Quantum Cryptography

Mithil Mishra

Edison High School STEM Academy
mithil.mishra@gmail.com

September 27, 2022

Abstract

Quantum cryptography is a safeguard against a near future where quantum supercomputers are able to perform at speeds many millions of times faster than classical computers. In this paper, three applications of quantum cryptography are discussed, with the first quantum protocol BB84, then an overview of quantum teleportation with China's QUESS initiative, and finally NIST's 6 year competition to find novel, suitable, quantum cryptography protocols are explored with its first released sequence of finalists. Finally, a series of tests on quantum computer efficiencies with a python based BB84 scheme is analyzed through IBM's quantum lab.

I. Introduction

As the development of the quantum industry progresses, with increased bit sizes and computational capabilities, a world where quantum supercomputers outclass current ones is rapidly approaching. However, as this world approaches, so does a world where current encryption standards aren't enough. A world where security is fully compromised. Therefore, a subset of quantum computing, quantum cryptography arises. Specifically, Quantum Key Distribution (QKD) uses unique quantum mechanical phenomena and theory to guarantee security of data and information. In this paper, quantum cryptology is broken down into three parts. First, BB84, a QKD scheme, is discussed along with the basics of encryption. Then, an application of long range quantum communications with teleportation is studied in regards to China's new quantum satellite program. Next, novel algorithms are discussed in regards to the future hazards of quantum supercomputer usage to break classical encryption. Finally, the BB84 protocol in python is run on IBM's quantum lab computers as well as quantum simulators.

Quantum Computing

Quantum computing is a new emerging technology that relies on fundamentals of quantum physics, a realm of physics at the smallest scale. At this scale, various features mesh together, exposing the concept of superposition, allowing a wave to act as a particle and vice versa. The way this theory is harnessed is through qubits, or quantum bits, an alternative to current classical bits. Unlike the convention of bytes that can have a value of either 1 or 0, qubits can take on a value of 1 or 0 and also be in a superposition state. This qubit exists within a two-state device or two-state quantum-mechanical system. Some examples of this include electron spin, up or down, or the polarization of photons. The photons can be polarized on a rectilinear basis, allowing for horizontal and vertical polarizations representing the 1s and 0s, but also in a coherent superposition of both orientations simultaneously, a diagonal polarization.

Vector Representation

Qubits are often represented as their quantum states, in Dirac or "bra-ket" notation. These states are shown by a set of vectors in a linear superposition of its two orthonormal basis states. $[0\rangle$ denotes a ket vector of $\vec{10}$ and $[1\rangle$ denotes a ket vector of $\vec{01}$. Similarly, these vectors can also be written using column notation. These two orthonormal basis states are taken as probabilities in the quantum state of a pure qubit. This coherent superposition of the basis states is taken as

$$[\Psi\rangle = \alpha[0\rangle + \beta[1\rangle, \tag{1}$$

where there is linear combination of probabilites bewteen state $[0\rangle$ and $[1\rangle$. Accordingly,

$$\alpha^2 + \beta^2 = 1 \tag{2}$$

These values, α and β, represent the probability amplitudes of the basis states of the qubit.

Bloch Sphere Representation

Another representation of qubit quantum states is the Bloch sphere. This is a geometrical description of a two-state quantum device. The sphere is a unit 2-sphere with poles denoting a pair of mutually orthogonal state vectors. For example, the north and south poles represent the $[0\rangle$ and $[1\rangle$ basis vectors respectively. These also correspond to the up and down spin states of electrons. Any value on the outside of the circle represents the pure states while the interior points show mixed states.

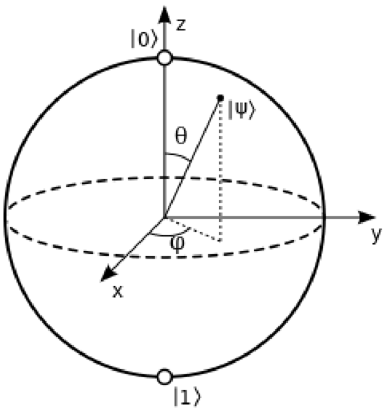


Figure 1: *Visualization of a Bloch sphere [1].*

II. BB84

Encryption has been around almost as long as the internet, a necessity for traveling through the world wide web. Simply put, it is a way to keep information safe, by encoding the data. Typically, encryption is broken up into 4 parts. First, the plaintext, a string of zeros and ones in binary, is inputted along with a key into an encryption algorithm to form ciphertext. This ciphertext is then sent to the receiver of the message who uses that secret key to decipher the encrypted ciphertext and return the plaintext message. There are many ways to go about this. Conventional methods are broken into symmetrical and asymmetrical cryptography. Symmetrical typically means that there is one key, while asymmetrical typically means that there are two keys.

Classical Encryption

Symmetrical or Private Key Encryption

This method uses a single key and is a basic encryption method. However, this does not work on a larger scale as individual secret keys have to be decided between the sender and receiver. Furthermore, if the key is lost or stolen, it renders the whole process useless. The usage of an individual key cannot also identify which user sent the message.

Asymmetrical or Public Key Encryption

This form of encryption uses two keys, one public and one private, to relay information between two parties. It follows the same layout as private key encryption, but instead one of the two keys is used for encryption and the other for decryption. When the message is sent, the pair of keys are matched but do not need to correlate in any other way, ensuring security. The advantage of public key encryption is that one of the keys can remain public and since only the receiver has the private key, it ensures that no one else can decipher the text. This can also allow authentication of a user sending or receiving the message.

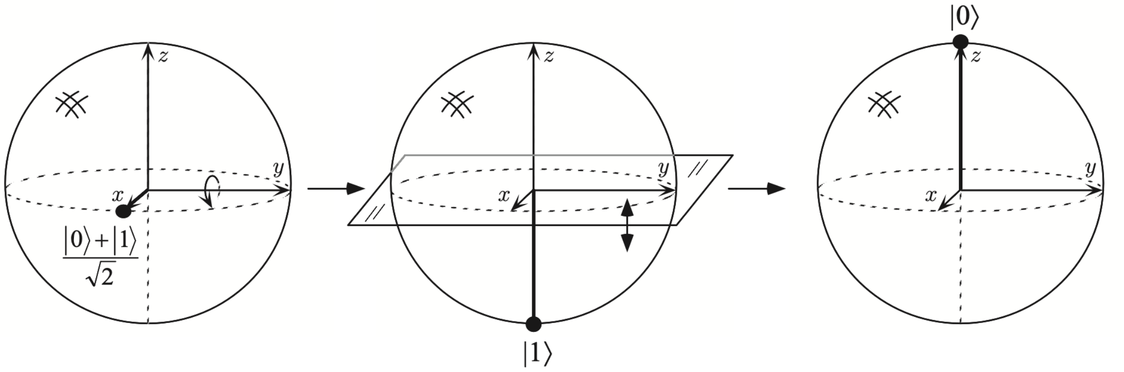


Figure 2: *Visualization of the Hadamard gate on the Bloch sphere, acting on the input state* $[0\rangle+[1\rangle/\sqrt{2}$ *[4].*

RSA encryption is a widely used encryption method for most computers and has proved successful in protecting data from bad actors using conventional computers. This method relies on the difficulty of factoring large prime numbers. The public key is generated by picking two random prime numbers and multiplying them together, and the process is similar to the private key. The large numbers that result can be 1024 bits or even 2048 bits. These large numbers are increasingly hard to factorize, but if they are, the whole system is compromised [2]. Although current computers are unable to achieve such tasks, the potential of quantum computers poses a threat to RSA encryption with the potential to break it.

Quantum Key Distribution

With the quantum computing age steadily approaching, there is a threat of classical encryption methods being jeopardized. Therefore, as a precaution, many researchers have looked toward the future and created equally secure cryptographic protocols to combat the computational powers of quantum computers. This new method of encryption relies on quantum mechanical principles, such as uncertainty and entanglement, to protect information. This is known as quantum key distribution (QKD).

BB84 is a quantum key distribution scheme created in 1984 by Charles Bennett and Gilles Brassard as the first quantum cryptography protocol [3]. It uses a quantum secure channel to deliver photons with a unique spin to convey a message. In this situation, a sender Alice would like to securely transmit a message to a recipient Bob. In order to get the key to encode a message, Alice creates two random strings of classical bits. One serves as the state and the other is the basis for encoding. The state determines whether a NOT (X) gate is applied to the qubit, this inverts the value of the bit, from either $[1\rangle$ or $[0\rangle$ to the other. If the classical bit is 1, then the gate is applied, and if it is 0, then no change occurs. The second string determines whether a Hadamard gate is applied. A Hadamard gate changes the value of the qubit to either a $[+\rangle$ or $[-\rangle$, depending on whether it is a 0 ket or 1 ket respectively. These gates can be represented on the Bloch sphere: the X gate has a as a 180° rotation about the center of the sphere, giving its mutually orthogonal value, and the Hadmard gate consists of a 90° rotation around the y-axis followed by a 180° rotation about the x-axis, shown in Figure 2. The Hadamard and X gates can also be shown through matrix notations, illustrated in Figure 3.

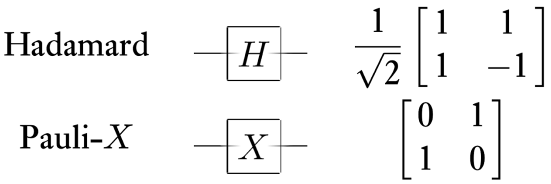

Hadamard
H
$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X
X
$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

Figure 3: *Hadamard and Pauli-X gates as matrices [4].*

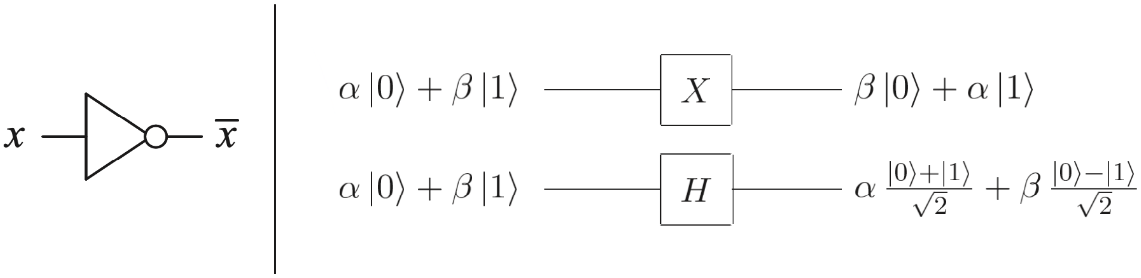

x
$\overline{x}$
$\alpha\,|0\rangle + \beta\,|1\rangle$
X
$\beta\,|0\rangle + \alpha\,|1\rangle$
$\alpha\,|0\rangle + \beta\,|1\rangle$
H
$\alpha\,\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Figure 4: *Single bit (left) and qubit (right) logic gates [4].*

Finally, these gates are also represented as circuits, depicted in Figure 4. While the Hadamard gate multiplies by its matrix, resulting in a complicated quantum state, simplified to a $[+\rangle$ and $[-\rangle$, the X gate's matrix multiplication simply results in the probabilities of the coherent superposition switching, or a swap of coefficients for each of the vector states. These gates are also applied by the receiver, Bob, who uses his random bases to apply a Hadamard function. Alice sends the resulting message as photons. Because the photons' states, encoded by the bits, are unable to be determined or recreated due to the no-cloning theorem, the channel of transfer is quantum secure. Then, Bob compares the bases, the spins of the polarized photons, with Alice. He publicly announces if the values of the bases are the same, keeping those that are and discarding the rest. This then forms the key for the encrypted message [5].

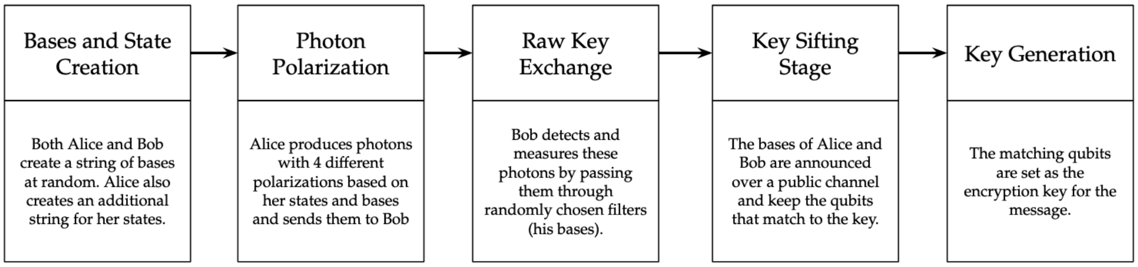
Implementation

For Alice to send the initial strings, photons have to be polarized in certain ways, either with a rectilinear basis or a diagonal basis. These polarizations are determined by the overall outcome of the two strings that Alice created. The photons are polarized with a rectilinear basis, vertical or horizontal if the result of the two strings is a $[1\rangle$ or $[0\rangle$, and polarized with a diagonal basis if the Hadamard basis is applied, $[-\rangle$ or $[+\rangle$. Once these photons are sent, Bob has to decode them by putting them through his basis, or filter. This is his basis, chosen randomly as well, and if the photons pass and he has chosen the right filter, the photon is kept. This is the Raw Key Exchange stage. Next, the Key Shifting stage is done when Alice and Bob both publicly broadcast their bases and they discard the bits that do not match or the ones that Bob was unable to determine. This forms the key for the encrypted message [6]. This is illustrated in Figure 5.

III. Quantum Experiments at Space Scale

Background

QKD has been theoretically proposed for many decades and is now being tested with satellites in China. The recent Quantum Experiments at Space Scale (QUESS) Chinese research project has taken QKD to another level. QUESS is a proof-of-concept mission to test QKD, experimenting with its capabilities from space as well as testing various theorems and quantum mechanical cryptography viability. It serves as a quantum optics mission, demonstrating the development of quantum security and quantum teleportation. In 2016, Tiangong-2, a Chinese space laboratory was launched and contains a communications module allowing for space-to-earth communications. The project also includes various project Micius satellites to transmit quantum signals from China, to multiple other stations set up in other regions of China as well as Vienna, at the Austrian Academy of Sciences [7]. The project expects a network of Micius satellites by 2030.



Both Alice and Bob create a string of bases at random. Alice also creates an additional string for her states.

Alice produces photons with 4 different polarizations based on her states and bases and sends them to Bob

Bob detects and measures these photons by passing them through randomly chosen filters (his bases).

The bases of Alice and Bob are announced over a public channel and keep the qubits that match to the key.

The matching qubits are set as the encryption key for the message.

Figure 5: *BB84 protocol implementation.*

Among other activities, these satellites have been tasked with researching the quantum entanglement of particles to gain further insights and facilitate quantum communications and teleportation.

Quantum Teleportation

Quantum teleportation is a technique which transfers quantum information from a sender to a receiver.. To facilitate this, there needs to be a sender Alice, the information as a qubit, a quantum channel, a classical channel, and a receiver Bob. The information also requires an entangled quantum state, or Bell State, between two external particles which creates a unified quantum state so that if one particle moves or is affected, a similar reaction will occur on the other particle. This state also means that if the particles are nonlocal and entangled, then the information will be transmitted instantaneously, faster than the speed of light, which is considered impossible. This is known as the Einstein-Podolsky-Rosen Paradox. Multiple different interpretations of the paradox have been taken throughout the years, such as Bohm's variant and Bell's Theorem, to explain the paradox.

Quantum teleportation is built upon Bell's Theorem, in which an electron-positron singlet, entangled pair, transmits information. This method of communication sends quantum information to the receiver but due to the involvement of a classical particle and the fact that the information cannot be fully received without it, the communication cannot be faster than the speed of light. For the communication to occur the measured states must be on an orthonormal basis. For example, if Alice measures her electron to a positive spin on the z-axis, Bob will measure the positron to a negative spin on the z, x, or y-axis, but any other non-orthogonal axis will not correlate with Alice's measurement [8]. For teleportation, take the particle to be transmitted as A, and the entangled singlet to be B and C. Alice will take A and unify its quantum state with B, causing a change in the unified quantum state, which is then sent to Bob. Bob measures his half of the pair, C, which allows him to determine the change on Alice's particle and hence the original particle. Then, Bob recreates A with the information from C. In this way, the original quantum information is not kept by Alice as it becomes part of the singlet's entangled quantum state, and therefore the no-cloning theorem is not violated once Bob receives his information. However, for the quantum information to be preserved, it must be accompanied by a classical channel that will transmit the change measurement result, hence the communication cannot occur faster than the speed of light [9].

Hardware

The first successful quantum teleportation and test of Bell's Theorem occurred as part of the QUESS initiative by China under lead scientist Jian-Wei Pan, transmitting a signal over 1200 km using a project Micius satellite [10]. This tested the nonlocality hidden-variable theory. Nonlocality is the concept of two separated particles of a singlet, in this case over 1200 km, while the hidden-variable theory suggests explanations for quantum mechanical phenomena relying on some unknown, unobservable, hypothetical entities. Both of these concepts apply to Bell's theorem. The project's testing of QKD has also proven fruitful, due to the success of a secure channel in space-to-ground communications. Previous tests of QKD have involved fiber-optic cables, underground, to transmit photons, since open air brings atmospheric interference and scattering, destroying the entangled state. However, sending quantum keys from space in an orbiting satellite reduces this scattering and allows distribution to occur over even greater distances. It is useful to note that instead of the single photon quantum teleportation described above, the materials aboard QUESS transmit several photons, increasing the magnitude of complexity. The procedure is performed by a "Sagnac effect" interferometer, a device that generates a pair of entangled particles by shining an ultraviolet laser on a nonlinear optical crystal to facilitate such QKD. Specifically, a mode-locked Ti-sapphire laser emits ultraviolet femtosecond pulses incident on two bismuth borate (BiBO) crystals, generating the two pairs of photons [11]. One of these pairs is created through collinear spontaneous parametric down-conversion (SPDC) in a crystal of optical non-linearity. This turns one of the received pump photons into two lower energy, entangled photons [12]. One photon in this pair will be used to detect a single photon which will be teleported. This photon can be initially polarized using a half-wave plate (HWP) and a quarter-wave plate (QWP). The other pair is generated through non-collinear SPDC in which the BiBO crystal is realigned. In order to conduct the Bell-state measurement on the photon singlet, the photons are overlapped on a photon beam splitter (PBS) which admits horizontal polarization and reflects vertical polarization, thus sorting and separating the unified quantum states. This allows the entangled pair to be used as the secure quantum channel, finally sending the photon down the classical channel completes the teleportation. A diagram of this process is shown in Figure 6. However, space-to-ground satellite quantum communications are limited in that it only works without sunlight as well as requires a direct line of sight. Further goals include long-distance entanglement before the measurement for more sophisticated and efficient space communications, reaching towards real network connections with QKD.

Current Developments

On July 27, 2022 the Lijian-1 carrier rocket lifted off, carrying 6 new Chinese micro-nano quantum satellites. The six satellites include the Space New Technology Experimental Satellite (SATech) containing 15 payloads of science experiments, developed by the Innovation Academy for Microsatellites under the Chemical Abstracts Service, a division of the American Chemical Society). The satellite also includes a hyperspectral camera, X-ray telescope, the CPT Atomic Magnetic Field Precision Measurement System, and Space Component Radiation Effect On-orbit Test Platform or the Space Center Weather Room [13]. These will conduct atmospheric experiments as well as solar, Earth, and infrared observations. Another satellite carried is called Jinan 1, which will perform QKD experiments at a smaller, less expensive scale than the Micius satellite. The rest of the spacecraft were spherical atmospheric density satellites, a pair of satellites for testing electromagnetic assembly systems, and the Nanyue Science Satellite for science popularization [14].

IV. NIST Post-Quantum Cryptography

Background

As the development of the quantum industry produces faster and larger supercomputers and as satellites prove theorems and demonstrate the potential for quantum space communications, it becomes ever more important to create reliable quantum protocols. In 2016, the National Institute of Standards and Technology (NIST) announced its Post-Quantum Cryptography competition, a competition to develop cryptographic systems that would be safe against both quantum and classical computers [15]. On July 5th, 2022, 6 years after the competition started, NIST announced the first group of 4 of 8 winners. One for general encryption, CRYSTAL-Kyber, and three for digital signature authentication, CRYSTALS-Dilithium, FALCON, and SPHINCS+. Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The other 4 are still in development and do not use lattices or hash functions [16].

New Protocols

CRYSTAL Kyber and Dilithium

Both Kyber and Dilithium are built by the "Cryptographic Suite for Algebraic Lattices" (CRYSTALS) based on module lattices. Both are variants of Keccak, an advanced cryptographic function part of the Secure Hash Algorithm family from NIST. Kyber is an IND-CCA2-secure key encapsulation mechanism (KEM) [17] using the learning with error (LWE) based encryption scheme of Oded Regev. This is built upon a CPA-secure cryptosystem which is based on the difficulty of the Module-LWE. Kyber also has three different parameter sets, aiming at different security levels: Kyber-512 comparable to AES-128, Kyber-768 comparable to AES-192, and Kyber-1024, comparable to AES-256[18]. AES, advanced encryption standard, is a specification for the encryption of data announced by NIST in 2001. This standard uses keys of 128, 192, and 256 bits and is used in federal departments and agencies when information is tagged as sensitive, but unclassified, information [19].

The module lattices that Kyber and Dilithium are built upon lie between the realm of the LWE problem and Ring-LWE, although they are closer to the unstructured lattices of the LWE problem as opposed to the more algebraic structure of Ring-LWE. The lattice problems in Regev's encryption scheme include the Short Vector Problem (SVP) and GapSVP. In the SVP, given a bases of vector space and a norm N, often designated as L2, one must find the shortest non-zero vector in terms of L [20]. This problem is known to be NP-hard, meaning that it is at least as hard as the hardest NP problems, NP being nondeterministic polynomial time, making its solution time solvable but undeterminable. These problems can be solved with a myriad of solutions, generally distinguished into two different types: algorithms requiring super-exponential time and a (2n) and poly(n) memory, and algorithms using exponential time as well as lattice dimensional space. Lattice enumeration and random sampling reduction are utilized in the first delineation while the second includes lattice sieving, computing the Voronoi cell of the lattice, and discrete Gaussian sampling. Kyber is also readily compatible with current classical and quantum computers. The protocol is already being tested by such platforms as Cloudflare, Amazon, and IBM's quantum computers.

Dilithium is built upon similar premises, the hardness of lattice problems over lattice modules, but is instead used for digital signatures[21]. Digital signatures are a mathematical construct that allows one to verify authenticity (that a message was sent by a known sender) and integrity (that the contents of the message were not altered in the sending process). These signatures are commonly used for software distribution, financial transactions, contract management for software, and other cases where it is vital to check for forgeries of or tampering with information. These signatures most commonly utilize asymmetric cryptography and a timestamp for the digital signature so that even if the key is exposed, the signature remains valid. The security notion is that an enemy, Eve, cannot produce a signature of a message they haven't seen yet, nor produce another signature of a message they signed. Dilithium is based on the "Fiat-Shamir with Aborts" technique by Lyubashevksy, using rejection sampling for lattice-based Fiat-Shamir schemes compact and secure. The Fiat-Shamir scheme, also referred to as the Fiat-Shamir heuristic, is a technique that verifies a user with an interactive proof of knowledge and then creates a digital signature based on the user. In this way the user can reveal some public information, such as knowledge of a unique string, without disclosing the important information. This technique was first proposed by Amos Fiat and Adi Shamir in 1986 [22]. A key part of the scheme relies on the interactive proof system being of the public coin type, in that the random choices by the verifier are made public [23]. In the "Fiat-Shamir with Aborts" technique, a key improvement is the reduction of the identification scheme to many millions of bits to an efficient 50,000 to 60,000-bit complexity from Girault's factoring-based digital signature scheme. The security of this lattice and factoring-based identification scheme lies in SVP, while the security of the signature scheme is based on the same assumption in the random oracle model [24].

Falcon

Falcon is also a lattice-based signature scheme like Dilitihum but instead based on the theoretical framework of Gentry, Peikert, and Vaikuntanathan [25]. An important component of the framework of Gentry et al. is the efficient algorithm for sampling lattice points from a discrete Gaussian probability distribution, in which the standard deviation is the length of the longest Gram-Schmidt vector of the basis for the SVP problem. A vital security aspect is that the output distribution of the algorithm is unrelated and unconnected to the unique geometry of the given basis [26]. This work centers around improvements in showing how to use a short basis in a theoretically secure way, based on the natural and innate "trapdoors" in lattices. Lattices have a number of these trapdoors useful in cryptography, and it has been a long-standing problem to find a method to give a direct construction of digital signatures with the simplicity and efficiency of other lattice-based primitives, low-level cryptographic algorithms, and even the random oracle model. In the work of Goldreich, Goldwasser, and Halevi, the "GGH" signature proposal, they theoretically created a secure system with direct relation to a lattice problem but lacked proof for security. Here it was intuitively believed that the short basis of a lattice, a basis in which all the vectors are relatively short, could serve as a trapdoor [27]. This framework is instantiated over NRTU lattices, a previous cryptographic algorithm for digital signatures, with "fast Fourier sampling," a trapdoor sampler. The underlying problem that is used in Falcon is the short integer solution problem (SIS), based on the SVP, an average case problem in lattice-based cryptography algorithms.

The SIS problem is a hard and average-case problem. Given, Z_q^n, a n-dimensional set of vectors, one must find a nontrivial and small

$$z_1, z_2, \cdots, z_m \subset Z \tag{3}$$

such that

$$z_1 \cdot (a_1) + \cdots + z_m \cdot (a_m) = (0) \subset Z_q^n \tag{4}$$

This problem can also be presented as matrix A of dimensions $n{\cdot}m$, multiplied by the vector $\vec{z}$:

$$(A) \cdot (z) = (0) \subset Z_q^n \tag{5}$$

In a paper by Miklós Ajtai, a family of one-way functions of the SIS problem was presented. He proved that in a lattice-based cryptographic construction, the SIS problem holds secure in the average case if the SVP_γ, where γ equals n to the power of some constant $c > 0$, is hard in a worst-case scenario [28]. In summary, given a random set of undetermined linear equations with many integer solutions, one must find a solution that uses only, or mostly, small numbers. More specifically, the sum of their squares should be small.

Sphincs+

Sphincs+ is a hash-based signature scheme, advancing a similar signature scheme called Sphincs, unveiled at EUROCRYPT 2015.

Sphincs+ specifically aims at reducing the signature size of its hash functions [29]. A hash-based signature scheme is a set of any hash-based cryptographic algorithms, based upon the notion of hash functions. A hash function is any function that simplifies data by assigning complicated values to simplified values called hashes. This works as an efficient data storage and retrieving system with these assigned low-data hashes. In cryptography, hash-based schemes combine a one-time signature scheme with a hash tree. One-time signature schemes can only sign a signal message securely, and to this end, the hash tree is implemented to combine the keys within an individual, larger structure. Due to this limitation, in its post-quantum cryptography competition NIST specified that any algorithm must support a minimum of 264 signatures safely. There are three variants of Sphincs+: SHAKE256, SHA-256, and Haraka. The first upgrade of Sphincs+ from Sphincs is its ability to protect against multi-target attacks. In Hülsing et. al, they introduce XMSS-T, a novel hash-based secure signature system. This new scheme achieves tight security while using hash functions with a smaller output length, leading to the previously mentioned smaller signature size [30]. The increased security is derived from new hash function properties against multi-target notions, defined and analyzed in their paper. Furthermore, this scheme is shown to be both resistant to classical and quantum generic attacks, allowing an estimation of the quantum security of XMSS-T. More specifically, quantum query complexity is tailored for cryptographic algorithms, overcoming limitations of standard quantum query techniques such as a limitation to purely worst-case complexity. The basic concept is to use different hash functions for each call, keyed with different keys and applied with varied bitmasks. These keys and bitmasks are pseudorandomly created from a specifying address and a public seed. There was also an introduction of tweakable hash functions in addition to the input value, the public seed, and the address. More improvements include tree-less WOTS+ public key compression, replacing the few-time signature scheme, HORST, with Forest of Random Subsets (FORS), and a verifiable index selection [31].

Rest of the Qualifiers

In the post-quantum cryptography competition, NIST will select a total of eight new protocols. While only the first four were chosen from Round 3 of submissions, and another four were submitted in Round 4, but no choice has been made thus far [32]. These four are BIKE, Classic McEliece, HQC, and SIKE. BIKE stands for Bit Flipping Key Encapsulation and is a code-based key encapsulation mechanism based on Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) [33]. Classic McEliece, dedicated to the memory of Robert J. McEliece who introduced the first code-based public-key encryption system in 1978, specifies random binary Goppa codes, an algebraic geometric code. This is an error-correcting code that belongs to the class of general Goppa codes, which is a general type of linear code with an algebraic curve over a finite field introduced by Valerii Denisovich Goppa. HQC, standing for Hamming Quasi-Cyclic, is a code-based public key encryption system. It is an IND-CCA2 KEM, similar to Kyber, with a small public key size, precise decryption failure rate analysis, and works on efficient implementations [34].

SIKE

SIKE, standing for Supersingular Isogeny Key Encapsulation, is an isogeny key encapsulation suite based on pseudo-random walks in supersingular isogeny graphs [35]. However SIKE was cracked not once, but twice, following its release. In a paper by Wouter Castryck and Thomas Decru, a new powerful key recovery attack was presented on the Supersingular Isogeny Diffie–Hellman key exchange protocol (SIDH) on which SIKE is based. The attack is based on a "glue-and-split" theorem from Ernst Kani in 1977 [36]. Moreover, on August 8th, 2022, this protocol was once again broken, this time by researchers at Bristol University, with arbitrary starting curves, described in a paper by Luciano Maino and Chloe Martindale [37].

V. BB84 Algorithm in Python

Using IBM's quantum lab I coded my own BB84 algorithm and ran it on quantum computers. For this project, I used Qiskit, NumPy, cryptography's Fernet, and base64 converters.

Tests

Multiple tests were run on the quantum computer's efficiency and simulator efficiencies based on qubit lengths. he quantum computer used was ibm_nairobi with a Falcon r5.11H processor, 7 qubits, a quantum volume of 32, and a circuit layer operations per second of 2600. The quantum simulator used was simulator_stabilizer, an efficient simulator of Clifford circuits. It can simulate noisy evolution if the noise operators are also Clifford gates. This simulator has 5000 qubits.

Table 1: *Qubit Length vs Runtime of Simulator*

Runtime	Qubit Length
1.0 sec	2
4.0 sec	4
1.8 sec	8
1.3 sec	16
1.2 sec	32
1.2 sec	64
1.0 sec	128
1.1 sec	256
7.5 sec	512
0.878 sec	1024
1.0 sec	2048
1.7 sec	4096

Overall the speeds as more qubits are added to the circuit, is negligible due to the small number of bits the computer and simulator can act on. The fluctuations are due to the time the code spent in the system, causing some erratic spikes in runtime.

Table 2: *Qubit Length vs Runtime of ibm_nairobi*

Runtime	Qubit Length
18.2 sec	2
10.3 sec	3
16.7 sec	4
16.1 sec	5
12.6 sec	6
13.4 sec	7

VI. Conclusion

Advances in quantum cryptography allows technology to be safe from the threat of the future. From early protocols like BB84, to current competitions in a race to find the best safeguard against quantum computers, this new method of communications is becoming more prevalent in the world. The preivous sections described applications and theory behind QKD, including branches like quantum teleportation. The world is apporaching a place where there is a greater need for guaranteed safety, through quantum mechanical principles.

References

[1] S. Meister, *The Bloch sphere, a geometric representation of a two-level quantum system.* Wikimedia, 2009.

[2] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, “Security of two quantum cryptography protocols using the same four qubit states,” *Physical Review A*, vol. 72, no. 3, 2005.

[3] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, Feb. 1978.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2021.

[5] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.

[6] B. Archana and S. Krithika, “Implementation of BB84 quantum key distribution using optsim,” *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, Jun. 2015.

[7] “First Quantum Satellite Succesfully Launched,” *First Quantum Satellite successfully launched.* [Online]. Available: https://www.oeaw.ac.at/en/first-quantum-satellite-successfully-launched. [Accessed: 27-Sep-2022].

[8] J. S. Bell, “On the einstein podolsky rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, pp. 195–200, 1964.

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[10] B. Li, Y. Cao, Y.-H. Li, W.-Q. Cai, W.-Y. Liu, J.-G. Ren, S.-K. Liao, H.-N. Wu, S.-L. Li, L. Li, N.-L. Liu, C.-Y. Lu, J. Yin, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, “Quantum State transfer over 1200 km assisted by prior distributed entanglement,” *Physical Review Letters*, vol. 128, no. 17, 2022.

[11] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Ground-to-satellite quantum teleportation,” *Nature*, vol. 549, no. 7670, pp. 70–73, 2017.

[12] M. G. McLaren, F. S. Roux, and A. Forbes, “Realising high-dimensional quantum entanglement with orbital angular momentum,” *South African Journal of Science*, vol. 111, no. 1/2, pp. 1–9, May 2013.

[13] Weather Room, "The domestic quantum magnetometer and chip radiation tester were launched successfully," *WeChat public platform*, 07-Jul-2022. [Online]. Available: https://mp.weixin.qq.com/s/DYYx-P1zSEpFVwBUjG_X1. [Accessed: 27-Sep-2022].

[14] A. Jones, “Big New Chinese rocket lofts 6 experimental satellites on debut launch (video),” *Space.com*, 10-Aug-2022. [Online]. Available: https://www.space.com/china-lijian-1-rocket-debut-launch-success. [Accessed: 27-Sep-2022].

[15] I. T. L. Computer Security Division, “Post-quantum cryptography: CSRC,” *CSRC*, 20-Dec-2016. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. [Accessed: 27-Sep-2022].

[16] “NIST announces first four quantum-resistant cryptographic algorithms,” *NIST*, 07-Jul-2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. [Accessed: 27-Sep-2022].

[17] C. Wang, Y. Liu, and J.-T. Kim, “An ind-CCA2 secure key-policy attribute based key encapsulation scheme,” *2009 International Conference on Multimedia Information Networking and Security*, Nov. 2009.

[18] “Crystals,” *Kyber*, 2017. [Online]. Available: https://pq-crystals.org/kyber/index.shtml. [Accessed: 27-Sep-2022].

[19] “Advanced encryption standard (AES),” Nov. 2001.

[20] S. Khot, "Hardness of approximating the shortest vector problem in lattices," *Journal of the ACM*, vol. 52, no. 5, pp. 789–808, Sep. 2005.

[21] "Crystals," *Dilithium*, 2017. [Online]. Available: https://pq-crystals.org/dilithium/index.shtml. [Accessed: 27-Sep-2022].

[22] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," *Advances in Cryptology — CRYPTO' 86*, vol. 263, pp. 186–194, Dec. 2000.

[23] S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, Feb. 1989.

[24] V. Lyubashevsky, "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures," *Advances in Cryptology – ASIACRYPT 2009*, pp. 598–616, 2009.

[25] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," *Proceedings of the fortieth annual ACM symposium on Theory of computing*, 2008.

[26] *Falcon*, 2017. [Online]. Available: https://falcon-sign.info/. [Accessed: 27-Sep-2022].

[27] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," *Advances in Cryptology — CRYPTO '97*, pp. 112–131, May 2006.

[28] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, Jul. 1996.

[29] *SPHINCS+*, 2017. [Online]. Available: https://sphincs.org/. [Accessed: 27-Sep-2022].

[30] A. Hülsing, J. Rijneveld, and F. Song, "Mitigating multi-target attacks in hash-based signatures," *Public-Key Cryptography – PKC 2016*, pp. 387–416, Feb. 2016.

[31] Andreas and Andreas, "Andreas Hülsing," *SPHINCS+ – The smaller SPHINCS*, 04-Dec-2017. [Online]. Available: https://huelsing.net/wordpress/?p=558. [Accessed: 27-Sep-2022].

[32] I. T. L. Computer Security Division, "Round 4 submissions - post-quantum cryptography: CSRC," *CSRC*, 21-Sep-2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions. [Accessed: 27-Sep-2022].

[33] "Bit flipping key encapsulation," *BIKE*, 2017. [Online]. Available: https://bikesuite.org/. [Accessed: 27-Sep-2022].

[34] "HQC (Hamming Quasi-Cyclic)," *HQC*, 2017. [Online]. Available: https://www.pqc-hqc.org/documentation.html. [Accessed: 27-Sep-2022].

[35] "Supersingular isogeny key encapsulation," *SIKE*, 2017. [Online]. Available: https://sike.org/. [Accessed: 27-Sep-2022].

[36] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH (preliminary version)," *Cryptology ePrint Archive*, 05-Aug-2022. [Online]. Available: https://ia.cr/2022/975. [Accessed: 27-Sep-2022].

[37] L. Maino and C. Martindale, "An attack on SIDH with arbitrary starting curve," *Cryptology ePrint Archive*, 25-Aug-2022. [Online]. Available: https://eprint.iacr.org/2022/1026. [Accessed: 27-Sep-2022].

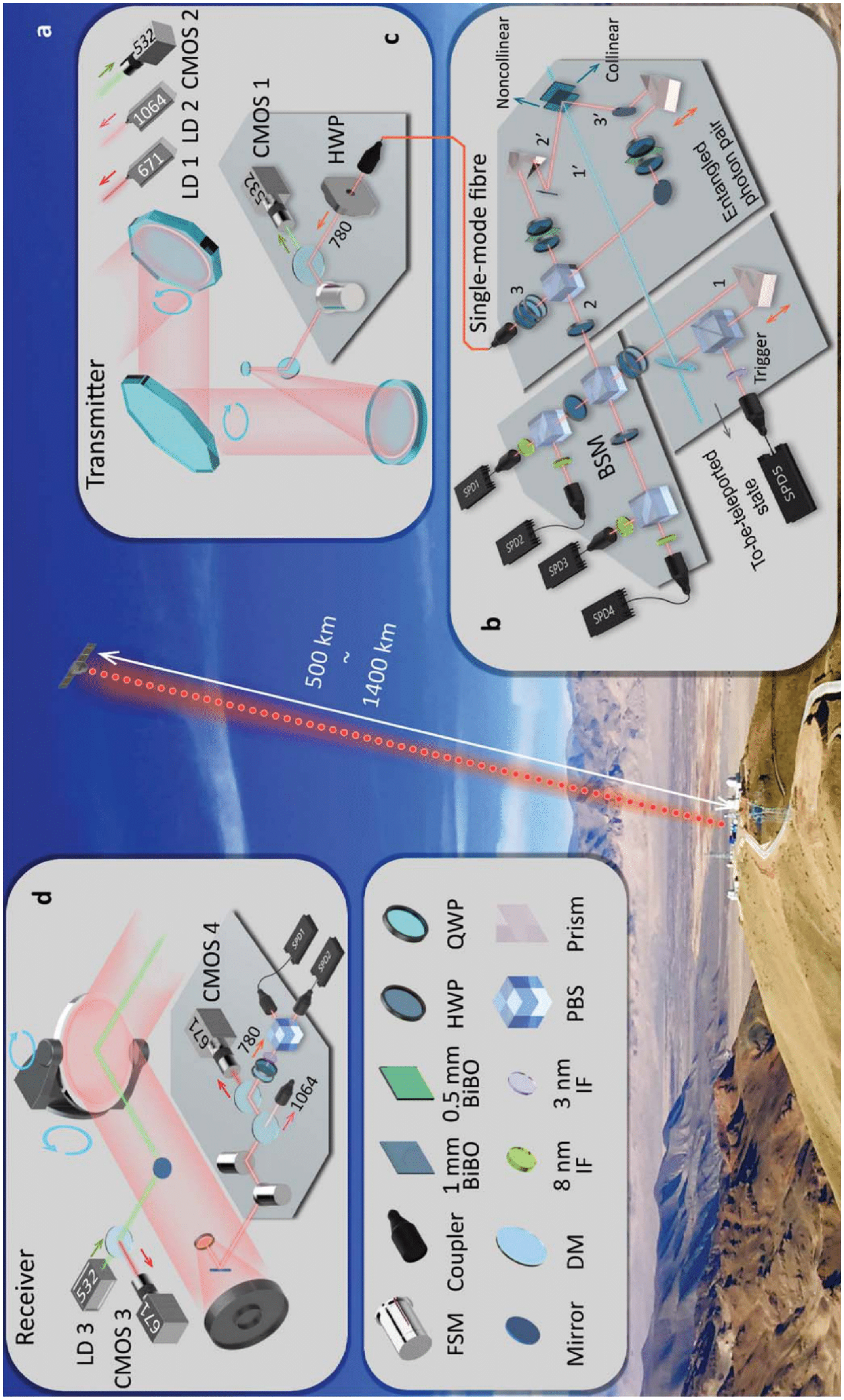


Figure 6: *Diagram of hardware for quantum teleportation [11].*