Cybersecurity in an era with quantum computers: will we be ready?

Michele Mosca*

Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario , Canada

Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

Canadian Institute for Advanced Research, Toronto, Ontario, Canada

1 The Problem

Cyber technologies are becoming an increasingly important part of all facets of our lives. Consequently, cybersecurity is a fundamental and growing part of what it means for us to be safe. One of the most fundamental pillars of cybersecurity is cryptography. Most of the cryptography tools we use today rely on computational assumptions, such as the hardness of factoring 2048 bit numbers. These computational problems are sometimes broken (e.g. [Tut00], [BFMV84], [FMS01], [WY05]) by algorithmic advances or increased computing power.

Two decades ago, we learned that the quantum paradigm implies that essentially all the deployed public key cryptography will be completely broken by a quantum computer [Sho94] and that brute force attacks of symmetric ciphers can also be sped up by roughly a quadratic factor [Gro96, BBHT98].

Most new paradigms are not initially greeted with great acceptance, as described nicely in the Max Planck quote [Kuh70]: "A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it." There has been much skepticism about the prospect of a large scale quantum computer in the forseeable future (or ever) capable of implementing Shor's algorithms or quantum searching. People naturally ask if they can continue to delay taking action, since there are many other urgent and serious matters at hand. Whether one can continue to delay roughly depends on three questions.

- Firstly, how long do you need your cryptographic keys to be remain secure? Denote this number by x, the *security shelf-life*. We may have $x = 0$ years for applications requiring only real-time security. Or maybe $x = 10, 20, 100$ years when protecting your personal health information, trade secrets, or national security information. The value of x is in general a personal or business or policy decision.
- Next, how long will it take to deploy a set of tools that are quantum-safe? Denote this number by y, the *migration time*. For example, we may have $y = 0$ years if this is simply a matter of deploying an auto-update that replaces AES-128 with AES-256 within a system fully controlled by a single vendor. However, we may have $y \geq 15$ years if it involves a relatively untested public-key encryption method that has to be adapted for a constrained environment with many players who must agree on a standard.
- Lastly, how long will it be before a quantum computer, or some other method, breaks the currently deployed public-key cryptography tools? Let z denote this number, the *collapse time.*

If $x + y > z$, we have a serious problem today [Mos13] , since information protected by quantum-vulnerable tools at the end of the next y years can be broken by quantum attacks in less than x years from then.

So what is z? In 2011, colleagues at IBM [SDCTK11] stated "Rapid improvements in experimental quantum hardware suggest that a threshold for the design and the construction of fault-tolerant systems may be reached in the next five years". Colleagues at Yale [DS13] nicely laid out seven stages to building a large-scale quantum computer, and report that several implementations, including superconducting qubits, have reached stage 3 and are working on stage 4. Impressive developments toward reaching stage 4 continue

[*] mmosca@uwaterloo.ca

Supported by NSERC, CIFAR, ORF, CFI and ONR. IQC and Perimeter Institute are supported in part by the Government of Canada and the Province of Ontario.

worldwide (e.g. [CMS+15] [RPH+15] [KBF+15]). The last 3 stages will involve an intense focused engineering effort to scale fault-tolerant designs of quantum computing systems. While it is hard to predict how long these final stages will take, there is no reason for cybersecurity experts to be confident that it will take much more than a decade or so. [1]

At present, as I also stated at NIST earlier this year [NIST15], I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031.

This estimate roughly follows from projections of some key values, such as:

- When will we reach the design of a fault-tolerant scalable qubit? For example, IARPA [IARPA15] have recently issued a broad agency announcement for proposals to build "a logical qubit from a number of imperfect physical qubits by combining high-fidelity multi-qubit operations with extensible integration" with a target end date in 2021.

- How many physical qubits will we need to break RSA-2048? This depends on a number of issues, including the efficiency of fault-tolerant error correcting codes, the physical error models and error rates of the physical quantum computer, optimizations in quantum factoring algorithms, and the efficiency of the synthesis of factoring algorithms into fault-tolerant gates. Current estimates range from tens of millions to a billion physical qubits.

- How long will it take to scale the scalable design to the size sufficient to break RSA-2048? At some point, we can expect some sort of Moore's Law scaling, with new tools and methods to allow further scaling being developed in a manner similar to what has happened with conventional computing technologies. However, before we reach this point, the rate of scaling may be hard to predict. Some of the required tools will already be available thanks to decades of scaling of conventional computing technologies. And some of the required tools are being developed in anticipation of the need to scale.

On a related note, very recently, the NSA has announced preliminary plans for transitioning to quantum resistant algorithms [NSA15].

2 The solutions

There are two complementary families of possible solutions.

One family of solutions is sometimes known as post-quantum cryptography, and refers to conventional ciphers based on mathematical problems other than factoring and discrete logarithms, and that we believe are secure against quantum attack. These solutions have the convenience of working on conventional hardware. With these solutions we are still in the situation of computational security based on the hypothesized hardness of some problem.

Another family of solutions is known as quantum cryptography. A downside is that one needs a quantum channel – a means for sending quantum bits between locations. While in the short term, such quantum channels are available from point to point over relatively short distances, in the medium and long term satellite quantum communication and quantum repeaters will enable global distance QKD. A big advantage is that there are no computational assumptions.

It is very important to emphasize that the cryptographic ecosystem is strongest if and when both families of solutions are available. For example, some users will benefit from "good enough" security at lower cost, while others will appreciate a highly reliable method for providing long-term confidentiality. Furthermore, together they can achieve security tools with useful properties that can cannot be achieved by either family of solutions on its own. For example [IM12], one can use post-quantum signatures based on hash-functions together with QKD-based key establishment in order to obtain, in a public-key setting, cryptographic keys

[1] It is important, for the purposes of dealing with the quantum threat to cybersecurity, to distinguish progress along this well-defined roadmap to a full-fledged large-scale quantum computer, from other research results that have been announced over the years. Once we reach stage 7 in the Devoret-Schoelkopf stages of building a fault-tolerant quantum computer, it will be valuable to ask the question "How big of a number has been factored?", or "How many logical qubits do you have?". Until then, these are not the right benchmarks for people concerned about quantum cryptanalysis. We should be asking about achieving the benchmarks needed for a scalable fault-tolerant quantum computer. Large-scale factorizations will be implemented on logical qubits composed of many physical qubits. In contrast, several proof of concept implementations of quantum factorization reported to date were implemented at the physical system level. Such experiments at best indirectly demonstrate some degree of control relevant to stages 1, 2 and 3, however, in most cases, these have been done in systems where there are no clear plans to achieve stages 4 through 7. Other implementations are even less relevant to gauging progress towards quantum factorization of large numbers (e.g. as discussed in [SSV13]).

Furthermore it is also worth distinguishing between experimental efforts aiming to achieve full-fledged large-scale quantum computation, which is known to be a threat to cryptography, from other efforts that may aim to capture *some* of the computational power of quantum physics, but that essentially bypass the critical step of achieving a fault-tolerant scalable design that can implement Shor's algorithm.

that are cryptographically unbreakable provided that the hash-function used is not broken at the time the key is established. The only known way to achieve this with only conventional cryptography, without adding additional assumptions (like bounded memory assumptions), is to use public-key encryption to establish the keys. In this case, for the keys to remain secure, the public-key encryption must not be broken. Complexity theory gives us much greater confidence in the short-term security of a hash function than in the long-term security of a public-key encryption scheme (which requires more mathematical structure).

While in principle we have solutions, how ready are we to quantum-proof in practice? What is y, the migration time? Can we do this quickly or will it take decades?

3 Next steps

A wide range of research, ranging from fundamental to applied, still needs to be done to take QKD from its current state to one where it is a widely deployed global solution that can be reliably certified and be a part of major standards. In the short term, it is a feasible point-to-point and trusted repeater solution that organizations may take advantage of (in addition to the best available conventional cryptography) in order to have the most secure quantum-safe cryptography solutions available today. While this potential market may be relatively small at present, it will grow immensely once satellite QKD and untrusted quantum repeaters are widely deployed. It is important that we design the next-generation cryptography standards to be compatible with these solutions.

Post-quantum cryptography also requires a wide range of research from fundamental studies of their resistance to quantum attacks, to studies of their efficiencies under various resources constraints, to studies of their side-channel resistance.

Practical deployments of both quantum and post-quantum cryptography sooner rather than later will enable the applied cryptography and security community to battle-test these solutions under real-world conditions and better prepare them for “show-time” when the current cryptography tools are no longer able to provide the required security.

Appropriate standards and practices will need to be in place, and it has been encouraging to see major standards organizations such as ETSI, NIST, NICT, and IETF involved in the quantum-safe cryptography space for a number of years.

We will also need a new generation of cryptographers who understand how conventional cryptography works, who understand the landscape of the quantum-safe cryptography options, and who understand how to take new cryptography tools into practical applications.

We are still many years away from the widespread deployment of reliable quantum-safe cryptography. There is no quick fix and we cannot quickly make up lost time. While a large-scale quantum computer is a medium-term threat, given the wide and deep range of work to be done in order to widely deploy quantum-safe cryptography in practice, it is unfortunately not clear that $y < z$, that the migration time is less than the collapse time.

Despite the many technical and scientific challenges to deploying quantum-safe cryptography, the main challenges in my opinion are the business and policy decisions that would drive the adoption of quantum-safe cryptography. If we have an opportunity to inform and influence such decisions, this would be very helpful. For example, one can ask people and organizations to articulate their plan for managing the risk associated with the quantum threat.

Harnessing the power of quantum mechanics in large-scale quantum computers will allow us to solve many valuable problems for humanity, but we must first take the catastrophic impact of breaking cybersecurity off the table by developing and deploying a suite a quantum-safe cryptographic tools before quantum computers arrive.

Quantum-safe cryptography is a necessary part of cybersecurity in an era with quantum computers.

There are many important and difficult research challenges we need to tackle so that we may be ready.

References

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, Alain Tapp, “Tight bounds on quantum searching,” *Fortschritte der Physik* 56(5-5) (1998), 493-505.

[BFMV84] I. F. Blake, R. Fuji-Hara, R. C. Mullin, S. A. Vanstone, “Computing logarithms in finite fields of characteristic two”, *SIAM J. Algebraic Discrete Methods* 5 (2), 276285, 1984.

[CMS+15] A. D. Córcoles , E. Magesan, S. J. Srinivasan, A. W. Cross, M. Steffen, J. M. Gambetta, and J. M. Chow. “Demonstration of a quantum error detection code using a square lattice of four superconducting qubits.” *Nature Communications* 6, 2015.

[DS13] M. Devoret and R. J. Schoelkopf, "Superconducting circuits for quantum information: an outlook", *Science*, 339, no. 6124, 1169-1174, 2013.

[FMS01] S. R. Fluhrer, I. Mantin and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", In *Selected Areas in Cryptography 2001*, Springer, 1 24, 2001.

[Gro96] L. Grover, "A fast quantum mechanical algorithm for database search" *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC 1996)*, 212-219, 1996.

[IARPA15] http://www.iarpa.gov/index.php/research-programs/logiq

[IM12] L. Ioannou, M. Mosca, "A new spin on Quantum Cryptography: Avoiding trapdoors and embracing public keys", In *Proceedings of the 4th International Conference on Post-Quantum Cryptography (PQCrypto 2011)*, Lecture Notes in Computer Science, Vol. 7071, 255-274, Springer, 2011.

[KBF+15] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, H. Wang, J. Wenner, M. Steffen, A. N. Cleland and J. M. Martinis, "State preservation by repetitive error detection in a superconducting quantum circuit." *Nature* 519, no. 7541, 66-69, 2015.

[Kuh70] Thomas Kuhn, "The Structure of Scientific Revolutions", p. 150, 1970.

[Mos13] M. Mosca, "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop", e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 26-27 September 2013.

[NIST15] NIST Workshop on Cybersecurity in a Post-Quantum World, April 2015. http://nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm

[NSA15] NSA Information Assurance web page. https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml, accessed Aug. 2015.

[RPH+15] D. Ristè, S. Poletto, M-Z. Huang, A. Bruno, V. Vesterinen, O-P. Saira, and L. DiCarlo. "Detecting bit-flip errors in a logical qubit using stabilizer measurements." *Nature Communications* 6, 2015.

[Sho94] Peter Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994), 124-134.

[SSV13] John A. Smolin, Graeme Smith, and Alexander Vargo "Oversimplifying quantum factoring", *Nature*, Vol. 499, Number 7457, (2013) 163–165.

[SDCTK11] M. Steffen, D. P. DiVincenzo, J. M. Chow, T. N. Theis, and M. B. Ketchen, "Quantum computing: An IBM perspective.", *IBM Journal of Research and Development* 55, no. 5, paper 13, 2011.

[Tut00] W. T. Tutte, "Fish and I". Springer Berlin Heidelberg, 2000.

[WY05] X. Wang and H. Yu. "How to break MD5 and other hash functions." In *Advances in Cryptology - EUROCRYPT 2005*, Springer, 19-35, 2005.