

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 $\text{spin-}\frac{1}{2}$ 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 and their unit tests. Section V will conclude with a discussion of the practicality of QKD. Solutions to selected exercises from Nielsen & Chuang's *Quantum Computation and Quantum Information* as well as outputs from the simulations are 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, an 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, introducing 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{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:

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

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 probability 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 is 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[15], 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

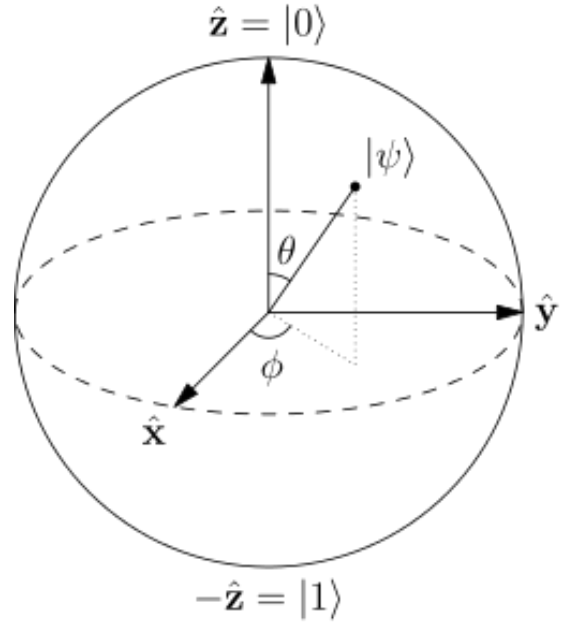


Fig. 1. The Bloch Sphere representation of a single qubit[14].

basis, $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. 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 $|\swarrow\rangle$ and $|\searrow\rangle$.

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 photon, 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 ($|\swarrow\rangle$) 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 ($|\searrow\rangle$) 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 announcement, 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 announce and then discard 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.

TABLE I
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	→	↖	↗	↖	↑	→	↗	↑
B's bases	X	X	Z	X	Z	Z	Z	X
B's results	1	1	1	0	1	0	1	0
A's key	1	-	1	-	-	-	1	0
B's 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

$$\begin{aligned} |\psi\rangle |u\rangle &\rightarrow |\psi\rangle |v\rangle \\ |\phi\rangle |u\rangle &\rightarrow |\phi\rangle |v'\rangle. \end{aligned}$$

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

$$\begin{aligned} \langle v|v'\rangle \langle \psi|\phi\rangle &= \langle u|u\rangle \langle \psi|\phi\rangle \\ \langle v|v'\rangle &= \langle u|u\rangle = 1 \end{aligned}$$

since inner products are preserved under unitary transformations[16]. Thus, it must be the case that distinguishing between two non-orthogonal states necessarily disturbs one of them.

Because of these limitations, Eve must resort to an intercept-resend strategy that will introduce bit flip errors in Bob's sifted key with high probability. Eve intercepts each of Alice's photons as they travel along the quantum channel to Bob. She measures each photon randomly in either the X or Z basis and records the result. In an attempt to disguise her interference, she re-encodes her result in her chosen basis

and forwards the new photon to Bob. As demonstrated for Bob, 50% of the time Eve and Alice will choose different bases and their bit values will be completely uncorrelated. If this is the case, Eve has a 50% chance of encoding her result such that Alice, Bob, and Eve all share the same value. By employing this strategy, Eve is able to gain information about 50% of the key. However, for each photon she measures, she has a 25% probability of introducing a bit-flip error and revealing her actions.

In practice, however, bit-flip errors often occur naturally due to imperfections in the quantum channel. One bit-flip error is not sufficient for Alice and Bob to distinguish between channel noise and eavesdropping. Instead, they must estimate a Quantum Bit Error Rate (QBER) for the channel to compare to their measured error rate. If the measured error rate deviates significantly from the QBER, Alice and Bob simply abort the protocol and try again on another channel. Thus, Eve must only measure a small subset of the $(4 + \delta)n$ qubits to minimize the number of errors she introduces.

TABLE II
BB84 EXAMPLE RUN (WITH EVE)

A's random bits	0	1	1	0	1	1	1	0
A's bases	X	Z	Z	X	Z	X	X	X
Qubits sent	↑	↗	↗	↑	↗	→	→	↑
E's bases	Z	Z	X	Z	X	X	Z	Z
E's results	1	1	1	0	0	1	0	0
New qubits	↗	↗	→	↖	↑	→	↖	↖
B's bases	X	X	Z	X	Z	Z	X	X
B's results	0	1	0	1	0	1	0	0
A's key	0	-	1	0	1	-	1	0
B's key	0	-	0	1	0	-	0	0

It is easy to see that the four states used in this protocol lie in the same plane in the Bloch sphere. The basis states of the X basis correspond to the North and South poles of the Bloch sphere, and the basis states of the Z basis correspond to the East-West antipodal points[12]. However, there are two more non-orthogonal states perpendicular to this plane which are not used in BB84. Increasing the number of bases from two to three leads to the 'six-state protocol', a generalization of BB84 which can be shown to reduce the information obtainable by an attacker (see Appendix A4).

B. Post-Processing

In the real world, assuming an imperfect channel, Alice's and Bob's sifted keys will contain errors with high probability, even in the absence of eavesdroppers. To correct these errors and guarantee their keys are identical they will need to perform some classical error reconciliation protocol. The CASCADE protocol[17] allows Alice and Bob to correct errors in their keys over a public classical channel without disclosing significant information about their keys. Using their sacrificed bits from step (5) of BB84, Alice and Bob can establish p^* ,

an estimate of the probability a bit is flipped in their sifted keys. They then proceed with the CASCADE protocol as follows[12]:

- 1) Alice and Bob choose a block size based on p^* and segment their keys K_A and K_B .
- 2) They perform their own parity measurement on each block and announce the results.
- 3) If the parity values for a given block differ, that block must contain an odd number of bit-flip errors. If this is the case, Alice and Bob perform the following recursive algorithm[17]:
 - a) Alice sends Bob the parity of the first half of her block.
 - b) Bob determines which half contains the odd number of errors by comparing his parity with Alice's.
 - c) This process is repeated until the error is found, then Bob flips his value to correct.
- 4) Alice and Bob repeat the protocol until they are confident that no errors remain.

After a sufficient number of applications, the CASCADE protocol will guarantee that Alice and Bob share the same key. Although this protocol is relatively simple to implement compared to other error correction schemes, it requires a large amount of communication overhead. Alice and Bob must announce a parity value for each block, and $\log_2 k$ bits for each k -bit block with an odd number of errors. For example, if they estimate a QBER of 5% using 1000-bit keys with $k = 15$, they will need to exchange approximately 350 parity values for a single application of CASCADE[18]. An alternative technique using sparse matrices called Low Density Parity Check (LDPC) codes[19] can be used to provide the same result with much lower overhead[20].

After error reconciliation, it is still possible for an eavesdropper to have obtained a small amount of information about the shared key. This information can come from the initial transmission of photons, assuming Eve chose a small enough N to avoid detection, or from the parities exchanged during error reconciliation. Alice and Bob should now apply a classical privacy amplification algorithm to generate a shorter, secure key that Eve has no information about.

Privacy amplification is typically accomplished using an authenticated two-universal hash function. A hash function f is two-universal if for any distinct $x_a, x_b \in X$, the random variables $f(x_a)$ and $f(x_b)$ are independent and uniformly distributed[21]. We can determine the amount of information leaked by measuring the uncertainty in Alice's and Bob's key strings. The Shannon entropy, $H(X)$, measures the uncertainty of a random variable X . Let X and Y be random variables over the finite sets $\{0, 1\}^n$ and $\{0, 1\}^r$. Then the Shannon entropy of X , $H(X)$, and the Shannon entropy of X conditioned

on Y , $H(X|Y)$, are defined as

$$H(X) = - \sum_{x \in X} Pr[X = x] \log_2 Pr[X = x],$$

$$H(X|Y) = - \sum_{x \in X} Pr[X = x|Y = y] \log_2 Pr[X = x|Y = y].$$

The mutual information[22] between two random variables X and Y , $I(X, Y)$ is defined as

$$I(X, Y) = H(X) - H(X|Y).$$

Assume Alice's original bits form string X , Bob's measurement results form string Y , and Z represents the information known to Eve. After Alice and Bob input their matching keys into an authenticated two-universal hash function, we get the result

$$I(X, Y) \approx 0.$$

C. The B92 Protocol

In 1992, Bennett[2] showed that only two non-orthogonal states are necessary to perform quantum key distribution, as opposed to the four required in BB84 ($|\uparrow\rangle$, $|\rightarrow\rangle$, $|\nwarrow\rangle$, and $|\nearrow\rangle$). This is accomplished by replacing the birefringent crystals used in BB84 with polarization filters, which transmit or absorb photons probabilistically based on the angle between the axis of measurement and the axis of polarization. For example, a vertically polarized photon measured with a vertical polarization filter will be transmitted with 100% probability, while a horizontally polarized photon will be absorbed by the same filter with 100% probability. A photon polarized at $\pm 45^\circ$ will be either transmitted or absorbed with 50% probability. It is important to note that the polarization axis of a transmitted photon is necessarily aligned with the axis of the filter, and thus the original state information is lost when measured.

The B92 protocol is described as follows[2]:

- 1) Alice uses a truly random number generator to obtain a long string of random classical bits. As in BB84, these bits form Alice's raw key.
- 2) Alice encodes each bit of her random classical bit string in the polarization state of a photon, according to the following strategy:
 - If Alice wishes to send a "0", she sends the $|0\rangle$ state in the X basis, $|\uparrow\rangle$.
 - If Alice wishes to send a "1", she sends the $|0\rangle$ state in the Z basis, $|\nwarrow\rangle$.
- 3) Bob randomly chooses one of two polarization filters to measure each photon with. The first possible polarizer is oriented such that it transmits the state $|\nearrow\rangle$ and blocks the state $|\nwarrow\rangle$. If Alice's original bit value was "1", her qubit will be absorbed with 100% probability. Otherwise it will be either transmitted or absorbed with 50% probability. Thus this filter can only test whether

Alice sent a “0”. The other possible filter transmits the state $|\rightarrow\rangle$ and absorbs the state $|\uparrow\rangle$, effectively testing for the value “1”. Thus, Bob will only obtain a measurement result for 25% of the photons sent by Alice. If Bob does obtain a result, however, he knows that his bit value for that photon is perfectly correlated with Alice’s (see Appendix A3).

- 4) After measuring the final qubit from Alice, Bob uses an authenticated classical channel to announce the photons for which he obtained a measurement result (but keeping his measured result secret). Since Alice knows the original bit values she sent, she can figure out the results of Bob’s measurements and derive the same shared key as Bob.
- 5) As in BB84, Alice and Bob attempt to detect any eavesdropping by comparing and discarding a subset of their sifted keys. They also monitor the number of qubits lost during the protocol to prevent against an attack specific to B92.

TABLE III
EXAMPLE RUN OF B92 (WITHOUT EVE)

A’s random bits	1	0	0	0	1	0	1	1
Qubits sent	\nwarrow	\uparrow	\uparrow	\uparrow	\nwarrow	\uparrow	\nwarrow	\nwarrow
B tests for	1	1	0	0	1	1	1	0
B’s results	1	-	-	0	-	-	1	-
A’s key	1	-	-	0	-	-	1	-
B’s key	1	-	-	0	-	-	1	-

While B92 requires fewer states than BB84, making it easier to implement, the fact that most of the photons are discarded leaves it vulnerable to a subtle eavesdropping strategy. While we have demonstrated that distinguishing between non-orthogonal states is impossible, Eve can simply discard failed attempts to determine Alice’s raw key with 100% accuracy[12]. The only way for Alice and Bob to detect this type of attack is to establish an expected qubit loss rate for the channel and compare it with the actual loss rate. However, if Eve controls the quantum channel while Alice and Bob perform their setup, she may be able to manipulate the expected loss rate and avoid detection. As a result of this vulnerability, B92 is rarely implemented in real-world QKD systems.

D. The E91 Protocol

The E91 protocol, developed by Artur Ekert[3], uses quantum entanglement to provide a guarantee of security. To provide context to this protocol, we must examine two assumptions made in 1935 by Einstein, Podolski, and Rosen[23]:

- Reality: The value of a measurement exists even before the measurement takes place.
- Locality: The measurement result for one object has no influence on the reality of distant objects.

In 1964, Bell demonstrated that measuring the state of one entangled particle immediately collapses the state of its complement, regardless of the distance between them[24]. This defies the theory of local realism described by EPR and represents the incompatibility between classical and quantum mechanics.

The E91 protocol is described as follows[3]:

- 1) Alice and Bob acquire n sets of entangled qubits in the singlet state

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

distributing one qubit from each pair to Alice and the other to Bob. Either party could generate the pairs and send half of the qubits to the other, or they could rely on a trusted third party to generate the entangled pairs.

- 2) For each qubit, Alice chooses an angle uniformly at random from the set

$$\phi_i^A = \{0, \frac{\pi}{8}, \frac{\pi}{4}\}.$$

She then rotates the vertical-horizontal basis by her chosen angle around the z-axis and measures the qubit with respect to the new basis. Bob then does the same, instead choosing his angle from the set

$$\phi_j^B = \{0, \frac{\pi}{8}, \frac{-\pi}{8}\}.$$

- 3) If Alice and Bob orient their measurement devices the same way, Bob’s result will be perfectly anti-correlated with Alice’s. That is, in two of the nine cases, Alice and Bob will always measure opposite bit values and can therefore establish a shared key.
- 4) The measurement values of qubits where Alice and Bob chose different measurement axes are announced and used to calculate the correlation coefficient of their measurements:

$$E(\phi_i^A, \phi_j^B) = P_{00}(\phi_i^A, \phi_j^B) + P_{11}(\phi_i^A, \phi_j^B) - P_{01}(\phi_i^A, \phi_j^B) - P_{10}(\phi_i^A, \phi_j^B),$$

where P_{00} represents the probability of Alice and Bob both obtaining 0 as the measurement result.

- 5) Alice and Bob calculate the quantity

$$S = E(\phi_1^A, \phi_2^B) + E(\phi_1^A, \phi_4^B) + E(\phi_3^A, \phi_2^B) - E(\phi_3^A, \phi_4^B),$$

composed from the correlation coefficients for which Alice and Bob chose different measurement axes. Bell’s Theorem requires that, in the absence of an eavesdropper, $S = -2\sqrt{2}$ [25]. If this does not match Alice’s and Bob’s measurements, then they detect Eve’s interference and abort the protocol.

The security of the E91 protocol lies in the fact that neither Alice nor Bob generates the key material to send to the other. Instead, the key does not exist until Alice

TABLE IV
EXAMPLE RUN OF E91 (WITHOUT EVE)

A's bases	2	2	1	3	1	1	3	1	3	1	1	2
B's bases	1	4	1	2	4	1	2	1	2	4	2	2
A's results	0	1	1	0	1	0	0	0	1	1	0	0
B's results	1	1	0	0	1	1	0	1	0	0	1	1
A's key	-	-	1	-	-	0	-	0	-	-	-	0
B's key	-	-	1	-	-	0	-	0	-	-	-	0

and Bob perform their measurements, meaning Eve cannot perform an intercept-resend attack as in BB84. Any attempt by Eve to substitute her own prepared data for Alice's and Bob's communication is the same as introducing elements of physical reality to the quantum system, bounding S to $-\sqrt{2} \leq S \leq \sqrt{2}$ and thus revealing her actions[26].

IV. SIMULATIONS

Each of the simulations prepared for this project was written in Python 2.7. Each uses the following modules:

- NumPy for random sampling and bitwise operations
- PyCrypto for cryptographic random number generation
- The Quantum Information Toolkit (QIT) to represent and measure quantum states
- Nose for unit testing

Each simulation accepts a desired key length as well as optional parameters to control eavesdropping or the QBER. It then performs the selected protocol up to the sifting phase and returns the sifted key, or failure in the case that an eavesdropper is detected. The Appendix of this report contains three outputs for the BB84 and B92 protocols:

- One run with no channel noise and no eavesdropping which yields identical keys.
- One run with a small amount of channel noise but no eavesdropping, leading to key errors but not an abortion of the protocol.
- One run with channel noise and eavesdropping, which Alice and Bob detect.

The E91 simulation does not simulate an eavesdropper due to the difficulty of implementing Eve's optimal strategy.

Three of the eleven unit tests, `test_bb84()`, `test_b92()`, and `test_e91()`, simply perform 20 trials of the appropriate protocol with a desired key size of 2048 bits and assert that a shared key is successfully established. Two of the tests, `test_decodeStateBB84_probabilistic()` and `test_getRandomBits()`, are probabilistic and assert that expected probabilities are met for large key sizes. The remaining six tests verify deterministic cases, such as measuring an entangled state along two identical axes of measurement.

V. CONCLUSION

Quantum key distribution is one of the most developed ideas quantum computing, as it is one of the only applications

of quantum computing with practical implementations in industry. However, classical public-key schemes remain the dominant method of distributing key material in the real world. The advantages of QKD over classical key distribution are immediately apparent, since breaking the security of QKD requires an attacker to violate fundamental physical laws. As technological advances lead to improvements in range and transmission rates, we may see protocols such as BB84 become the standard for key distribution in the near future.

Each of the three protocols surveyed has its own advantages and disadvantages relative to the others. The protocol most likely to be adopted on a large scale is BB84, as it is relatively intuitive, easy to implement, and provably secure. The E91 protocol, which relies on entangled particles, provides a similar guarantee of security to BB84 but is not as well-documented or intuitive, making it an unlikely candidate for a QKD standard. E91 shows potential at longer distances, however, as it can be implemented without the use of a noisy quantum channel if Alice and Bob generate their entangled pairs in person and save them until the protocol is performed. B92, while originally celebrated as a more intuitive version of BB84, will likely not see much real-world implementation due to the extra monitoring and precautions it requires.

Besides relatively poor range and transmission rates, the largest barrier to adoption for QKD is the difficulty of producing specific quantum states outside of the laboratory. In all protocols, but especially in E91, users will likely be forced to rely on a trusted third party to generate and distribute the necessary qubits. While protocols like BB84 have the potential to replace classical key distribution schemes, significant advances in hardware will be necessary before QKD becomes practical for the average user.

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] S. Wiesner, "Conjugate Coding," *SIGACT News*, Volume 15, Number 1, Jan. 1982.
- [16] M. Nielsen and I. Chuang, "Quantum Computation and Quantum Information," Cambridge UP, 2015. Print.
- [17] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," *Proc. Eurocrypt 93 Workshop on the Theory and Application of Cryptographic Techniques*, pp. 410-423, 23-27 May 1993.
- [18] J. Johnson, "An Analysis of Error Reconciliation Protocols for Use in Quantum Key Distribution," Master's Thesis, Air Force Institute of Technology, Feb. 2012.
- [19] R. Gallager, "Low-Density Parity-Check Codes," Doctoral Thesis, Massachusetts Institute of Technology, 1960.
- [20] D. J. MacKay, "Good Error-Correcting Codes Based on Very Sparse Matrices," *IEEE Transactions on Information Theory*, Jan. 1999.
- [21] R. Renner, R. König, "Universally Composable Privacy Amplification Against Quantum Adversaries," In: Kilian J (eds) *Theory of Cryptography*, TCC 2005. *Lecture Notes in Computer Science*, Volume 3378. Springer, Berlin, Heidelberg.
- [22] A. S. Ribeiro, S. A. Kauffman, J. Lloyd-Price, B. Samuelsson, and J. Socolar, "Mutual Information in Random Boolean Models of Regulatory Networks," *Physical Review E*, 77(1):011901, 2008.
- [23] A. Einstein, B. Podolski, N. Rosen, "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?" *Phys. Rev.* 47 (10), pp. 777-780. 1935.
- [24] J. S. Bell, "On the Einstein-Podolski-Rosen Paradox," *Physics*. 1, pp. 195-200. 1964.
- [25] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," *Phys. Rev. Lett.* 23 (15), pp. 880-884. 1969.
- [26] D. Bouwmeester, A. Ekert, A. Zeilinger, "The Physics of Quantum Information," Springer-Verlag, Berlin, 2000.