MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy
NET Nexus of Emerging Technologies

NOTE FOR NATIONAL DEFENCE:
Quantum Computing Threats and How to Anticipate Them

Authors: Saman Asvadi[1] and Mohsen Farhadloo[2]

[1] Graduate student, John Molson School of Business, Concordia University, Montreal, Canada
[2] Professor, John Molson School of Business, Concordia University, Montreal, Canada

SUMMARY

- Quantum computer, is a strong computer, using quantum physics rules, to store data more efficiently, and to do computation much faster than traditional computers [4].
- Quantum computing is the use of quantum computers in solving problems that would usually take a long time, when solved by traditional computers. It is believed that such problems would be solved very fast using quantum computing [3]. Although quantum computing has not been used effectively by the time being, it is deemed a great threat to decode encryptions, which are the basic block of all cyber data transfer and transactions today [2].
- The use of quantum computing is deemed to enable solving equations which will result in breaking encryptions. Breaking encryptions endangers all transactions, sensitive data transformation and cyber security [2].
- Designing encryption algorithms that are note breakable by either traditional or quantum computers, is a trending vein of research, investing on which is essential for cyber security and protraction of sensitive data [1].
- As suggested in [1], nations must prepare for the quantum computing era. Changing infrastructures and encryption methods is not possible to be done in a short period on time. It should be planned ahead and implemented gradually.

CONTEXT

- Quantum computing threats:
    - ❑ Google recently announced that, its quantum computer was able to solve fundamental encryption equations in 200 seconds. For today’s super computers, it takes more than 100 years to solve such equations [6].
    - ❑ Quantum computing is a serious threat that should be considered in advance. Quantum computers will have the capability to solve many of the problems which are considered unsolvable today. Among such problems, there are mathematical problems serving as the core of encryption [2].
    - ❑ As mentioned in [2], quantum computers may be able to solve many of encryption codes being used today. Hence, there is a need to consider new encryption algorithms that would not be breakable, neither by existing computers, nor by emerging quantum computer.

- ❑ It is indicated that, symmetric encryption systems are more reliable than asymmetric encryption systems. Many asymmetric encryption systems being used today, are either insecure, or have a great risk of usage [2].
- ❑ National Institute of Standards and Technology (NIST) is looking these security threats in advance, and is trying to set standards to post-quantum encryption. NIST has launched a public competition, in which the competitors will propose algorithms to secure encryption in quantum era. NIST will then select the best algorithm(s) proposed in this competition, to be included in its standards and guidelines [2].
- ❑ Although quantum computing is a big threat, the good news is that, some of the cryptography algorithms being used today, can still be used as is, or need a few non-fundamental changes to be used, in the quantum era [2].

RECOMMENDATIONS

- In this section some policy guidelines are mentioned, based on recommendations by Dutch Payment Association in [2].
- It is suggested that decision makers follow all developments in quantum computing in real-time by following related conferences, journal papers and technology news.
- Governments must urge those in charge of telecommunication infrastructures to prepare for quantum era. Also, to maintain and extend current telecommunication infrastructure.
- Develop symmetric encryption systems and replace asymmetric encryption systems with symmetric alternatives. This change of encryption system will be time taking. Hence, it is important to act in this direction as soon as possible.
- Nations across the world are suggested to cooperate with one another and share their findings and roadmaps to a secure post-quantum encryption [1].

References

[1] Grody, A. D. (2020). Addressing cyber risk in financial institutions and in the financial system. *Journal of Risk Management in Financial Institutions*, *13*(2), 155-162.

[2] How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure

[3] https://en.wikipedia.org/wiki/Quantum_computing

[4] https://www.newscientist.com/question/what-is-a-quantum-computer/

[5] Chen, L., Jordan, S., Liu,Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016)'NISTIR 8105 Report on Post-Quantum Cryptography', available at: https://csrc.nist.gov/ publications/detail/nistir/8105/final (accessed 20th April, 2020).

[6] Wired (2019) 'Google's 'quantum supremacy' isn't the end of encryption', 24th September, available at: https://www.wired.com/story/ googles-quantum-supremacy-isnt-endencryption.