meeting. Alternatively, they could rely on a trusted third party to generate the key material and distribute it to both of them. However, this would mean that the key is not known only to Alice and Bob, intoducing a new potential attack vector and making the key unusable for digital signing. QKD protocols address these limitations of private-key cryptography by providing a method for Alice and Bob to generate truly random, shared key material over long distances, even in the presence of eavesdroppers.

B. Quantum Mechanics

Part of the security of QKD arises from the fact that neither party intends to use any specific key at the outset. Instead, the key is generated truly randomly from quantum mechanical phenomena such as thermal noise[9]. In most QKD protocols, we assume Alice begins by generating a long string of truly random classical bits. Her goal is to encode this classical information in the states of quantum bits which are subject to the physical laws discussed in Section I.

Quantum bits (hence 'qubits') are binary systems like classical bits, with a "0" state, $|0\rangle$, and a "1" state, $|1\rangle$. Unlike classical bits, however, a qubit can exist in a linear combination of these states called a superposition:

$$\alpha\,|0\rangle + \beta\,|1\rangle\,.$$

According to the Measurement Postulate[10], measuring a state

$$|\Psi\rangle = \sum_i \alpha_i\,|\phi_i\rangle$$

with respect to the basis $B = \{|\phi_i\rangle\}$ outputs the label i with probability $|\alpha_i|^2$ and leaves the system in state $|\phi_i\rangle$. Because measurement necessarily collapses a superposition state to one of its basis states, it is impossible for Eve to measure Alice's qubits without disturbing them and revealing her actions.

In quantum mechanics, measurements correspond to operators called 'observables'. The eigenvectors of an observable represent the possible measurable values of a quantum state and thus form an eigenbasis for the state space in which the observable exists[11]. If two observables share at least one common eigenbasis, they are said to 'commute' and can be measured simultaneously. If they do not commute, the Heisenberg Uncertainty Principle requires that measuring one observable imparts a minimum degree of disturbance on the other[12]. Thus, it is impossible to measure a quantum state with respect to incompatible bases simultaneously.

The No-Cloning Theorem states that it is impossible to clone an unknown quantum state[13]. To prove this, assume that there exists some unitary operator U which, when applied to a quantum state $|\Psi\rangle$, produces a copy of the original state along with the original state. That is,

$$U\,|\Psi\rangle \rightarrow |\Psi\rangle\,|\Psi\rangle\,.$$

The contradiction occurs when U is applied to a superposition such as

$$\alpha\,|0\rangle + \beta\,|1\rangle\,.$$

Using the linearity of unitary operators, the application of U on such a superposition can be written as

$$U(\alpha\,|0\rangle) + U(\beta\,|1\rangle) \rightarrow \alpha\,|00\rangle + \beta\,|11\rangle\,.$$

However, this is not the result we expect from our definition of cloning. A cloning operator should produce the result

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle),$$

which is the original superposition state along with an exact copy of itself. Therefore, it is not possible to clone an

unknown state[12].

Any two-level quantum mechanical system can be used to implement a qubit. The most common physical examples of qubits are:

- The energy states of electrons in an atom.
  - $|0\rangle$, $|1\rangle$ could be defined as ground and excited states, respectively.
- The magnetic spin states of spin-$\frac{1}{2}$ particles such as electrons.
- The polarization states of photons.

This paper will assume qubits are implemented as polarized photons, with the state $|0\rangle$ representing vertical polarization and the state $|1\rangle$ representing horizontal polarization. The possible polarization states of a photon can be visualized geometrically as three-dimensional complex vectors bounded by a unit sphere called the Bloch Sphere (see Fig. 1). For example, the pure state $|0\rangle$, representing vertical polarization, corresponds to the unit vector in the $\hat{\mathbf{z}}$ direction. Pure superposition states, where $\theta \neq \{0, \pi\}$ and $|| \, |\psi\rangle \, || = 1$, correspond to polarization axes that lie somewhere between horizontal and vertical polarization. If a photon is measured with respect to the $\{|0\rangle, |1\rangle\}$ basis, the probability it will collapse to either basis state depends on θ as well as ϕ, the relative phase between the basis states:

$$|\psi\rangle = \cos(\frac{\theta}{2}) \, |0\rangle + e^{i\phi} \sin(\frac{\theta}{2}) \, |1\rangle \, .$$

Measuring a photon's polarization with respect to any basis is equivalent to performing a rotation operation and measuring the resulting state in the computational basis, $\{|0\rangle, |1\rangle\}$. For example, to measure the pure state $|0\rangle$ in the Hadamard basis, $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$, one can increment θ by $\frac{\pi}{2}$ to get the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

which will collapse to either the $|0\rangle$ or the $|1\rangle$ state with equal probibility when measured in the computational basis. The QKD protocols examined in this paper leverage the fact that the results of a measurement depend on the basis in which the measurement in performed to guarantee that any eavesdropping will be detected with high probability.

III. Survey

A. The BB84 Protocol

The BB84 protocol, based on Stephen Wiesner's work on conjugate coding[**?**], was the first QKD scheme to be proposed and is the most common QKD protocol used today. Its security relies on the fact that two non-commuting observables cannot be measured simultaneously. The protocol requires Alice and Bob to select one of two non-orthogonal bases at random when encoding or measuring a polarization state. These bases are the X basis, $\{|0\rangle, |1\rangle\}$, and the Z basis, $\{|+\rangle, |-\rangle\}$, where

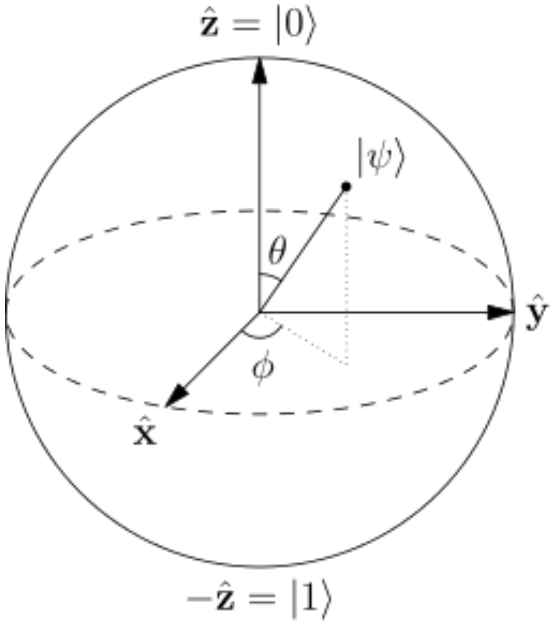

Fig. 1. The Bloch Sphere representation of a single qubit[14].

$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. We have seen that $\{|0\rangle, |1\rangle\}$ correspond to the polarization states $|\uparrow\rangle$ and $|\rightarrow\rangle$, respectively, and that $\{|+\rangle, |-\rangle\}$ correspond to the polarization states $|\nwarrow\rangle$ and $|\nearrow\rangle$.

The BB84 protocol is described as follows[1]:

1) Alice uses a truly random number generator to obtain $(4+\delta)n$ random classical bits. These bits form the 'raw key', and a subset of the raw key will form the final key shared between Alice and Bob.
2) Alice encodes each bit of her random classical bit string in the polarization state of a qubit, according to the following strategy:
   - If Alice wishes to send a "0", she sends the $|0\rangle$ state in either the X basis ($|\uparrow\rangle$) or the Z basis ($|\nwarrow\rangle$) with 50% probability.
   - If Alice wishes to send a "1", she sends the $|1\rangle$ state in either the X basis ($|\rightarrow\rangle$) or the Z basis ($|\nearrow\rangle$) with 50% probability.
3) Alice sends each polarized photon one at a time over a quantum channel to Bob, who measures each using a birefringent crystal. For each qubit, he randomly chooses to orient his crystal to measure in either the X or the Z basis. If Alice and Bob choose the same basis for encoding and decoding, Bob will measure Alice's original bit value, assuming no channel noise or eavesdropping. Otherwise, his measurement result will be completely uncorrelated with Alice's original bit (see Appendix A2).
4) After measuring the final qubit from Alice, Bob uses an authenticated classical channel to announce his chosen basis for each qubit (but keeping his measured result secret). After Bob has made his announcment, Alice

reveals the bases she used to encode the sequence and the two parties discard any bits where they chose differently. In the absence of external noise, the resulting 'sifted' key shared by Alice and Bob must be identical.

5) Alice and Bob agree to sacrifice a subset of their sifted keys to test for the presence of an eavesdropper. We will show that each time Eve measures a qubit as it travels from Alice to Bob, she will disturb the key in a detectable way with 25% probability. If Alice and Bob publicly disclose N bits from their sifted keys, they will be able to detect Eve with probability $1 - \frac{3}{4}^N$. Thus, assuming a large enough N it will be extremely unlikely for an eavesdropper to remain undetected.

BB84 Example Run (without Eve):

A's random bits	1	0	1	0	0	1	1	0
A's bases	X	Z	Z	Z	X	X	Z	X
Qubits sent	$\rightarrow$	$\nwarrow$	$\nearrow$	$\nwarrow$	$\uparrow$	$\rightarrow$	$\nearrow$	$\uparrow$
B's bases	X	X	Z	X	Z	Z	Z	X
B's results	1	1	1	0	1	0	1	0
Sifted key	1	-	1	-	-	-	1	0

Eve wishes to obtain information about Alice's qubits without being detected. In Section II, it was demonstrated that the No-Cloning Theorem prohibits Eve from making a copy of each qubit to measure later. Assume instead that Eve uses an ancillary register (hence 'ancilla') prepared in a standard state $|u\rangle$ to interact with the non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$. Her goal is to distinguish between $|\psi\rangle$ and $|\phi\rangle$ without disturbing either state and revealing her actions. Assuming this is possible, in the first case Eve obtains

$$|\psi\rangle\,|u\rangle \rightarrow |\psi\rangle\,|v\rangle$$
$$|\phi\rangle\,|u\rangle \rightarrow |\phi\rangle\,|v'\rangle\,.$$

To distinguish between the two states, $|v\rangle$ and $|v'\rangle$ must be different. However, we can show that

$$\langle v|v'\rangle\,\langle\psi|\phi\rangle = \langle u|u\rangle\,\langle\psi|\phi\rangle$$
$$\langle v|v'\rangle = \langle u|u\rangle = 1$$

since inner products are preserved under unitary transformations[15]. Thus, it must be the case that distinguishing between two non-orthogonal states necessarily disturbs one of them.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Intl. Conf. on Computers, Systems, & Signal Processing, 12 Dec. 1984.

[2] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," Phys. Rev. Lett., Volume 68, Number 21, 25 May 1992.

[3] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett., Volume 67, Number 6, 5 August 1991.

[4] R. Rivest, A. Shamir, and L. Adleman, "On Digital Signatures and Public Key Cryptosystems," Commun. Ass. Comp. Mach., Volume 21 (1978) pp. 120-126.

[5] M Rosing, "Implementing Elliptic Curve Cryptography," Manning Publications, Greenwich (1999) ISBN 1-884777-69-4.

[6] E. W. Weisstein, "RSA-640 Factored," MathWorld Headline News, 8th November (2005), http://mathworld.wolfram.com/news/2005-11-08/rsa-640/.

[7] P. Shor, "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," Siam Journal on Computing, Volume 26, Issue 5 (1997) pp. 1484-1509.

[8] N. Heninger, Z. Durumeric, E. Wustrow, J. A. Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices," Proc. 21st USENIX Security Symposium, Aug. 2012.

[9] B. Jun and P. Kocher, "The Intel Random Number Generator," Cryptography Research, Inc. white paper prepared for Intel Corp., 22 Apr. 1999.

[10] P. Kaye, R. LaFlamme, M. Mosca, *An Introduction to Quantum Computing*, Oxford UP, 2010. Print. ISBN 978-0-19-857049-3.

[11] H. Wimmel, *Quantum Physics & Observed Reality: A Critical Interpretation of Quantum Mechanics*, World Scientific, 1992. Print. ISBN 981-02-1010-8.

[12] C. Williams, *Explorations in Quantum Computing*, Springer, 2011. Print. ISBN 978-1-84628-886-9.

[13] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot Be Cloned," Nature, Volume 299, pp. 802-803. 28 Oct. 1982.

[14] Wikipedia, the free encyclopedia, "Bloch Sphere," URL: https://upload.wikimedia.org/wikipedia/commons/thumb/f/f4/Bloch_Sphere.svg/256px-Bloch_Sphere.svg.png

[15] M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information," Cambridge UP, 2015. Print.