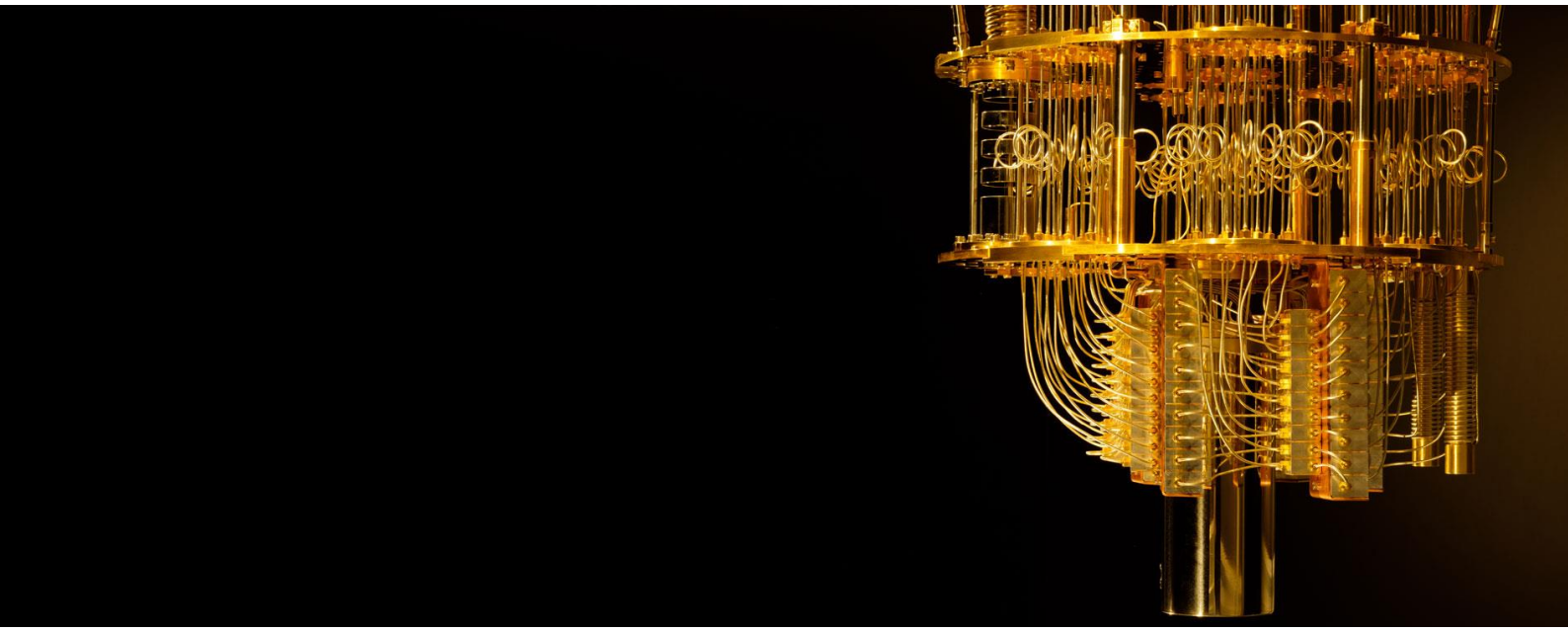
Studies on Quantum Cryptography

By Julio Nevado Delgado

Tutor: Luis Enrique García Muñoz

Universidad Carlos III de Madrid

11th December, 2019, Leganés



Index

Abstract

It should come as no surprise the fact that technology develops by leaps and bounds, not mattering which subject we are talking about. In this report, we are going to focus on quantum mechanics and its applications to security.

First, I am going to summarize some lectures from "Quantum Mechanics. The Theoretical Minimum. What You Need to Know to Start Doing Physics" by Leonard Susskind and Art Friedman. This way, I will introduce quantum mechanics in order to apply these concepts on later sections.

Next, I will talk about the manual of our set-up, were some concepts of the ones present in the first part of the essay are applied to our specific experiment. Here, I will analyse any possible outcomes both situations, in the presence of an eavesdropper and as a point-to-point safe link (it is, no eavesdropping)

Following, I will represent and explain my own experiment using the set-up previously mentioned. We transmit a 10-bit keys using 10 different basis. Behaviour, goals and advantages of this kind of technology shall be cleared up in this section.

Concluding, I am going to analyse how quantum cryptography is used nowadays, most used protocols, and which companies or institution are developing quantum cryptography systems. I will also talk about various tests done in this field.

Keywords: quantum, cryptography, crypto, spin, state, entanglement, BB84, network, encoding, technology, companies, commercial, orthonormal, basis, bit.

Index

1. Summary of "Quantum Mechanics. The Theoretical Minimum. What You Need to Know to Start Doing Physics"

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.

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.

1.1 Systems and Experiments

As mentioned before, quantum mechanics studies the behaviour 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.

1.1.1 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).

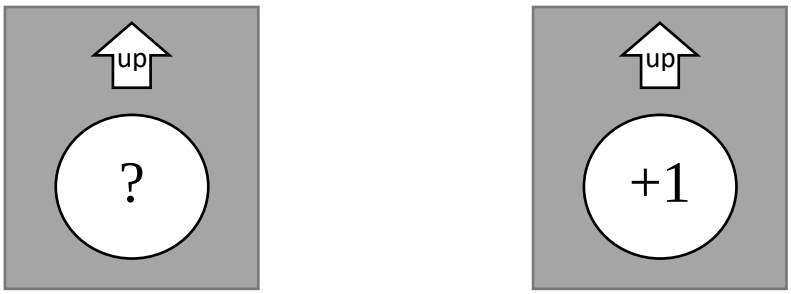
1.1.2 An experiment

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.

1.1.3 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 measurements, 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". There is no way to know the components of a spin along two different directions simultaneously.

1.1.4 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.

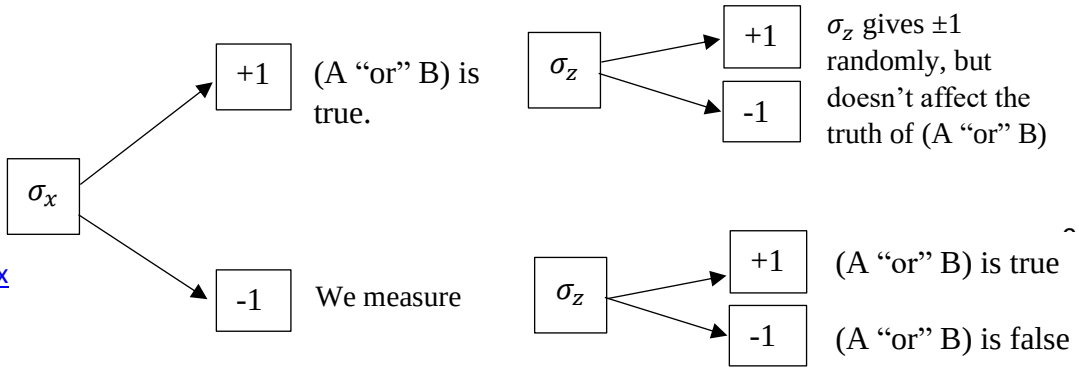
Now for testing quantum propositions we will also use "and", "or" and "not". Taking the following two propositions:

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.



Index

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.

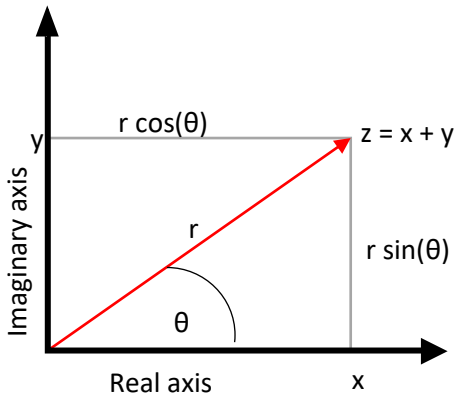
To test (A "and" B) the same procedure is followed. There is a possibility that the results are σ_z= +1 and σ_x= +1 after the first two measurements but we have to remember that the act of taking the second measurement disrupts the first one, making it not confirmable. This is called the uncertainty 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.

1.1.5 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:

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

$$z^* z = 1$$

1.1.5.1 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.
   $z\{|A\rangle + |B\rangle\} = z|A\rangle + z|B\rangle$
   $\{z + w\}|A\rangle = z|A\rangle + w|B\rangle$

1.1.5.2 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.

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

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

1.1.5.3 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 $\langle A|=(\alpha_1^* \quad \alpha_2^*)$

1.1.5.4 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 $\langle B|A\rangle=0$

1.1.5.5 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.

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

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

1.2 Quantum states

1.2.1 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:

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

$P_d = \langle A|d\rangle\langle d|A\rangle$ $\qquad$ Because $|A\rangle$ 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.

1.2.2 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 $|o\rangle$.

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

1.3 Quantum mechanics principles

1.3.1 Mathematical approach

First place, I should clarify some recurrent concepts now on. Firstly, 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. Classic vision of vectors will be referred now on as 3-vectors.

Observables are the things we measure and, despite de 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 thinking 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 in.

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.

1.3.1.1 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 say $[\boldsymbol{M}^{T}]^{*}$ where conjugation will be applied element-by-element

1.3.1.2 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 a 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.

1.3.1.3 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 eigenvector 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.

1.3.2 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:

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

1.3.3 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 We could get this way 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 a 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.

1.3.4 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:

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

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

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.

2. Quantum cryptography demonstration kit

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 is 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.

2.1 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. 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		

2.2 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 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 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.

2.3 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 only half of the time.

To summarize this last case, we see that, even though Alice and Bob have chosen the same basis, they obtained a 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.

2.4 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 to this. As an example, a particle such 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.

2.5 What prevents from simply 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, taking it, 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.

2.6 The 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 is to send. Bob, also chooses randomly the basis he is going to measure in. The choice of both basis 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.

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

2.8 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 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 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.

2.9 Analysing the experiment

Alice		**Bob**		
State	**Basis,bit**	**Basis**	**State**	**Bit**
$\|0^o\rangle$	+,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 or 1 50%
$\|90^o\rangle$	+,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 or 1 50%
$\|45^o\rangle$	x,1	+	$M_+\|45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle - \frac{1}{\sqrt{2}}\|90^o\rangle$	0 or 1 50%
		x	$M_x\|45^o\rangle = \|45^o\rangle$	1
$\|-45^o\rangle$	x,0	+	$M_+\|-45^o\rangle = \frac{1}{\sqrt{2}}\|0^o\rangle + \frac{1}{\sqrt{2}}\|90^o\rangle$	0 or 1 50%
		x	$M_x\|-45^o\rangle = -\|-45^o\rangle$	0

Green cases show 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**	**Measured 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 or 1 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 or 1 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 or 1 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 or 1 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 or 1 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 or 1 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 or 1 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 or 1 50%
					x	$M_x\|-45^o\rangle = -\|-45^o\rangle$	0

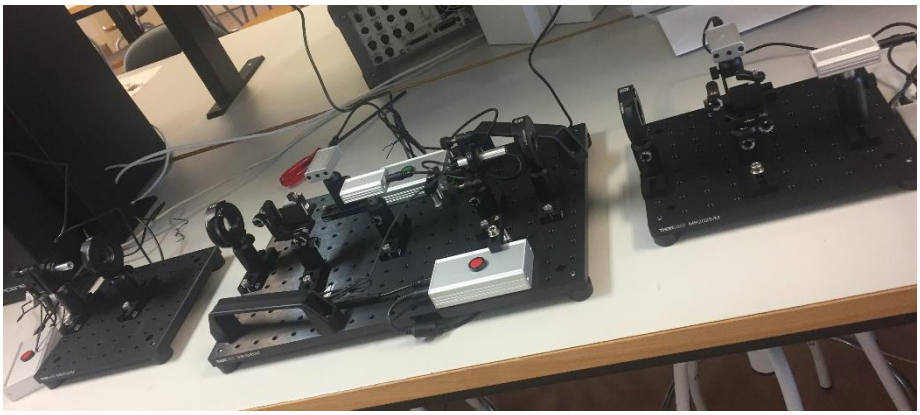
In this chart, the grey cases correspond to Alice and Bob using different basis, so the effect of Eve would not be relevant because these bits would be removed from the key.

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.

3. Our experiment

In order to demonstrate the functioning of the Quantum Cryptography Demonstration Kit, we made an experiment where we repeated 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 chose a 10-bit long string of 0s and 1s as the key. We simulated the transmission of that key using ten different and random sets of bases. Bob also chose ten sets of bases randomly to measure each transmission from Alice. Lastly, Eve only chose one set of bases she used 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 the 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's not.

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

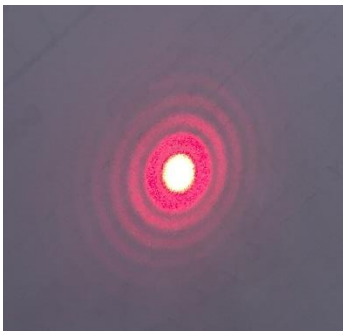
These two previous cases take place when Eve has a different basis than Alice and Bob so when she measures Alice, she will get either 0 or 1 with same probability, and Bob will also read 0 or 1 randomly. According to Bob's chart, Eve is caught thirteen times while she is unnoticed sixteen times (among 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.

3.1 Testing transmission maximum 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 longer than the one specified in the manual (60 cm).

At a distance of approximately 6 metres 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.

4. Use and development of quantum cryptography nowadays

Quantum cryptography seems to be a major target for many huge companies worldwide. However, this technology is still growing. It is no more about bits, it is about qubits, in other words, quantum systems. This technology is based on one of the main principles of quantum mechanics, that is, no quantum system can be measured without disturbing it. This report is going to analyse what are some of the main technologic companies looking for and where are they going. Despite this, not only companies are interested in this subject, also some institutions are looking for a top position. Before starting, it is worth mentioning the fact that this is still a developing technology so most of the following cases of study are approaches to this kind of technology there being only a few cases were this technology was really put in practice.

First, let's define some recurrent concepts now on:

- QKD: stands for quantum key distribution. This means the use of quantum crypto to create ultra-safe keys. It is often confused with the quantum crypto concept itself because most of current applications of this kind of cryptography are based on quantum key distribution.
- No-cloning theorem: This theorem is based on the fundamental principle of quantum mechanics, which says no quantum system can be measured without disturbing it in some way.

4.1 Current Protocols

In this section I am going to describe shortly how most significant existing protocols work, however, its use will be shown in the remaining sections of the report. It is worth clearing up the fact that most of existing protocols are based on the previously mentioned no-cloning theorem.

4.1.1 BB84 protocol

This protocol was originally developed by Charles Bennett and Gilles Brassard. It lays on single photons which are sent with a certain polarization. It involves two channels which interconnect both endings of the communication. The first channel is a quantum channel, where the key is going to be created and exchanged, while the second one is a classic channel such as a phone line.

In this protocol there are two different basis, x basis and + basis. In + basis, 0º means sending a 0 and 90º a 1, while in the x basis -45º means a 0 and +45º a 1. All these degrees are referred to the vertical component and represent the direction in which the photon is polarized, in which the photon vibrates.

As a first step, Alice (the sending end) sends Bob (the receiving end) a series of 1s and 0s (randomly) choosing random basis. Bob receives them using a random basis too. If Alice and Bob are using the same base, then the bits Bob will read will be the same Alice sent. Nevertheless, if Alice and Bob use different basis, the results Bob will read will be completely unpredictable (always between 0 and 1). These bits Bob receive are known as the raw key.

Next, Bob and Alice exchange basis (only the basis, not the bits) through the classic channel. Both keep the bits Alice transmitted when the two of them used the same basis and discard the rest. These bits are called the shifted key. However, this is not the final key since Alice and Bob will exchange some of these bits (using the classic channel) aiming to detect eavesdropping. If no eavesdropping is detected (bits exchanged are the same), then these bits are removed from shifted key giving place to the secret key, the final key. In the case bits do not match, eavesdropping is supposed to be detected and protocol is aborted.

4.1.2 Decoy state protocol

One of the main weaknesses of QKD is that many lasers are not always able to emit a single photon. Sometimes, due to manufacture issues, these sources send a set of photons. If BB84 was applied, then an eavesdropper (supposed to be technologically super-advanced) could take some photons from the flow and take the information they are carrying, leaving the rest undisturbed. That way the no-cloning theorem would not be violated, and communication could be taken by entities outside the link. This kind of hack is known as photon number splitting or PNS.

This protocol was first designed in 2003 by Won-Young Hwang, who proposes a way to solve this problem. This solution is based on two photon sources, the first one transmits the photons which will produce the key and a second one used as a trap for eavesdroppers. The first source is used to apply the BB84 protocol previously described (a single photon is sent except isolated cases when, as a result of unavoidable imperfections during sources manufacturing process, a group of photons is sent). Alice uses with certain probability p the trap source. The polarization of the photons produced by both sources must be equal (always within the basis described in previous section) so that a potential eavesdropper cannot be able to detect which source was used. After the photons are exchanged, Alice announces through the conventional channel which source was used in the transmission of each bit. If the yield of the set of photons transmitted by the fake source is much higher than the transmitted by the real one, then eavesdropping is detected and protocol aborted.

4.1.3 E91 protocol

This protocol is quite similar to BB84. Its main difference is the need for a source of entangled photons which could be either Alice or Bob. Here we also have two different basis, X and +. A sequence of entangled pair of photons must be generated, and a photon from each pair is sent to each end. The result obtained by Alice and Bob obtained if measuring using the same basis is exactly the opposite due to entanglement and total anticorrelation.

So functioning is each end using random basis measure the sequence spin of the sequence of photons. Then, Alice and Bob exchange basis and as in BB84 protocol, keeping the measurements where both used same basis. Bob then switches the bits where both used same basis.

They take the results obtained when using different basis and check if it fulfils Bell's equation. If no Eve is present, then these values should not fulfil Bell's equation. However, if eavesdropping occurs, Bell's equation is fulfilled and then eavesdropper is detected.

It is useful noticing the key would be absolutely random since we do not know the initial polarization of each pair of photons.

4.1.4 SARG04 protocol

SARG04 is quite similar to BB84 protocol. The differences show up in the stage where Alice and Bob exchange basis, where Alice tells Bob a pair of non-orthogonal states, being one of them the one used to encrypt the bit. If Bob chose the correct basis, his measure will match the bit sent by Alice. Other way, his measure could not match the bit sent, so it is discarded. The security of SARG04 protocol is quite similar to BB84, the difference remains mainly in the fact that a single-photon source is not needed since laser pulses are used instead.

However, SARG04 protocol main weakness is the presence of quantum channel losses, where the QBER (i.e. quantum bit error rate) increases notably.

4.2 QKD: Advantages and disadvantages

4.2.1 Advantages

Physics laws

This kind of crypto is based on physics laws, rather than solving complex mathematical problems. Because of this, no supercomputer could break into our communication, since it is not a matter of power, it is a matter of physics.

Ultra-safe

As a result of the previous section, hacking it is impossible if correctly implemented, or at least impossible hacking it without noticing. This is due to the fact that quantum crypto relies in physics and no one could cheat on physics. As said in the protocols section if someone was to hack us, we would probably detect.

Of course it could happen (only as a matter of chance) the eavesdropper would not be detected since there is still a little opportunity for Eve to remain unnoticed. Even though, we are always supposing Eve has the means needed to spy on our communication. Despite in other areas of security hacking is ahead of security itself, here we are talking about a developing technology yet. Furthermore, when quantum crypto systems will be fully developed, devices needed to carry out espionage will probably still unavoidable for hackers. It is not like common algorithms relying in complex mathematical problems, where most people could have access to a powerful computer and a brilliant mind.

Despite all of this, we will probably never get rid of hackers and mis intentioned people.

Simple to use

As shown in the section “Our experiment”, the performance is quite simple. We only have to choose a random basis at both ends of the communication. The complexity relies more in creating trustworthy sources of single photons rather than in the performance itself.

4.2.2 Disadvantages

Implementing this technology is quite complex

As said previously, the most difficult part in this technology is implementing it.

Firstly, today's protocols are based on ideal sources (the majority), but used sources are not always ideal so these protocols are still not as safe as they shall be in the future. For example, BB84 implies an ideal source since if the source produced a set of photons, the eavesdropper could take some photons from the flux in order to measure the information sent and left the rest of the photons undisturbed so Alice and Bob would never notice Eve. This is called PNS. There are some other protocols such as Decoy State protocol which tries to solve this issue but are not such advanced today as BB84 is.

Another problem is the fact that a different channel is needed for each different user connected to the network since we cannot multiplex and demultiplex the quantum information due one more time to physics laws.

Still developing

Nowadays quantum crypto is a growing technology. That is why it cannot be deployed as a reliable a functional system yet. More research is needed in order to allow this technology interconnect hundreds or even thousands of simultaneous users. Most current implementations are simply testbeds as we will see later, only in some exceptional cases quantum is used in "real life", such as the internal network of an enterprise or to carry out trustworthy election.

Very expensive

As a result from previous point, quantum crypto is still too expensive. This keep non-huge firms far from this technology. Only big firms and research institutions can afford using this technology. In fact, the cases this is used are mainly due for test purposes rather than the fact quantum crypto is safer than common crypto. In fact, nowadays common cryptographic technics are enough in the vast majority of cases.

Long distance communications

The distance between both ends of the link is quite limited (if communication is terrestrial) because of the no-cloning theorem. A special amplifier is needed because the photon's polarization could be easily disturbed.

Despite existing amplifier nodes currently, they are a weak point of the communication.

4.3 Companies and institutions which develop QKD systems

4.3.1 BBN Technologies

BBN Technologies is a company settled in Cambridge (Massachusetts) focused on I+D. It was founded in 1948 by Leo Beranek and Richard Bolt, who were both professors at MIT (Massachusetts Institute of Technology). Among its achievements the following should be emphasised:

- Development and implementation of ARPANET
- First email person to person.

In 2004, collaborating with DARPA (Defence Advanced Research Projects Agency), an organization dependent from the Pentagon, developed the first quantum network containing more than two nodes, which was called the Qnet. This network was composed of 6 nodes at first (reaching 10 later), interconnected by optic fiber. Four of them were inside BBN Technologies facilities. This network was based on two transmitters applying BB84 protocol. It interconnected BBN headquarters with Boston and Harvard Universities. The networks contained a switch which allowed every node to connect each other. Qnet was 10km between BBN and Harvard and 19km between BBN and Boston University. It had a 3% QBER and could be integrated with nowadays internet networks. Precisely it was the Internet security protocols where keys obtained from this system were integrated in order to protect user traffic.

According to BBN, this quantum networks would be quite useful to many enterprises and to protect the connection between client homes and their ISPs.

This network was used between 2004 and 2007 although some tests were done a year earlier (these tests inside a lab).

The aim of this network, as most of described in this report, was mainly to be a trial in order to make an approach to this technology.

4.3.2 Mitsubishi & NEC

These companies developed the first quantum network in Tokyo in 2006. This network interconnects Koganei and Otemachi through a link of about 45km. It also connects Otemachi with Hakusan (12 km link) and Hongo (13 km link). According to Mitsubishi, this network divides in three layers: the quantum layer, the key layer, and communication layer.

Figure 1. This picture shows the interconnection of the network. (Mitsubishi Electric, 2010)

The first one is responsible for carrying out QKD, while de second one supervises this process (acts like a link between first and third layer). The third layer carries out ultra-safe communications using the key it is given by previous layers.

The goal of this network is said to be mainly as a test, aiming to work with worldwide companies in order to achieve interconnecting different QKD networks. Nevertheless, the Japanese also want to be able to transmit video in an ultra-safe way.

Despite this, Japanese actual desire is to use quantum networks in government agencies and critical infrastructures, although this is a long-term goal.

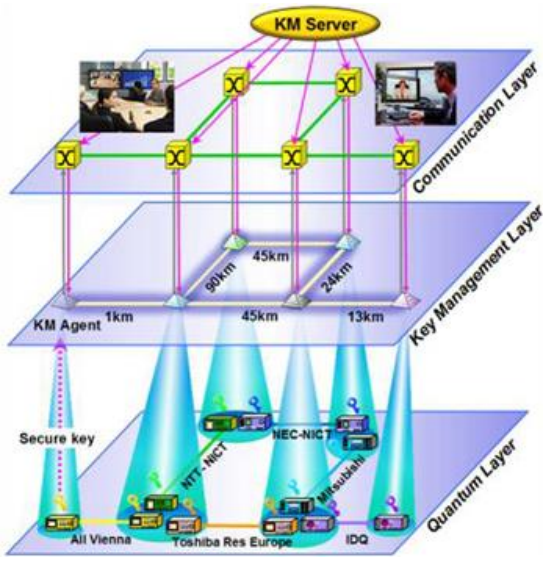


Figure 2. The set of three layers which build up the network. (Mitsubishi Electric, 2010)

This network is still working for test purposes.

4.3.2 ID Quantique

ID Quantique is a Swiss enterprise settled in Geneva and founded in 2001 by physicists from University of Geneva. Its aim is to use quantum mechanics as the key in the future of technology. It is specialized in security and it is responsible of some of the achievements later discussed:

- Swiss election.
- Battelle Memorial Institute private network.

In this section I am going to talk about SwissQuantum, a network developed by ID Quantique joining forces with the University of Geneva. This network was composed by three nodes: The University of Geneva itself, CERN (European Organisation for Nuclear Research) and Hepia, Geneva School of Engineering and Architecture. This network allowed the interconnection between the three nodes in pairs. This was the first international quantum network since one of its nodes (CERN) is in France, while the other two are in Switzerland. This network consisted of 3 layers:

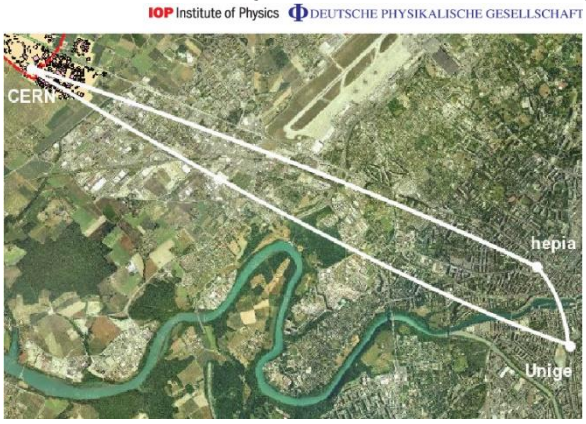


Figure 3. SwissQuantum schematic Hepia and Geneva University in Swizterland. CERN in France. (ResearchGate, 2012)

1. The first layer was known as the quantum layer. It was built up by point-to-point quantum links and was implemented by servers developed by ID Quantique (id5100 devices). These servers could perform both, the BB84 protocol (described before) and the SARG protocol (which differ with the BB84 because of its robustness in matter of PNS). Because of this, only SARG protocol was used.
2. Second layer managed keys all around de net. It was a kind of adapter between already developed infrastructures and this emerging technology.
3. This third layer was an application layer. It was a common communication which used the key supplied by the previous layers.

Encoding was at layer 2 (link layer) reaching a bit rate of 10Gbps. Each node used WDM (wavelength division multiplex) making the network able to use all of the classic channels existing in each of the three ends.

This network ran for about 2 years (2009 – 2011), however, its aim was, like most of existing networks nowadays, purely as a testbed of the quantum layer. Despite this, SwissQuantum network proved QKD systems are developed enough to be commercially used in telecommunicating networks.(RW.ERROR - Unable to find reference:doc:5dc1705de4b08420b0b38a36)

4.3.3 Los Alamos National Laboratory

Los Alamos National Laboratory is settled in Nuevo Mexico. It is managed by the University of California and its aim is to watch over national security through science

This laboratory developed in 2012 a quantum smart card known as QKarD. This card is a mini transmitter which can be used to encode a computer or a mobile phone among many other devices. "A user needs only to periodically insert the device into a base station for authentication, requiring both a fingerprint and a personal identification number (PIN)." (Los Alamos National Laboratory). This way, we would get a random key from a trusted server to carry out the encoding. This key will be stored in the memory of the encoded device.

Figure 4. First generation of QKarD. (ResearchGate, 2013)

It is the laboratory itself which points out some useful situations for this QKarD, from which most important are:

- Telecommunication (phone calls, videoconferences…)
- Electronic voting.
- Digitalized businesses.

QKarD was tested in the University of Illinois by securing control data in electric grids. Due to the appearance of alternative energy sources, data must be transmitted between control centres, but this data must be trusted, and the communication must have low latency. That is why QKarD has an especial interest for controlling electric grids. Even some enterprises from this sector have already asked Los Alamos National Laboratory for the licence of QKarD.

It has also been tested that both, QKD and data transmission could take place using the same optic fiber.

New versions of QKarD are said to have a generator of quantum numbers, with data rates of about 5Gbps.

4.3.4 Telefonica

Telefonica is researching on how quantum cryptography can help improving its security. However, this company has already reached some milestones. It has achieved, with the help of UPM and using technology provided by Huawei, interconnect three of its POPs (points of presence, places where two or more networks interconnect) in Madrid using quantum cryptography. This connection is carried out through optic fiber.

This network is based on CV-QKD (continuous variable quantum key distribution) which has as a main feature its greater immunity to noise. Despite this, this network is prepared to work with any other kind of QKD.

Even though this is a great achievement, it is only a test, that is why its use is quite limited.

4.3.5 QuTech and ABN AMRO

In 2019, the research group QuTech and ABN AMRO bank announced an association to develop what is called MDI-QKD (Measurement-device-independent quantum key distribution). Both firms settle on the Netherlands. The first one is headquartered in the University of Delft while ABN AMRO, founded in 1991, in Amsterdam.

MDI-QKD solves problems related to single photon detectors. In addition, this kind of QKD allows thousands of users interconnect each other as a result of the fact that it is no longer a point-to-point connection. Now each user of the network sends photons to a kind of central. It's necessary to think about what this would mean to a sector like banking because this is a service which could be used by thousands of users at the same time and this way it would not be necessary to have an end of the connection for each connected user.

However, the great disadvantage of MDI-QKD is the fact that it has not been tested within classic data transfer systems yet, so it is not guaranteed that these technologies could be integrated together. The issue with using MDI-QKD in the same optic fiber used for classic data is that distortion in photons could appear so that the information it carries could be thrown away.

This network is planned to run over optic fiber and air. ABN AMRO's plan is to implement this technology as soon as possible because of their awareness of the weaknesses of conventional cryptographic techniques if we think of them as being threatened by quantum

computers in the future. They hope being able transmitting data by the end of 2020 through this network.

4.3.6 IBM

IBM is doubtlessly the firm which harder works in the development of this technology, not only regarding to cryptographical applications though. IBM has been the first enterprise in building a quantum computer for commercial use, the IBM Q System One, which was announced in January 2019. Its power is 20 qubits, 2.7m high and 2.7m wide. However, it is clear this technology is still far from being present in our daily life.

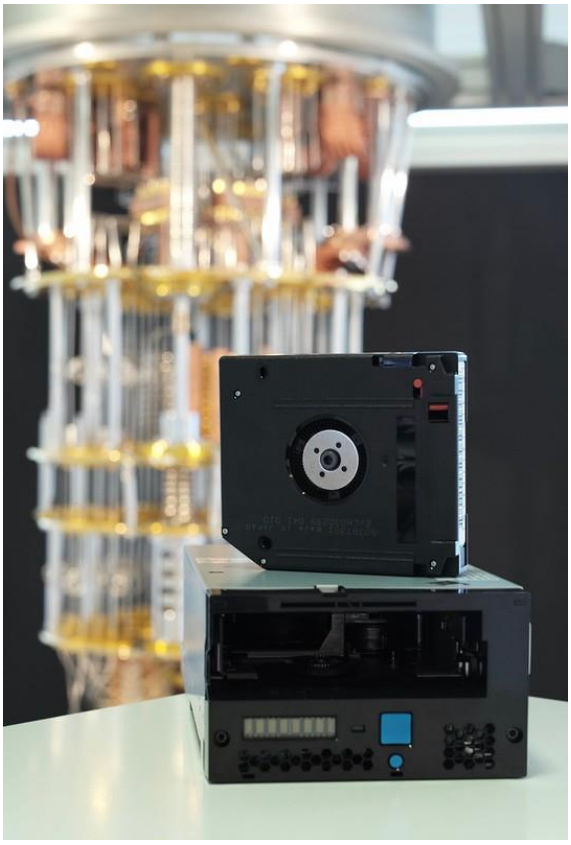


Figure 5. A picture of the ultra-safe tape drive. (IBM, 2019)

Despite this, IBM has announced the development of a quantum computer with about 53 qubits. This quantum computer will be part of IBM quantum computing centre, which will also hold five 20-qubit quantum computers.

IBM is concerned about danger coming from future quantum computers, who could break down nowadays encryption algorithms. They have recently developed an ultra-safe tape drive (a storage system based on magnetic tape) which is said to be resistant to these kinds of attacks. It is based on Kyber and Dilithium, two algorithms prepared to face quantum computers, along with symmetric encryption. These algorithms are part of tape drive's firmware so that current users could get this improved security through a firmware update.

Even though IBM is already working on postquantum cryptography, they believe this kind of encoding would not be truly necessary until ten to thirty years. Nevertheless, IBM shows this way they are a foresighted firm, aiming users not to have a drastic change some years in the future.

4.3.7 Google

Google is thought to be in the pole in terms of quantum computing development due to a 72-qubit quantum computer they are creating. They have also announced having reached quantum supremacy, this means, having performed using a quantum computer a task which would have been impossible using the most powerful supercomputer. Even though no details about this milestone have been unveiled, it is said it would have taken nowadays fastest supercomputer about 10,000 years while it only took 200 seconds Google quantum computer solving this unknown task.

However, quantum computing could also be a hard opponent for conventional cryptographical algorithms. This is because common algorithms lay on complex mathematical problems, problems that quantum computer shall easily solve due to their huge computational power. Postquantum cryptography is referred to algorithms aiming to face attacks from quantum computers. Although quantum computers are still harmless, Google is already implementing postquantum crypto in the test version of its browser, Google Chrome Canary.

4.4 Companies, institutions or areas where quantum cryptography is used

4.4.1 NASA

Nasa has invited the Australian start-up Quintessence Labs to its Ames Research Centre in Silicon Valley. This company suggests using quantum mechanics to establish an ultra-safe communication with JPL (Jet Propulsion Laboratory) located in Los Angeles, setting up this way a 600km connection. Nasa makes clear this way its interest in this kind of cryptography, being aware of future danger coming from quantum computers.

Quintessence Labs is a company headquartered in Canberra. It was founded in 2006 by Vikram Sharma, a doctorate from Australian University. Australia is conscious Quintessence Labs is a leading company in this sector, that is why the Australian army subsidized it with 1.1M$.

4.4.2 Banking

As technology has been developing in last years, Banks have been adapting this progress. That is why years ago online banking appeared. Through this platform every kind of transfers and payments can be done, something very attractive to hackers, who constantly try to take advantage of the weaknesses of current encryption systems to carry out different types of fraud.

That's why many Banks (as mentioned in previous section) are focusing con quantum crypto. However, QKD is not something new in this sector. The first bank transfer using this kind of crypto dates from 2004 in Vienna between Bank Austria Creditanstalt and Vienna's city hall both away by 1.4km of optic fiber. This transfer used entangled photons. These entangled photons were created by splitting two pairs of photons using a special glass. A photon from each pair of entangled particles was sent to the hall of Vienna while the remaining particles stayed at the bank. This protocol consists of (which should come as no surprise) measuring the polarization of the "sending" photon. Due to quantum mechanics, disturbing polarization of an electron belonging to an entangled pair would immediately disturb the polarization of its pair. This, done in a controlled way, was used for the transmission of the key. This occurs because particles are correlated. If the case of eavesdropping was given, the eavesdropping itself would destroy this correlation, so the spy would be detected immediately.

This achievement was carried out by the University of Vienna.

4.4.3 Barclays PLC

Barclays is a well-known English bank established in 1960. It is headquartered in London and it is considered one of the most important banks worldwide.

Barclays has created a section which is investigating what quantum computing could offer the firm, not only referring to crypto, but also referring to the computational power of this devices. They even have been using IBM's quantum computer.

Barclays' goal is to use quantum computing in solving problems that would impossible for common computers in a realistic time. These operations could be solved by quantum computers in few minutes. Despite the fact that the quantum computer they are using to carry out their tests is a 16-qubit computer, they think this will be less than they would need in the future. They estimate they will need thousands of qubits to carry out their operations. As we can see, this technology is still far away.

4.4.4 Election

On 21 October 2007, federal election took place in Switzerland. A quantum connection was used to send the votes from counting centres to the data central in Geneva. This technology was supplied by ID Quantique. This connection is based on the combination of layer two encryption with Cerberis, a QKD system created by this swiss enterprise.

Cerberis is a successful quantum encryption system. The third and newest version is built up by a transmitter and a receiver who distribute ultra-safe keys for communication. It also involves a node controller which function is to send the key to the link encoders or to other link users.

Because of the success of this system, the Canton of Geneva has been using quantum crypto in both, general and Canton election as well as for citizens' initiative voting. This way, Switzerland has become one of the top countries regarding security in choosing their political representatives. After the US crisis due to privacy violation of many clients by companies like Google, many other enterprises have focused on Switzerland in order to keep safe their data,

raising Switzerland this way as a standard bearer referring to security. This could not have been possible without the appearance of companies of this nature like ID Quantique.

4.4.5 Battelle Memorial Institute

Battelle Memorial Institute is a non-profit organization established in Ohio state. Its activity focuses in technological development and research. “Battelle’s vision is to be a major force in science and technology discovery and in the translation of knowledge into innovative applications that have significant societal and economic impacts” (Battelle Memorial Institute).

This company uses QKD in order to interconnect their headquarters in Columbus and Dublin (both cities in Ohio state). It uses Cerberis, developed by ID Quantique. The encoder used in this network is also provided by ID Quantique. The whole system supplies a layer 2 encryption (link layer): “Combined with ID Quantique’s Centauris encryptor, this provides a 1Gbps link with Layer2 encryption” (Batelle Memorial Institute).

Apart from using quantum cryptography between its headquarters, Battelle says to be working along with ID Quantique aiming to solve the main limit to this technology, long-distance communications. The goal of this two firms is developing a new quantum device, the QKD Trusted Node™ which “…will allow a quantum network to expand the distance of QKD and to allow multiple destinations while retaining the secure nature of QKD.” (Batelle Memorial Institute). Battelle’s objective is to connect three of their headquarters in Columbus, creating a ring (Battelle quantum network o BQN) which will allow Battelle and other potential users connect this network in order to obtain ultra-safe keys.

However, Battelle’s ambition does not stop as they hope to connect their offices in Ohio with the ones in Washington DC, getting a quantum network more than 700km long.

4.4.6 Ultra-safe audio and video communications

On September 29th, in 2017, the first videocall using quantum cryptography was carried out between Chinese Academy of Sciences and Austria Academy of Sciences, both separated by 76000km. This system is based on the transmission of photons between both ends through Micius satellite. The use of this satellite is due to the main obstacle in QKD systems in long distances,

which is the losses because of the channel. Losses are notably reduced regarding the fact that most part of the link is in vacuum, where losses are minimum

This communication was carried out using BB84 protocol. This system is astonishingly high. QBER detected is between 1% and 2.4% due to polarization errors and noise.

This video conference lasted about eighty minutes. The amount of data transmitted was about 2GB.

These entities plan to higher-orbit satellites in order to increase the area and time coverage along with multipoint connections. They explain that the main weaknesses of this system are the fact that they have to trust the satellite, something which could be avoided by using entangled photons.

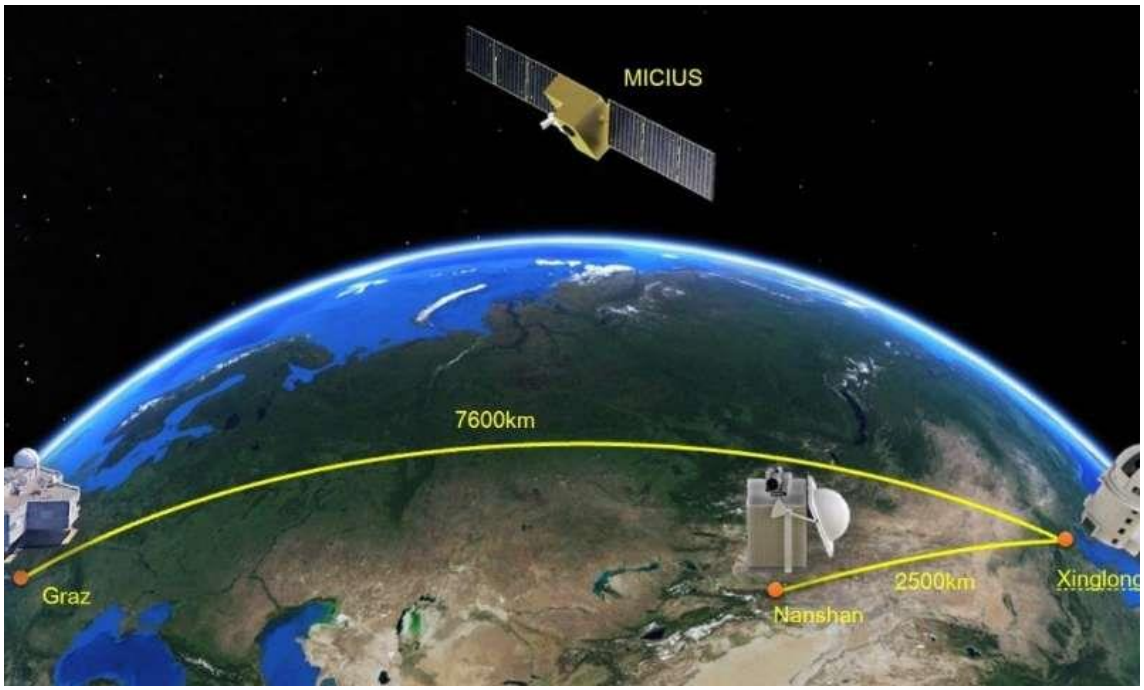


Figure 6. Diagram of the network established for this long-distance communication. (Phys.org, (2018))

4.5 SECOQC

It is worth briefly talking about SECOQC despite not being a company or a specific organization working on quantum cryptography. SECOQC was a project launched by EU in 2004 by investing about 11M€ in order to develop this technology. This project resulted in a quantum backbone network which interconnected different Siemens headquarters in Vienna.

The demonstration of this network involved mainly a one-time pad encrypted phone call as well as a videoconference with each of the settled nodes of this network.

The project ended on September 2008 with an overall budget of about 17M€ (including EU investment).

5. Quantum funding

In this section of the report, I am going to analyse where quantum founding comes from and where it goes to, not only referring to cryptography, but also referring to computing and other quantum areas. We will see how lion's part of quantum funding comes from VC, which stands for Venture Capital. Venture Capital refers to risk capital, money which is invested in totally uncertain projects, as it is nowadays quantum tech, which although promising, still immaterial for real purposes. In order to start this section I will analyse the following diagram in order to settle a basis for the following appendices:

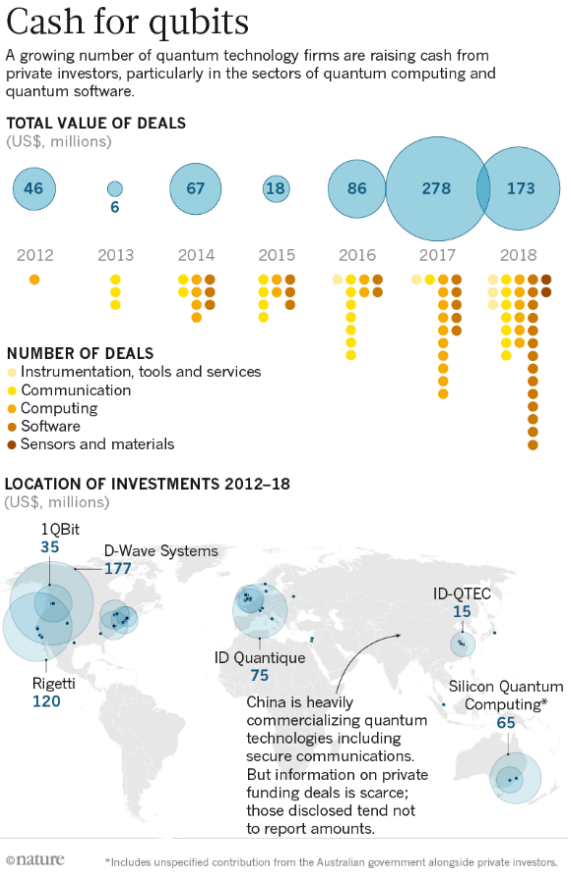


Figure 7. Investments in million dollars. (Nature, 2019)

This image clears the increasing importance given to quantum technology, expressed as millions of dollars invested which is probably the best sign for a growing technology. It is clear most companies settle in North America and Europe (mainly Great Britain, Switzerland and Austria). We can also see some spots in Australia.

While through this diagram China could be thought not to focus quantum technology, in fact is one of the main powers in these terms. This is because of the secrecy about all its developments.

We can also see greatest investments are made for software and communication purposes.

5.1 EUROPE

5.1.1 Quantum Flagship

Europe Union is conscious of the importance of rising technologies and specially about quantum, since it gives a new approach to supercomputing and security. That is why what is called "Quantum Flagship" has been deployed.

"Plans to build two working quantum computers are among the first winners to be announced in a ***€1-billion (US$1.1 billion) funding initiative of the European Commission.***

The Quantum Flagship was first announced in 2016, and on 29 October, the commission announced the first batch of fund recipients. ***The 20 international consortia, each of which includes public research institutions as well as industry, will receive a total of €132 million over 3 years for technology-demonstration projects.****"* (Castelvecchi, 2018)

EU's project focuses on different areas: *"The quantum flagship comprises* ***five thematic areas****:* ***quantum computers****; quantum simulations; quantum sensing and metrology;* ***quantum communications****; and basic quantum science."* (Castelvecchi, 2018)

Despite €1 billion could seem a lot, many experts think it will not make the difference in quantum R&D since that money is distributed along 10 years and destined to different areas.

5.1.2 Horizon 2020

Horizon 2020 is a R&D program promoted by Europe Union which started in 2014 not only quantum focused. It counts with an 80 thousand million euros budget and despite starting some years ago, it still has recent projects which will last some years past the fixed date. Quantum projects are an important part of this program and I will analyse some of them forwardly.

5.1.2.1 OPENQKD

OPENQKD is a project belonging to Horizon 2020 EU's plan coordinated by Austrian Institute of Technology GmbH. This project is expected to last until 2022.

OPENQKD was launched the 2nd September 2019. It involves thirteen countries aiming *"…to demonstrate the transparent integration of quantum-safe technologies and solutions broadly across the European digital landscape as well as advancing initiatives for the standardization and certification of QKD-enabled technologies. The work in the OPENQKD testbed should lay the foundations for rolling out a pan-European quantum-safe digital infrastructure"(Open european quantum key distribution testbed | OPENQKD project | H200.2019)*

This project is mix-funded among EU and some private investors. The overall budget of **OPENQKD** is almost **18M€, being EU investment 15M€.**

5.1.2.2 QUCUBE

This is another quantum focused project from H2020. Starting in 2019 and foreseeing to last until 2025, QUCUBE project aims to build a several-hundred qubits quantum computer. This project is **fully EU funded** with a total invest of **14M€** and it is hosted by the COMISARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES in France.

5.1.3 Germany

It is necessary talking about Germany, since it has been one of the leading countries referring to quantum investment due to a 650 million euros bet form federal government. The goal is to provide Germany with a key role in what experts call "the second quantum revolution" through its firms and institutions.

The initiative has been scheduled between 2018 and 2022, but probably extended to 2028. According to Andreas Toss in LaserFocusWorld:

"The program sets a number of goals that go far beyond basic research:

1. Expanding the research landscape of quantum technologies

2. Creating research networks for new applications

3. Establish lighthouse projects for industrial competitiveness

4. Ensuring security and technological sovereignty

5. Shaping international cooperation

6. Taking the people of our country with us

*These goals will extend the successful funding policy of the first quantum revolution, namely the laser technology. That means the program will fund basic research as well as common projects with industrial partners to ensure maximum impact of the involved money." (*Thoss, *2018)*

5.1.4 United Kingdom

If talking about Europe in terms of quantum funding, it is almost a duty talking about UK, one of the most active countries in the old continent referring to quantum research. This is clearly shown in the near **1 billion pounds** spent in quantum R&D along **ten years**. "*Driven by the efforts of a number of individuals, the UK government announced the NQTP in 2013 in order to take quantum information science in the UK toward a quantum technology that would provide new, worldleading information processing technology and seed a tech sector that would open new business opportunities and create economic opportunity for the UK."* (Knight & Walmsley, 2019) This project is divided in different phases. **The first one comprised the period between 2014 and 2019 was worth £380M.**

The second phase is said to start at the end of 2019: "*The largest enhancement in our second phase concerns the engagement with industry through the UK Industrial Strategy Challenge Fund (ISCF). A pilot scheme started in 2018 focussing on four industry-led challenges in the competition with £20M of government funding from Innovate UK and matched funding from industry. The aim was to explore the production of prototype devices that provide breakthrough capabilities to answer key end user challenges in sensing and secure information exchange. […] The success of this pilot industry engagement programme allowed us to bid for a further extended ISCF support for quantum technology and* ***on Monday 10th June 2019 the UK Prime Minister announced a further £153M*** *of government support with an* ***industry commitment of £205M.****"* (Knight & Walmsley, 2019)

5.2 North America

In this section, funding in America and Canada is going to be Analysed. According to a Forbes report, US is leading the funding of quantum tech:

"In December 2018, President Trump signed H.R. 6227 to fund the National Quantum Initiative Act (NQI). 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.

After President Trump signed the NQI, he followed up with an executive order to establish a National Quantum Initiative Advisory Committee composed of 22 experts from industry, research and federal agencies. The committee will meet at least twice a year to provide advice on our quantum activities."(Smith-Goodson, 2019).

However, United States hunger does not stop here and in addition: *"A few days after the executive order was signed,* ***the Department of Energy announced $80 million in funding for quantum research****."*(Smith-Goodson, 2019).

In fact, the US Department of Energy recently announced a new bet on quantum research of ***"$60.7 million*** *in order to develop quantum computing and networking"* (US Department of Energy, 2019)

This investment will be distributed as follows:

"Funding of ***$47 million will be provided for three five-year projects aimed at accelerating progress in quantum computing****. Projects will focus on the development of algorithms as well as the creation of a suite of traditional software tools and techniques— including programming languages, compilers, and debugging approaches—specifically designed for quantum computing.*

Funding of ***$13.7 million will be provided for five four-year projects aimed at developing wide-area quantum networks****, with the goal of greatly boosting the range of quantum-based communications. The goal is to develop long-distance quantum communication using existing fiber optic connections. New science and technology, such as quantum repeaters, will be*

needed to extend the current very limited range of such quantum networks." (US Department of Energy, 2019)

Nevertheless, this $1.2 billion are thought to be pretty poor if compared to China's efforts and investments, a rivalry which will be fully analysed later.

Concerning to quantum development we also find DARPA (Defence Advanced Research Projects Agency) which, as explained in previous sections in this report, aims to bring together army and new technologies (obviously including quantum ones). DARPA's budget for 2020 is $3.6 billion (not only focused to quantum research). However, DARPA's funding has been decreasing recent years, always according to Forbes, something obviously harmful for quantum development.

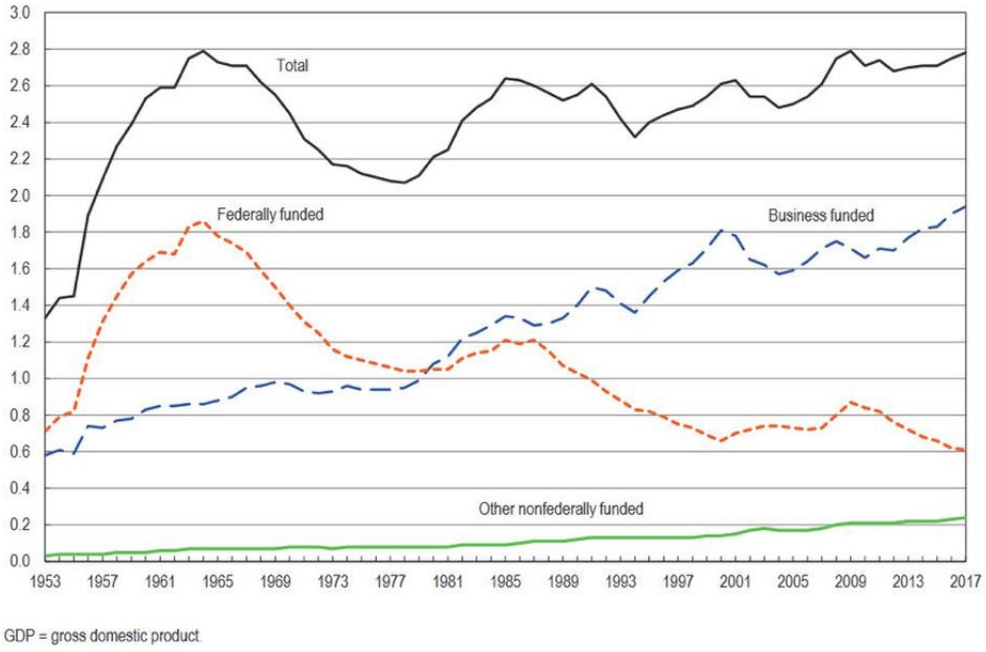


Figure 8. Evolution of technological funding. (Forbes, 2019)

Despite not showing data specifically about quantum technology, it is interesting to analyse the previous diagram as it shows the evolution of US R&D funding through years itemized in federal and non-federal investment as a percent of GDP. It is clear how government funding has decreased heavily the last fifty years. We can see nowadays federal investments is about 30% of total R&D funding. Obviously, as this affects to technology in general, it also affects to quantum technology. However, despite the decreasing in federal investment, R&D should not be damaged due to the astonishing increase of private funding. In fact, we can see how total funding has incremented in previous years, so good for R&D itself, worse for the people.

In respect to the US upper neighbour, Canada has also experienced some growth in this field as shown by Nature in one of its reports: "*North America has long been the world's leader in attracting VC cash, and Nature's analysis shows that the region also dominates private quantum investment. But the boom is not restricted to Silicon Valley*. ***Firms in Canada have attracted $243 million****, led by quantum-computing pioneer* ***D-Wave Systems, which alone has raised $177 million.*** *A whole ecosystem has emerged to support quantum companies around academic hubs in Waterloo and Toronto, which have benefited from public and philanthropic investment, tax advantages and successful incubators, says Jurczak.* ***A perceived immigration crackdown in the United States is also giving Canada an advantage in attracting talented quantum physicists,*** *says Xanadu's Weedbrook."*(Gibney, 2019). The mentioned Jurczak and Weedbrooks are both manager of their respective firms, this is, Quantonation the first (a venture fund looking for physics start-ups) and Xanadu the second (focuses in quantum computing).

5.3 China

The opposing party to North America is found in China. Although not referring to the amount of investment, but to the amount of information we get about those investments: *"Reports in English-language media and by Western analytics firms rarely cover deals in China, which often involve state-backed VC firms, so our analysis is likely to miss a large number of contracts there. And in our data, only one in ten fund-raising deals secured by Chinese firms disclosed its value."(Gibney, 2019)*

However, we could gain some insight through *The Washington Post: "Pan is also overseeing plans for a* ***new national lab for quantum research*** *in Anhui province, which he said had drawn about* ***$400 million in government funding****."*(Whalen, 2019) As we can see, China is secretly investing in this technology, in this case, in terms of infrastructure and facilities.

Some information about China's interests in quantum world could be obtained through the analysis of patents, something I will talk about in the next section.

5.4 US vs China

The perpetual competition among these two countries also comes to the field of quantum research. Despite China's secrecy, we can obtain some insight from data about patents.

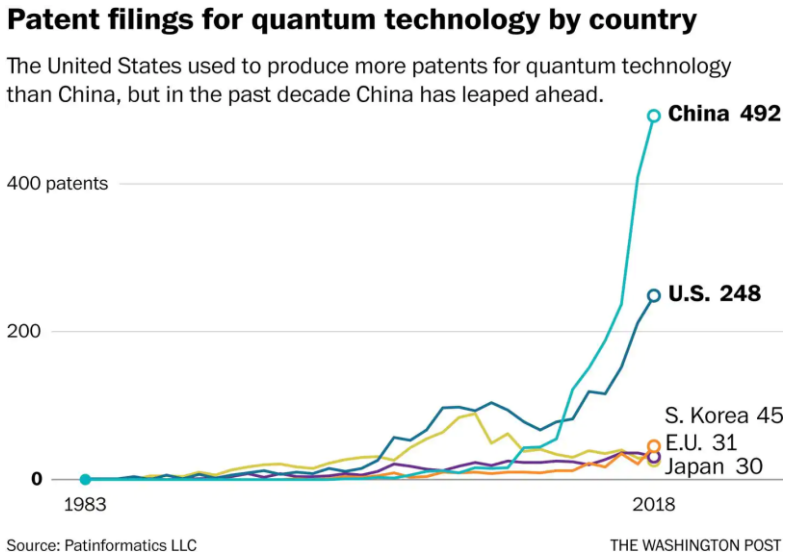


Figure 9. (The Washington Post, 2019)

In the previous diagram, patents by countries are represented through years. We can see how China has overtaken United States widely. In 2018, China filled almost twice the patents US did. Despite not talking about it publicly, it is clear China is focusing on quantum technology.

However, it is surprising analysing the number of patent fillings only referring to quantum computers.

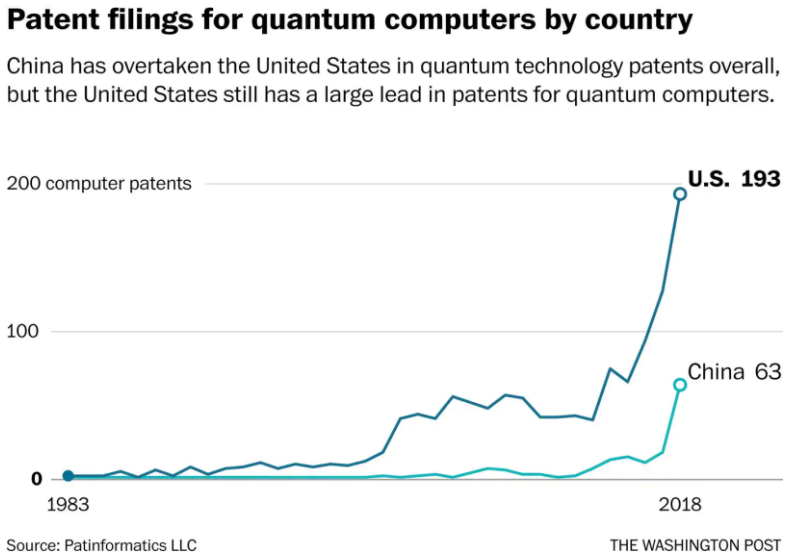


Figure 10. (The Whashington Post, 2019)

In terms of quantum computers China is clearly behind with less than three times the US patents. China is said to be focused on quantum technology but mostly regarding to secure communications.

This focus on ultra-safe communications by China is clearly showed in the long-distance communication between China and Vienna using the Micius satellite.

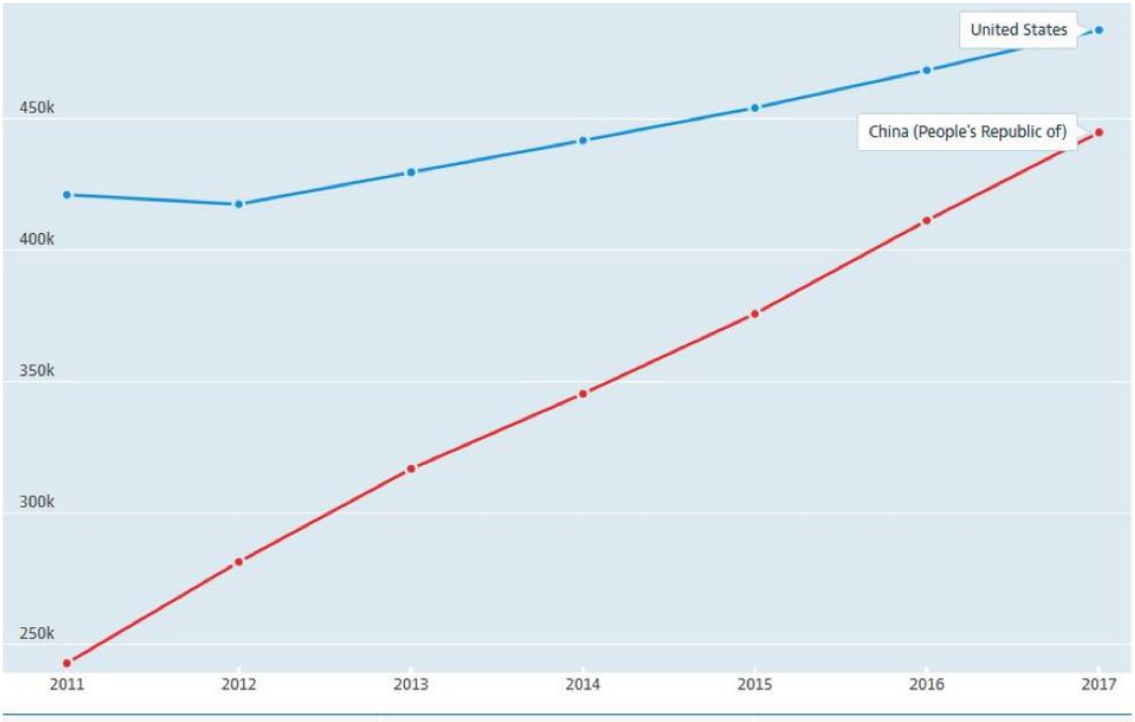


Figure 11. R&D investments in million dollars. (Forbes, 2019)

It could be useful analysing this photo since it helps us in gaining some insight in how China has move closer and closer in few years in terms of R&D investment (not only referring to quantum but could help us understanding Chinas approach to US). It only shows up to 2017 and, probably, nowadays China is already ahead of the United States.

It is clear the "quantum race" it is not between Google, IBM or any other US company, this battle faces United States and China. *"In implementation and use for strategic advantage then I would agree completely that China has an edge because no company in the world can compete against an entire country and China acts as a unit or as a collection of organizations while in the West we are not nearly as well coordinated"*(Trippe, 2019).

It is obviously not a secret in the United States: *"China's advances in quantum science could impact the future military and strategic balance, perhaps even leapfrogging*

traditional U.S. military-technological advantages. Although it is difficult to predict the trajectories and timeframes for their realization, these dual-use quantum technologies could "offset" key pillars of U.S. military power, potentially undermining critical technological advantages associated with today's information-centric ways of war, epitomized by the U.S. model. As China shifts its most sensitive military, governmental, and commercial communications to quantum networks, this transition could enhance information security, perhaps frustrating U.S. cyber espionage and signals intelligence capabilities, though these systems will likely remain susceptible to exploitation nonetheless."(Kania & Costello, 2018). China's investment in this kind of technology is so powerful it is believed to spend in R&D more than any other country.

However, some voices claim for collaboration instead of competition: *"Pan said he believed collaboration would bring only rewards in quantum science."(Whalen, 2019)* Pan thinks this academic collaboration would be positive for both parts, adding he believes no one should be concerned as a result of the advances of the other *"I see no reason whatsoever that the United States government should be concerned and discourage normal academic activities. Recall that quantum mechanics was first developed in Europe, and then moved to the United States.* (as citated in The Washington Post, 2019)*"*

Meanwhile, many others only claim for non-interference: *"... I believe the United States needs to continue to pressure China for a trade agreement that includes durable protection for our intellectual property and stiff penalties for its theft. China cannot be allowed to steal the US's quantum technology either. Nor can we afford to allow China to maintain its current quantum lead. The long-term security of the United States depends on both."*(Smith-Goodson, 2019). Here, the author clearly shows his concerns not only about the possibility China is eavesdropping US, but also about US being clearly behind China referring to quantum development.

5.5 Japan

Japan, conscious of the importance of quantum mechanics in the future of technology is aiming to catch China and US in a short period of time. Among its objectives, there are building a 100-qubit computer in ten years time and a fully developed quantum computer by 2039, some realistic goals compared to those who claim that in five years time a completely developed quantum computer will be released.

However, forgetting about decades in the future, Japan nearest plans are building five new quantum research centres in the following five years.

*"The government will seek about **30 billion yen ($276 million)** in funding for **quantum research** for the budget year beginning April 2020, roughly double the year-earlier request. The technology also will be one focus of a "moonshot" R&D program in which the government will invest a total of 100 billion yen." (Koshikawa, 2019).*

5.6 Australia

Australian Universities have been aware of the importance Quantum would have in the future. That's why they have been teaching many students focusing in quantum mechanics recent years. As a result of this is that Sydney is known by many experts as the '*Quantum Silicon Valley'.* As a result for this rush in quantum is Sydney Quantum Academy, a society formed by Macquarie University, UNSW Sydney, the University of Sydney and the University of Technology of Sydney.

In order to help the creation of this group, **the New South Wales government invested 15.4 million Australian dollars.** Despite this investment might be quite small compared to the data analysed in previous appendices, we should remind New South Wales is only an state inside Australia, I mean, the rest of the investments analysed came from private finance or whole countries, even societies of several countries as seen in EU. This is a clear evidence how important quantum research is becoming in Australia.

In addition, this **contribution together with these four universities support and industry help, would reach a total amount of 35 million Australian dollars for Sydney Quantum Academy.**

5.7 Funding for investors

In this brief section, I am going to analyse something crucial for investors, the CAGR and how do potential investors see quantum field through it.

CAGR measures the increase of investment capital. In other words, the percentage of the increase of money in respect to the money invested through the years the inversion lasts. It is a "linear" estimation, what is, does not consider great changes. It is defined as follows:

$$CAGR(\%) = ((\frac{Initial\ investment}{Final\ Investment})^{\frac{1}{Number\ of\ years}} - 1) \times 100$$

CAGR is used as an estimation to decide whether ending the investment or keeping it. The previous one is the common formulation although there are more complex ones in order to consider some other factors.

Referring to quantum investment, *"according to BCC Research's Quantum Computing: Technologies and Global Markets, its expansion into key industries will boost demand for quantum-scale solutions. The industry anticipates a compound annual growth rate (**CAGR**) of **37.3 per cent to 2022**, when it could be worth **$161m**; this date falls before the earliest estimate for mainstream penetration to begin. The report further estimates that **between 2022 and 2027**, the market will see a **CAGR approaching 53 per cent and be worth $1.3bn**. **By sector application, the financial services will see a CAGR from 2022-2027 of 62.6 per cent.**"* (Hayes, 2019)

References

3D integration technology for silicon spin qubits | QUCUBE project | H2020. (2019). Retrieved from https://cordis.europa.eu/project/rcn/220722/factsheet/en

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., . . . Martin, V. (2019). The engineering of software-defined quantum key distribution networks. *IEEE Communications Magazine, 57*(7), 20-26. doi:10.1109/MCOM.2019.1800763

Los alamos director echoes cyber concerns. (2013). Retrieved from https://www.tdworld.com/grid-opt-smart-grid/los-alamos-director-echoes-cyber-concerns

Ali, S., & Farag, W.How is quantum cryptography used for secure financial transactions?

Archivo:Logo UC3M.svg - wikipedia, la enciclopedia libre. Retrieved from https://commons.wikimedia.org/wiki/File:Logo_UC3M.svg

Australian firm assists NASA. Retrieved from https://www.upi.com/Defense-News/2012/10/09/Australian-firm-assists-NASA/73881349812319/

Batelle Memorial Institute.Quantum key distribution. Retrieved from https://www.battelle.org/case-studies/case-study-detail/quantum-key-distribution

Battelle Memorial Institute.About us. Retrieved from https://www.battelle.org/about-us

Battelle memorial institute (2019). Retrieved from https://en.wikipedia.org/w/index.php?title=Battelle_Memorial_Institute&oldid=915523180

Baumhof, A. (2019). Quantum computers: Why google, NASA and others are putting their chips on these dream machines. Retrieved from https://www.weforum.org/agenda/2019/10/quantum-computers-next-frontier-classical-google-ibm-nasa-supremacy/

Biever, C.First quantum cryptography network unveiled. Retrieved from https://www.newscientist.com/article/dn5076-first-quantum-cryptography-network-unveiled/

Bolt, beranek y newman (2019). Retrieved from https://es.wikipedia.org/w/index.php?title=Bolt,_Beranek_y_Newman&oldid=117852861

Canberra start-up to help NASA in secure messaging. (2012). Retrieved from https://www.smh.com.au/technology/canberra-startup-to-help-nasa-in-secure-messaging-20121008-2780e.html

Castelvecchi, D. (2018). Europe shows first cards in €1-billion quantum bet. *Nature, 563*, 14-15. doi:10.1038/d41586-018-07216-0

Clavis3 QKD platform. (). Retrieved from https://www.idquantique.com/quantum-safe-security/products/clavis3-qkd-platform-rd/

Criptografía cuántica (2019). Retrieved from https://es.wikipedia.org/w/index.php?title=Criptograf%C3%ADa_cu%C3%A1ntica&oldid=117344387

Crosman, P. (2018). Why banks like barclays are testing quantum computing. Retrieved from https://www.americanbanker.com/news/why-banks-like-barclays-are-testing-quantum-computing

Development of a global network for secure communication based on quantum cryptography | SECOQC project | FP6. Retrieved from https://cordis.europa.eu/project/rcn/71407/factsheet/en

Elliott, C. (2002). Building the quantum network. *New Journal of Physics, 4*, 46. doi:10.1088/1367-2630/4/1/346

Figure 1. map of the SwissQuantum network. two nodes are in geneva city. Retrieved from https://www.researchgate.net/figure/Map-of-the-SwissQuantum-network-Two-nodes-are-in-Geneva-city_fig1_221901486

Gibney, E. (2019). Quantum gold rush: The private funding pouring into quantum start-ups. *Nature, 574*, 22-24. doi:10.1038/d41586-019-02935-4

H/Creada:16-06-2018, CCS/T21 | La RazónÚltima actualización:25-10-2019 | 20:52. (2018). España, pionera mundial en criptografía cuántica. Retrieved from https://www.larazon.es/tecnologia/espana-pionera-mundial-en-criptografia-cuantica-AP18714271/

Hayes, J. (2019). Quantum on the money: Fintech is banking on the future of computing. Retrieved from https://eandt.theiet.org/content/articles/2019/04/quantum-on-the-money-fintech-is-banking-on-the-future-of-computing/

Hwang, W. (2003). Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters, 91*(5), 057901. doi:10.1103/PhysRevLett.91.057901

Iain Thomson. (2013). 'Quantum network? we've had one for years,' says los alamos. Retrieved from https://www.theregister.co.uk/2013/05/07/quantum_cryptography_network_los_alamos/

ID quantique (2019). Retrieved from https://en.wikipedia.org/w/index.php?title=ID_Quantique&oldid=919204052

IDQ celebrates 10-year anniversary of the world's first real-life quantum cryptography installation. (2017a, -11-23T15:33:01+00:00). Retrieved from https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/

IDQ celebrates 10-year anniversary of the world's first real-life quantum cryptography installation. (2017b, -11-23T15:33:01+00:00). Retrieved from https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/

Juskalian, R. (2014). Para la industria de datos suiza las filtraciones de la NSA valen su peso en oro. Retrieved from https://www.technologyreview.es/s/4120/para-la-industria-de-datos-suiza-las-filtraciones-de-la-nsa-valen-su-peso-en-oro

Kanamori, Y., Yoo, S., & Sheldon, F. T. (Jan 1, 2006). Bank transfer over quantum channel with digital checks. Paper presented at the Retrieved from https://www.osti.gov/biblio/931719

Kania, E. B., & Costello, J. (2018). Quantum hegemony? Retrieved from https://www.cnas.org/publications/reports/quantum-hegemony

Katwala, A. (2019, -10-25). The real quantum supremacy race is between china and the US. *Wired UK,* Retrieved from https://www.wired.co.uk/article/quantum-supremacy-google-china-us

Kirk, J.Google tests post-quantum crypto. Retrieved from https://www.bankinfosecurity.com/google-tests-post-quantum-crypto-a-9253

Knight, P., & Walmsley, I. (2019). UK national quantum technology programme. *Quantum Science and Technology, 4*(4), 040502. doi:10.1088/2058-9565/ab4346

Knight, W. (2004). Entangled photons secure money transfer. Retrieved from https://www.newscientist.com/article/dn4914-entangled-photons-secure-money-transfer/

Koshikawa, N. (2019). Japan plots 20-year race to quantum computers, chasing US and china. Retrieved from https://asia.nikkei.com/Business/Technology/Japan-plots-20-year-race-to-quantum-computers-chasing-US-and-China

Laboratorio nacional de los álamos (2019). Retrieved from https://es.wikipedia.org/w/index.php?title=Laboratorio_Nacional_de_Los_%C3%81lamos&oldid=117255409

Lantz, M., & Hill, M. (2019). World's first quantum computing safe tape drive. Retrieved from https://www.ibm.com/blogs/research/2019/08/crystals/

Liao, S., Cai, W., Handsteiner, J., Liu, B., Yin, J., Zhang, L., . . . Pan, J. (2018). Satellite-relayed intercontinental quantum network. *Physical Review Letters, 120*(3), 030501. doi:10.1103/PhysRevLett.120.030501

MARKS, P. (2007). Quantum cryptography to protect swiss election. Retrieved from https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/

Morrow, A., Hayford, D., & Legre, M. (Nov 2012). Battelle QKD test bed. Paper presented at the 162-166. doi:10.1109/THS.2012.6459843 Retrieved from https://ieeexplore.ieee.org/document/6459843

Open european quantum key distribution testbed | OPENQKD project | H2020. (2019). Retrieved from https://cordis.europa.eu/project/rcn/224682/factsheet/en

Pajic, P. (2013). Quantum cryptography.

Peev, M., Poppe, A., Maurhart, O., Lorunser, T., Langer, T., & Pacher, C. (Sep 2009). The SECOQC quantum key distribution network in vienna. Paper presented at the 1-4. Retrieved from https://ieeexplore.ieee.org/document/5287038

Quantum cryptography explained: Applications, disadvantages, & how it works. (2018). Retrieved from https://www.plixer.com/blog/quantum-cryptography-explained/

Quantum cryptography put to work for electric grid security. Retrieved from https://phys.org/news/2013-02-quantum-cryptography-electric-grid.html

Quantum key distribution. Retrieved from https://www.battelle.org/case-studies/case-study-detail/quantum-key-distribution

Quantum technology makes secure internet banking future-proof ABNAMRO, qutech and TNO space in collaboration. Retrieved from /en/about-tno/news/2019/6/quantum-technology-makes-secure-internet-banking-future-proof-abnamro-qutech-and-tno-space-in-collaboration/

Sasaki, M., Fujiwra, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., . . . Zeilinger, A. (May 2011). Tokyo QKD network and the evolution to secure photonic network. Paper presented at the 1-3. doi:10.1364/CLEO_AT.2011.JTuC1 Retrieved from https://ieeexplore.ieee.org/document/5950989

Secure communication based on quantum cryptography (2019). Retrieved from https://en.wikipedia.org/w/index.php?title=Secure_Communication_based_on_Quantum_Cryptography&oldid=880258501

Singh, H., Gupta, D. L., & Singh, A. K.Quantum key distribution protocols: A review.

Smith-Goodson, P. (2019). Quantum USA vs. quantum china: The world's most important technology race. Retrieved from https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/

Strom, M. (2019). Universities welcome NSW government backing for sydney quantum academy. Retrieved from https://sydney.edu.au/news-opinion/news/2019/03/09/universities-welcome-nsw-government-backing-for-sydney-quantum-a.html

Stucki, D., Legré, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., . . . Zbinden, H. (2011). Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics, 13*(12), 123001. doi:10.1088/1367-2630/13/12/123001

Thoss, A. (2018). €650 million for quantum research in germany. Retrieved from https://www.laserfocusworld.com/lasers-sources/article/16571451/650-million-for-quantum-research-in-germany

US Department of Energy. (2019). Department of energy announces $60.7 million to advance quantum computing and networking. Retrieved from https://www.energy.gov/articles/department-energy-announces-607-million-advance-quantum-computing-and-networking

Valivarthi, R., Umesh, P., John, C., Owen, K. A., Verma, V. B., Nam, S. W., . . . Tittel, W. (2019). Measurement-device-independent quantum key distribution coexisting with classical communication. *Quantum Science and Technology, 4*(4), 45002. doi:10.1088/2058-9565/ab2e62

Whalen, J. (2019). The quantum revolution is coming, and chinese scientists are at the forefront. Retrieved from https://www.washingtonpost.com/business/2019/08/18/quantum-revolution-is-coming-chinese-scientists-are-forefront/

Xue, P., & Zhang, X. (2017). A simple quantum voting scheme with multi-qubit entanglement. *Scientific Reports, 7*(1), 7586-4. doi:10.1038/s41598-017-07976-1

Image references

Mitsubishi electric (2010). Inaguration of the Tokyo QKD Network [Figure]. Retrieved from https://www.mitsubishielectric.com/news/2010/1014-b.html

Stucki D, Legre M. and Buntschu F. (2012). Long term performance of the SwissQuantum quantum key distribution network in a field environment [Figure]. Retrieved from https://www.researchgate.net/figure/Map-of-the-SwissQuantum-network-Two-nodes-are-in-Geneva-city_fig1_221901486

Hughes, R., Nordholt, J., Mccabe, K., Newell, R. (2013). Network-Centric Quantum Communications with Application to Critical Intrastructure Protection [figure]. Retrieved from https://www.researchgate.net/figure/Generation-1-quantum-smartcard-or-QKarD-See-text-for-details_fig2_236597234

Lantz, M., Hill, M. (2019) World's First Quantum Computing Safe Tape Drive [figure]. Retrieved from https://www.ibm.com/blogs/research/2019/08/crystals/

Phys.org (2018) Real-world intercontinental quantum communications enabled by the Micius satellite [figure]. Retrieved from https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html

Gibney, E. (2019). Quantum gold rush: the private funding pouring into quantum start-ups [figure]. Retrieved from https://www.nature.com/articles/d41586-019-02935-4

Smith-Goodson, P (2019). Quantum USA Vs. Quantum China: The World's Most Important Technology Race [figure]. Retrieved from https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/#588f78b72de9

Roche. Calculating the unimaginable [figure]. Retrieved from: https://www.roche.com/quantum-computing.htm