National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CRITICAL TIME FOR CLASSIC ENCRYPTION

Major Michael Janelle

JCSP 45

Service Paper

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.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2019.

PCEMI 45

Étude militaire

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

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2019.

Canada

CANADIAN FORCES COLLEGE
JCSP 45
2018 - 2019

DS545 COMPONENT CAPABILITIES

CRITICAL TIME FOR CLASSIC ENCRYPTION

By Major Michael Janelle

"This paper was written by a candidate attending the Canadian Forces College in fulfillment 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: 2,275

« 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. »

Nombre de mots: 2,275

CRITICAL TIME FOR CLASSIC ENCRYPTION

AIM

1. The aim of this paper is to inform the Chief of Staff Army Strategy (COS Army Strat) and Director Land Command and Information (DLCI) on the current advances in commercially available cryptography, the emergence of quantum computing, and how the Canadian Army (CA) should approach network security in the future in order to mitigate potential security concerns. Quantum computing has potentially become a threat to the most recent encryption algorithms, and the development of new standards to counter this phenomenon has initiated significant investments into the next generation of cryptographic algorithms. This paper will provide an overview of the most recent theory on cryptographic, examine the threat of Shor's algorithm and the emergence of quantum computing on network security, and provide a summary of the future of cryptographic capability development.

INTRODUCTION

2. Communication links and classified information systems (IS) are critical enablers for the CA Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) given the full spectrum of operations that it must force generate for in support of contemporary missions. The CA IS must be agile in nature and could be deployed anywhere at anytime. The ability to operate in a degraded environment and difficult terrain, where the infrastructure is minimal and in which the threat of attack is permanent, communicating quickly and securely is a challenge. To meet this vital need, the CA must protect the IS, which enable C4ISR, against information loss by using robust cryptographic capabilities.

3. The materialization of quantum computing poses a significant threat to current cryptographic algorithms, and the solution to this problem is the foundation of all future encryption. Over the last twenty-five years, the expansion of the information theory encompassing pure quantum effects has been of increasing interest. The realization of a quantum information processing system, a quantum computer, however, presents numerous challenges, and while quantum computing is far from being operational on a large scale, national security agencies and military organizations are seriously concerned about the emergence of quantum computing as a threat to their classified IS and communication links.[1]

DISCUSSION

Classic Cryptography

4. Cryptology is the science of secrets and includes cryptography, which secures the information emitted. In the case of public key asymmetric cryptography, encryption only exploits public keys and decryption relies on public and private keys. Decryption exploits only public keys by seeking to deduce private keys by calculation, often intensive.

5. Cryptography secures the information transmitted in several ways: by confidentiality (only the recipient can recover the unencrypted version of the information transmitted), by integrity (the information has not been modified during transmission), by authentication (everyone is the one they claim to be), non-repudiation (the issuer can not deny having transmitted the encrypted information) and access control (only those authorized by the issuer and the recipient can access unencrypted information).

[1] Runser, Robert. "Progress Toward Quantum Communication Networks: Opportunities and Challenges." Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/digital-media-center/publications/research-papers/assets/files/progress-toward-quantum-comms-networks.pdf.

6. There exist different types of cryptography. Suite A (also known as Type 1) uses classified algorithms and is the most commonly used to protect data on military IS. Suite B uses unclassified algorithms developed by industry. While Type 1 offers great protection and security, it is difficult and costly to develop, maintain and implement, and must be handled only by personnel with appropriate security clearances.[2] The use of commercial-off-the-shelf (COTS) cryptographic algorithms is perhaps the most effective way of fighting off the effects of technology obsolescence, enabling network-centric military operations, coping with a flood of data dissemination and data sharing, making imagery and video a central component of military intelligence and situational awareness, keeping the costs of developing and maintaining cryptographic technology to a minimum, inserting the latest cryptographic capability into legacy secure systems, and ensuring interoperability among allies secure communications and information systems.[3]

The Threat of Shor's Algorithm and Quantum Computing

7. Peter Shor's algorithm, invented in 1994 and which makes it possible to quickly factor whole numbers, has shaken the world of network security for at least a good twenty-five years.[4] Indeed, it theoretically breaks the number codes of public key cryptography systems that are commonly used on the Internet. Shor showed that with a quantum computer, we could factor numbers made of thousands or even millions of numbers. Shor uses the link between the factorization problem and the search for a period in a function. Using quantum superposition, it

[2] Keller, John. "Crypto Modernization Transforms Military Communications December 2011." *Military and Aerospace Electronics*, Vol. 22, no. 12 (2011). Accessed on 10 October 2018. https://www.militaryaerospace.com/articles/print/volume-22/issue-12/special-report/crypto-modernization-transforms-military-communications.html.

[3] *Ibid*.

[4] Hayward, Matthew. "Quantum Computing and Shor's Algorithm." Accessed on 10 October 2018. https://pdfs.semanticscholar.org/8072/dc7247460849b18abbb463429a09cfb2e3e6.pdf.

shows how to resonate quantum states around the period of the function to find it, and then uses this result to factor quickly. For comparison, the best current algorithms for factorizing a 600-digit number need millions of millions of years to factorize such a number, whereas a fully functional quantum computer could do this in minutes.[5]

8. Quantum computers operation is deeply rooted in the world of quantum physics. Instead of using bits to do their calculations, like traditional computers, they use qubits, which essentially are controlled subatomic particles. The bits can take a value of 0 or 1. The qubits, through a quantum property called superposition, can in one direction take both values at the same time, which allows them to perform multiple calculations simultaneously. Qubits also have the ability to be connected to each other through another property called entanglement, which means that even if they are physically separated, when the state of a qubit changes, the state of the other is instantly affected. Scientists have not yet succeeded in explaining the causes behind these phenomena, but that does not prevent them from exploiting them in quantum computers. With equal efficiency, they can do in minutes what conventional computers could do in an enormous amount of time.

9. The Rivest, Shamir and Adleman (RSA) algorithm is one of the most widely used public key systems. This algorithm is based on the use of a key pair composed of a public key to encrypt and a private key to decrypt confidential data. The public key is a key that is accessible by anyone wishing to encrypt data, while the private key is reserved for the holder who created the key pair. The main advantage of public key cryptography lies in the ease of management of users' key pools. Indeed, the increase in the number of users does not over complicate the

[5] Rouse, Margaret. “RSA Algorithm.” Accessed on 10 October 2018. https://searchsecurity.techtarget.com/definition/RSA.

procedure. In addition, the influx of new users and their integration requires very little effort and does not change the parameters of others. Thus, public key cryptography solves the problem of key distribution that can be encountered in private key cryptography. However, asymmetric techniques suffer from their slowness. Encrypting a message is 100 to 1000 times longer than some symmetric techniques.

10. In the current state of the art, the decryption of RSA keys of 2048 or 4096 bits, the most used, is theoretically impossible to achieve with the computing power available. Note that a key 2048 is a number with 617 digits.[6] If RSA keys of 1024 bits can be broken with the use of artificial intelligence, this is not the case with RSA keys of 2048 or 4096 bits, and experts[7] believe that it is unlikely that it is possible in the short term, including with the most powerful calculators. However, the situation will be radically different with quantum computers for which such keys could be decrypted in just a few minutes. Therefore, this requires a complete rethinking of network security and cryptographic algorithms in the quantum environment, and the scientific community is actively looking to achieve a standard for a filed that does not yet exist.

11. Today's network security relies on computational assumptions and the inability of current computers to solve certain mathematical problems.[8] We often hear about cryptographic attacks and security breaches but very rarely attacks on these computational assumptions themselves. Clearly, the mathematical foundations of our network security are relatively strong. For example, the RSA cryptographic algorithm, used in many protocols on the Internet (Internet Protocol (IP)

[6] *Ibid*.

[7] Runser, Robert. "Progress Toward Quantum Communication Networks: Opportunities and Challenges." Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/digital-media-center/publications/research-papers/assets/files/progress-toward-quantum-comms-networks.pdf.

[8] Maji, Hemanta. "Cryptographic Complexity Classes and Computational Intractibility Assumptions." Accessed on 10 October 2018. https://www.cs.purdue.edu/homes/hmaji/papers/MajiPrRo10a.pdf.

based networks), relies on the difficulty of factoring large numbers. The arrival of a quantum computer would therefore greatly reduce the computational assumptions on which we can base ourselves to guarantee the security of our networks. Therefore, investments in cryptographic capabilities cannot be delayed until quantum computing becomes a reality. Cryptographic developers must develop effective solutions that will adapt to new attack techniques or technology, and encryption products must be neutral, non-intrusive, simple to use, and reliable.[9]

Current State and Future Development

12. The move towards a complete networking of all domains (the Internet of things) in a theoretically unlimited global data space (cyberspace) offers great opportunities for military and technological advancements, but also multiple possibilities of attacking the flow of communication (including cyber-attacks), which could have devastating consequences on our security and our military ability to establish this security.[10]

13. In general, the main deficiencies identified for most IS include the end of life cryptographic algorithms, the inability to share key material with some coalition partners or allies, a lack of programmability for algorithms and application software, and inadequate cryptographic bandwidth to support current communication requirements.[11]

14. The Land Command Support System (LCSS) is the CA operational network supporting classified C4ISR information exchange at the strategic, operational and tactical levels, and relies

[9] National Security Agency. "Virtual Private Network Capability Package." Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/vpn-cp.pdf

[10] Richards, Rebecca. "Internet of Things." The Next Wave, Vol. 21, no. 2 (2016). Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-21-2.pdf.

[11] Pelletier, Francis and Leslie Guyatt. "Defence Cryptographic Modernization Project Link Encryption." Brief to Annual Senior Review Board, Ottawa, 8 June 2015. *Capability Investment Database (CID)*. Accessed on 19 July 2012. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Canadian Cryptographic Modernization Project."

on cryptography procured from allies (mainly United States (US)) to safeguard the confidentiality of data-in-transit. As quantum computing may disrupt cryptography technology in the future, it is being assessed as a liability not yet fully quantifiable, and with limited mitigation.

15. History has shown us that when an encryption protocol became breakable, more secure encryption solutions came into being at the same time. We can imagine that if one day a quantum computer can break a classic encryption, a more robust encryption solution, potentially based on quantum cryptography, will be available. The National Security Agency (NSA) in the US uses a series of Suite B algorithms to protect its documents and communications. These algorithms defined by the National Institute of Standards and Technology (NIST) are used in particular for file encryption or identification by electronic signature. But the NSA explains that these algorithms, based on elliptic curve cryptography (ECC), are not the long-term cryptographic solutions it has hoped for. The ECC relies on extremely complex mathematical calculations, out of reach of traditional calculators, but the agency considers that the speed of progress in the development of quantum computers represents for it a danger. The ECC uses encryption keys that are smaller than those of other techniques with equivalent security, which might be considered as an advantageous feature, but really makes it more vulnerable to quantum computing.[12]

16. Until these new algorithms are developed, the NSA recommends that companies and government agencies that have not yet made the transition to elliptical curve cryptography not invest too much in these technologies and prepare themselves to the transition to algorithms designed to withstand quantum computing.

[12] National Security Agency. “Virtual Private Network Capability Package.” Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/vpn-cp.pdf

17. The NSA has embarked on a program to replace all of the Type 1 cryptographic equipment in the US inventory.[13] In response to this US initiative, the Canadian Security Establishment (CSE) initiated a national Canadian Cryptographic Modernization Program (CCMP) to replace all of the Type 1 cryptographic equipment in Canada, about 80% of which is used by DND/CAF.[14] The Defence Cryptographic Modernization Project (DCMP) will replace affected Type 1 End Cryptographic Units (ECU) in the DND/CAF inventory and strive to develop the in-service support (ISS) concept required to maintain and sustain new cryptographic capabilities being delivered over the next ten years.[15]

18. Including CCMP and DCMP, there are six projects under the Cryptographic Capabilities Program (CCP) delivering cryptographic and radio equipment in order to address the deficiencies. These projects are grouped under initiative 65 of Canada's Defence Policy (Strong, Secure, Engaged (SSE)).[16]

CONCLUSION

19. In cryptography, sovereignty is at stake with the challenge of protecting sensitive communications. While scientific uncertainty seems to be partly removed with respect to the feasibility of commercially exploitable quantum computers, there are still significant

[13] Keller, John. "Crypto Modernization Transforms Military Communications December 2011." Military and Aerospace Electronics, Vol. 22, no. 12 (2011). Accessed on 10 October 2018. https://www.militaryaerospace.com/articles/print/volume-22/issue-12/special-report/crypto-modernization-transforms-military-communications.html.

[14] Pelletier, Francis and Leslie Guyatt. "Canadian Cryptographic Modernization Project." Brief to Annual Senior Review Board, Ottawa, 8 June 2015. *Capability Investment Database (CID)*. Accessed on 10 October 2018. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Canadian Cryptographic Modernization Project."

[15] Gibeault, Etienne and Tony Moffa. "Defence Cryptographic Modernization Project." Brief to Annual Senior Review Board, Ottawa, 10 February 2016. *Capability Investment Database (CID)*. Accessed on 10 October 2018. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Defence Cryptographic Modernization Project."

[16] Guyatt, Leslie. "Advanced Cryptographic Capabilities Project Increment 1." Delivering SSE Initiative 65 Business Case Analysis Brief, Ottawa, 4 December 2017. *Capability Investment Database (CID)*. Accessed on 10 October 2018. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Advanced Cryptographic Capabilities Project Increment 1."

technological hurdles to overcome in order to achieve this, including the thorny issue of qubit noise and correction of quantum errors.

20. At this time, there is no requirement for the CA to get in a panic mode. Even the most optimistic predictions about how quickly quantum computing will become a reality indicate that products with a lifespan of less than ten years are protected. That being said, the CA would benefit from the integration of more agile cryptographic solutions. The goal would be to have a feature that can replace keys and algorithms as soon as they become obsolete. This mechanism would make it possible to maintain a fleet of resistant products, even if certain algorithms become vulnerable. At this time, the key is to stay informed on the evolution of cryptographic capabilities and remain engaged in the emergence of quantum computing.

RECOMMENDATION

21. In line with CSE and DND/CAF, the CA would benefit from investing into future cryptographic capability development to address the threat posed by quantum computing, to minimize the ISS resources required to manage and distribute key material and maintain classified communication links, network security and interoperability with the US and allies.[17] The desirable characteristics of the CA future cryptographic capabilities should include:

a. **Agility:** Future algorithms need to be adaptable to the threat posed by quantum computing or the emergence of other new technologies.

b. **Ease-of-Use:** The cryptographic solution must strive to achieve timely distribution of keys and software upgrades via an automated system, and have the ability to switch algorithms as required while not compromising security.

[17] Harris, Michael. “Advanced Cryptographic Capabilities Project Increment 1.” Business Case Analysis brief to Defence Capabilities Board, Ottawa, 12 December 2017.

c. **Cost Effective Support:** Improved availability of cryptographic equipment and the ability to maintain the overall capability through proper lifecycle management and increased support from the original equipment manufacturer (OEM).

d. **Interoperability:** Ability to share key material and equipment with allies through updates to cryptographic algorithms or application software.

e. **Cryptographic Bandwidth:** The next generation of cryptographic algorithms and equipment must support the increase of data throughputs, information exchange requirements (IER) and user demands.

BIBLIOGRAPHY

Cassie, Michael. "Cryptographic Capabilities Program." Brief to Program Management Board, Ottawa, 5 April 2018.

Gibeault, Etienne and Tony Moffa. "Defence Cryptographic Modernization Project." Brief to Annual Senior Review Board, Ottawa, 10 February 2016. *Capability Investment Database (CID)*. Accessed on 10 October 2018. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Defence Cryptographic Modernization Project."

Guyatt, Leslie. "Advanced Cryptographic Capabilities Project Increment 1." Delivering SSE Initiative 65 Business Case Analysis Brief, Ottawa, 4 December 2017. *Capability Investment Database (CID)*. Accessed on 10 October 2018. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Advanced Cryptographic Capabilities Project Increment 1."

Harris, Michael. "Advanced Cryptographic Capabilities Project Increment 1." Business Case Analysis brief to Defence Capabilities Board, Ottawa, 12 December 2017.

Hayward, Matthew. "Quantum Computing and Shor's Algorithm." Accessed on 10 October 2018. https://pdfs.semanticscholar.org/8072/dc7247460849b18abbb463429a09cfb2e3e6.pdf.

Keller, John. "Crypto Modernization Transforms Military Communications December 2011." *Military and Aerospace Electronics*, Vol. 22, no. 12 (2011). Accessed on 10 October 2018. https://www.militaryaerospace.com/articles/print/volume-22/issue-12/special-report/crypto-modernization-transforms-military-communications.html.

Maji, Hemanta. "Cryptographic Complexity Classes and Computational Intractability Assumptions." Accessed on 10 October 2018. https://www.cs.purdue.edu/homes/hmaji/papers/MajiPrRo10a.pdf.

National Security Agency. "Virtual Private Network Capability Package." Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/vpn-cp.pdf

Pelletier, Francis and Leslie Guyatt. "Canadian Cryptographic Modernization Project." Brief to Annual Senior Review Board, Ottawa, 8 June 2015. *Capability Investment Database (CID)*. Accessed on 10 October 2018. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Canadian Cryptographic Modernization Project."

Pelletier, Francis and Leslie Guyatt. "Defence Cryptographic Modernization Project Link Encryption." Brief to Annual Senior Review Board, Ottawa, 8 June 2015. *Capability Investment Database (CID)*. Accessed on 19 July 2012. DWAN: http://cid-bic.forces.mil.ca/CID/search_e.asp. Search for "Canadian Cryptographic Modernization Project."

Richards, Rebecca. "Internet of Things." *The Next Wave,* Vol. 21, no. 2 (2016). Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-21-2.pdf.

Rouse, Margaret. "RSA Algorithm." Accessed on 10 October 2018. https://searchsecurity.techtarget.com/definition/RSA.

Runser, Robert. "Progress Toward Quantum Communication Networks: Opportunities and Challenges." Accessed on 10 October 2018. https://www.nsa.gov/resources/everyone/digital-media-center/publications/research-papers/assets/files/progress-toward-quantum-comms-networks.pdf.