Cybersecurity in the Quantum World

Michele Mosca, Ph.D., is one of the world's leading researchers in quantum computing and quantum cryptography. Mosca is cofounder of the Institute for Quantum Computing at the University of Waterloo (Ontario, Canada) and a founding faculty member at Perimeter Institute for Theoretical Physics. He cofounded CryptoWorks21, a training program in quantum-safe cryptography funded by the Canadian government. In 2015, Mosca cofounded evolutionQ Inc., where he serves as chief executive officer and president with chief technology officer Norbert Lütkenhaus, a pioneer and leader in quantum cryptography, to support organizations as they evolve their quantum-vulnerable systems and practices to quantum-safe ones.

Most people probably lock their doors when they are not at home. They trust that the things they value—family photographs, artwork, financial information and medical files—will be protected, thanks to steel deadbolts that can be unlocked only with their own key.

But what if we learned that, one day soon, someone would invent a universal lock pick that could instantly and easily open any locked door?

Most would likely investigate whether a new kind of lock might be impervious to the universal lock pick. And, most likely, people would not wait until after a first break-in to change the locks. Instead, one would want to do it before burglars had a chance to test their new tool in one's neighborhood.

MODERN CRYPTOGRAPHY

In the Information Age, many of one's most valuable belongings—finances, medical histories and, to a large extent, identities—are kept safe behind digital deadbolts.

The reason people can safely make money transfers and buy products online, and why major institutions and governments can exchange vast amounts of private data, is that information is protected by the complex "keys" of cryptography.

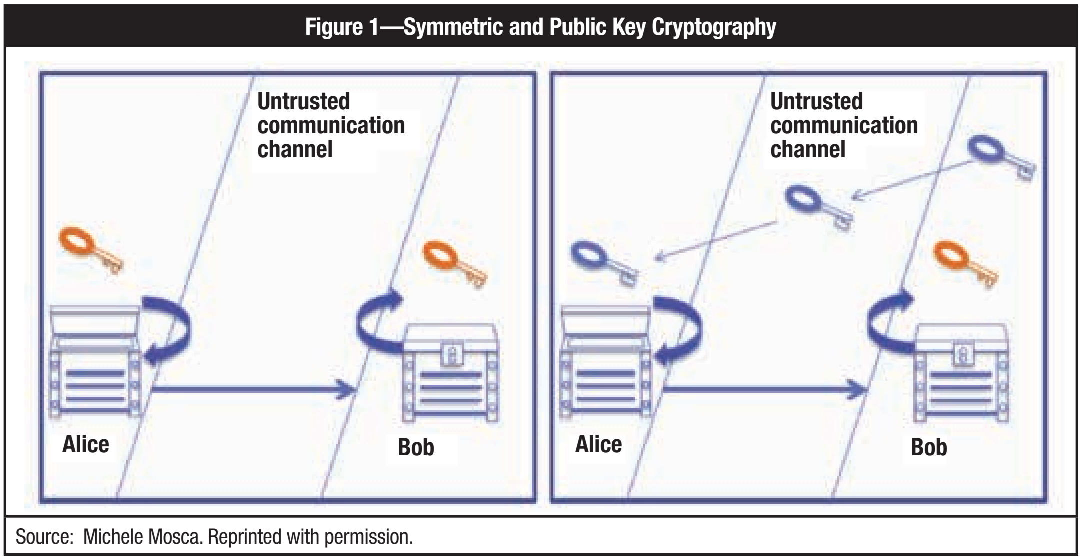
Present-day cybersecurity, like the lock on a front door, is reliable because the key used for an online transmission is digitally unique from countless other possible keys—and it is practically impossible for a cybercriminal to guess which one will unlock the door to private data. Online, keys are typically based on mathematical problems that are too difficult for even the most powerful computers to crack. One can trust that an online mortgage payment, for example, cannot be intercepted and stolen because a unique cryptographic key is shared between the payer and the bank, and the safety of that key is assured by the mathematical problem on which it is based.

Also available in Korean
한국어로도 가능

Figure 1 illustrates that in symmetric key cryptography (left), two parties, typically referred to as Alice and Bob, share the same private key (illustrated in orange). For example, Alice may encrypt a message with the key, send the ciphertext through an untrusted channel, and Bob may decrypt the message with the same key.

In public key cryptography (right), each party, say Bob, has its own private key (again, illustrated in orange) that it shouldn't share with anyone, and a public key (blue) that may be

Figure 1—Symmetric and Public Key Cryptography


Untrusted communication channel
Alice
Bob
Untrusted communication channel
Alice
Bob

Source: Michele Mosca. Reprinted with permission.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

freely disseminated to anyone interested in communicating with Bob. Any party, say Alice, may, for example, encrypt a message with Bob's (nonsecret) public key and send the ciphertext to Bob through an untrusted channel, and only Bob can decrypt the message. Public key cryptography may also be used to confirm the authenticity of the origin of information received and its integrity (e.g., during automatic software updates in order to confirm the updates are not malware).

The impact of quantum computers on symmetric key cryptography is serious; however, doubling key lengths protects against the currently known quantum attacks. In contrast, quantum cryptanalysis will fundamentally break RSA and elliptic curve cryptography (ECC)-based cryptography, as well as any other system, based on the difficulty of factoring large integers or finding discrete logarithms. Longer key lengths will not suffice, and fundamentally new methods for establishing keys in a public key setting will be needed.

But what if it was found that a kind of universal digital lock pick is on the horizon—one that could efficiently solve such mathematical problems? Would users seek a new kind of lock?

This once might have been a purely hypothetical question, but not anymore. It is a question that every person and, crucially, every organization needs to ask before it is too late.

It is the question of cybersecurity in the Quantum Age.

QUANTUM TECHNOLOGIES

Quantum computers are machines that harness and control the phenomena of the quantum world, the world of atoms, electrons, photons and nature's other building blocks, to process information in a radically different way than present-day computers.

Whereas today's computers perform operations by manipulating binary bits of ones and zeros, quantum computers process information with quantum bits (qubits), which behave in profoundly different ways than classical bits.

The laws of quantum mechanics, a pillar of modern physics, alongside Einstein's general relativity, allow quantum particles to be in a superposition of states. An oversimplified, but not entirely inaccurate, way to think of superposition is that a quantum particle can be in two different places, or states, at the same time.

It is a counterintuitive idea because human intuition has evolved in the bigger, messier world where quantum effects are not directly evident.

But the everyday world and the quantum world are converging. Computers, which just a half century ago filled an entire room, now fit in pockets and are extraordinarily powerful. Engineers have perpetually found new ways to make transistors, the on/off switches that enable computing, smaller and smaller, thereby allowing more to be crammed onto every microchip and increasing their efficiency and power.

This miniaturization of transistors is quickly nearing a threshold, however. Before long, transistors will shrink to the size of atoms and the rules governing their behavior will flip from classical to quantum. This threshold was long considered a kind of dead end for innovation in computing, until some scientists (the famous Richard Feynman among them) wondered if the switch from classical to quantum could somehow be turned into an advantage. The superposition principle, they argued, could mean that a qubit in a quantum computer could be not only a "one" or "zero," but both simultaneously, leading to a special form of parallel computation and a drastic, even exponential, increase in power.

QUANTUM CRYPTANALYSIS

Until recent decades, though, quantum computing sounded like the stuff of science fiction. Even if it were possible, and most people doubted that given how tiny and difficult to control quantum particles are, it was unclear for what it might be useful.

That changed almost overnight when applied mathematician Peter Shor demonstrated an algorithm that, if run by a quantum computer, could do something it was believed no classical computer could efficiently achieve: the mathematical feat of factoring very large numbers.

This is exactly the mathematical problem on which much of today's cybersecurity is based.

Quantum computers are still in the research and development stage. The science behind them is extremely complex, but working prototypes are emerging from research groups around the world.

Once the question was if quantum computers would become a reality. Now the question being asked is: "When will they become a reality?"

MANAGING QUANTUM RISK

An even more urgent question, especially for people and organizations that rely on cybersecurity, is whether they will be ready for the threat that quantum computers will pose to their ability to protect data from cyberattack.

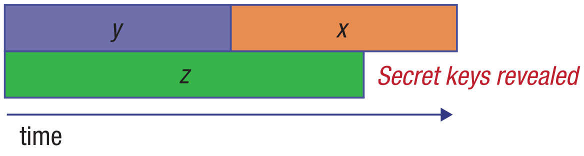
Although the digital burglars are not yet in the neighborhood, so to speak, updating cybersecurity to be quantum safe is much more complicated and time-consuming than changing the deadbolt on a front door.

What organizations need to begin thinking about now is not an immediate, drastic overhaul of their security infrastructure, but rather an "ounce of prevention" as quantum technologies begin to take shape on the horizon. It is better to evolve in pace with technologies rather than react reflexively to a major disruption; it is the more strategic, efficient and, ultimately, cost-effective approach.

Most cybersecurity infrastructures are extremely complex, particularly for large organizations, institutions and governments with varying security demands, and no two systems are exactly alike, so there is no one-size-fits-all solution for quantum readiness.

If powerful quantum computers become available, say, 10 years from now, but it takes a given organization 11 years to retool its infrastructure to become quantum safe, it is already too late for that organization to be impervious to the quantum threat. Furthermore, to protect against the compromise of information that was communicated a certain number of years in the past, the changeover to quantum-safe techniques must happen at least that many years before quantum computers are available (**figure 2**).

Figure 2—Will Your Secrets Be Revealed?



Source: Michele Mosca. Reprinted with permission.

Even if one is able to deploy quantum-safe tools before the quantum threat is realized, organizations responsible for keeping information confidential for some number of years, say x, must be sure that they are utilizing quantum-safe tools and practices at least x years before the quantum threat is at their doorstep. In other words, if it takes y years to quantum-proof their tools and systems, and z years for the quantum threat to become reality, then it is critical that x+y<z. Otherwise, the confidentiality guarantees will be compromised.[1] For example, if 5 (x) years of confidentiality are required and the quantum threat is 15 (z) years away, then the organization must quantum-proof its systems in under 10 (y) years.

It is impossible to predict exactly when full-scale quantum computers will be available, but the pace of research and innovation is accelerating every day.[2, 3]

Quantum computing research is well motivated and well funded at research facilities around the world, and the potential benefits of quantum computing are great. But the double-edged sword of quantum computing is the threat it poses to information security if it is used for the wrong reasons. For the advent of quantum computers to be a positive milestone in human history, the cyberinfrastructure must be quantum-proofed in time.

QUANTUM-SAFE OPTIONS

Thankfully, quantum technologies also make possible one solution to that threat. Quantum cryptography capitalizes on quantum phenomena to protect private information in ways that even a quantum computer cannot crack. It is based on the law of quantum mechanics that says that observing quantum data necessarily disturbs them; this means that any eavesdropping on a quantum transmission used for key establishment can be instantly detected before any data can possibly be compromised. Such quantum key distribution (QKD) is already commercially available and has been used to protect important bank transfers and other communications.

There are also forms of postquantum cryptography, which are not themselves based on quantum techniques. Like today's public key methods, they use conventional technologies and rely on assumptions about the infeasibility of some mathematical computations; however, they are secure against all currently known forms of quantum or conventional cryptanalytic attacks.

Determining which of these approaches, or what combination of them, is required for an organization to face the coming quantum threat to cybersecurity is something that needs to be determined on a case-by-case basis.

For many organizations, the urgency lies not in drastically overhauling cybersecurity infrastructure today, but in analyzing the potential vulnerabilities and laying the groundwork so that a transition can be undertaken if/when the need becomes imminent.

Assessing those vulnerabilities and determining what is needed to remedy them is the essential first step in charting a course toward quantum readiness.

The consequences of unpreparedness are potentially enormous: the compromise and potential collapse of financial systems, energy grids, e-commerce, stock markets and other essential digital infrastructures on which society relies. Those consequences vastly outweigh the relatively small investments required to make those infrastructures quantum-ready.

It may not yet be necessary to install a new digital deadbolt. But for the sake of what is most valuable, the time is now for organizations to look carefully at their current security systems to ensure that the threat, when it arrives, will not get past the front door.

REFERENCES

Pecen, Mark; *et al.; Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges*, white paper, European Telecommunications Standards Institute, October 2014

Menezes, A. J.; P. C. van Oorschot; S. A. Vanstone; *Handbook of Applied Cryptography, (Discrete Mathematics and Its Applications)*, CRC Press, England, 1996

ENDNOTES

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

[2] Steffen, M.; D. P. DiVincenzo; J. M. Chow; T. N. Theis; M. B. Ketchen; "Quantum Computing: An IBM Perspective," *IBM Journal of Research and Development*, vol. 55, no. 5, paper 13, September/October 2011

[3] Devoret, M. H.; R. J. Schoelkopf; "Superconducting Circuits for Quantum Information: An Outlook," *Science*, vol. 339, no. 6124, 8 March 2013, p. 1169-1174