EasyChair Preprint

№ 4012

Quantum Computing Era in Perspective of Cyber Security

Nasrullah M Nafis

August 9, 2020

Quantum Computing era
In perspective of Cyber Security

Nasrullah M Nafis
Flinders University, South Australia

nafi0001@flinders.edu.au

Introduction

Quantum Computers shall play vital role in the future of mankind. Quantum theory was one of the major scientific innovation of 20th century. In recent years, both interest and investment in development of quantum computers are accelerated, which makes possibility of further progress of it. Countries like Australia, Canada, China, EU, Japan, Netherlands, Russia, Singapore, U.K. and U.S.A have launched quantum technologies programs investing from millions to billions. Along with, big companies like Google, Atos, IBM, Microsoft, Alibaba, Intel are also developing quantum hardware and software (Wallden, 2019). Quantum computers are devices that exploit quantum phenomena. They are capable of delivering greater computational power than classical computers. Quantum technologies already exists. For example: with very low rates of error, Google's quantum processor "Bristlecone" has a record of 72 qubits and is expected to be larger in size than what the best classical supercomputer can simulate (Physics, 2020). Extremely serious impact may happen to cyber security due to the development of the large fault tolerant quantum computers. Widely used protocols like RSA, ECDSA and DSA use problems like discrete log and factoring to ensure their hardness of security, can easily be solved by a fault tolerant, sufficiently large and universal quantum computer (Shor, 1997). (Wallden, 2019) said, "quantum cyber security is the field that studies all aspects affecting the security and privacy of communications and computations caused but the development of quantum technologies". It seems like negative impacts can be brought to cyber security by quantum computers, but positive impacts will also happen if quantum technologies are used by honest parties.

Key Words: Quantum Computer, Cryptography, Quantum Cryptography, Quantum Technology

Methodology

It is assumed that cyber security in quantum computing era will be vulnerable if it continues to follow the current factoring and discrete log method. Studies were made to define the vulnerabilities and come up with potential solutions. Data were collected from secondary sources. Searched for sources on Flinders University online library, Science Direct and Google Scholar. The content analysis method was used in the study.

Cyber Security and Quantum Computer

What is quantum computer?
Quantum computers are different than classical computers because they operate using qubits. According to (Benenti et. al., 2004; Le Bellac, 2006), classical computers use bits which can exist in a single state either 1 or 0 at a time. On the other hand, qubits stay in a vector space where they can be both 1 and 0 at a time. This is called superposition (Groom et.al., 2018). Because of this special feature of qubits or quantum bits, quantum computers are capable of solve larger number of mathematical problems than classical computers in a short period of time.

What is the method of current cryptography?
The process of converting data into unreadable text to secure it from third party intervention and safely send to the intended second party is called cryptography. Cryptography not only saves the data from intervention, it is also important for user authentication (Economic Times, 2020). According to (Grimes, 2020), two large prime numbers (A and B) are used by today's most popular cryptographic solutions, the result of which is much larger number (C). It is hard for the classic computers to factorize large prime numbers. Even if someone knew the value of a large number C, they would have hard time finding the number A and B.

Which means every encrypted data today are secured by using the method of factorizing.

How are quantum computers threat to current method of cyber security?
Cryptography is essential to many models of cyber security (Cyber Security, 2020). (Grimes, 2020) in his research, showed that encrypted data today use the method of factorizing to secure themselves. Which means if a computer powerful enough to factorize large numbers in a short time, the current method of cryptography leaves our cyber world vulnerable. On the other hand, multiple studies have found evidence that because of the special characteristic of qubits, large fault tolerant quantum computers will be able to easily factorize these big numbers in a very short time and break the encryption (Jean-Philippe, 2017; Marie, 2000; Andy et. al., 2015).

However, (Fehr, 2010) shows in his research that cryptography schemes of quantum cryptography guarantee the security solely because of the laws of nature. The paper showed how the traditional application of quantum cryptography, quantum key distribution (QKD) will secure our cyber space. QKD requires 2 parties and it transmits data among them by photons that are polarized and vibrating in four different directions, where the receiver uses polarized detectors for each photon one at a time. 1st party informs the 2nd party of the type of detectors to be used. The detectors translate the photons into bits. If an eaves dropper tries to intercept the photons with the wrong detectors, the message will be damaged (Djordjevic, 2019). There has been a successful secure quantum communication at a distance of 200 km using fibre-optic link (Tang, 2014). Though it is a potential security solution against the future quantum computing technology, QKD can be disrupted by factors like sunlight. To implement this solution, our whole internet system needs to be rebuilt.

Conclusion

Quantum computers use qubits where classical computers use bits. Qubits can be 1 and 0 at a time, this unprecedented

natural phenomenon gives quantum computers lot more power than classical computers. As a result, our current cyber security system is in threat. To mitigate the threat, scientists have come up with new solutions like quantum key distribution (QKD) which uses the same quantum mechanics as quantum computers. This method of quantum cryptography is also vulnerable to several aspects like bright light and others. To mitigate vulnerability and increase its efficiency, further research is needed.

Reference:

Andy Majot, Roman Yampolskiy.*Global catastrophic risk and security implications of quantum computers*.Futures.Volume 72. 2015. Pages 17-26. ISSN 0016-3287.https://doi.org/10.1016/j.futures.2015.02.006. [Accessed 7 April 2020]

Benenti, Giuliano, et al. Principles of Quantum Computation and Information - Basic Concepts : Basic Concepts, World Scientific Publishing Co Pte Ltd, 2004. Flinders Library, (pp 100-101)

Cyber Security and Cryptography - Computing Concepts. 2020. Cyber Security and Cryptography - Computing Concepts. [ONLINE] Available at: https://computing-concepts.cs.uri.edu/wiki/Cyber_Security_and_Cryptography. [Accessed 7 April 2020].

Djordjevic I.B. (2019) Quantum-Key Distribution (QKD) Fundamentals. In: Physical-Layer Security and Quantum Key Distribution. Springer, Cham. https://doi-org.ezproxy.flinders.edu.au/10.1007/978-3-030-27565-5_6. [Accessed 7 April 2020].

Fehr, S. Quantum Cryptography. Found Phys 40, 494–531 (2010). https://doi-org.ezproxy.flinders.edu.au/10.1007/s10701-010-9408-4. [Accessed 5 April 2020].

Grimes, Roger A. "Introduction to Quantum Computers." Cryptography Apocalypse. Hoboken, NJ, USA: John Wiley & Sons, 2019. 31-58. Flinders Library.

Groom, Charlotte, and Mark Taylor. "Quantum Computers: An Introduction." Computer and Telecommunications Law Review 24.2 (2018): 44-45. [ONLINE] Available at: https://signon.thomsonreuters.com/?productid=PLCUK&viewproductid=UKPL&lr=0&culture=en-GB&returnto=https%3a%2f%2fuk.practicallaw.thomsonreuters.com%2fCosi%2fSignOn%3fredirectTo%3d%252fDocument%252fIBF99D8D00AD611E89F7D96763E9AC9A1%252fView%252fFullText.html%253fskipAnonymous%253dtrue%2526transitionType%253dDefault%2526contextData%253d(sc.Default)%2526firstPage%253dtrue&tracetoken=04152001202707M47SXB-aeK4qdZhJ5LFr1mQTGI3OizZvVRK0NJH7FH44XuqOBOX9Gv-XSDO-iS3LCQTqYlCdCVKgF7kRnmClwrw9oVYXE0F6kQrMecSgS6YrOISE_qgLRpJpQg789K5WS5j0d2Ifb5ZlFw9pFitXOxM4yIiYBRx5GboiMmrnsrK65YjAnlHkx0kjWHste6z9SWeLxyRqvLwKZWjaDYuIVFMZf0N0nm_ibLH_k3105cVLBJgYdQ64qm-he7qqQz_Y6mDnvFzyGzyRumDvOdaWxegWxHuCRySExs4EwwUNk64UvMyXyqLtjYb1Vz3EGEhrZKM8Is5h511pTQsM758TFVA4HH-mRld8Xg8gm_4-9E&bhcp=1 [Accessed 11 April 2020].

Jean-Philippe Aumasson, The impact of quantum computing on cryptography, Computer Fraud & Security, Volume 2017, Issue 6, 2017, Pages 8-11, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(17)30051-9. [Accessed 7 April 2020].

Le Bellac, Michel. A Short Introduction to Quantum Information and Quantum Computation. Cambridge, UK ; New York: Cambridge UP, 2006. (PP - 7 - 32).

Marie A Wright,
The Impact of Quantum Computing on Cryptography,
Network Security,
Volume 2000, Issue 9,
2000,
Pages 13-15,
ISSN 1353-4858,
https://doi.org/10.1016/S1353-4858(00)09027-9. [Accessed 6 April 2020]

Physics World. 2020. Google aims for quantum supremacy – Physics World. [ONLINE] Available at: https://physicsworld.com/a/google-aims-for-quantum-supremacy/. [Accessed 5 April 2020].

Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." SIAM Journal on Computing 26.5 (1997): 1484-1509. Web.

The Economic Times. 2020. What is Cryptography? Definition of Cryptography, Cryptography Meaning - The Economic Times. [ONLINE] Available at: https://economictimes.indiatimes.com/definition/cryptography. [Accessed 10 April 2020].

Wallden, Petros, and Elham Kashefi. "Cyber Security in the Quantum Era." Communications of the ACM 62.4 (2019). (PP - 120).