Ensuring Online Security in a Quantum Future

By Lucian Comandar, Jean-Francois Bobier, Michael Coden, and Stefan Deutscher

Consider two predictions. Google CEO Sundar Pichai expects that quantum computing will break encryption as we know it today in the next five to ten years. Michele Mosca, a founder of the University of Waterloo's Institute of Quantum Computing, believes that quantum computing has a one in seven chance of breaking RSA-2048 encryption (considered the gold standard for public key encryption) by 2026 and a 50-50 chance of doing so by 2031.

The online security game is about to change. Once quantum computers are sufficiently capable of factoring products of large prime numbers – an achievement that is no longer believed to be far into the future – current standards for cryptography, and therefore online security, will be as useful as a 1950s mainframe. The system that for years has protected our online activities and communications is in danger of becoming obsolete. Companies in all industries need to take note now and plan for encryption in a quantum future.

Breaking the Public Key Encryption Standard

Quantum computing promises major advances and value generation in such sectors as biopharma and materials development. But it also eventually will enable rapid factorization of products of prime numbers (using Shor's algorithm), and that will threaten the underpinnings of public key cryptography (PKC). Cryptographic systems can be divided into two categories. Symmetric cryptography (such as the Advanced Encryption Standard or AES) is used for message encryption and has been only partly affected by known quantum computing attacks. Doubling the length of the current encryption key would mitigate an attack from a quantum computer. Asymmetric cryptography (such as RSA) is the basis for PKC and relies on difficult mathematical problems (factoring prime numbers is most common). Asymmetric cryptography is widely used in digital steps such as signatures and key exchanges to secure communications and networks that are critical to the use of the internet. These include email exchanges, virtual private networks (VPNs), secure webpage connections, most forms of e-commerce, and digital supply chains, among others. Symmetric and asymmetric cryptography are commonly used together: asymmetric cryptography to do key establishment and agreement, and symmetric cryptography for message encryption as in the https protocol, most widely used for web browsing.

Since PKC enables more than 4.5 billion internet users to securely access some 200 million websites and engage in some $3 trillion of retail e-commerce annually, a lot is at stake. An estimated 20% of all IT applications, or more, rely on public key encryption. Furthermore, data currently transmitted based on RSA-2048 is vulnerable to "store now, break later" attacks since public internet traffic is easily duplicable.

Enter (Gradually) Post-Quantum Cryptography

Post-quantum cryptography (PQC) is a class of PKC algorithms that relies on a set of mathematical problems that


Companies with a high degree of crypto-agility will be better equipped to handle the coming transitions.

have no currently known fast solutions using either quantum or classical computers, but the key words here are "currently known." PQC is therefore vulnerable to future advances in solving the mathematical problems or to implementation errors.

PQC standards are now being defined. The US National Institute of Standards and Technology (NIST) is conducting an open competition to determine the set of PQC standards that will augment and ultimately replace RSA. It plans to release these standards in the 2022-24 time frame. This implies that the window for upgrading existing infrastructure is seven to nine years – too short for such an ambitious goal. (See Exhibit 1.)

In the past, cryptographic transitions have taken significantly longer to implement fully. For example, it took more than 20 years for the Secure Hash Algorithm 1 and AES to completely replace the data encryption standard (DES) and 3DES. Higher-value systems are usually transitioned first while less critical systems (including segments of product IT) remain in place until the end of their life cycle. Some experts estimate the necessary transition time for PQC standards to be 10 years. (See the sidebar, About This Article.) In the words of Brian LaMacchia, who heads the security and cryptography team at Microsoft Research, "When you are upgrading the internet, that is not a lot of time."

Companies Will Need Crypto-Agility

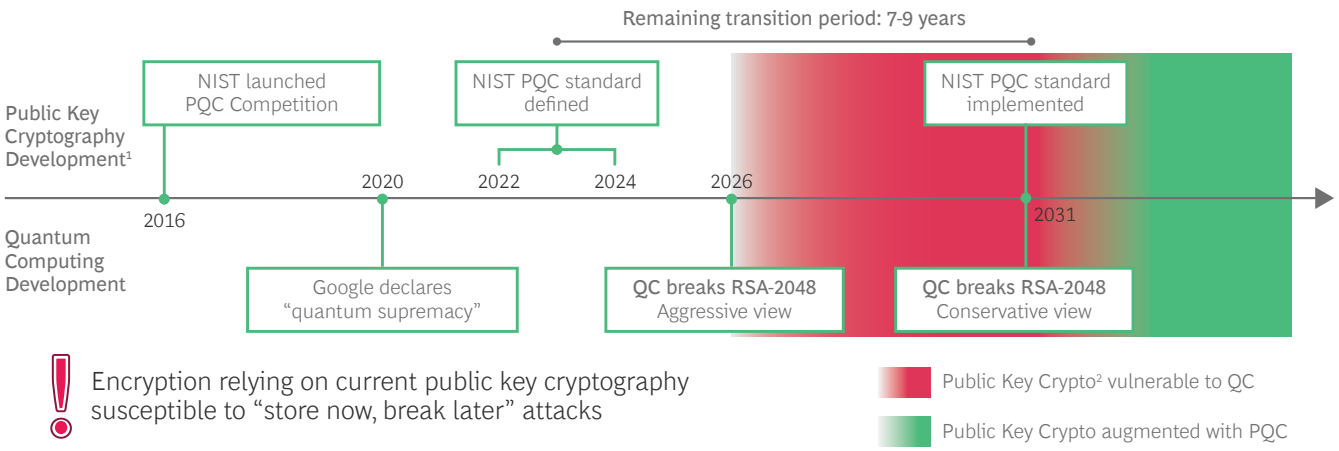
Crypto-agility is the ability to adopt and switch rapidly among multiple cryptographic standards that perform at varying levels. It will play a differentiating role in reducing vulnerabilities – and consequently the cost of securing data in transit – during and after the cryptographic transition.

For several reasons, we expect the transition to PQC standards will require a staged hybrid approach. One reason is the need to address different use-case constraints, such as communicating among varying IoT devices as opposed to simply emailing PC to PC. Another is increasing security levels. A third is ensuring backward compatibility. In the first phase, multiple security standards will be stacked and used in conjunction. (See Exhibit 2.) These will include RSA and most likely a few PQC standards. In the middle phase, PQC standards will be upgraded as needed and continue to work alongside RSA. In the end phase, RSA will be superseded and PQC standards will continue to evolve.

Simply put, companies with a high degree of crypto-agility will be better equipped to handle the coming transitions than those without it.

The danger of standardization fracturing along national or regional lines is complicating matters further. For example, China concluded its PQC standardization in January 2020, while US-based NIST has yet to complete its work.

Exhibit 1 - The Time Window for Upgrading Cryptographic Infrastructure Is Closing Rapidly



Sources: NIST Post-Quantum Cryptography timeline, BCG analysis.

Note: PQC: Post-Quantum Cryptography. NIST: National Institute of Standards and Technology USA.

[1]Based on NIST PQC timeline.

[2]Public Key Cryptography (up to RSA-2048).

About This Article

In the preparation of this article, the authors talked with more than 20 experts in quantum computing, cryptography, and cybersecurity. They are grateful to the following for their insights and assistance: Greg Bullard, AGB Advisors; Martijn Dekker, ABN AMRO; Chris Erven, KETS; Edouard Giard, Credit Agricole Corporate Investment Bank; Noel Goddard, Qunnect; Grantly Mailes, BCG; Bruno Huttner, ID Quantique; Christophe Jurczak, Quantonation; Marc Kaplan, VeriQloud; Carlos Kuchkovsky, BBVA; Paul Kwiat, University of Illinois at Urbana-Champaign; Brian LaMacchia, Microsoft; Antia Lamas-Linares, SpeQtral; Alexander Ling, National University of Singapore; Andrew Lord, BT; Pascal Maillot, European Commission; Mehdi Namazi, Qunnect; Momtchil Peev, Huawei; Ludovic Perret, CryptoNext; Escolastico Sanchez, BBVA; Vikram Sharma, QuintessenceLabs; Dirk Stegemann, BCG; Phil Venables, Goldman Sachs; and Eitan Yehuda, BCG.

In a connected world with such fractured standardization, a high level of adaptability will be required. Companies and systems will need to support not only different algorithms from a single entity, but potentially algorithms from multiple standardization bodies, such as NIST, the Chinese Association for Cryptologic Research, Europe's ETSI, and the IEEE. Furthermore, the time intervals for transitioning standards will shrink as the rate of change rises, driven by different bodies updating a variety of PQC standards. Companies must start to analyze now the value of their data from a security point of view, as some data is time-sensitive and critical.

For all these reasons, crypto-agility is likely to emerge as a differentiating factor in business. The transition will happen too quickly for some categories of product IT that are in the early phases of long life cycles, as is the case in the automotive and aerospace industries. Companies will find themselves quite soon using legacy products that require special solutions – and for some, such solutions might not be achievable. But as digitalization drives more companies to update their applications in the cloud – a trend exacerbated by the COVID-19 pandemic – firms now have the window of opportunity to integrate crypto-agility in their implementations.

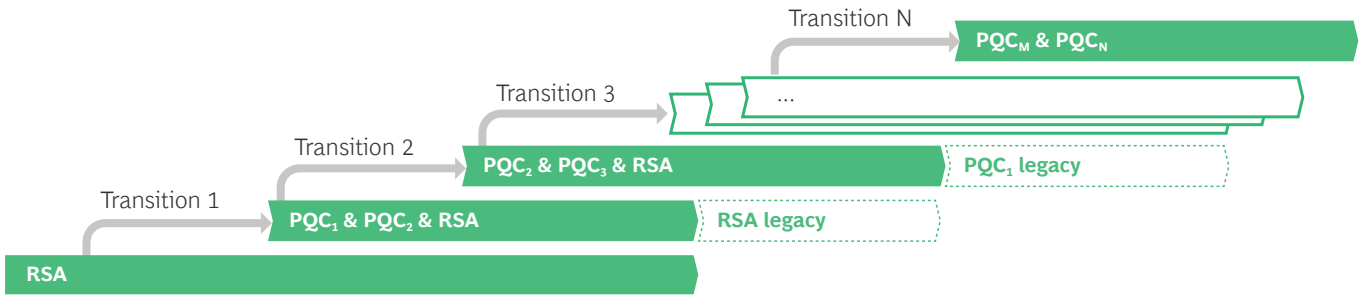
Quantum Key Distribution Promises Future-Proof Security – for Some

Some companies handle data today that will continue to be sensitive well into the future, including those in privacy-sensitive or strategic industries such as health care, defense contracting, and advanced equipment design and manufacturing. Data in transit over the public internet, even though currently considered secure, is still susceptible to "store now, attack later" schemes in which bad actors steal and duplicate encrypted communications for decryption once the necessary quantum computers become available. Companies may want to consider an additional layer of security for data with long-term criticality.

Fortunately, quantum technology not only creates the threat, it also provides a solution. Quantum-based tools can be used to detect the presence of attackers on a link when distributing the encryption key through a protocol known as quantum key distribution (QKD). The protocol, used in association with one-time-pad cipher, promises unbreakable encryption security. However, this scenario carries stringent requirements, including true randomness, absolute secrecy, one-time use, and a key that is the same size as the message, which makes it cumbersome and complicated to employ. Thus, it appeals primarily to those interested in securing their highest-value links for long periods of time and with the highest level of security, such as public sector and military users.

QKD is still an emerging technology, and key distribution rates do not match the rates of conventional high-speed communication (Gb/s). Use cases are restricted to those with short key rates (they can be measured in Kb/s or Mb/s) or lower encryption security levels. A more likely scenario is to use QKD with conventional symmetric proto-

Exhibit 2 - Crypto-Agility Will Be the Key to Managing Rapid Transitions in Security



Hybrid transitions will soon enable:
- Security against both classical and quantum computers
- Backward compatibility during transitions
- Continuous updates of algorithms

Companies will need to cope with:
- Interoperability with multiple standards
- Diverse technical requirements for standards
- Rapid cycles for standard updates

Sources: Expert interviews, BCG analysis.

Note: PQC: Post-Quantum Cryptography. RSA: Rivest–Shamir–Adleman cryptosystem.


The goal should be to make the cost of compromising data greater than its value to attackers.

cols (such as AES) and post-quantum signatures, thus enabling high-speed throughputs and higher security than conventional schemes.

At this stage, development of QKD is largely funded by the public sector and has limited private sector adoption. It is expected that over time technological breakthroughs will decrease cost, improve performance, and therefore increase the rate of adoption. Toshiba estimates the global QKD market will reach $12 billion in a 10-year time frame and grow to $20 billion in 15 years.

Some of the breakthroughs that would advance the development of QKD include:

- Miniaturization and integration of optics and electronics.
- The advent of quantum-safe solutions as a differentiating factor to existing networks. Field trials by Huawei and Telefonica, SK Telecom and ID Quantique, and BT and Toshiba are under way, with applications in 5G, health care, and critical infrastructure operations.
- Development of space distribution networks (for which commercial solutions are expected as early as 2022).
- Development of standards and certifications around the world to support enterprise adoption.

Strategic considerations are also driving QKD development. China's launch of the Micius satellite and its investment of €10 billion in quantum technology development has triggered new funding programs in the US (National Quantum Initiative) and the EU (Quantum Flagship or France's and Germany's national plans), among others. That said, in 2016, more than two-thirds of all global patents related to QKD originated in China. Chinese-based institutions held the same number of total patents as the US and Japan combined. Several actors (including the US, the EU, China, and Russia) are racing to develop security technology. However, they are focusing on the development of local or regional ecosystems and supply chains, limiting export and localizing funding, thus hindering international cooperation.

What Should Companies Do?

The ability to use quantum computing to decrypt critical assets will evolve over time, and companies (and other organizations) that plan ahead will be able to cost-effectively and efficiently navigate the post-quantum environment. The first step is to identify and understand the criticality of their data assets. Companies can then apply two principles to deploy quantum-safe solutions, such as PQC and QKD, that will protect their most critical assets.

The first principle is that no entity can possibly protect all of its data, so companies must prioritize which data is most critical. The second principle is that no company needs to spend more than the value of an asset to protect it. Put another way, the security goal should be to make the cost of compromising data greater than the value of the data to attackers. If the cost of stealing the data is greater than the value, the bad guys will move on to another victim.

With this understanding at hand, companies can take the necessary steps to increase their crypto-agility. This capability should become a requirement in the development of new services and products and a prerequisite for suppliers of future products. Companies can also initiate support for ecosystem measures that increase crypto-agility by replacing legacy solutions in a forward-looking manner.

Lastly, businesses need to prepare for a quantum future. They need a system for keeping updated on developments in quantum computing and quantum-safe solutions and a roadmap to mitigate vulnerabilities. Companies that deal with critical data, and those with higher risk profiles, should start piloting the integration of quantum-safe solutions now.

Quantum computing has long been the stuff of science fiction. But recent developments, and the big commitments of major players, put usable machines within sight and ramp up the urgency of dealing with the implications of a powerful new capability – both good and bad. Companies of all sizes and levels of technological sophistication now have the knowledge and tools that allow them to plan ahead and invest in protecting their most valuable assets in this fascinating and exciting next era of our information age.

About the Authors

Lucian Comandar is a consultant in the Munich office of Boston Consulting Group. You may contact him by email at comandar.lucian@bcg.com.

Michael Coden is a managing director of BCG Platinion in the firm's New York City office. You may contact him by email at coden.michael@bcg.com.

Jean-Francois Bobier is a partner and director in the firm's Paris office. You may contact him by email at bobier.jean-francois@bcg.com.

Stefan Deutscher is a partner and associate director in BCG's Berlin office. You may contact him by email at deutscher.stefan@bcg.com.

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders – empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.