Quantum Computation and Cybersecurity

Inigo Perez Gamiz, MS student in ECE, Boston University

***Abstract*—The irruption of Quantum Computing has completely changed the computational outlook. It has such great potential that it is supposed to have a huge impact in many areas of society, from technology to industry, finance... One of these areas, and probably the most sensible one, is Cybersecurity. Scientists are really worried about the possible consequences of this impact, and that is why they are trying to build a new context where Quantum Computation and Cybersecurity can live in harmony. In this paper, the influence of Quantum Computation on Cybersecurity is analized, and some possible outcomes are considered.**

***Index Terms*—Quantum Computation, Quantum Computing, Cybersecurity, Cryptography**

I. Introduction

CYBERSECURITY refers to the practice of protecting critical systems and sensitive information from digital attacks [1]. The same way there are robberies in stores everyday, there are also cyberattacks that aim to steal data. In an attempt to avoid these cybercrimes, cybersecurity comes into play. One of the most popular practices in cybersecurity is cryptography. So far, many robust encryption algorithms have been developed to preserve the integrity of data, and they are based on mathematical problems that are almost unbreakable for any classical computer.

In recent years, the situation has changed with the growth of quantum computing. According to theory, quantum computers could solve the mathematics behind classical encryption algorithms considerably faster than classical computers. This means that the algorithms would not be safe against this kind of computers. While quantum computers are still in development, an important issue raises for scientists: what to do with current cybersecurity and how will it be in the near future.

II. Basics of Quantum Computation

Before analyzing the impact of quantum computation on cybersecurity, it is important to know which are the basic concepts that characterize it.

A. Classical vs Quantum Computation

In classical computers, the information is stored in bits, being the bit (0 or 1) the minimum unit of information. In quantum computation, the corresponding unit of information is called the qubit, which is denoted by $|0\rangle$ or $|1\rangle$. So far, they apparently work the same way. The difference is that while in classical computers a system made of 1-bit can only be in either 0 or 1, in a quantum computer a 1-qubit system can be expressed as a superposition of the states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{1}$$

where a and b are complex numbers [2]. This means that the system can be in both states ($|0\rangle$ and $|1\rangle$) at the same time. If the system is measured, the result is non-deterministic: the possible results are $|0\rangle$ with probability $|a|^2$, and $|1\rangle$ with probability $|b|^2$, satisfying that

$$|a|^2 + |b|^2 = 1 \tag{2}$$

Considering now a 2-bit classical system, it can be in either 00, 01, 10 or 11, but only in one of them at the same time. The corresponding 2-qubit quantum state would be the superposition of:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + b|11\rangle \tag{3}$$

with probability $|a|^2$ of getting $|00\rangle$ after measurement, $|b|^2$ for $|01\rangle$, $|c|^2$ for $|10\rangle$ and $|d|^2$ for $|11\rangle$, and the sum of all these probabilities equal to 1.

The argument can be extrapolated to a N-bit/qubit system. For a classical computer, the state would be a string of N bits 010...10, whereas for a quantum computer, the superposition of 2^N possible states [2]:

$$|\psi\rangle = \sum_{x=0}^{2^N-1} a_x|x\rangle \tag{4}$$

where $|x\rangle$ represents each of the 2^N possible combinations of N qubits (for instance, $|010...10\rangle$) and a_x are complex coefficients called complex amplitudes. In this case, the probability of obtaining the state $|x\rangle$ after a measurement is $|a_x|^2$ and these coefficients satisfy that $\sum_x |a_x|^2 = 1$.

The concept of quantum superposition gives way to another important property known as quantum parallelism. Quantum parallelism allows quantum computers to perform multiple operations at the same time, which means they can work faster than the classical computers that can only perform one operation at a time. This is the basis of many interesting quantum algorithms [2].

Another conclusion that can be inferred from the structure of quantum systems is that a quantum computer could simulate a classical computer. As an example, the state 01 in a 2-bit classical system is a particular case of the 2-qubit quantum system (3) with $a = c = d = 0$. But, what about the inverse? Could a classical computer simulate a quantum one? The answer is yes, but inefficiently. According to the general formulation of a N-qubit quantum system (4), there are 2^N complex numbers a_x, so to represent just a N=100 qubit system (which is small), $2^{100} \approx 10^{30}$ complex numbers would be needed, something impossible for any classical computer [3].

B. Quantum Limitations

Even though quantum computing seems to have a great potential, it also suffers from certain limitations:

- Sor far, many interesting quantum algorithms have been developed, but there is a problem with hardware. The growth of quantum software and hardware is not being parallel. There are physical platforms with complete control over few qubits, but incomplete control over 50-200 qubits. Companies are trying to build different hardware solutions, from superconducting circuits (IBM, Google...), to the use of neutral atoms, photons, ions or quantum dots. The objective is to find a physical platform that could have control over approximately 20 million qubits with an error rate around 10^{-3} to be able to run some of the developed algorithms [3].
- Quantum computation is probabilistic, which means that after one operation, a quantum computer returns many solutions, but only one is the correct. This implies the need of doing proper measurements and verifying the right answer, weakening the advantage of quantum computing speed. Finding a useful algorithm for quantum computers is mostly about constructing it in such a way that the probability of measuring the desired outcome is maximized [4].
- Quantum computation is fragile. A superposition state can easily collapse to one of the states composing it, with the consequent loss of information. Moreover, not only can quantum computers have bit flip errors as classical computers, but they are also susceptible to have phase flip errors [3].

III. The influence of Quantum Computation on cybersecurity

Once a general overview of quantum computation has been given, it is time to analyze its impact on the different areas of cybersecurity.

A. Shor's Algorithm

In 1994, Peter Shor presented a quantum algorithm that seemed to efficiently factorize integer numbers and compute discrete logarithms [5]. These two problems have always been some of the hardest to solve for a classical computer. Just to give an idea, the approximate time that a classical computer requires to factorize a number n is exponential [3]

$$T \sim \exp(1.9(\ln n)^{1/3}(\ln \ln n)^{2/3} \tag{5}$$

For this reason, current public-key (also known as asymmetric) encryption algorithms rely on the difficulty to factorize numbers and compute discrete logarithms. For instance, that is the case of the well-known RSA (Rivest–Shamir–Adleman) algorithm used for secure data transmission. It was developed supposing that it is practically impossible for any classical computer to factorize the product of two prime numbers that are large enough [6].

In this context, Shor's Algorithm changes the scenario. According to Shor, the problem of factorizing a number using quantum mechanics can be solved in polynomial time [3]

$$T \sim O((\ln n)^3 \tag{6}$$

This implies that the factorization problem is not an issue for quantum computers and that all the public-key encryption methods could be broken. Another example of a typical asymmetric encryption method is the ECC (Elliptic-curve cryptography). It is known for providing the same security as the RSA but with a shorter encryption key, which makes even easier for a quantum computer to break it [6].

Regarding this situation, it is important to remark that the TLS protocol, a widely-used security protocol for communications that is characterized by its robustness, relies on public key encryption methods such as RSA and ECC. Consequently, it becomes weak against quantum computers and its utility in the future is uncertain.

B. Grover's Algorithm

Grover's algorithm [7] is another quantum algorithm with a huge impact on quantum cybersecurity. It was initially designed for searching in unsorted databases. In the classical framework, the number of steps needed to search in an unsorted database of N entries is in the order of $O(N)$, whereas the number of steps that a quantum computer would need for this problem is in the order of $O(\sqrt{N})$.

This algorithm also endangers encryption methods, particularly the symmetric ones. It presents a square root speed-up over classical brute force algorithms. For instance, if a classical computer needs 2^{128} attempts to force a 128-bit symmetric key, the quantum computer would do it in 2^{64} attempts, meaning that the security of the key is reduced to 64-bits. However, unlike for asymmetric methods, quantum computation is not considered such a great threat for symmetric encryption algorithms. Current encryption methods such as the AES (advanced encryption standard) allow up to 256-bits keys, and 80 effective bits keys are already considered to be safe, so scientists are much more worried about what can happen with asymmetric methods [6].

IV. Recent quantum advances

Quantum computing is a real threat to classical cybersecurity. That is why scientists are moving on to investigate a new quantum framework for cybersecurity. Currently, there are two main techniques: Quantum Key Distribution (QKD) and Post-quantum cryptography.

A. Quantum Key Distribution (QKD)

The Quantum Key Distribution is a security protocol that allows the safe transmission of keys by encoding the information in qubits. The objective of this technology is to find algorithms that rely on the laws of physics rather than the difficulty to perform certain calculations. A QKD protocol is composed of a quantum communication channel and a public classical channel. The latter is used to make possible the authentication between the sender and the receiver of the information, and for the key sifting phase. Meanwhile, the quantum channel is

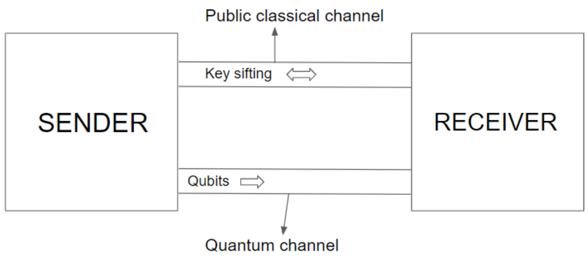

Fig. 1. Structure of the Quantum Key Distribution (QKD) protocol.

where the qubits of the key are transmitted [8]. The structure can be visualized in Figure 1.

The first Quantum Key Distribution protocol was introduced by Charles H. Bennett and Gilles Brassard in 1984 and is called BB84 [9]. It is interesting to understand how it works because it inspires the subsequent protocols that have been developed. The algorithm uses 2 different basis to encode the qubits: the rectilinear (R) and the diagonal (D) basis [10].

$$\{|0\rangle, |1\rangle\} \qquad \left\{|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\} \tag{7}$$

The communication between the sender (Alice) and the receiver (Bob) is done using the quantum channel. Alice initially builds a random string of bits and for each bit, she selects a random basis from (7). When Bob receives the code, if he chooses the right basis to measure a bit, he will get the correct bit data. On the contrary, he will read a random bit.

Once Bob has read all the bits, he sends back to Alice through the classic channel the information that indicates which basis he had used to measure each bit, and Alice will report Bob if he chose the right basis for each bit. Now it is time for both to discard the bits that Bob measured with a wrong basis. The remaining bits they have should be equal for both and form the shared key [10]. Table I shows an example about how the shared key is constructed.

Alice's bit	0	1	0	1
Alice's basis	R	R	D	D
Alice's state	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Bob's basis	R	D	R	D
Bob's measurement	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|-\rangle$
Shared secret key	0			1

TABLE I
EXAMPLE OF HOW QKD WORKS.

BB84 belongs to the so called protocols based on Heisenberg's uncertainty principle. Apart from it, some other more sophisticated protocols have been developed, such as B92, SARG04 or KMB09, which are mainly based on BB84 principles. There is also another kind of QKD protocols that take advantage of the entanglement property of quantum mechanics, as it is the case of E91 or BBM92 [8].

The quantum and classical channels are just a small part of the whole QKD technology. These protocols become interesting when they are integrated within more complex architectures that provide shared keys in different situations. These architectures are known as Quantum Key Distribution Networks (QKDN), and are composed of nodes and quantum key distribution protocols that link them. There are currently around 10 standards for QKDN architectures and four standards for QKDN security. However, these networks are still also vulnerable to potential attacks, and that is why an extensive research on the topic is being conducted [8].

B. Post-quantum cryptography

Post-quantum cybersecurity refers to the part of cybersecurity devoted to develop and implement public-key cryptographic methods and security protocols that are safe against quantum computers. In other words, algorithms for which quantum computers do not show a relevant speed-up with respect to classical ones. There are four main types of Post-quantum cryptoghraphic algorithms [8]:

- Code-based, which rely on the difficulty of code theory problems like Syndrome Decoding and Goppa Bounded Decoding.
- Lattice-based, which are based on lattice theory problems like the Shortest Vector problem (SVP) and Learning with error (LWE).
- Multivariate, which rely on multivariate polynomials and the hardness to solve linear problems.
- Hash-based, which are based on cryptographic hash functions.

  So far, there are many interesting projects and libraries that encourage the development of Post-quantum algorithms, as it is the case of Codecrypt, Java Lattice-based Cryptography Library or Microsoft's Lattice Cryptography Library. Nevertheless, most of post-quantum algorithms tend to require larger encryption keys than classical algorithms and more running time to execute, which makes them not such an attractive option [8].

V. A LOOK AT THE FUTURE

Now that a general overview about the situation of quantum computation and cybersecurity has been given, it is time to analyze some possible outcomes. It is evident that the irruption of quantum computing has completely changed the cybersecurity framework. Some of the currently most used public-key encryption methods (RSA, ECC...) , and security protocols that rely on them (TLS), are no longer safe against quantum attacks. This is a real problem since most of the internet is built based on these technologies. For this reason, it is necessary to put a great effort into the research of possible solutions to this situation. But, exactly in which direction? Should scientists try to expand Quantum Key Distribution Networks or would it be better to focus on developing new Post-quantum cryptographic algorithms? As I see it, they are not incompatible, so both are good options. However, there are some points that should be taking into consideration before inferring any conclusion.

A first important question is which role are quantum computers going to play in the future. Are they going to be used at a user level or only by companies and institutions? The hardware that is being developed is too complex to be produced at a massive scale and to be kept in ”regular” houses, so for now it seems that in the near future the users of quantum computers will be companies and institutions. In this case, the expansion of Quantum Key Distribution technologies could be a great option for them. They rely on the laws of quantum mechanics so they are more likely to be efficient with quantum computers. However, even though most people may not have a quantum computer, they could be affected by the presence of others. If there are both classical and quantum computers working, there should be a cybersecurity that is efficient for both of them at the same time. That is, it should be able to prevent attacks from quantum computers to classical ones and vice-versa, as well attacks between computers of the same type. In this context, Post-quantum cryptography plays an important role, since it aims to develop conventional algorithms that are safe against quantum computers. Classical computers need Post-quantum cryptography to be able to work without threats.

Another relevant aspect is how fast the development of quantum computers is going to be. So far, there are only reliable quantum computers for less than 50 qubits, a number far away from the desired 20 million qubits. If the development of quantum hardware continues at a slow pace, Post-quantum cryptographic products will have a bigger market in the near future since they are necessary as long as there are classical computers remaining. Nevertheless, if a total transition from classical to quantum computers finally happens, the potential of QKD is greater and Post-quantum cryptography will probably become obsolete.

In light of the above mentioned reasons, I believe that both QKD and Post-quantum cryptography should be developed simultaneously. Even though QKD probably has a greater potential, regarding the slow transition from classical to quantum computers, Post-quantum cryptography should be the priority. First of all, I would suggest to focus on developing a safe framework for classical computers against quantum ones, that is, enhancing Post-quantum cryptography. Then, I would gradually move on to create successful QKD networks if quantum computers finally replace the classical ones. At the same time, it would be helpful to investigate some other potential new quantum technologies that could improve the mentioned ones.

VI. ChatGPT

A. Answer

The influence of quantum computing in cybersecurity is profound and has the potential to reshape the entire cybersecurity landscape. Here are some key aspects of how quantum computing affects cybersecurity and the future steps that organizations and researchers are taking to address these challenges:

1) Threats to Classical Cryptography:
   Quantum computers have the potential to break widely used classical cryptographic algorithms, such as RSA and ECC, by efficiently solving mathematical problems like integer factorization and discrete logarithms. Future quantum computers could compromise the confidentiality and integrity of data encrypted with classical encryption methods.
2) The Need for Post-Quantum Cryptography:
   To mitigate the threat posed by quantum computing, researchers are actively developing and standardizing post-quantum cryptographic algorithms. These algorithms are designed to be secure against quantum attacks. Organizations need to plan for the transition from classical to post-quantum cryptography to ensure the long-term security of their data and communication.
3) Quantum Key Distribution (QKD):
   Quantum Key Distribution technology, which leverages the principles of quantum mechanics to provide secure key exchange, is gaining importance as a means of securing communication against quantum threats. Future steps include expanding the deployment of QKD in critical applications and improving its practicality and range.
4) Quantum-Safe Practices:
   Organizations should adopt quantum-safe cybersecurity practices that include:
   - Assessing their current cryptographic infrastructure to identify vulnerabilities.
   - Preparing for the eventual arrival of quantum computers by implementing quantum-resistant algorithms.
   - Ensuring the security of hardware and software supply chains.
5) Security Awareness and Education:
   Raising awareness and educating cybersecurity professionals, developers, and decision-makers about the implications of quantum computing and the importance of quantum-resistant security is crucial.
6) Standardization and Collaboration:
   Standardization organizations like NIST play a significant role in the development and adoption of quantum-resistant cryptographic standards. Collaboration between industry, academia, and government is essential in this effort.
7) Quantum-Safe Infrastructure:
   Future steps involve the integration of quantum-safe cryptographic algorithms and protocols into network infrastructure, secure messaging systems, and secure communication protocols.
8) Quantum-Enhanced Threats:
   As quantum computing advances, new types of cyber threats may emerge, leveraging the computational power of quantum computers. Ongoing research is required to understand and counter these threats.
9) Quantum Computing Research:
   - Quantum computing research should continue to explore quantum-safe cryptographic algorithms and technologies.
   - Researchers should also investigate quantum-resistant solutions for other aspects of cybersecurity, such as authentication and secure hash functions.

In conclusion, the influence of quantum computing on cybersecurity necessitates proactive measures to ensure the security of data and communication in a quantum-enabled world. Organizations should prepare for the quantum era by adopting quantum-resistant security measures and staying informed about developments in quantum technology and cryptography. Collaboration among stakeholders and ongoing research are vital components of addressing quantum-related cybersecurity challenges.

B. Analysis

Regarding ChatGPT's answer to the influence of quantum computation on cybersecurity, it can be said that it is similar in certain aspects to what has been analyzed. It explains the main threats to classical cryptography and then proposes solutions like post-quantum cryptography and QKD. It also mentions another interesting aspect that is the one of awareness and education. People entering the world of quantum computation and cybersecurity should be aware of the current fragile situation and should be well-educated to avoid malicious actions.

In general, ChatGPT gives an acceptable answer to have a general overview of the topic, but its information is not deep enough to understand certain aspects. Moreover, it only provides data up to September 2021.

VII. Conclusion

Quantum computation has completely changed the situation regarding cybersecurity. The speed-up that some quantum algorithms present with respect to classical algorithms to solve certain mathematical operations puts in doubt the efficiency of conventional cybersecurity. That is the case of Grove's Algorithm, which is able to reduce to its square root the number of attempts that a classical computer needs to run a brute force algorithm. This is a great threat for symmetric encryption algorithms, but not as big as Shor's algorithm for public-key encryption methods. Shor's algorithm can factorize integer numbers and compute discrete logarithms reducing the execution time from an exponential function to a polynomial one. This means that the asymmetric encryption algorithms that relied on the difficulty that a classical computer has to perform these operations are not efficient against quantum computers.

In this context, scientists have started to look for an alternative safe framework. There are currently two main technologies that aim to develop a robust cybersecurity: Quantum Key Distribution (QKD) and Post-quantum cryptography. The first one is based on the principles of quantum mechanics, while the second one looks for algorithms that are computationally expensive even for quantum computers.

Considering the current evolution of quantum computation, it has been concluded that the best path would be to try to expand Post-quantum cryptography as much as possible, and gradually start introducing Quantum Key Distribution Networks as quantum computers replace classical ones.

References

[1] IBM, ”What is cybersecurity?”, URL: https://www.ibm.com/topics/cybersecurity

[2] John Preskill, ”Lecture Notes for Physics 219: Quantum Information and Computation”, California Institute of Technology, URL: http://theory.caltech.edu/~preskill/ph229

[3] Anushya Chandran, Lecture notes from CAS PY536, Boston University

[4] Rietsche, Roman, Dremel, Christian, Bosch, Samuel, Steinacker, Léa, Meckel, Miriam et al. 2022. ”Quantum computing.”, DOI: https://doi.org/10.1007/s12525-022-00570-y

[5] Peter W. Shor, ”Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer” (1996), URL: https://arxiv.org/pdf/quant-ph/9508027.pdf

[6] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, ”The Impact of Quantum Computing on Present Cryptography” (2018), URL: https://arxiv.org/abs/1804.00200v1

[7] Lov K. Grover, ”A fast quantum mechanical algorithm for database search” (1996), URL: https://arxiv.org/abs/quant-ph/9605043

[8] E. Lella et al., ”Cryptography in the Quantum Era,” 2022 IEEE 15th Workshop on Low Temperature Electronics (WOLTE), Matera, Italy, 2022, pp. 1-4, DOI: 10.1109/WOLTE55422.2022.9882585

[9] Charles H. Bennett, Gilles Brassard, ”Quantum cryptography: public key distribution and coin tossing” (1984), URL: https://arxiv.org/ftp/arxiv/papers/2003/2003.06557.pdf

[10] Mart Haitjema, ”A Survey of the Prominent Quantum Key Distribution Protocols”, Washington University in St. Louis, URL: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#bb84