Quantum Cryptography - Cryptography Case Study #3

José Donato, donato@student.dei.uc.pt, 2016225043

I. Introduction

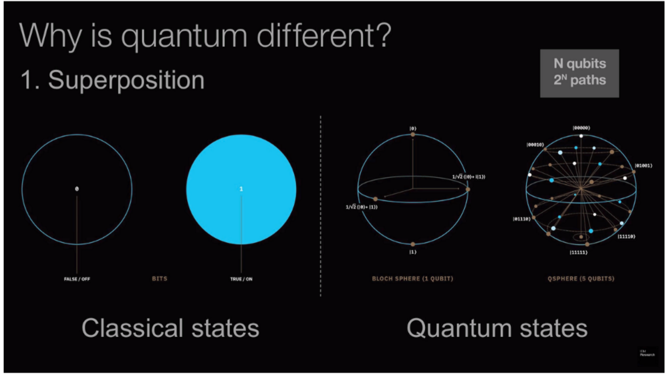
This article aims to study the basis of quantum cryptography and its future. I start by defining what quantum cryptography is and what it consists of, i.e., on what it is based. Next, I explain the threats of the rise of quantum computers bring to the current cryptography solutions considered safe nowadays. Finally, I talk about Post Quantum Cryptography, i.e., the research about the cryptosystems that are being made capable to resist against the threats of quantum computing.

II. Quantum Mechanics

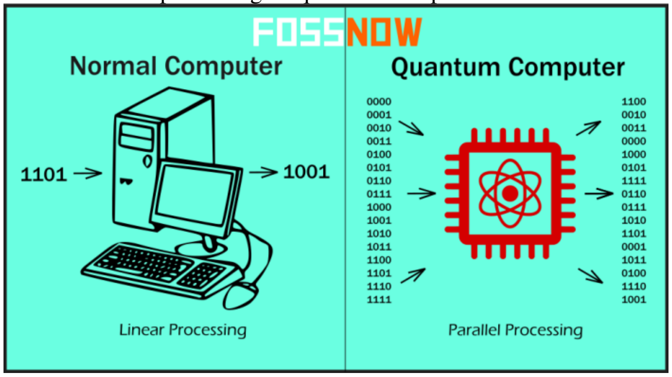
Quantum computing are based on the quantum mechanics. In general, the main performance difference between normal computers and quantum computers is the higher processing power (higher capacity to perform operations on data) of quantum computers. It started in 1980 [1] but Quantum Computing is still nowadays limited to experimental environments.

But what is the main difference between the normal and quantum computers? Current computers process the most basic unit of information: bits. Bits can have only two possible values zero and one. This means that, on a classical computer with ”n” bits, it can be at most in one of the 2^n different states.

On the other hand, quantum mechanics deal with a different unit of information: Qubits. They assume the two possible values of Bits (zero and one) plus the superposition state of both zero and one. This means that a quantum computer with ”n” bits can be at any overlapping of at most 2^n different states simultaneously.



As you can imagine, the possibilities in being at different superpositions at the same time brings a new concept of parallelism when comes to processing in quantum computers.



This parallelism in the operations is what makes quantum computing so powerful. The main quantum algorithms presented in the next section use this concept of parallelism in processing data.

III. Main Quantum Algorithms

When it comes to quantum computing we have two main algorithms [2] related to processing data (usually used in cryptography systems):

1) **Shor Algorithm**: in 1994 [3] , Peter Shor showed that a quantum computer could break any public-key cryptosystem based on the hard number theory problems (integer prime factorization used by RSA for example and discrete logarithm used by Diffie–Hellman key exchange or elliptic curve cryptography algorithms).
2) **Grover Algorithm**: in 1996 [4] , Lov Grover developed a search quantum algorithm. It searchs a unsorted database of X elements within efficient time. It was proved that it can achieve quadratic speedup on unstructured search problems. Although its use on capable Quantum Computers doesn't make current symmetric algorithms obsolete it demands longer key sizes. This will be explored in more detail in next sections.

Both algorithms are the ones that that make physicians and cryptographers believe that in 20 years quantum computing will break any public key scheme based on the hard number theory problems [4]. When quantum computing becomes a reality, attackers will use this two algorithms to break cryptosystems that are now considered safe to use gaining the ability to decrypt any information by bruteforcing it with quantum computers.

This is the reason that makes so urgent to seek for solutions that are resistant to brute force attacks using such algorithms.

IV. Quantum Computing Threats

Despite the complexity of implement quantum computers, quantum computing is increasingly starting to become a reality. For example, Google is already achieving quantum supremacy [5], i.e., the point that a quantum computer can do something that an ordinary computer can't.

With this rise of quantum computers, much more processing power will come and algorithms that were thought to be secure will no longer stay safe (at least with the current key sizes). This algorithms will no longer be safe against brute force attacks from certain quantum computers. Their facility of doing operations like factorization will put into question RSA, Diffie-Hellman or elliptic curve cryptography algorithms [1].

If they don't become obselete, they need longer keys and in, at least, RSA case because of its already long key sizes, it will become unusable. Tests were done and cryptographers think symmetric algorithms like AES and SHA-3 will remain safe with 256-bits and 384-bits keys, respectively [4].

Nowadays, attackers are storing encrypted communications that will be decrypted in years by attackers with quantum computers [6].

It is presented below a table with the impact of this threats on some of the current cryptography solutions [2] [4]:

Impact of Quantum Computing on cryptography			
Algorithm	Type	Purpose	Impact
AES	Symmetric	Encryption	Increase key size (256 bits)
SHA-2/3	Symmetric	Hash	Increase Key size (256/384 bits)
ECC	Asymmetric	Digital Signatures, Key Exchange	No longer safe to use
DSA	Asymmetric	Digital Signatures, Key Exchange	No longer safe to use
RSAE	Asymmetric	Digital Signatures, Key Exchange	No longer safe to use

Summing up, with Quantum Computing, public-key cryptosystems will break and some symmetric algorithms will remain safe if the key size is increased. Therefore, solutions must be found and that is what next section is about.

V. Post Quantum Cryptography

With the emerging of the threats exposed in last section we need to have solutions. That is where Post Quantum Cryptography enters. Post Quantum Cryptography refers to the cryptography solutions that resist to attacks made by quantum computers [6]. It is becoming a very big topic of research because of the reasons already referred and, in 2016, NIST called for post-quantum proposals (5 year competition) [6].

Also, many people think that Cryptography will be the first commercial use of quantum computers [7]. In fact, there are already companies that offering quantum resistant algorithms (for example, Isara Radiate: https://www.isara.com/isara-radiate/).

For the rest of the section, some post quantum cryptography applications will be explained.

To understand why quantum computing can be beneficial to develop cryptography solutions we need to understand one rule of quantum physics [7]:

- one cannot take a measurement without disturbing the system

So, imagine two people, Alice and Bob, communicating using Quantum channels. They both can check if someone was listening to their communication by simply comparing a randomly subset of their data.

Imagine Alice sends the message to Bob, if Bob receives the subset unperturbed this means that there were no perturbation of the system.

No perturbation means that the quantum channel was not measured so it was impossible to happen eavesdropping/main-in-the-middle attacks.

Although, this solution only ”protects” afterwards. We want to protect the communication in advance. One possible solution to this is to use a quantum channel to exchange the key and use that key to further communication.

Again, if the system is not perturbed we can be sure that no one got the key exchanged. Even if someone did get the key we would know and could just discard it and use another.

Another quantum cryptography implementation is called Quantum Teleportation. It is the quantum version of One-Time Pad.

Basically, they both (Alice and Bob) have the same shared secret and instead sending the plain message, they send the message compared to this shared secret. The difference between the quantum and the classical version is that the shared secret in the classical is a simple key and in quantum version is a pair with X and Z even parity. The main advantage of this is that with quantum teleportation, because it moves qubits and the state of a qubit is defined by continuous amplitudes, with just 2 bits of communication continuous infinity of detail can be moved.

This is just some possible implementation for post quantum algorithms. Many others could be and are being implemented. In the beginning of 2019, NIST revealed that they were already analysing 26 post quantum advanced algorithms [8].

VI. Conclusion

To conclude, we can see that is urgent to get solutions. It is only a matter of time until current asymmetric cryptosystems get obsolete. Big organizations like NIST and Google are already seeking solutions and post quantum cryptography is now a hot topic of research. As a NIST guest researcher said [8] although there are no indications that a quantum computer capable to brute force current algorithms will happen soon, there are lot of people (Google and IBM, for example) spending a lot of effort and time on it. Because of this, it is important and urgent to develop algorithms resistant to this type of attacks, otherwise all modern communication (and many other applications that use current cryptography) will be at stake.

References

[1] Fernando Boavida and Mário Bernardes. INTRODUÇÃO À CRIPTOGRAFIA. https://www.fca.pt/pt/catalogo/informatica/seguranca-ciberseguranca-protecao-de-dados/introducao-a-criptografia/.

[2] Andreas Ahrens Olaf Grote and Cesar Benavente-Peces. Paradigm of Post-quantum Cryptography and Crypto-agility: Strategy Approach of Quantum-safe Techniques. https://www.insticc.org/Primoris/Resources/PaperPdf.ashx?idPaper=81628.

[3] Johannes Buchmann Daniel J. Bernstein and Erik Dahmen. Post-Quantum Cryptography. https://link.springer.com/book/10.1007/978-3-540-88702-7.

[4] NIST. Report on Post-Quantum Cryptography. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[5] Scientific American. Hands-On with Google's Quantum Computer. https://www.scientificamerican.com/article/hands-on-with-googles-quantum-computer/.

[6] Tanja Lange Daniel J. Bernstein and Peter Schwabe. Post-quantum cryptography. https://hyperelliptic.org/tanja/vortraege/20170704-energy.pdf.

[7] Wolfgang Tittel Nicolas Gisin, Gregoire Ribordy and Hugo Zbinden. Quantum cryptography. https://cdn.journals.aps.org/files/RevModPhys.74.145.pdf.

[8] NIST. NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'. https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals.