Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

# BN-33-Emerging technology and military application-Oct2020

INSTITUTIONAL TRANSITION TO POST QUANTUM CRYPTOGRAPHY

Authors: Attila Arslaner [1] and Julian Spencer-Churchill[2]

[1] Student in Department of Political Science, Concordia University, Montreal, Canada

[2] Associate Professor, Department of Political Science, Concordia University, Montreal, Canada

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

Security-Policy NET Nexus of Emerging Technologies

SUMMARY

As today's cryptographic standards are challenged by advances in Quantum Computing, this report aims to study the difficulties facing government institutions in how they should adapt to the forthcoming technological developments.

The Challenge Presented by Quantum Computers

The Communications Security Establishment (CSE), which is tasked with safeguarding Canada's networks, is consistently hard at work to prevent major attacks on Canada's information infrastructure. Nevertheless, a leap in the technology available to our adversaries that would propel them far ahead of our capabilities could see cyberattacks magnitudes larger in scale than any previous attack. Without the appropriate means in place to prevent this, the CSE would be helpless. Over the horizon, one such leap is the advancement of quantum computers, with countries such as China making considerable progress.[1]

Most commonly used encryption protocols, though theoretically possible to decrypt, would take a classical computer constantly working for years to decrypt the encryption of one message, making it effectively safe from outsiders. This security should not be taken for granted. More powerful quantum computers than the ones available today will be able to solve the complex task of decryption with fewer steps, solving it in days or even several hours, making them considerably faster and more efficient than a conventional computer.[2]

Quantum computers capable of decryption are still several years away, and it remains a point of speculation when they will arrive.[3] In 2015, a study at the University of Waterloo estimated a one in seven chance of the strongest among the presently used encryption standards (RSA-2048) being broken by 2026, and a one-half chance of it being broken by 2031 by quantum computers.[4] Since then, estimates for the computational power required by quantum computers to decrypt these algorithms have been reduced as more efficient means are discovered,[5] compared to previous estimates.[6] In addition, considerable progress has been made in the hardware itself,

[1] Huang Yi-Ming, Lei Hang, and Li Xiao-Yu, "A Survey on Quantum Machine Learning," *Chinese Journal of Computers*, January 2018, https://en.cnki.com.cn/Article_en/CJFDTotal-JSJX201801009.htm; Liu Xuejuan et al., "Speed up DDC Based on Quantum Computing," *Journal of Central South University(Science and Technology)*, July 2018, http://en.cnki.com.cn/Article_en/CJFDTotal-ZNGD201807014.htm; Sheng Kai Liao et al., "Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters* 120, no. 3 (January 19, 2018): 030501, https://doi.org/10.1103/PhysRevLett.120.030501.

[2] Robert S Sutor, *Dancing with Qubits* (Birmingham, UK: Packt Publishing, 2019).

[3] Sutor.

[4] Michele Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," *IEEE Security and Privacy* 16, no. 5 (September 1, 2018): 38–41, https://doi.org/10.1109/MSP.2018.3761723.

[5] Craig Gidney and Martin Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," May 23, 2019, http://arxiv.org/abs/1905.09749.

[6] Sutor, *Dancing with Qubits*.

though still falling short of the power required for decryption.[7] The true potential of quantum computers partly remains a mystery, but what remains certain is that every year new advances are made, and we are one step closer to the current cryptographic standards becoming obsolete.

Potential Solutions

With this coming obsolescence of cryptographic standards taken as a given; the literature identifies two potential solutions. The first one being what is termed "post quantum cryptography" and the second as "quantum cryptography".[8] The latter presents an entirely new technology for encrypted communication and data storage. Quantum cryptography uses the inherent quantum properties of photons to communicate over long distances and presents a means of communication more secure than any other method, though presently it remains very much under development. Conversely, looking at "post-quantum cryptography", multiple solutions are already available at present. These algorithms are similar to those currently employed, but the mathematics required to decrypt them are theorized to be more difficult than what quantum computers would be able to solve. It is this latter which forms the principal recommendation for the easiest transition of cryptographic standards in order to secure them from quantum computers. The principal challenges that lay ahead are twofold: which post quantum safe algorithm can be trusted, and how the implementation of it will take place.

For the first issue, some of these proposed algorithms go as far back as the 1970s,[9] as such they are not all entirely unfamiliar to cryptographers. Though the issue remains of what quantum computers will truly be capable of as they become more powerful, and in what ways it will compromise the encryption standards currently in use. The National Institute of Standards and Technology (NIST) in the United States is working at determining a standard common encryption that is resistant to quantum attacks, with the NIST leaving the door open to the possibility of there being multiple accepted standards for different applications.[10] Each of these new standards will have varying technical requirements, some more demanding than others, which might hinder the universal adoption of a single protocol across industries and institutions.[11] This itself has multiple difficulties surrounding it, such as hampering interoperability with other systems and creating a fragmented market.[12] As a result, flexibility of being able to implement alternate

[7] Benjamin Villalonga et al., "Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation," *Quantum Science and Technology* 5, no. 3 (May 1, 2019), https://doi.org/10.1088/2058-9565/ab7eeb.

[8] Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?"

[9] Hang Dinh, Cristopher Moore, and Alexander Russell, "The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks," August 13, 2010, http://arxiv.org/abs/1008.2390.

[10] Dustin Moody et al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process" (Gaithersburg, MD, July 2020), https://doi.org/10.6028/NIST.IR.8309.

[11] Lidong Chen, "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?," *IEEE Security and Privacy* 15, no. 4 (2017): 51–57, https://doi.org/10.1109/MSP.2017.3151339.

[12] Michael Vermeer and Evan Peet, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*, *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption* (RAND Corporation, 2020), https://doi.org/10.7249/rr3102.

protocols must be built into upcoming systems as an integral feature, encouraging adaptability to new challenges.[13] There is no easy solution to determining with certainty the most appropriate post quantum safe algorithm for a universal application across every potential use.

A subsequent issue arises from a transition in protocol, that is the difficulty of implementation. Assuming problems surrounding the choice of algorithm having been eventually resolved, how the chosen algorithms will be implemented presents multiple openings for exposure. Security vulnerabilities in otherwise secure systems with strong encryption have been exploited in the past as a result of poor implementation or a lack of quality assurance through side attacks.[14] Consequently, testing and a development of expertise is vital in the build up to implementing any new technology.[15]

Conclusions

The most prevalent conclusion of a majority of the literature and expertise on the matter is the following. A coordinated response is absolutely vital in order to mobilize the considerable amount of expertise and resources available in the country.[16] It is estimated to take several years to a decade for an institution to migrate to or adopt a new technical protocol, as such beginning the process of the migration to post quantum safe protocols now is a timely matter.[17] Conversely, the possibility of the emergence of quantum computers capable of decryption before the country is ready must also be accounted for.[18] As such protocols for all possible contingencies must be made ready in time.

Further research could also include a deeper study on whether changing to or implementing quantum safe cryptography is enough, and where the paradigm of cybersecurity will lie in the future. The role of active and passive cybersecurity is increasingly put into question, whether it is simply enough to reinforce the information infrastructure and if there are other possible approaches that could be taken.[19]

[13] Vermeer and Peet.

[14] Marco Lucamarini et al., "Implementation Security of Quantum Cryptography" (Sophia Antipolis, France, 2018), https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf.

[15] Johannes Buchmann, Kristin Lauter, and Michele Mosca, "Postquantum Cryptography-State of the Art," *IEEE Security and Privacy* 15, no. 4 (2017): 12–13, https://doi.org/10.1109/MSP.2017.3151326.

[16] Vermeer and Peet, *Secur. Commun. Quantum Comput. Age Manag. Risks to Encryption*.

[17] Sutor, *Dancing with Qubits*.

[18] Buchmann, Lauter, and Mosca, "Postquantum Cryptography-State of the Art."

[19] Bryan Reinicke, Jeffrey Cummings, and Howard Kleinberg, "The Right to Digital Self-Defense," *IEEE Security and Privacy* 15, no. 4 (2017): 68–71, https://doi.org/10.1109/MSP.2017.3151324.

References

Buchmann, Johannes, Kristin Lauter, and Michele Mosca. “Postquantum Cryptography-State of the Art.” *IEEE Security and Privacy* 15, no. 4 (2017): 12–13. https://doi.org/10.1109/MSP.2017.3151326.

Chen, Lidong. “Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?” *IEEE Security and Privacy* 15, no. 4 (2017): 51–57. https://doi.org/10.1109/MSP.2017.3151339.

Dinh, Hang, Cristopher Moore, and Alexander Russell. “The McEliece Cryptosystem Resists Quantum Fourier Sampling Attacks,” August 13, 2010. http://arxiv.org/abs/1008.2390.

Gidney, Craig, and Martin Ekerå. “How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits,” May 23, 2019. http://arxiv.org/abs/1905.09749.

Liao, Sheng Kai, Wen Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, et al. “Satellite-Relayed Intercontinental Quantum Network.” *Physical Review Letters* 120, no. 3 (January 19, 2018): 030501. https://doi.org/10.1103/PhysRevLett.120.030501.

Lucamarini, Marco, Andrew Shields Freng, Romain Alléaume, Christopher Chunnilall, Ivo Pietro Degiovanni, and Marco Gramegna. “Implementation Security of Quantum Cryptography.” Sophia Antipolis, France, 2018. https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf.

Moody, Dustin, Gorjan Alagic, Daniel C Apon, David A Cooper, Quynh H Dang, John M Kelsey, Yi-Kai Liu, et al. “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process.” Gaithersburg, MD, July 2020. https://doi.org/10.6028/NIST.IR.8309.

Mosca, Michele. “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” *IEEE Security and Privacy* 16, no. 5 (September 1, 2018): 38–41. https://doi.org/10.1109/MSP.2018.3761723.

Reinicke, Bryan, Jeffrey Cummings, and Howard Kleinberg. “The Right to Digital Self-Defense.” *IEEE Security and Privacy* 15, no. 4 (2017): 68–71. https://doi.org/10.1109/MSP.2017.3151324.

Sutor, Robert S. *Dancing with Qubits*. Birmingham, UK: Packt Publishing, 2019.

Vermeer, Michael, and Evan Peet. *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*. *Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption*. RAND Corporation, 2020. https://doi.org/10.7249/rr3102.

Villalonga, Benjamin, Dmitry Lyakh, Sergio Boixo, Hartmut Neven, Travis S. Humble, Rupak Biswas, Eleanor G. Rieffel, Alan Ho, and Salvatore Mandrà. “Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation.” *Quantum Science and Technology* 5, no. 3 (May 1, 2019). https://doi.org/10.1088/2058-9565/ab7eeb.

Xuejuan, Liu, Yuan Jiabin, Xu Juan, and Duan Bojia. “Speed up DDC Based on Quantum Computing.” *Journal of Central South University(Science and Technology)*, July 2018. http://en.cnki.com.cn/Article_en/CJFDTotal-ZNGD201807014.htm.

Yi-Ming, Huang, Lei Hang, and Li Xiao-Yu. “A Survey on Quantum Machine Learning.” *Chinese Journal of Computers*, January 2018. https://en.cnki.com.cn/Article_en/CJFDTotal-JSJX201801009.htm.