QUANTUM COMPUTER ATTACKS ON SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEMS.

მაქსიმ იავიჩი - კავკასიის უნივერსიტეტი

Maksim Iavich – Caucasus University

გიორგი წიკლაური – ევროპული სკოლა

Giorgi Tsiklauri – European School

ნუგო ამონაშვილი - ვლადიმირ კომაროვის თბილისის ფიზიკა-მათემათიკის N199 საჯარო სკოლა

Nugo Amonashvili - Vladimir Komarov Tbilisi School of Physics and Mathematics N199

რატი ტაბიძე - ქალაქ თბილისის კერძო სკოლის ბრიტანიკა

Rati Tabidze – Private School of Tbilisi

ნიკა ფანქველაშვილი - ვლადიმირ კომაროვის თბილისის ფიზიკა-მათემათიკის N199 საჯარო სკოლა

Nika Panqvelashvili - Vladimir Komarov Tbilisi School of Physics and Mathematics N199

გიორგი კვერნაძე - 61 საჯარო სკოლა

Giorgi Kvernadze – 61st Public School

ABSTRACT: This article analyzes at how Symmetric and Asymmetric cryptosystems and how they can be broken with the usage of quantum computers. The article also delves into who this is truly a problem for and what can be done to curb it. The paper covers the Integer Factorization Problem, Discrete Logarithm Problem, Grover's Algorithm, and Shor's Algorithm.

KEYWORDS: *Qubit, Symmetric Encryption, Asymmetric Encryption, Public Key, Private Key.*

აბსტრაქტი: ეს სტატია აანალიზებს, თუ როგორ მუშაობს სიმეტრიული და ასიმეტრიული კრიპტოსისტემები და როგორ შეიძლება მათი გატეხვა კვანტური კომპიუტერის გამოყენებით. გარდა ამისა, ეს სტატია განიხილავს, თუ ვისთვის წარმოადგენს ეს საფრთხეს და რა ზომებია მისაღები საშიშროების ასაცილებლად. სტატიაში განხილულია მთელი რიცხვების ფაქტორიზაციის პრობლემა, დისკრეტული ლოგარითმის პრობლემა, გროვერის ალგორითმი და შორის ალგორითმი.

საკვანძო სიტყვები: *ქიუბიტი, სიმეტრიული დაშიფვრა, ასიმეტრიული დაშიფვრა, საჯარო გასაღები, კერძო გასაღები.*

INTRODUCTION

Quantum computers are devoloping fast, however with those advantages come potential threats, but just how big are those threats? We often hear of how Quantum Computers will be able to do amazing and terrifying things such as predict the future, model the universe, and break all the encryptions we know, but how much of that is true? In this article we will examine the last claim and to what extent we need to worry about it. While the claim does have some truth to it, it is also quite hyperbolic and not completely accurate, this is because while certain encryptions are quite succeptible to Quantum Computers and must be replaced, others are much more resistant and need little to no enhancement to take on Quantum threats.

SYMMETRIC AND ASYMMETRIC ENCRYPTION

Symmetric Encryption

One key which must be kept secret is shared between users in this method and is used for both encryption and decryption. Often used as the method for bulk encryption.

$E_K(M)=C$

$D_K(C)=M$

Where M is the message, C is the encrypted message, K is the key, and E and D the encryption and decryption algorithms, respectively, E and D must be inverse functions such that $E_k(D_k(x))=x$.

Pros:

1. It is much faster than Asymmetric encryption.

2. If a large key size is used it is extremely resistant to brute force attacks.

Cons -

1. Leaks information with each usage and thus keys must be cycled.

2. Can only be used for ensuring secrecy and not authenticity.

Examples of symmetric cryptography are DES, AES, RC5, RC6. DES was the most commonly used block cipher in the world in the early days of computers. It encrypts 64-bit data using a 56-bit key. But with the advancement of technology, this method has become vulnerable to attacks. So people have tried alternatives like AES. AES is faster and more powerful than DES.

However the main disadvantage of Symmetric cryptosystems is that the keys must be exchanged in a secure manner before it can be used, and if the keys are not yet held by both parties it is impossible to deliver the keys to each other in a secure manner thus another system for delivering the keys is required. This is where Asymmetric encryption comes in.

Asymmetric Encryption

Asymmetric encryption is also known as public key cryptography. With this method, two keys are utilized which each decrypt the other's encryption. The first is a public key known by everyone and the second a private key known only to one user. This method was developed to address two key issues. How to share information securely without having to meet up in person to exchange keys, and how to verify that the information comes from the correct user.

There are two main areas of application of asymmetric cryptography:

1. Open key encryption - Only those who have a private key can decrypt text with open key encryption. That is, anyone can send secret information to the key holder. If there are N persons in the network, only N-1 key pairs are required to exchange information between them. Open keys are freely interchangeable or placed in a common database.

2. Digital Signature - Anyone can decrypt the text encrypted with a secret key, i.e. anyone can refer to a common database of public keys and make sure that this information was indeed encrypted, signed, by the sender.

Having an open key poses an additional problem, system users need to be sure that the open key really belongs to the owner and has not been altered. This is achieved by creating an open key infrastructure where one key holder (certificate issuer) confirms to others (by digital signature) that their keys are owned.

These two methods are often used together in the most common usage of Asymmetric encryption, sharing the private keys for the faster Symmetric encryption. How this works in practice is each user sends the other their public key, then the user with the Symmetric key sends the other the key encrypted twice, first with the recipient's public key, and then with their own private key, then the recipient uses their private key to decrypt it, ensuring secrecy, and then the sender's public key, ensuring the key is from the correct sender.

Asymmetric encryption commonly utilizes one of two mathematical problems: The Integer Factorization Problem, and The Discrete Logarithm Problem. The Integer Factorization problem deals with the fact that once you multiply two large prime numbers it is extremely difficult for classical computers to factor the multiple back into the two large numbers. The Discrete Logarithm Problem is that it is similarly difficult for clasical computers to find the discrete logarithm of a number in a multiplicative cyclic group.

QUANTUM COMPUTERS AND THEIR ATTACKS ON SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Difference between Quantum and Classical Computers

A classical computer performs operations using bits whose values can be 0 or 1. As for the quantum computer, it uses quantum bits, also known as qubits. Various physical objects can be used as quantum bits (i.e. individual photons, electrons ...). Let us consider the case of an electron as a quantum bit. Every electron has its own magnetic field, hence the spin. Place the electron in the magnetic field. Define two positions, spin up and spin down (similar to 1 and 0), according to the directions between the electron magnetic field and the external magnetic field. The main advantage of the quantum bit lies in the following, it can be both 1 and 0 in the at the same time. This is called quantum superposition. When determining the instantaneous value of a quantum bit, we assume a value of 0 or 1, although prior to measurement it exists in both 0 and 1 states with certain coefficients (i.e. 64% probability of spin up or 1 and 36% probability of spin down or 0).

Compare two classical and two quantum bits. With two bits we can get four different options (00, 01, 10, 11). Classic bits can take only one value from a given four variants, while two quantum bits are all four of them with certain coefficients (α-00, β-01, γ-10, δ-11). As a result, to determine the state of this two-spin system, we would need four numbers (coefficients), while two numbers are sufficient to describe a two-classical system. Which means that two quantum bits contain information equivalent to four classical bits. A quantum bit of N contains the equivalent information of a 2N classical bit.

Quantum Computer attacks on Cryptosystems

As we have already seen in some respects the power of a quantum computer is significantly greater than that of a classical computer. Consequently the risk of hacking some ciphers increases. Consider one of the most common occurrences of asymmetric cryptography, encryption using RSA. Its sustainability is based on the fact that the factoring of "large numbers" is very difficult. When we refer to large numbers we are not talking about hundreds, thousands, or millions. We are talking about a 2048-bit number, which is equivalent to a 617-digit number in decimal systems. If we find an easy way to factorize such a large number, RSA will be rendered ineffective. We can also try every possible case, but it takes a long time on a classic computer. Yet for a quantum computer it represents nothing. If we had a 4099 ideally stable quantum bit computer, it would break the RSA-2048 in 10 seconds! To be fair, it should be noted that the most powerful quantum computer has 72 quantum bits (Google Bristlecone) with an error probability of 0.6%. Nevertheless, quantum computing is evolving day by day and is becoming more and more of a threat to cryptography.

Symmetric cryptosystems are in much less danger from quantum computer attacks than their Asymmetric counterparts as the best algorithm to break them, Grover's Algorithm provides only a quadratic speedup, while this is significant common systems such as AES-128 can deal with this by doubling their key size, AES-256 is acceptably safe against quantum attacks.

Asymmetric Cryptosystems on the other hand are in much more danger, Shor's algorithm gives exponential improvement over classical methods for both the Integer Factorization, and Discrete Logarithm problems and even increasing key size by large factors has too little of an effect to keep these systems Quantum-Proof.

What can be done?

Experts estimate that quantum computers will be strong enough to break encryptions within one to two decades, thus if you have information which must remain secret for longer than ten years it is important to start encrypting data with Quantum-Proof algorithms, AES-256 is strong enough to stand against Quantum Computers, and has already stood the test of time against classical computers, and thus is a good choice in the Symmetric encryption department, but what about Asymmetric encryption? While there are no fully tested Asymmetric cryptosystems which can hold their own against Quantum Computers IBM's CRYSTALS looks promising, it uses a lattice based mathematical problem at it's core where numbers are taken from a pool and added together, while for smaller sets it may seem simple to figure out which numbers were added together for larger sets it's nearly impossible to do so in a viable amount of time by classical computers, and Quantum Computers provide no advantage for solving this problem. There are also other organisations such as NIST working on proving the efficacy of a Quantum-Proof system.

Conclusion

While Quantum Computers are a real threat against classical encryptions there are recourses to take such as increased key size for Symmetric encryption and new algorithms for Asymmetric encryption. Thus while it is a problem it is not a panic-worthy one and should be handled effectively, without dropping everything else to work solely on it as other reputable organisations such as NIST and IBM are already working on viable solutions.

REFERENCES:

1. S.Bushwick - New Encryption System Protects Data from Quantum Computers - Scientific American, 2019
2. J.Lake - What is RSA encryption and how does it work? , comparitech 2018
3. V.Timofeev/iStock, How Do Quantum Computers Work? sciencealert
4. M.Brinon J.Daubin C.Derland P.Boito A.Bostan A.Poteaux M. Safey El Din Journées Nationales de Calcul Formel (JNCF) 2014 CIRM, Luminy.3 – 7 Novembre 2014
5. K.Martin, Waiting for quantum computing: Why encryption has nothing to worry about techbeacon
6. M. Iavich, S. Gnatyuk, A. Arakelian, G. Iashvili, Y. Polishchuk, D. Prysiazhnyy, Improved Post-quantum Merkle Algorithm Based on Threads, International Conference on Computer Science, Engineering and Education Applications, Springer, Cham, 454-464