An ontology for quantum networks

By Pablo Casal
netlabs CEO

In this article we will discuss Quantum Networks, the types that exist, their applications and what can be expected in the future. Later on, in a following post, we will delve into what is beginning to be known as Quantum Internet and why it may be a viable option for scaling the processing capacity of Quantum Gate Computers.

It is our purpose to make this post understandable to different types of audiences. Therefore, we will first present the ideas in a very conceptual way, ignoring all the technicalities considered from an engineering perspective. Afterwards, and for those who wish to go deeper, we will explain the implementation details, which are generally as challenging and as captivating.

Quantum Networks are applied today in two ways mainly:

- For **Quantum Communication**, which consists of sending qubits between two quantum processors separated by at least a moderate distance.
- For **Computational Quantum Networking**, based on distributing the processing among different quantum processors, which is similar, in principle, to classical distributed computing (we will later discuss how they differ).

Computational Quantum Networking is particularly interesting since it provides an attractive and orthogonal alternative to the inevitable scaling of the quantum processor. The main goal in quantum computing research is to achieve more stable qubits than in a traditional computer (approximately 60). One way to achieve this is to have a quantum processor simulate them.
While great advances have been made in this regard, physical qubits are already reaching three digits, and IBM has recently promised to create a 1000-qubit quantum computer (QC) by 2023. The road ahead is still quite long.

There is no simple way of determining how many qubits a QC should have in order to simulate 60 stable qubits, but according to current consensus, which is mostly based on educated guesses, a processor of some 50k to 100k qubits might be able to do the job.

> Today, QCs are measured in tens of qubits, there are still great challenges in terms of error handling, decoherence prevention, control system management, etc.

As such, it seems to me that IBM is not close of achieving its goal, if ever it will be achieved..

QUANTUM INTERNET

Another way to increase the number of stable qubits would be to connect several quantum processors together through a **Quantum Internet**. (link to paid paper reference)

Let's imagine we have 2 QC of 20 qubits each. If we partition the space of a problem in two, and we give each QC one half of the problem, then we would have a processing capacity of about 2*2^20 qubits, a performance similar to classical distributed processing.
However, if we managed to connect the QCs through quantum networking, the processing capacity of the cluster would be equivalent to that of a 2*38-qubit virtual processor, which is an exponential growth in its processing capacity. In the second part of this post, I will go deeper into this concept and some implementation details to build this *Quantum Internet*.

Within Quantum Communication Networks, the most common ones so far are those being used for quantum **encryption** algorithms such as **Quantum Key Distribution** (QKD) or **Superdense Coding** .

The first one is based on using the principles of quantum mechanics, either measurement or interlacing, to create a shared encryption key and then transmit classical bits between the two systems.
In the second case, it is a communication protocol that allows both systems to improve the transmission of classical information through a quantum channel.
In other words, two bits of classical information are exchanged as a result of the exchange of a single qubit. Neither of these two systems is actually used to transmit qubits to process quantum algorithms; rather, qubits and quantum processors are instead used to transmit classical information.

For a long time, discussing about quantum networks was tantamount to discussing about QKD and Superdense Coding, and that is because they have relatively simple requirements: they only need one qubit quantum processors. Nonetheless, these two algorithms are sufficient to enrich classical communications with some very attractive properties of quantum communications. In particular, they are able to make communications more secure and impossible to intercept, at least with our current knowledge of quantum physics.

To this day, QKD remains probably the most popular application of quantum networking and likely the most widely used ***quantum encryption*** system (not to be confused with *post-quantum encryption* (link to last article)). For this reason, and without any doubt, it deserves some attention as well as an explanation of why it is used and how it works.

AUTHENTICATION / MESSAGE SECURITY

Our current traditional systems of secure communication are designed to solve two problems: **authentication**, that is, confirming that who we connect with is who they say they are; and **message security**, which refers to encrypting the message, so it isn't understandable it in case it is intercepted.

For instance, in our everyday life, we all come across authentication mechanisms when we go to a bank or a state agency and are asked for identity documents to verify that we are who we say we are. From our own perspective, there is, in fact, an implicit verification, since the person we interact with sits at a counter of the institution we visit. As such, both parties are effectively authenticated.

As per message security, imagine you are at a party and you want to say something to someone, but you know many people might hear you. You don't want anyone else to understand the message, so you say something along the lines of *"tell you-know-who that I've been giving it a thought and I'm fine with it."* Even if someone eavesdrops what you say, nothing can be grasped from it since they would be lacking the necessary context to 'decrypt' the message.

Or IT security systems don't work exactly as the examples above, but they basically provide us with the same guarantees in a conceptual level. Authentication and message encryption are solved with a **public key encryption**, based on the computational complexity of certain mathematical functions. These are functions for which there is no mathematical proof to demonstrate the complexity of reversing them; no one would know how to do it either, so they are presumed to be safe.

QKD, on the other hand, does not base its security on the computational complexity of a mathematical problem, but on a very special property that is inherent to it: the ability of any of the two communicating parties to detect the presence of a third party trying to read the shared key. This is possible thanks to a fundamental property of quantum mechanics: when a quantum system is measured, the measurement process itself modifies it. Thus, any third party trying to spy on the communication will have to measure it, and in this way will be introducing detectable anomalies.

Therefore, by making use of **quantum superposition** or **quantum entanglement** and then transmitting information about the quantum states used, a communication system can be implemented that is capable of detecting any third party attempting to spy. Generally speaking, it is convenient that, if the spying attempt is below a certain threshold, the communication be considered as good or, in the opposite case, it should be restarted until this need is satisfied.

So far it seems that there's nothing but advantages for QKD and quantum encryption. But there is a general big disadvantage: authentication.

None of these mechanisms provide a quantum native authentication system. This is why, for authentication, either you end up trusting the physical medium used (today this is still a reasonable premise since it is not easy to pose as the quantum processor with which you wanted to make the connection) or you use classical authentication systems, generally based on digital certificates.

As it is, QKD ends up solving quantumly only a part of the problem. There is some controversy among the cryptography community about the usefulness of quantum encryption, since this limitation in its capacity to authenticate quantumly makes it incomplete solution. Some think that it is nothing more than a very sophisticated stream cipher and much more expensive than the classical ones available on the market.

Today there are at least four companies that provide commercial QKD solutions: ID Quantique (link), MagiQ Technologies (link), QuintessenceLabs (link), SeQureNet (link) and most of the big brands have a research program working on the subject. On the other hand, there has been at least 5 networks built around this technology:

- DARPA (DARPA Quantum Network), which had 10 nodes.
- SECOQC (Secure Communication based on QC), which interconnected 6 locations over 200km of fiber.
- SwissQuantum (SwissQuantum network project).
- QUESS, which interconnects China with Austria via satellite over a land distance of 7500km and supports video calls. Apart from this, the network has a 2000km stretch of fiber between Beijing, Jinan, Hefei and Shanghai.
- Tokyo QKD.

Perhaps the most dramatic demonstration of QKD so far is that of the renowned Chinese physicist Pan Jianwei (link), who is leading the quantum revolution in his country. Together with his team, Jianwei managed to measure quantum entangled photons over a distance of 1204 km between two land bases. The experiment involved the use of a satellite to triangulate the transmission of the photon, which represented a transmission over a total of 2400 km. Later that year, this infrastructure was used to implement BB84 (link) between Austria and China, a structure capable of transmitting video and images.

DESIGN & WEAKNESSES

Continuing with the above, it is time to present the design details and, later on, the weaknesses of what was the first QKD protocol. Published by Charles Bennett (link) and Gilles Brassard (link) in 1984, it is now known as BB84 (link). Although it is a generic mechanism of Quantum Key Distribution (QKD), it is generally presented as a method for securely communicating a key between two duly authenticated parties, and then exchanging information using classical one-time pad encryption.

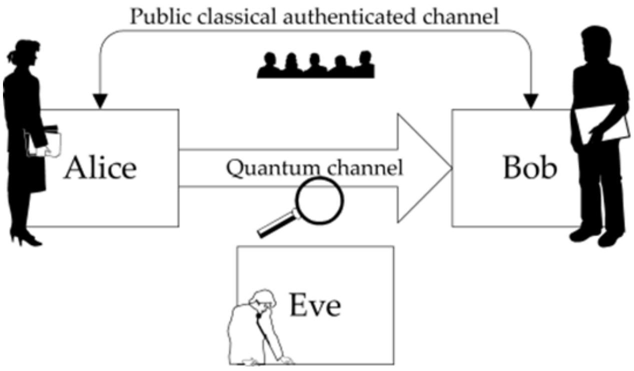
BB84, Description

To describe BB84, we will use 3 fundamental ideas of quantum physics:

1- Any measurement of an unknown system modifies the system itself

2- No cloning. Quantum properties cannot be cloned

3- When the measuring device is aligned at the same angle as the transmission device, then the system is not modified by the measurement



QUANTUM CRYPTOGRAPHY

Let's examine a classic scenario: Alice wants to communicate a message to Bob.

The first thing Alice does is generate a random sequence of bits. Alice can do this because she has a quantum processor capable of generating random information. Alice's final objective will be to send this random sequence of bits to Bob in order to use, later, a part of that sequence (approximately 50%) in a one-time pad (link), which guarantees a communication that is supposed to be 100% safe, at least based on our current understanding.

Alice and Bob are connected by two links. The first channel is traditional, easy to visualize and spy, and the second one is a quantum channel.

Alice will transmit this random sequence of bits encoding it in polarized photons. She will transmit bit 1 with a vertical polarization, represented in this text by the symbol | and bit 0 with a horizontal polarization, represented in this text by the symbol

Now, what would happen if Eve intercepts the photons to spy on the message? She could measure the polarization of the photon with a polarized filter, for example, with a vertical polarization filter. Every time a photon goes through the filter, she would know that she received a 1 and every time the photon does not go through the filter, she would know that she received a 0. So, she would write down the result of every bit and then she would generate a photon with the same polarization that she read, and she would transmit it to Bob. He would then receive Alice's message, and neither of them would suspect that Eve has intercepted it.

But why was Eve able to intercept the message? The reason is that Eve had information about how the bits were going to be encoded. Eve knew that a vertical alignment was a 1 and a horizontal alignment was a 0. However, if Eve did not know how to align the polarized filters, she would not know how to read the information.

As an example, this would be a sequence of bits that Alice could send through the quantum channel:

0 1 0 0 1 1 1 0 1 0 1 1 <— **Alice's sequence**

+ + X + X X + X + X X X <— **Random coding of photon polarization**

- | \ - / / | \ | \ / / <— **Polarization angle sent by Alice**

—> QUANTUM COMMUNICATION CHANNEL <—

X + + X X X + X X + X + <— **Bob's assumption regarding the coding used by Alice**

? 1 ? ? 1 1 1 0 ? ? 1 ? <— **Bob decodes the photons based on his assumption of how they were encoded**

Every time Alice decides to use a horizontal and vertical coding, we represent it with the + symbol. On the other hand, every time Alice decides to use a coding rotated 45 degrees, we represent it with the X symbol. We will use the same symbols to

represent the encoding that Bob assumes Alice used.
Note that since Alice used a random coding for the polarization of the photon and Bob also made a random assumption to read them, the amount of hits in the coding used by Alice has to be 50%. With which, the number of bits correctly read by Bob is going to be approximately half of those that Alice sends; Bob will have to read the other half of bits without guarantees of being correct.

The reason why Bob is not guaranteed a correct reading is because of the quantum nature of the interaction of a photon that has a polarization of 45 degrees to a polarized filter. In this case, the probability that the photon goes through the filter (and therefore that it comes out aligned with the polarization of the filter) is 50% and the probability that it does not go through is the other 50%. So, the fact that it goes through it or not does not give any information about which is the bit coded in that photon.

How does Bob know which assumptions were correct and which were not? How does he know which decoded bits are guaranteed to be correct and which are not? The answer is very simple: Alice transmits the codification used in the transmitted photons via the traditional, public channel.

In other words, Alice sends this information through the classical, public channel:

+ + x + x x + x + x x x

Keep in mind that Alice is not sending the information of the secret message, but the information of how she encoded the secret message.

Bob receives it, compares it to his assumptions, and discards all the bits resulting from his assumptions that did not match the coding used. To ensure the privacy of the communication, it is essential that Alice only transmits the encryption used after the message has been transmitted over the quantum channel.

Then Bob, using the same classical and public channel, sends Alice his assumptions about the polarization angle of the photon. With which, both parts (Alice and Bob) will know which of the bits were correctly received and which were discarded.
The bits that were correctly transmitted and received are then used as an encryption key for some secure algorithm. Finally, the message that was wanted to be transmitted ends up being transmitted with the one-time pad through the classical and public channel. Thus, quantum communication was used to negotiate a secure key.

Why should the coding information of the photon polarization angle be sent after and not before the transmission through the quantum channel? Because, if Eve had that polarization angle encoding, she could intercept the message without Alice or Bob noticing it, as explained before.

If the encoding is sent after the message through the quantum channel, it will already be too late for Eve to intercept the information. If Eve tried to intercept the quantum communication without knowing the polarization angle, the same thing would happen to her as to Bob: in some cases, she would read the bits, and in other cases the reading would not be guaranteed to be correct. Thus, when she retransmitted this communication to Bob, corruption would be generated in the data that could be detected between Alice and Bob, for example, by transmitting a hash (a digital signature) of the negotiated key between them.

If Alice and Bob detect data corruption, they would simply eliminate the exchanges and start the whole process over again. In the end, they should have no problem establishing a secret way they would use to transmit information using a one-time pad.

SUMMARY

BB84 allows Alice and Bob to exchange a shared secret key using public communication channels. Once a secret key is shared, it can be used to transmit information 100% securely. The security of the system is based on the quantum properties of photons. These properties, in turn, are based on the laws of physics, which never change, no matter how much technology advances. As a result, this protocol will always be safe.

This is very relevant, since other encryption systems based on complex mathematical problems can become vulnerable over time, as technological advances may render these mathematical problems less difficult to solve.

POTENTIAL VULNERABILITIES

Intercepting and forwarding

This vulnerability was analyzed above, when we described BB84. If Eve had access to the codification in the photon polarization, she could intercept each photon and transmit it again. That is why it is fundamental that the codification of the polarization is random. It should ideally be generated with a quantum processor to guarantee this hypothesis.

Man-in-the-middle

As previously discussed in this article, there is no QKD that provides a quantum authentication mechanism, and BB84 is no exception. The reason is that no phenomenon has been found in quantum physics that can be used to authenticate an agent. Therefore, this type of process is sensitive to man-in-the-middle attacks. PKI authentication must be used to prevent them.

Denial of service

Since physical transports for quantum channels are so sensitive (fiber or line of sight), it is very easy to cut or block them and thus interrupt the communication.

Trojan attack

If the photon transport layer is accessible and the emitting or receiving device is illuminated with a strong light, the polarization of the devices in the light reflection could be observed. In this way, in the previous case, Eve would have access to the coding used by Bob and Alice.

In general, BB84 has been shown to be immune to any security attack admitted by quantum physics, but the conditions under which the protocol is implemented are not always ideal. The following conditions must be met to ensure the security of the protocol:

- Eve should not have physical access to Alice or Bob's communication devices
- The random number generator for the secret key and polarization coding must be genuinely random. For example, a quantum processor
- The classical communication channel should be properly authenticated, for instance, with PKI
- The message sent should be sent using a one-time pad