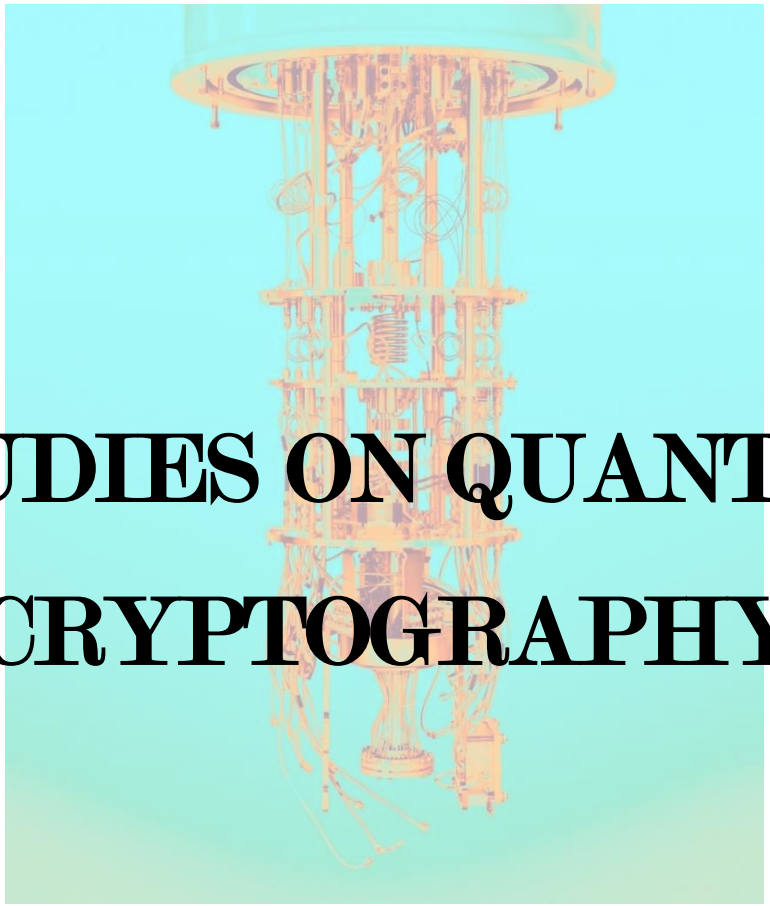


STUDIES ON QUANTUM CRYPTOGRAPHY

Autor: Isabel Carnoto Amat.

Tutor: Luis Enrique García Muñoz.

Leganés, Diciembre 2019.

INDEX

The major difference between classical and quantum mechanics is that, classical mechanics has surrounded us all our lives, we know how things behave just by intuition. Quantum mechanics studies things so small, cold and isolated that they are completely out of the range of human senses.

Chapter I. Quantum Mechanics

As an introduction, here is a summarize of the first three chapters of the book "Quantum Mechanics. The Theoretical Minimum. What You Need to Know to Start Doing Physics" from authors Leonard Susskind and Art Friedman [1].

Lecture 1. Systems and Experiments

As mentioned before, quantum mechanics studies the behavior of objects so small that human senses are uncapable of visualizing them. The best way to approach this is by using mathematical abstractions. Even though classical mechanics also uses mathematical abstractions, these ones differ from quantum mechanics for two reasons. First, the idea of a state in quantum mechanics is conceptually different from the classical mechanics one, and secondly the relation between states and measurements changes. In classical mechanics the state of a system can be determined by measuring, but in quantum mechanics it can't be, states and measurements are two very different things.

Spins and qubits

Particles have properties like location, mass or electric charge, depending on the specific particle. An electron, for instance, has an extra degree of freedom called its spin. The spin can be pictured as an arrow pointing to certain direction, but this approach is too classical. The quantum spin, isolated from the electron that carries it, is a system that can be studied by itself and is an example of the systems we will call qubits (quantum bits).

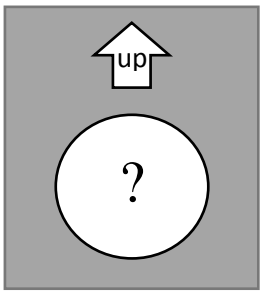
An Experiment

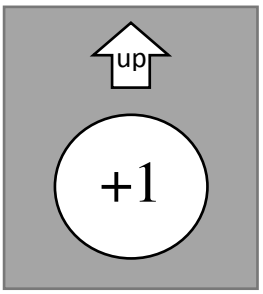
In classical mechanics we can find the simplest of deterministic systems: a coin that can give heads (H) or tails (T). This is a two-state system, analogous to a bit because it can only be in two states, H or T, 0 or 1 and nothing in between.

In quantum mechanics we will think of this system as a qubit.

To get the states through an experiment we will picture a measuring apparatus ***A*** involved. ***A*** interacts with the system and records the state of the spin, we will call this state σ (sigma) and σ can have two values: +1 or -1.

Let's imagine the apparatus ***A*** as shown in the picture, with a screen to display the measurement result and an arrow to indicate the apparatus orientation in space.





The initial value of σ is unknow, and the goal is to use ***A*** to determine it. Before measuring, the apparatus's screen will show a question mark and after the measurement it will show σ = +1 or σ = -1.

For the first measurement, ***A*** is oriented along z axis and it gives σ = +1. After repeating the measurement several times, without altering the spin, the apparatus shows the same result, σ = +1. It seems like the first measurement sets the state and the subsequent ones confirm that state.

Now after setting the state to σ = +1 with one measurement, the apparatus is flipped 180 degrees to measure along -z axis. ***A*** gives σ = -1 as a result, from this we may conclude that the apparatus measures a direction in space, like if σ were a vector. If this is true, this vector would have three components: σ_x, σ_y and σ_z.

To confirm the assumption that σ is the component of a vector, the state is measured along σ_x, after it has been set to σ = +1 along the z axis. If σ is really the

component of a vector we would expect this measurement to be zero, but instead the apparatus shows $\sigma_x = +1$ or $\sigma_x = -1$ randomly.

To get some sense out of this result the experiment is repeated many times following the same steps:

- ✓ With ***A*** along the z axis, σ is set to σ = +1.
- ✓ ***A*** is rotated 90 degrees to be oriented along σ_x.
- ✓ ***A*** measurement is made.

After many iterations the results are 50% of the time σ = +1 and the other 50% σ = -1. Instead of the classical result, σ_x being directly zero, we get that the average of these repeated measurements is zero.

If instead of setting σ along σ_z, σ= +1 is set along $\hat{m}$, the following measurements, with *A* oriented along $\hat{n}$, give as a result: $< \sigma >= \hat{n} \cdot \hat{m}$

Even if the results seem random, after repeating the experiment many times the average value can follow the classical expectations, up to a certain point.

Experiments are never gentle

In classical mechanics the act of measuring something will not disrupt any aspect of that object. It all changes in quantum mechanics, where if an apparatus is strong enough to measure some aspect of a system, it is also strong enough to distort another aspect of the same system.

As an example, the ***A*** apparatus is used to set σ= +1 along the z axis, then it's rotated 90 degrees to measure along the x axis, and finally placed back to its original position. The act of making an intermediate measurement leaves the spin at a random configuration, which causes the following measurement, along the z axis, to give a different result from the original one. "One may say that measuring one component of the spin destroys the information about another component" [1]. There is no way to know the components of a spin along two different directions simultaneously.

Propositions

The fundamental idea in Boolean logic is that a proposition is either true or false, with no values in between. If we take a dice as an example, we could write the following propositions:

A: the dice shows a pair-numbered face.

B: the dice shows a number greater than 3.

From the whole set of possible values for a dice face {1, 2, 3, 4, 5, 6}, the subset of the proposition A is {2, 4, 6}, and the subset of B is {4, 5, 6}.

It is possible to combine propositions to make more complicated ones by using **and, or** and **not.** With **not** we obtain the opposite of a proposition, for example:

Not A: the dice shows an odd-numbered face.

And is used with a pair of propositions and is true if both propositions are true.

The subset of A **and** B is {4, 6} both pair numbers greater than 3.

Lastly, the inclusive version of **or** (the one used by Boolean logic) is true if either or both propositions are true.

The subset of A **or** B is {2, 4, 5, 6} pair numbers and numbers greater than 3.

Now for testing quantum propositions we will also use **and, or** and **not.** Taking the following two propositions:

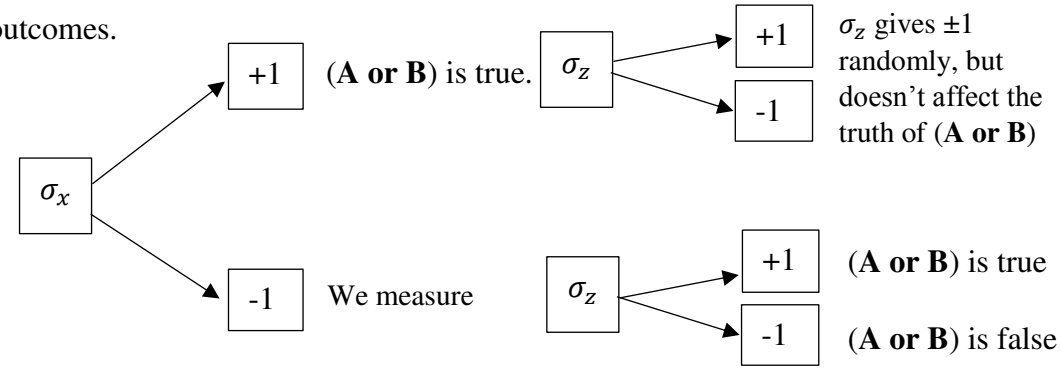
A: along the z axis, the state of the spin σ= +1.

B: along the x axis, the state of the spin σ= +1.

Both can be tested by orienting the *A* apparatus along the desired direction. The negation of these also makes sense, giving us that the state of the spin is σ= -1

With **or** and **and** there are some steps to follow. First, let's consider that someone unknown has set the spin in the σ_z= +1 state. To determine if (**A or B)** is true we begin by measuring σ_z, since it was already prepared, the result is σ= +1 and the proposition is true. If we measure along the x axis, we will obtain σ= +1 or σ= -1 randomly, but neither of the results affects the truth of (**A or B**). To determine if (**B or A**) is true we start by

measuring σ_x, since the spin was initially prepared as σ_z= +1, we can have several outcomes.



In 25% of the cases this quantum proposition is false, this shows that **(A or B)** is not symmetric, as it is in classic Boolean logic. The truth may depend on the order chosen to make the measurements and this demonstrates that the foundations of logic are different in quantum physics.

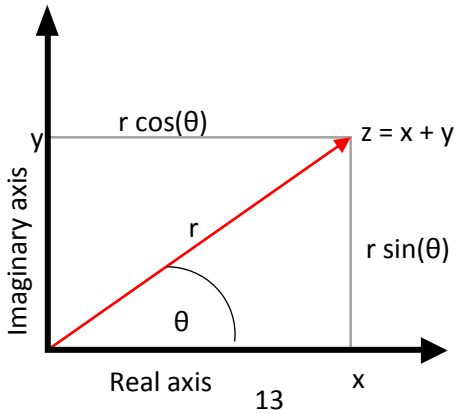
To test **(A and B)** the same procedure is followed. There is a possibility that the results are σ_z= +1 and σ_x= +1 after the first two measurements but we have to remember that the act of taking the second measurement disrupts the first one, making it not confirmable. This is called the uncertainty principle and it states the inability to know a pair of measurable quantities simultaneously. Therefore, the proposition **(A and B):** the z component of the spin is +1 **and** the x component of the spin is +1, is meaningless.

Mathematical Introduction to Complex Numbers

A complex number can be written in different ways.

$$z = x + iy = re^{i\theta} = r(\cos\theta + i\sin\theta)$$

Where $i^2 = -1$, z is a point on the complex plane, and x and y are real numbers.



Every complex number has a complex conjugate:

$$z^* = x - iy = re^{-i\theta}$$

$$z^* z = r^2$$

We will think of z^* and z to be part of different number systems. Lastly, there is a special type of complex numbers, whose r-component is 1, called "phase-factors". For this class of complex numbers, we have:

$$z = e^{i\theta} = \cos\theta + i\sin\theta$$

$$z^* z = 1$$

Vector Spaces

The space of states of a quantum system is a vector space, understanding the word vector as an abstract construction that may have from 1 to ∞ dimensions and integers, complex numbers, real numbers or other things as components.

A vector space, in quantum mechanics, is composed of ket-vectors $|A\rangle$, that meet the following axioms:

1. $|A\rangle + |B\rangle = |C\rangle$
2. $|A\rangle + |B\rangle = |B\rangle + |A\rangle$
3. $\{|A\rangle + |B\rangle\} + |C\rangle = |A\rangle + \{|B\rangle + |C\rangle\}$
4. $|A\rangle + 0 = |A\rangle$
5. $|A\rangle + (-|A\rangle) = 0$
6. If z is a complex number.
   $z|A\rangle = |zA\rangle = |C\rangle$
7. If z and w are complex numbers.
   $z\{|A\rangle + |B\rangle\} = z|A\rangle + z|B\rangle$
   $\{z + w\}|A\rangle = z|A\rangle + w|B\rangle$

Functions and Column Vectors

The ket-vector $|A\rangle$ can be represented as column vectors, for example a two-dimensional column vector with two complex numbers as components.

$$|A\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

Column vectors can be added or multiplied by a complex number z.

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} + \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 + \gamma_1 \\ \alpha_2 + \gamma_2 \end{pmatrix}$$

$$z\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} z\alpha_1 \\ z\alpha_2 \end{pmatrix}$$

Bras and Kets

As we saw, a complex number z has a complex conjugate z^*, complex vector spaces have, as well, a complex conjugate vector space composed of bra-vectors $\langle A|$. Bra-vectors follow the same axioms mention before for ket-vectors with an addition.

1. The bra corresponding to $z|A\rangle$ is $\langle A|z^*$.
2. If $|A\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$, its corresponding bra is $\langle A| = (\alpha_1^* \quad \alpha_2^*)$

Inner Products

The inner product for bras and kets is an analogous operation to the dot product between ordinary vectors and its written with this notation: $\langle B|A\rangle$

If $|A\rangle$ and $\langle B|$ are represented as column vectors the inner product is defined the following way:

$$\langle B|A\rangle = (\beta_1^* \quad \beta_2^*)\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \beta_1^*\alpha_1 + \beta_2^*\alpha_2$$

The axioms for inner product are:

1. $\langle C|\{|A\rangle + |B\rangle\} = \langle C|A\rangle + \langle C|B\rangle$
2. $\langle B|A\rangle = \langle A|B\rangle^*$

- ✓ Normalized Vector: $|A\rangle$ is a normalized vector if $\langle A|A\rangle = 1$
- ✓ Orthogonal Vector: $|A\rangle$ and $|B\rangle$ are orthogonal if $\langle B|A\rangle = 0$

Orthonormal Bases

The dimension of a space is the number or orthogonal vectors in that space or the number of components on a column vector. An orthonormal basis is an orthogonal basis where all the vectors have unit-length.

If $|i\rangle$ and $|j\rangle$ are two orthonormal bases, to find the components of a ket-vector $|A\rangle = \alpha_1|i\rangle + \alpha_2|j\rangle$ we calculate the inner product of $|A\rangle$ with each of the basis.

$$\langle i|A\rangle = \alpha_1\langle i|i\rangle + \alpha_2\langle i|j\rangle = \alpha_1$$

$$\langle j|A\rangle = \alpha_1\langle j|i\rangle + \alpha_2\langle j|j\rangle = \alpha_2$$

Lecture 2. Quantum States

Representing Spin States as State-vectors

There are two spin states oriented along each of the coordinate axis. Along the z axis the A apparatus can prepare the state of the spin as σ= +1 or σ= -1, we will label each of these states as up $|u\rangle$ and down $|d\rangle$ respectively. Similarly, when the apparatus is oriented along the x axis, it can prepare the states right $|r\rangle$ and left $|l\rangle$ and when is oriented along the y axis, it prepares in $|i\rangle$ and out $|o\rangle$. All these spin states can be represented in a two-dimensional vector space.

Choosing two basis vectors arbitrarily we can write a generic state as a linear superposition of these vectors, for example:

$$|A\rangle = \alpha_u|u\rangle + \alpha_d|d\rangle$$

α_u and α_d (complex numbers) are the components of the state along the basis directions, these can be calculated by using the inner product for each of the basis as shown before (orthonormal bases).

$|A\rangle$ can represent any state of the spin, α_u and α_d don't represent anything by themselves, but their magnitudes do.

If the spin was prepared in the state $|A\rangle$, and we proceed to measure with the apparatus along the z axis, the value $\alpha_u\alpha_u^*$ is the probability of the spin being up. In the same way $\alpha_d\alpha_d^*$ is the probability of the spin being down. These probabilities can be calculated the following way:

$$P_u = \langle A|u\rangle\langle u|A\rangle \qquad P_u + P_d = 1$$

$$P_d = \langle A|d\rangle\langle \quad \text{Because } |A\rangle \text{ is normalized}$$

An important thing to remember is that, while it's true that up and down are not orthogonal directions in space, in quantum mechanics they are, which means that if a spin is set up, the probability to measure it down is zero and vice versa.

Since $|A\rangle$ can be any generic state, it is possible to represent $|r\rangle$ and left $|l\rangle$ as a linear combination of up and down. From the experiment with the apparatus A, if the $|r\rangle$ state is set and then we measure along the z axis, the result is randomly +1 or -1. By calculating the average of subsequent measurements, we see that 50% of the time we get +1 and the other 50%, -1. Thus, $\alpha_u\alpha_u^*$ and $\alpha_d\alpha_d^*$ must be ½.

$$|r\rangle = \frac{1}{\sqrt{2}}|u\rangle + \frac{1}{\sqrt{2}}|d\rangle$$

Likewise up and down, the directions right $|r\rangle$ and left $|l\rangle$ are orthogonal, which means that if the spin is right it has zero probability of being left and vice versa. We express $|l\rangle$ as:

$$|l\rangle = \frac{1}{\sqrt{2}}|u\rangle - \frac{1}{\sqrt{2}}|d\rangle$$

Using the same reasoning as before we can obtain the states: in $|i\rangle$ and out $|o\rangle$, as linear combinations of up $|u\rangle$ and down $|d\rangle$.

$$|i\rangle = \frac{1}{\sqrt{2}}|u\rangle + \frac{i}{\sqrt{2}}|d\rangle$$

$$|o\rangle = \frac{1}{\sqrt{2}}|u\rangle - \frac{i}{\sqrt{2}}|d\rangle$$

As before, in $|i\rangle$ and out $|o\rangle$ are orthogonal.

Representing Spin States as Column Vectors

Facing the need to perform future calculations we have to write the state-vectors in column form. Even though there are many options for unit length and mutually orthogonal vectors, it is better to choose the simplest ones. Choosing first up $|u\rangle$ and down $|d\rangle$ as

$$|u\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |d\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

is easier to write right $|r\rangle$, left $|l\rangle$, in $|i\rangle$ and out $|o\rangle$.

$$|r\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \qquad |l\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad |i\rangle = \begin{pmatrix} \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} \qquad |o\rangle = \begin{pmatrix} \frac{i}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{pmatrix}$$

Lecture 3. Quantum Mechanics Principles.

Mathematical Approach

First, I should clarify some recurrent concepts we will use from now on. Quantum sates (in which most of the applications we will later see are based on) are represented by vectors, not as a mathematical object with a magnitude and an orientation, but as an object to store information. These vectors will correspond to a vector space which neither fit is classical version, and which is known as Hilbert space. We will refer to classical vectors as 2-vectors from now on..

Observables are the things we measure and, despite the fact that they are also associated to vector spaces, they are not state vectors and they are represented by linear operators (matrices).

This way, we could represent a measurement over a ket-vector as follows:

$$\boldsymbol{M}|A\rangle = |B\rangle$$

It could be interpreted as the system being in state $|A\rangle$ and after measuring, it goes to state $|B\rangle$.

It is reasonable to think that as a linear operator, it will fulfil the two necessary properties of every linear system/function:

- ✓ Scalar product: $z * \boldsymbol{M}|A\rangle = z * |B\rangle$ with z being any complex number
- ✓ Distributive: $\boldsymbol{M}(|A\rangle + |B\rangle) = \boldsymbol{M}|A\rangle + \boldsymbol{M}|B\rangle$

$\boldsymbol{M}$ matrix dimension will depend on the vector space we are working with.

We shall realise the importance of these equations as mathematical objects since through them, we have a powerful and well-known weapon to study a branch of physics very unknown compared to other branches.

Eigenvectors and Eigenvalues

Typically, when a linear operator acts on a vector, the result is a vector with an arbitrary direction (not in the sense of quantum mechanics). However, in some situations, the resulting vector is the same vector the linear operator acted on but multiplied by a scalar. If this happens, the vector, the linear operator acts on, is an eigenvector and the value that multiplies this vector is the associated eigenvalue. We represent eigenvector like $|\lambda\rangle$ and their associated eigenvalues as λ. When this happens, the measurement can be expressed as:

$$\boldsymbol{M}|\lambda\rangle = \lambda * |\lambda\rangle$$

Linear operators can also act on bra-vectors:

$$\langle A|\boldsymbol{M}^{\dagger} = \langle B|$$

and if $|A\rangle = |\lambda\rangle$:

$$\langle\lambda|\boldsymbol{M}^{\dagger} = \langle\lambda| * \lambda^{*}$$

Where super index † shows the Hermitian of $\boldsymbol{M}$ which is equivalent to saying $[\boldsymbol{M}^{T}]^{*}$ where conjugation will be applied element-by-element.

Hermitian Operators

We are talking about a Hermitian operator when:

$$\boldsymbol{M}^{\dagger} = \boldsymbol{M}$$

In other words, when the transposed matrix element-by-element conjugated is equal to the original matrix. There is clearly a reason to properties of Hermitian operators being so useful. In this case it is that eigenvalues of Hermitian operator are always real.

This is quite useful in this filed because when we measure a quantum system using an apparatus, what this apparatus gives to us is nothing but the eigenvector of the linear operator "we are using", I mean, if we were measuring the spin along the x component, what we would obtain is one of the eigenvalues of the linear operator σ_x. As seen in

previous lectures, after every measurement of a spin we will get either or a +1 or a -1. This case, the eigenvalues of σ_x will be +1 y -1.

Any measurement device will give us either +1 or -1 which are, clearly, real numbers. This is quite reasonable because an apparatus like this measures a physical magnitude, so it would be confusing if we got a complex number since they are only an abstraction to make complex mathematical problems easier. It is worth noticing that according to this, the values we get are restricted to a certain set of values. In the spin case, we will only obtain +1 or -1. However, this is not exclusive of spin since measuring the energy of an atom will always report us a certain value of a possible set.

That is why we are so interested in Hermitian operators, because their eigenvalues (the values we get) are always real.

This property is quite simple to prove:

$$\boldsymbol{M}|\lambda\rangle \;=\; \lambda * |\lambda\rangle$$

and:

$$\langle\lambda|\boldsymbol{M}^{\dagger} \;= \langle\lambda| * \lambda^{*}$$

Using the fact that $\boldsymbol{M}$ is an Hermitian operator, $\boldsymbol{M} \;=\; \boldsymbol{M}^{\dagger}$, and multiplying the first equation by $\langle\,\lambda|$ and the second by $|\lambda\rangle$ we will get:

$$\langle\lambda|\boldsymbol{M}|\lambda\rangle \;=\; \lambda * \langle\lambda|\lambda\rangle$$

and:

$$\langle\lambda|\boldsymbol{M}|\lambda\rangle \;=\; \lambda^{*} * \langle\lambda|\lambda\rangle$$

If the left part of both equations is equal, then the right must be so. So $\lambda \;=\; \lambda^{*}$, a characteristic only fitted by real numbers.

The Fundamental Theorem

In this section I will explain the most important points of the fundamental theorem as well as the huge importance of this theorem.

The fundamental theorem firstly says that eigenvectors of a linear operator establish a basis that is able to generate every possible vector resulting from the application of that linear operator. In other words, every vector resulting from the application of the linear operator could be expressed in terms of these eigenvectors.

In addition, if λ_1 and λ_2 are different, their corresponding eigenvector will be orthogonal each other. This could be demonstrated by:

$$\langle\lambda_1|\boldsymbol{M} = \lambda_1 * \langle\lambda_1|$$

and:

$$\boldsymbol{M}|\lambda_2\rangle = \lambda_2 * |\lambda_2\rangle$$

Multiplying the first equation by $|\lambda_2\rangle$ and the second by $\langle\lambda_1|$ we get:

$$\langle\lambda_1|\boldsymbol{M}|\lambda_2\rangle = \lambda_1 * \langle\lambda_1|\lambda_2\rangle$$

$$\langle\lambda_1|\boldsymbol{M}|\lambda_2\rangle = \lambda_2 * \langle\lambda_1|\lambda_2\rangle$$

if we subtract both equations:

$$(\lambda_1 - \lambda_2) * \langle\lambda_1|\lambda_2\rangle = 0$$

So, if we assumed $\lambda_1 \neq \lambda_2$, then $|\lambda_1\rangle$ and $|\lambda_2\rangle$ must be orthogonal.

Even if they were equal, their corresponding eigenvector could be expressed in terms of an orthogonal basis. This situation is known as degeneracy. This situation can evidently be proven:

$$|A\rangle = \alpha_1|\lambda_1\rangle + \alpha_2|\lambda_2\rangle$$

Using the distributive property mentioned before:

$$M|A\rangle = M(\alpha_1|\lambda_1\rangle + \alpha_2|\lambda_2\rangle = \alpha_1 * M|\lambda_1\rangle + \alpha_2 * M|\lambda_2\rangle$$

Then we would get:

$$M|A\rangle = \alpha_1 * \lambda|\lambda_1\rangle + \alpha_1 * \lambda|\lambda_2\rangle = \lambda * (\alpha_1|\lambda_1\rangle + \alpha_2|\lambda_2\rangle) = \lambda|A\rangle$$

From where we could deduce that any combination of two eigenvectors with equal eigenvalues will also be an eigenvector of the linear operator with the same eigenvalue. We will assume that both eigenvectors despite the fact of having the same eigenvalue, are linearly independent, other way they would represent the same state.

Finally, this theorem proves that if the vector space is N-dimensional, then there will be N linearly independent eigenvectors. This is due to the fact that if the set of eigenvectors from a linear operator sets a basis for every vector resulting from the application of that linear operator, is well-known that N vectors are needed to generate every vector in an N-dimensional vector space.

Quantum Mechanics Principles

I will now list the four principles of quantum mechanics, even though they have already been explained before:

1. Observables are represented by linear operators.
2. Possible results of a measurement are the eigenvalues of the linear operator.
3. Orthogonal vectors represent mutually exclusive states. This is, if we know a system is in state A, we definitely know it is not in state B. For example, up and down are represented by orthogonal vectors since if we measured the spin along the z axis, we would get either +1 or -1, which will set up or down and completely discard the opposite. However, up and left (for example) are not orthogonal states since if the spin was prepared left, measuring along de z component and obtaining +1 would not confirm up and discard left, since in this case

we would have obtained +1 or -1 with a probability of 0.5 We could assert the state is up and definitely now down though (if we obtained a +1).

4. If a system is in state $|A\rangle$ and we want to know the probability of obtaining a certain eigenvalue λ_i,we shall compute the squared magnitude of the product between ket $|A\rangle$ and the eigenvector associated to that eigenvalue:

$$P(\lambda_i) = \langle\lambda_i|A\rangle\langle A|\lambda_i\rangle$$

Pauli Matrices

In this section I will show how Pauli matrices are built. These matrices are linear operators used to represent the measurement of the spin along one of the three main directions of space x,y,z.

I will start with the linear operator corresponding to the z axis

$$\sigma_z = \begin{pmatrix} \sigma_{z_{11}} & \sigma_{z_{12}} \\ \sigma_{z_{21}} & \sigma_{z_{22}} \end{pmatrix}.$$

We know we always get +1 or -1 when measuring the spin, so we already know the eigenvalues of the linear operator. We also know when we measure up, we obtain +1 and when measuring down we get -1 so we already know the eigenvectors associated to these eigenvalues. So, having this into account we can set an equation system which result will be our first Pauli matrix:

$$\sigma_z|u\rangle = +1\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix} \sigma_{z_{11}} & \sigma_{z_{12}} \\ \sigma_{z_{21}} & \sigma_{z_{22}} \end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix} \sigma_{z_{11}} * 1 + \sigma_{z_{12}} * 0 \\ \sigma_{z_{21}} * 1 + \sigma_{z_{22}} * 0 \end{pmatrix} = \begin{pmatrix} \sigma_{z_{11}} \\ \sigma_{z_{21}} \end{pmatrix}$$

We obtain from this that $\sigma_{z_{11}} = 1$ and $\sigma_{z_{21}} = 0$.

$$\sigma_z|d\rangle = -1\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix} \sigma_{z_{11}} & \sigma_{z_{12}} \\ \sigma_{z_{21}} & \sigma_{z_{22}} \end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix} \sigma_{z_{11}} * 0 + \sigma_{z_{12}} * 1 \\ \sigma_{z_{21}} * 0 + \sigma_{z_{22}} * 1 \end{pmatrix} = \begin{pmatrix} \sigma_{z_{12}} \\ \sigma_{z_{22}} \end{pmatrix}$$

It is easy to see that $\sigma_{z_{22}} = -1$ and $\sigma_{z_{12}} = 0$. Therefore:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The process to get σ_x y σ_y is the same. In order to obtain σ_x we remind:

$$|r\rangle = \frac{1}{\sqrt{2}}|u\rangle + \frac{1}{\sqrt{2}}|d\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

$$|l\rangle = \frac{1}{\sqrt{2}}|u\rangle - \frac{1}{\sqrt{2}}|d\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

Repeating matricial operations done in the case of σ_z :

$$\sigma_x|r\rangle = +1\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \sigma_{x_{11}} & \sigma_{x_{12}} \\ \sigma_{x_{21}} & \sigma_{x_{22}} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \sigma_{x_{11}} * 1/\sqrt{2} + \sigma_{x_{12}} * 1/\sqrt{2} \\ \sigma_{x_{21}} * 1/\sqrt{2} + \sigma_{x_{22}} * 1/\sqrt{2} \end{pmatrix}$$

$$= \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

$$\sigma_x|l\rangle = -1\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \sigma_{x_{11}} & \sigma_{x_{12}} \\ \sigma_{x_{21}} & \sigma_{x_{22}} \end{pmatrix}\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

$$= \begin{pmatrix} \sigma_{x_{11}} * 1/\sqrt{2} - \sigma_{x_{12}} * 1/\sqrt{2} \\ \sigma_{x_{21}} * 1/\sqrt{2} - \sigma_{x_{22}} * 1/\sqrt{2} \end{pmatrix} = -1\begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

We get the following equation system:

$$\begin{cases} \sigma_{x_{11}} * 1/\sqrt{2} + \sigma_{x_{12}} * 1/\sqrt{2} = 1/\sqrt{2} \\ \sigma_{x_{11}} * 1/\sqrt{2} - \sigma_{x_{12}} * 1/\sqrt{2} = -1/\sqrt{2} \end{cases}$$

$$\begin{cases} \sigma_{x_{21}} * 1/\sqrt{2} + \sigma_{x_{22}} * 1/\sqrt{2} = 1/\sqrt{2} \\ \sigma_{x_{21}} * 1/\sqrt{2} - \sigma_{x_{22}} * 1/\sqrt{2} = 1/\sqrt{2} \end{cases}$$

From the first system we get $\begin{cases} \sigma_{x_{11}} = 0 \\ \sigma_{x_{12}} = 1 \end{cases}$ and from the second $\begin{cases} \sigma_{x_{21}} = 1 \\ \sigma_{x_{22}} = 0 \end{cases}$ so:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Obtaining σ_y is exactly the same. If we remind this:

$$|i\rangle = \frac{1}{\sqrt{2}}|u\rangle + \frac{j}{\sqrt{2}}|d\rangle = \begin{pmatrix} 1/\sqrt{2} \\ j/\sqrt{2} \end{pmatrix}$$

$$|o\rangle = \frac{1}{\sqrt{2}}|u\rangle - \frac{j}{\sqrt{2}}|d\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -j/\sqrt{2} \end{pmatrix}$$

we would finally get:

$$\sigma_y = \begin{pmatrix} 0 & -j \\ j & 0 \end{pmatrix}$$

Despite the importance of these three matrices, they are not enough because we could want to measure the spin along an arbitrary direction of space. The fact that we are working with linear operators allows us to linearly combine them in order to obtain a new linear operator so that we can represent the measurement of the spin along any direction of space. This way, we manage to get a linear operator to represent the measurement of the spin along an arbitrary direction $\vec{n}$:

$$\sigma_n = n_z\sigma_z + n_x\sigma_x + n_y\sigma_y = \begin{pmatrix} n_z & n_x - jn_y \\ n_x + jn_y & -n_z \end{pmatrix}$$

It is worth noting that $\vec{n}$ will be an unitary vector since we are only interested in its direction.

However, we would need the eigenvector and eigenvalues of this linear operator if we wanted to know the possible outcomes of the measurements or the probability to obtain a certain value.

Average value of a Linear Operator

As seen in the first chapter, if we prepare the spin in a certain direction of space and we measure in an orthogonal direction, we will always get either +1 or -1. However, this series of 1s whit changing signs is distributed in such a way that the total average of the successive measurements is 0, the result we would expect from a classical measure. If we measured in a direction forming a θ with that in which the spin is prepared, the average of those -1s and 1s would be $cos(\theta)$.

The average value of a linear operator fits with the previous value. It is expressed as $\langle M \rangle$ and it is calculated as follows:

$$\langle M \rangle = \sum_i P(\lambda_i) * \lambda_i$$

This way if we had a spin prepared along z axis and we wanted to measure it along a direction laying in XZ plane forming a θ angle with z axis, we would get:

$$\vec{n} = sin(\theta)\vec{x} + 0\vec{y} + cos(\theta)\vec{z}$$

$$\sigma_n = \begin{pmatrix} cos(\theta) & sin(\theta) \\ sin(\theta) & -cos(\theta) \end{pmatrix}$$

This linear operator will have therefore the following eigenvalues and eigenvectors:

$$\lambda_1 = 1 \; y \; |\lambda_1\rangle = \begin{pmatrix} cos(\theta/2) \\ sin(\theta/2) \end{pmatrix}$$

$$\lambda_2 = -1 \; y \; |\lambda_2\rangle = \begin{pmatrix} -sin(\theta/2) \\ cos(\theta/2) \end{pmatrix}$$

Supposing the spin is in the up state, the probability of obtaining each eigenvalue will be:

$$P(\lambda_i) = \langle \lambda_i | u \rangle \langle u | \lambda_i \rangle$$

According to his, the average value of σ_n will be:

$$\langle \sigma_n \rangle = \sum_i P(\lambda_i) * \lambda_i$$

$$= 1((\cos(\theta/2)^2 * 1 + (\sin(\theta/2)^2 * 0) - 1((\sin(\theta/2)^2 * 1$$

$$+ (\cos(\theta/2)^2 * 0) = \cos(\theta/2)^2 - (\sin(\theta/2)^2 = cos(\theta)$$

Which is the expected outcome as said before.

Chapter II. Quantum Cryptography Demonstration Kit

The following section is a summarize of the functioning of a Quantum Cryptography Demonstration Kit used to simulate, using light pulses, how an actual quantum channel would generate the encryption key. [2]

This kit simulates the functioning of the BB84 protocol using a pulse laser instead of individual photons. Even though the setup works with classical physics, the functioning is the same as in quantum physics, making it a very good analogous experiment.

Encryption is a process that transforms a message into unreadable text, that can only be understood by a sender and a receiver that share a secret key. The security of the key is based on how hard it is to solve the algorithms use to generate it. Classical cryptography has the disadvantage that there is no way to know if the key will get hacked at some point.

The basic principles of quantum mechanics solve this problem for two reasons: first, the act of observing the state of a particle disrupts the state, and second, quantum physics allows the generation of a key composed of true random numbers.

The One-Time Pad

Is a classical technique that consists on using a key to encrypt a message, just once. If some requirements are met, the technique is 100% secure [19]. Quantum physics helps meet these requirements:

1. The key is at least as long as the message.
2. The key must be only used once.
3. The must be completely random.
4. The key must be known only by the sender and the receiver.

To encrypt a message, we take its binary representation and the key (also a string of 0's and 1's) and perform a binary addition, according to the following rules:

A	B	A + B
0	0	0
0	1	1
1	0	1
1	1	0

To decrypt it, the receiver performs the same binary addition using the encrypted message and the key, as shown:

Message to transmit	T					E					S					T				
Message in bits	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
+																				
Key	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
↓																				
Encrypted message	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
+																				
Key	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
↓																				
Message in bits	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
Message to transmit	T					E					S					T				

Key Distribution

The idea of this section is to explain how to use the experimental setup to transmit data with one basis, even though actual quantum cryptography usually works with two. Alice, the transmitter, has a λ/2 plate that rotates the polarization of the incident light by double the physical rotation of the plate, this means that a plate rotated 45 degrees will polarize the light by 90 degrees. A photon polarized horizontally is interpreted as a "0" and a photon polarized vertically is interpreted as a "1".

The receiver, Bob, consists of a polarizing beamsplitter cube and two sensors. If Alice sends a "0" (horizontal polarization) the photon passes through the beamsplitter and goes into the sensor detecting the bit, if she sends a "1" (vertical polarization) the light gets reflected and goes into the other sensor.

Adding Another Basis

We will now distinguish the basis with 0^o and 90^o, calling it the "+ basis", and the basis with -45^o and 45^o, calling it the "x basis". With this addition, Alice can send bits following the next configurations of the polarization plate:

- ✓ A 0 with the + basis means setting a 0^o.
- ✓ A 1 with the + basis means setting a 90^o.
- ✓ A 0 with the x basis means setting a -45^o.
- ✓ A 1 with the x basis means setting a 45^o.

An important thing to clarify is that when we talk about setting angles, we are referring to the rotation angle of the polarization and not the physical rotation of the $\lambda/2$ plate.

If Bob chooses the same basis as Alice, he will obtain a true measurement of the bit. If not, he will obtain a "0" or a "1" with a 50% of probability each.

To finally agree on a key, Alice and Bob will tell each other which basis, x or +, they used for each measurement. If the two are different, both Alice and Bob will discard that measurement. But, if they match, Alice and Bob will save that bit as part of the key.

The moment they finish comparing basis, each of them will be in possession of the secret key. To start the transmission of information Alice encrypts the message and sends it to Bob in the + basis. Bob reads the message with the + basis so he is able to decrypt it.

Detection of an Eavesdropper

The eavesdropper, Eve, is placed between Alice and Bob to try to measure the light coming from Alice and then attempt to retransmit that same information to Bob. Eve also chooses a random set of bases to measure, according to these choices we can see different outcomes:

- ✓ If Eve chooses the same basis as Alice, she will be able to measure and send the information correctly to Bob with the same basis used by Alice. Now Bob has two possibilities:
    - ✓ If Bob chooses the same basis as Alice, he will read correctly the signal sent by Eve without him noticing the presence of the eavesdropper.
    - ✓ If Bob chooses a different basis, he will obtain a random result, but in the end, Eve will not be noticed since Alice and Bob will discard that measurement after comparing basis.
- ✓ If Eve chooses different basis, her sensors will respond randomly, giving her the wrong measurement 50% of the time. Since she doesn't know whether the measurements are right or wrong, she will send the bits she obtained with the basis she originally chose. Bob also has two possibilities:
    - ✓ If Bob chooses a different basis than Alice, the measurement will be discarded.
    - ✓ If Bob chooses the same basis as Alice, an error may occur allowing Alice and Bob to detect Eve. Because of Eve's interference Bob will read the bit as Alice sent it half of the time.

To summarize this last case, we see that, even though Alice and Bob have chosen the same basis they obtain different bit. Through a simple test, Alice and Bob can see if there has been and eavesdropper. After generating the secret key, they choose some bits and share them through a public channel. If 25% or more of the bits don't match, the communication was interfered by a third party.

What is a Random Number?

Pseudorandom numbers created by traditional computers do not ensure total security referring to some encryption algorithms. Quantum mechanics provides a solution for this. As an example, a particle such as an electron, which arrives a non-polarizing beamsplitter, is either transmitted or reflected with a probability of 0.5 each. This is not the only totally random process, other processes such as radioactive breaking up is also fully random.

What Prevents from Copying Transmitted Information?

Someone could think hacking a system like this could be easy. Simply, an eavesdropper, Eve, could take the photon carrying the information and duplicate it to send it to Bob. However, this is not possible because of the no-cloning theorem which asserts it is impossible to measure a quantum system without disturbing it in some way.

Experiment

This experiment is based on the BB84 protocol. Forwardly, its steps are detailed:

1. As a first step we have the transmission of the key. Alice chooses randomly between the two possible basis (x or +) and the bit she wants to send. Bob also chooses randomly the basis he is going to measure with. The choice of both bases is carried out by a polarizer the both ends of the communication has on their plates. This step is repeated several times, being both ends able to change their basis whenever they want.
2. Through a classic channel Alice and Bob exchange basis and keep those bits where both used the same basis.
3. Alice and Bob choose some of these bits and exchange them in order to detect eavesdropping. If these bits fit each other, then no eavesdropping is detected, so these test bits are removed from the key and the remaining ones will define the final key. In the other hand, if the bits do not match, then eavesdropping has been detected and the protocol is aborted

4. Alice encrypts the message with the key both ends generated.
5. Alice sends the message to Bob using the classic channel.
6. Bob decrypts the message using the key.

Classic Light vs Single photons

Lasers (sources) used in this set-up do not generate individual photons so this system could not be implemented as a reliable quantum cryptography system. This results from the fact that if we faced a technologically super advanced eavesdropper (it is sensible thinking this), Eve could take a sample from the flow of electrons to take the information, leaving the rest arrive Bob undisturbed so that both ends could never detect eavesdropping.

This weakness is very common among quantum crypto protocols because it is really hard to build ideal sources.

Mathematical Description: Dirac's Notation

In this experiment there are four possible states which can be expressed in Dirac's notation, as follows:

$$|-45^o\rangle$$

$$|0^o\rangle$$

$$|45^o\rangle$$

$$|90^o\rangle$$

First and third build up the x basis, while second and fourth build up the + basis. These representations indicate the angle formed by the direction in which the photon vibrates in respect to the vertical component.

It is reasonable taking state vectors which are orthogonal to each other because other way, transmitting a 0 would not mean undoubtedly not having transmitted a 1. This way:

$$|0^o\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$

$$|90^o\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

If we take a photon with $|45^o\rangle$ polarization, the probability to obtain 1 or 0 measuring in the + basis would be 0.5. We also know this state vector can be expressed in terms of the opposite basis so that:

$$|45^o\rangle = \alpha|0^o\rangle + \beta|90^o\rangle$$

According to the Law of Total Probability, the probability of being $|45^o\rangle$ and measuring 1 in the + basis plus the probability of measuring 0 must be equal to 1. According to this:

$$\langle 0^o|45^o\rangle\langle 45^o|0^o\rangle + \langle 90^o|45^o\rangle\langle 45^o|90^o\rangle = \alpha^2 + \beta^2 = 1$$

Because of symmetry:

$$\alpha = \beta = \frac{1}{\sqrt{2}}$$

$$|45^o\rangle = \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}$$

We already know that the states $|45^o\rangle$ and $|-45^o\rangle$ must be orthogonal each other for the same reason that $|0^o\rangle$ and $|90^o\rangle$, so state $|-45^o\rangle$ is represented as follows:

$$|-45^o\rangle = \begin{pmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{pmatrix}$$

We could also have chosen $|45^o\rangle$ and $|-45^o\rangle$ as our basis. $|0^o\rangle$ and $|90^o\rangle$ could, this way, have been expressed in terms of this new basis. The process to obtain them would be analogous.

Measurements can be represented mathematically through linear operators. A measurement in the + basis is represented by the $\boldsymbol{M}_+$ operator. If the photon vibrates in the direction corresponding to 0º (a 0 is transmitted using + basis) we could represent this measurement like this:

$$M_+|0^o\rangle = |0^o\rangle\langle 0^o|0^o\rangle - |90^o\rangle\langle 90^o|0^o\rangle = |0^o\rangle$$

As we can see, the first addend gives us $|0^o\rangle$ because the square module of $|0^o\rangle$ is 1 (we are using an orthonormal basis) while the second addend collapses to 0 due to the fact that the elements of the basis are orthogonal each other. We can realize now that $|0^o\rangle$ is an eigenvector of M_+ which has +1 as the associated eigenvalue.

If a 1 using + basis was transmitted and we were measuring with the x basis, we would get $-|90^o\rangle$. This means $|90^o\rangle$ is the other eigenvector of M_+ with -1 as the associated eigenvalue.

If we were using x basis, the results would be analogous:

$|45^o\rangle$ eigenvector of M_x with +1 as the associated eigenvalue.

$|-45^o\rangle$ eigenvector of M_x with -1 as the corresponding eigenvalue.

We should analyse the case in which we measure a state using the opposite linear operator. Let's show it with the case in which we transmit 1 in x basis ($|45^o\rangle$) and measuring in the + basis (mathematically M_+). This measurement could be represented as follows:

$$M_+|45^o\rangle = |0^o\rangle\langle 0^o|45^o\rangle - |-90^o\rangle\langle 90^o|45^o\rangle = \frac{1}{\sqrt{2}}|0^o\rangle - \frac{1}{\sqrt{2}}|90^o\rangle$$

We should clarify this result because it would be intuitive thinking that after carrying out the measurement in + basis of a 0 transmitted using x basis, the resulting state would be a little $|0^o\rangle$ and a little $|90^o\rangle$. However, the previous result is the probability of measuring 1 or 0. I mean, the beamsplitter will transmit or reflect the photon with a probability of 0.5, but it will never transmit and reflect it at the same time. According to this, the probability of receiving a 0 will be:

$$|A\rangle = \frac{1}{\sqrt{2}}|0^o\rangle - \frac{1}{\sqrt{2}}|90^o\rangle$$

$$P(0) = \langle 0^o|A\rangle\langle A|0^o\rangle = \frac{1}{2}$$

The probability of measuring a 1 will be the same.

The whole experiment without eavesdropping is summarized in the next chart:

ALICE		**BOB**		
STATE	**Basis, bit**	**Basis**	**State**	**Bit**
$\|\mathbf{0^o}\rangle$	+,0	+	$M_+\|0^o\rangle = \|0^o\rangle$	0
		x	$M_x\|0^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle - \frac{1}{\sqrt{2}}\|-45^o\rangle$	0 o 1 al 50%
$\|\mathbf{90^o}\rangle$	+,1	+	$M_+\|90^o\rangle = -\|90^o\rangle$	1
		x	$M_x\|90^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle + \frac{1}{\sqrt{2}}\|-45^o\rangle$	0 o 1 al 50%
$\|\mathbf{45^o}\rangle$	x,1	+	$M_+\|45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle - \frac{1}{\sqrt{2}}\|90^o\rangle$	0 o 1 al 50%
		x	$M_x\|45^o\rangle = \|45^o\rangle$	1
$\|\mathbf{-45^o}\rangle$	x,0	+	$M_+\|-45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle + \frac{1}{\sqrt{2}}\|90^o\rangle$	0 o 1 al 50%
		x	$M_x\|-45^o\rangle = -\|-45^o\rangle$	0

Green cases show when Alice and Bob have used the same basis, so without eavesdropping, the bit transmitted by Alice will be the same as the bit measured by Bob.

ALICE		EVE			BOB		
BASIS, BIT	**State**	**Basis**	**State**	**Sent State**	**Basis**	**State**	**Read Bit**
+,0	$\|0^o\rangle$	+	$M_+\|0^o\rangle = \|0^o\rangle$	$\|0^o\rangle$	+	$M_+\|0^o\rangle = \|0^o\rangle$	0
					x	$M_x\|0^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle - \frac{1}{\sqrt{2}}\|-45^o\rangle$	0 o 1 al 50%
		x	$M_x\|0^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle - \frac{1}{\sqrt{2}}\|-45^o\rangle$	$\|45^o\rangle$ o $\|-45^o\rangle$ al 50%	+	$M_+\|\pm 45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle \mp \frac{1}{\sqrt{2}}\|90^o\rangle$	0 o 1 al 50%
					x	$M_x\|45^o\rangle = \|45^o\rangle$ o $M_x\|45^o\rangle = -\|-45^o\rangle$	1(case 1) 0(case 2)
+,1	$\|90^o\rangle$	+	$M_+\|90^o\rangle = -\|90^o\rangle$	$\|90^o\rangle$	+	$M_+\|90^o\rangle = -\|90^o\rangle$	1
					x	$M_x\|90^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle + \frac{1}{\sqrt{2}}\|-45^o\rangle$	0 o 1 al 50%
		x	$M_x\|90^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle + \frac{1}{\sqrt{2}}\|-45^o\rangle$	$\|45^o\rangle$ o $\|-45^o\rangle$ al 50%	+	$M_+\|\pm 45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle \mp \frac{1}{\sqrt{2}}\|90^o\rangle$	0 o 1 al 50%
					x	$M_x\|45^o\rangle = \|45^o\rangle$ o $M_x\|45^o\rangle = -\|-45^o\rangle$	1(case 1) 0(case 2)
X,1	$\|45^o\rangle$	+	$M_+\|45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle - \frac{1}{\sqrt{2}}\|90^o\rangle$	$\|0^o\rangle$ o $\|-90^o\rangle$ al 50%	+	$M_+\|0^o\rangle = \|0^o\rangle$ o $M_+\|90^o\rangle = -\|90^o\rangle$	0(case 1) 1(case 2)
					x	$M_x\|0^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle - \frac{1}{\sqrt{2}}\|-45^o\rangle$ $M_x\|90^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle + \frac{1}{\sqrt{2}}\|-45^o\rangle$	0 o 1 al 50%
		x	$M_x\|45^o\rangle = \|45^o\rangle$	$\|45^o\rangle$	+	$M_+\|45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle - \frac{1}{\sqrt{2}}\|90^o\rangle$	0 o 1 al 50%
					x	$M_x\|45^o\rangle = \|45^o\rangle$	1
X,0	$\|-45^o\rangle$	+	$M + \|-45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle + \frac{1}{\sqrt{2}}\|90^o\rangle$	$\|0^o\rangle$ o $\|-90^o\rangle$ al 50%	+	$M_+\|0^o\rangle = \|0^o\rangle$ o $M_+\|90^o\rangle = -\|90^o\rangle$	0(case 1) 1(case 2)
					x	$M_x\|0^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle - \frac{1}{\sqrt{2}}\|-45^o\rangle$ $M_x\|90^o\rangle = \frac{1}{\sqrt{2}}\|45^o\rangle + \frac{1}{\sqrt{2}}\|-45^o\rangle$	0 o 1 al 50%
		x	$M_x\|-45^o\rangle = -\|-45^o\rangle$	$\|-45^o\rangle$	+	$M_+\|-45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle + \frac{1}{\sqrt{2}}\|90^o\rangle$	0 o 1 al 50%
					x	$M_x\|-45^o\rangle = -\|-45^o\rangle$	0

In this chart, the grey cases correspond to Alice and Bob using different basis, so the effect of Eve would not be relevant because these bits would be removed from the key.

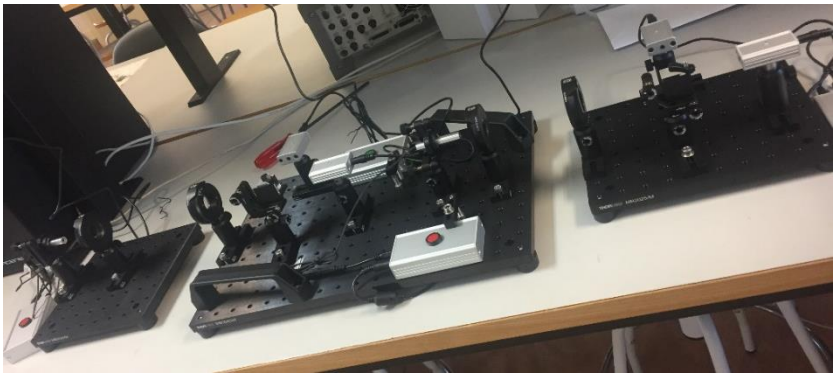
Green cases are those in which Alice, Eve and Bob use all the same basis, so Alice and Bob will have the same bits. In this case, Eve is not detected.

Finally, white cases are those in which Alice and Bob have same basis, but Eve's differs. Here is where eavesdropping could be detected with a probability of 0.5 (among these cases). Blue cases are those in which Eve is not detected while red ones are those in which eavesdropping is detected.

Chapter III. Experiments

Experiment 1. Standard Key Generation

To demonstrate the functioning of the Quantum Cryptography Demonstration Kit, we made an experiment where we repeat the process of generating a key, between Alice and Bob, ten times, while in the presence of an eavesdropper (Eve). We chose keys only 10-bits long.



Initially, Alice chooses a 10-bit long string of 0's and 1's as the key. We have simulated the transmission of that key using ten different and random sets of bases. Bob also chooses ten sets of bases randomly to measure each transmission from Alice. Lastly, Eve has chosen one set of bases she will use to measure the information coming from Alice, and then retransmit it to Bob.

ALICE	1	2	3	4	5	6	7	8	9	10
BASIS 1	+	+	+	X	X	+	X	+	X	X
BASIS 2	+	X	+	X	X	X	+	+	X	X
BASIS 3	+	+	X	+	+	+	X	X	X	+
BASIS 4	+	X	X	+	X	+	+	X	X	+
BASIS 5	+	X	X	+	+	X	+	X	X	+
BASIS 6	+	+	X	+	+	X	X	+	X	+
BASIS 7	+	+	X	+	X	X	X	+	X	X
BASIS 8	+	X	X	+	X	+	X	+	+	+
BASIS 9	+	X	X	+	+	+	+	+	X	+
BASIS 10	+	X	X	X	X	+	X	X	X	X
BITS	1	0	0	1	1	1	1	0	1	0

EVE	1	2	3	4	5	6	7	8	9	10
BASIS	X	X	+	X	+	+	+	+	X	X
READ 1	0	0	0	1	1	1	1	0	1	0
READ 2	0	0	0	1	0	1	1	0	1	0
READ 3	0	0	1	1	1	1	0	1	1	1
READ 4	0	0	1	1	0	1	1	0	1	0
READ 5	1	0	0	0	1	0	1	1	1	1
READ 6	0	0	0	1	1	0	1	0	1	1
READ 7	1	0	1	1	1	1	1	0	1	0
READ 8	1	0	0	0	0	1	1	0	1	1
READ 9	1	0	0	0	1	1	1	0	1	0
READ 10	1	0	1	1	0	1	1	0	1	0

BOB	1	2	3	4	5	6	7	8	9	10
BASIS 1	X	X	+	+	X	+	X	+	+	+
READ 1	0	0	0	1	0	1	0	0	1	0
BASIS 2	X	X	X	+	+	X	+	+	+	+
READ 2	0	0	1	1	0	0	1	0	1	0
BASIS 3	X	+	X	+	+	+	X	X	+	X
READ 3	0	0	0	1	1	1	1	0	1	1
BASIS 4	+	+	X	+	+	X	X	X	X	+
READ 4	0	0	0	0	0	0	0	0	1	0
BASIS 5	X	+	X	X	X	+	X	+	X	X
READ 5	1	0	0	0	0	0	1	1	1	1
BASIS 6	+	+	+	X	+	X	X	+	X	X
READ 6	1	1	0	1	1	1	1	0	1	1
BASIS 7	X	X	X	+	+	+	+	X	+	X
READ 7	1	0	1	0	1	1	1	0	0	0
BASIS 8	X	X	+	+	X	+	X	+	X	+
READ 8	1	0	0	0	1	1	1	0	1	0
BASIS 9	+	+	+	X	X	+	X	+	+	X
READ 9	1	0	0	0	1	1	0	0	0	0
BASIS 10	+	X	X	+	X	X	X	X	+	+
READ 10	0	0	1	1	0	1	1	0	1	1

Not coloured cases (white or grey) are those where Alice and Bob use different basis, so these ones do not matter when trying to detect eavesdropping since they are going to be discarded.

Basis coloured in blue (in Bob's chart) point out situations where the three of them share basis so what is transmitted by Alice is the same received by Bob. Obviously, Eve will not be uncovered.

Green boxes represent cases where Eve has been discovered. Here, Alice and Bob basis are the same, but Eve doesn't.

Orange cases happen when Alice and Bob have same basis and even though Eve does not, she is not detected.

These two previous cases take place when Eve has a different basis than Alice and Bob, so when she measures Alice, she will get either 0 or 1 with same probability, and Bob will also read 0 or 1 randomly. According to Bob's chart, Eve is caught thirteen times while she is unnoticed sixteen times, among those situations she could be caught almost 50% times each, which fits theory.

Even though we only caught Eve disturbing approximately half of the bits, we can see that, at least one bit is disrupted on eight out of the ten transmissions. Supposing no noise or channel errors, we have managed to caught Eve around 80% of the time.

Experiment 2. Testing Maximum Transmission Distance

To test the range of the laser, we tried to set Alice and Bob as far as possible to see if it was possible to transmit information correctly at a distance bigger than the one specified in the manual (60 cm).

At a distance of approximately 6 meters the laser started to scatter in a certain pattern, as shown in the picture:

The phenomenon we see is called “Fraunhofer’s Diffraction”, and it occurs when a flat wave stumbles upon a long and narrow slit. In our case the laser light must go through the little opening on the laser. As it scatters, the power in the centre is not enough for the receiver to detect it.

Chapter IV. Introduction to Quantum Cryptography.

Quantum cryptography was developed using classical cryptography methods as inspiration. To use these methods both parties communicating need to know a secret key, that must be exchanged prior to the communication, through a physical way. Up until recently the key trade was made through face-to-face meetings, a trusted third party or through another already existing encryption channel. But the arrival of quantum technologies has changed this transaction to a more secure one. [3]

Classical Methods

Public-key Systems

This system uses a pair of keys, one public and one private. The receiver's public key is used to encrypt a message and the receiver's private one is used to decrypt it. Even though the public key is widely known, and it's related to the private key, obtaining this last one is almost mathematically impossible [4]. Some of the most used systems currently:

- ✓ RSA: uses an algorithm based the mathematical difficulty of the factorization of the product of two large prime numbers [5].

- ✓ Diffie-Hellman: allows the two parties, that have no previous knowledge of each other, to jointly create the secret key using an insecure channel [6]. Each party chooses a public number and a secret number and performs mathematical operations with both public numbers and their secret one. After this, they exchange the result of the calculation through a public channel and use it, in combination with their secret number, to obtain the shared key through a formula. This has been a really used algorithm because of the great difficulty of reversing the calculation in order to find the secret numbers [7].

- ✓ Elliptic-curve cryptography (ECC): uses a mathematical algorithm based on elliptic curves equations ($y^2 = x^3 + Ax + B$). Initially, a point G from the curve and a private key number k are chosen. The public key P is calculated as $P = k \cdot G$. The security of this algorithm relies in the difficulty of deducing k from P [8].

Private-key Systems

This system uses the same key for encryption and decryption. This key must remain a shared secret between sender and receiver to ensure a private communication channel. The fact that both parties need to have access to the secret key is a disadvantage in comparison with public-key systems [9]. An example of this type of system is:

- ✓ Advanced encryption standard (AES): it encrypts by performing a series of transformations on the data stored in an array, i.e. changing every letter by its previous one on the alphabet. The message sent seems like a text of random characters that can only be decrypted by the receiver using the same transmission key [10].

Nowadays there are many ways people can get key information, eavesdroppers from within a company or the fast development of powerful malware are some of them. We also must consider that the endurance of this classic algorithms relies on the computing power and the mathematical knowledge we currently have. The moment a computer has the pattern and power to factorize the product of two large prime numbers, the RSA system will no longer be useful.

"To summarize that, modern cryptography is vulnerable to both technological progress of computing power and evolution in mathematics to quickly reverse one-way functions such as that of factoring large numbers" [11].

Because of this reason, scientist have tried to find a different type of cryptography that is immune to these problems. This has led to the development of quantum cryptography.

Principles of Quantum Cryptography

The goal of quantum cryptography is to use quantum mechanics properties to provide secure transmissions of information. To do this, it relies on two principles and a theorem:

- ✓ Principle of photon polarization: this principle states that a photon can be polarized in a certain direction.

- ✓ Heisenberg uncertainty principle: this principle states that there is uncertainty when measuring a variable of a particle. If a pair of particle properties are related, the act of measuring precisely one of them increases the uncertainty of the other one, making it impossible to know the exact value of both simultaneously [12].

- ✓ No-cloning theorem: demonstrated by William Wootters and Woicech Zurek in "a single quantum can't be cloned". This theorem states that it is impossible to create an exact copy of a random unknown quantum state [13].

The big difference between quantum cryptography and classic cryptography is that, through quantum mechanics properties, sender and receiver can agree on a key without having to meet in person or use a preexisting channel and be completely sure that the key is exclusively known by them.

Discrete-Variable Quantum Key Distribution Protocols

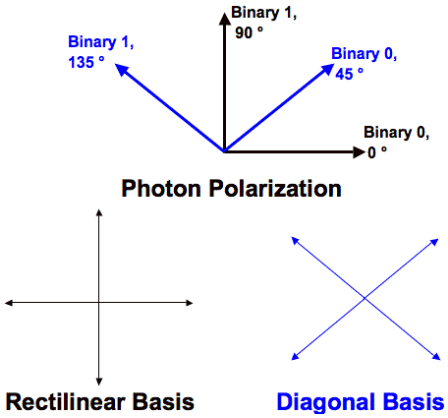
These protocols use the discrete variables of a quantum state, such as the polarization of a particle.

BB84 Protocol

This protocol starts by defining two bases, a rectilinear and a diagonal one. It also defines a binary 0, as a polarization of 0 degrees in rectilinear bases or 45 degrees in

diagonal bases and a binary 1 is defined as a 90-degree polarization in rectilinear bases and 135 degrees in diagonal bases.

Image from [14]



Initially, the sender (Alice), will choose a random string of 0's and 1's, and for each one of these Alice will pick a random basis, rectilinear or diagonal, to encode that bit. She will then transmit a photon for each bit with the polarization previously chosen, to Bob, the receiver. Bob will also choose randomly the basis he will use to measure the polarization of the photons sent by Alice. If for one photon the basis chosen by Alice and Bob are the same, he will, in principle, correctly measure the polarization and infer what Alice sent. If he chooses the wrong basis, his result will be a random bit.

At last, Bob uses an insecure channel to communicate to Alice the basis he used to measure the photons. Alice will tell Bob if he chose the correct basis for each photon, so he can discard the bits measured wrongfully. After this step, both Alice and Bob have the same string of bits, called sifted key.

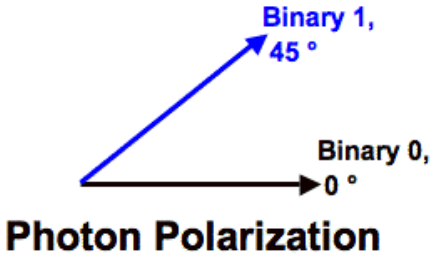
As a security measure, Alice and Bob will compare some of the bits of the key. If all of them match, they keep the remaining bits as the final key. If there is no noise or measurement errors, any inconsistency indicates the presence of an eavesdropper (Eve).

In Eve's attempt to ascertain the key, she must measure the polarization of the photons sent by Alice using a chosen basis, if she measures with the wrong basis the original information of the photon, according to the Uncertainty Heisenberg Principle, will be lost. When the photons reach Bob, his measurement will also be random, and he will read a bit incorrectly 50% of the time. In average Eve will chose the basis wrong 50% of the time, this implies that 25% of Bob's bits will differ from Alice's [14].

B92 Protocol

This protocol is a simplified version of the BB84, introduced by Charles H. Bennett in 1992. It states that key distribution can be performed using only two nonorthogonal states instead of four [14].

Image from [14]



To begin, Alice prepares a random string of 0's and 1's to send to Bob, as photons polarized in the corresponding basis. Bob chooses, also randomly, which basis he will use to measure. If he chooses the wrong basis, he will not measure anything because of a property of quantum mechanics called erasure. Lastly, Bob publicly tells Alice in which occasions his measurements didn't get erased, without telling her which basis he used to measure. This way they end up with a key after discarding the bits read incorrectly. As in the BB84 protocol, Alice and Bob, exchange publicly some of the bits of the key to make sure there was no eavesdropping [15].

Six-State Protocol SSP

This protocol is the already known BB84 but with one additional basis, orthogonal to the other two. Because of the use of three basis instead of two, the probability of Bob choosing the same one as Alice id 1/3, which means they discard 2/3 of the bits read by Bob [16]. The advantage of this protocol, over the BB84, is that the eavesdropper would also have to choose a basis from three. This extra choice makes Eve generate a higher error rate and, therefore, is easier to detect [15].

SARG04 Protocol

This is one of the most recent variants of the BB84 protocol. It uses the same states as the BB84 protocol but modifies the classical communication between Alice and Bob. The transmission and measuring phases of SARG04 protocol are the same as in the BB84 [17].

After this, Alice doesn't announce her bases, instead she announces a pair of non-orthogonal states, one of which she used to encode her bit [15].

Bob will proceed to measure this photon with his chosen basis, if he chose right, he will read the bit correctly, if not he will not be able to know the bit, the same way it happened with the B92 protocol [17].

Quantum Key Distribution Protocols Based on Entanglement

Entanglement is a quantum physics property that stablishes a correlation between two parts of a quantum system [28]. It is possible to entangle two particles in such a way that when a variable is measured in one particle, the opposite state will appear on the other particle instantaneously regardless of the distance between them [14].

Eckert's Protocol

In this protocol, Alice doesn't choose the key bits, instead there will only be one source emitting entangled particles. To stablish a key, both Alice and Bob will choose random bases to measure the state of the photon they received from the source. After the reading they will share through a public classical channel the basis used for the measurements. When the basis doesn't match the bit is discarded, but when it does, Alice and Bob will have a bit that is the binary complement of the other, according to the quantum entanglement property. It only takes one of the parties to invert their key to have finally the same one [14].

Almost all variants of the protocol BB84 mentioned before, have been tested using the entanglement property and a two-photon source instead of a single-photon one (Alice). SARG04 protocol has and entanglement- based version [14].

Continuous-variable Quantum Key Distribution (CV QKD)

Unlike the Discrete-variable QKD protocols, the CV QKD protocols use continuous quantum variables, such as quadratures of quantized electromagnetic modes (coherent states), to encode the key information. The use of CV coding provides a useful way to approach quantum information processing, since it can be built onto standard telecommunications technology such as the coherent detection method without the need of a single photon counting technique. CV coding gives the possibility to encode more than one bit per pulse achieving a higher secret key rate per pulse [18].

Quantum Key Distribution Limitations

Quantum key distribution links have several limitations, such as limited distance, before the information is lost or distort, can only occur through one physical channel at a time, and it is sensitive to disruptions caused by cuts on the fiber, because it relies on a single point of failure. These problems can be almost completely eliminated by designing fully QKD network instead of QKD links [20].

Chapter V. Investment in Quantum Research

Venture Capital Investment

In recent years, governments and big technology firms have nurtured quantum research with billions of dollars, and since the support has increased, venture capital investors are eager to get in this fledgling industry as well.

According to the analysis made by *Nature*, private investors have funded at least 52 quantum-technology companies, globally, since 2012, with these companies receiving around $450 million only between 2017 and 2018. Alongside government investments, lots of firms are rushing to invest in quantum, with names like Google, IBM, Tencent, Baidu, Huawei, Hewlett, Alibaba and Packard all doing their own research.

Venture investors can inject money on different fields of quantum research, such as: instrumentation, tools and services, communication, computing, software and, sensors and materials, as seen in the graph. But most of them tend to invest on the "most likely" to be a game-changer, such as achieving a multipurpose quantum computer. [29]

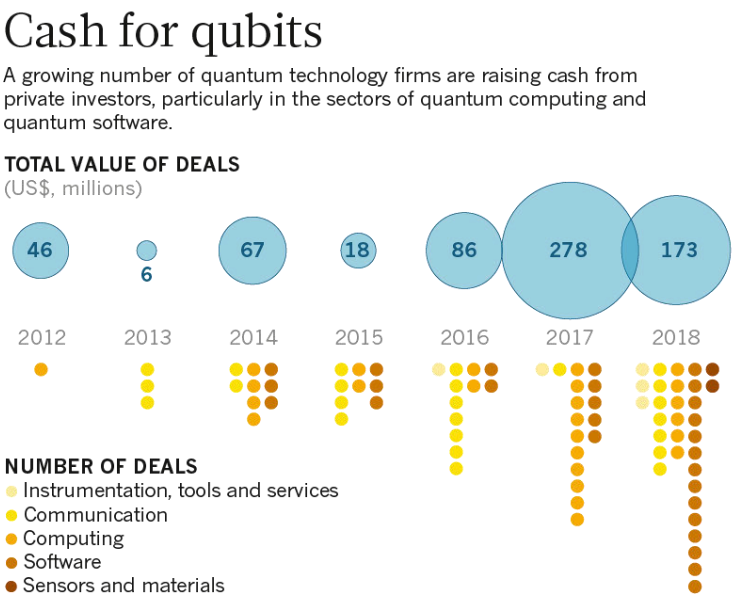


Image from [29]

Firms developing the hardware for quantum computers are receiving the biggest share of the venture capital investment.

Another field receiving big investments is quantum software development. Even if it's written for hardware that still doesn't exist, around 20 firms raised more than $110 million, in 28 deals, from 2012 to 2018. These algorithms are written to translate problems such as optimizing supply chains or simulating drug molecules, into software that could run on early quantum computers. A relevant thing to mention is that purely profit-driven venture capital investors are not too interested in algorithm development, since gains are not coming any time soon. Nevertheless, some firms are willing to pay to develop them. Software start-ups like Zapata Computing, 1Qbit and UK-based Cambridge Quantum Computing, have raised tens of millions of dollars each.

Lastly, one of the most popular quantum fields: communications, which uses entangled photons to create cryptographic keys that enable secure data transmission. The investments on this field are hard to quantify because out of the 27 deals, announced by thirteen firms that work in secure quantum communication, only around half have disclosed amounts. The leaders in the field, Chinese firms QuantumCTek and Qasky, have not revealed how much private funding they have received.

Nature's analysis, made between 2012 and 2018, shows that North America has long been the world's leader on attracting venture capital money. But it's not all restricted to the United States, firms in Canada have attracted $243 million, with D-Wave Systems raising alone $177 million.

The biggest gap in *Nature's* analysis is caused by the lack of private investment information from China. According to the data only one in ten fund-raising deals secured by Chinese firms disclosed its value.

Elsewhere around the world there are private funding hotspots in Australia, Singapore, the U.K and across Europe. [29]

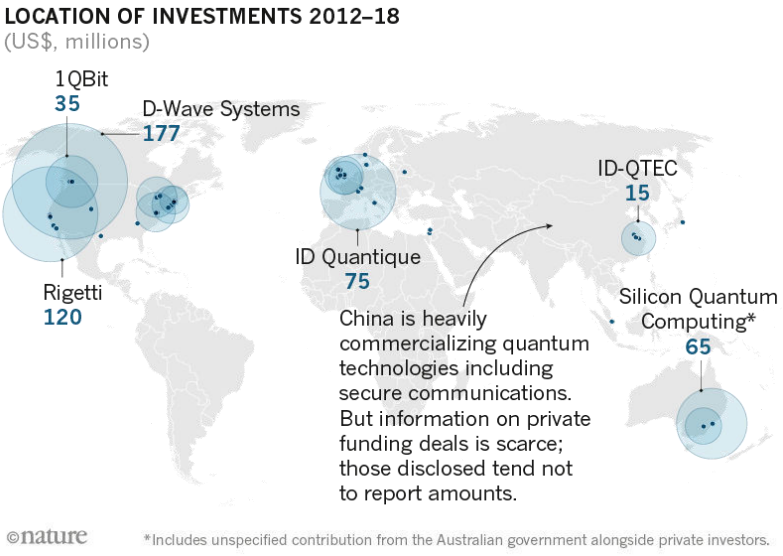


Image from [29]

Public Funding Around the World

According to the consulting firm McKinsey, in 2015 about 7000 people worldwide, with a combined budget of $1.5 billion were working on quantum-technology research [30]. This budget was distributed around the globe as seen in the image:

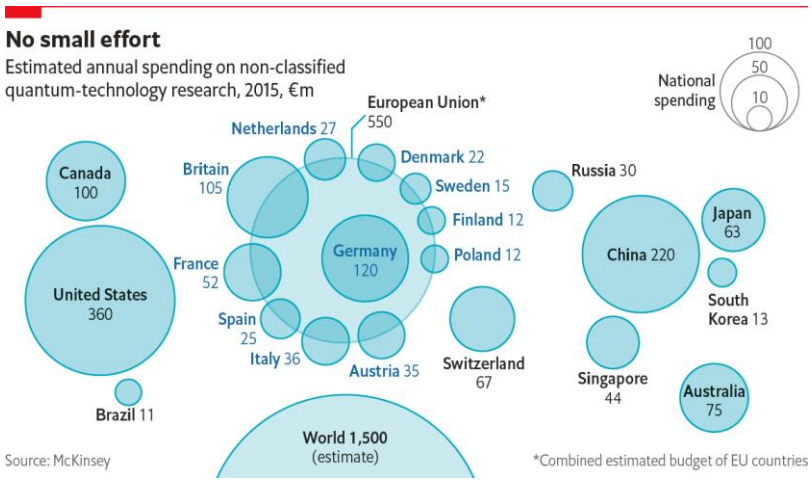


Image from [30]

Europe

In Europe, investors are more risk-averse, but the European Union launched a flagship to ensure that the region's strengths in basic research translate to commercial success. [29]

The Quantum Technologies Flagship is a large-scale, long-term research initiative that brings together research institutions, industry and public funders, consolidating and expanding European scientific leadership and excellence in this field. The Flagship will run for ten years, with an expected budget of €1 billion. In its ramp-up phase (October 2018-September 2021), it will provide €132 million of funding for 20 projects in four application areas: quantum communication, quantum simulation, quantum computing and quantum metrology and sensing. [31]

The flagship will be structured along four mission-driven application domains:

- ✓ Communication, to guarantee secure data transmission and long-term security for the information society by using quantum resources for communication protocols.

- ✓ Computation, to solve problems beyond the reach of current or conceivable classical processors by using programmable quantum machines.

- ✓ Simulation, to understand and solve important problems, e.g. chemical processes, the development of new materials, as well as fundamental physical theories, by mapping them onto controlled quantum systems in an analogue or digital way.

- ✓ Sensing and metrology, to achieve unprecedented sensitivity, accuracy and resolution in measurement and diagnostics by coherently manipulating quantum objects. [32]

The UK also counted with a research 5-year program called the UK National Quantum Technologies Program. Founded in 2013 with an initial investment of £270 million from the UK Chancellor of the exchequer, George Osborne and a further investment of £30 million from the UK Defence Science and Technology Laboratory. [33]

Not European Countries

The United States, Japan, Singapore, Canada and China are also ploughing hundreds of millions of dollars, from public-investment initiatives, into quantum technologies. [29]

USA Quantum vs. China Quantum

Over the past two years, China has aggressively stepped up its pace of quantum research. In 2016, President Xi Jinping established a national strategy for China to become technologically self-reliant. One of China's main goals is to surpass the United States and to become the global high-tech leader. [34]

President Xi funded a multi-billion-dollar quantum computing mega-project with the expectation of achieving significant quantum breakthroughs by 2030. The country has also announced plans to invest $10 billion to build a national laboratory for quantum science, that will open in 2020. [35]

To counter-punch China's investments, President Trump signed H.R. 6227 to fund the National Quantum Initiative Act (NQI) in December 2018. The law authorizes $1.2 billion to be invested in quantum information science over five years.

NQI funding will go to the National Institute of Standards and Technology (NIST), National Science Foundation (NSF) Multidisciplinary Centers for Quantum Research and Education and to the Department of Energy Research and National Quantum Information Science Research Centers.

A few days after the executive order was signed, the Department of Energy announced $80 million in funding for quantum research.

Although these are positive actions, they are small compared to the enormous investments being made in quantum research by the Chinese. [34]

At a conference last summer, Chinese physicist Pan Jian-Wei spoke about the hacking-resistant communication networks they are building across China, the sensors they are designing and the prototype computers that will, someday, surpass the

computational power of any computer. These advances are certainly a threat to the United states.

If China transitions its military telecommunications to the quantum networks, the US will have a big problem to maintain surveillance.

Quantum sensors, powerful enough, could compromise US domination over electromagnetic domain in combat environments and could also threaten the US lead in stealth technology. [34]

Jonathan Dowling, a physics professor at Louisiana State University said, "I predict China to go black in two to three weeks – we won't be able to read anything" [36]

Increased federal funding for quantum research is the only way the United States can achieve and maintain a quantum lead over China.

To achieve this, it is key that the US military has access to new technologies such as quantum computing and artificial intelligence. Therefore, President Trump's targeted 2020 DARPA (Defense Advanced Research Projects Agency) budget is $3.6 billion.

Despite DARPA's focus on quantum and other high-tech projects, the agency's funding as a percentage of total defense science and technology has fallen almost five percent over the past few years. During the same period, China's high technology funding has increased. [34]

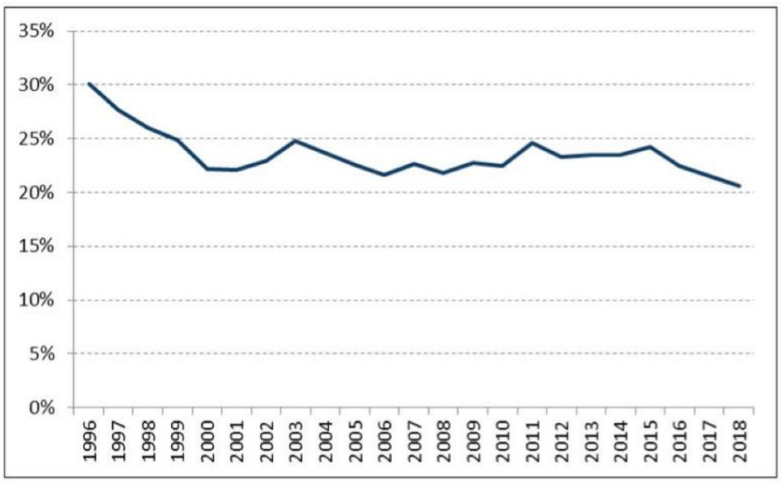


Image from [34]

DARPA Funding as a Share of Defense S&T Funding

Quantum Patents

More than 43% of quantum-technology innovations patented between 2012 and 2017 came from Chinese firms and universities [29]. In the graphic we see that last year China had nearly twice as much patents as the United States in quantum technology overall, a category that includes mostly communications and cryptology devices.[36]

Nevertheless, the United States leads the world in patents relating to the most prized segment of the field, quantum computers [36]. In 2018, IBM obtained more patents than any other US company. [34]

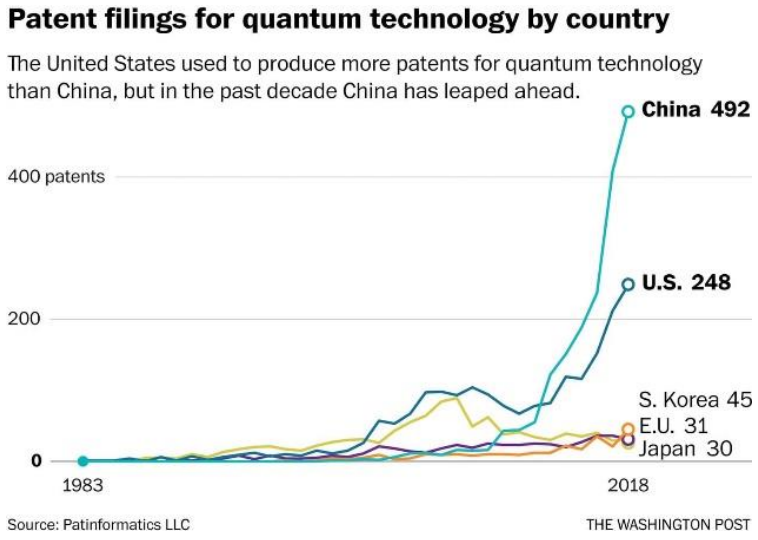


Image from [36]

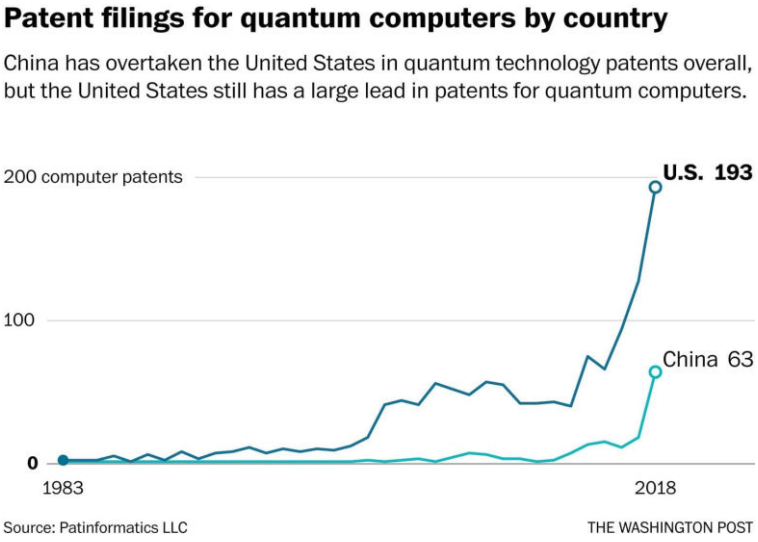


Image from [36]

We can also see in the next graphic the patents from other countries. This was updated for the last time in 2015.

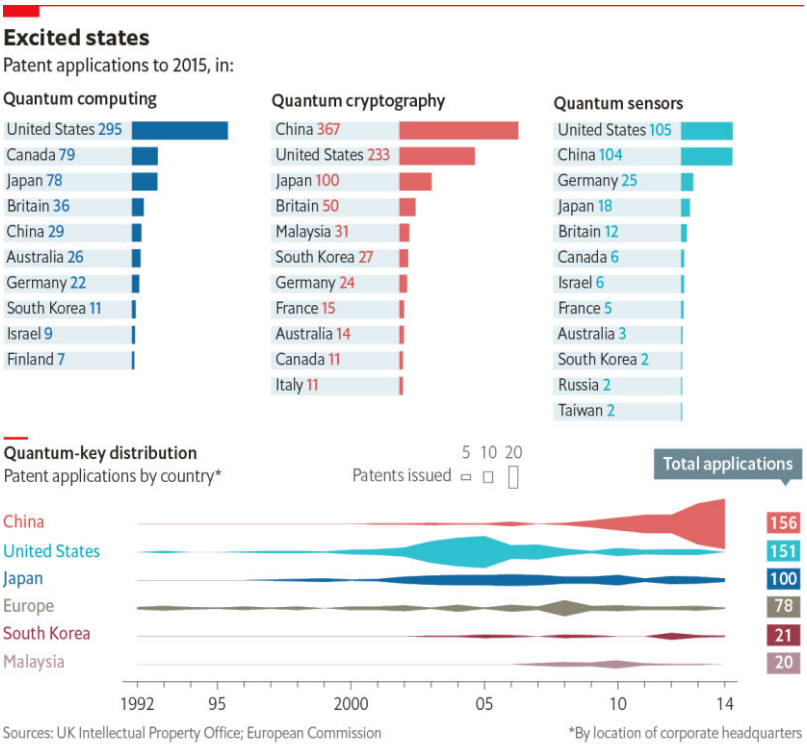


Image from [30]

Quantum Winter

A report from the US National Academies of Science, Engineering and Medicine, points out that quantum research could face a "valley of death" in which investments weaken, if some early form of quantum computer doesn't appear with profitable uses soon. Researchers worry about a "quantum winter" similar to the "AI winter" [29]. This has happened often in the past, according to Carlota Perez, an economic historian, revolutionary technologies always go through a "gilded age", usually accompanied by an investment bubble that pops, before entering the "golden age". [35]

Quantum Bottleneck

Even though many scientists, who have founded start-ups, still teach and do research in universities, there are others that have left the life on campus completely. This boom in quantum start-ups means that there are already too few qualified quantum engineers to work for the firms and it also risks draining academic talent out of universities. This is one of the reasons why the US National Quantum Initiative dedicates a major strand of the money to train a new generation in quantum-related jobs. [29]

How to make Computing more Sustainable

Some firms are over-promising on technology they can deliver. Researchers wouldn't name any particular efforts they felt were too hyped, but some pointed out that the amount of investments in companies that only focus on quantum software development is a sign of an investment bubble [29]. Observers of the quantum-computing scene warn that much of the software written today may become obsolete if quantum technology takes an unexpected turn in the future. [35]

Some firms have raised tens of millions of dollars which seems to indicate a lot of hype, but they argue that they need that money for intensive development and to hire staff. This companies also cover their costs for more than the two years that are typical in funding, stating that is a way to maintain scientists away from stable academic positions.

If data from 2019 indicates that private US investment in quantum technologies is dropping, it might be because of fears of a quantum winter or the long wait until there are any profits for the firms. The increasing competition and the appearance of new start-ups can also play a part. Even with all these in consideration, there are solid reasons to think that quantum technologies will create game-changing advances. It's more a thing of when, rather than questioning if it will actually happen. Ten years ago we would never have predicted the technology would be where it is today, so it's reasonable to think that "we are going to be reaching useful quantum computations faster than people think".[29]

Chapter VI. Quantum Technology Applications.

The Quantum Computer

Since we already have a basic knowledge on qubits and quantum states we can go now into the practical implementation of these properties. Classical computers use bits to represent two states, "0" and "1", true or false. Quantum computers use qubits, which are typically subatomic particles such as electrons or photons, to represent the states. [37]

There are various ways to build quantum computers, many university research groups bet on trapped ions. But the industrial giants do not necessarily agree with that. The superconducting circuit seems to be their top choice, since many corporations acquire semiconductor experts who, instead of using atoms to store quantum information, print artificial "quantum systems" in a circuit for the qubits.

A trapped ions quantum computer uses lasers to change the energy level of laser-cooled ions trapped in an electric field. On the other hand, IBM Q quantum computer holds superconducting circuits to create a quantum system. In this type of quantum computers, the quantum processor is the most important thing of the computer. The processor is kept in the bottom of a cylinder that contains a dilution refrigerator to cool the processor down to 15 mKelvin, in order to isolate the qubits and to avoid heat disturbances. The IBM Q contains cables to send microwave pulses at different frequencies and durations to control and to measure the qubits. [38]

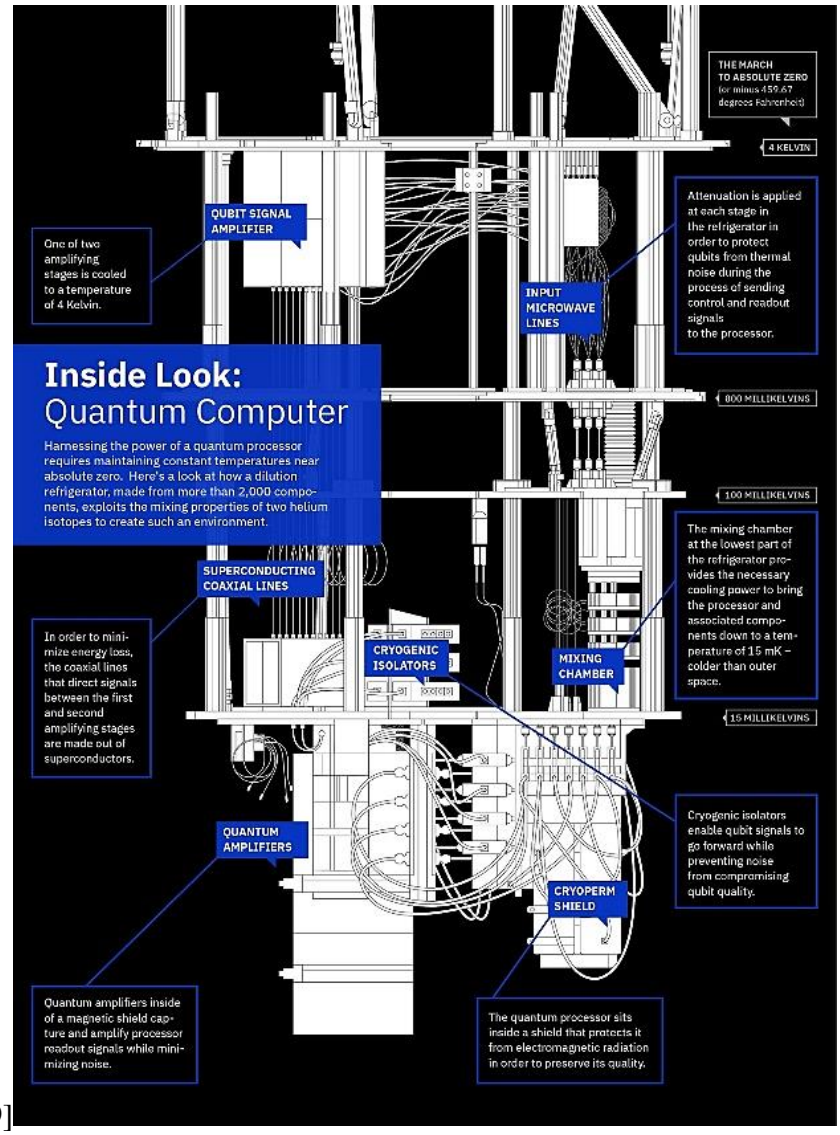


Image from [39]

IBM Q (IBM Quantum Computer)

The circuitry implementing the artificial quantum system is constructed with a superconducting material which has zero resistance when cooled below a certain temperature. Each qubit is actually a LC circuit, an inductor and a capacitor.

The representation of a superposition of $|0\rangle$ and $|1\rangle$ is accomplished with the manipulation of the circuit's energy state. The energy level can be modeled as a quantum harmonic oscillator with quantized energy level. A present challenge is that the energy difference between levels is evenly separated. This is a problem since a control signal may accidentally promote a quantum state to an unwanted one in a higher level of energy.

To overcome this, the superconducting circuit includes a Josephson Junction. It contains two Aluminum superconducting electrodes which are weakly couple and are separated by a thin insulator about a thousandth of a hair thick. The junction provides the non-linearity such that the states can be controlled unambiguously.

Once combined with a linear capacitor using Niobium superconductor, the circuit behaves like an atom with two quantum energy levels.[38]

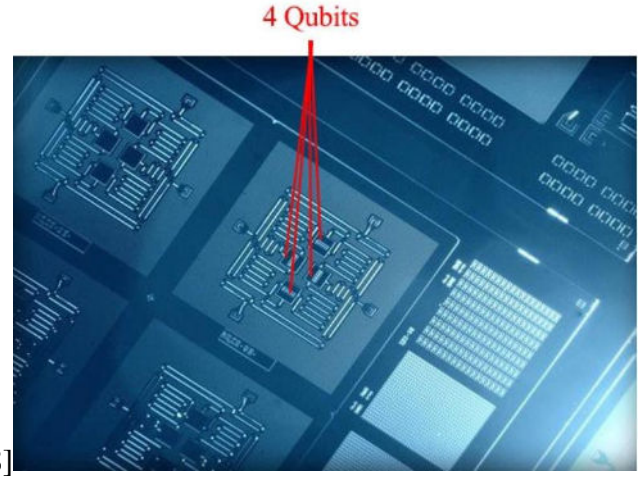


Image from [38]

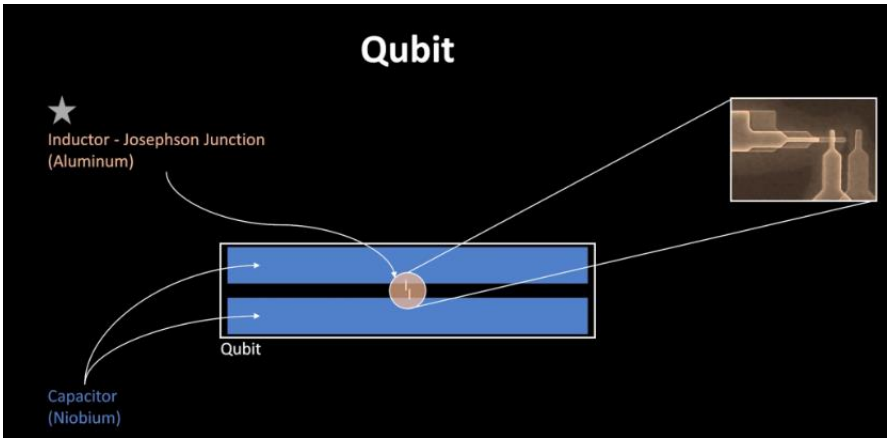


Image from [38]

Quantum operations are performed by sending electromagnetic impulses at microwave frequencies to a resonator coupled to the qubit. The duration of the pulse controls the angle of rotation of the qubit state.

Measurement

To make a measurement, a microwave tone is sent to the resonator and the signal that reflects back is analyzed. The amplitude and phase of the reflected signal depend on the qubit state. [38]

Trapped Ion Quantum Computer

As mentioned before, many universities, with a strong expertise in atomic physics, prefer ion trapped quantum computers because they know how to manipulate quantum information at an atomic level. The problem is that scaling up the solution is not necessarily their strength.

To build this type of quantum computer, coherent sources of photons with a specific frequency (lasers) are used to control the energy level of an ion. This is made to select the two separate energy states for the computation basis $|0\rangle$ and $|1\rangle$.

Electrons release or absorb a photon when they drop to a lower or jump to a higher energy state, respectively. The emission of a photon is used to control the state of an atom, and therefore initialize the state of the qubit.

Measurement

To measure the qubit's state, the qubit gets shined with another laser with a specific calculated frequency. The qubit will fluoresce in a state or else remain dark. [40]

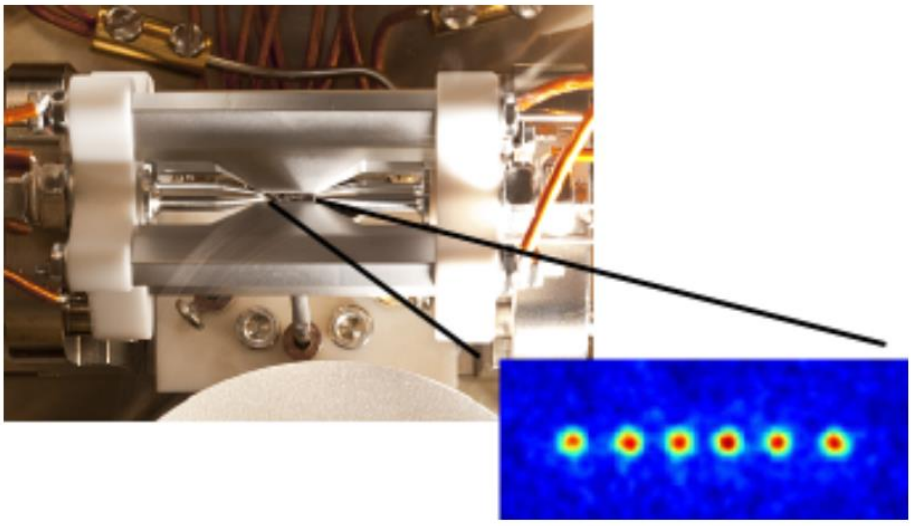


Image from [41]

Googles Quantum Supremacy

Quantum Supremacy is said to be achieved when a quantum computer does something a classical one can't do.

Google, by using their processor, named "Sycamore", with programmable superconducting qubits, manage to create states on 53 qubits. This allowed them to sample one instance of a quantum circuit a million times in only three minutes and twenty seconds, a task that would take a classical computer, allegedly, around 10.000 years to complete.

Sycamore Processor:

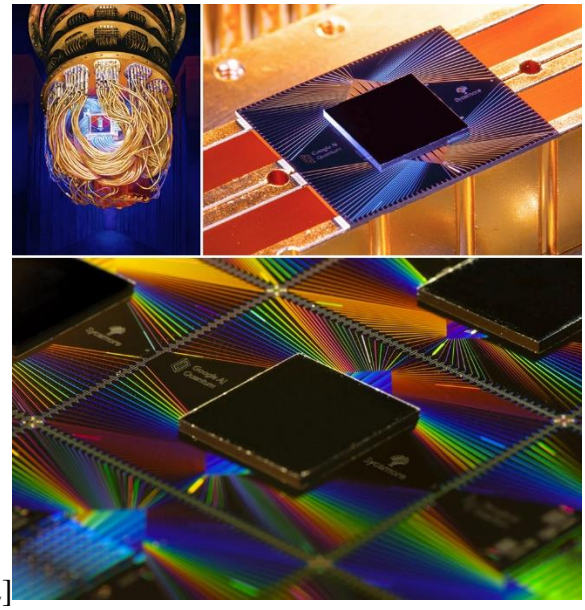


Image from [42]

To show quantum supremacy, Google designed a circuit that entangles a set of qubits and gave the quantum processor and the classical computer the same task. The goal was to sample the output of this pseudo-random circuit. Because of the quantum nature of the circuit, the probability distribution of the outputs (strings of bits), resembled the pattern produced by light interference in laser scatter. This meant an advantage for the quantum computers since it works on particle principles. The computation difficulty of this probability, when using a classical computer, grows exponentially as the number of qubits get higher [24].

The processor is made of aluminum for metallization and Josephson junctions (current that flows across two superconductors joined by a weak link, without the need to apply voltage [23]), and indium. Then the chip is wired onto a superconducting circuit and cooled to below 20mKelvin. This chip can achieve high-fidelity operations with one or two qubits, while also performing real computation, with the use of gate operations, on many qubits simultaneously [24].

Even though Google, with this achievement, declared Quantum Supremacy on an article, IBM was quick to respond. IBM states that an ideal simulation of the same task can be performed on a classical system in 2.5 days and with far greater fidelity [25].

IBM also states that the estimate of 10.000 years to accomplish the simulation on a classical computer is based on the fact that the RAM memory requirements are not enough to save full state vectors. The simulation made by IBM features both RAM and hard disk space, and more techniques such as circuit partitioning, tension contraction deferral, cache-blocking and double-buffering in order to optimize the experiment. The following graph shows the IBM's estimated runtime of this task on a classical computer:

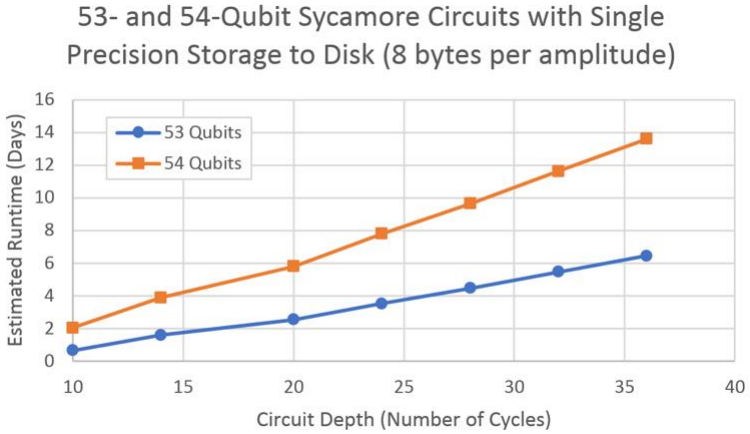


Image from [25]

Google's Sycamore processor has a circuit depth of 20 and, as we can see in the image, the runtime estimated for a 53-qubit quantum computer is approximately 2.5 days and 6 days for a 54-qubit one. [25]

Quantum Networks

Quantum networks are defined as infrastructures that have quantum links connecting separated nodes. The goal of this networks is to distribute a secure secret key to any pair of authorized users that access the network.

DARPA Quantum Network

This network, based in Cambridge, Massachusetts, is the world's first Quantum Key Distribution network. It was sponsored by the Defense Advanced Research Projects Agency (DARPA) [43], an agency of the United States Department of Defense, as part of the Quantum Information Science and Technology Program (QuIST program) and built and operated by BBN Technologies in close collaboration with colleagues at Harvard University and the Boston University Photonics Center.

The QuIST was a five-year, $100 million DARPA research program that ran from 2001 to 2005. It was created to accelerate the development in the fields of quantum computing and quantum communications. [44].

The DARPA network is an optically switched quantum network since some nodes apply optical functions, such as switching, on the quantum signals sent through the quantum channel [21].

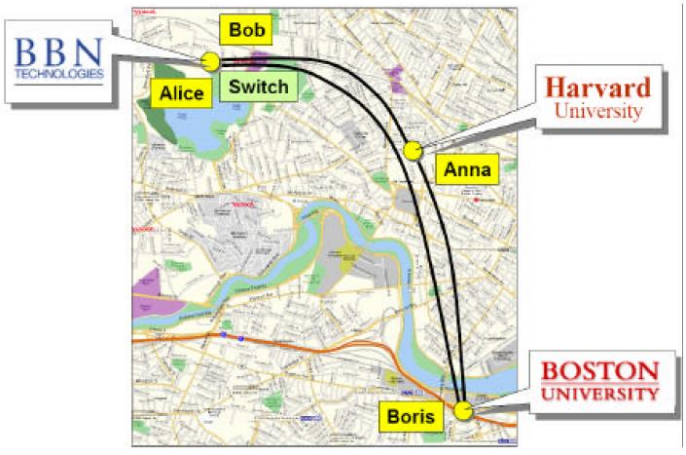
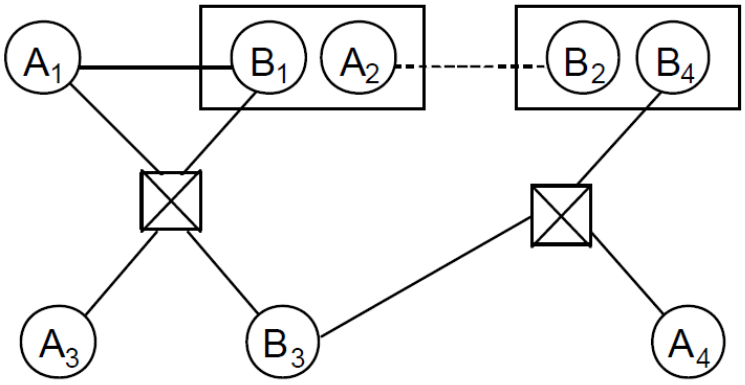


Image from [20].

This quantum network consists of two BB84 transmitters (Alice and Anna), two receivers (Bob and Boris) and a switch that can couple any transmitter to any receiver. Alice, Bob and the switch are in BBN Technologies Laboratory, Anna is at Harvard University and Boris at Boston University. The difference between this network and a stand-alone quantum link is that both Alice and Bob are "QKD endpoints" that are part of a network working as an isolated "link". This means that the nodes in the network can be connected through different channels and each one of them can communicate with all the others. As we see in the figure Alice and Bob (A1, B1) are connected via a fiber strand, but A2 and B2 have a connection over free space. Another advantage is that a node like Alice can agree upon a key, not only with her direct neighbors, but with another node thanks to the quantum key distribution network. Even more surprising is that two transmitters (A1 and A2) can agree upon a key if they rely on a trusted middleman like B1.



This network undertook the implementation of traffic in the internet using Virtual Private Network (VPN) based in quantum key distribution [20]. The implementation of a key distribution network brings many advantages as shown in the chart:

Benefit	Discussion
Longer Distances	QKD key relay can easily extend the geographic reach of quantum cryptography. As one example, quantum cryptography could be performed through telecommunications fiber across a distance of 500 km by interposing 4 relays between the QKD endpoints, with a span of 100 km fiber between each relay node.
Heterogenous Channels	QKD key relay can mediate between links based on different physical principles, e.g., between freespace and fiber links, or even between links based on entanglement and those based on weak laser pulses. This allows one to "stitch together" large networks from links that have been optimized for different criteria.
Greater Robustness	QKD networks lessen the chance that an adversary could disable the key distribution process, whether by active eavesdropping or simply by cutting a fiber. When a given point-to-point QKD link within the network fails – e.g. by fiber cut or too much eavesdropping or noise – that link may be abandoned and another used instead. Thus QKD networks can be engineered to be resilient even in the face of active eavesdropping, fiber cuts, equipment failures, or other denial of- service attacks. A QKD network can be engineered with as much redundancy as desired simply by adding more links and relays to the mesh.
Cost Savings	QKD networks can greatly reduce the cost of large-scale interconnectivity of private enclaves by reducing the required (N x N-1) / 2 point-to-point links to as few as N links in the case of a simple star topology for the key distribution network.

Chart from [20].

Application of Quantum Cryptography in Commercial Optical Networks for Safe Communications by Huawei, Telefónica and Polytechnic University of Madrid

On June 14, 2018, Telefónica, Huawei and the Polytechnic University of Madrid ran a pilot test of quantum cryptography through commercial optical networks using technologies based on SDN (Software Defined Networking).

For this pilot they used fiber provided by Telefonica of Spain, infrastructure connecting three different centers in the metropolitan area of Madrid, along with CV-QKD equipment developed by Huawei's research laboratories in Munich in which also helped the UPM, installed at these centers, SDN-based management modules developed by the team of innovation in network technologies of the GCTIO of Telefónica, and the mechanisms of integration of quantum cryptography technologies, SDN and NFV (Network Function Virtualization) developed by the UPM. [45]

The integration of Huawei's CV QKD devices with standard devices for optical transport, and the use of networks and quantum cryptography technologies based on SDN, is what gives the developers the ability to control everything by software. There are other advantages, such as being able to reuse the classical coherent communication systems, without having to implement complex detectors that operate at ultralow temperature [22].

"The integration of all these elements allows us to demonstrate the use of QKD techniques in a real production environment, by combining the transmission of data and quantum keys over the same fiber strand" [22].

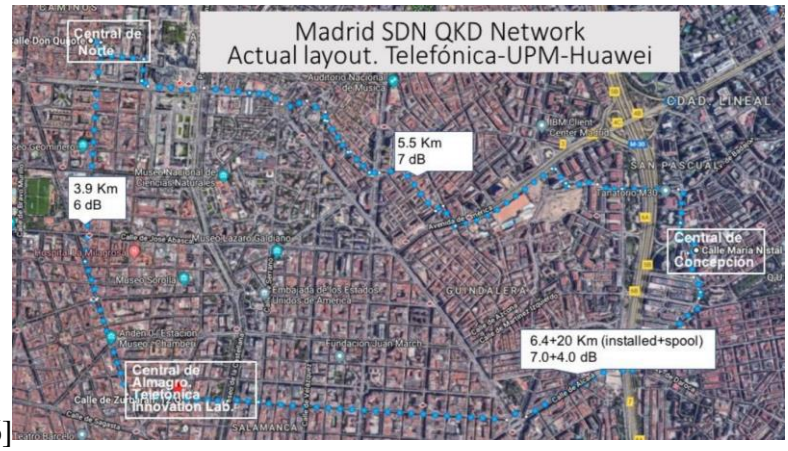


Image from [46]

The SECOQC Quantum Key Distribution Network

The Global Network for Secure Communication based on Quantum Cryptography (SECOQC) was a project that started in 2004 and ended in 2008. It had a budget of around €16.8 million of which, around €11,3 million were a contribution from the European Union; 25 universities, 4 national research centers, 8 multinational enterprises and 4 small and medium-sized enterprises (SMEs) [47] from Austria, Belgium, Switzerland, Czech Republic, Germany, Denmark, France, Italy, Russia, Sweden and the U.K. [48]

The team behind the SECOQC project set out to design and validate a network for dependable and secure long-range communication built upon quantum key distribution (QKD) technology. [48]

SECOQC is a trusted relays QKD network, this means that the keys generated using QKD links are stored at nodes located at both ends of each link. To achieve its goal of having secure communications, the whole architecture of the network is designed to work with trusted nodes. The innovative thing of the SECOQC network is that it has an infrastructure called "network of secrets" completely dedicated to save, send and manage the secret keys generated by QKD. Because of the use of dedicated links and network and transport layers we can think of the "network of secrets" as an independent part of the network, separated from the key generation processes. This independence provides flexibility and advantages, such as: an increase in reliability and balancing of the load and traffic through routing algorithms [22].

The "network of secrets" is essentially a classical network, but, since the key establishment is made through quantum key distribution, it offers high security communications, that may only be threatened if the nodes are not trusted [21].

During the project, the technology was used to perform the world's first bank transfer using quantum cryptography by sending €3.000 over a 1.45-km fiber-optic link between Vienna City Hall and the headquarters of Bank-Austria Creditanstalt. [48]

In October 2007, it was also used to provide a secure line for counting votes cast in Geneva in the Swiss national elections, marking the first real-world use of the technology. [48]

China's Quantum Satellite

Micius satellite, named after an ancient Chinese philosopher, was launched in August 2016. The satellite is the foundation of the $100 million Quantum Experiments at Space Scale program, one of several missions that China hopes will make it a space science power on par with the United States and Europe.

In their first experiment, the team sent a laser beam into a light-altering crystal on the satellite. The crystal emitted pairs of photons entangled so that their polarization states would be opposite when one was measured. The pairs were split, with photons sent to separate receiving stations in Delingha and Lijiang, 1200 kilometers apart. Both stations are in the mountains of Tibet, reducing the amount of air the fragile photons had to traverse. They found the photons had opposite polarizations far more often than would be expected by chance, thus confirming the success of the transmission. [49]

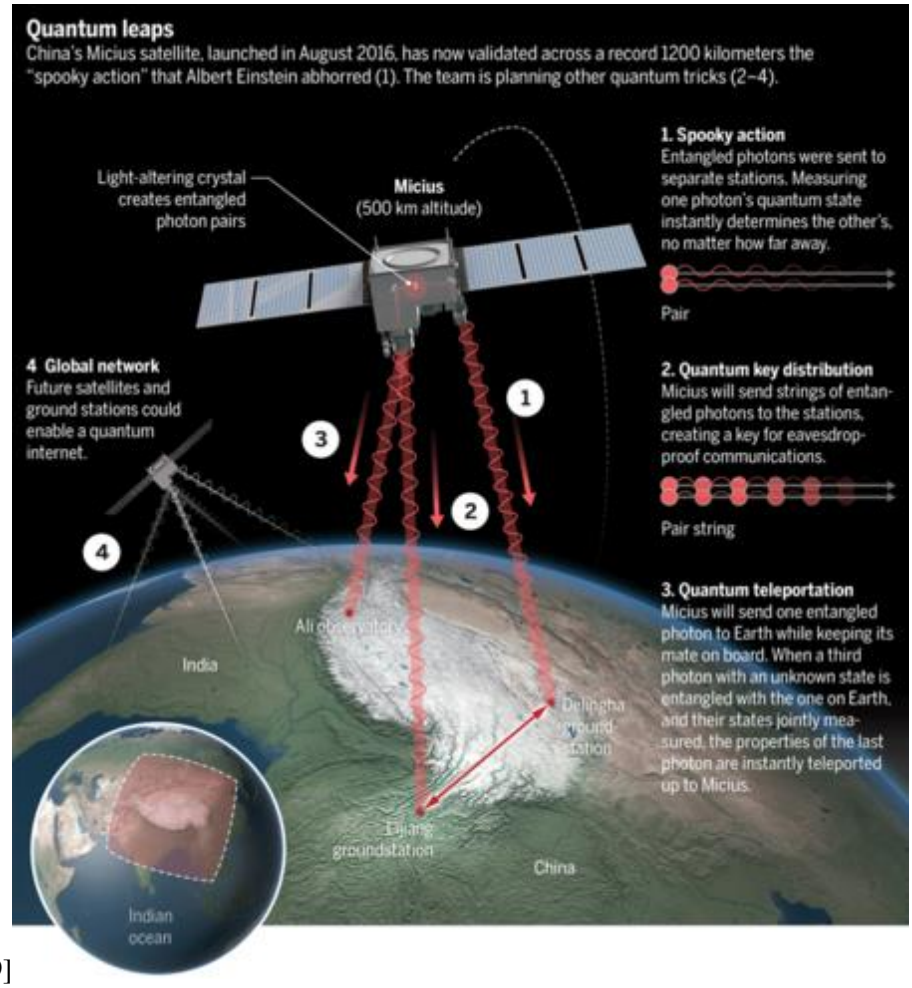


Image from [49]

In another experiment, when the satellite was over the Chinese ground station at Xinglong in China's northern Hebei province, it sent the one-time pad to the ground, encoded in the entangled photons. As the Earth rotated beneath the satellite and as the ground station at Graz in Austria came into view, Micius sent the same one-time pad to the receiver there.

After that, the two locations possess the same key that allows them to initiate completely secure communication over a classic link. [50]

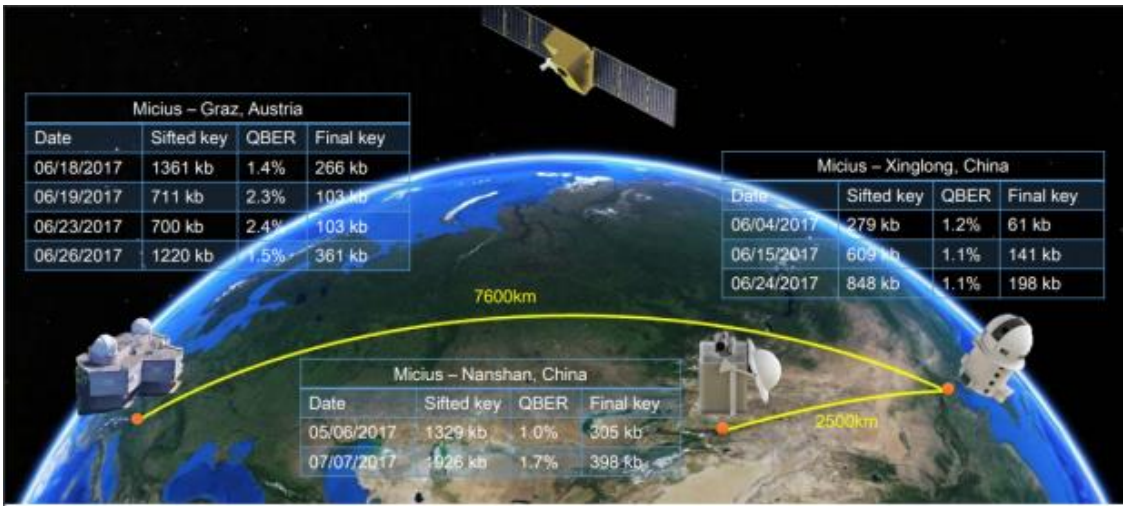


Image from [50]

However, the experiment goes one step further. The goal was to set up a videoconference between the Chinese Academy of Sciences in Beijing and the Austrian Academy of Sciences in Vienna, so the key has to be distributed securely to both these locations. And for that the teams use ground-based quantum communication over optical fibers.

Finally, they set up a video link secured by the Advanced Encryption Standard (AES) that is refreshed every second by 128-bit seed codes. In September, they held a pioneering videoconference that lasted for 75 minutes with a total data transmission of roughly two gigabytes

Quantum Radar

In 2017, the Chinese defense industry claimed a breakthrough in mastering quantum radar technology, but Western defense industry officials said that such a system is not likely to exist outside a laboratory. China Electronics Technology Group Corporation (CETC) announced it had tested such a radar at ranges of roughly 60 miles. While 60 miles is not particularly huge feat, the fact that such a radar would be able to provide a weapons quality track on a stealth aircraft at those distances is impressive.

After this big announcement, even Chinese researchers were skeptical about the CETC development. The South China Morning Post clarified saying that CETC made a breakthrough in single-photon detectors, and certainly, once the technology improves, it could have a wide range of applications for quantum radar technology. [51]

In 2019, two years after the announcement of the Chinese "quantum radar", the real first quantum radar was created and tested thanks to the work of Shabir Barzanjeh at the Institute of Science and Technology Austria and a few colleagues.

The radar works with the phenomenon of entanglement. The researchers create pairs of entangled microwave photons using a superconducting device called a Josephson parametric converter. They beam the first photon, called the signal photon, toward the object of interest and listen for the reflection. In the meantime, they store the second photon, called the idler photon. When the reflection arrives, it interferes with this idler photon, creating a signature that reveals how far the signal photon has traveled. [52]

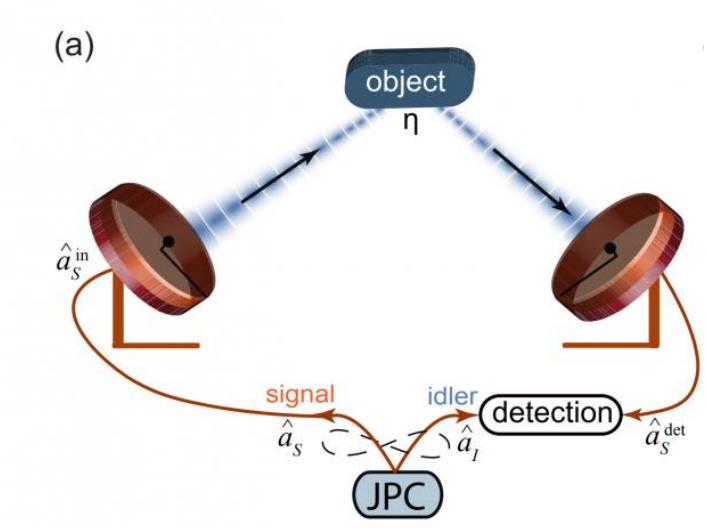


Image from [52]

One of the major advantages of this radar is that the signal and idler photons are so similar that it is easy to filter out the effects of other photons. So it becomes straightforward to detect the signal photon when it returns. Another advantage is the low levels of electromagnetic radiation required, making this radar a potential non-invasive scanning method for biomedical applications or a stealth radar so subtle that is difficult for adversaries to detect over background noise. [52]

Chapter VII. Technologies Threaten by Quantum Computing

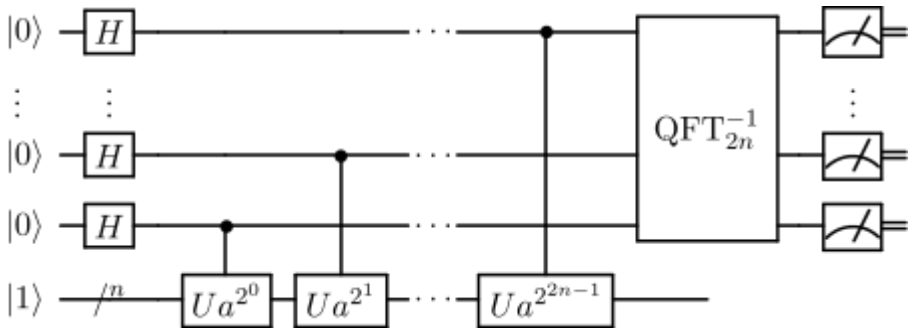
Post-Quantum Cryptography

Many of the most crucial communication protocols rely principally on three core cryptographic functionalities: public key encryption, digital signatures, and key exchange. Currently, these functionalities are primarily implemented using Diffie-Hellman key exchange, the RSA cryptosystem, and elliptic curve cryptosystems. The security of these depends on the difficulty of certain number theoretic problems such as integer factorization or the discrete logarithm problem, over various groups.

Quantum algorithms achieving exponential speedup have been discovered for several problems relating to physics simulation, number theory, and topology. [53]

Some algorithms, like Schor's or Grover's, can solve those really difficult mathematical operations. If they can be executed in quantum computers with enough qubits, classical cryptographic algorithms could be cracked easily and fast.

Schor's algorithm, for example, is an algorithm for integer factorization. It can find the prime factors of a given number. This means that it can solve the mathematical problem on which the RSA cryptosystem is based on.



Schor's algorithm. [54]

Because of the improvements in quantum technologies, cryptographers have reached a point where they have started to look for new alternatives, new algorithms to fight the

possibility of quantum computers cracking the whole classical cryptographic system we have today. This has led to the creation of Post-quantum cryptography.

Post-quantum cryptography refers to the algorithms that are supposed to be secure against an attack by a quantum computer. Currently in 2019, this has not been accomplished, since most of the public-key algorithms can be broken by a sufficiently powerful quantum computer. Nevertheless, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers. [55]

The urgent need for stronger cryptography is driven by advances in both classical and quantum computing technologies. To maintain security against classical attacks, NIST has already recommended transitions from key sizes and algorithms that provide 80 bits of security, to key sizes and algorithms that provide 112 or 128 bits of security. To provide security against quantum attacks, NIST will have to facilitate a more difficult transition, to new post-quantum cryptosystems.

It remains unclear when scalable quantum computers will be available. However, in the past year or so, researchers working on building a quantum computer have estimated that it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars. This is a serious long-term threat to the cryptosystems currently used. [54]

Blockchain and Quantum Cryptography

Blockchain is a distributed data structure composed of information blocks that are linked to each other. Blockchain technology is the new way to document data on the internet. For a new piece of information to be stored on a blockchain, it needs a sort of authentication provided by other devices on the network. Once this information is documented on the blockchain, it can’t be removed or altered.

The security of this system is based on the fact that every record documented on a blockchain has a unique cryptography key, created with the information and secret key of the previous block added to the chain. If another block is created, its key will be created with all the information and keys of the previous two blocks and so on.

This is the reason why altering a block is almost impossible, all the following blocks would have to be edited too [26].

Even though blockchain keys are highly secure, because they rely on a lot of previous information, the mathematical formulas used to create these keys are based mostly on RSA algorithms, which are currently vulnerable to the fast advance of quantum computing. In order to keep a blockchain secure from quantum cryptography, this one can be based on Quatum Key Distribution and implemented on a QKD network. An example of this was carried out in Moscow. A blockchain protocol was designed and tested on a three-node urban QKD network. The network consists on two layers, the first one is a QKD network that allows the private key generation between two nodes, the second one is used to transmit with authentication tags created using the keys.

The protocol has two steps: first, the transaction is created by one of the nodes, but is not stored as a block until all the other nodes get to the second step, authenticating the transaction and agreeing on creating the block. Since all the authentication is based on QKD, a node that tries to process inconsistent transactions gets eliminated.

This protocol is thought to be useful not only against current quantum computing, but also as a solution to the potential discovery of ways to make quantum-resistant algorithms vulnerable [27].

Conclusion

Some say that Quantum Cryptography is a product for the few with lots of money, and not for a massive number of clients, since the cryptography techniques that are currently in use are inexpensive and pass unnoticed to a lot of people.

Research on quantum methods is going fast, the implementation of full Quantum networks is improving the benefits of Quantum links and ensuring more secure communications. Ways of implementing a quantum network on a preexistent telecommunication network have been tested presenting new advantages, such as not needing to use specific detectors at ultralow temperature and having a more flexible network.

Another research advancing fast is the look for quantum-resistant cryptography algorithms, since some of the most used classical algorithms can be solved by using quantum computers.

Even a technology as blockchain, presented as bulletproof, is searching for a way to implement quantum properties, links and networks, to ensure security when facing quantum computing advances.

References

[1] Susskind, L., Friedman, A., *Quantum Mechanics. The Theoretical Minimum. What You Need to Know to Start Doing Physics.* Basic Books, A Member of the Perseus Books Group, Copyright @ 2014 Leonard Susskind and Art Friedman, Publication, ISBN 978-0-465-08061-8.

[2]THORLABS Discovery. (2017) *EDU-QCRY. EDU-QCRY/M. Quantum Cryptography Demonstration Kit.* https://www.thorlabs.com/drawings/da2025f890d466ab-BEDB677B-A5A4-4E99-279E155781474117/EDU-QCRY1_M-EnglishManual.pdf

[3] Key distribution. https://en.wikipedia.org/wiki/Key_distribution

[4] Public-key cryptography. https://en.wikipedia.org/wiki/Public-key_cryptography

[5] RSA (cryptosystem). https://en.wikipedia.org/wiki/RSA_(cryptosystem)

[6] Diffie–Hellman key exchange. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[7] "Diffie-Hellman Key Exchange" in plain English https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english

[8] Elliptic-curve cryptography. https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

[9] Symetric-key algorithm. https://en.wikipedia.org/wiki/Symmetric-key_algorithm

[10] Advanced Encryption Standard (AES) https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

[11] Mehrdad S. Sharbaf. "Quantum Cryptography: A New Generation of Information Technology Security System". *IEEE Computer Society*, *Sixth International Conference on Information Technology: New Generations,* 2009, p. 1644.

[12] Heisenberg's Uncertainty Principle. https://chem.libretexts.org/Bookshelves/Physical_and_Theoretical_Chemistry_Textboo

k_Maps/Supplemental_Modules_(Physical_and_Theoretical_Chemistry)/Quantum_Mechanics/02._Fundamental_Concepts_of_Quantum_Mechanics/Heisenberg's_Uncertainty_Principle

[13] Wootters, W. K., & Zurek, W. H., "A single quantum cannot be cloned". *Nature,* 299, 1982, p. 802.

[14] Mart Haitjema, A Survey of the Prominent Quantum Key Distribution Protocols http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

[15] Bennett, C., "Quantum Cryptography Using Any Two Nonorthogonal States". *Physics Review Letter,* 68, 1992, p. 3121- 3124.

[16] Bechmann-Pasquinucci, H., & Gisin, N., "Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography". Arxiv preprint quant-ph/9807041v2, 2018.

[17] Yuanyuan, Z., Xuejun Z., & Xiaoqiang, L., "Performance of Scarani-Acin-Ribordy-Gisin Protocol in Quantum Key Distribution". *2nd International Conference on Future Computer and Communication,* 2, 2010, p. 96-100.

[18] Yong-Min, L., Xu-Yang, W., Zeng-Liang, B., Wen-Yuan, L., Shen-Shen, Y., & Kun Chi, P. "Continuous variable quantum key distribution". *Chinese Physics B,* 26, 2017, p. 040303-1 - 040303-7.

[19] One-time pad. https://en.wikipedia.org/wiki/One-time_pad

[20] Elliot, C., "The DARPA Quantum Network". *Quantum Communications and Cryptography,* 2006, p. 1-34.

[21] Alleaume, R., "SECOQC White Paper on Quantum Key Distribution and Cryptography". Reference Secoqc-WP-v5, 2007.

[22] Telefónica, 2018. "Telefónica, Huawei y la Universidad Politécnica de Madrid realizan una experiencia pionera a nivel mundial de aplicación de criptografía cuántica en redes ópticas comerciales para comunicaciones seguras". https://www.telefonica.com/documents/23283/142759921/ndp-14062018-tecnologia-cuantica.pdf/17896d55-ec3e-d52e-837e-46a10b99dfd3?version=1.0

[23] Josephson effect. https://en.wikipedia.org/wiki/Josephson_effect

[24] Arute, F., Arya, K., Babbush, R. et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510 (2019) doi:10.1038/s41586-019-1666-5

[25] Pednault, E., Gunnels, J., Maslov, D. & Gambetta, J. 2019. "On "Quantum Supremacy"". https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[26] Lisk, "What is Blockchain?". https://lisk.io/what-is-blockchain

[27] Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A.S., Yunusov, R.R, Kurochkin, Y.V., Lvovsky, A.I., & Fedorov, A.K. "Maintaining quantum-secured blockchain with urban fiber quantum key distribution network",2017. http://2017.qcrypt.net/wp-content/uploads/2017/09/We422.pdf

[28] Zhou, N., Wang, L., Gong, L., Zuo, Xiangwu., & Liu, Y. "Quantum deterministic key distribution protocols based on teleportation and entanglement swapping", *ScienceDirect,* 248, p. 4836-4842.

[29] Gibney, E. "Quantum gold rush: the private funding pouring into quantum start-ups". *Nature*, October 2019. https://www.nature.com/articles/d41586-019-02935-4

[30] Palmer, J. "Quantum technology is beginning to come into its own". *The Economist,* 2015. https://www.economist.com/node/21717782/sites/all/modules/custom/ec_essay

[31] European Union. "Quantum Technologies Flagship". November 2019. https://ec.europa.eu/digital-single-market/en/quantum-technologies

[32] Max F Riedel. "The European Quantum Technologies flagship program". *Quantum Sci. Technol.* 2017, 2 030501. https://iopscience.iop.org/article/10.1088/2058-9565/aa6aca/pdf

[33] UK National Quantum Technologies Programme. https://en.wikipedia.org/wiki/UK_National_Quantum_Technologies_Programme

[34] Smith-Goodson, P. "Quantum USA Vs. Quantum China: The World's Most Important Technology Race". *Forbes*, October 2019. https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#6c6b028772de

[35] "The race is on to dominate Quantum Computing". *The Economist.* August 2018. https://www.economist.com/business/2018/08/18/the-race-is-on-to-dominate-quantum-computing

[36] Whalen, J. "The quantum revolution is coming, and Chinese scientists are at the forefront". *The Washington Post*. August 2019. https://www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront/

[37] Giles, M. "Explainer: What is a quantum computer?" *MIT Technology Review.* January 2019. https://www.technologyreview.com/s/612844/what-is-quantum-computing/

[38] Hui, J. "QC — How to build a Quantum Computer with Superconducting Circuit?". January 2019. https://medium.com/@jonathan_hui/qc-how-to-build-a-quantum-computer-with-superconducting-circuit-4c30b1b296cd

[39] Moss, S. "IBM reveals 50 qubit quantum computer; 20 qubit system available on IBM Cloud". November 2017. https://www.datacenterdynamics.com/news/ibm-reveals-50-qubit-quantum-computer-20-qubit-system-available-on-ibm-cloud/

[40] Hui, J. "QC — How to build a Quantum Computer with Trapped Ions?" January 2019. https://medium.com/@jonathan_hui/qc-how-to-build-a-quantum-computer-with-trapped-ions-88b958b81484

[41] Ross, C., Hainzer, H., Kiesenhofer, D. and Franke, J. "Simulating 2D Spin Lattices with Ion Crystals" *University of Innsbruck.* https://quantumoptics.at/en/component/content/index.php?option=com_content&view=category&id=10&Itemid=121

[42] "Google Achieves Quantum Supremacy with its 54-qubit Sycamore Processor" *TecheBlog.* October 2019. https://www.techeblog.com/google-quantum-supremacy-sycamore-processor/

[43] DARPA. https://en.wikipedia.org/wiki/DARPA

[44] QuIST. https://en.wikipedia.org/wiki/QuIST

[45] "Spain, world pioneer in quantum cryptography" June 2018. https://quitemadorg.wordpress.com/2018/06/19/spain-world-pioneer-in-quantum-cryptography/

[46] Martin, V. "Madrid SDN Quantum Network". *CCS Center for Computational Simulation.* May 2019. https://plataforma-aeroespacial.es/wp-content/uploads/2019/05/UPM-VICENTE-MARTIN.pdf

[47] Langer, T. "SECOQC" https://slideplayer.com/slide/8594272/

[48] CORDIS, EU research results. "Development of a Global Network for Secure Communication based on Quantum Cryptography. SECOQC". April 2004. https://cordis.europa.eu/project/rcn/71407/factsheet/en

[49] Popkin G. "China's quantum satellite achieves 'spooky action' at record distance". *AAAS.* June 2015. https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

[50] Emerging Technology from the arXiv. "Chinese satellite uses quantum cryptography for secure videoconference between continents". *MIT Technology Review.* January 2018. https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/

[51] Majumdar, D. "Quantum Radars: China's New Weapon to Take Out U.S. Stealth Fighters (Like the F-22)?". *The National Interest.* February 2019. https://nationalinterest.org/blog/buzz/quantum-radars-chinas-new-weapon-take-out-us-stealth-fighters-f-22-44652

[52] Emerging Technology from the arXiv. "Quantum radar has been demonstrated for the first time". *MIT Technology Review*. August 2019. https://www.technologyreview.com/s/614160/quantum-radar-has-been-demonstrated-for-the-first-time/

[53] Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. "Report on Post-Quantum Cryptography" *NIST. National Institute of Standards and Technology.* NISTIR 8105, April 2016.

[54] Shor's Algorithm. https://en.wikipedia.org/wiki/Shor%27s_algorithm

[55] Post-quantum Cryptography. https://en.wikipedia.org/wiki/Post-quantum_cryptography