Canadian Global Affairs Institute
Institut canadien des affaires mondiales

How Canada Can Prepare for the Quantum Threat

by Nina Bindel and Kristen Csenkey

June 2021

POLICY PERSPECTIVE

How Canada Can Prepare for the Quantum Threat

by Nina Bindel[1] and Kristen Csenkey[2], CGAI Fellow

June 2021

Canadian Global Affairs Institute
Institut canadien des affaires mondiales

Prepared for the Canadian Global Affairs Institute
1800, 150 – 9th Avenue S.W., Calgary, AB T2P 3H9
www.cgai.ca

ISBN: 978-1-77397-192-6

[1] This work was partially supported by the Institute for Quantum Computing (IQC). IQC is supported in part by the Government of Canada and the Province of Ontario.

[2] Funding for a portion of this research was made possible by the Department of National Defence through a Mobilizing Insights in Defence and Security (MINDS) Targeted Engagement Grant (TEG) award to the author. She would like to thank Aniksa Graver for her research assistance.

The current hype about quantum computers and related technologies leaves space for confusion, especially about the “quantum threat”. Quantum computers (QCs) enable faster computations, but also threaten to break many of our current crypto-algorithms used to ensure security on the internet. How should this threat be identified and what should be done to respond to it and address it? Moreover, what are the current strategic visions and policy directions that shape these responses?

This policy perspective provides a brief exploration on how the Five Eyes (FVEY: Australia, Canada, New Zealand, the United Kingdom and the United States) prepare against the quantum threat. In addition, this paper discusses a paradox: transparency about security decisions could be a governance option to address the quantum threat.

Quantum Computers 101

Quantum technology, and in particular large-scale QCs, promises efficient computations for many important applications, and therefore offers economic benefits. While conventional computers compute their operations on bits that can be one or zero, QCs use quantum physical principles to process and save data on so-called quantum bits (qubits). This allows speed-ups for some computations but certainly not all. As exciting as this opportunity may seem, QCs are a double-edged sword.

The Double-Edged Sword

The double-edged sword analogy shows us that although there are benefits to using large-scale QCs, it will be possible to essentially break all public-key cryptography (PKC) in use today, such as the famous RSA algorithm. This is not as intangible or removed as one would think. For example, this includes the cryptography that is used today to establish secure connections on the internet. Secure connections allow accessing websites, such as the one on which you are reading this article, or permit you to conduct online banking securely. If large quantum computers are built, these secure algorithms will be broken.

Due to the increasing digitalization of most areas of our lives, a break in IT security poses a threat to the health, safety and economic well-being of people, governments, the military and industry. The double-edged sword of opportunities and risks leaves us with an important question to contextualize the threat: Is it possible to build a large-scale QC that will be able to break the RSA algorithm? In short, the answer to this question is perhaps.

The current record-holding QC uses 72 qubit.[3] A new study shows that to break RSA-2048, 20 million qubits are necessary.[4] Regardless of the missing 19,999,928 qubits, researchers[5] and governments[6] expect that QCs able to break RSA will likely exist in the next 15 to 30 years. This means that governments and industry need to prepare for the quantum threat. It is important to ensure IT security in the future, but also to reduce possibilities for back traffic attacks, where attackers already store huge amounts of data.

In short, the main issue is that data sent securely and stored today will be decrypted as access to large QCs becomes a reality for many actors in the near future. What are Canada and its allies doing to specifically address the quantum threat? The FVEY's strategies paint a complex and mixed picture.

How the FVEY Deal with the Threat

Through the intelligence alliance of the FVEY, Australia, Canada, New Zealand, the U.K. and the U.S. co-operate to share information related to defence and security. A systematic analysis of defence, security and quantum-related strategies and other documents[7] finds that co-operation in addressing the quantum threat is not clear across the board.

For example, one strategy is to support research to develop crypto-algorithms that are secure even in the presence of quantum attackers (i.e., attackers with access to a powerful QC), and that can inter-operate with our existing communications protocols and infrastructure. Such new algorithms are also called post-quantum or quantum-safe algorithms. Post-quantum standardization is a process developed, for example, by the U.S. National Institute for Standards and Technologies (NIST),[8] which aims to standardize basic post-quantum algorithms such as public-key encryption and signature schemes in 2024 (as seen in Figure 1).

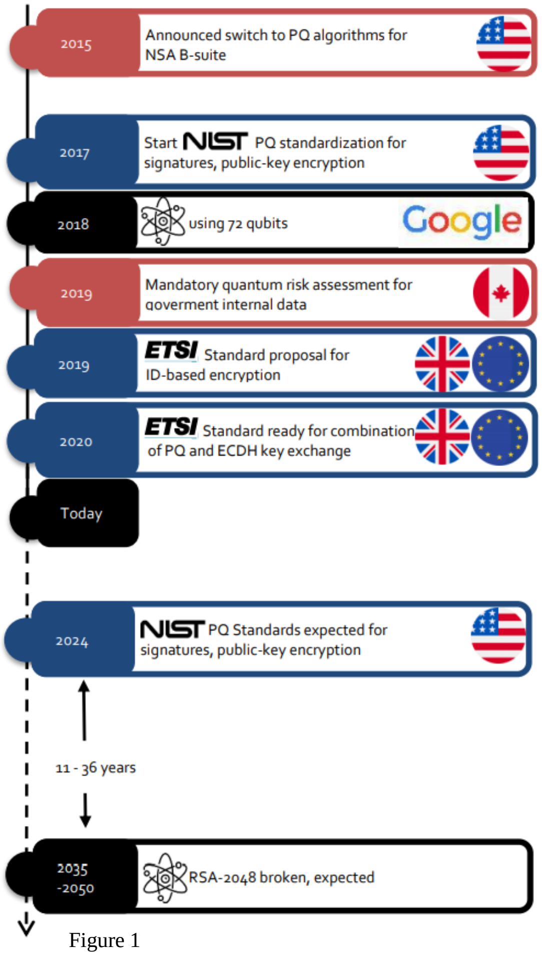
2015
Announced switch to PQ algorithms for NSA B-suite
2017
Start NIST PQ standardization for signatures, public-key encryption
2018
using 72 qubits
Google
2019
Mandatory quantum risk assessment for goverment internal data
2019
ETSI Standard proposal for ID-based encryption
2020
ETSI Standard ready for combination of PQ and ECDH key exchange
Today
2024
NIST PQ Standards expected for signatures, public-key encryption
11 - 36 years
2035 -2050
RSA-2048 broken, expected

Figure 1

[3] Julian Kelly, "A Preview of Bristlecone," Google AI Blog, March 5, 2018. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

[4] C. Gidney and M. Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits," *Quantum* 5, 433, Cornell University, May 2019 (last revised April 13, 2021). https://arxiv.org/abs/1905.09749.

[5] Michele Mosca and Marco Piani, "Quantum Threat Timeline," Global Risk Institute, October 2019. https://globalriskinstitute.org/publications/quantum-threat-timeline/.

[6] Qurope.eu, "Quantum Manifesto: A New Era of Technology," Report, May 2016. http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf.

[7] Preliminary work in progress by authors.

[8] More information about the process can be found at https://csrc.nist.gov/projects/postquantum-cryptography.

Not all states have the same strategic perspective. Some states, like Canada and the U.K., focus on education, among other areas, but understand it as raising awareness to industry bodies and the public (as seen in the simplified diagram in Figure 2), while other states focus on standardization in addition to other priorities. Although these strategies are important, by themselves they highlight limited options to ensure security against quantum attackers. In addition to this, other measures are needed to enable a smooth and secure transition that is mindful of the current infrastructure. Moreover, it is important to develop and standardize crypto-algorithms with advanced functionality to ensure that all crypto-applications can be protected against quantum attackers. For example, the European Telecommunications Standards Institute (ETSI) started a process for so-called ID-based public-key encryption, but more algorithms are necessary. The bottom line is that new algorithms for all applications need to be standardized, implemented and used securely.

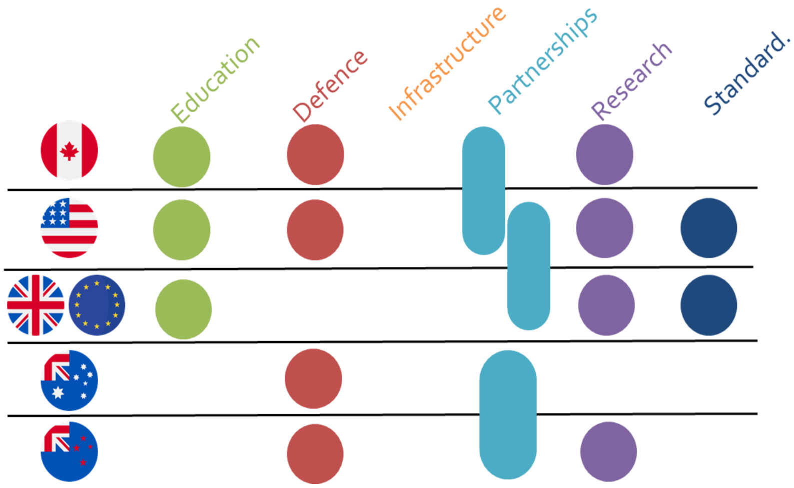

Figure 2

How to Achieve More Security by Being More Transparent

Replacing all current public-key crypto with quantum-safe algorithms is a complex endeavour, for which Canada needs to prepare.[9] Some sources of this complexity include the internet's interconnected nature and transfer of data beyond geographical borders. Co-operation is key to achieve secure standards and to transition to these standards, and thus maintain security also in the future.

If Canada wants to stop worrying about the quantum threat, then it should explore co-operation for increased transparency. This is an inherently difficult goal to justify in the defence field because the reality of this transparency may seem counterintuitive at first. Yet, there are examples of this goal in practice, such as the NIST post-quantum standardization project which already relies on open communication and advice from the research community. Although ongoing, NIST's approach to transparency is a project to watch and could be seen as a collaborative opportunity for the FVEY to engage in and potentially consider in future decision-making.

Transparency would enable a faster and therefore more secure post-quantum standardization and transition process. This is also an opportunity for the FVEY to expand the parameters of information sharing by working towards the standardization of different algorithms. For example,

[9] Michele Mosca, "Is Canada 'Quantum Ready'? Securing Our Critical Infrastructure for an Age of Tech Disruption," CDA Institute, May 4, 2021. https://cdainstitute.ca/michele-mosca-is-canada-quantum-ready-securing-our-critical-infrastructure-for-an-age-of-tech-disruption/#.

while the U.S. focuses on standardizing basic crypto-algorithms, other states could focus on standardizing composite schemes that combine current algorithms such as RSA with quantum-secure ones. This would aim to preserve the security guarantees of well-established algorithms while adding security against quantum attackers. Moreover, many crypto-algorithms with advanced functionality need to be analyzed and standardized. There is room for states to make independent decisions on standardization, while contributing to collective security co-operation. This process should be transparent in decision-making so that other co-operating states could evaluate the decision. This could increase the efficiency of the process and reduce costs associated with a single state's standardization project.

It is important to recognize that other actors beyond states are involved in the post-quantum transition. Industry co-operation is an important collaborator because there is a continual need to evaluate critical applications and openly communicate findings; for example, following a step-by-step guide to assess the quantum risk.[10] As there are so many different algorithms that need to be analyzed and standardized, it is important to prioritize algorithms according to the industry's need. Depending on most urgent security applications identified by industry, governments and research bodies could help develop and standardize the critical algorithms accordingly. Transparency is needed from these actors to make the process work. This could take the form of open-access publications and open-source licence software libraries. These libraries are already an important part of making security through transparency, such as for example liboqs.[11]

Conclusion

It seems paradoxical to suggest that more transparency could be equated with increased security, yet something as complicated as the quantum threat needs a rethink of the usual logics of defence. Canada should rethink the security possibilities of QCs, and in the context of the quantum threats, there need to be tangible policy options based on best practices from allies. As other allies navigate this threat area and technology, Canada could identify a focus area through open collaboration with domestic expertise available in academia and industry. This way, Canada could actively address the quantum threat.

[10] Michele Mosca and John Mulholland, "A Methodology for Quantum Risk Assessment," Global Risk Institute, January 5, 2017. https://globalriskinstitute.org/publications/3423-2/.

[11] "Software for prototyping quantum-resistant cryptography, liboqs - Open Quantum Safe (openquantumsafe.org)"

About the Author

Dr. Nina Bindel *is a post-doctoral Fellow at the Institute for Quantum Computing (IQC) and the University of Waterloo. Dr. Nina Bindel researches how to maintain internet security in the future. This includes constructing cryptographic algorithms that are secure even in the presence of quantum attackers and finding weaknesses therein. She also has been the principal submitter of qTESLA, a quantum-secure digital signature scheme that had been submitted to NIST's post-quantum standardization effort and advanced to the second of three rounds. In addition, she is working with Kristen Csenkey to examine emerging technologies and their implications. Before joining IQC, she received her PhD from TU Darmstadt, Germany in 2018. In addition, Nina was a research visitor at the lattice program of the Simons Institute at UC-Berkeley in spring 2020 and interned at Microsoft Research, Redmond (U.S.), during the summer of 2019. Dr. Nina Bindel is an experienced researcher and speaker with 14 peer-reviewed publications, and nine invited talks that are well received and have been circulated by interested attendees on Twitter. A list of her publications and selected presentations can be found on her website.*

Kristen Csenkey *is a Fellow with the Canadian Global Affairs Institute (CGAI) and a PhD candidate at the Balsillie School of International Affairs in Waterloo. Her research focuses on the management of emerging technologies, innovation and cyber-governance in Canada. Kristen is also a fellow with the Defence and Security Foresight (DSF) Group and the North American and Arctic Defence and Security Network (NAADSN). She is a Women in International Security (WIIS) Emerging Thought Leader in Digital Security and was the 2020 Women in Defence and Security (WiDS)-CGAI Fellow. Kristen is the principal investigator of a Canadian Department of National Defence Mobilizing Insights in Defence and Security (MINDS) targeted engagement grant to examine emerging technologies with military applications. She has published widely on a variety of cyber-related topics, including on cyber-capacity building, innovation governance, technology procurement, continental defence and cyber-considerations for military operations.*

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.