An Elementary Introduction to Quantum Cryptography

Abhiram Cherukupalli
(Dated: July 31, 2022)

Quantum cryptography is one of the most researched fields of Information Theory. New theoretical cryptographic protocols are constantly being developed and realised experimentally. Fundamentally these cryptographic protocols are rendered secure by the laws of quantum mechanics. In this review, we introduce the concepts of quantum mechanics, the idea of measurement collapse, the uncertainty principle and some insightful solutions of the Schrödinger Equation. Then, we discuss the EPR paradox, Bell's Theorem leading up to Entanglement and Quantum Cryptography. Next, we examine the Standard Classifications of cryptographic Protocols, the no-cloning theorem, basic protocols like the BB-84 protocol and other similar protocols like bit commitment and entanglement based protocols. Finally, we review their experimental realisations and a few protocols beyond standard key distribution.

CONTENTS

I. QUANTUM MECHANICS BACKGROUND:

A. The Wave Function:

In classical mechanics we can predict the position $x(t)$ and momentum $p(x,t)$ of a particle as a function of time(t) when given the initial conditions and the forces acting on the particle [1]. However, in quantum mechanics that is not the case. Rather we attempt to find the wave function $\psi(x,t)$ of the particle.

To calculate this wave function we need to solve the Schrödinger equation:

$$i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi}{\partial x^2} + V\Psi \tag{1}$$

This seemingly arbitrary function has an important physical significance, given by Born's statistical interpretation: $\int_a^b |\Psi(x,t)|^2 dx$ signifies the probability of finding a particle between a and b at a time t given its wave function

This means that quantum mechanics is indeterminate, that is, you cannot predict the outcome of any experiment, but you can gain statistical information about all the possible outcomes. However, we can say with certainty that the particle has to be somewhere in space and time. Therefore, we can normalise the wave function (provided it is square integrable).

$$\int_{-\infty}^{\infty} |\Psi(x,t)|^2 dx = 1 \tag{2}$$

This is useful for determining the magnitude of the complex multiplicative factor A (note that we cannot determine the phase of A by normalisation), as if $\psi(x,t)$ is a solution to (1), so is $A\cdot\psi(x,t)$.

$$\begin{aligned} f:[a,b]\to\mathbb{C} \text{ square integrable on } [a,b] \\ \iff \quad \int_a^b |f(x)|^2, \mathrm{d}x < \infty \end{aligned} \tag{3}$$

An important consequence of the Schrödinger equation is that if a wave function is normalized at any time, the normalization remains preserved [1]. If the normalization hadn't been preserved, then all wave functions would become non-normalizable (not physical states) and the whole theory would collapse as the Born's interpretation would be deemed incompatible with the Schrödinger's equation.

B. What happens when you make a measurement?

Let us assume an arbitrary wave function of a particle (Figure 1), with probabilities of being at different points.

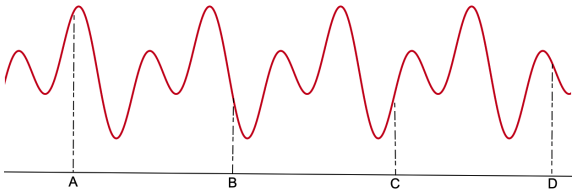


FIG. 1: An arbitrary wave function with different probabilities of finding the particle at different points

FIG. 2: The collapse of the wave function into a delta function when the particle was found at B

The figure in 2 represents the Dirac delta function

$$\delta(x) = \begin{cases} +\infty, & x = 0 \\ 0, & x \neq 0 \end{cases} \text{ Where: } \int_{-\infty}^{\infty} \delta(x)\,dx = 1. \tag{4}$$

After the measurement, the wave function instantly spreads out, while obeying the Schrödinger equation but with different initial conditions, so the wave function gets modified.

Now, the question arises, when we measured the particle to be at B at some time t_0 where is B *just before* the measurement?

There are three different positions scientists take on this question:

1. The realist position: The realist believes that the particle was at C and quantum mechanics could not predict it, making it an "incomplete theory" that needs a hidden variable along with the wave function for it to be rendered complete. They believed that nothing is indeterminate, and that indeterminacy is just a reflection of our ignorance.

2. The orthodox position: The particle was not anywhere. You only know where the particle is when you make a measurement, otherwise, its position is indeterminate, and it can be anywhere. We compel the particle to attain a definite position by measuring it.

3. The agnostic position: The agonist believes that the in-determinacy problem is indeterminable. Because you must make a measurement to know the state of a system, you cannot know the state of a system between measurements.

Interestingly Albert Einstein was a realist, as he believed quantum mechanics defied causality.

All these positions were popular among scientists until the Bell's theorem was postulated (Sec I.G).

This "indeterminacy" of Quantum mechanics leads to a fundamental quantum mechanical principle.

C. Heisenberg Uncertainty Principle:

There is a famous example to explain the Uncertainty Principle: suppose you have a rope which is tied to a wall on one end and is held by you on the other end. The rope is the "medium" in which the wave travels in. Now if you periodically move the string up and down and generate a wave (Figure 3). We can find the wavelength of this wave, but if you ask me the position of the wave, it would not be defined as the wave is "everywhere" so there is no clearly defined position unlike the wavelength.

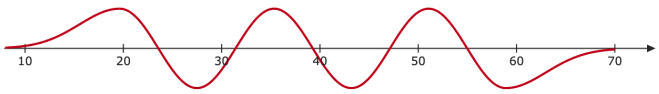


FIG. 3: Wave having a well-defined wavelength but an unclear position

Now what if I produce a wave with a jerk, it is possible to find the position of the wave as the wave is not periodic, so we cannot determine its wavelength.

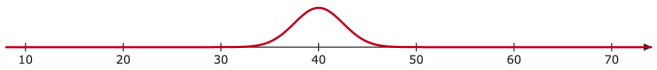


FIG. 4: Wave having a well-defined position but an unclear Wavelength

There seems to be a *trade-off* between the precision of wavelength and position: The more precise a wave's position the less precise its wavelength and vice versa.

We can relate the wavelength λ of the particles wavefunction ψ with the particle's momentum operator $\hat{p}$ ($\hat{p}\ \Psi(x,t) = \frac{h}{i}\frac{\delta}{\delta x}\Psi(x,t)$) using the de-Broglie's formula:

$$p = \frac{h}{\lambda} = \frac{2\pi\hbar}{\lambda} \tag{5}$$

So, if the wavelength of the particle is less precise, its momentum is also less precise and its position is more precise. Mathematically the Heisenberg Principle is given by:

$$\Delta x * \Delta p \geq \frac{\hbar}{2} \tag{6}$$

Here, Δx and Δp represent the uncertainties in position ad momentum respectively. The Heisenberg Principle represents a trade-off between precision of the measurement of position and momentum.

D. Time-invariant Schrödinger's Equation

When we come to solve the Schrödinger's Equation, for simplicity we try to find separable solutions for the wave function. Separable wave functions are simple products:

$$\Psi(x,t) = \psi(x) * f(t) \tag{7}$$

Where ψ does not depend on t and f does not depend on x. Such separable solutions are important, because as we will see soon when we combine separable solutions we can obtain a general solution. If we assume the wave function is separable then we can simplify the Schrödinger equation to obtain:

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V\psi = E\psi \tag{8}$$

(8) is known as the time invariant Schrödinger Equation (V is assumed to be independent of time).

The wave function that is obtained from this Equation is:

$$\Psi(x,t) = \psi(x) * e^{\frac{-iEt}{\hbar}} \tag{9}$$

Notation: ψ is only a function of x whereas Ψ is a function of both x and t.

The separable wave function in (9) is important because of 3 reasons:

1. **They have a definite total energy**: The Hamiltonian in classical mechanics is the sum of kinetic and potential energies of the system:

$$H(x,p) = \frac{p^2}{2m} + V(x) \tag{10}$$

By substituting p as $\frac{h}{i}\frac{\delta}{\delta x}$ in (15a) we get the Hamiltonian operator to be:

$$\hat{H} = -\frac{\hbar^2}{2m} * \frac{\delta^2}{\delta x^2} + V(x) \tag{11}$$

So the Schrödinger equation can be written as:

$$\hat{H}\psi = E\psi \tag{12}$$

Hence for any separable solution, the value of the total energy must always return the value E [1].

2. The general solution to the Schrödinger Equation (1) is a **linear combination of separable solutions**.

$$\Psi_1(x,t) = \psi(x) * e^{\frac{-iE_1 t}{\hbar}}, \Psi_2(x,t) = \psi(x) * e^{\frac{-iE_2 t}{\hbar}}, \ldots \tag{13}$$

Each wave function has its own corresponding energy, so there is a different Ψ for each energy level.

$$\Psi(x,t) = \sum_{n=1}^{\infty} c_n \psi_n(x,t) e^{\frac{-iE_n t}{\hbar}} = 1 \tag{14}$$

It happens to be that every general solution to the Schrödinger equation can be expressed as a linear combination of separable wave-functions, all we need to do is adjust the constant c_n.

3. **It renders a stationary problem**: Though the wave function in (9) has a time-dependent factor, the probability function doesn't. This is because $|\Psi(x,t)|^2 = \Psi^*(x,t) \times \Psi(x,t)$, hence the time dependent factor cancels out

$$|\Psi(x,t)|^2 = \Psi^* \times \Psi = \psi(x) e^{\frac{-iEt}{\hbar}} \times \psi^*(x) e^{\frac{+iEt}{\hbar}} = |\psi(x)|^2 \tag{15a}$$

Note that we could cancel out E in (15a) because for normalizable solutions E must be real [1].

E. Particular solutions of the time-independent Schrödinger equation

To better understand the intricacies of the laws of quantum mechanics let us take a look at a few particular solutions of the Schrödinger equation.

1. *The Free Particle*

This a very simple, yet insightful, solution of the Schrödinger equation. Here, V(x)=0 everywhere and as a consequence of Schrödinger equation $E > V_{min}$ for all normalizable solutions. This implies that the free particle, due to the absence of any boundary conditions, can have any positive energy.

Putting this into (8) we get

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} = E\psi \tag{16}$$

The resulting differential equation's solution can be written as:

$$\psi(x) = Ae^{ikx} + Be^{-ikx} \tag{17}$$

With $k = \frac{\sqrt{2mE}}{h}$ (from (16))

$$\Psi(x,t) = \psi(x) * e^{\frac{-iEt}{\hbar}} = Ae^{ik(x - \frac{\hbar k}{2m}t)} + Be^{-ik(x + \frac{\hbar k}{2m}t)} \tag{18}$$

But we know that whenever a continuous function f(x,t) obeys the wave equation (19), it represents a wave

$$\frac{\partial^2 f(x,t)}{\partial x^2} = \frac{1}{c^2}\frac{\partial^2 f(x,t)}{\partial t^2} \tag{19}$$

Where c is the speed of the wave.

Then if at time $t = 0$, the wave was represented by f(x) then at time t_0 the wave is represented by $f(x - vt_0)$ as the x-axis has translated to the right at rate of v m/s.

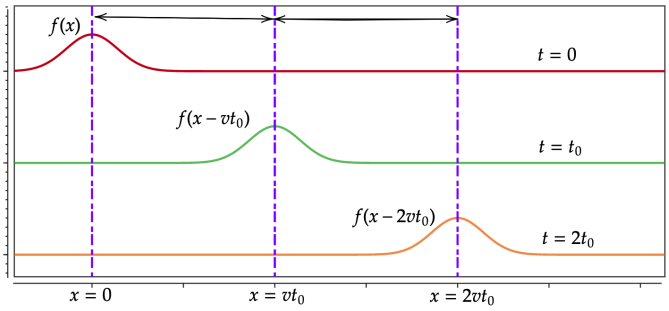


FIG. 5: A wave which is given by f(x) at t=0 is given by $f(x - vt_0)$ at t=t_0

In this case the velocity is $\frac{\hbar k}{2m} = \sqrt{\frac{E}{2m}}$ as $k = \frac{\sqrt{2mE}}{h}$

But if this was a classical particle its energy would be $E = \frac{1}{2}mv^2 \Rightarrow v = \sqrt{\frac{2E}{m}}$

How is this possible for the classical speed to be double that of the quantum mechanical speed? To understand this let us imagine a wave packet in which there is a sinusoidal wave contained. The classical particle velocity represents the velocity of the whole envelope (group velocity) whereas the wave velocity (phase velocity) represents the velocity of the waves contained in it.

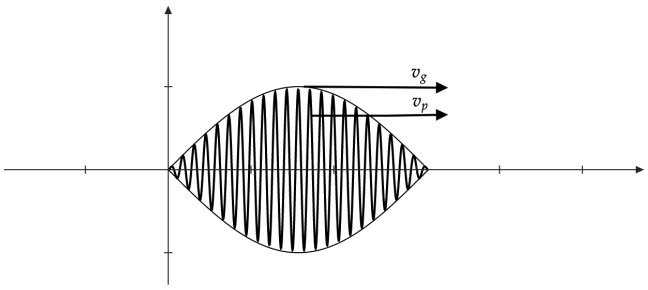


FIG. 6: A wave packet. The envelope moves at the group velocity v_g. Whereas the waves inside it move at the phase velocity v_p

A real life example of the distinction between v_g and v_p is given by waves of water, though the water itself travels in a single direction, say left to right, the particles of water inside it move in elliptical paths, as their motion is a superposition of transverse and longitudinal motions, and the eccentricity depends on the depth of the water.

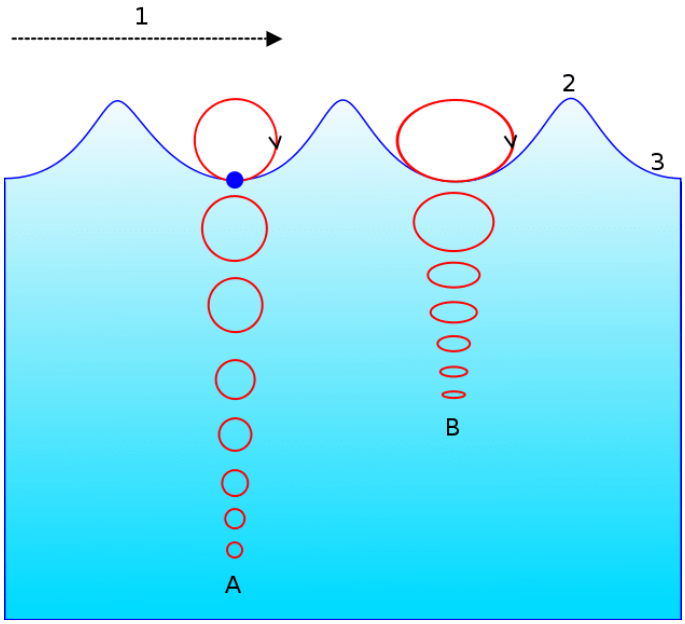


FIG. 7: Motion of a Particle of Water inside a water wave as a superposition of both longitudinal and transverse motions, the particles end up taking elliptical paths (Wikimedia Commons)

If we look closely at the free particle's wave function we notice that it is non-normalizable, implying that it doesn't represent a physical state. Though that's the case, the free-particle example is still one of great importance as it gives us useful insight into quantum mechanics.

2. *The Infinite square well*

Another important case is when $V(x)$ behaves kind of like a delta function, suppose $V(x) = 0$ from $0 \leq x \leq a$ but V(x)=∞ elsewhere. The particle behaves as a free particle from $0 \leq x \leq a$ until it reaches the ends which it cannot cross so it "bounces" back.

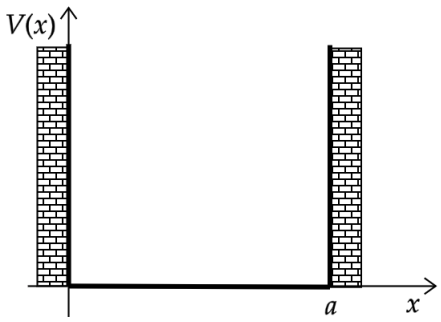


FIG. 8: The infinite square well

If we write (17) in trigonometric form we get:

$$\psi(x) = A\sin kx + B\cos kx \tag{20}$$

$\psi(0) = \psi(a) = 0$ (as ψ when $x < 0$ and $> a$ is 0 and ψ is continuous). So B =0

$$\psi(a) = A\sin ka = 0; k = \frac{\pm n\pi}{a} \tag{21}$$

$$E_n = \frac{\hbar^2 k^2}{2m} = \frac{\hbar^2 n^2 \pi^2}{2ma^2} (\text{from } (16)) \tag{22}$$

Also,

$$\psi_n(x) = \sqrt{\frac{2}{a}} sin(\frac{n\pi}{a}); (A = \sqrt{\frac{2}{a}} \text{ from normalisation}) \tag{23}$$

This means that a particle in the infinite square well can only have a set of allowed values of energy. n=1 has the lowest energy and is called as the ground states all other values of $n > 1$ are called as excited states ($n = 0$ is rejected as you would not be able to normalise the wave function). This example gives us a peek into the core of quantum mechanics: quantization.

Important note: All the wave functions $\psi_n(x)$ are mutually orthogonal:

$$\int (\psi_m(x)^* \psi_n(x)) = 0 \ (m \neq n) \tag{24}$$

If any two wave-functions obey (23) we say they are orthogonal.

3. The Harmonic Oscillator

To further our understanding of quantization let us consider another example of typical harmonic oscillations of a block of mass m attached to a spring of spring constant k.

$$F = -kx = ma = m\frac{d^2x}{dt^2} \tag{25}$$

$$x = Asin(wt) + Bcos(wt);\ w = \sqrt{\frac{k}{m}} \tag{26}$$

$$V(x) = \frac{1}{2}kx^2 \tag{27}$$

We can approximate any oscillation to be a simple harmonic motion (a type of periodic motion where the restoring force is proprtional to displacement and acts towards the mean position), via a parabolic approximation provided the amplitude is small.

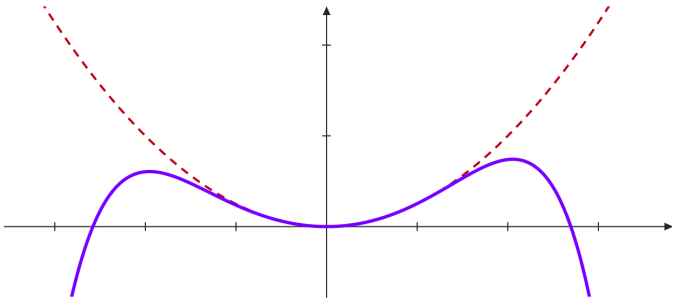


FIG. 9: In the small region around a local minimum we can always assume the graph is parabolic (via the Taylor series expansion of V(x))

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + \frac{1}{2}m\omega^2x^2 = E\psi \tag{28}$$

If we simplify this expression we can use the fact that: $a^2 + b^2 = (a + ib)(a - ib)$

$$\frac{1}{\sqrt{2m}}(\frac{\hbar}{i}\frac{d}{dx} + im\omega x) * \frac{1}{\sqrt{2m}}(\frac{\hbar}{i}\frac{d}{dx} - im\omega x) = E\psi \tag{29}$$

Let us denote the first term as $a_+ = \frac{1}{\sqrt{2m}}(\frac{\hbar}{i}\frac{d}{dx} + im\omega x)$ and $a_- = \frac{1}{\sqrt{2m}}(\frac{\hbar}{i}\frac{d}{dx} - im\omega x)$

These are called the ladder operators because they have a special property: If ψ obeys the Schrödinger's equation, with an energy E, then $a_+\psi$ obeys the Schrödinger's equation with an energy $E + \hbar\omega$ and same applies for a_-. Now we can see why they are called the ladder operators, a_+ allows us to climb the quantized ladder of energy whereas a_- makes us descend it.

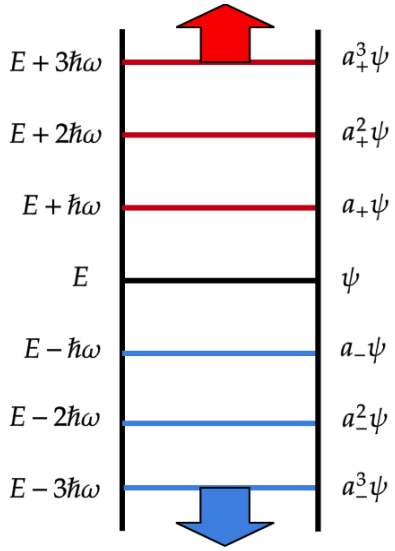


FIG. 10: The ladder operators and the quantized ladder

This is another good example of the Schrödinger which kind of gives an intuitive feel for quantization. Also, it is important to note that quantum mechanics predicts that particles can cross a infinite barrier, quantum tunneling, which has been proven to be the case and is now used in scanning tunneling microscopy [2].

F. The EPR paradox:

Coming back to our discussion of what happens when we take a measurement, Einstein, Podolsky and Rosen believed in the realist interpretation. These three came up with the infamous EPR paradox.

Assume we have a neutral pi meson (of zero spin) which decays to produces a electron-positron pair, $\pi^0 \rightarrow e^- + e^+$. Since spin angular momentum should be conserved, the spin of the electron and positron must be opposite in sign. Therefore, if the spin of the electron is measured as spin up $\uparrow$, the spin of the positron as spin down $\downarrow$ is automatically measured. Quantum mechanics cannot tell you what the spin would be deterministically. All it tells you that no matter how far apart they are their measured spins must be of opposite parity. This implies that as soon as one of the particle's spin is measured, the wave function of the other particle collapses instantaneously. Einstein and other realists felt such "spooky action at a distance" to be impossible, because if the mutual wave function collapse was instantaneous, then the travel speed of the causal influence between them appears to be faster than light. A Paradox!

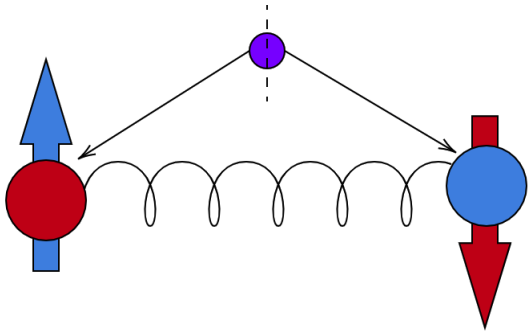


FIG. 11: Two Particles very far away always have the opposite spin, as if there is some sort of spring attached to them

The realists believe that the electron always had spin up since the time it was made and, quantum mechanics being incomplete, was not able to predict the spin as it needed some hidden variable to be complete. They did not believe quantum mechanics to be wrong, they believed it was incomplete.

G. Bell's Theorem:

Different hidden variable theories were put forward forward in the following decades, but none were considered plausible. Considerable theoretical work was put into finding a hidden variable theory, but without success until J.S. Bell came along, who proved that any hidden variable theory is incompatible with quantum mechanics [3]. The idea is as follows: We orient the detectors in a non-parallel direction, allowing them to rotate freely. Let $P(a,b)$ denote the average of the product of the spins measured by the detectors oriented along unit vectors a and b,

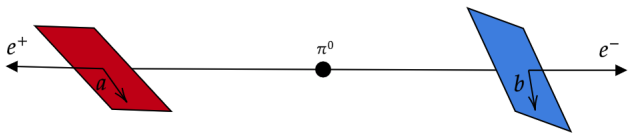


FIG. 12: The Bell configuration non-parallel detectors

If $b = a$, then we get back the original EPR orientation so $P(a,a) = 1$, similarly $P(a,-a) = -1$. Quantum mechanics predicts that for any configuration (a,b)

$$P(a,b) = -a * b \tag{30}$$

If there is a hidden variable needed to describe the complete state of both the particles, then some new functions $A(a,\lambda)$ and $B(b,\lambda)$ give the results of the electron and positron measurement successfully (Here we assume that the electron measurement is independent of orientation of b). We can see that $A(\vec{a},\lambda) = -B(\vec{a},\lambda)$. Also:

$$P(\vec{a},\vec{b}) = \int \rho(\lambda)A(\vec{a},\lambda)B(\vec{b},\lambda)d\lambda = -\int \rho(\lambda A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda \tag{31}$$

If $\vec{c}$ is another unit vector, on simplifying (31) we arrive at:

$$\mid P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) \mid \leq 1 + P(\vec{b},\vec{c}) \tag{32}$$

This can be proven to be inconsistent with quantum mechanics by taking all three vectors in the same plane with **b** and **c** making angle 45° and 90° with **a** respectively. Clearly the inequality in (32) will not hold, implying that there can be no hidden variable theory that can save us from the non-locality of quantum mechanics.

The Bell's inequality was tested in 1970 by Aspect, Grangier and Roger [4] and the results were in agreement with quantum mechanical prediction and was incompatible with the Bell's inequality. This shocked the physics research world as this proves nature being fundamentally non-local. But why is non-locality so disturbing? How can the influence between the electron and positron travel faster than light?

To explain this, we have to make an important distinction: A causal influence cannot travel faster than the speed of light, but other influences, such as instantaneous wave collapse, could. The latter influences carry no energy; hence, they are by no circumstance bound to be traveling slower than light. This is proven by the no-communication theorem, which states that during the measurement of one of the particles, it is not possible for one observer to communicate information to another observer, thereby preserving causality.

II. QUANTUM ENTANGLEMENT

States such as the EPR pair, where there is an inherent dependency of one particles measurement on the other, are called entangled states. Any composite state of two quantum systems A and B can be represented as: $H_A \otimes H_B$ where H_A and H_B are their respective Hilbert Spaces having base states $\{|a_i\rangle \otimes |b_j\rangle\}$, and$\otimes$ represents the tensor product. So,

$$|\psi\rangle = \sum_{i,j} c_{i,j}(|a_i\rangle \otimes |b_j\rangle) = \sum_{i,j} c_{i,j}|a_i b_j\rangle$$

If $|\psi\rangle \in H_1 \otimes H_2$ can be written as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ the state is said to be separable, otherwise it is entangled.

For example, the EPR configuration can be represented as:

$$\tfrac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right)$$

It is impossible to separate this wave function into $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, thus making this configuration entangled. If Observer A measures 0, the state of the system becomes $|0\rangle_A|1\rangle_B$ and vice versa.

III. THE IDEA OF QUANTUM CRYPTOGRAPHY

"No measurement can be made without perturbing the system." This unusual property of quantum mechanics underlies the core concept involved in secure communication channels. If, for example, two people, Alice and Bob, want to communicate with each other quantum information (e.g., photons carrying the information). Eve, an eavesdropper, cannot obtain any information without perturbing the system, thus revealing her presence. Alice and Bob can simply check whether someone is eavesdropping by comparing the data that is passed through the public channel. This would be of no use, though, as they will get to know of eavesdropping after the data transfer takes place. However, when this idea is complemented with a key, it can ensure privacy before any data transfer. A key is a random sequence of bits (qubits), which is sent through the channel. If the key is unperturbed, it means the data channel is secure, so the parties can start sending information encoded in the keys [5, 6].

IV. CRYPTOGRAPHY:

Cryptography is the science of constructing protocols that prevent eavesdroppers from reading private encrypted messages. An algorithm can be used to achieve this, with the help of a key to encrypt the message. For it to be considered secure, it should be impossible to unlock a cryptosystem without its key. Modern cryptosystems can be broadly divided into two categories.

- **Asymmetrical cryptosystems:** Also known as public-key cryptosystems, Alice and Bob use different keys. Bob prepares a public key using a secret private key and Alice uses this public key to encrypt a message which can **only** be decrypted by Bob's private key. A classical version of this protocol is prime factorisation. Given the prime factors of a large number, it is easy to compute the number but it becomes much harder in the other direction (Computing $127 \cdot 71 \cdot 7$ is easy but given 63119 it is much harder to find the prime factors). That is, a type of an one way function. Fortunately, the backward process can be made easier if one of the factors is known, in this case the key. However, prime factorisation isn't "proven" to be secure.

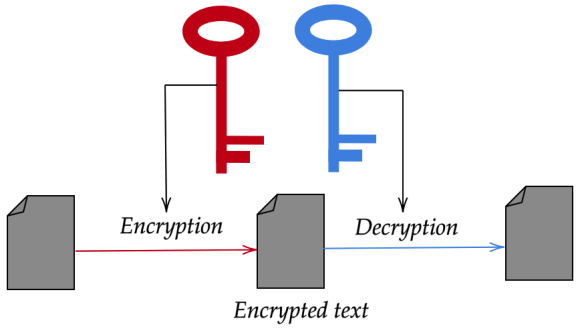


FIG. 13: An Asymmetrical cryptosystem where different keys are used encrypt and decrypt

- **Symmetrical cryptosystems:** Both Alice and Bob use the same private key to encrypt and decrypt the message. Let us assume, Alice adds a key (k) to the message (m) in a binary system ($s = m \otimes k$) now Bob can simply subtract k from Alice's message and decrypt it. This system is provably secure because s is as random as m and hence it doesn't contain any information so it is provably secure. However, notable disadvantages exist with this cryptosystem: Alice and Bob must posses the same private key (which must be longer than the message it self). This key must be pre-shared in a secure manner and also should necessarily be used only once (like an one time password). This is because, if the same key is used twice Eve can gain some information about the messages by just adding the public messages ($s_A \otimes s_B = m_A \otimes k \otimes m_B \otimes k = m_1 \otimes m_B$, using commutation). Interestingly, asymmetrical cryptosystems are often used to send the private sessions key used in symmetrical cryptosystems.

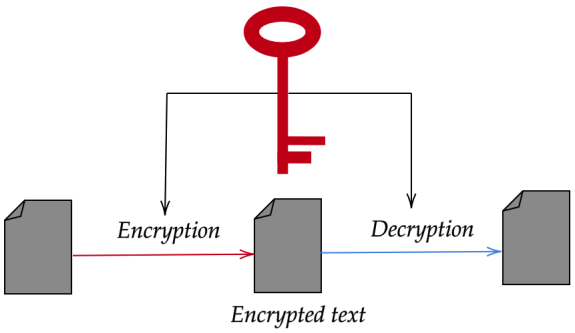


FIG. 14: An Symmetrical cryptosystem where the same key is used encrypt and decrypt

If these cryptographic algorithms were broken by advances in mathematics, Quantum Cryptography would be the only solution.

V. SHANNON INFORMATION THEORY

Information can be thought of in terms of randomness, that is, entropy or probability. If a certain event is likely to occur, you gain lesser information from it; higher the probability of occurrence lesser is the information transferred. This entropy is represented mathematically by using Shannon Entropy or Information entropy (H):

$$H = -\sum_j p_j \log_2(p_j) \tag{33}$$

where p_j is probability of occurrence of j^{th} value. Shannon, continued this discussion, in 1984 by proving that no matter how noisy a channel is, it is possible to communicate data, almost error free, up to a **maximum number** known as the channel capacity which only depends on the statistics of the channel [7].

$$C = B^2 \log(1 + \frac{S}{N}) \tag{34}$$

where C is the channel capacity (maximum bit rate), B is the bandwidth of the Channel, $\frac{S}{N}$ is the signal-to-noise ratio where S is the average signal power received and N is the average power of the noise. Similarly, we can think of this quantum mechanically, where Eve gains information from a quantum tunnel between Alice and bob at the cost of introducing noise into the system which lowers the bit rate. It is a constant tug of war between perturbation and information.

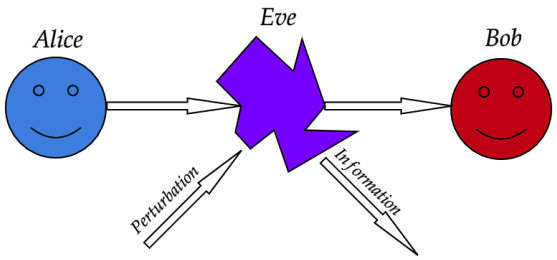


FIG. 15: The tug of war between perturbation and information

VI. THE NO-CLONING THEOREM:

Suppose Eve intercepts the message between Alice and Bob, she could just measure the quantum state and then resend a duplicate of it without perturbing the system, staying "undetected".

Conveniently as a consequence of quantum mechanics it can be proven that "no arbitrary quantum state can be perfectly cloned". This is the no-cloning theorem. An intuitive proof for this statement is that if we could make perfect copies, then the person could make as many identical copies as he wanted and measure every parameter with arbitrary precision, thereby breaking the uncertainty principle.

However, remember that the no-cloning theorem only prevents against making perfect copies, but you can make as many "imperfect" copies as you want.

Its important to note than non-orthogonal states can never be perfectly cloned so whatever Eve does should bring in some errors.

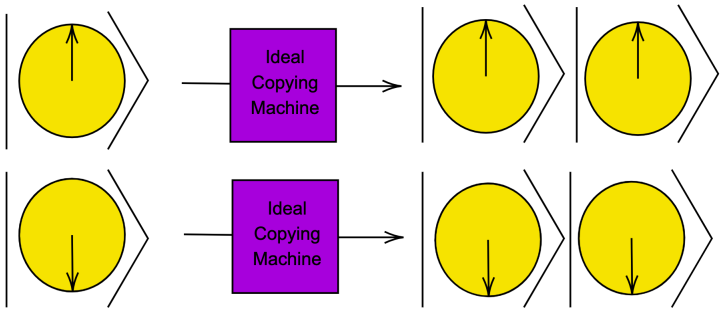


FIG. 16: Depiction of an ideal copying machine which clones the states $|0\rangle$ and $|1\rangle$ perfectly

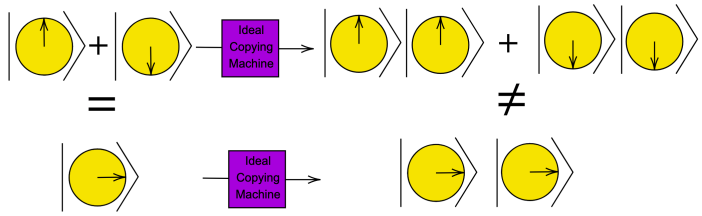


FIG. 17: If such an ideal cloning machine did exist then it would give the wrong answer for the superposition state of $|0\rangle + |1\rangle$[8]

VII. THE BB-84 PROTOCOL:

This protocol, aptly called the BB84 protocol, was proposed by Charles H. Bennett and Gilles Brassard in 1984 at the IEEE conference in India [9]. In this protocol Alice encodes the bit in a polarization state of a photon in one of two non-orthogonal bases either rectilinear or diagonal. The binary 0 state is defined as 0° polarization in the rectilinear state or a 45° polarization in the diagonal state. Similarly, a Binary 1 state is defined as 90° polarization in the rectilinear state or a 135° polarization in the diagonal state.

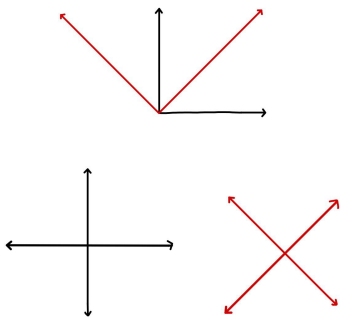


FIG. 18: polarized states in the BB84 Protocol

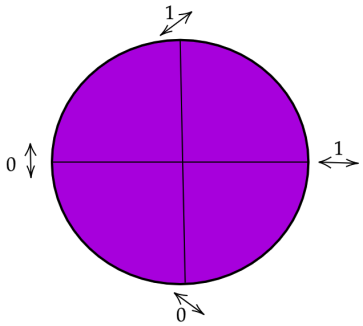


FIG. 19: The Bases of BB 84 protocol

Initially, Alice sends a key to Bob over a quantum channel. First, she chooses a random string of bits (for the binary states) and a basis for each bit to get a polarized state. Alice then sends her qubits to Bob, who measures the photons using a random non-orthogonal basis. If Bob chooses the same basis as Alice then he would get the same polarization (if no one eavesdropped on the photon). If, however, Bob chooses a different basis the qubits he reads would be random. Next, Bob discloses the bases he chose to Alice over a public channel (but, importantly, he does not disclose his result). Alice reports which bases are correlated and they discard the other bits where the bases are not correlated. If Eve does not eavesdrop on the channel both Alice and Bob would have the same perfectly correlated key called the sifted key. However, the crucial step, is that both Alice and Bob agree upon a random subset of the bits, and they compare them. If there is no measurement error or noise in the channel, the bits will be perfectly correlated and if they are no, it reveals the presence of Eve, who modified the photon by measuring it. If there was a measurement error, then error correction protocol can be used (Sec X.). Due to the Quantum No-cloning Theorem, Eve cannot replicate the photon she measures as she doesn't know with certainty the quantum state of the photon.

However, how safe really is this protocol? To answer, let us assume Eve intercepts the photon (an imperfect copy) and re-sends it to Bob (the intercept-resend strategy). Eve has to guess the random base and she has a 50% chance of guessing it right. A total of 25% of Bob's bases will be uncorrelated which gives Eve a **maximum** of 75% probability of not being detected. If the string of bits is long enough this probability will tend to 0 (as it depends on $(\frac{3}{4})^n$) [10].

VIII. THE ONE TIME PAD:

Classically, a One time pad can be achieved if Alice and Bob have an arbitrarily long pre-shared secret key which is used to encrypt and decrypt the messages. In theory, Alice could measure her classical system with arbitrarily high precision and then use the one-time pad to securely communicate this information to Bob, who can then, in principle, reconstruct (a copy of) the classical system. This however will not work in a Quantum Cryptographic Algorithm.

Let us say Alice wants to send a copy of a quantum system to Bob, she cannot do that as that violate the no-cloning theorem. However, they could sharea quantum key and a classical channel. Alice could "teleport" her quantum state to Bob without gaining any information about the quantum state, while Bob would end up with a state isomorphic with the original state (but he doesn't learn anything about the quantum state). This was aptly called "quantum teleportation" [11].

This is the only provably secure QC, you can show that if the quantum channel used to the share the key was secure, so is the one time pad [12, 13].

IX. OTHER SIMILAR PROTOCOLS:

A. Quantum Bit commitment and Coin-tossing:

1. *Bit commitment:*

Continuing with our two communicating parties, let us suppose that Alice chooses a bit (0 or 1), which she commits to, and wants to show Bob the evidence that she, indeed, has a bit in mind and cannot alter it. However, with this evidence, Bob should not be able to figure out the bit Alice chose. In case Alice changes her bit after commitment, it is considered as cheating, which a bit commitment protocol should protect against.

As it surprising turns out, there can never exist any bit-commitment protocol which is secure! This can be proved rigorously [14], but I would like to focus more on the implications of the impossibility of a bit-commitment protocol, it means that we could never trust Alice! She could cheat all she wants without Bob finding out.

2. Coin Flipping:

Similar to the idea of bit-commitment is that of coin flipping. Assume Alice and Bob are far away from each other and playing a game. The idea of the game is that one of Alice and Bob, say Alice, flips a coin, and the other, Bob, guesses the face of the coin. If the guess is correct, then Bob wins. Otherwise, Alice wins. However, in a classical coin tossing game, we could never know if Alice cheated. Of course, with the use of a trusted third party who flips the coin this problem is solved, but what if we could make a protocol that solely relied on the laws of quantum mechanics to ensure no cheating in this coin-flipping game without the help of any third party. If a secure bit-commitment protocol was available, then making this coin-flipping scheme would be trivial (But, importantly not the other way around). It just so happens that as long as Alice and Bob do not share any entangled state, any quantum flipping scheme would be impossible. Another really fascinating outcome of quantum mechanics! It shows that Alice can really cheat if she wanted without Bob finding anything out [15].

For a while it was believed that these classical protocols have "provably unbreakable" quantum counterparts, but quantum bit commitment and ideal coin tossing was also proven to not be secure [16].

B. Entanglement-Based Protocols using the Bell's theorem:

1. Eckert E91 protocol:

In this protocol a quantum channel sends two entangled particles (preferably polarized photons) one each for Alice and Bob. They choose on a random basis and they correct their raw keys, as in the BB84 protocol to obtain the sifted keys. If there was no eavesdropping, Bob's key would be the perfect complement of Alice's key. Here is the interesting part: to know whether Eve was peeking into the quantum channel, all they need to do is measure the photons where they used two different bases, now they measure the photons in a third predetermined base and then compare their results. If their results obeyed the Bell's inequality (which does not hold for entangled particles), it reveals the presence of Eve as the photons are no longer entangled[17].

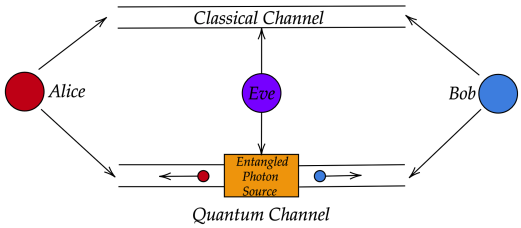


FIG. 20: The Eckert entanglement protocol

2. BBM92 Protocol and Other Variants:

Bennet and Brassard in 1992 made a variation of the E91 protocol which does not require the Bell's test. Similar to the E91 protocol there is an entangled photon source, Alice and Bob make measurements on a random basis, and they publicly announced their bases. Therefore, when they are correlated the spin must be opposite. If it isn't, it reveals the presence of Eve. Furthermore, Bennet and Brassard proved that any variant of the BB84 protocol could be adapted to use an entangled photon source without the use of the Bell test [18]. Enzer, in 2002, proposed another entanglement-based protocol, which is an entangled version of the Six-State Protocol [19].

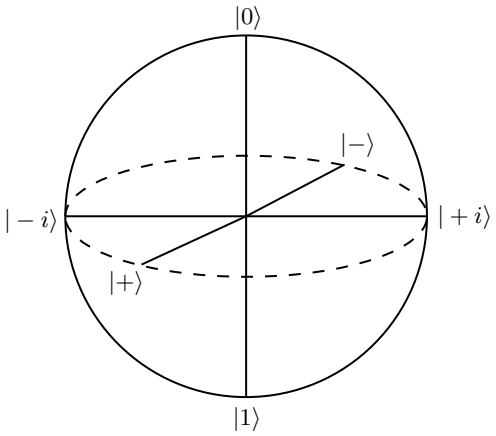


FIG. 21: The Six State Protocol

X. EAVESDROPPERS, THEIR STRATEGIES AND HOW TO COUNTER THEM:

If their bases are correlated, Alice and Bob should, in theory, have identical sifted keys. However, in reality that is not the case as there are many errors that are introduced, which eavesdroppers capitalise on. To counter them we need to apply some information protocols:

1. **Error Correction:** The error rate, called the quantum bit error rate, QBER (to avoid confusion

with the classical Bit error rate BER) is usually of the order of a few percent. This error rate would be reduced down to the order of $10^{-9}\%$ using classical algorithms.

2. **Privacy Amplification:** After error correction, both Alice and Bob have the same sifted keys. However, Eve might still have information; this is where privacy amplification comes in. It reduces the information Eve has to almost zero. We assume that Alice, Bob and Eve respectively have the variables α, β, ϵ and their entire probability distribution is given by $P(\alpha, \beta, \epsilon)$. Both Alice and Bob know what $P(\alpha, \beta)$ is, and from (35) we can get a lower bound on $S(\alpha, \beta||\epsilon)$ in terms of the difference between Alice and Bob's mutual information $I(\alpha, \beta)$ and Eve's mutual information [5].

$$S(\alpha, \beta||\epsilon) \geq \max\{I(\alpha, \beta) - I(\alpha, \epsilon), I(\alpha, \beta) - I(\alpha, \epsilon)\} \tag{35}$$

To establish a secret key using this idea, Alice and Bob compare a random subset of their sifted keys and estimate the QBER. If (35) is not satisfied ,they stop the protocol, and if it is satisfied they continue on with error correction protocols. In other words, as Alice and Bob share an identical key, they can transform their key into a new shortened key in such a way that Eve cannot gain information unless she also has an identical key. Therefore, even if Eve has substantial information on the key, it would be of no use after privacy amplification.

The aim of eavesdropping analysis is to find "ultimate proofs" (security that works against all types of eavesdropping attacks) for cryptosystems. Eavesdropping attacks that Eve carries out are broadly classified into two categories:

1. Individual attacks: Here, Eve attaches independent probes to each photon individually, and measures each probe, one at a time. It is also known as an Incoherent Attack.

2. Joint attacks: In the most general case of a joint attack, Eve can measure multiple probes at once coherently; hence, they are also called coherent attacks. A commonly used subset of a joint attack is the collective attack, which assumes that each photon is probed only once but many probes can be measured at once.

Individual attacks can be translated into a classical problem using the idea of privacy amplification of imposing constraints on the joint probability distribution using the laws of quantum mechanics.

A. The Intercept resend strategy:

Assuming we use the BB84 protocol, we know that there is a 25% QBER and Eve gains 0.5 bits of information for each qubit measured. From Shannon Information theory, we know that the amount of information Eve gains is the amount of entropy decrease.

$$I(\alpha, \epsilon) = -\Delta H \tag{36}$$

where $I(\alpha, \epsilon)$ denotes how much information Eve ϵ has on Alice and H is the Shannon entropy. We can simplify (36) using (33) and the fact that $H_{initial}$ is 1 as Alice's bit is uniform. We find, as expected, that Eve gains 1/2 a bit for each qubit measured.

$$h(p) = p\log_2(p) + (1-p)\log_2(1-p) \tag{37}$$

In addition, the probability of Eve guessing the correct bit is 0.75 (as expected). However, if Eve measures the bit in an intermediate basis, the Breidbart Basis.

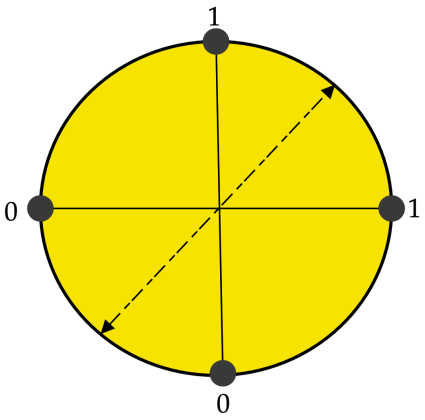


FIG. 22: The Breidbart Basis

Then the probability that she gets the bit correct is $cos^2\frac{\pi}{8} = 0.85$ and curiously by using (37), we find that Eve only gains 0.4 bits per qubit but has a higher probability of getting it right, this is because in the Breidbart basis in half of the cases the information is deterministic, but in the regular BB84 protocol the information is always probabilistic.

B. "Ultimate" security proofs for any noisy channel:

In an ideal channel with no noise, it is easy to prove that quantum cryptography (QC) is secure. However, it is interesting to note that this proof can be extended to any noisy channel provided the equipment is perfect. Obviously, QC is only secure up to a threshold of QBER which is what we need to find. The proof provided in [5]

uses two theorems:

Theorem 1. For a given joint distribution $P(\alpha, \beta, \epsilon)$, Alice and Bob can form a shared secret key if and only if $I(\alpha, \beta) \geq I(\alpha, \epsilon)$ or $I(\alpha, \beta) \geq I(\beta, \epsilon)$. In other words, this means that Bob must have more knowledge on Alice's bits than Eve does. This can be understood visually in the figure below.

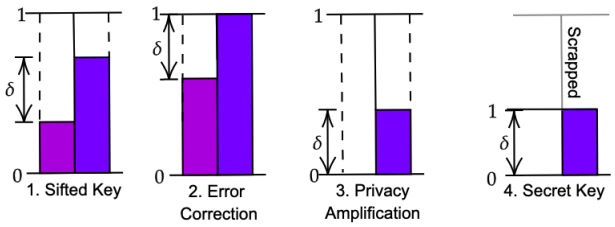


FIG. 23: A feel for Theorem 1. The initial situation is given in 1. After Error Correction Bob's information becomes 1. After Privacy Amplification, Eve's information becomes 0. As Bob disregarded all the random bits so he loses information. And finally, scrapping this random bits gives us a secret key.

Theorem 2. If Eve performs a measurement giving her some information $I(\alpha, \epsilon)$, then, because of the perturbation, there is a limit on the amount of information Bob can gain.

If n is the number of qubits,which Bob receives, that are in the same basis then Theorem 2 implies that:

$$I(\alpha, \epsilon) + I(\alpha, \beta) \leq n \tag{38}$$

Essentially information per qubit both Bob and Eve gained when combined should be ≤ 1. Combined with (37) we obtain:

$$QBER \leq 11\% \tag{39}$$

Therefore, whenever (39) is obeyed an ultimate security protocol can be developed. Note that this proof is valid only when the key is much longer than the number of qubits Eve intercepts.

XI. TWO WAY QUANTUM COMMUNICATION PROTOCOLS:

Two-way quantum protocols have a distinct advantage over unidirectional protocols in that they are deterministic. Generally, in a two-way protocol, Bob prepares quantum states and sends them to Alice via the quantum channel, who encodes the states and re-sends it back to Bob, who performs a measurement. There are two common two-way protocols: The LM-05 protocol and the ping pong protocol.

A. LM-05 protocol:

Here Bob sends of qubit in one the forms $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$. Alice does one of two things to this qubit, she either uses this qubit as a control to test with a probability of c (control mode) or uses it to encode information (encoding mode), with a probability of $1 - c$. The way Alice tests for noise is similar to the BB84 protocol, wherein she measures the qubit on a random basis. In the original protocol, Alice now sends the qubit back with the exact same wavelength, amplitude, time gap, or else Eve could determine Alice's chosen mode. However, this is not feasible in real life. Instead, Alice encodes this bit into information and re-sends it to Bob, who decodes it using the same base he sent the qubit in. As we can observe, this is a deterministic protocol as Bob know Alice's bases without a need for base-reconciliation which would be non-deterministic. In addition, for the two-way tunnel protocol to work, a direct test on at least one direction of the tunnel is necessary. Therefore, a two-way quantum tunnel protocol is susceptible to attacks such as the Trojan horse attack (Sec XII.C). without the control mode [20, 21].

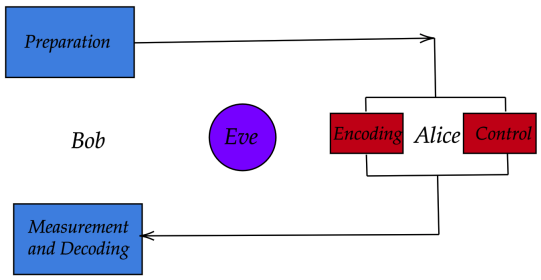


FIG. 24: The LM-05 Protocol: Bob Prepares a Qubit and sends it to Alice who uses the qubit as a control or to encode information. She sends the encoded bit to Bob who decodes it.

B. Ping Pong Protocol:

In the ping-pong protocol, an entangled orthogonal state is used in the following form:

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$$

As you can see they are just the EPR states. What Bob does is that he makes two, qubits one being the home qubit and the other being the travel qubit. Bob sends this travel qubit $|\psi^{+}\rangle$ to Alice who randomly chooses whether to do a message mode or control mode. Let us asuume that Alice chooses the message mode and encodes the

qubit she received from Bob using an encoding operation σ_α^b where b is either 0 or1. If $b = 0$ then the qubit $|\psi^+\rangle$ will be transformed into $|\psi^-\rangle$. However, if $b = 1$ it will be left untouched. Alice sends this encoded bit to Bob who performs a Bell measurement to get the wave function to be one of $|\psi^+\rangle$, $|\psi^-\rangle$ hence revealing the value of b [22].

If instead Alice chooses the control mode, she measures the qu-bit in basis $|0\rangle$, $|1\rangle$ and then reveals the result publicly to Bob, now Bob also makes a measurement in the basis $|0\rangle$, $|1\rangle$ and announces his result. If their results do not differ it indicates the presence of Eve and the protocol is aborted.

XII. REAL LIFE EXAMPLES:

A. Photon Number Splitting (PNS) Attacks

The entanglement protocols are difficult to work with in real life, as modern-day equipment cannot reliably produce and measure singular photons. In real life, a laser produces a number of coherent photons. Eve can exploit this by splitting off a small number of photons for each qubit and lets the rest of the photons pass on to Bob, leaving no trace. This attack is called the photon number splitting or PNS attack [23].

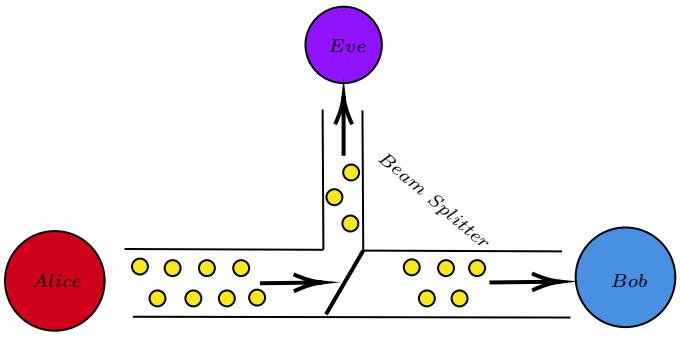


FIG. 25: The PNS attack, Eve uses a Beam Splitter to Divert some Photons to her without perturbing Bob's Measurement but gaining a small amount of information.

This attack can be countered in two ways: the first is the SARG-04 protocol where Alice does not reveal her bases publicly but reveals a pair of non-orthogonal states in which the bit might be encoded in. If Bob measures on the same basis, he would have measured one of the non-orthogonal states and, if not, they simply discard the bit. Now, all Eve can do is guess, so her Shannon information is significantly lower [24]. Unfortunately, the SARG-04 protocol, which was theorized to be the same as the BB-84 protocol, but experimentally it under performs due to errors introduced [25].

The second method uses decoy pulses where Alice sends the beams of varying intensities, with only one being the signal pulse and all others being decoy pulses. The so called "Decoy State Protocol". With the help of these decoy pulses Alice can detect the presence of Eve as she cannot maintain the bit error rate when multi-photon sources are involved [24, 26, 27].
Accounting for more such real-life quantum channel imperfections, Gottesmann's paper [28] explains the real life security of BB84-based protocols.

B. Intensity based attacks:

When Huang tested the decoy state protocol in real life using a source that could regulate the intensity, he found that different intensities in general corresponded to different times at which the pulses were sent [29]. This means theoretically, Eve can differentiate between a decoy pulse and the actual signal according to the time of sending. However, Alice can counter this attack by modulating the intensity of the photons after they are sent, and it was found that when an external modulator was used, all photons were simultaneous. However, as recently discovered Eve can heat up Alice's source using high-intensity sources, and this shifts the timings of different intensity pulses, Alice cannot compensate for this time delay unless she finds out that they have been changed [30].

C. Trojan horse and Back-flash attacks:

Trojan horse attacks are a classical case of QC, which reminds us that the security of QC is not determined just by the laws of Quantum mechanics but it also depends on the technical measures. In this attack, Eve sends a light pulse through a quantum channel, in this case an optical fiber, entering Alice's or Bob's detector, and then Eve analyzes the reflected light. This provides her information about the polarization settings of the apparatus by calculating the phase shift. We cannot however, simply just block the optical fiber as it would not allow for communication between Alice and Bob. To be protected against this attack, Alice should first reduce the time period (Δt_{phase}) in which a phase shift occurs to the order of nanoseconds, forcing Eve to send the pulse at the same time as Bob. Next, Alice using an attenuator reduces the energy of the pulse from Bob to, let's say 0.2 photon per pulse. For, Eve to gain, say 1 photon per pulse she has to send a photon of twice the energy. Alice, can easily detect the sudden increase in energy in Bob's pulse which reveals Eve. However, Eve could however send ultra-short pulses (a low Δt_{phase}) or could use a pulse of different energy (wavelength). So, Alice must use a optical band-pass filter which allows Alice's transmission to go through with a bandwidth compatible with Δt_{phase}.

Trojan Horse Attacks, though preventable using technical measures, are threatening attacks and should be kept in mind while making a channel [31–34].

In principle, a back-flash attack is similar to a Trojan horse attack, an avalanche photodiode (APD) in real practice emits some light when it measures [35]. This "back-reflected" has a lot of information in it, for example, its polarization could give information about the basis Bob used and even gives information about Eve's source.

D. Faked State Attacks:

As we found from the PNS attack, the light is not really a single photon but a bunch of photons. Thus, detectors can echo the effect of a single photon using very weak light sources. This reliance on weak light sources is exploited in the faked state attack. The core weakness is the APD of Bob, which is supposed to measure only only one photon by registering a click, but an APD has a certain recharge time (in the order of μs). This implies that if a beam of light is shone on the diode continuously then the diode cannot recharge and hence it just becomes a classical photodiode. Further, this also implies that Eve can adjust the timing of the light to essentially control the time at which the detector clicks and forces Bob to unknowingly use Eve's basis. It is called a faked state attack because Eve does not actually send a quantum state, but rather makes Bob's detector think it is detecting a quantum state.[36–39]

This can be illustrated by an example in which Eve detects a bit 1 of base X from Alice, she sends a photon of opposite bit (bit 0) and opposite basis W to Bob and while sending this "faked" state, she simultaneously shines continuous light onto Bob's 1 bit detectors, blinding them. If Bob measures the bit in basis X, he has a 50% chance of not detecting anything, and if he measures anything other than in base X he would not detect anything. Thus, Eve can now control the basis in which Bob measures.

XIII. PROTOCOLS BEYOND STANDARD KEY DISTRIBUTION:

A. Quantum random access codes (QRAC):

The principle of random access codes is simple, Alice needs to encode n bits into m and send them to Bob ($n > m$), and Bob should be able to recover all the bits with probability $> p$. Such a random access code is represented by $n \xrightarrow{p} m$. Classically, you encode n-classical bits into m classical bits, but you could however encode them into m-qubits. Here is where it becomes interesting, when Bob recovers one bit, the whole wave function collapses, risking the loss of other bits. Therefore, there will always be a threshold probability for Bob to recover all the bits.[40] Let us investigate this!

1. *Visualising qubits using Bloch Spheres:*

A qubit is a composition of bits $|0\rangle$ and $\|1\rangle$. So it can be represented as: $|\psi\rangle = A\|0\rangle + B\|1\rangle$ and since ψ must be normalized, $A^2 + B^2 = 1$. Therefore, we can write (without the loss of generality) $A = \frac{\cos(\theta)}{2}$, $A = e^{\iota\phi}\frac{\sin(\theta)}{2}$ ($e^{\iota\phi}$ term represents phase.)
This can be re-interpreted in terms of spherical coordinates: $\vec{r} = \sin\theta\cos\theta\hat{i} + \sin\theta\sin\theta\hat{j} + \cos\theta\hat{k}$. This is the Bloch Sphere:

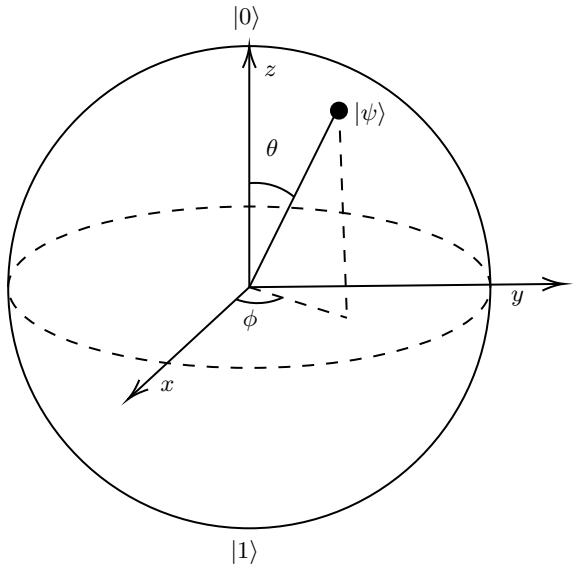
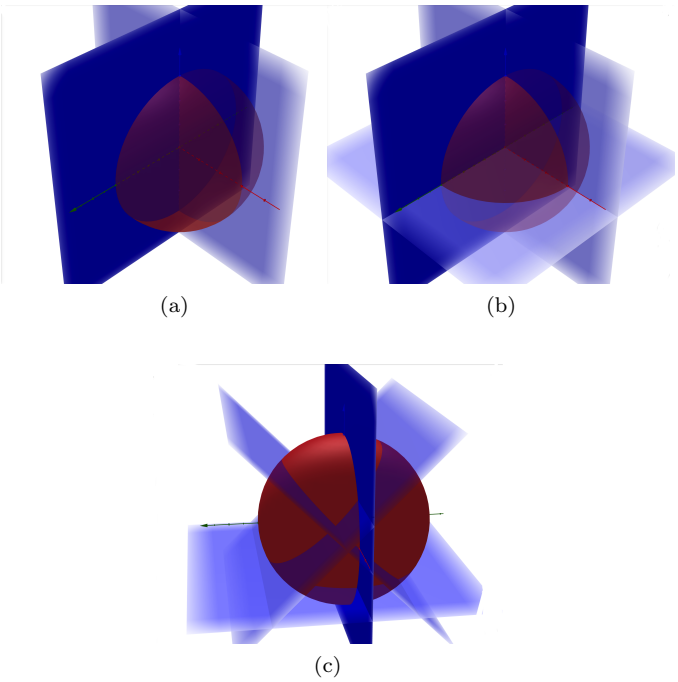


FIG. 26: The Bloch Sphere

From this representation we can find the probability of $|\psi\rangle$ collapsing to $|\phi_0\rangle$ to be $\frac{1}{2}(1 + cos(\theta)$ [41].

For a $2 \xrightarrow{p} 1$ QRAC the probability threshold is just $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$ [42], and for $3 \xrightarrow{p} 1$ it is $\frac{1}{2} + \frac{1}{2\sqrt{3}} \approx 0.79$ [43]. Let us assume the minimum probability threshold is 0.5 (better than a coin flip). For a $n \xrightarrow{p} 1$ to have a probability greater than 0.5, a sphere must be able to be divided into 2^n parts (as our minimum probability is 0.5) by n planes. As you can see, in the figure below, it is possible to cut a sphere into four parts using two planes and eight parts using three planes, but it is impossible to cut a sphere into 16 parts using four planes, we can at most cut it into 14 parts. Hence a $4 \xrightarrow{p} 1$ never works for $p > 1/2$ [44].



(a) (b)

(c)

FIG. 27: A sphere can be cut into a. four regions by two plane b. eight regions by two planes c. but it can be cut into at most 14 regions by 3 planes

2. *Communication complexities:*

The main aim of finding communication complexity is to calculate the number of communication bits that Alice and Bob must exchange in order to perform a certain task. The simplest example is that proposed by Yao ([45]), where Alice and Bob each have bits x and y, bits, respectively. They need to send these bits to a third party (the referee), and then all three collectively need to calculate the value of a function f(x,y) while minimizing the amount of information used.

$$f(x) = \begin{cases} 1, & x \neq y \\ 0, & x = y \end{cases} \tag{40}$$

A trivial communication strategy is just Alice sending x to the referee and Bob sending y to the referee but this is highly inefficient with a complexity of $O(2n)$ (sending two bits of length n). The "communication cost" of this strategy could be highly reduced if only a part of the bit is sent instead of the whole bit. This is where tools like Quantum fingerprinting can be applied, and used to distinguish two strings by using the least amount of bits. Instead of comparing the entire string, only the fingerprint of the string will be compared which reduces the communication complexity significantly.

Another way to decrease the communication complexity is to use the concept of shared randomness, where since Alice and Bob are entangled, less amount of information transfer is needed.

B. Quantum Data Locking (QDL):

The idea behind QDL is pretty simple, Alice and Bob initially share no mutual information, now Alice using a key of length k encodes a n-bit message into a n-bit code-word sends the code-word to Bob. They now share a mutual information of n. When Alice shares the key, the mutual information could potentially increase by more than k by quantum mechanical means. Now, the regular BB84 protocol follows but with an important difference: in QDL Eve is assumed to be able to store quantum information only for a limited time or a limited amount of information can be stored at any time. What this means is that, if Eve intercepts n qubits she has to measure them instantaneously (or after some time), she cannot gain all the information. The amount of information that Eve can extract from a quantum system is called the accessible information; in this case Eve can only have a maximum information of $\frac{n}{2}$. Thus, Eve loses half the information, and if the length of the bit is long enough the information Eve has would be negligible. In addition, for any QDL protocol to be deemed "good", the length of the message transferable should be much greater than the length of the key itself. QDL works best for locking information in quantum states using exponentially small pre-shared keys [46].

C. Quantum Digital Signatures (QDS):

In cryptography, many a times we need to verify the origin of a message. This can be achieved by using a digital signature.

A classical digital signature is very similar to the way asymmetric cryptosystems work, by using one-way functions (Given x we find f(x) but not the other way around). A common one-way function used is prime-factoring, but as we know, no provably secure one-way function has been found. For example,the prime factoring function is not secure against a quantum computer. This leaves a hole in cryptography which quantum signatures attempts to fill.

A QDS Scheme ensures that:

1. The message was created by the sender, which he cannot deny
2. The message has not been tampered with
3. The message if accepted at one receiver should be acceptable at all receivers

1. *The Gottesman-Chuang protocol:*

The Gottesman-Chaung protocol uses the ideas of quantum one-way function, similar to classical one way

functions, they return a public quantum bit-key from a provate classical/quantum string [47].

In a simplified Gottesman scheme we consider the former case of using a classical string. It goes as follows:

As we can see, Alice has to sign every bit in the message. For this she chooses R pairs of private keys k_0^j, k_1^j $(0 < j < R$, where all k_0^j will be used to sign bit 0 and all k_1^j will be used to sign bit 1. The function $k \mapsto |f_k\rangle k \mapsto |f_k\rangle$ is public and Alice converts k_0^j and k_1^j into $|f_{k_0}^j\rangle$ and $|f_{k_1}^j\rangle$, the public quantum keys. She can make as many identical copies of these keys as she wants but more the number of copies lesser the security of the system. ,Now she sends this to Bob, who now has the bit a, private keys, and their corresponding public keys. Bob now uses the k_a and calculates the value of $|f_{k_a}\rangle$.

But a problem arises here, lets say we have two quantum states $|f_k\rangle$ and $|f'_k\rangle$, how do we find out if they are the same? Classically this problem is trivial, as we can just look at the strings and find out if they are the same. However, it becomes interesting when we look at it quantum mechanically. We perform the SWAP test to achieve this, instead of delving into the details, all we need to know about the SWAP test is that it is not deterministic. There is always a probability that it gives you the wrong answer.

What this means is that Bob can compare the values of $f_{k_a}^j$ that he found with $f_{k_0}^j, f_{k_0}^j$ and as we discussed earlier the SWAP test can give incoorect results, therefore there will be a few mismatched bits (m). Now, as long as m is below a certain pre-fixed threshold Bob accepts the signature or else He rejects them as forgeries.

XIV. CONCLUSIONS

Quantum Cryptography is a beautiful combination of information theory and the laws of quantum mechanics. In our review we presented the basic laws of quantum mechanics, delved into a few Key distribution protocols, looked and how to counter eavesdroppers, real life attacks and finally at some non-key distribution protocols like data locking and digital signatures. The tremendous progress in quantum optics and optical fibers makes such protocols to be realised in the real world. Privacy Amplification (Sec X.), is a classical protocol heavily inspired from Quantum Cryptography. Though, Quantum Cryptography is mature there are still a lot of technological challenges that remain.

For example, the compatibility of the advanced detectors with the communication fibers. Another issue of Quantum Cryptography concerns its range, QC protocols even with modern range technology have a short distance range compared to other communication methods. Practical quantum repeaters could be the key for long range QC. Quantum repeaters detect and correct errors, provided error rate is low enough. We can hope that such techniques could potentially lead to realise QC over long distances. QC's however still have many loopholes like side channel attacks, errors in random number generators and imperfection in the detectors which Eavesdropper's can Exploit.

Despite these loopholes, humanity will master this technology and QC will become a commercial product potentially for secure financial transactions among other applications, we just do not know when that is going to happen.

[1] D. J. Griffiths, *Introduction to Quantum Mechanics (2nd Edition)*, 2nd ed. (Pearson Prentice Hall, 2004).
[2] G. Binnig and H. Rohrer, Reviews of Modern Physics **59**, 615–625 (1987).
[3] J. S. Bell, Physics Physique Fizika **1**, 195 (1964).
[4] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020).
[7] C. E. Shannon, The Bell System Technical Journal **27**, 379 (1948).
[8] W. Dür and S. Heusler, "What we can learn about quantum physics from a single qubit," (2013), arXiv:1312.1463 [physics.ed-ph].
[9] C. H. Bennett and G. Brassard, Theoretical Computer Science **560**, 7–11 (2014).
[10] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, and et al., Advances in Optics and Photonics **12**, 1012 (2020).
[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[12] S. M. Bellovin, Cryptologia **35**, 203–222 (2011).
[13] W. Peng, S. Cui, and C. Song, Plos One **16** (2021), 10.1371/journal.pone.0245506.
[14] G. Chiribella, G. M. D Ariano, P. Perinotti, and D. Schlingemann, Physics Letters A **377**, 1076–1087 (2013).
[15] I. Damgård and C. Lunemann, Advances in Cryptology – ASIACRYPT 2009 Lecture Notes in Computer Science , 52–69 (2009).
[16] H.-K. Lo and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible," (1996), arXiv:quant-ph/9605026 [quant-ph].
[17] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[18] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[19] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, Proceedings of 1994 IEEE International Symposium on Information Theory (1915), 10.1109/isit.1994.394668.
[20] M. Lucamarini and G. Di Giuseppe, International Journal of Quantum Information **03**, 189 (2005).
[21] M. Lucamarini and S. Mancini, Physical Review Letters **94**, 140501 (2005).

[22] C. Zuning and Q. Zheng, in *2010 5th IEEE Conference on Industrial Electronics and Applications* (2010) pp. 1805–1810.

[23] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[24] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[25] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, Laser Physics Letters **11**, 095201 (2014).

[26] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[27] X.-B. Wang, Physical Review Letters **94** (2005), 10.1103/physrevlett.94.230503.

[28] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Info. Comput. **4**, 325–360 (2004).

[29] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, Physical Review A **98** (2018), 10.1103/physreva.98.012330.

[30] Y.-y. Fei, X.-d. Meng, M. Gao, Y. Yang, H. Wang, and Z. Ma, Optics Communications **419**, 83–89 (2018).

[31] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Physical Review A **73** (2006), 10.1103/physreva.73.022320.

[32] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, IEEE Journal of Selected Topics in Quantum Electronics **21**, 168 (2015).

[33] A. Vakhitov, V. Makarov, and D. R. Hjelme, Journal of Modern Optics **48**, 2023 (2001).

[34] S. E. Vinay and P. Kok, Physical Review A **97** (2018), 10.1103/physreva.97.042335.

[35] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, Journal of Modern Optics **48**, 2039 (2001), https://doi.org/10.1080/09500340108240905.

[36] V. M. * and D. R. Hjelme, Journal of Modern Optics **52**, 691 (2005), https://doi.org/10.1080/09500340410001730986.

[37] M. Stipčević, "Preventing detector blinding attack and other random number generator attacks on quantum cryptography by use of an explicit random number generator," (2014), arXiv:1403.0143 [quant-ph].

[38] V. Makarov, A. Anisimov, and J. Skaar, Physical Review A **74** (2006), 10.1103/physreva.74.022313.

[39] B. Qi, C. Fung, H. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[40] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," (2009), arXiv:0810.2937 [quant-ph].

[41] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," (2009), arXiv:0810.2937 [quant-ph].

[42] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, "Dense quantum coding and a lower bound for 1-way quantum automata," (1998), arXiv:quant-ph/9804043 [quant-ph].

[43] J. S. Bell, American Journal of Physics **70** (2002), 10.1119/1.1463744.

[44] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, New Journal of Physics **8**, 129–129 (2006).

[45] A. C.-C. Yao, in *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, STOC '79 (Association for Computing Machinery, New York, NY, USA, 1979) p. 209–213.

[46] Y. Liu, Z. Cao, C. Wu, D. Fukuda, L. You, J. Zhong, T. Numata, S. Chen, W. Zhang, S.-C. Shi, and et al., Physical Review A **94** (2016), 10.1103/physreva.94.020301.

[47] D. Gottesman and I. Chuang, "Quantum digital signatures," (2001), arXiv:quant-ph/0105032 [quant-ph].