

Quantum Cryptography

Wyatt Furois, Mason Hawver
Dan Hawker, Blake Briol

University of Minnesota - Twin Cities

Professor Gennady Lyubeznik
MATH 5248

April 2025

Abstract

Classical cryptography, such as RSA, Diffie-Hellman, and DES, depend on mathematical complexity and shared secrets to ensure secure communication. Its security is based on assumptions about computational hardness, which can be undermined by algorithmic breakthroughs or advances in computing power, such as quantum computers. Quantum cryptography, by contrast, leverages simple quantum systems, such as light polarization, to transmit information in a way that is fundamentally and provably secure. Any attempt to measure a quantum state inevitably disturbs it, making eavesdropping provably detectable. Hence, cryptographic protocols that use quantum communication can securely share information, even in the presence of an adversary and without any pre-shared secrets. Unlike classical methods, the security of quantum cryptography is guaranteed by the laws of physics, not assumptions about computational limitations. In this paper, we will introduce the basic principles of quantum information theory and show how they can be used to construct cryptographic protocols with provable security.

CONTENTS

Contents	1
1 Introduction	2
2 Quantum Fundamentals	2
2.1 Light Polarization	2
2.2 Dirac Notation	3
2.3 Hilbert Space	3
2.4 Classical vs Quantum Bits	3
2.5 Formal Definition of Qubit	4
2.6 Superposition	4
2.7 Measurement Collapse	4
2.8 Quantum Gates and Basis Transformation	5
2.9 Multi-Qubit Systems and Tensor Products	5
2.10 Entanglement	5
2.11 Quantum Registers and Circuits	6
2.12 Conjugate Bases	6
2.13 Probabilistic Definition of ψ^n	7
3 Quantum Cryptography	7
3.1 Quantum Public-Key Distribution (QKD)	7
3.2 Quantum Coin Flipping (QCF)	9
3.3 Quantum-Secure Zero-Knowledge Proofs (QZP)	12
4 Quantum Attacks on Classical Cryptography	14
4.1 Prime Factorization	14
4.2 Shor's Algorithm	15
5 Conclusion	16
6 Appendix	16
6.1 Einstein–Podolsky–Rosen Effect	16
References	17

1 Introduction

Quantum communication is the transmission of information using quantum systems, such as the polarization states of single photons, through optical fibers or free-space channels. Unlike classical communication, which relies on digital and analog signals that can be measured, copied, and amplified without disturbance, quantum communication leverages the unique properties of quantum mechanics, such as the uncertainty principle and the no-cloning theorem, to enable fundamentally secure information sharing. It was first described by Stephen Wiesner in his "Conjugate Coding" paper [12]. Wiesner used quantum communication for two applications: making money that is in principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. The Achilles heel of quantum communication is the practical application of it. Quantum signals are very weak in practice and can't be amplified due to the laws of physics¹, so quantum communication can only happen over short distances.

Quantum cryptography is the cryptographic application of quantum communication. It makes use of quantum communication to share information that is provably secure against eavesdropping, by exploiting the fundamental principles of quantum mechanics. It was first introduced by Charles Bennett and Gilles Brassard in a series of papers [1, 2]. In their work, Bennett et al. proposed a quantum secret key distribution protocol, BB84, which allows for two parties to share a secret key in the presence of an adversary and without any pre-shared secrets. It achieves the same goal as public-key cryptography without the need for assumptions about computational difficulty. Instead its security is rooted in the fundamental laws of physics. Furthermore, In their work, Bennett et al. also proposed a quantum coin tossing protocol, which allows two remote parties to generate a shared random bit without either having any influence on the outcome. The only assumption made for its security is that either party cannot violate the principles of quantum mechanics. This was the birth of quantum-based cryptography. Since then, more practical implementations have been developed, and its scope has expanded significantly. Quantum cryptographic protocols now extend beyond simple key distribution to encompass secure communication networks involving multiple parties. Notably, quantum key distribution (QKD) has been deployed in real-world network settings, including satellite-based systems. Furthermore, Quantum computing has emerged as a powerful tool capable of breaking many classical cryptographic schemes. Algorithms such as Shor's algorithm demonstrate that quantum computers can efficiently factor large integers and compute discrete logarithms, tasks that are computationally infeasible for classical machines. This directly threatens widely used public-key systems like RSA and Diffie-Hellman, whose security rests on the presumed hardness of these problems. As a result, quantum cryptography represents both a defense against and a response to the capabilities of quantum computation, offering new tools for secure communication while challenging the foundations of classical cryptographic infrastructure.

2 Quantum Fundamentals

In classical systems, their states are distinct and deterministic, for example the position and velocity of a ball as it rolls down a hill or the binary value of a c-bit. In quantum mechanics, however, the state of a quantum system is fundamentally probabilistic. Their state doesn't encode just one singular outcome, but instead encodes a superposition of all possible outcomes each weighed with a different probability. This fundamental difference between classical and quantum systems will form a foundation for understanding how quantum information is represented, manipulated, and ultimately used in secure communication and computation.

2.1 Light Polarization

Classically, light is understood to be a wave in the electromagnetic field. Light, as an electromagnetic wave, consists of oscillating electric and magnetic fields that are always perpendicular to each other and to the direction of propagation. This behavior is a direct consequence of Maxwell's equations, which describe how changing electric fields generate magnetic fields and vice versa. Light polarization refers to the direction in which the electric field of an electromagnetic wave oscillates as it propagates. A 3D visualization of Light's wave dynamics can be seen here: <https://www.desmos.com/3d/q0iqi1fnnh>. And a visualization of the wave on the plane normal to its direction of propagation can be seen here: <https://www.desmos.com/calculator/1pyuuvcavy>.

2.1.1 Classical vs. Quantum Behavior. For a light wave polarized at a constant angle α relative to the horizontal axis $|\leftrightarrow\rangle$ ², the direction of the electric field's oscillation can be expressed as a linear combination, a superposition, of the horizontal and

¹the laws of physics that ensure security for quantum cryptography are also the same laws that prevent quantum communication from being practical.

²See Section 1.2.1 for an Explanation of Dirac Notation

vertical axes: $\cos \alpha |\leftrightarrow\rangle + \sin \alpha |\uparrow\rangle$. When such a wave passes through a vertical polarization filter³, classical wave theory predicts that only the vertical component survives:

$$\sin \alpha |\uparrow\rangle. \quad (1)$$

However, the discovery that light's energy is quantized—carried in discrete packets called photons—reveals a fundamental limitation of the classical picture. In classical wave theory, the energy of a polarized light wave is proportional to the square of its amplitude, which can be continuously divided between components like $|\leftrightarrow\rangle$ and $|\uparrow\rangle$. But quantum mechanics tells us that a single photon's energy is indivisible: it cannot be split across multiple directions. When a photon encounters a polarization filter, it is not partially transmitted—it either passes through or is entirely absorbed. The act of measurement collapses the photon's wavefunction into one of the two basis states, $|\leftrightarrow\rangle$ (blocked) or $|\uparrow\rangle$ (transmitted), with probabilities determined by the angle α . And before a measurement photon doesn't carry definite polarization but a superposition, a linear combination, of definite polarization states. This behavior is inherently probabilistic and cannot be explained by any hidden classical mechanism—only one bit of information is revealed per photon, and the outcome is fundamentally random. Thus, light polarization is the simplest physical realization of a two state quantum system, a *qubit*, and it is used to transmit qubits for most practical applications.

2.2 Dirac Notation

Dirac Notation, also known as *bra-ket notation*, is a compact and powerful way to describe the states and operations of quantum systems. The notation consists of Kets, $|\psi\rangle$, and Bras $\langle\phi|$. Kets describe the state of a quantum system and exist as a column vector v in a complex vector space known as a Hilbert space H^4 . For a two state quantum system, it can be written as a superposition of two basis states: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. To measure a quantum state we use the corresponding Bra. A Bra is the dual (or conjugate transpose) to a Ket, and describes the transformation of a Ket to a complex number. It acts as a measurement of the Ket, and it exists as a row vector v^* in a dual Hilbert space H^* . The inner product of a Bra and Ket is $\langle\psi, \phi\rangle$. It represents the projection of the state $|\psi\rangle$ onto the state $|\phi\rangle$, and returns a complex number. Physically, if a system is in state $|\psi\rangle$, and we measure it in the state $|\phi\rangle$, the probability of obtaining that outcome is given by the squared magnitude of the inner product:

$$P(\phi \text{ observed from } \psi) = |\langle\phi|\psi\rangle|^2 \quad (2)$$

2.3 Hilbert Space

The Hilbert space is a mathematical space in which quantum states can be described and supports superpositions, inner products, and completeness. This will allow us to describe a quantum system rigorously. An n -th dimensional space H^n is a Hilbert space [9] if and only if:

- H^n is a metric space.
- For every point M in the Cauchy sequence a_n found in H^n , the limit of the a_n , L , is also in H^n . This is to say the space H^n is *Cauchy Complete*.
- There exists an inner product⁵ operation in H^n such that $\langle\vec{x}, \vec{y}\rangle$ is *complete*.

Furthermore, the inner product operation on a space is said to *induce* the Hilbert Space H^n ⁶. For all objects discussed in this paper can be found withing some Hilbert Space H^n .

2.4 Classical vs Quantum Bits

The foundation of classical information theory is the *c-bit*, which exists in one of two distinct states: 0 or 1. By contrast, the foundation for quantum information theory is the *quantum bit*, or *q-bit*. A qubit is a two state quantum system that can also exist in the states $|0\rangle$ and $|1\rangle$, analogous to classical 0 and 1. However, due to the principle of superposition, a qubit can also exist in a continuous combination of both states:

³Your sunglasses are polarization filters.

⁴See Section 2.3.1 for more explanation

⁵An inner product can be read as an abstraction of the dot-product such that you can have an operation acting on two vectors which will yield a scalar value.

⁶In mathematical structures, we observe that a Hilbert Space is a subset of topological spaces, metric spaces, and normed vector spaces.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{where} \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

$$\langle 0|0\rangle = 1 \quad \langle 1|1\rangle = 1 \quad \langle 0|1\rangle = 0 \quad (3)$$

A possible row and column vector representation in the space $\mathbb{H}^2$ of the Kets and Bras of the classical 0 and 1 states could be:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \langle 0| = [1 \quad 0] \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \langle 1| = [0 \quad 1] \quad (4)$$

The polarization of a light wave can be represented as a two state quantum system, a qubit. A light wave may be in a horizontally polarized state $|\leftrightarrow\rangle$ (analogous to $|0\rangle$), or vertically polarized $|\updownarrow\rangle$ (analogous to $|1\rangle$). But it can also be in a diagonal superposition of the two:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle) \quad (5)$$

This diagonal state has no classical analog — it's not simply halfway between horizontal and vertical; it is genuinely both at once until measured. When measured in the horizontal-vertical basis, the photon randomly collapses into one of the two outcomes, with equal probability. This probabilistic nature is intrinsic, not due to experimental uncertainty. Classical bits are deterministic and discrete, while quantum bits are probabilistic and continuous within a two-dimensional space. This fundamental difference opens the door to powerful new computational and cryptographic possibilities, many of which will be explored in later sections.

2.5 Formal Definition of Qubit

Ψ is a matrix representation of an isolated qubit if and only if:

$$\Psi = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \quad \text{such that} \quad a, c \in \mathbb{R}^1 \quad b \in \mathbb{C}^2 \quad ac - |b|^2 \geq 0 \quad (6)$$

We can now admit the typical notation, describing the qubit (Ψ) as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ such that: $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. While we have defined a qubit, it is of little value to us if we are unable to perform operations on it, just as we perform operations on bits. As it turns out, we can certainly do that. There are several methods by which to achieve this including the use of the Bloch Sphere and Pauli Operators.

2.6 Superposition

The principle of superposition states: a quantum system can exist in a *superposition* of classical states. This doesn't mean it's in a probabilistic mixture of basis states, but it exists in all basis states at once. And at any time it carries information about each basis state as probabilistic amplitudes. This allows for unique quantum effects like interference and entanglement.

2.7 Measurement Collapse

Measurement of a quantum system reduces its superposition into a single distinct state from all the possible basis states the system was in a superposition over. This is called measurement collapse. For a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, when it is measured it can collapse into either basis state $|0\rangle$ or $|1\rangle$. The probability of each outcome, given by the Born rule, is the absolute square of the inner product between the Bra of the outcome and the Ket of the qubit:

$$P(0) = |\langle 0|\psi\rangle|^2 = |\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle|^2 = |\alpha|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2 = |\alpha\langle 1|0\rangle + \beta\langle 1|1\rangle|^2 = |\beta|^2 \quad (7)$$

After the measurement, the qubit's state collapses to the observed outcome, and any prior information encoded in the superposition is lost.

2.8 Quantum Gates and Basis Transformation

Classical gates, like NOT, AND, and OR, are used to manipulate c-bits. Quantum gates are used to manipulate quantum systems including qubits. They are mathematically represented as unitary matrices to preserve the length and norm of a quantum superposition. The quantum equivalent to the classical NOT gate is the Pauli-X gate:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{with} \quad X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle \quad (8)$$

Another important quantum gate is the Hadamard gate, denoted $\mathfrak{H}$. It has no classical equivalent as it transforms a basis state of a qubit into an equal superposition. And it transforms the rectilinear (computational) basis, $\{|0\rangle, |1\rangle\}$, into the diagonal basis, $\{|+\rangle, |-\rangle\}$:

$$\mathfrak{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{with} \quad H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \quad (9)$$

This alternative basis, the Diagonal basis $\{|+\rangle, |-\rangle\}$, will be important for our later discussions of quantum cryptographic protocols like BB84 and coin flipping, as well as in quantum algorithms like Shor's. So far we have measured a qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, in the rectilinear basis, but we can measure it in other bases too since quantum states exist in a vector space. For example, if the qubit, $|\psi\rangle$, was measured in the diagonal basis then it will collapse into either the positive diagonal basis state, $|+\rangle$, or the anti diagonal basis state, $|-\rangle$. And the outcome probabilities of measurement are still given by the Born rule:

$$\begin{aligned} P(+) &= |\langle +|\psi\rangle|^2 = \left| \left(\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) \right) (\alpha|0\rangle + \beta|1\rangle) \right|^2 = \left| \frac{1}{\sqrt{2}} (\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle + \alpha\langle 1|0\rangle + \beta\langle 1|1\rangle) \right|^2 = \frac{1}{2}|\alpha + \beta|^2 \\ P(-) &= |\langle -|\psi\rangle|^2 = \left| \left(\frac{1}{\sqrt{2}}(\langle 0| - \langle 1|) \right) (\alpha|0\rangle + \beta|1\rangle) \right|^2 = \left| \frac{1}{\sqrt{2}} (\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle - \alpha\langle 1|0\rangle - \beta\langle 1|1\rangle) \right|^2 = \frac{1}{2}|\alpha - \beta|^2 \end{aligned} \quad (10)$$

For example, if a qubit with either the $|0\rangle$ or $|1\rangle$ state are measured by the diagonal basis the probability of collapsing into either diagonal basis state is $1/2$. Furthermore, if a qubit is prepared in either the $|+\rangle$ or $|-\rangle$ state and is measured by the rectilinear basis the probability of collapsing in to either rectilinear basis state is also $1/2$.

2.9 Multi-Qubit Systems and Tensor Products

Multi-qubit systems are created by combining multiple single qubits together. The tensor product, denoted $\otimes$, of two qubit states represents combining them into a 2-qubit system. The tensor product can also combine an (n) -qubit system and (m) -qubit system to create an $(n + m)$ -qubit system. An n -qubit system exists in the 2^n -dimensional Hilbert space and is a superposition over all 2^n basis states: $\{|i_1 i_2 \dots i_n\rangle \mid i_k \in \{0, 1\}\}$. If a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$ are combined to form a 2 qubit system, then the combined state is written as:

$$|\psi\rangle \otimes |\phi\rangle = |\psi, \phi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \quad (11)$$

Not all 2-qubit systems can be factored back into a tensor product of two single qubits, however. These cases are called entangled states, and they are central to some quantum cryptographic protocols.

2.10 Entanglement

Entanglement is a unique quantum property. It happens when the state of one qubit is linked to another, and their combined state cannot be factorized into a tensor product of individual qubits. For example, the Bell states are the four maximally entangled 2-qubit systems and are defined as:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (12)$$

Lets show $|\Phi^+\rangle$ cannot be factorized by contradiction. Let $|\Phi^+\rangle = |\psi\rangle \otimes |\phi\rangle$, $|\psi\rangle = a|0\rangle + b|1\rangle$, and $|\phi\rangle = c|0\rangle + d|1\rangle$. Then, $|\Phi^+\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$. Implying, an unsolvable system of equations:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \implies ac = \frac{1}{\sqrt{2}} \quad ad = 0 \quad bc = 0 \quad bd = \frac{1}{\sqrt{2}} \quad (13)$$

This system of equations has no solutions, contradicting our assumption that a Bell state could be factorized. Thus, the defining feature of entanglement is the fact the quantum state cannot be factorized. Let $|\psi\rangle$ be the entangled state of two qubits X and Y. Due to the fact their entangled state cannot be factorized, when one is measured both collapse to a joint outcome. For example, if $|\phi\rangle = |\Phi^+\rangle$ then X and Y will share the same outcome when either is measured because it a superposition of only the states: $|0\rangle \otimes |0\rangle = |00\rangle$ and $|1\rangle \otimes |1\rangle = |11\rangle$.

Entanglement and the tensor product also allows us to describe systems where part of the state is controlled by one party and part by a second party — which is useful in quantum cryptographic protocols. For instance, a quantum coin flipping system can exist as a joint entangled shared coin state and an auxiliary system (or "witness" state):

$$|\psi_{\text{coin}}\rangle = \sum_{i_1, \dots, i_N} c_{i_1, \dots, i_N} |i_1, \dots, i_N\rangle \otimes |\psi_{\text{witness}}\rangle \quad (14)$$

Each outcome of the N coin flips is encoded by the superposition of $|i_1, \dots, i_N\rangle$ states, and each is entangled to the witness $|\psi_{\text{witness}}\rangle$ state. So when the outcome of the N coin flips is measured it also collapses the witness state — enabling verifiability and security assurances for multi-party quantum protocols.

2.11 Quantum Registers and Circuits

Quantum computing, used by algorithms like Shor's, is formulated by quantum registers and circuits. Quantum registers are n -qubit systems that store a quantum information. Each register exists in a superposition of quantum states, and they can be entangled with other registers to encode correlations between quantum systems. Quantum Circuits apply unitary transformations (quantum gates), like the Pauli-X and Hadamard gates, to registers to manipulate, transform, and entangle their states. The progress of a quantum system is determined by the application of gates until measurement collapse returns a classical outcome.

2.12 Conjugate Bases

Two orthonormal bases $\mathcal{A} = \{|a_1\rangle, |a_2\rangle, \dots, |a_n\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$ are conjugate bases in the Hilbert space, $\mathbb{H}^n$ if and only if for all pairs of indexes $i, j \in \{1, 2, \dots, n\}$ this equality holds:

$$|\langle a_i | b_j \rangle|^2 = \frac{1}{2} \quad \text{and} \quad |\langle b_i | a_j \rangle|^2 = \frac{1}{2} \quad (15)$$

That is to say that there is equal odds of measuring each state of one basis, $\mathcal{A}$ or $\mathcal{B}$, in the other conjugate basis. Conjugate bases are the cornerstones of quantum cryptographic protocols like BB84 and coin flipping. They rely on the unpredictability introduced by measuring in a conjugate basis for provable security. The rectilinear basis has two conjugates bases: the diagonal basis, $\{|+\rangle, |-\rangle\}$, and the basis formed by transforming the rectilinear basis with the Hadamard-Y gate into the imaginary basis. The imaginary basis is defined as:

$$\{|+i\rangle, |-i\rangle\} = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \quad (16)$$

The imaginary basis' states represents circularly polarized light - the direction of the electromagnetic wave's oscillation rotates in a circle as it propagates. The imaginary basis and the rectilinear basis are conjugates bases too by the transitive property. In our latter discussions, however, of quantum cryptographic protocols just the rectilinear and diagonal basis are used for simplicity.

2.13 Probabilistic Definition of ψ^n

In defining the classical probability states of ψ , we will observe the general case of ψ^n . Thus, the system of classical probabilities is defined as the following[4]:

$$\psi^n = \begin{bmatrix} p_1 & 0 & 0 & \dots & 0 \\ 0 & p_2 & 0 & \dots & 0 \\ 0 & 0 & p_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & p_n \end{bmatrix}$$

This square matrix now allows us to observe the system of classical probabilities for some n -dimensional quantum state ψ^n .

3 Quantum Cryptography

A major development in classical cryptography was the discovery and development of public-key ciphers, such as the Diffie Hellman key exchange, RSA, and El Gamal. Before their invention, parties would have to first exchange a secret key in private before they could communicate securely. Public-key ciphers now allow parties to share a secret key in public! In quantum cryptography, the development of quantum based public-key ciphers has further developed this revolutionary concept.

3.1 Quantum Public-Key Distribution (QKD)

In classical public-key cryptography, trapdoor functions are used to ensure the security of encryption and digital signature protocols without shared secret information. They enable operations that are easy to perform in one direction (e.g. encryption or signature verification), but are assumed to be computationally infeasible in reverse without privileged knowledge (e.g. decryption or signature generation). Trapdoor functions are not provably secure, however, and are vulnerable to eavesdroppers with advanced computational capabilities that can reverse these trapdoor functions. Quantum public-key cryptography, by contrast, is provably secure due to its use of quantum communication channels. By leveraging the fundamental nature of quantum mechanics, QKD protocols can detect eavesdropping attempts due to the no-cloning theorem, the Heisenberg uncertainty principal, and measurement collapse. That is why quantum public-key distribution is the most fundamental and trans-formative application of quantum mechanics to cryptography.

3.1.1 The BB84 Protocol. The BB84 protocol, developed by Bennett et al. in 1984 [1], was the first and remains the most widely used quantum public-key distribution (QKD) scheme. The protocol establishes a secret key between two parties, Alice and Bob, over both a quantum and a classical communication channel, without requiring prior shared secret information. The quantum channel is used to transmit a stream of randomly prepared qubits, which serve as the basis for a proposed secret key. The classical channel is then used to verify whether the key was transmitted without eavesdropping by comparing a subset of their measurements. If the error rate is below a certain threshold, the remaining bits can be used to form a secure secret key. Once established, the secret key can be used in an one-time pad (OTP) cipher for further communication.

To start the protocol, Alice and Bob first publicly agree on two conjugate bases that they will use to encode and measure their qubits with. For example, they could choose to use polarized photons as a physical realization of qubits, and choose the Rectilinear basis, $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$, and Diagonal basis, $\{|\nearrow\rangle, |\nwarrow\rangle\}$, as conjugate base pairs. Alice then generates two random bit strings a_i and b_i and keeps them secret. The Alice uses them to prepare N random qubits $|\phi_i\rangle$.

$$|\phi_i\rangle = \begin{cases} |\leftrightarrow\rangle & \text{if } a_i = 0, b_i = 0 \\ |\updownarrow\rangle & \text{if } a_i = 0, b_i = 1 \\ |\nearrow\rangle & \text{if } a_i = 1, b_i = 0 \\ |\nwarrow\rangle & \text{if } a_i = 1, b_i = 1 \end{cases} \quad \begin{matrix} a_i, b_i \in \{0, 1\} \\ P(a_i = 0) = .5 \\ P(b_i = 0) = .5 \end{matrix} \quad (17)$$

The bit a_i chooses one of the conjugate bases and the bit b_i chooses one of the two states that form that basis to encode $|\phi_i\rangle$. Importantly, the qubit $|\phi_i\rangle$ is prepared with two classical bits of information, but it can reveal at most one bit of information when measured due to the Heisenberg uncertainty principal. This asymmetry acts as the fundamental mechanism that secures the protocol. Bob then generates a random bit string $a'_i \in \{0, 1\}$ to select the basis he will use to measure $|\phi_i\rangle$. Alice then sends

$|\phi_i\rangle$ to Bob over an insecure quantum channel. Bob then records the state of $|\phi_i\rangle$ in the bit b'_i after measuring it with the basis selected by the bit a'_i .

$$b'_i = \begin{cases} b_i & \text{if } a'_i = a_i \\ \text{random in } \{0, 1\} & \text{if } a'_i \neq a_i \end{cases} \quad P(b'_i = b_i) = \begin{cases} 1 & \text{if } a_i = a'_i \\ \frac{1}{2} & \text{if } a_i \neq a'_i \end{cases} \quad (18)$$

Assuming no eavesdropping occurred during Alice's transmission, when Bob chooses to measure $|\phi_i\rangle$ with the same basis as Alice, then the qubit is prepared in one of Bob's two basis states. So it will deterministically collapse into the same state that Alice encoded it with. When Bob chooses to measure $|\phi_i\rangle$ with a different conjugate basis than Alice, then the qubit is prepared in equal superposition of Bob's measurement basis states:⁷ Hence, by the Born rule⁸, when Bob measures $|\phi_i\rangle$ it has an equal probability of collapsing into $|0\rangle$ or $|1\rangle$ since the absolute square of the qubits superposition is equal one half.

$$a_i \neq a'_i \implies |\phi_i\rangle \in \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(i|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \right\} \implies$$

$$P(b_i = b'_i) = P(b_i \neq b'_i) = |\langle 0|\phi_i\rangle|^2 = |\langle 0|\phi_i\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \left|\frac{-1}{\sqrt{2}}\right|^2 = \left|\frac{i}{\sqrt{2}}\right|^2 = \frac{1}{2} \quad (19)$$

A subset of the bits in b_i and b'_i will become the proposed secret key. Then over an authenticated classical communication channel Alice and Bob publicly share their encoding bases, a_i , and measuring bases, a'_i . Now Bob knows which of his measured bits, b'_i , should match Alice's encoded b_i bits. Only if an eavesdropper has also measured $|\phi_i\rangle$ with the same encoding basis as Alice, then they have enough information to know b_i . Now Bob chooses a subset $B_p \subset \{b'_i | a_i = a'_i\}$ of his measured b'_i bits where the bases matched. Bob then sends which of the bits he chose to include in B_p to Alice over the classical communication channel. Alice then responds with which bits matched hers. Every bit should match unless an eavesdropper has also measured $|\phi_i\rangle$ with a different sending basis than Alice. If that has happened, the qubit $|\phi_i\rangle$ will collapse into a state consistent with the eavesdropper's measurement basis. When Bob then measures $|\phi_i\rangle$ with the same basis as Alice after the eavesdropper, it will no longer collapse into b_i deterministically - introducing mismatches between b_i and b'_i . So if there are more mismatches beyond a specified error rate, it implies the presence of an eavesdropper, and Alice and Bob should abort the protocol and try again to establish a secret key. Otherwise, Alice and Bob discard the bits in b_i that were publicly shared and didn't share the same measuring and encoding basis to establish their secret key. A successful example of the BB84 protocol is demonstrated with table 1.

3.1.2 BB84 Security. The BB84 protocol derives its security from the foundational principles of quantum mechanics, ensuring that any attempt at eavesdropping introduces detectable anomalies in the communication.

Suppose an eavesdropper Eve intercepts each qubit $|\phi_i\rangle$ as it travels from Alice to Bob. Since Eve has no knowledge of Alice's chosen basis a_i before measurement, her optimal strategy is to measure each qubit in one of the two conjugate bases at random, each with probability $1/2$. When Eve measures $|\phi_i\rangle$ with the same basis as Alice, the qubit is prepared in one of Eve's basis states. So it will deterministically collapse into the same state before measurement. So, when Bob then measures $|\phi_i\rangle$ after Eve, he will compute the same measurement as if there were no eavesdropper. Alternatively, when Eve measures $|\phi_i\rangle$ with a the conjugate of Alice's encoding basis, then by definition the qubit is prepared in an equal superposition of Eve's basis states. Hence, there is an equal probability, when measured, the qubit collapses into one of Eve's basis states. So, when Bob then measures $|\phi_i\rangle$ after Eve, his measurement may be different than if there were no eavesdropper. If Bob uses the same encoding basis as Alice, then Eve has prepared the qubit in an equal superposition in Bob's basis states since Eve is using the conjugate of Alice and Bob's basis. Hence, there is an equal probability that the qubit collapses into one of Bob's basis states when measured by Bob. And even though Bob used the same encoding basis as Alice, there is a $1/2$ probability that Bob's computed bit b'_i doesn't match Alice's chosen bit b^i . If Bob uses the same basis as Eve that is conjugate to Alice's encoding basis, then the measured qubit will be the same as Eve prepared it and the computed bit b'_i will still only have a probability of $1/2$ to match b_i . Therefore, when Bob chooses the same basis as Alice, and Eve chooses the conjugate basis, there is a $1/2$ probability that the bits measured by Bob b'_i mismatch the bits chosen by Alice b_i .

⁷Here, $|0\rangle$ and $|1\rangle$ denote the basis states of the basis Bob chooses.

⁸See section 1.2.3 for a further discussion of the Born rule

QUANTUM TRANSMISSION	1	2	3	4	5	6	7	8	9	10	11
Alice's random bits, b_i	0	1	1	0	1	0	0	1	0	1	1
Random sending bases, a_i	$\otimes$	$\leftrightarrow$	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$	$\otimes$	$\leftrightarrow$
Photons Alice sends, $ \phi_i\rangle$	$\nearrow$	$\uparrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\leftrightarrow$	$\nearrow$	$\nwarrow$	$\leftrightarrow$	$\nwarrow$	$\uparrow$
Bob's random receiving bases, a'_i	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$
Bits as received by Bob, b'_i	1	0	1	0	1	0	0	1	0	1	1
PUBLIC DISCUSSION											
Bob reports bases	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$
Alice says which bases match			OK	OK		OK	OK			OK	OK
Presumed shared bits			1	0		0	0			1	1
Bob reveals some bits, B_p				0			0				
Alice confirms				OK			OK				
OUTCOME: shared secret key			1			0				1	1

Table 1. BB84 Protocol Step-by-Step Example

$$P(b'_i \neq b_i \mid a'_i = a_i \text{ and there's eavesdropping}) = P(a_i^{\text{Eve}} = a_i) \cdot 0 + P(a_i^{\text{Eve}} \neq a_i) \cdot \frac{1}{2} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \quad (20)$$

To detect eavesdropping, Bob will select a subset of the measured b'_i bits, where Alice and Bob's bases matched, and share them with Alice to confirm how many of them match Alice's chosen b_i bits. Let X be the number of mismatches in the M test bits. If Eve is eavesdropping, then $X \sim \text{Binomial}(M, p = \frac{1}{4})$. And if Alice and Bob specify there can be at most m mismatches before they abort the protocol, then the probability that they detect Eve is given as:

$$P(\text{detection}) = P(X > m) = 1 - \sum_{k=0}^m \binom{M}{k} \left(\frac{1}{4}\right)^k \left(\frac{3}{4}\right)^{M-k} \quad (21)$$

For example, if Alice and Bob want to catch Eve 95% of the time and they plan to use 64 bits for testing, then they should have at most 9 bits can mismatch before Alice and Bob should abort the protocol. You may question: why not allow even one bit to mismatch? If that were the case then Eve can abort our transmission by intercepting on average 4 test bit transmissions. Therefore, we set a higher bar for Eve forcing here to expend the resources to intercept on average $4 \cdot 9 = 36$ test bits. And if our total transmission includes another 4096 bits for the key, then she has no idea which bits will be used for testing eavesdropping. So

3.2 Quantum Coin Flipping (QCF)

The goal of coin flipping is to establish a random outcome between two parties without either having control of it. Both participants help generate the outcome, and if any attempt is made to influence the result it should be detected and nullified. Manuel Blum complicated the problem of generating shared randomness when he introduced "Coin Flipping by Telephone", in his 1983 paper [3]. Now both parties distrust each other, are separated by a distance, and only communicate via telephone. A commonly cited example of this is problem is a divorced couple deciding on who keeps the dog randomly with equal odds. Each loves the dog and will do anything to influence the outcome. Many classical approaches have been developed to address this problem, but they all rely on assumptions of computational difficulty. So they are all vulnerable to algorithmic and technological advancements.

3.2.1 The Quantum Coin Flipping Protocol. The quantum coin flipping protocol was also developed by Bennett et al. in the same paper as the BB84 protocol [1], and it has a similar setup. Alice and Bob both want to establish a random bit between

themselves with fair odds without the other having influence on the outcome even if they have infinite computing power. Both a quantum and classical communications channel are established between Alice and Bob.

Alice starts the protocol by choosing an encoding basis, $\{|\psi\rangle, |\psi^\perp\rangle\}$, and a bit string $b_i \in \{0, 1\}$, and she keeps them secret. If Alice is following the rules, then her encoding basis will be either the rectilinear basis or its conjugate the diagonal basis. Bob then chooses a measuring basis, $\{|\varphi_i\rangle, |\varphi_i^\perp\rangle\}$, for each qubit. If Bob is following the rules, each measuring basis should be either rectilinear or diagonal, Alice then prepares N qubits $|\phi_i\rangle$, choosing one of the encoding basis states based on bit b_i , and sends them to Bob.

$$|\phi_i\rangle = \begin{cases} |\psi_a\rangle & \text{if } b_i = 0 \\ |\psi_a^\perp\rangle & \text{if } b_i = 1 \end{cases} \quad (22)$$

Bob then measures each transmitted qubit and records the collapsed state of it in the bit b'_i , and keeps it secret. After measuring all the transmissions, Bob guesses Alice's encoding basis. Bob sends his guess over an authenticated classical communications channel. He has fair odds of guessing the correct base, and his bit string b'_i will prove so. Alice responds with the outcome, either "You Lose" or "You Win". If Alice is following the rules, then she correctly report if Bob guessed her encoding basis. This implies Bob now knows Alice's measuring basis.

$$P(b'_i = 0) = |\langle\varphi_i|\phi_i\rangle|^2 \quad P(b'_i = b_i) = |\langle\varphi_i^\perp|\phi_i\rangle|^2$$

$$\text{Alice and Bob followed the rules} \implies P(b'_i = b_i) = \begin{cases} 1 & \text{if Alice and Bob's bases match} \\ \frac{1}{2} & \text{otherwise} \end{cases}$$

Assuming Alice and Bob are following the rules, when Bob measures the qubit $|\phi_i\rangle$ with the same basis as Alice, then the qubit will deterministically collapse into the basis state it was prepared with, and Bob's computed bit b'_i will match Alice's chosen bit b_i . When Bob measures the qubit $|\phi_i\rangle$ with the conjugate of Alice's encoding basis, then the qubit will be in an equal superposition of Bob's measuring basis states. Hence there is an equal probability that Bob's computed bit b'_i will match Alice's chosen bit b_i or not. If there is cheating, then it will be revealed after Alice's chosen bits b_i are compared to Bob's bits b'_i and Alice's supposed encoding basis is compared to Bob's measuring bases.

Alice continues the protocol by publishing here bits b_i on the classical communications channel to Bob. Bob compares them to his measured bits b'_i , and using his knowledge of Alice's implied measuring basis he determines if Alice followed or broke the rules. If he suspects foul play, then he will publish his bits b'_i and label their measuring bases as either rectilinear or diagonal. If Alice suspects foul play by Bob, then she will request Bob to publish his bits b'_i and label their measuring bases as either rectilinear or diagonal. Both parties now have all the information they need to prove that the other cheated. If no proof is found, then the outcome determined by Alice is valid, otherwise its nullified and the protocol starts again. To see a step by step example of the quantum bit flipping protocol see table 2.

3.2.2 Quantum Coin Flipping Security. For Bob to cheat, he would have to guess Alice's encoding basis with a probability greater than 50%. Alice knows her encoding basis and will not be swayed Bob's reported bits, so guessing her encoding basis is Bob's only opportunity to cheat. If Alice chooses a random bit string, then no measuring apparatus can discern the base of a random stream of photons. It would have to break the Einstein-Podolsky-Rosen effect because it would discern useful information at a speed faster than the speed of light. Thus violating the laws of physics and eliminating Bob's opportunity to cheat.

Alice's first opportunity to cheat is when she prepares the qubits to transmit to Bob. If she either uses a mixture of rectilinear or diagonal bases or any other basis, then she will not be able to reproduce the section of Bob's bit string that was measured with the basis she claimed to use. Due to the probabilistic nature of measurement unless she used the exact measuring basis as Bob for a subset of transmitted qubits, she will not be able to reproduce the measured results. Alice's second opportunity to cheat is after Bob guesses her encoding basis. If Alice finds that she lost, she could lie and report that she had won. But to prove that, she would need to produce the same sequence of bits that Bob measured with a conjugate basis to hers. Due to the probabilistic nature of measuring in a conjugate basis only half of Bob's bit string measured by that basis would match Alice's original bit string on average. Furthermore, Alice doesn't know which bits Bob measured in her supposed basis (the basis

QUANTUM TRANSMISSION	1	2	3	4	5	6	7	8	9	10	11
Alice's random bits, b_i	0	1	1	0	1	0	0	1	0	1	1
Alice's random sending basis	"Rectilinear"										
Photons Alice sends, $ \phi_i\rangle$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$
Bob's random receiving basis, a'_i	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$	$\otimes$	$\leftrightarrow$	$\otimes$	$\otimes$	$\leftrightarrow$
Bob's rectilinear bits	0		1			0		1			1
Bob's diagonal bits		0		1	0		0		1	1	
PUBLIC DISCUSSION											
Bob's guess	"Diagonal"										
Alice's reply	"You Lose"										
Alice's sends her random bits, b_i , to clarify	0	1	1	0	1	0	0	1	0	1	1
Bob's rectilinear bits	0		1			0		1			1
Bob's diagonal bits		0		1	0		0		1	1	
OUTCOME	"Bob Lost"										

Table 2. Quantum Coin Flipping Protocol Step-by-Step Example

conjugate to what she actually used), so its incredibly unlikely that Alice would be able to produce a bit string that would fool Bob.

3.2.3 Practical Quantum Coin Flipping. In 2011, a new method was theorized[8] that built upon previous iterations. In classical coin flipping, one dishonest player can always force an outcome with probability 1 in an asynchronous model, while in a synchronous model, there is a fundamental limit on fairness. This method has a lower cheating probability than any (asynchronous or synchronous) classical coin flipping method, specifically approaching the proven minimum of $\frac{1}{\sqrt{2}}$. Additionally, this method solved the issue of real-world implementation, accounting for multi-photon pulses and other disturbance while still maintaining that all-important low cheating probability. It does this by implementing an attenuated laser source, which is feasible to currently implement.

The protocol is as follows

- Alice sends quantum states to Bob
 - Alice generates K photon pulses
 - For each pulse $i = 1, 2, \dots, K$, she randomly picks a basis $\alpha_i \in \{0, 1\}$ and a bit $c_i \in \{0, 1\}$
 - Alice prepares a state, defined as follows. Basically, it generates a unique state for any combination of α_i and c_i . The parameter a is optimized for reducing the cheating probability:

$$|\phi_{\alpha_i, c_i}\rangle = \begin{cases} \sqrt{a}|0\rangle + (-1)^{\alpha_i}\sqrt{1-a}|1\rangle, & \text{if } c_i = 0 \\ \sqrt{1-a}|0\rangle - (-1)^{\alpha_i}\sqrt{a}|1\rangle, & \text{if } c_i = 1 \end{cases}$$

- Alice sends the state to Bob
- Bob measures
 - For each received pulse i , Bob chooses $\alpha'_i \in \{0, 1\}$
 - If Bob does not detect a photon in any pulse, he aborts. Otherwise, he records the first successful detection as j
 - For this pulse, he picks $c'_j \in \{0, 1\}$, and sends j and c'_j to Alice
- Alice reveals
 - After receiving j , Alice reveals α_j and c_j
- Bob verifies
 - If the bases match, then Bob checks whether his measurement result matches the expected quantum state
 - If not, he aborts

- Final output
 - The final output of the protocol is $b = c_j + c'_j \pmod 2$

Aborts and Cheating

In certain cases, a player will be forced to abort due to interference. This is known as an "honest abort". This can happen when Bob's detectors never click for a photon pulse, his first detection is due to a dark count, or the noise in the channel alters the state of the photon. In other cases, one player may attempt to cheat. Alice has much control over the system, so it is easier for her. She could send an entangled state, and measure it in a way that allows her to force the outcome of the flip. Her cheating probability is determined by the parameter a in the quantum state equation. For Bob to cheat, he can use his control over measurement. Depending on how many photons are in Alice's pulses, Bob can use this to guess Alice's original bit. If one contains 2 photons, he can guess the bit with probability a . In order to ensure that this protocol is fair, we set a to give an equal cheating probability to both sides. This protocol is not perfectly fair, but adjusting a properly can put upper bounds on the cheating probabilities for both players.

3.2.4 Quantum Coin Flipping Networks. As we move toward large-scale quantum communication, the ability of quantum networks to securely generate randomness is increasingly important. Quantum networks are the backbone of many technologies, such as quantum key distribution. In 2022, Qian explored the scalability of quantum coin flipping in the context of quantum networks, which will allow for secure communication between multiple parties[7]. Specifically, the paper describes three methods for N party quantum coin flipping.

Central Review Protocol The central review protocol is one of three methods proposed, and involves a witness to ensure that the process is fair and verifiable. It is simple as it requires few materials to set up, and an outcome is produced very quickly. However, if the witness is not trusted, or if it does something wrong, then the final result could be invalid.

- Initial state: The coin flips starts with all players sharing an entangled quantum state according to the following formula

$$|\psi_{\text{coin}}\rangle = \sum_{i_1 \dots i_N} c_{i_1 \dots i_N} |i_1 \dots i_N\rangle \otimes |\psi_{\text{witness}}\rangle$$

- Preparation: The Hadamard operation is applied to each player's qubit, putting it into a superpositions of $|0\rangle$ and $|1\rangle$, representing a coin for each player.
- The Coin Flip: Each player measures their qubit in the $\{0, 1\}$ basis, and guarantees an outcome for each player. The witness can track the results by measuring all of the entangled qubits, ensuring fairness. At each flip, the quantum state will evolve.
- After all players have flipped, then a bit can be deduced from the final quantum state

Peer to Peer Review Protocol The peer to peer review protocol is another method proposed, but does not involve a witness. Instead, all participants review each others results. It is, however, complex and slower than the central review protocol.

- Initial state: The game starts with all players sharing an entangled quantum state
- The Coin Flip: Each player flips their coin by measuring their qubit in the $\{0, 1\}$ basis. After each flip, the quantum state evolves, and players can observe their confirmation qubits to see the outcomes of other flips.
- Review: After all flips have been completed, the results are reviewed for each player, by everyone. An agreement ratio is calculated based on how many parties do or don't agree.
- Assuming all ratios are above a threshold, the outcome can be deduced from the final quantum state.

As an extension to this protocol, another method uses a mix of this and the central review protocol. But, in any case, the ability to use quantum coin flipping in situations with more than two players is what will really have an impact on future practices, as we move towards communication through quantum networks.

3.3 Quantum-Secure Zero-Knowledge Proofs (QZP)

A zero-knowledge proof[6] allows a statement to be proven without revealing any additional information. For example, imagine that Alice wants to prove to Bob that she can open a locked door hidden inside a cave. The cave forms a loop, and the door connects its left and right paths, out of Bob's view. Alice enters from one side without Bob seeing. Then, Bob randomly asks her to exit from the left or the right. If Alice is always able to exit from the correct side, Bob can be convinced that she knows

how to open the door without seeing her do it. ZKPs have applications in preserving privacy on the blockchain, digital identity verification, and secure voting protocols.

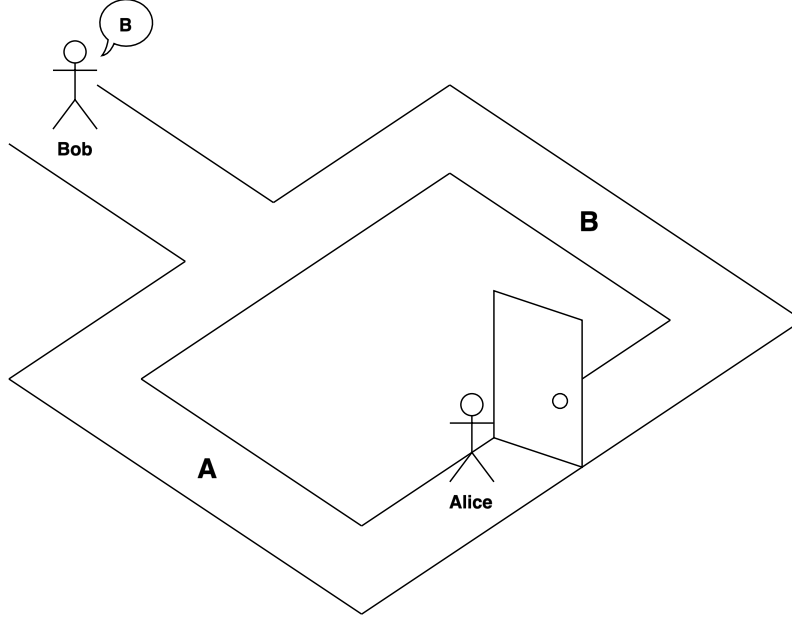


Figure 1. Visualization of the Cave example

Specifically, a zero-knowledge proof must satisfy three properties:

1. **Completeness:** If the statement is true, an honest verifier should be convinced by an honest prover
2. **Soundness:** If the statement is false, no dishonest prover should convince an honest verifier that the statement is true
3. **Zero-Knowledge:** The verifier learns nothing other than the validity of the statement. Formally, secrecy is proven by showing every verifier has some simulator that, given said statement, can produce a transcript that looks like an interaction between an honest prover and said verifier.

3.3.1 Zero Knowledge Proof of a Discrete Log. Let p be a large prime, g a generator for multiplicative group $\mathbb{G}$ of order p . Alice wants to prove to Bob that she knows a secret key $x \in \mathbb{Z}_p$ such that $y = g^x \mod p$. We use the Schnorr protocol, an interactive protocol that proves knowledge of the discrete logarithm of y with respect to g . The protocol is as follows:

1. Alice selects a random number $r \in \mathbb{Z}_p$ and computes $t = g^r \mod p$, then sends t to Bob.
2. Bob selects a random challenge $c \in \mathbb{Z}_p$ and sends c to Alice.
3. Alice then computes $s = r + c \cdot x \mod p$ and sends s to Bob.
4. Bob checks $g^s \stackrel{?}{=} t \cdot y^c \mod p$

Revisiting the three properties:

1. If Alice and Bob follow the protocol honestly, Bob will always accept a valid proof.
2. If Alice can correctly provide two correct s for two different challenges c under the same t , x will be leaked
 - We now have $g^s = t \cdot y^c$ and $g^{s'} = t \cdot y^{c'}$, so

$$\frac{g^s}{g^{s'}} = \frac{t \cdot y^c}{t \cdot y^{c'}} = \frac{y^c}{y^{c'}} = y^{c-c'}$$

then

$$g^{s-s'} = y^{c-c'} = (g^x)^{c-c'} = g^{x(c-c')}$$

so

$$s - s' \equiv x(c - c') \mod p$$

then

$$x = (s - s') \cdot (c - c')^{-1} \bmod p$$

Thus, any prover with the ability to consistently producing valid s knows x with a high probability.

3. A simulator will produce valid t without knowing x , given Bob chooses c honestly.

- Let's fake a transcript (t, c, s) that passes verification (step 4).
- Choose some c , pick a random $s \in \mathbb{Z}_p$
- Now, we solve for t .

$$t = g^s \cdot (y^c)^{-1} \bmod p$$

- We now have a valid (t, c, s) without knowing x , and thus zero-knowledge holds.

This zero-knowledge proof is used to create digital signatures known as Schnorr signatures. These signatures are used to validate ownership of assets and authenticate transactions in bitcoin.

3.3.2 Using The Quantum Coin Flip. In the Schnorr protocol, the soundness and zero-knowledge properties rely on the verifier choosing a truly random challenge c , it's possible to break zero knowledge by selectively choosing c . For instance, a malicious verifier sets $c = 1$ if the last bit of t is 1, and $c = 0$ if the last bit of t is 0. Since c now depends on t , the simulator cannot derive t from c , thus breaking zero-knowledge.⁹ To address this issue, we may replace the verifier's choice in c with a jointly generated challenge protocol, based on our quantum coin flipping primitive shown in 3.2.3. This ensures neither party can unfairly influence c . The modified protocol is as follows:

1. Alice selects a random number $r \in \mathbb{Z}_p$ and computes $t = g^r \bmod p$, then sends t to Bob.
2. Alice and Bob engage in the **coin flip protocol** k times to generate k random bits
3. Let $c = \text{coin}_1 \cdots \text{coin}_k \bmod p$ be the resulting challenge in binary.
4. Alice then computes $s = r + c \cdot x \bmod p$ and sends s to Bob.
5. Bob checks $g^s \stackrel{?}{=} t \cdot y^c \bmod p$

Using the quantum coin flip ensures that c is unpredictable for both the prover and verifier. Since c is generated jointly, there is no need to trust the verifier nor rely on a third party for a pre-generated challenge. The result is a quantum-secure¹⁰ zero-knowledge proof.

4 Quantum Attacks on Classical Cryptography

Classical cryptographic schemes like RSA and Diffie–Hellman rely on the assumed computational hardness of problems such as integer factorization and discrete logarithms. However, these assumptions lacked formal proof of intractability. Peter Shor broke these assumptions by introducing a quantum algorithm that can solve both problems efficiently. Known as Shor's algorithm, it demonstrated that a quantum computer could factor large integers and compute discrete logarithms in polynomial time, effectively breaking the security guarantees of widely used public-key systems [11]. Shor's algorithm accomplishes this by solving a related problem to prime factorization and discrete logarithms and then using its solution to tackle them.

4.1 Prime Factorization

The security of the RSA cryptosystem is based on the difficulty of factoring integers into their prime components. Classical algorithms for this task, such as the General Number Field Sieve, run in sub-exponential time but are still computationally infeasible for sufficiently large key sizes. However, Shor's algorithm enables efficient prime factorization on a quantum computer, reducing the complexity to polynomial time.

Shor's algorithm works by reducing the problem of factoring an integer $n = p \cdot q$ to finding the order of an element x in the multiplicative group $(\bmod n)$, denoted $\mathbb{Z}/n^\times$. The order of an integer x $\bmod n$ is the smallest positive integer r such that $x^r \equiv 1 \pmod n$. Once the order of x , r , is found by Shor's algorithm, we can attempt to factor n . The only criterion for r is that it must be even and $x^{r/2} \not\equiv \pm 1 \pmod n$. If Shor's algorithm has computed r and it fits those criteria, then to factor n we first let $y = x^{r/2}$:

⁹While it feels unsatisfying that breaking zero-knowledge in this way does not explicitly leak x , the simulator is the **only** thing to **guarantee** no info leaks.

¹⁰Note that a quantum secure group is required, else Shor's algorithm (discussed in the next section) makes Schnorr's protocol pointless

$$y^2 \equiv 1 \pmod{n} \implies y^2 - 1 \equiv 0 \pmod{n} \implies (y-1)(y+1) \equiv 0 \pmod{n} \quad (23)$$

Hence, the factorization of $y^2 - 1$ as $(y-1)(y+1)$ is divisible by n . Implying that $(y-1)(y+1)$ is also divisible by the prime factors of n , p and q . To prove that p and q divide at least one factor of $(y-1)(y+1)$, suppose that p doesn't divide either $(y-1)$ or $(y+1)$. This implies that p doesn't divide $(y-1)(y+1)$ contradicting our earlier statement that it does. Thus p must divide at least one of the factors of $(y-1)(y+1)$. The same argument can be used for q , so it also divides at least one of the factors of $(y-1)(y+1)$. To prove p and q don't divide the same factor, let's assume p and q both divide $(y-1)$ then:

$$\begin{aligned} p \mid (y-1) \text{ and } q \mid (y-1) &\implies pq \mid (y-1) \implies y-1 \equiv 0 \pmod{n=p \cdot q} \implies \\ y &\equiv 1 \pmod{n} \implies x^{r/2} \equiv 1 \pmod{n} \end{aligned} \quad (24)$$

Our assumption implies that $p \cdot q$ divides $(y-1)$ and $x^{r/2} \equiv 1 \pmod{n}$ contradicting our criterion for r that $x^{r/2} \not\equiv \pm 1 \pmod{n}$. Thus, p and q cannot both divide the factor $(y-1)$. The same argument can be made for the factor $(y+1)$. Therefore, one of the primes must divide $(y-1)$ and the other prime must divide $(y+1)$.

Let's say p divides $y-1$ and q doesn't. Because p divides $(y-1)$ and n it also divides $\gcd(y-1, n)$. The value $\gcd(y-1, n)$ cannot be n since q doesn't divide $y-1$ and it also cannot be 1 because p divides both terms, $y-1$ and n . Hence, $p = \gcd(y-1, n)$. The same argument can be made for the other factor $y+1$, therefore:

$$\begin{cases} p = \gcd(y-1, n) \\ q = \gcd(y+1, n) \end{cases} \quad (25)$$

And, we have found the prime factors of n given the order of x and the prior criterion holds. If x is chosen to be a primitive root $\pmod{n}$, then r is guaranteed to be even. Furthermore, there is a 3/4 chance¹¹ that the criterion $x^{r/2} \not\equiv \pm 1 \pmod{n}$ is met. So once r is found by Shor's algorithm, there is a good chance you will also be able to find the prime factors of n and break the classical cryptographic scheme's that rely on prime factorization for security. A downside quantum cryptography doesn't face.

4.2 Shor's Algorithm

The goal of Shor's algorithm is to find the order of x in the multiplicative group $\pmod{n}$. The algorithm accomplishes this by finding the period of the powers of $x \pmod{n}$. Let's define the powers of x as the function $f(a) = x^a \pmod{n}$. Then the period, b , is the smallest positive integer such that, $f(a+b) = f(a)$. Notice:

$$x^r \equiv 1 \pmod{n} \implies f(a+r) = x^{a+r} = x^a \cdot x^r = x^a \cdot 1 = f(a) \pmod{n} \quad (26)$$

Thus, the powers of x are periodic and the period is the order of $x \pmod{n}$ which is r . Shor's algorithm is designed to find this hidden period, r , efficiently by exploiting the Quantum Fourier Transform.

Shor's algorithm starts by preparing the first quantum register, $|\psi_0\rangle$, to hold all integers $a \in \{0, 1, \dots, 2^t - 1\}$, the exponents of x , in an uniform superposition with t -qubits. The second quantum register, $|\psi_1\rangle$, is prepared to hold all powers of x , $f(a) = x^a \pmod{n}$, in an uniform superposition across t -qubits. The first register is prepared by applying t Hadamard gates to the initial qubit state $|0\rangle^{\otimes t} = |00\dots 0\rangle$. The second register is prepared by applying a modular exponentiation circuit to the first register. That circuit maps the state $|a\rangle \otimes |0\rangle$ to $|a\rangle \otimes |x^a \pmod{n}\rangle$.

$$|\psi_0\rangle = \frac{1}{\sqrt{2^t}} \sum_{a=0}^{2^t-1} |a\rangle \otimes |0\rangle \quad |\psi_1\rangle = \frac{1}{\sqrt{2^t}} \sum_{a=0}^{2^t-1} |a\rangle \otimes |x^a \pmod{n}\rangle \quad (27)$$

¹²

After preparing the second register, it is entangled with the first register. The entangled state of the entire quantum system contains all input-output pairs of the modular exponentiation of x , $a \mapsto f(a) = x^a \pmod{n}$. We will then measure the second

¹¹this is derived from the proof in Shor's 1994 paper [10]

¹²The state $|a\rangle$ is equivalent the binary encoding of a . For example, $|13\rangle$ maps to $|1101\rangle$.

register, and it will collapse to an output value $y = x^k \bmod n$. Because the input of this function, in the first register, is entangled to the output of this function, in the second register, the first register also collapses to a superposition of all values of a that map to y ; hence a satisfies $y = x^a \bmod n$. The resulting values of a left in the first register's superposition are spaced apart by r , the period of the modular powers of x . We can't directly measure these values without collapsing the state, but we can measure the period of these values with the Quantum Fourier Transform. Applying the Quantum Fourier Transform to the first register transforms the superposition over evenly spaced values into a superposition over frequency components, where the amplitudes are concentrated around integer multiples of $2^t/r$. The state becomes:

$$|\psi_q\rangle = \sum_{c=0}^{2^t-1} \alpha_c |c\rangle \quad (28)$$

After the first register is transformed by the Quantum Fourier Transform, we measure it. The outcome is a value c such that $\frac{c}{2^t} \approx \frac{s}{r}$ for some integers s and r . And there is a high probability that r is the period we have been looking for and s is co-prime to r . Thus we can use the continued fractions algorithm to recover r from the real number $\frac{c}{2^t}$. Once we have done so, we check whether r satisfies the congruence $x^r \equiv 1 \pmod{n}$. And if it does, then we have found the order of $x \pmod{n}$, and we can use that to solve a prime factorization or discrete log problem to break classical cryptographic schemes like RSA or Diffie-Hellman.

5 Conclusion

Quantum cryptography offers multiple advances over classical methods. Transmitting data over systems that leverage this technology will provide security against eavesdroppers, true randomness, and a reduced chance of any party cheating. One example of this is the quantum coin flip. It could replace its classical counterpart and improve it on all facets. Quantum techniques can also help us work with public keys. Quantum Key Distribution, such as the BB84 Protocol, allows two parties to generate a shared secret key with more security than traditional systems, which rely on a Certificate Authority. Other uses of quantum technology could break our current systems by factoring large prime numbers. Encryption algorithms like Diffie-Hellman, which rely on the difficulty of this task, may be broken and useless in the future. Still, lots of work remains to be done to ensure quantum technology can overcome the challenges posed by implementing it in the real world. As it is very susceptible to interference, many theoretical proposals have fallen flat when used in the real world. As these problems are solved and more applications of quantum cryptography are found, the technology promises to change the landscape of modern crypto.

6 Appendix

6.1 Einstein-Podolsky-Rosen Effect

Theorized by Albert Einstein, Boris Podolsky, and Nathan Rosen, is the notion that quantum mechanics does not yield a complete theory of physics[5]. The premise of this effect lays in the existence of two particles. Let there exist particle A and particle B . Now let us imagine we allow these particles to interact and observe that A moves away from the position of B . We now observe the momentum of A . Quantum theory stipulates that we are unable to measure such a characteristic of a particle without its observation, however, in this instance, that we know B has the same quality as a result of the interaction. Thus, we know the momentum of B without having measured it. As a result, quantum mechanics cannot perfectly encapsulate the laws of physics and is thus incomplete. This notion is also referred to as the Einstein-Podolsky-Rosen paradox.

References

- [1] Charles H. Bennett and Gilles Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (Dec. 2014), 7–11. <https://doi.org/10.1016/j.tcs.2014.05.025>
- [2] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. 1982. Quantum Cryptography, or Unforgeable Subway Tokens. In *Advances in Cryptography: Proceedings of CRYPTO '82*. Plenum Press. To appear.
- [3] Manuel Blum. 1983. Coin Flipping by Telephone—A Protocol for Solving Impossible Problems. *SIGACT News* 15, 1 (1983), 23–27.
- [4] Nilanjana Datta. 2019. *Quantum Information & Computation*. DAMTP, University of Cambridge, Cambridge.
- [5] Arthur Fine. 2020. The Einstein-Podolsky-Rosen Argument in Quantum Theory. In *The Stanford Encyclopedia of Philosophy* (Summer 2020 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.
- [6] S Goldwasser, S Micali, and C Rackoff. 1985. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing* (Providence, Rhode Island, USA) (STOC '85). Association for Computing Machinery, New York, NY, USA, 291–304. <https://doi.org/10.1145/22145.22178>
- [7] Kazuki Ikeda and Adam Lowe. 2023. Quantum protocol for decision making and verifying truthfulness among N-quantum parties: Solution and extension of the quantum coin flipping game. *IET Quantum Communication* 4, 4 (Aug. 2023), 218–227. <https://doi.org/10.1049/qtc2.12066>
- [8] Anna Pappa, André Chailloux, Eleni Diamanti, and Iordanis Kerenidis. 2011. Practical quantum coin flipping. *Phys. Rev. A* 84 (Nov 2011), 052305. Issue 5. <https://doi.org/10.1103/PhysRevA.84.052305>
- [9] Steven Roman. 1992. *Advanced Linear Algebra*. Springer.
- [10] Peter W. Shor. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 124–134.
- [11] Peter W. Shor. 1999. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Rev.* 41, 2 (1999), 303–332.
- [12] Stephen W. Wiesner. 1983. Conjugate Coding. *SIGACT News* 15, 1 (1983), 78–88. Originally a manuscript from circa 1970.