Quantum-Safe Cryptography

Phong Q. Nguyen[1]

There has been significant investment in building a universal quantum computer for the past few years. Although the exact power of a quantum computer has yet to be determined, we already know that its impact on cryptography would be dramatic: Shor's 1994 breakthrough results implied that a quantum computer would solve integer factoring and discrete logarithms in polynomial time, thereby breaking RSA and elliptic-curve cryptography, which are the only public-key cryptosystems currently deployed to secure the Internet. This threat is now taken seriously: in early 2016, the NIST announced an open international competition for post-quantum public-key cryptography standards, i.e. algorithms resistant to quantum computers, with proposals due by late 2017.

In the past few years, there has been significant investment in quantum technologies, from both the industry and governments. In 2013, the UK Chancellor G. Osborne announced a £270 million investment into quantum technologies. On the invitation of Mr. G. Oettinger, the EU Commissioner for the Digital Economy and Society and Mr. H. Kamp, Minister of Economic Affairs in The Netherlands, a European team issued in May 2016, a "Quantum Manifesto" to formulate a common strategy for Europe to stay at the front of the second Quantum Revolution. The Quantum Manifesto called upon Member States and the European Commission to launch a €1 billion Flagship-scale Initiative in Quantum Technology, preparing for a start in 2018 within the European H2020 research and innovation framework programme. It was endorsed by a broad community of industries, research institutes and scientists in Europe. Of particular interest was the construction of a universal quantum computer. On the industry side, major companies such as Google, IBM, Microsoft, Intel and Alibaba have announced quantum computing projects. For instance, Google and NASA jointly created a Quantum Artificial Intelligence Lab in 2013, where they acquired the D-Wave Two computer, a very special type of quantum computer which was not universal. Very recently, IBM released in May 2016, a quantum computing platform, which allowed users to run algorithms and experiments on IBM's quantum processor, currently composed of five superconducting qubits and housed at the IBM T.J. Watson Research Center in New York.

A universal quantum computer is fundamentally different from a classical computer. A classical computer works with n-bit registers, which are elements of {0,1}n. On the other hand, a quantum computer works with n-qubit registers, which can be viewed as unit vectors in a 2n-dimensional complex vector space. Determining exactly which problems can be solved efficiently with a quantum computer is a major open problem. However, we already know several problems for which there is a quantum algorithm which is much faster (often, exponentially faster) than the best classical algorithms known. The most famous example is Shor's algorithm, which can solve in quantum polynomial time, the following cryptanalytic problems: integer factoring (finding the prime factors of a given number) and discrete logarithms. For integer factoring, the best classical algorithms known have subexponential complexity, whereas the best discrete logarithm algorithms known in the general case run in exponential time. These two problems are very important, because the security of public-key cryptosystems deployed to secure the Internet depends on their hardness. Public-key cryptography is a special type of cryptography invented by Diffie and Hellman in 1976, for which they received the Turing award in 2016. It allows certain keys to be disclosed, like the encryption key or the signature-verification key and is used to authentify applications downloaded on smartphones and to encrypt credit card numbers.

[1] JFLI,Dept. of Computer Science, Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-Mu, Tokyo 113-8656, Japan
*Corresponding author (Phong Q. Nguyen, e-mail: Phong.Nguyen@inria.fr)

Although no large-scale universal quantum computer has been built yet, post-quantum or quantum-safe cryptography has emerged as an important concern for the community in the past few months.In August 2015, the NSA announced its upcoming transition to quantum-resistant algorithms. In February 2016, the NIST announced an open international competition for post-quantum public-key cryptography standards, with proposals due by late 2017. Currently, there are four main proposals for quantum-safe public-key cryptography: hash-based cryptography, multivariate cryptography, coding-based cryptography and lattice-based cryptography.

We will study quantum-safe cryptography by developing discussions between two communities, cryptanalysts and experts in quantum complexity, across three countries: France, Singapore and Japan. We want to better understand the impact of quantum computers on cryptography, including algorithmic assumptions and security models. In particular, we hope to find new applications of quantum algorithms to cryptanalysis, possibly designing new quantum algorithms.

Our cooperation between France, Singapore and Japan will build upon the CNRS network in Asia: it will involve two international mixed units (UMI), namely Majulab (UMI 3654) in Singapore and JFLI (UMI 3527) in Japan, which are both connected to local organisations such as the Center for Quantum Technologies (CQT) and the University of Tokyo. It will also involve at least two French teams: the Cryptography team of the University of Rennes, and the Algorithms and Complexity team of IRIF (CNRS UMR 8243).

REFERENCES

P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of FOCS 1994: 124-134

NIST. Report on Post-Quantum Cryptography, Feb. 2016: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf

de Touzalin, C. Marcus, F. Heijman, I. Cirac, R. Murray and T. Calarco, The Quantum Manifesto, May 2016.