Request for Information (RFI):
Quantum Information Science and the Needs of U.S. Industry

Quantum-Safe Cryptography

Docket Number: **150218152–5152–01**

Submission Date: **May 8, 2015**

Organization Name:	Quantum-Safe Cryptography Group, Institute for Quantum Computing (IQC), University of Waterloo
Organization Address:	200 University Avenue West Waterloo, Ontario N2L 3G1 Canada
Document Title:	Request for Information (RFI): Quantum Information Science and the Needs of U.S. Industry Quantum-Safe Cryptography

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1 Overview

The Quantum-Safe Cryptography Group of the Institute for Quantum Computing (IQC), University of Waterloo, is pleased to submit this note on quantum-safe cryptography in response to the request for information (RFI) on Quantum Information Science and the Needs of U.S. Industry. This white paper is structured to address the questions provided in Docket No. 150218152-5152-01.

1.2 About the Institute for Quantum Computing (IQC)

The Institute for Quantum Computing (IQC), a research institution located at the University of Waterloo, seeks to aggressively explore and advance the application of quantum mechanical systems to a vast array of relevant information processing techniques.

The University of Waterloo initiated a quantum computing group led by Prof. Michele Mosca within its Centre for Applied Cryptographic Research in 1999. Shortly after, with the vision and support of founder and former co-CEO of BlackBerry Mike Lazaridis and other leaders in Waterloo, this group was the beginning of a multi-disciplinary IQC that was officially established in October 2002. The Institute is devoted to interdisciplinary research bridging foundational issues to technology development through both theoretical and experimental investigations. The main application areas of the research are quantum computing, communication and sensors. IQC is strongly involved in the standardization of quantum key distribution systems within the European Telecommunications Standards Institute (ETSI), as well as the standardization of quantum-safe cryptography (including both "post-quantum cryptography" and QKD) through the newly founded ETSI ISG on Quantum-Safe Cryptography. On a related front, IQC is a member of the Updating Quantum Cryptography team that puts together reports and roadmaps for the Japanese Government regarding QKD, and is also a representative for QKD in the U.S. Quantum Information Meeting in advising U.S. funding agencies.

Figure 1 – The Institute for Quantum Computing (IQC) at the University of Waterloo

1.3 Point-of-Contact

Inquiries related to this note should be directed to the following point-of-contact:

Dr. Michele Mosca
Institute for Quantum Computing
University of Waterloo
200 University Avenue West
Waterloo, Ontario
N2L 3G1 Canada
michele.mosca@uwaterloo.ca
519-888-4567 x37484

2. OPPORTUNITIES

A promising area of pre-competitive QIS research and development is quantum-safe cryptography, which has two main thrusts. The first is "post-quantum" cryptography, which is comprised of conventional ciphers believed to be resistant to quantum attacks, and the second is quantum cryptography, which uses some quantum technology but not large-scale quantum computers. Pre-competitive research is required on the following:

- Quantum algorithms, in order to assess the strength of these new crypto primitives and to pick proper key lengths
- New crypto primitives that can be efficiently and robustly implemented while being resistant to conventional and quantum attacks
- Tools for achieving global networks capable of establishing quantum key distribution (QKD) across long distances through untrusted infrastructure (e.g. quantum repeaters, satellite-based QKD, etc.)
- Methods and standards for testing and certifying the behavior of quantum apparatus
- Tools for the extraction of quantum keys in resource constrained settings
- Large-scale quantum-safe systems that include both post-quantum and quantum cryptography (e.g. security models and proofs that can handle both kinds of tools)
- Large-scale full-fledged quantum computers
- Software tools for compiling quantum programs and controlling quantum systems
- Large-scale quantum communication networks, with broad ranges of applications such as distributed quantum computing, cloud quantum computing, etc.

Quantum-safe cryptography is one of the highest priorities for investment because it must be in place before large-scale quantum computing services are available. Since it takes decades to develop and deploy such a new cryptographic infrastructure – even without quantum cryptography – this priority needs to be addressed as soon as possible. Quantum cryptography should be designed into future systems alongside post-quantum cryptography, thereby offering a more robust and reliable cyber-security infrastructure.

Quantum cryptography is clearly a significant emerging frontier, driven by an evolving threat that could compromise the current public key cryptographic systems upon which much of the information and communications technology (ICT) infrastructure depends. It is cryptography that allows us to leverage a relatively small amount of physical security and trust in order to be able to use the wider untrusted ICT infrastructure in a practical manner with reasonable assurances of privacy and security. Reliable cryptography is absolutely fundamental to national security and economic prosperity.

Encryption technologies make use of cryptographic keys that must be distributed to the parties involved in some data security requirement (e.g. private communication of data, authentication of identities, secure storage of data, etc.). The privacy of these keys is essential to the security of the cryptographic operations that follow, and ultimately to the security of the underlying data.

Historically, cryptographic keys were distributed manually, by trusted couriers. This technique of manually distributing cryptographic keys in advance is typically referred to as pre-placed key (PPK). Unfortunately, PPK is too inefficient to meet the real-time demands of today's ICT infrastructure. A widely used method for establishing cryptographic keys is through the use of public-key cryptography (PKC). The security of PKC is based on the assumption that it is exceedingly difficult to performing certain mathematical operations (e.g. factoring large numbers) even with the most powerful classical computers available today. There is no known proof for this assumption, however (and indeed has been disproven by the advent of quantum computing). Security based on such unproven assumptions about the difficulty of performing certain computational tasks is referred to as computational security.

Due to the fact the security of PKC rests on computational security, a sudden or unexpected algorithmic innovation could immediately comprise any current security systems that use PKC. Over twenty years ago, Peter Shor discovered that quantum computers will break factoring and discrete-logarithm based cryptographic systems (which account for nearly all deployed PKC). Fortunately, there were no quantum computers at the time. However, based on the tremendous progress in quantum computing technologies and fault-tolerant quantum error correction in the past 20 years, there is a significant likelihood of large-scale quantum computers within the next 10-20 years. When this happens, most current public key encryption methods will be broken.

These public key cryptographic systems are not "future-proof". Many organizations need to secure data over the long-term (in some cases for decades). An unexpected innovation in algorithms or the advent of practical quantum computers would not only compromise future data security but would also make historical records vulnerable. This means that if quantum computers become a reality in 20 years, data that requires 20 years of security will *now* need an alternative to current PKC systems. Given that the task of replacing all the PKC elements in a cryptographic infrastructure is expected to take many years, we are already behind the curve in responding to the quantum computing threat.

Systems based on quantum cryptography have the opportunity to offer "future-proof" data security in terms of resistance to mathematical cryptanalysis. Since quantum cryptography relies upon fundamental laws of science rather than mathematical assumptions, it will never be threatened by new algorithms or more powerful computers. Quantum key distribution (QKD), which was co-invented by Gilles Brassard of Université de Montréal and Charles H. Bennett of IBM, will be a valuable part of future information technologies. This protocol transmits quantum states of light and is secure because these photons behave according to the laws of quantum mechanics and cannot be tapped, copied or measured without leaving tell-tale signs of observation. The system provides peace of mind that any eavesdropping can be immediately detected and addressed.

Quantum key distribution is a present day reality. A number of companies are currently selling commercial QKD systems, and several other firms offer related products and services. Terrestrial QKD networks using fiber optic cables or free-space atmospheric transmission are in operation today for both research and niche commercial applications such as secure bank transactions and data transfers.

Due to some fundamental physical constraints, a complementary solution would be required to cover distances beyond a few hundred kilometers. Light signals inevitably attenuate as they are transmitted through fiber optic cables, and conventional signal amplifiers cannot be used because they would compromise the quantum mechanical phenomena upon which QKD depends for the detection of eavesdropping. Free-space atmospheric QKD links are limited to line-of-sight, subject to local geographical constraints and ultimately the curvature of the Earth. With current technology, one can offer long-distance QKD services using satellites as complementary trusted nodes bridging the distance between geographically dispersed QKD ground networks, for example, between cities or continents.

Information security is a societal concern that can be supported by quantum communications. People expect continued advances in computer and communication technology and are willing to support investments in such ventures, particularly if they provide long-term value to improve health, safety and security. Industrial spin-offs in new data services and the security of private information will catalyze social and economic benefits. As people increasingly use mobile devices and Internet technology, and as their personal data becomes more widely disseminated in cyberspace, the need for privacy and protection will become a main focus of communications.

3. MARKET AREAS AND APPLICATIONS

In terms of quantum-safe cryptography applications for the cyber security market, research into quantum algorithms is needed to know which conventional ciphers will be quantum-safe before they are deployed wide-scale. This should happen before the emergence of large-scale practical quantum computers. Quantum communications networks would provide robust cryptography for long-term security and critical applications that warrant higher grade security.

IQC has also conducted an internal *Quantum Cryptography Market Study and Business Opportunity Assessment*,[1] a copy of which could be provided to NIST upon request.

4. BARRIERS

In the field of quantum-safe cryptography (both "post-quantum" and quantum cryptography), a significant barrier to advancement is the challenge of transitioning to new cryptographic tools. There is a perceived lack of urgency to quantum-proof, not appreciating that some information needs to remain secure for many years and will be compromised when quantum computers emerge, and that it takes many years to quantum-proof. It is often asked if quantum-proofing is really something that needs to be a concern at the present time. This depends[2] on three variables x, y and z:

- x is the number of years that cryptography must remain unbroken, i.e. how long are you supposed to protect health information, or national security information, or trade secrets?

[1] Jennewein, T., Choi, E., *Quantum Cryptography: 2014 Market Study and Business Opportunities Assessment*, Institute for Quantum Computing, University of Waterloo, IQC-QPL-R-1403001, Rev. C, 9 July 2014.

[2] M.Mosca, G. Lenhart, M. Pecen (editors), *e-proceedings of 1st Quantum-Safe-Crypto Workshop*, Sophia Antipolis, Sep 26-27, 2013.
http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/e-proceedings_Crypto_2013.pdf

- *y* is the number of years it will likely take to replace the current system with one that is quantum-safe or not based on unproven assumptions of mathematical complexity
- *z* is the number of years it will take to break the current encryption tools, using quantum computers or otherwise.

If $x + y > z$, then there is a problem right now and immediate action needs to be taken. This means that for the latter part of those *y* years, we will have to either stop doing business or continue to use the current tools with the knowledge that they will be compromised in less than x years. Neither of these are desirable options and near-term alternatives are essential, if only to protect against unexpected algorithmic advances. These alternatives should also be quantum-safe in order to provide protection against the imminent threat posed by quantum computers.

There are many technological and scientific challenges to developing and deploying quantum-safe cyber tools, but perhaps the biggest barriers are the social or business challenges of addressing a threat that is not currently present, despite the clear logical case that immediate action should be taken in order to be ready before the threat is real.

The information security requirements of many organizations are driven by regulation and compliance, so revising regulatory frameworks would be one way to encourage network security and encryption stakeholders to take active steps in implementing next-generation cryptosystems. The establishment of standards and procedures for certification will be an important driver for the widespread acceptance of quantum cryptography. Policy decisions requiring a quantum-proofing plan or roadmap to be in place for both governments and industry, and investments in R&D, would be other possible drivers.

5. WORKFORCE NEEDS

A lack of a qualified workforce is one of the greatest barriers to advancing important near-term and future applications of quantum information science. Knowledge of both classical and quantum cryptography, as well as higher level cyber security and global standards and quantum technologies more generally, are required in addition to a basic understand of what quantum technologies can do today and what they will be able to do in the medium and long-term. The quantum workforce is relatively weak with regards to having commercially focused workers that drive technology adoption and application to demonstrate early adopter benefits in their respective market areas and application verticals.

Funded through a Collaborative Research and Training Experience (CREATE) grant from the Natural Sciences and Engineering Research Council of Canada (NSERC), the IQC CryptoWorks21 (cryptoworks21.uwaterloo.ca) training program aims to build the workforce for the quantum-safe cryptographic infrastructure of the 21st century. It is a collaborative program led by IQC with colleagues from University of Calgary and Université de Montréal. CryptoWorks21 has a network of partners and collaborators in research centers worldwide focusing on quantum and conventional cryptography and quantum information science. The network provides a collection of expertise, mentorship and training opportunities and experimental facilities both within Canada and internationally. CryptoWorks21 encourages graduate students and postdoctoral fellows to expand their technical and professional skills through a series of workshops and courses. This innovative program out of IQC develops QIS experts with the ability to connect cutting-edge research to commercial innovation and bridge the gap between academia and industry.