Adopting Quantum-Safe Technologies to Address the Urgency of Securing our Digital Future

📅 Date: Thursday, May 8th, 2025; ⏰ Time: 8:40am-13:00pm, Room NI 4010, Carleton University

📍 Registration: https://sprott.carleton.ca/cu-event/adopting-quantum-safe-technologies-to-address-the-urgency-of-securing-our-digital-future/

The unprecedented advances of Quantum Computing (QC) come with a promise to transform industries and bring in revolutionary applications spanning across drug development, new materials, supply chain optimization, finance, and cybersecurity. QC promises performance advantages that are impossible to achieve with classical computing. However, these performance advantages come with a serious warning. According to the Canadian Centre for Cyber Security (CCSC, Feb. 2025) "*Your organization's cyber security is at risk as quantum computing advances. Although quantum computers cannot break cryptography now, a sufficiently powerful device could be available as early as the 2030s*."[1]

2030 is the deadline defined by cybersecurity professionals. It is a point of time when emerging technologies like AI, QC, and the increasing interconnectedness of devices will significantly exacerbate cyber threats, requiring a major shift in security strategies. This includes concerns about potential attacks on critical infrastructure like power grids and self-driving cars, but also on highly competitive small and large businesses, as well as concerns about the growing need for skilled cybersecurity professionals to manage these evolving risks.

The Canadian Centre for Cyber Security recommends migrating to standardized Post-Quantum Cryptography (PQC) solutions as the best option for organizations to achieve quantum safety. There are alternative quantum-safe solutions such as Quantum Key Distribution (QKD) and Symmetric Key Establishment (SKE), that could provide further safety measures when combined with PQC. "However, these alternatives can significantly increase operational complexity and implementation costs. Furthermore, these alternatives lack security accreditation options based on recognized standards" (CCSC).

The problem is clear. The deadline is fast approaching. Solutions exist and are commercially available. More importantly, Ottawa happens to be at forefront of the development of such solutions.

---

[1] https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

What are the factors that can accelerate the adoption of quantum-safe solutions to enable our digital future?

The event will focus on discussing the factors that could accelerate the adoption of quantum-safe technologies such as Post-Quantum Cryptography (PQC). It will bring together domain experts from both the supply and demand side to discuss how PQC and other quantum-safe technologies can be used to secure businesses and society.

Key messages of the renowned team of Keynote Speakers

- Quantum-safe technologies are a fundamental part of a broader vision for a radically advanced digital world enabled through quantum capabilities
- Advancing quantum technology for the betterment of society cannot be achieved without assuring the quantum-readiness of our digital business and social environments
- The urgency to act unites the QC, cybersecurity, business and innovation communities in accelerating the adoption of quantum safe technologies

The urgency to act requires the engagement of a variety of key stakeholders such as regulatory and standard bodies, vendors and users, the broader business and innovation communities, in making adoption happen.

Tentative Schedule (Speakers' bios provide details on their organizations and topics)

08:40-08:45   **Opening**: Stoyan Tanev (*TIM, Sprott, Carleton*), Bruno Couillard (*Crypto4A*)

08:45-8:55   **Welcome**: Sandra Crocker, Assoc. VP, Strategic Initiatives and Operations, Carleton University

08:55-9:00   **Welcome**: Joanne Hyland, ISPIM Fellow & President of the *rInnovation Group*

09:00-09:20   Bruno Couillard, *Crypto4A*

09:20-09:40   Martin Charbonneau, *Nokia*

09:40-10:00   Philip Lafrance, *ISARA Corporation*

10:00-10:20   Tony Rosati, *evolutionQ*

10:20-10:40   Rajat Ghosh, *National Quantum Strategy*

10:40-11:00   Nicholas Scott, *Canadian Center for Cyber Security*

11:00-11:20   **Coffee Break**

11:20-11:40   Koray Karabina, *National Research Council of Canada*

11:40-12:00   Martin Laforest, *Quantacet*

12:00-12:20   David Hudson, *TIM, Sprott School of Business, Carleton University*

12:20-13:00   **Panel discussion** moderated by David Hudson

Keynote Speakers' Bios

Martin Charbonneau is the Head of Quantum-Safe Networks in the Network Infrastructure Business Group at Nokia. Martin Charbonneau pioneered the commercialization of Quantum-Safe networking solutions at Nokia. His focus on Quantum-era cybersecurity fosters global collaborations with research and technology leaders in the quantum cryptography sphere, aiming to craft solutions for a dynamic security landscape. Martin partners with critical infrastructure organizations and enterprises in emphasizing the urgency of securing network infrastructure through comprehensive defense-in-depth strategies. His mission is to ensure an enduring trust in our data and digital communication infrastructures. This commitment is rooted in a clear understanding of the transformative power of Quantum technologies and the necessity to protect our digital future. Martin was raised and educated in Canada and attended the Canadian Royal Military College (RMC, St-Jean, Canada). https://www.nokia.com/people/martin-charbonneau/

Bruno Couillard, CEO & Co-Founder, www.crypto4a.com. Bruno is co-founder of Crypto4A Technologies Inc., developing crypto-agile and post-quantum cybersecurity products. These products are designed for deploying, managing, and protecting digital keys, workloads, and information across diverse environments. https://crypto4a.com/teams/bruno-couillard/

Rajat Ghosh, Manager, National Quantum Strategy Secretariat at Innovation, Science and Economic Development Canada (ISED). Dr. Rajat Ghosh received his Ph.D. in experimental quantum physics from Princeton University in 2009 where he helped pioneer advances in quantum sensors including for use in navigation, remote munitions detection, tests of fundamental physics and brain imaging, resulting in two successful spin-off companies. From 2010 to 2015, Dr. Ghosh worked at the University of Pennsylvania's Department of Radiology where he developed pre-clinical quantum technologies to support the imaging and treatment of cancer and various pulmonary conditions. From 2010 to 2017, Dr. Ghosh led private sector-academic partnerships to advance medical imaging, gave invited talks at universities including Harvard and Berkeley and provided advice to several Fortune 500 companies and US government agencies related to emerging technologies. In 2018, Dr. Ghosh joined Innovation, Science and Development Canada as a Senior Policy Advisor where he has helped develop, coordinate and implement Canada's National Quantum Strategy. https://www.linkedin.com/in/rajat-ghosh-07956492/?originalSubdomain=ca

Title: *Canada's Quantum communications and post-quantum cryptography roadmap*. The talk will summarize stakeholder consultations that describe the opportunities, challenges, and supports needed to grow the vibrant quantum communications and PQC sector in Canada. The talk will also highlight potential actions to support the sector from the federal and provincial governments, along with academia and industry.

David Hudson, Adjunct Professor, TIM Program, Sprott School of Business, and ICT Advisor at Innovation, Science and Economic Development Canada, Ottawa, Ontario, Canada. David is a capable technology executive with over 30 years total experience in industry. He has a PhD in Management and substantial experience in the management new and emerging technologies. https://ca.linkedin.com/in/dvhudson

The tile of David's talk is *Value Propositions for Post Quantum Cryptography*. PQC appears to be an initial wave that is part of a larger quantum technology sea change. The technology management field provides useful theories and frameworks for understanding disruptive technology change and why certain groups will buy in before others. This presentation will discuss research into possible value propositions for PQC.

Koray Karabina leads the Cryptography and Quantum Computing Team at NRC, Canada. He is also an Adjunct Professor at the University of Waterloo. Koray Karabina's research focuses on the design of cryptographic algorithms and protocols. His key interests are in post-quantum cryptography, secure biometrics, and the interplay between machine learning and cryptography. https://www.linkedin.com/in/koray-karabina/?originalSubdomain=ca

Martin Laforest holds a PhD in quantum computing from the University of Waterloo's Institute for Quantum Computing (IQC). For 9 years, he led the quantum outreach efforts at IQC, interacting with government, industry, the media, and the public, on the impact of quantum technologies. He then joined ISARA Corporation, a quantum-safe cybersecurity startup, and then launched Quantacet. https://www.quantacet.com/en/team/

Philip Lafrance, CISSP, Standards Manager at ISARA Corporation, Kitchener, Ontario, Canada. Philip is Information Security professional holding a master's degree in mathematics and a CISSP certification. He is the Interim Lead for the Quantum Industry Canada's Standards Working Group, specializing in quantum-safe migration strategies, cryptographic discovery, risk management, and zero trust architectures. https://www.linkedin.com/in/philip-lafrance/

The title of Philip's talk is *The Great PQC Transition: Lights, Cameras, Then Action*, focusing on the paramount importance of cryptography for the daily operations of every modern organization. Unfortunately, organizations tend to take an "out of sight, out of mind" approach to their cryptographic solutions. With the coming arrival of Cryptographically Relevant Quantum Computers, this approach has become unsustainable and dangerous. It is important for organizations to assess their cryptographic posture, of quantifying their cryptographic risk, and the criticality of the urgency of transitioning to PQC.

Tony Rosati, Vice President of Product Strategy and Business Development at *evolutionQ*, leading the deployment of cutting-edge quantum-safe technologies. A distinguished fellow of the Center for Applied Cryptographic Research (CACR) at the University of Waterloo, he brings extensive expertise in applied cryptography and telecommunications to the quantum security landscape. Tony Rosati will provide an overview of the state of the post quantum transition, including Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD) and Symmetric Key Infrastructure (SKI), standards, industry initiatives, addressing current progress and hurdles to overcome. https://www.linkedin.com/in/tonyrosati/?originalSubdomain=ca

Nicholas Scott, Manager, Cryptographic Engagement and Standards, Canadian Centre for Cyber Security (CCCS). Nicholas Scott is a seasoned professional with over 20 years of experience in cyber security practices and development. He currently serves as the Manager of Cryptographic Engagement and Standards at the Canadian Centre for Cyber Security (CCCS). Nick has been instrumental in advancing cyber security initiatives within the Communications Security Establishment, leveraging his extensive expertise to enhance national security.

Stoyan Tanev, Associate Professor, Technology Innovation Management Program, Sprott School of Business, Carleton University. Dr. Tanev's research and teaching interests focus on digital innovation and entrepreneurship, artificial intelligence and value creation, design thinking and digital transformation. Stoyan is part of the leadership of the ISPIM Digital Disruption and Transformation Special Interest Group: https://www.ispim-innovation.com/sig-digital-disruption.

Participating Organizations

Crypto4A Technologies: World leader in developing products and solutions that enable the cryptographic agility, mobility, and scalability needed by enterprises and government agencies to secure their digital assets and infrastructure. https://crypto4a.com/

Nokia: Delivers the key ingredients of Quantum-Safe Networks (QSN) that can adapt to the needs of every business, building confidence in securely scaling Quantum deployments inline with globally emerging business trends. https://www.nokia.com/

ISARA Corporation: A security solutions company specializing in cryptographic risk management and in creating crypto-agile and quantum-safe security solutions for today's information technology ecosystems. https://www.isara.com/

evolutionQ: Provides scalable defense-in-depth with PQC and QKD software solutions for resilience and quantum-safe security. It offers quantum-safe cybersecurity products to help clients deploy and manage quantum-safe technologies across their networks. https://www.evolutionq.com/

Canada's National Quantum Strategy (NQS) Secretariat, Innovation, Science and Economic Development Canada (ISED): The National Quantum Strategy sets out Canada's key missions to ensure it stays on the path of quantum innovation and leadership: https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy

Canadian Centre for Cyber Security: the Cyber Centre is part of the Communications Security Establishment Canada. It is the single unified source of expert advice, guidance, services and support on cyber security for Canadians. https://www.cyber.gc.ca/en

National Research Council of Canada: The NRC partners with Canadian industry to take research impacts from the lab to the marketplace, where people can experience the benefits. This market-driven focus delivers innovation faster, enhances people's lives and addresses some of the world's most pressing problems. https://nrc.canada.ca/en/corporate/about-nrc

Quantacet: The first and only VC fund based in Quebec focused on the global quantum technology market by investing early-on in ambitious quantum startups. https://www.quantacet.com/en/

Technology Innovation Management (TIM) Program, Sprott School of Business, Carleton University: A set of Master level program pathways in the Sprott School of Business at Carleton University's focusing on empowering highly qualified personnel to foster the adoption of quantum-safe technologies in Canada. https://carleton.ca/tim/

ISPIM: The International Society for Professional Innovation Management - is a community of members from research, industry, consulting and the public sector, all sharing a passion for innovation management. ISPIM is the oldest, largest and most active truly global innovation network. It hosts the Digital Disruption & Transformation Special Interest Group whose mission is to provide a platform for scholars and practitioners interested in the digital phenomena, particularly their transformative and disruptive nature, to discuss the opportunities, assess threats and implications to how we understand and practice innovation management today. https://www.ispim-innovation.com/sig-digital-disruption