PROJECT 5: POST-QUANTUM CRYPTOGRAPHY

UNIVERSITÉ DE NAMUR

hénallux HAUTE ÉCOLE DE NAMUR-LIÈGE-LUXEMBOURG

Bodson Fabrice

MASI 2022 - 2023

Table des matières

Introduction

As public key cryptographic systems will be vulnerable against quantum computers, post-quantum crypto needs to be implemented to prevent attackers to use quantum cryptography to deploy attacks.
As for RSA in the 70s, the NIST has organized a contest for people to create post-quantum algorithms. But as this is very new so it will need some time to prove and get stronger to become better.
Today, a big question remains : should we implement post-quantum cryptography today ?
The answer can be to not necessarily do it today, but the world needs to prepare for the transition : a company must have knowledge of every cryptographic protocol used by them.

Setting up quantum computers is easier said than done because there are many physical constraints that need to be considered as the temperature of the environment using the quantum processor, the noise around, etc.

Finally, Post-Quantum Cryptography is not only about encryption algorithms but also about the keys exchange. Quantum Key Distribution gives a lot of advantages when used.

Main Content

History and recent developments

In 1994, Peter Shor discovered new algorithms (polynomial time quantum) solving problems that are found in the public key cryptography: it could factor integers exponentially faster than a classical algorithm. This means that one day, the current cryptographic algorithms will become insecure against a quantum computer. Fortunately, we are not there yet so it means that we need to improve cryptography. This is where post-quantum cryptography intervenes.

Why quantum computers are powerful than classical ones?

A computer's power depends on the number of transistors and so on physical components. While a quantum computer's power depends on the number of qubits (bits representing the states 0 and 1 at the same time). So, there is no physical limitation to its power and to increase it. Though, it will not be well suited for most people's everyday life, and it will be used for data analysis or other processing consumption tasks.
As example of the difference between the two types of computers there is Google's Sycamore, a 53 qubits quantum computer, capable of computing a task in a few minutes that would take thousands of years for today's most powerful classical computers.

What are the main approaches for building quantum computers?

What we are trying to do is using our knowledge of classical physics to build environments to manipulate quantum physics. To do so, such environments need specific infrastructure like a powerful refrigerating system to create an environment where the temperatures reach the absolute zero (-273°C) to make the atoms behavior more quantum.

Also, these environments need to be completely isolated from the ‘world’, from parasites photons to be precise.

What are the main problems in building practical quantum computers?

It is called decoherence the fact of losing coherence due to physical vibrations, temperatures fluctuation (quantum needs very cold temperature) and electromagnetic waves that affects the quantum properties. Nowadays, it is the main concern of the big actors from this domain to create hardware capable of hosting quantum computing.

Grover’s algorithm

What are the main steps and how to implement them with quantum computers ?

It uses N elements of unstructured data where each element has one and only one qubit state. To solve the problem which the algorithm tries to answer to, one element from the N, the Oracle, is chosen if it matches a particular criterion. This oracle is then used in the algorithm to solve the problem.

Grover’s algorithm first prepares the uniform superposition, then the oracle reverses the state and then it applies an amplitude amplification operator so it can amplify the targeted state and lower the others. Then these 2 lasts steps are iterated (PI / 4) * sqrt(8) ~ 2 times.

What are the time complexity and memory complexity ?

The time complexity is sqrt(N) where a classical computer needs N/2 for the same entry and the memory complexity is log(N).

What are the impacts on the security of symmetric key cipher? How to mitigate quantum attacks based on Grover’s algorithm?

Grover’s algorithm is dangerous against some symmetric cryptographic algorithms but, according to NIST, for some of them, like AES, if the key size is big enough (192 or 256 bits), it will not break if a quantum computer uses Grover’s algorithm.
Another way to prevent against quantum attacks is to implement quantum key distribution.

Post quantum public key cryptosystems

As more and more research are done on quantum computers, it is beginning to represent a risk for actual public key encryption algorithms. Indeed, these quantum computers will be more powerful than classical computers for whom these PKE algorithms were made.
The solution to this problem, is to build post-quantum algorithms for cryptography that will be resistant to potential attacks coming from quantum computers. The Post-Quantum Cryptography needs to be secure against both quantum and classical computers but also it needs to be easy to implement into the protocols used like TLS.

Several algorithms exists and NIST has organized the same kind of competition as for RSA : people propose their solutions and the best one will be used and recommended as standard. The actual solutions that exist are :

- Lattice-based
- Multivariate polynomial
- Hash-based
- Code-based

But classical cryptographic solutions as AES can still be used if we use bigger sized keys like 256 bits. The main challenge of post-quantum cryptography is to implement it into classical systems.

Another way to resolve these problems is to use what is called Quantum Key Distribution. QKD is the process of exchanging keys during post-quantum cryptography algorithms and where an attacker cannot interfere nor intercept the ciphertext. For now, an attacker can put himself between two person and intercept the communication and try to recover the original message. With QKD, he would not be able to do it. QKD detects when someone listens to the communication and can stop it before any secure information was exchanged. QKD detects the attacker with the alteration of the quantum state. Because if someone intercepts the data, he must measure the key and so introduce an alteration. This way, an attacker will never be able to intercept traffic and so decrypt data and use it.

Interesting algorithms

Firstly, I find the QKD very interesting as it can detect if someone is listening and so the information will never be exchanged. I would recommend the solution coming from 'ID Quantique' as they originally come from the University of Geneva and have some experience since their creation.

For Post-Quantum, I would recommend CRYSTAL-Kyber as the NIST recommends it because they have small encryption keys and so they can be easily exchanged. For signatures, the FALCON for applications that need smaller signatures or the SPHINCS+ as the mathematical approach is different from FALCON.

Summary

Quantum computers are way more powerful than classical ones since there is no physical limitation to its power and to increase it. Even though, it will not be well suited for most people's everyday life, and it will be used for data analysis or other processing consumption tasks. This is due to the infrastructure that is required to use quantum processors. Indeed, it needs to be used in a very cold environment without any noise nor disturbing photons because it could cause a loss of coherence and make the system fail.

Grover’s algorithm could be dangerous for public key encryptions unless bigger sized keys are used, like 256 bits, or new algorithms based on post-quantum cryptography are developed.
In fact, these new algorithms need to be able to be used on nowadays protocols and networks but also on both classical and quantum computers. Another way to increase security against quantum computers is to implement the Quantum Key Distribution to prevent an attacker to listen to a communication by detecting its presence and stopping the communication immediately.

Finally, there are several algorithms worth to have a eye on like FALCON for signature or CRYSTAL-Kyber for encryption.

References

- « *Post-quantum cryptography* ». Wikipedia. (https://en.wikipedia.org/wiki/Post-quantum_cryptography)
- “*Post-Quantum Cryptography: State of the Art*”. Darmstadt University. By Johannes A. Buchmann, Denis Butin, Florian Göpfert, Albrecht Petzoldt. (https://core.ac.uk/download/pdf/144828958.pdf)
- “What is Post-Quantum Cryptography ?”. YouTube. Dr Graham Steel. (https://www.youtube.com/watch?v=N6mvo9ZyoPo)
- “*Quantum Computing Vs. Classical Computing In One Graphic*”. CBInsights, 02/02/21 (https://www.cbinsights.com/research/quantum-computing-classical-computing-comparison-infographic/)
- “*Why Do We Care About Quantum Computers At All?”.* TowardsDataScience. Franck Zickert. (https://towardsdatascience.com/why-do-we-care-about-quantum-computers-at-all-403dd6191c2b)
- “The problem with Quantum Computers”. Scott Pakin and Patrick Coles, 06/10/19. (https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/)
- “Difficulties in the Implementation of Quantum Computers”. Abhilash Ponnath. (https://arxiv.org/pdf/cs/0602096.pdf)
- “New Approaches To Building Quantum Computer”. D. Raghu Ram, 10/12/21. (https://www.electronicsforu.com/technology-trends/new-approaches-building-quantum-computer)
- “How to build a quantum computer”. Leentje Chavatte. (https://pulse.microsoft.com/en/videos/making-a-difference-en/education-en/fa1-how-to-build-a-quantum-computer/)
- IBM Quantum Composer Grover’s Algorithm. IBM. (https://quantum-computing.ibm.com/composer/docs/iqx/guide/grovers-algorithm)
- “Algorithme de Grover”. Wikipedia. (https://fr.wikipedia.org/wiki/Algorithme_de_Grover)
- “The impact of quantum computing on present cryptography”. Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang. (https://arxiv.org/pdf/1804.00200.pdf)
- « Report on Post-quantum cryptography ».NIST. (https://csrc.nist.gov/publications/detail/nistir/8105/final)
- « An Introduction to Post-Quantum Public Key Cryptography”. Joseph Stephen Savariraj, Sergio De Simone. (https://www.infoq.com/articles/post-quantum-cryptography-introduction/)
- “Quantum Key distribution”. Wikipedia. (https://en.wikipedia.org/wiki/Quantum_key_distribution)
- “NIST Announces First Four Quantum-Resistant Cryptographic Algorithms”. Chad Boutin. 07/05/22. (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms)