National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE CRYPTOGRAPHIC THREAT OF QUANTUM COMPUTERS ON ARMY COMMUNICATIONS

LCol B.C. Cornell

JCSP 42	PCEMI 42
Service Paper	**Étude militaire**

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

JCSP SERVICE PAPER – PCEMI ÉTUDE MILITAIRE

THE CRYPTOGRAPHIC THREAT OF QUANTUM COMPUTERS ON ARMY COMMUNICATIONS

LCol B.C. Cornell

“This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

Word Count: 2496

“La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.”

Compte de mots: 2496

THE CRYPTOGRAPHIC THREAT OF QUANTUM COMPUTERS ON ARMY COMMUNICATIONS

AIM

1. The purpose of this paper is to appraise the Director General Land Capability Development / Chief of Staff (Land Strategy) and the Army G6 of the potential threat posed by the emergence of quantum computers to the communication security of the Canadian Army. As the largest single user of cryptographic devices within the Government of Canada, the Canadian Army would be disproportionately affected by the risks posed. However, the threat needs to be balanced against other factors that would limit the utility of a quantum computer against the tactical environment. This paper will examine the theoretical threats posed by a quantum computer, evaluate the publicly acknowledged state of research, and discuss mitigation measures and other factors that would limit the risks.

INTRODUCTION

2. The Army relies on access to classified information delivered and shared via encrypted telecommunication links. These links are secured using cryptographic algorithms approved by national cryptologic agencies that evaluate and ensure the algorithm is practically, and theoretically, difficult to break based on known threats. In recent years, theoretical threats to conventional algorithms have arisen predicated on the emergence of a general-purpose quantum computer.

3. A quantum computer uses the quantum properties of particles to achieve a significant improvement in computing performance in certain areas. In particular, efficient quantum algorithm are known to exist that would jeopardize the strength of many current cryptographic systems. In August 2015, the United States' National Security Agency (NSA) openly acknowledged their pursuit of *quantum resistant* algorithms, and their expectation that transition

to these algorithms would need to be undertaken in the coming years.[1] Given Canada's reliance on US cryptographic devices to secure our communication links, any change made by the Americans will have repercussions in Canada.

DISCUSSION

Theoretical Risks

4. Cryptographic systems can be sub-divided based on their key types – (a) symmetric, or (b) asymmetric. In symmetric cryptographic systems, the same key is used for both encryption and decryption. In asymmetric systems, a different key is used for encryption and decryption. In the Army, most secure tactical radios rely on symmetric key systems. The Canadian and Army Key Management Systems (CKMS / AKMS) provide end-to-end security for the creation, storage, transmission, use and destruction of symmetric keys.

5. Asymmetric key systems, also commonly referred to as Public Key Systems, exploit an asymmetry in a mathematical operation.[2] The commonly known Rivest, Shamir and Adleman (RSA) algorithm exploits the difference in difficulty between multiplying two numbers versus factoring their product.[3] Asymmetric keys come in pairs, which are related by a mathematical operation. One key is usually published (known as the *public key*) based on the belief that calculating the related key (known as the *private key*) is mathematically difficult. Users employ the *public key* to encrypt their message before sending it to the private key holder. This type of cryptographic system is the foundation for information security on the internet.[4]

[1] Dan Goodin, "NSA advisory sparks concern of secret advance ushering in cryptoapocalypse," *Ars Technica*, 22 October 2015, accessed on 12 January 2016, http://arstechnica.com/security/2015/10/nsa-advisory-sparks-concern-of-secret-advance-ushering-in-cryptoapocalypse/.

[2] Neal Koblitz, *A Course in Number Theory and Cryptography, Second Edition* (New York: Springer-Verlag, 1994), 83 – 84.

[3] Neal Koblitz, *Algebraic Aspects of Cryptography* (Germany: Springer-Verlag, 1998), 5 - 6.

[4] Koblitz, *A Course in Number Theory and Cryptography, Second Edition*, 83 – 84.

6. From an Army perspective, asymmetric key systems are not used to secure communications at the tactical level. However, they are widely employed within the Land Command Support System (LCSS), the Defence Wide Area Network (DWAN), and the Consolidated SECRET Network Infrastructure (CSNI) to provide file encryption and digital signatures.

7. In 1994, mathematician Peter Shor created one of the first quantum algorithms that showed a marked improvement over its classical counterpart. *Shor's algorithm* could factorize a number using a general-purpose quantum computer much more quickly than could a classical one.[5] For those using the RSA algorithm, this creates a race between the size of the key and the strength of the quantum computer pursuing it. To preserve cryptographic strength, the keys need to grow, but this makes them more computationally expensive, consuming additional computing resources on the host.[6] As this weakness to RSA has been known since 1994, alternate public key solutions are under development, but have not been adopted.[7] Although they are not vulnerable to Shor's algorithm, this does not preclude the emergence of another quantum algorithm that compromises their security.[8] Current public key cryptographic systems continue to rely on RSA, Elliptic Curve Cryptography (ECC) and Diffie-Hellmann for their security, despite all of them being vulnerable to known quantum algorithms.

8. For symmetric key systems, quantum computers provide a more efficient method for brute force attacks. *Grover's algorithm* is a quantum algorithm that efficiently searches the key space for

[5] Paul Lopata, "Beyond digital: A brief introduction to quantum computing," *The Next Wave* 20, no. 2 (2013), accessed on 12 January 2016, https://www.nsa.gov/research/tnw/tnw202/article6.shtml.

[6] Campagna, Matthew et al. "Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges." *ETSI*, October 2014. Accessed on 12 January 2016. https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf, 11.

[7] Ibid., 13.

[8] Stephen Jordan, "Quantum Algorithm Zoo," accessed on 12 January 2016, http://math.nist.gov/quantum/zoo/. Dr. Jordan is a physicist with the US National Institute of Standards and Technology (NIST) and maintains a comprehensive list of all published quantum algorithms grouped by mathematical application.

a solution. Whereas a classical brute force attack on a key of length N would require approximately half of the key space to be tested before a solution was most likely found (i.e. 50% chance of success after checking 50% of the keys), the quantum attack does so in the square root of N. Consequently, a 256 bit key being attacked by a quantum computer only has the strength of a 128 bit key being attacked by a classical computer. Although this may not seem like a lot, it's useful to remember that a 256 bit key is 2^{128} times larger than a 128 bit key. This is equal to approximately 3.403 x 10^{38} more possibilities. The 128 bit key is not half as large, but *38 orders of magnitude* smaller.[9]

9. Separate from the key type, the NSA has also separated algorithms into two *suites*. *Suite A* algorithms are themselves classified, and are used to secure government communications up to the Top Secret and above levels. *Suite B* algorithms are publicly available, and are intended for use commercially, and to secure select government (including military) communications systems with classifications up to Secret.[10] Both suites of algorithm are jeopardized by quantum computers, although Suite B algorithms, being more widely known and used, are subject to more scrutiny. Most modern military radios use symmetric keys from a combination of Suite A and Suite B algorithms.

Public State of Quantum Computing

10. This section is specifically about the *public* state of quantum computing. Although it is likely that organizations such as the United States' National Security Agency (NSA) and Canada's Communication Security Establishment (CSE) are pursuing their own research, what they have achieved, if anything, remains unknown at this time. That they have publically acknowledged the

[9] Markus Grassl et al, "Applying Grover's algorithm to AES: quantum resource estimates," *ArXiv.org*, 15 December 2015, accessed on 12 January 2016, http://arxiv.org/abs/1512.04965.

[10] National Security Agency, "Cryptography Today," accessed on 12 January 2016, https://www.nsa.gov/ia/programs/suiteb_cryptography/.

threat, however, suggests that they view the emergence of a quantum computer as a question of *when*, and not *if*.

11. Understanding the current state of the art in quantum computers requires differentiating between a *quantum computer* and a *general-purpose quantum computer*, with the latter being a subset of the former (but not vice-versa). *Special-purpose quantum computers* already exist. The Canadian company, D-Wave, has been manufacturing a quantum computer based on *quantum annealing* techniques since 2010.[11] For many years, the limited numbers of *quantum bits* (known as *qubits*) employed by their system made it difficult to discern whether the expected quantum effect was taking place. However, recent research by the US National Aeronautics and Space Administration (NASA) and Google Artificial Intelligence Laboratories demonstrated a performance improvement of 10^8 over a classical computer.[12] This has definitively proven the value of quantum over classical computers for certain problems.

12. A *quantum annealing* computer works by establishing a quantum system is an excited state that encodes a particularly problem. By allowing the system to evolve naturally, the resulting steady-state that materializes corresponds with a *probable* answer. The likelihood of any state emerging is probabilistic with the states corresponding with a solution being the most likely. Through successive iterations of the same problem, a dominant solution should emerge which represents a best-possible answer.[13] By contrast, a *general-purpose quantum computer* works along the lines of a classical computer, with qubits being manipulated by quantum gates that replicate their classical analogues. This system does not evolve naturally, but is manipulated by a

[11] D-Wave, "Meet D-Wave – Our Vision and History," accessed on 12 January 2016, http://www.dwavesys.com/our-company/meet-d-wave.

[12] Hartmut Neven, "When can Quantum Annealing win?" *Google Research Blog*, 08 December 2015, accessed on 12 January 2015, http://googleresearch.blogspot.ca/2015/12/when-can-quantum-annealing-win.html.

[13] In some cases, an answer is easily checked. For instance, factorization can be quickly checked by simply multiplying the factors together to see if they yield the original number. Only more complex problems in which the correct answer is difficult to determine require multiple iterations.

program to achieve a desired result. Like its special-purpose counterpart however, the answer that results is still only probabilistic, so successive iterations may still need to be undertaken to arrive at a consensus answer.

13. The Shor and Grover algorithm were intended for use on a *general-purpose quantum computer*. To date, their use in the real world has been severely limited with the largest known factorizations being quite small.[14] Furthermore, no publically acknowledged algorithm using quantum annealing for factorization has emerged. D-Wave's quantum computer is designed for optimization problems, such as the well-known *travelling salesman problem*, and has no publically acknowledged applicability to cryptography.

14. Separate from D-Wave, academic interest in quantum computing remains fierce with several hundred new publications each year.[15] Increasingly, these publications have shifted away from fundamental research and into engineering, highlighting the emergence of practical investigations into manufacturing elements of a quantum computer including the qubits themselves, temporary and long term memory, and logic gates. Due to the sensitive nature of quantum systems to external input, most quantum systems to date can only exist for a fraction of a second. This limits their overall processing capacity to what can be physically conducted in that limited time. However, new techniques in qubit stabilization including quantum error detection and correction are enabling these systems to persist over longer periods, significantly increasing the complexity of the operations that they can undertake.[16]

Impact on Army Communications

[14] Lisa Zyga, "New largest number factored on a quantum device is 56,153," *Phys.org*, 28 November 2014, accessed on 26 January 2016, http://phys.org/news/2014-11-largest-factored-quantum-device.html.

[15] M.I. Dyakonov, "State of the Art and Prospects for Quantum Computing," *Research Gate*, December 2012, accessed on 01 February 2016, https://www.researchgate.net/publication/233917770_State_of_the_art_and_prospects_for_quantum_computing, 1.

[16] Larry Hardesty, "Advance in quantum error correction," *MIT News*, 26 May 2015, accessed on 01 February 2016, http://news.mit.edu/2015/quantum-error-correction-0526.

15. The Army is in the midst of a cryptographic upgrade as part of the Defence Cryptographic Modernization Program (DCMP). DCMP is a subset of the larger, Government-wide upgrade known as the Canadian Cryptographic Modernization Program (CCMP) which is being run by CSE. As part of DCMP, legacy algorithms at jeopardy from faster *classical* computers are being upgraded in a selection of radios and encryption devices.[17] Most notably, the Combat Net Radio (Primary) is being upgraded with new algorithms as part of the Combat Net Radio Enhancement (CNRE) project. This will provide improved cryptographic security against existing threats, but suffers from the same deficiencies against quantum threats discuss above. Fortunately, the radio incorporates a software-programmable cryptographic module allowing for future upgrades that could incorporate quantum resistant algorithms.

16. The remainder of the Army radio fleet has also been evaluated for upgrade under DCMP. Like CNRE, most of the radio fleet and in-line network encryptors procured in the past decade are software-upgradeable. However, as highlighted by the DCMP project, the volume of radios and cryptographic devices makes the scale of a recall, upgrade, and re-issue difficult.[18] It also assumes that the device vendor will implement the new algorithms on their hardware vice trying to sell an entirely new device. The complexity of quantum resistant algorithms are also, still, largely theoretical, so the computing power required for their use is unknown. Algorithm development typically balances strength with efficiency, especially for algorithms supporting real-time

[17] The *Capability Deficiency* states that “Canadian cryptographic equipment is reaching a time when the algorithms will be out of date and some equipment will no longer be maintainable.” (DWAN: https://cid-bic.forces.mil.ca/Cid/project-home_e.asp, Search for – “Defence Cryptographic Modernization Project.”)

[18] Francis Pelletier and Leslie Guyatt, “Defence Cryptographic Modernization Project Annual Senior Review Board Brief – 08 June 2015,” *Capability Investment Database (CID),* accessed on 26 January 2016, DWAN: http://cid-bic.forces.mil.ca/Cid/project-home_e.asp. Search for “Defence Cryptographic Modernization Project.” The DCMP began in 2008. The schedule on slide 11 of the presentation shows the sub-projects for the Classified Security Management Infrastructure and Secure Radio stretching into 2020 and beyond.

encryption. Depending on the age of the device, it may not possess sufficient computing power to properly implement a new solution, necessitating a complete replacement with associated costs.

17. Future upgrades to radios only protect future traffic from decryption. Any traffic previously recorded by an adversary would be susceptible to decryption using future means. Although most people assume that past transmissions are lost forever, the presence of cheap receivers and inexpensive storage make it easy and cost effective to maintain recordings for a long time. Although this is unlikely in general, it is not past the capabilities of near-peer adversaries like the Russians or the Chinese. Fortunately, tactical communications are time sensitive and likely to lose relevance within 24 - 48 hours. However, strategic communications using satellite communications or leased lines as the medium may be jeopardized by hostile signals intelligence. This is a threat today, independent of future quantum risks, but doubly highlights the importance of operational, information, and communication security processes and procedures. Communications recorded today using current algorithms may be susceptible to quantum attacks in the future.

18. The tactical nature of most Army communications protects against the likelihood of a real-time attack on our communications. In their earliest incarnations, quantum computers are likely to be physically sensitive, and unsuitable for use in a hostile environment. Although tactical communications can be recorded, and transmitted for off-air decryption, the volume and turn-around time will dictate the utility. In order to deny real-time access to communications, limitations on the length of time a key can be used need to be re-examined. If the key is not changed before it is cracked, it would provide an opportunity for real-time monitoring. In the case of symmetric keys with quantum susceptible algorithms, quantum attacks substantially reduce the length of time that a key can be used due to the more efficient search of the key space. This is the case for many radios and cryptographic devices being upgraded by DCMP. More rapid turnover in

key material would be required to minimize the threat (e.g. monthly changing becomes weekly, weekly becomes daily, etc…) both to defeat concerns about real-time interception, and also limit the volume of historical data that could be recovered for any given key. Automated solutions for re-keying should be pursued to facilitate timelier turnover, and alleviate the risks from human intervention failing to do so.

CONCLUSION

19. Quantum computers represent a significant threat to existing cryptographic security. Asymmetric algorithms are particularly vulnerable when they publish a portion of their keys. Symmetric algorithms are more vulnerable to brute force attacks. The emergence of quantum annealing computers has proven that a quantum computer is possible with real world applications today. The elements for a general-purpose quantum computer are being prototyped in academic and industrial laboratories around the world, overcoming many of the hurdles in designing and building a fully functional system. Classified development in this area is unknown, but is likely to be on par, if not several years beyond, the public state of affairs. The public warning by the NSA highlights their belief that the threat is real, and on the horizon.

20. For the Canadian Army, as the largest single user of cryptographic devices in the Government of Canada, the requirement to defend against this threat in the future is real. Fortunately, the tactical nature of the land environment limits opportunities for interception, and the perishability of tactical information limits its value in the future. Even with the sudden emergence of a viable quantum computer, the Army could adopt a more aggressive re-keying schedule to minimize the risk at the tactical-level. However, the wider risk to operational networks employing public key systems is much more alarming.

RECOMMENDATION

21. The Army is ill-suited to monitor the development of quantum computing closely. It should rely on the national cryptologic agencies to evaluate and warn of any impending threats. However, it should be aware of potential threats, and plan acquisition and upgrade of future cryptographic devices and systems accordingly such that –

a. They are easily upgraded with new algorithms, and that the vendor is committed to long term support along these lines;

b. Automated key exchange and roll-over is pursued to ensure swift and reliable re-keying;

c. The Army Key Management System (AKMS) is capable of handling increased key volume to counter the unexpected emergence of quantum computers through an accelerated re-keying schedule;

c. The AKMS remains sufficiently flexible to integrate new key material suitable for quantum-resistant algorithms; and,

d. The Army should plan for participation in a *Next-Generation Cryptographic Modernization Project* beginning sometime in the next five years.[19]

[19] The *Capability Investment Database (CID)* already lists a new project entitled the *Advanced Cryptographic Capabilities Project (ACCP)* that identifies the requirement to produce quantum resistant cryptographic algorithms for end cryptographic units using the Enhanced Firefly (EFF) protocol. However, it is not yet part of the Strategic Capability Investment Plan (SCIP), and so has no dates associated with it. Furthermore, the scope should be re-addressed to consider quantum resistant algorithms beyond the EFF protocol. (DWAN: http://cid.bic.forces.mil.ca/CID/ - Search for "Advanced Cryptographic Capabilities Project")

BIBLIOGRAPHY

Deangelis, Stephen F. “Closing in on quantum computing.” *Wired,* October 2014. Accessed on 12 January 2016. http://www.wired.com/insights/2014/10/quantum-computing-close/.

D-Wave. “Meet D-Wave – Our Vision and History.” Accessed on 12 January 2016. http://www.dwavesys.com/our-company/meet-d-wave.

Dyakonov, M.I. “State of the Art and Prospects for Quantum Computing.” *Research Gate,* December 2012. Accessed on 01 February 2016. https://www.researchgate.net/publication/233917770_State_of_the_art_and_prospects_for_quantum_computing.

Campagna, Matthew et al. “Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges.” *ETSI,* October 2014. Accessed on 12 January 2016. https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf.

Goodin, Dan. “NSA advisory sparks concern of secret advance ushering in cryptoapocalypse.” *Ars Technica*, 22 October 2015. Accessed on 12 January 2016. http://arstechnica.com/security/2015/10/nsa-advisory-sparks-concern-of-secret-advance-ushering-in-cryptoapocalypse/.

Goodin, Dan. “NSA preps quantum-resistant algorithms to head off crypto-apocalypse.” *Ars Technica*, 21 August 2015. Accessed on 12 January 2016. http://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/.

Grassl, Markus, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. “Applying Grover’s algorithm to AES: quantum resource estimates.” *ArXiv.org*, 15 December 2015. Accessed on 12 January 2016. http://arxiv.org/abs/1512.04965. To appear in *Proceedings of the 7th International Conference on Post-Quantum Cryptography*.

Hardesty, Larry. “Advance in quantum error correction.” *MIT News,* 26 May 2015. Accessed on 01 February 2016. http://news.mit.edu/2015/quantum-error-correction-0526.

Jordan, Stephen. “Quantum Algorithm Zoo.” Accessed on 12 January 2016. http://math.nist.gov/quantum/zoo/.

Koblitz, Neal and Alfred J. Menezes. “A Riddle Wrapped in an Enigma.” Accessed on 12 January 2016. http://eprint.iacr.org/2015/1018.pdf.

Koblitz, Neal. *A Course in Number Theory and Cryptography, Second Edition*. New York: Springer-Verlag, 1994.

Koblitz, Neal. *Algebraic Aspects of Cryptography*. Germany: Springer-Verlag, 1998.

Lopata, Paul. "Beyond digital: A brief introduction to quantum computing." *The Next Wave* 20, no. 2 (2013). Accessed on 12 January 2016. https://www.nsa.gov/research/tnw/tnw202/article6.shtml.

Metz, Cade. "Google's Quantum Computer just got a big upgrade." *Wired*, 28 September 2015. Accessed on 12 January 2016. http://www.wired.com/2015/09/googles-quantum-computer-just-got-a-big-upgrade-1000-qubits/.

Metz, Cade. "Google's Quantum Computer proven to be the real thing (almost)." *Wired*, 28 June 2013. Accessed on 12 January 2016. http://www.wired.com/2013/06/d-wave-quantum-computer-usc/.

National Security Agency. "Cryptography Today." Accessed on 12 January 2016. https://www.nsa.gov/ia/programs/suiteb_cryptography/.

Neven, Hartmut. "When can Quantum Annealing win?" *Google Research Blog*, 08 December 2015. Accessed on 12 January 2015. http://googleresearch.blogspot.ca/2015/12/when-can-quantum-annealing-win.html.

Pelletier, Francis and Leslie Guyatt. "Defence Cryptographic Modernization Project Annual Senior Review Board Brief – 08 June 2015." *Capability Investment Database (CID)*. Accessed on 26 January 2016. DWAN: http://cid-bic.forces.mil.ca/Cid/project-home_e.asp. Search for "Defence Cryptographic Modernization Project."

Zega, Lisa. "New largest number factored on a quantum device is 56,153." *Phys.org*, 28 November 2014. Accessed on 26 January 2016. http://phys.org/news/2014-11-largest-factored-quantum-device.html.