Quantum Cryptography

Abstract

Our privacy is hiding under the factors of some prime numbers.
The safest algorithm that is being used today, RSA, DH key exchange works in the fact that finding the factor of a large prime numbers need high computing power which even the modern supercomputer can take trillion years to brute force them. And if the message is encrypted with public key only private key can decrypt it and vice versa. 2048 bits of keys are used to encrypt and decrypt the messages which is up to this date could not be broken. It is completely based on mathematics and has anyone thought if someone finds simple way to factor even the large prime numbers, or if we will be able to create such large processing computers which can decode our encrypted texts within a minute. Obviously, it will create the disaster, Internet will be no longer safe and everything about us in internet, our social numbers, credit card information, medical reports, our passwords and even our secret messages will be exposed within a minute. We cannot deny the fact it can happen, because the safest algorithm before 30 years is not longer been trusted, for example DES. The greatest prime numbers that were thought impossible to factorised 20 years ago, are no longer recommended. Furthermore, we are computing to create the quantum computers and some of the companies even suggested that they have created one, that means those computers hundred times more computational power than today's supercomputer and they can break the beyond strongest algorithms within a minute. Many articles have even suggested, the algorithm that we are using today will be broken by 2028. That brings us in the same position where we were five decades ago, but definitely the risk has increased. Is it the time to worry? Is it the time to concern on something else?
Well, there has been a technology being developed in the field, named "QUANTUM CRYPTOGRAPHY", which is based on the physics rules, and is believed cannot be broken. Let's discuss how this irreversible method can secure our future.

Table of Contents

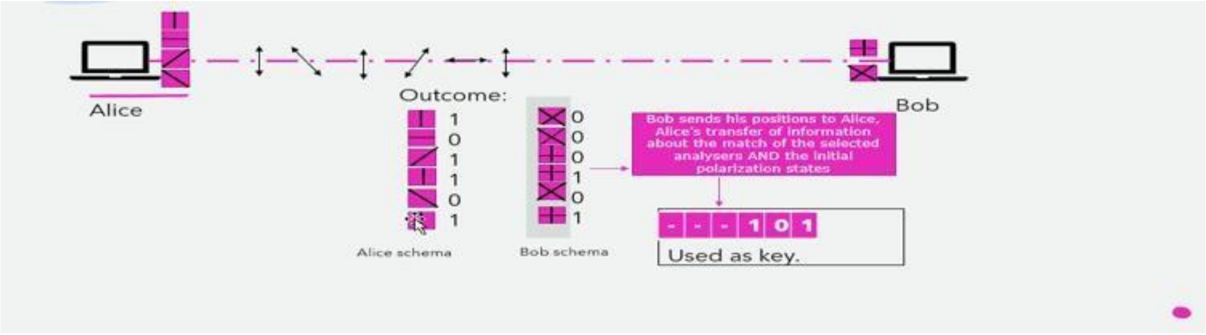
Introduction

Quantum Key Distribution (QKD), generally termed as Quantum Cryptography is the process of encrypting data generating the key using the principles of quantum mechanics proven unbreakable and irreversible. Based on Heisenberg Uncertainty principle which states, (i) the particles in the universe are uncertain and can exist in different place or different state at a time, (ii) the quantum property of a photon cannot be measured without changing or disturbing, (iii) photons are generated randomly in one of two quantum states.

Instead of using mathematics principle, quantum cryptography uses physics to generate keys. Series of photons to transmit data from one location to another over fiber optic cable and the measurement of properties of photons in two ends provide the safe key to use. The nature of production of photons state is completely unpredictable, and any measurement of the photon in between will disturb the property of the photon which secure the process from eavesdropping attack.

Technological details

Following figure shows the process of key generation using quantum mechanics, in which Alice and Bob are trying to generate the key to encrypt and decrypt the data.


Alice
Outcome:
1
0
1
1
0
1
Alice schema
0
0
0
1
0
1
Bob schema
Bob
Bob sends his positions to Alice, Alice's transfer of information about the match of the selected analysers AND the initial polarization states
- - - 1 0 1
Used as key.

Steps:

Alice computer uses photon generator, which generates completely random state of photons and are passed through different vertical, horizontal, right and left diagonal surfaces, polarizers randomly, whose values are noted 1, 0, 1,0 respectively.

The photons reach to bob computer using fiber optic cable and passed through either linear or diagonal schemes, the photons send using horizontal and vertical polarizer can pass through linear scheme and so with the diagonal polarizer can pass through diagonal scheme, but cannot in other way, bob records his results.

The scheme used by both is shared with one another using open channel (not the bits), they calculate the matching schemes and unmatching scheme are discarded, it gives the result of matching bits rest are discarded.

Probability gives at least 50% of bits match and are used as key for the encryption, taken as one-time pad for the communication.

Eve trying to Eavesdrop the communication.

Any observance or interference to the photon in the Middle, changes the state of photon, which will also produce the error in photon reaching to Bob. Eve cannot confirm her result with Alice and is left with useless data. Too many errors in the result of Bob and Alice will make them to suspect some interference going in the middle. This one-way mechanism and properties of photons will completely terminate.

Feasibility within the short or long term

The safest algorithm that is being used today, RSA, DH key exchange works in the fact that finding the factor of a large prime numbers need high computing power which even the modern supercomputer can take trillion years to brute force them. And if the message is encrypted with public key only private key can decrypt it and vice versa. 2048 bits of keys are used to encrypt and decrypt the messages which is up to this date could not be broken. It is completely based on mathematics and if someone finds simple algorithm to factor even the large prime numbers, or if we will be able to create large processing computer, no longer these algorithms are safe. We cannot deny the fact it can happen, because the safest algorithm before 30 years is no longer been trusted, for example DES. [1] greatest prime numbers that were thought impossible to factorised 20 years ago, are no longer remained unfactorized.

In [2] google claims, their quantum computer solved the complex computation in 200 seconds that a supercomputer could take 10,000 years to finish. Further [3] says, RSA today is vulnerable and is approaching the end and [4] suggests, RSA is expected to be broken in eight years by large-scale quantum computer.

Concluding the scenario, for the long-term secure encryption achievement there is the need of development of quantum cryptography. [5] reports China has successfully developed QKD system that can tolerate a channel loss beyond 833.8 km.

From this we can say, in short term it can be challenging and expensive, however in the long term it is only the alternative to secure and continue the privacy and confidentiality.

Social issues arising from the lack or presence of Quantum Cryptography

Right to privacy is the fundamental human right, and lack of cryptography will definitely breach it. The breakdown of the available encryption methods today, certainly exposes the confidentiality, and integrity. Not only this fraudulent actor can deduplicate the data and fake the source of data to commit the serious cybercrimes and will hinder for the investigation of the crimes.

The continuation of privacy of personal data, financial data, medical data of a social being, more security of the data and assurance of inevitable to leak. Implementation will help to thrive the technology socially.

Ethical issues arising from the possible use of this technology.

Quantum Computing will be beneficial to protect our ethics, and values, then creating the issues, in the way that it will protect our right of privacy. From my point of view, it will provide the feasibility to share our opinions, documents to the specific group we want to share it with. It will also help to protect our ethics in a sense that only the trusted and viable source can reach out to us, whom we trust, it provides security to everyone.

In contract of this, many negative points such as many illegal activities a group can share, channels can be created which are not happening this time because of fear of decryption of such thing at one time even it is said strongly secure. Even a government authority might be helpless performing forensic in the issue [6].

Political issues arising from the lack or presence of this technology.

It is common to collapse many political parties due to the data leakage and many government and population's data exposed which breach the confidentiality and integrity of data, some examples are, [6], [7], [8], One of the causes is lack of encryption or the weak encryption. This can be stopped if we can implement the un-hackable encryption.

Furthermore, if the available algorithms break, every political data, citizen's data will be exposed, therefore, nothing will be secret that time, unless the alternative like quantum cryptography is implemented.

Business issues arising from the lack or presence of this technology.

Buying and selling of data has been the trend of social medias. Running a small to large enterprises are working analysing the data that they legally or illegally obtain. Data leakage of the costumers is the common problem today, in addition, the data of business, leakage of business data such as business transition, policies and online meetings has collapsed many businesses and help rise of others. Every business today is dependent in network and technology, social business, online businesses, financial business (banks, e-payments) and every other business depend in internet, cloud are going to be affected positively, and negatively with arise of this technology.

Conclusion

To sum up, the change to the technology need to change in different aspect as well, which is because there is the demand to develop Quantum cryptography. In this report I have tried to explain the quantum cryptography, the technologies involved in it and the issues that can arise in the different level of society such as social, political, ethical, and business levels with the lack of this technology in brief. In addition, I have highlighted some benefits of quantum cryptography in each aspect.

References

[1] Wikipedia.org, “RSA numbers,” 07 09 2022. [Online]. Available: https://en.wikipedia.org/wiki/RSA_numbers.

[2] T. Childers, “Google's Quantum Computer Just Aced an 'Impossible' Test,” 25 10 2019. [Online]. Available: https://www.livescience.com/google-hits-quantum-supremacy.html.

[3] L. Kee, “RSA Is Dead — We Just Haven’t Accepted It Yet,” 06 05 2021. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-justhaventaccepted-ityet/?sh=7b422a795d22.

[4] M. Brown, “The Quantum Threat To Cryptography: Don't Panic, But Prepare Now,” 11 01 2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2022/01/11/thequantum-threat-to-cryptography-dont-panic-but-prepare-now/?sh=2da9a504713a.

[5] S. X. N. P. Thamarasee Jeewandara, “Twin-field quantum key distribution (QKD) across an 830km fibre,” 24 01 2022. [Online]. Available: https://phys.org/news/2022-01-twin-field-quantumkey-qkd-km.html.

[6] P. G. Jenny shearer, “Government, Cryptography, and the Right To Privacy,” [Online]. Available: https://www.cs.auckland.ac.nz/~pgut001/pubs/jucs96.pdf.

[7] Aljazeera, “Unprecedented leak exposes inner workings of UK Labour Party,” 23 09 2022. [Online]. Available: https://www.aljazeera.com/news/2022/9/23/unprecedented-leak-exposesinner-workings-of-uk-labour-party.

[8] Learn German, “German political data hacker identified,” [Online]. Available:

https://learngerman.dw.com/en/german-hacker-behind-massive-political-data-leakidentified/a-46991625.

[9] noyb, “Massive political data leak in Malta,” 24 06 2020. [Online]. Available: https://edri.org/our-work/massive-political-data-leak-in-malta/.