Quantum Key Distribution: Current Imperfections

Margarita Demkina

September 14, 2019

1 Introduction

1.1 Motivation

Quantum computers are estimated to break modern cryptography within the next few decades, and the limit of their advantages and computational power is yet to be determined [9] [2]. With their peculiar phenomenon of superposition – using qubits that can be 0, 1, or both simultaneously – they are deemed to revolutionize modern private communications and encryption methods [18]. Currently, security of most cryptosystems rely on the mathematical complexity of factoring large prime numbers or difficulty of solving discrete logarithm problems [31]. Because of the high cost of solving these problems using classical computers, cryposystems remain secure and guarantee privacy in communications. Quantum computers, however, will be able to break those systems faster with their greater computational power, enabled by qubits, which exist in several states simultaneously, decreasing the number of steps it takes a computer to process an algorithm [18].

In cryptography, it is customary to consider three main characters: Alice, the sender of the message, Bob, the receiver of the message, and Eve, the eavesdropper who tries to intercept the message. The field of cryptography is concerned with the security aspect of Alice and Bob's communication to prevent Eve from reading messages or decrypting the key.

On the other hand, coding theory, a field that is often confused with cryptography, enables clear transmission between Alice and Bob. Its main goals are to detect errors and correct them [31].

The standard problem in cryptography involves creating a method for Alice and Bob to exchange information privately, without having any previous contact. Nowadays, such systems are called *public key cryptosystem* (e.g., RSA) that use a *channel* to establish a *key*, allowing for secure communications between Alice and Bob [31]. However, the advent of quantum computers will make classical public key exchanges insecure and susceptible to quantum attacks [31]. Thus, an eavesdropper Eve will gain an access to the sent messages

– the *plaintext*. If the current security systems do not switch to more sophisticated methods of encryption and key exchanges, Eve will be able to read and meddle with any information transmitted over the internet: starting from text messages to secret corporate and governmental documents.

This paper will provide a sufficient mathematical background in group theory to formulate the discrete logarithm problem in the general form, examine a classical example of the public key exchange, give an overview of quantum computing, discuss the history of the quantum key distribution (QKD) and its mechanics, the current state of its development and implementations, and obstacles of practical applications of QKD and quantum technology. The paper's main focus will be on the potential of quantum computers, current technological imperfections, and possible future improvements to minimize eavesdropping and hacking. After all, to become trustworthy and popularized, quantum technology needs to be advanced in order to ensure security in the years to come.

For more than 30 years, starting with the publication of "Quantum Cryptography: Public key Distribution and Coin Tossing," the BB84 was described as one of the most famous quantum algorithms [3]. It has been vastly studied and analyzed by teams of mathematicians, physicists, and computer scientists from all over the world, who have addressed numerous issues with implementation of the theory. Their findings were quickly picked up by the firms wanting to take the quantum computing to the markets (e.g., IBM [16], Battelle [26], and IDQ [17]). Synthesizing theoretical papers and practices, this paper presents a detailed insight into the main obstacles in QKD. The paper incorporates findings from the articles, studies, and books from the 1970s to the present day.

1.2 Group Theory

To understand the commonly used key exchange problems and quantum algorithms, we will introduce several underlying concepts, including number theory and group theory. Group theory is a topic in Abstract Algebra that studies groups, rings, and fields. In our case, we will use group theory to describe the discrete logarithm problem and Shor's algorithm. Below are the fundamental theorems and definitions to consider:

1.2.1 "A *binary operation* $*$ on a set S is a function mapping $S \times S$ into S" [11]. For instance, addition and multiplication are binary operations on integers or real numbers. Binary operation must be a function that is defined for every element within the domain and is closed on S [11].

1.2.2 A *group* $(G, *)$ is a set G that is closed under the binary operation, such that a) the binary operation * is associative; b) there is an identity element e in G with $g * e = e * g = g$ for all $g \in G$; c) for every element a, there is an inverse a^{-1} such that $a * a^{-1} = a^{-1} * a = e$ [11].

1.2.3 H is a subgroup of G if it is a subset that is a) closed under the binary operation *; b) "with the induced operation from G is a group itself" [11]. We denote that $H \leq G$.

1.2.4 If G is a group and α is an element in G, then the *cyclic subgroup* of G is defined by $\{\alpha^x | x \text{ is an integer}\}$ [11].

1.2.5 A group G of order k is called *cyclic* if there is an element $\alpha \in G$ such that $G =< \alpha >= \{e, \alpha, \alpha^2, \alpha^3, ...\alpha^{k-1}, \alpha^k = e = \alpha^0\}$, where e is the identity element of the group [10]. Note that $< \alpha >$ represents all powers of α.

1.2.6 We say that α *generates* G and is a *generator* of G if $< \alpha >= G$ [11].

1.3 Discrete Logarithm Problem (DLP)

Similar to RSA, discrete logarithm problem (DLP) is a computationally expensive mathematical problem in number theory and has valuable applications in classical cryptography. First, we will examine DLP using a general cyclic group G. Using abstract algebra concepts, DLP can be described as following: given a cyclic group G, a generator of a group α, and a nonzero integer β, find x:

$$\beta = \alpha^x \text{ in } G \text{ and } x = L_\alpha(\beta) \text{ [31][11].}$$

A more concrete formulation of DLP comes from studying a specific cyclic group Z_p; a group Z_p is also known as calculations mod p. Observe that Z_p is a more precise way to describe DLP because it is closed under multiplication and 0 is excluded in calculations (unlike in modular arithmetic).

To begin, recall that $13 \equiv 4 \pmod 9$ is equivalent to saying that 4 is a remainder of 13 divided by 9: $13 - 4$ is divisible by 9. $13 \equiv 4 \pmod 9$ is pronounced as "thirteen is congruent to 4 mod nine."

Another topic is Euler's totient function $\phi(n)$, where $\phi(n)$ denotes a number of divisors of n that are relatively prime with it. For instance, $\phi(4) = 2$, because 4 is relatively prime with 1 and 3, and $\phi(11) = 10$, because 11 is relatively prime with $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

To understand the complexities of the DLP through a lens of number theory, this paper provides the following background:

1.3.1 "The order of a modulo n... is the smallest possible integer k such that $\alpha^k \equiv 1 \pmod n$," where $n > 1$ and $\gcd(\alpha, n) = 1$ [7].

1.3.2 If α has order $k \pmod n$ and $\alpha^i \equiv \alpha^j \pmod{\text{n}}$, then $i \equiv j \pmod k$ [7].

1.3.3 If α has order $k \pmod n$ and α^h has an order k, then $\gcd(h, k) = 1$ [7].

1.3.4 "If $\gcd(\alpha, n) = 1$ and α is of order $\phi(n)$ modulo n, then a is a primitive root of the integer n." [7] Alternatively, α "is taken to be a primitive root mod p, which means that every β is a power of $\alpha \pmod p$" [31].

1.3.5 If α is the generator and $\alpha^{m_1} \equiv \alpha^{m_2} \pmod p$, then $m_1 \equiv m_2 \pmod{p-1}$ [31].

Below is another DLP definition using modular arithmetic, a specific group of G: given a large fixed prime p, a primitive root α, and a nonzero integer β, find x:

$$\beta \equiv \alpha^x \pmod{p} \text{ and } x = L_\alpha(\beta), \text{ for } x\ 1 \leq x \leq p-1 \text{ [31].}$$

For example, to find $L_2(3)$ when $p = 13$, we observe the powers of 2 (mod 13) and compute the sequence $1, 2, 4, 8, 3, ...$ Thus, $x = 4$. However, several values can satisfy the equation: $2^4 \equiv 2^{16} \equiv 2^{28} \equiv 3 \pmod{p}$, but we consider as a solution the smallest nonzero value out of them to avoid confusion and simplify problems [31].

As seen in this trivial example, solving problems with small values of α, β, and p is straightforward by trying out a list of exponents. In general, computing β from α and x takes at most $2*\log_2 p$ steps, but the problem of computing x from β and α has not yet been solved using an efficient algorithm on classical computers [19] [25]. Of course, we can solve DLP by manually trying different integers until we find x that solves the equation; however, it would be infeasible because of the limit of time. In other words, if we try to run an algorithm to solve DLP on a classical computer, we are likely to receive a memory overflow errors because the problem takes too long to compute. On the contrary, quantum algorithm can efficiently solve this problem in polynomial time [30].

1.4 Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is a classical key exchange problem based on DLP; it relies on the insecure public channel to allow parties (Alice and Bob) without previous contact to communicate privately. The fundamental concept is to exchange the keys between Alice and Bob until they arrive at a common one, and the eavesdropper Eve should "find it computationally infeasible to compute the key from the information heard" [8].

The Diffie-Hellman key exchange represents the following algorithm. One of the communicating parties (Alice or Bob) picks a large prime p and a large primitive root (a generator) α. Both may be made public. [31] Then, Alice and Bob each pick a random large integer less than or equals to $p - 2$, and keeps them secret. [31] Suppose Alice's number is x, she then computes α^x in Z_p and sends the result to Bob. Bob picks his number y, computes α^y in Z_p and sends the result to Alice. [31] Finally, from each other's messages, they compute the session key $K = \alpha^{xy}$ in Z_p[31]. In simpler terms:

1. Alice and Bob pick p and α.
2. Alice picks x, computes, and sends to Bob α^x in Z_p. Bob picks y, computes, and sends to Alice α^y in Z_p.
3. Both Alice and Bob compute $K = \alpha^{xy}$ in Z_p to get the key [31].

If Eve intercepts α^x and α^y, she will not guess the key unless she can solve the Diffie-Hellman problem for x and y. Alternatively, she will need to find α^{xy} from α^x and α^y directly, namely a Computational Diffie-Hellman Problem [31]. Either way, similar to the classic RSA algorithm, Eve will face computational infeasibility because of the limitations of the current computing power.

For Alice, Bob, and even Eve, to compute α^x and α^y efficiently, they can use the Square-and-Multiply algorithm, simplifying exponentiation with modular p

(or in a general group G). The algorithm requires only $log_2(e)$ steps instead of $e-1$ where e is an exponent − a significant improvement that speeds up computations, considering that we work with long numbers.

For example, suppose we need to raise m to $e = 83$. The first step is to convert e into a binary representation:

$$e = (83)_{10} = 64 + 16 + 2 + 1 = 2^6 + 2^4 + 2^1 + 2^0 \rightarrow e = (1010011)_2$$

$$\text{Thus, } m^{83} = m^{64} * m^{16} * m^2 * m^1.$$

So, instead of multiplying m until $e = 83$, this algorithm requires multiplications only up to the highest power of two that is smaller than e (in this case, it is 64). Note that because we square m, we do not need to perform each step of multiplication (i.e., we calculate m^2, then m^4, m^8, $m^{16}, m^{32}, m^{64}, ...$ instead of m^2, m^3, m^4, m^5.) To compute m^{83}, we only need to multiply m^{64}, m^{16}, m^2, and m^1 together, comparing to modular after each multiplication.

2 Quantum Computing

2.1 Overview

To understand the Quantum Key Distribution, we give an overview of the quantum technologies. In the 1980s, Richard Feynman, also known for his two-slit-diffraction experiments, proposed the creation of quantum computers to increase computational power for "the efficient simulation of quantum systems" [20]. Originally, the idea came from wave mechanics (now called quantum mechanics), the dual behavior of light waves, and contributions from Born and Schrödinger [10]. Similar to a classical computer, a quantum computer has software and hardware, but its main components are photons, detectors, and quantum bits (or qubits) − a polarization state of a photon discussed earlier [20]. The underlying concepts include the dual nature of light particles in physics, Boolean algebra (similar to its use in the classical computers), and statistical probability that helps to determine the state of electrons or photons [10].

Security is the primary goal of cryptography; however, in practice, it is hard to achieve *unconditional security* that guarantees that Eve cannot break the system even if she has sophisticated computational power and unlimited time [31]. One-time pad is an example of an unconditionally secure encryption method that can be used only once. However, this costly method requires a key to be as long as the message; the key also needs to be exchanged privately in a secure manner in advance (meaning that Alice and Bob need to have communicated before or sent a trusted courier with the key before) [31]. Because a new key needs to be generated for each message, these inconveniences make the key impractical in the urgent situations or if Alice and Bob are located far apart.

On the other hand, *quantum cryptography*, an improved method of encryption and key exchanges, would theoretically allow unconditionally secure communications using unbreakable codes. When quantum computers become more

advance, current algorithms like RSA or Diffie-Hellman's, all online communications, and even the internet might become insecure unless *quantum codes* are used [1]. The *quantum key distribution* guarantees that if an eavesdropper attempts to intersect and access the key, she will inevitably change it, thus being unable to read the messages [1]. Therefore, it is impossible for Eve to mimic Alice and Bob's encryption key.

2.2 Introduction to Quantum Mechanics

Technicalities behind quantum mechanics start with explaining *a state* of a particle, also known as "probability wave" or "condition" [10]. A state can refer to a single particle or a system of them.

In 1939, P. A. M. Dirac created a standardized notation of the states to represent linear operations and abstract vectors. Recall that a complex number z is denoted by $z = a + ib$, where a and b are real numbers and imaginary i equals to $\sqrt{-1}$. In vector notation, $z = (z_1, z_2, ...z_n)$. In Dirac notation, a vector (z_1, z_2) is denoted as $|z\rangle$ [10].

Let's examine how to describe more complicated scenarios of interactions of particles. We know from physics that ψ is a wave function of the system (e.g., it is used in the Shrödinger equation); in quantum mechanics it is described by a vector representing quantum states (i.e., the general state of qubit): $|\psi\rangle$ (pronounced as "kets") [1]. "Bra" describes a complex conjugate of a wave function, denoted as $\langle\phi|$ [10]. The product of the "ket" and "bra" is $\langle\phi|\psi\rangle$, a scalar called "bracket" (also written as "bra–ket" or "bra/ket") [10]. If $\langle\psi|\psi\rangle = 1$, then ψ is *normalized* [10].

In Quantum Mechanics, states exist in a *Hilbert space* or we can say that states form a *basis* of the Hilbert space. Unlike Cartesian coordinates or Euclidean plane, Hilbert space goes beyond 2D and 3D spaces and can describe finite or infinite dimensions [10]. A quantum state can be described as a vector in the Hilbert space [10].

Now that we have introduced quantum notations, we will explain *quantum phenomena*. As we have noted, there are numerous difference between classical and quantum computers. First, classical computers use bits that represent 1's or 0's, while quantum computers use *qubits* that can be 1, 0, or both at the same time [18]. In mathematical terms, a *qubit* is a normalized state vector that exists in the Hilbert space C^2, where:

$$|0\rangle = \begin{vmatrix}1\\0\end{vmatrix} \text{ and } |1\rangle = \begin{vmatrix}0\\1\end{vmatrix} \text{ [10].}$$

In more general terms, an element in C^2 can be written as a combination of two states, where α and β are complex numbers:

$$\psi_{\pm} = \alpha|0\rangle \pm \beta|1\rangle \text{ and } \alpha^2 + \beta^2 = 1 \text{ [1].}$$

The phenomenon of storing a qubit of 0 and 1 simultaneously is called *superposition*; we can think about it as a "mixed wave" of two normalized waves ψ_A and ψ_B:

$$\psi_{\pm} = 1/\sqrt{2}(\psi_A \pm \psi_B) \text{ [10][1].}$$

It also can be written as

$$\psi_{\pm} = 1/\sqrt{2}(|\uparrow\downarrow\rangle \pm |\uparrow\downarrow\rangle),$$

where $\uparrow\downarrow$ denotes polarization state of a photon (an equivalent to the spin of an electron) [10][1]. Feynman described the state of photon polarization $|\psi\rangle$, in terms of two orthogonal vectors:

$$\psi = \alpha|\uparrow\rangle + \beta|\downarrow\rangle \text{ or } \psi = \alpha|\nearrow\rangle + \beta|\searrow\rangle \text{ [20][1].}$$

We will discuss polarization states and bases more in section 3.1 when describing QKD.

We should note that this work in C^2 is a simplified version of the actual interactions of particles. Moreover, these formulas do not allow us to predict the result of the interaction between two waves or particles: they only give us a probability of the the event happening (see Heisenberg's principle of uncertainty) [10].

In addition to qubits and superposition, quantum computers rely on several other key concepts that enable higher computational speed, including:

Quantum entanglement. Quantum entanglement is an interaction between several particles, which prevents us from describing a single particle in the entangled state without the presence of another one [16]. Imagine the following scenario. After a contact of two particles, A and B, they are separated; we cannot precisely describe either of them individually, unless we bring A and B back together [15].

Quantum interference. Quantum interference is an interaction between two quantum states that, as a result, transform one another (conceptually analogous to the Young's double slit experiment). [16]. It can be understood as two waves constructing or destructing each other.

Quantum gates. Just as classical computers need circuits to function through logic gates based on the Boolean algebra, quantum computers need special quantum gates to accommodate qubits and run quantum algorithms [1].

2.3 Current Challenges

Several research models for quantum machines exist now, and some are soon-to-become commercialized [16][26][17]. For example, both quantum Turing Machine and quantum gates already serve as computational models but they encounter several practical difficulties [1]. To advance the creation of quantum computers there are several crucial practical and theoretical problems that need to be solved. In addition to the security problems, examples and explanations of those include:

2.3.1 *Decoherence.* Qubits are the underlying building blocks of quantum computers; however, they are hard to implement in real life. Outside factors (e.g., noise in the quantum channel) and interaction between particles easily

affect and change quantum states [1]. Decoherence is also a main obstacle to the NMR quantum computers; in 2001, researchers from IBM have used "a predictive tool for modelling quantum errors" to create a decoherence-free model [32].

2.3.2 *Quantum Computer Structure.* To build functioning quantum hardware, one need to combine phenomena of superposition, quantum interference, and quantum entanglement without decoherence [16]. Additionally, the quantum gates and quantum randomness need to be addressed as well. Only when all these criteria are satisfied in the quantum architecture can the qubits be generated [1][16].

2.3.3 *Quantum Software.* First, hardware is often required for software testing but its architecture is still under development [1]. Quantum software poses several obstacles from implementing new quantum programming languages to developing algorithms and writing practical quantum programs (e.g., Shor's algorithm is discussed in the section 3.4) [1].

2.3.4 *Communication Distance of QKD.* Current quantum communication distance can reach only up to several hundreds of kilometers, an insufficient coverage for global purposes [14]. For example, the Battelle company based in Ohio installed the first commercial version of the QKD in the U.S. [26]. Battelle is currently designing a "QKD Trusted Node^{TM}" that should expand the communication distances by installing such nodes across the country [26]. Their estimation of the maximum distance is 700 km with a goal of connecting Columbus, Ohio to Washington, DC [26]. However, the problem of connecting Western and Eastern Hemispheres is yet to be solved via this method.

2.3.5 *Speed.* As mentioned before, the superposition phenomenon allows for a faster speed of quantum computers [18][16]. As for the QKD, because quantum keys need to be sufficiently long to provide secure communications, the quantum key generation rate appears to be much slower than expected so far (currently, the maximum rate is approximately 1 Mbps) [14].

2.3.6 *Number of Qubits.* As mentioned above, decoherence presents the main threat to the formation of qubits (and their deformation). Even if all criteria for quantum phenomena are satisfied, decoherence will reduce the quantum states and all information that they carried will be lost [16]. Thus, qubits exist in unstable, hardly-achieved states with the ability to undermine the entire quantum computer system.

2.4 Applications of Quantum Technology

Quantum computers also allow for *quantum communication* or *quantum teleportation* as a part of quantum information theory. One can send large quantities of classical information encrypted as quantum states on higher speed with efficient error correction because of the quantum communications [1]. Claude Shannon proposed to encrypt information in quantum states instead of using bit strings in 1948 [29]. His algorithm transforms alphabetical messages into

quantum states that are later sent via quantum channel to the recipient who then converts them back to the algorithm [29].

Quantum teleportation uses several entangled particles that are related to each other by their nature [1]. In other words, Alice and Bob share quantum entanglement in advance, and construct a quantum circuit that can be disrupted by any interference [6]. However, the circuit preserves the information despite alterations, even if qubits were measured (recall that qubits change their span according to the base used to measure them) [6]. This phenomena is justified by the entanglement and can be used inside a quantum computer for teleportation. Quantum teleportation is widely incorporated in quantum communications and requires both classical and quantum channels to send information [1].

Quantum programming is another application of quantum computers that can be implemented via software or hardware. Both are under development and the latter requires a lot of time and financial resources to advance [1]. Programming languages, like Quantum Computational Language (QCL) and Quantum Lambda Calculus, allow a simulation of costly quantum gates because of their independence of hardware, for instance [1]. They also "deal with quantum algorithms at the abstract level by means of quantum programming languages" [1]. Most of the current quantum languages are extensions of classical languages like C or $C++$ [1].

Artificial Intelligence, a fast-growing field nowadays, will also benefit from the quantum computer's computational power, performing large AI algorithms at "ultra high speed" [1]. All scientific simulations and optimizations, from the fields of mathematics and finance to chemistry and physics, can already be processed on the online quantum computer simulator [16].

3 Quantum Key Distribution

As one of the most mature and advanced quantum cryptosystems, quantum key distribution (QKD) is a type of quantum communications and quantum information processing [34]. In theory, QKD allows for unconditionally secure communications between Alice and Bob − a perfect way to communicate sensitive information. It creates a secure random key, relying on peculiar qualities of photons and uncertainty principle. In practice, it requires well-functioning, widely spread quantum computers to maintain stable states of qubits in order to store and pass information. Unlike quantum teleportation, hardware and circuits needed for successful QKD are far more intricate [6]. In the following sections, we will explain how quantum computers will change a network of information transmissions.

3.1 QKD: History and BB84

The need for a new secure key led to the discovery of QKD, and its "best-known QKD protocol (BB84) was published by Bennett and Brassard in 1984" [23]. It guarantees the unconditional security, despite Eve's capabilities or intercepted

information. In addition to this, the receiver Bob can detect if the transmitted message was intercepted as the concept of the security largely depends on the physical properties of the key: photons and the uncertainty principle [3]. The original paper, "Quantum cryptography: Public key Distribution and Coin Tossing," describes that the information is encoded into the bits of "single photons with polarization directions 0, 45, 90, and 135 degrees" (see the table below) [3].

Bit	0	1
Direction	↑→	↗↘
Basis	X	+
Name	diagonal	rectilinear

Alice (the sender who encrypts the message) first chooses a random string of bits, where 0 corresponds to the first two black arrows, representing the polarization directions of the photons, and 1 to the second two. Then she picks a "random sequence of polarization bases (rectilinear or diagonal)" and sends the sequences of strings of photons through corresponding bases to Bob [3]. Bob, in his turn, randomly picks a basis for each received photon, without any information about the basis or a photon, and translates a photon into a bit [3]. However, because of the Heisenberg's uncertainty principle, which states that one can only know the position or momentum of an electron, Bob (or Eve) will decode any polarized photon as "0" if they use diagonal basis, and "1" if they use the rectilinear. Thus, Bob receives meaningful information only from the bits that he has guessed correctly. In addition, some of the photons "would be lost in transit or would fail to be counted by Bob's imperfectly-efficient detectors" [3]. With basic counting, one would approximate that Bob will correctly guess about half of Alice's key.

To find the matching bits between Alice's sent key and Bob's received key, they may use any public communications channel even if Eve might intersect it (but cannot inject or alter it)[3]. Then, after Bob reveals the bases he used for decryption and Alice confirms the correct guesses, they discard the ones that did not match, and generate a key from the remaining bases [23].

To limit the length of the sent key and increase the yield rate efficiency, Hwang *et al.* proposed a modified version of the QKD BB84 called the Hwang Protocol, which forms the key from all sent photons, instead of a half of them (as it is in the case of BB84) [14]. Because of the implemented decoy-state, the Hwang Protocol also allows for a transmission distance up to 140 km, a substantial improvement from the first experimental distance of 30 cm in 1989 [14].

3.2 QKD Components and Requirements

Although the hardware of current quantum computers requires advancement, there are several key components to the QKD transmission. Similar to the classical algorithms of encryption (e.g., RSA or Diffie-Hellman key exchange), QKD requires a channel for message transmission, a number randomizer, and error

detection and correction algorithm [23]. A quantum channel serves the same role as the classic channel: it provides virtual space Alice and Bob to exchange the key without any prior secure contact. An efficient number randomizer (or random number generator) helps to create a random bit sequence or choose a basis. An error detection and correction algorithm based on the coding theory provides a clear transmission between Alice and Bob and enables the shortening of the key length [13].

Additionally, successful QKD transmission needs light sources that emit photons or attenuated laser pulses, standard linear optical components (e.g., beam-splitters, amplitude and/or phase modulators), and single photon detectors that limit light detection [23].

IBM Q provides to the public an online simulator of a quantum computer, "composer," using an IBM Cloud platform [18]. It teaches how to approach quantum software, starting with basic definitions and explanations. This simulator can also mimic procedures that are up to 32 qubits long, as opposed to IBM's implementation of Shor's algorithm in 2001 mentioned in section 3.5 [16].

As mentioned in 2.2.4, an operational distance of QKD is rather limited now. Even with working components, QKD will not be a convenient method if the solutions like "Trusted Nodes" guarantee unconditional security [26]. An alternative to the connections on the ground is a satellite connection [21]. Satellite-to-ground connect on has proven to function on greater distances and have fewer losses of messages (due to alterations of the photon's state or loss of the entanglement) [27]. In 2016, a group of Chinese scientists developed and successfully launched a satellite "Micius," designed for quantum experiments. Through a decoy-state QKD transmitter based on the BB84, it can communicate over a distance of up to 1,200 km [21]. The BB84 encoding module incorporates the main components discussed before, including " a half-wave plate, two polarizing beam splitters and a beam splitter, which randomly prepares the emitted photons in one of the four polarization states" [21]. It has a thermal noise device that generates a 4-bit random number, controls several lasers, and determine polarization and intensity levels of of photons [21]. Electric control of these lasers obtains the average photon number in the output of the telescope: μ of high intensity of the original state is 0.8, μ "moderate" is 0.1 (as described in the BB84 protocol), and μ in vacuum is 0 [21] [23]. To transmit a message, the researchers sent these several intensity levels with different probabilities to maximize the secrecy of the photon emission rate as a security measure [21]. They could successfully create and transmit the key with an experimental quantum bit error rate averaged 1.1% after error corrections [21].

Despite the impressive findings, this over-space transmission still encounters major problems such as noise in the channels, "channel loss, including beam diffraction, pointing error, atmospheric turbulence and absorption" [21]. In addition, weather and atmospheric conditions can affect the transmission, jeopardizing its efficiency [21]. Realizing the fullest potential of quantum computing and fixing problems will require costly research and development.

For instance, the communication length can be increased by adding more satellites and transmitting the key on the ground through metropolitan quan-

tum networks or quantum nodes, for instance [26] [21]. Overall, after a few improvements, this satellite transmission has a potential to provide an unconditionally secure quantum channel between two places on Earth.

All these methods to use QKD to encrypt messages require expensive quantum computers, but will all of us need to have them to cherish privacy? Fortunately, the answer is no. In 2007, Boyer *et al.* published a paper describing how Alice and Bob can securely exchange messages when only the sender has an access to the quantum technology [5]. This semi-quantum key distribution scheme (BKM07 SQKD) is theoretically secure against attacks and show if Eve is present [34][5]. Bob would only need to be able to perform the following operations:

(1) Measuring qubits using basis ($|0\rangle$ or $|1\rangle$);
(2) Requesting retransmission of the qubits;
(3) Prepare a qubit in the basis ($|0\rangle$ or $|1\rangle$);
(4) Receiving and sending back qubits without disturbing them [34].

If these four operations are satisfied, then Bob and bits are considered as "classical," while Alice can continue to operate a quantum computer [34]. However, the system raises several security concerns, some of which are discussed in the next section.

3.3 Attacks on QKD

As it has been shown before, theoretically, if Eve intercepts the channel with the Alice's message, she would randomly try bases to decode. Just as Bob, she would change the spins of some photons; as a result, during the public exchange, she would not be able to match her decrypted sequence with Alice's and Bob's. In addition, eavesdropping will alter the original message.

To check for the presence of Eve, Alice and Bob "randomly [select] subset of data and verify that it is below a certain threshold value," using a quantum bit error rate [3]. Alice and Bob can also use error detection and correction from the coding theory by adding detection bits in the message (classically, in the end), or use "the polarization states of two-photon system" [1]. Because of the one-time pad principle of the BB84, Alice and Bob must have the message retransmitted if the threshold value is greater than expected.

However, there are several difficulties in implementing theoretical QKD and detecting the presence of an eavesdropper. First, the single-photon sources, "imperfect devices, and lossy/noise channel" make the channel susceptible to eavesdropping, thus require further improvements in QKD [22][33]. The original paper on BB84 assumed the use of "phase-randomized weak coherent pulses (WCP's) with a typical average photon number of 0.1 or higher" [23]. However, the weak photon sources can likely emit more than one photon at a time, jeopardizing the system:

> If there are more than one photon, Eve could remove one of the photons and store it. Otherwise, she blocks the one-photon pulse with a certain probability, which can be hidden by the channel loss.

> At the end of the protocol, she would utilize these photons to learn partial information about the key without introducing any errors [22].

Such photon-number splitting (PNS) attacks happen as follows: Eve takes at least one of the split photons, stores it in a quantum memory, sends the rest to Bob, receives Alice's information on the basis, and decrypts the information [33]. Additionally, Eve can simply obtain the number of photons by counting them without disturbing their spins [22]. In either case, Bob cannot determine the eavesdropper unless he has access to the statistics of photons or to the detection rate of photons [12]. For instance, he could use a photon-number resolving (PNR) device that determines the "number of photons in pulse or time-gap with high fidelity" or "bright reference pulses (BRPs) [that] prevent against the PNS attack" [12][33].

There are a few "true" single photon emitting sources that function at room temperatures [12]. However, the technology is costly, premature, and does not provide a high rate of emission [12]. A more plausible alternative to them is an attenuated laser light [17].

In addition, quantum hacking can affect any part of the QKD setup. The types of such attacks include time shift, time information, detector control, channel calibration, phase remapping, Faraday mirror, phase information, and device calibration [23].

For instance, device-independent quantum key distribution (DIQKD) prevents Eve from installing a forged photon emitting device that she controls and gaining information to Alice's and Bob's measurements of quantum states [24]. As a provable secure system, DIQKD does not depend on the dimension of the Hilbert space, photon emitting sources, operators, state measuring devices or states of the input [24].

3.4 Shor's Algorithm

Without quantum algorithms, quantum computers will not be helpful in solving concrete problems. In this section, we will discuss a quantum algorithm that poses a threat to the classical cryptography and key exchanges.

Peter W. Shor has developed an algorithm for quantum computers that solves both prime factorization (the problem on which RSA relies) and the discrete logarithms problem (the basis of Diffie-Hellman key exchange, section 1.4) [30]. Similar to the quantum Turing machine and quantum gate arrays, Shor's algorithm runs in polynomial time as opposed to exponential − the most efficient algorithm known to find prime factors [35][30][32]. The keystone concepts include modular arithmetic and group theory or, more precisely, it "is a special case of the hidden subgroup problem" [30][28].

Below is a step-by-step description of the Shor's Algorithm to factor a large integer N:

1. Select an integer x such that $x < N$;

2. Compute $\gcd(x, N) = a$. Finding greatest common divisor can be done by the Euclid algorithm in polynomial time;

3. If $a \neq 1$, then a is a factor of N and we are done;

4. Otherwise, find the order r of x in the group Z_N^* (a multiplicative group of integers mod N excluding 0). Using modular, the same can be described as $x^a \equiv 1 \pmod{N}$;

5. If r is odd or $x^{r/2} \equiv -1 \pmod{N}$, repeat with a different x. Compute $\gcd(x^{r/2} \pm 1,\ N)$. If at least one of the gcd is not 1, then it is a factor of N [1][30].

This algorithms transforms the problem of prime factorization into the problem of finding the period of a function and solves it through the Discrete Fourier Transform [1]. The main difficulty of the Shor's algorithm is to find r, and that is where quantum mechanics and quantum algorithms come to help.

In his original paper, Shor pointed out that current quantum computer limitations need to be overcome prior to the full implementation of the algorithm [30]. The simulation of Shor's algorithm to factor 15 was successfully performed on a 7-qubits Nuclear Magnetic Resonance (NMR) quantum computer by IBM in 2001 [32][1]. After the original paper by Vandersypen *et al.*, with a minimization algorithm of the same purpose as Shor's, the largest number known to be factored is now 56153 using only four qubits in 2012 [36].

Once quantum computers become widely available, Shor's algorithm can be used to break classical algorithms. Theoretical algorithms provide solutions to the complex mathematical problems that are currently deemed computationally intractable; however, to overcome the practical barrier and pose a threat to the current developments, quantum technologies need to solve crucial problems such as sufficient number of qubits and decoherence (discussed in section 2.2) [28].

3.5 Conclusion

The remarkable discovery of Shor's algorithm has brought more attention to quantum technology as it has shown its potential. Although quantum computers have yet to become widespread, they bear an immeasurable potential to revolutionize our perception and use of electronic security systems. What will we do when security systems become obsolete?

We cannot change the laws of physics; we can work around them and overcome obstacles in our way. Of course, it is still a quite long way to solve current quantum challenges: from advancing quantum software and hardware to educating students in math, physics, cryptography, and computer science at the same time to work with quantum technologies.

Current security systems may fall and give in to the quantum technology, starting a new era of privacy. Even now, in the current technological world, privacy and security are one of the most important values as the concept of a "Big Brother" progresses. From social media and online purchases to satellite findings and governmental secrets, we are becoming more and more depended on the online interactions. Without secure cryptosystems, the world would be on

the verge of chaos. Just imagine that you are unable to transfer any information over the internet without an eavesdropper intercepting it.

The promises that quantum computers make cannot leave us indifferent to their potential. The potential to solve problems in a couple of hours that used to be deemed computationally intractable, advance AI or even create teleportation is mesmerizing.

Will qubits create a world of unconditional security or destroy our privacy?

References

[1] Akama, S. (2015). *Elements of quantum computing: History, theories and engineering applications.* Cham: Springer.

[2] Armasu, L. (2019, March 15). Quantum Computers May Not Break Encryption for Decades, Say Researchers. *Tom's Hardware.* Retrieved from https://www.tomshardware.com/news/quantum-computers-encryption-decades-researchers,38819.html

[3] Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public key distribution and coin tossing. *International Conference on Computers, Systems and Signal Processing*, 175-179. doi:10.1016/j.tcs.2011.08.039

[4] Blum, M. (1981, November 10). Coin Flipping by Telephone — a Protocol for Solving Impossible Problems. *ACM SIGACT*, pp. 23-27.

[5] Boyer, M., Kenigsberg, D., & Mor, T. (2007, 5 October) Quantum Key Distribution with Classical Bob. *Physical Review Letters.*

[6] Brassard, G. (1996). Teleportation as a quantum computation. *Physica D.* 43-47.

[7] Burton, D. M. (2016). *Elementary Number Theory* (4th ed.). New Delhi, India: McGraw-Hill Education (India) Private Limited.

[8] Diffie, W., & Hellman, M. E. (1976, November). New Directions in Cryptography. *IEEE Transactions on Information Theory*, pp. 644-654.

[9] Emerging Technology from the arXiv. (2019, May 30). How a quantum computer could break 2048-bit RSA encryption in 8 hours. *MIT Technology Review.* Retrieved from https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/

[10] Fano, G., & Blinder, S. M. (2017). *Twenty-First Century Quantum Mechanics: Hilbert Space to Quantum Computers Mathematical Methods and Conceptual Foundations.* Cham: Springer International Publishing.

[11] Fraleigh, J. B. (1982). *A First Course in Abstract Algebra.* Reading, MA: Addison-Wesley.

[12] Gaidash, A. A., Egorov, V. I., & Gleim, A. V. (2016). Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. Journal of Physics: Conference Series, 735, 012072. doi:10.1088/1742-6596/735/1/012072

[13] Hankerson, D. R., Hoffman, D. G., Leonard, D. A., Linder, C. C., Phelps, K. T., Rodger, C. A., & Wall, J. R. (2000). *Coding Theory and Cryptography: The essentials* (2nd ed.). New York: Marcel Dekker.

[14] Hwang, W., Koh, I., & Han, Y. (1998, August 3). Quantum Cryptography Without Public Announcement of Bases. *Physics Letters A*, 489-494.

[15] IBM Research Editorial Staff. (2019, February 8). Quantum Computing: You Know It's Cool, Now Find Out How It Works. Retrieved from https://www.ibm.com/blogs/research/2017/09/qc-how-it-works/

[16] IBM Q Experience. (n.d.). Retrieved from https://quantum-computing.ibm.com/

[17] ID Quantique's quantum solutions. (n.d.). Retrieved August 23, 2019, from https://www.idquantique.com/single-photon-systems/solutions/

[18] Kinnaird, D. (2016, June 17). Leap into the Future with the First Quantum Computer Anyone Can Use. Retrieved August 9, 2019, from https://www.ibm.com/blogs/cloud-computing/2016/06/17/first-quantum-computer-anyone-can-use/?mhsrc=ibmsearch _a\&mhq=quantum\$20computers

[19] Knuth D. (1969) *The Art of Computer Programming*, Semi-Numerical Algorithms. Reading, MA.: Addison-Wesley.

[20] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010, March 04). "Quantum computers." Retrieved from https://www.nature.com/articles/nature08812

[21] Liao, S.-K. Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., & Pan, J.-W. (2017, August 9). Satellite-to-ground Quantum Key Distribution. *Nature*, 549, 43–47.

[22] Lin, S., & Liu, X. (2012). A Modified Quantum Key Distribution Without Public Announcement Bases Against Photon-Number-Splitting Attack. *International Journal of Theoretical Physics*, 51(8), 2514-2523. doi:10.1007/s10773-012-1131-9

[23] Lo, H., Curty, M., & Tamaki, K. (2014). Quantum key distribution secure against partly malicious devices. *Nature Photonics*, 595-604. doi:10.1038/NPHOTON.2014.149

[24] Pironio, S., Acín, A., Brunner, N., Gisin, N., Massar, S., & Scarani, V. (2009, April), Device-Independent Quantum Key Distribution Secure Against Collective Attacks. *New Journal of Physics*, 11(4).

[25] Pohlig, S. & Hellman, M. E. (1978, January). An Improved Algorithm for Computting Algorithms in GF(p) and Its Cryptographic Significance. *IEEE Trans. Inform. Theory,* 106-110.

[26] "Quantum Key Distribution." Battelle. Accessed August 22, 2019. https://www.battelle.org/case-studies/case-study-detail/quantum-key-distribution.

[27] Rarity, J. G., Tapster, P. R., Gorman, P. M. & Knight, P. (2002). Ground to Satellite Secure Key Exchange Using Quantum Cryptography. *New J. Phys.* 4, 82.

[28] Rees, D., Braunstein, S., Gay, S., Lawson, M. V., & Kambites, M. (n.d.). Case for support: Quantum Computation, Foundations, Security, Cryptography and Group Theory.

[29] Shannon, C. E., & Weaver, W. (1999). *The mathematical theory of communication. Urbana: University of Illinois Press.*

[30] Shor, P. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing* 26.

[31] Trappe, W., & Washington, L. C. (2006). *Introduction to Cryptography: With coding theory.* Upper Saddle River, NJ: Pearson Prentice Hall.

[32] Vandersypen, L., Steffen, M., Breyta, G., Yannni, C., Sherwood, & M., Chuang, I. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* 414, 883-887

[33] Wu, G., Chen, J., Li, Y., Xu, L., & Zeng, H. (2006). Preventing eavesdropping with bright reference pulses for a practical quantum key distribution. *Physical Review* A, 74(6). doi:10.1103/physreva.74.062323

[34] Yang, Y.-G., Sun S.-J.,& Zhao, Q.-Q. (2014, 12 November). Trojan-Horse Attacks on Quantum kKey Distribution with Classical Bob. *Quantum Inf Process*, 14, 681–686.

[35] Yao, A. (1993). Quantum circuit complexity, in Proc. 34th Annual Symposium on Foundations of Computer Science, *IEEE Computer Society Press*, Los Alamitos, CA, 352–361.

[36] Zyga, Lisa (2014, 28 November). New Largest Number Factored on a Quantum Device is 56,153. *Phys.org. Science X Network.*