

## Quantum-Safe Canada session at Quantum Days

2:15-3:30pm Thursday, January 14, 2021

**Roundtable participants:** Michele Mosca, Director, Quantum-Safe Canada (host and moderator); Gwen Beauchemin, CEO, Tillet Consulting and member of QSC Governing Board; Marc Brouillard, Acting CIO, Treasury Board Secretariat of Canada; Mike Brown, CTO, ISARA Corporation; Bruno Couillard, CEO, Crypto4A; Norbert Lütkenhaus, Professor of Quantum Communication, University of Waterloo; Keith Marquis, Manager, Office of the Superintendent of Financial Institutions Canada; Atefeh Mashatan, Director, Cybersecurity Research Lab, Ryerson University; Brian O'Higgins, Executive Fellow, Mistral Venture Partners, and member of QSC Governing Board, Gilles Piché, Director, Cyber Security Architecture and Assurance, Bank of Canada; John Scott, CEO, 2Keys Corporation / Interac; Sherry Shannon-Vanstone, CEO, Profound Impact Corporation; Bridget Walshe, Director General, Secure Solutions and Services, Canadian Centre for Cyber Security

- **Opening Remarks and Introduction to the Topic**

Michele Mosca opened the session by welcoming the audience and introducing the panellists for this moderated, 75-minute virtual roundtable. He noted that the plan is to walk through seven or so questions, each directed initially to specific roundtable participants. A report will be produced to capture and share the discussion.

Michele Mosca then walked through a short presentation deck that set out the basic elements of the quantum threat – that quantum computers will be able to break currently deployed public-key cryptography. He went on to summarize some of the latest views on the timing of this threat, and provide an overview of the known solutions. He closed by stressing that quantum cryptography lets us replace the existing cryptography base with something that is even better and more resilient.

- **Question 1: How big a deal would it be for our everyday lives if we don't mitigate the threat and hackers are able to break our public-key signatures and key agreement?**

**Bruno Couillard**, using the internet of things (IoT) as an example, noted that with lightly protected sensors the main problem will be leakage of sensitive – and potentially actionable – environmental, operational and personal data. Still, these sensors can be replaced relatively easily, whereas actuators (which do the 'thinking') will be installed with the understanding that they will be in use for 10 years or more.

**Mike Brown** added that root certificates, which systems rely on to authenticate senders, receivers and content of messages, all rely on public-key infrastructure (PKI), which is generally recognized as especially vulnerable to the quantum threat.

- **Question 2: If we don't get ahead of this transition to quantum-safe cryptography, might there be serious calls to control access to dual-use quantum technologies, especially quantum computing?**

## Quantum-Safe Canada session at Quantum Days

2:15-3:30pm Thursday, January 14, 2021

**Gwen Beauchemin** agreed that this is a serious possibility given the national-security ramifications if these technologies are allowed to get into the hands of our adversaries.

**Sherry Shannon-Vanstone** warned that such an approach, however attractive it may appear on the surface, is a bad idea because it would be very difficult to implement effectively – meaning that restricted technologies would still leak out to our adversaries while we would lose access to the beneficial aspects of the technologies.

- **Question 3: People outside of cryptography and security might wonder why it will take so long to replace the cryptography that is now in use. Are there parallels in past transitions?**

**Atefeh Mashatan** provided examples from her previous experience in the banking industry, which underwent protracted (and in some cases still ongoing) migrations from DES to Triple-DES, and from Triple-DES to AES. Even after awareness is in place, there is a very large number of installations in banking (and other sectors), and a plethora of upstream and downstream dependencies that must be considered before action can be taken. Furthermore, there is no roadmap, an insufficient supply of the necessary skills, and a heterogeneity among systems and installed cryptography bases.

**Mike Brown** added that even after implementation, things need to be ‘tuned’ following testing so as to ensure ‘backwards compatibility’ with older technologies that are still in use; this too can take time.

- **Question 4: It is clear that achieving quantum readiness calls for much more than a simple software update? Are there risks in delaying action, beyond not finishing the job in time to defend against quantum attack?**

**Bridget Walshe** points out that delay at the outset could result in rushing things at the end. Such approaches often result in a lack of the documentation needed by future users and technicians, a lack of necessary testing, and a failure to meet user demands. Furthermore, exploitable errors may be missed, and there may be a loss of interoperability with other systems. Planning to update should happen early, so that work can begin when standardized, certified products are available.

- **Question 5: Are federal government departments and agencies taking or considering quantum-readiness policy or regulatory steps?**

**Bridget Walshe** noted that the Canadian Centre for Cyber Security, and before that the Communication Security Establishment, have worked for decades to protect government systems and advise the private sector on how best to protect their own systems from cyber intrusions – now including the quantum threat.

**Marc Brouillard**, as Canada’s Acting Chief Information Officer, noted two significant recent trends: 1) the substantial increase in Canada’s ‘digital reliance’ during the pandemic, and 2) the related substantial increase in the amount of digital information

## Quantum-Safe Canada session at Quantum Days

2:15-3:30pm Thursday, January 14, 2021

that must be protected. Dealing with these threats calls for partnerships with industry, academia and standards groups. Among other things, his office has been working with Public Services and Procurement Canada to put in place a government procurement process that will encourage vendors to the Government of Canada to ensure their products are quantum-safe. This will involve suggestions and recommendations at first, followed by the introduction of regulations.

**Keith Marquis** from the Office of the Superintendent of Financial Institutions (OSFI) pointed out that OSFI takes a principles-based approach to regulation. Their recent public consultation paper, *Developing Financial Sector Resilience in a Digital World*, includes consideration of emerging threats such as the quantum threat. It is clear that financial institutions' technology operations and risk management must keep pace to ensure stability, and OSFI is now preparing its own expectations on cyber risk.

**Gilles Piché** notes that while the Bank of Canada is looking into how quantum technologies can help with some operations, his job is to look at and prepare for the quantum threat. Time is of the essence, and "the problem is not something you can just throw money at at the last minute." The sectoral engagement with the CFDIR Quantum-Readiness Working Group (QRWG) that QSC has been facilitating is very helpful. The underlying need is to protect public trust in the banking sector.

**John Scott** commented on the work of the CFDIR QRWG from the industry side of financial services. The Canadian Financial Industry Quantum Working Group had existed for some years, but it was the creation of the CFDIR QRWG that really sparked significant movement toward sector-wide quantum readiness.

- **Question 6: Is there a realistic opportunity for Canada to reap economic rewards by being a global leader in providing quantum-safe solutions and in implementing the necessary migration?**

**Brian O'Higgins** asserted that there is indeed an opportunity for Canada in this space. He recounted the "start-up story" of Entrust (which he co-founded) as a good example. Entrust built the world's first public-key infrastructure (PKI) for the Government of Canada, whose "stamp of approval" was enough to cause 50 other countries around the world to go with Entrust as the standard. He once again stressed the value of early and strong support from the federal government as a buyer of technology products (and not just a funder of research). The federal government may not realise how much global clout it has as a customer. We have many specific areas of leadership, but what it needed is a general 'root of trust' – and the global root of trust could be Canada. The US, China and Israel are viewed as non-starters for a variety of reasons, and the UK is distracted by post-Brexit realities.

**John Scott** stressed that with respect to defending our own systems from the quantum threat, there is a definite need for Canada to get going right away on making ourselves quantum-safe. With respect to cybersecurity offence (i.e., exporting our quantum-safe

## Quantum-Safe Canada session at Quantum Days

2:15-3:30pm Thursday, January 14, 2021

products and services abroad), we have the skills and the technology, so why couldn't we be global leaders?

**Sherry Vanstone** noted that we have already shown that we are the leader in cryptography – Certicom (and ECC) in addition to Entrust. “We have this global legacy. Why don't we build on it?”

- **Question 7: How about global leadership in research and commercialization – what are the gaps we need to address?**

**Norbert Lutkenhaus** pointed out that Canada provided original academic leadership in both post-quantum cryptography (PQC) and quantum key distribution (QKD – his area of concentration). QKD will continue to be a necessary backup for PQC, but Canada needs to focus more on commercialization as Japan, China and Europe are all ahead of us in QKD deployment.

**Atefeh Mashatan** noted that much changed in 2015 with the US National Security Agency and National Institute of Standards and Technology (NIST) decisions regarding the need for quantum-safe cryptography. It has been very encouraging to see the strong Canadian contributions to the subsequent NIST standard-setting exercise. However, that addresses just the technology; we also need to think about the people (skills) and processes needed to make us quantum ready. Unfortunately, we have lagged in these areas. She stressed that we need a “turnkey blueprint example” that ties everything together into a single coherent package.

- **Closing Remarks**

The moderator invited each speaker to offer any final thoughts that they wished to share. **Mike Brown** noted the recent formation of two significant associations that bring together significant players in the Canadian quantum-safe space – Quantum-Safe Canada (QSC) and Quantum Industry Canada. **Gwen Beauchemin** stressed that there is “an endless market” where we should play. **Brian O'Higgins** acknowledged the great work from QSC in bringing people together to have this sort of discussion. **Atefeh Mashatan** made the point that other sectors need working groups like the banking industry has. **Bridget Walshe** said that we are nearing an “inflection point”, so we must be ready and information must be available. **Marc Brouillard** noted that it's important to look at the positive side. **Keith Marquis** said that we must focus on maintaining trust in the stability of the financial system. **Gilles Piché** made the point that it's not time to panic, but the time for serious planning. **John Scott** noted that executive-level messaging must be improved. **Norbert Lutkenhaus** stressed that we must keep up the momentum.

Michele Mosca closed the session by thanking the speakers for so ably showcasing the full vision, importance and depth of Quantum-Safe Canada – and, more importantly, helping raise awareness of the very significant challenges related to the ability of quantum computers to render our existing cryptography base vulnerable to attack.