Deloitte. Insights

FEATURE

Preparing the trusted internet for the age of quantum computing

The data security threat may be more imminent than you think

Deborah Golden, Colin Soutar, Itan Barmes, Scott Buchholz, and Caroline Brown

Understand and prepare for the potential security threat posed by quantum computers.

THE TRUSTED INTERNET relies on cryptographic algorithms, and the digital economy depends on this trust. Such cryptographic algorithms are embedded in hardware and software throughout enterprise infrastructure. Like a reliable and unbreakable lock, they help safeguard sensitive personal and financial information and verify the integrity of internet transactions, as well as the identity of users and systems.

The underlying algorithms in today's cryptographic systems have generally been immune to attacks by even the fastest computers. However, some experts predict that within a decade, cybercriminals and nation-state actors with access to quantum computing capabilities may gain the ability to crack public-key cryptography algorithms that serve as the backbone of today's secure internet.[1] Furthermore, even before quantum computers are available, advanced attackers could conduct "harvest now, decrypt later" attacks, in which they collect and store encrypted data and related communications today, with the goal of decrypting the data in the future.

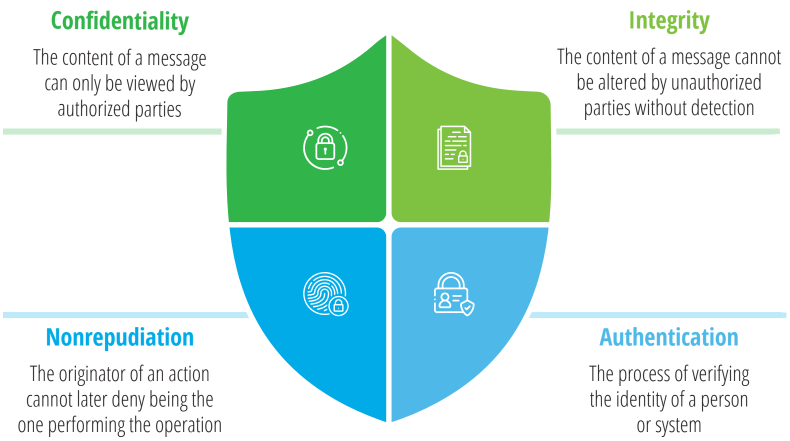
To ready your organization for this, it's important to understand the quantum threat, the current state of postquantum cryptography, and how to prepare for quantum-safe cryptographic systems and procedures.

Understanding the potential threat to public-key cryptography

Cryptographic algorithms are used to digitally encode messages and data, thus providing four security services that are foundational to network communications and e-commerce transactions: confidentiality, integrity, nonrepudiation, and authentication (figure 1).

FIGURE 1

The four foundations of secure communications and transactions


Confidentiality
The content of a message can only be viewed by authorized parties
Integrity
The content of a message cannot be altered by unauthorized parties without detection
Nonrepudiation
The originator of an action cannot later deny being the one performing the operation
Authentication
The process of verifying the identity of a person or system

Source: Deloitte analysis.

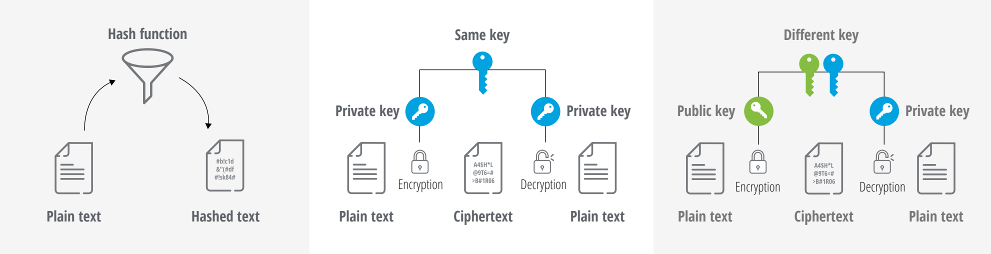
To implement these critical functions, three types of algorithmic techniques are used to perform cryptographic operations: hash functions, symmetric-key algorithms, and public-key algorithms (figure 2).

The quantum threat to hash functions and symmetric algorithms comes from an algorithm invented by computer scientist Lov Grover in 1996.[2] Although Grover's algorithm significantly speeds up the time it takes to attempt all potential numerical keys or hash values until finding the right one, this algorithm can be readily thwarted by doubling the key length or using other currently available hash functions.

On the other hand, a quantum algorithm designed in 1994 by mathematician Peter Shor[3] poses a more serious threat to public-key cryptography. Shor's algorithm can theoretically break the mathematical relationship between public and private keys in a matter of hours.[4] Public keys are widely distributed—consider, for example, web certificates—and could be used to determine the private key, which would effectively render current public-key cryptography useless.

FIGURE 2

Types of cryptographic techniques



	Hashing	Symmetric cryptography	Public-key cryptography
	Generating a checksum (fingerprint) for a piece of data is a way to uniquely identify the data. For a good hash function, it is infeasible to find a second piece of data that generates the same hash value.	Encryption method that uses the same key for both encryption and decryption	Relies on two mathematically related keys (private and public keys). A cryptographic operation done with one key can only be reversed (for confidentiality) or verified (for integrity, authentication, and nonrepudiation) with the other key.
Cryptographic application	Storing and verifying passwords and checking data integrity	Bulk encryption of large amounts of data	Basis of internet communication and e-commerce encryption protocols such as SSL, TLS, and HTTPS
Quantum impact	Reduces security; more secure hash functions exist and can be used	Reduces security; the minimal key size should be doubled for most algorithms (e.g., AES)	Breaks all currently used public-key algorithms

Source: Deloitte analysis.

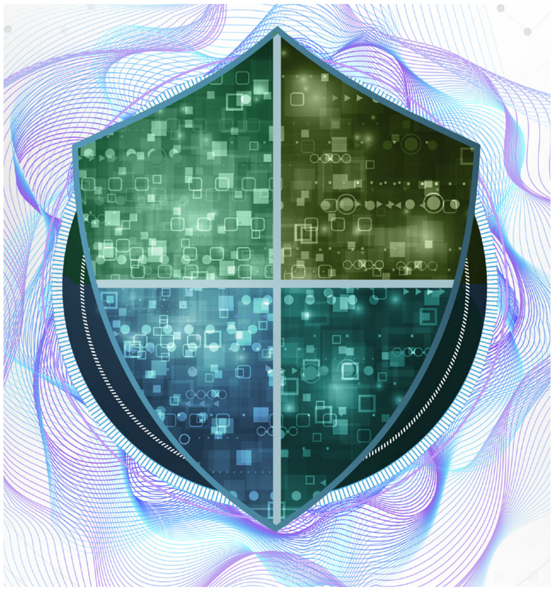
As such, the quantum threat to public-key cryptography—used for such things as key exchange and digital signatures—is significantly higher than to hash functions or symmetric algorithms. Security experts differ on when quantum computers will be mature enough to use Shor's algorithm to crack public-key cryptography. Estimates range from between five and 20 years.[5] Given that public keys are widely available, encrypted data and related communications can be collected now and decrypted once hackers gain access to sufficiently mature quantum computers, thus jeopardizing the long-term security of today's internet communications and transactions.

Fortunately, the National Institute of Standards and Technology (NIST) is working to standardize postquantum, public-key cryptography algorithms that can be used to develop systems that are secure against both quantum and traditional computers. After a multiyear process of soliciting, evaluating, and standardizing one or more postquantum cryptography algorithms, NIST plans to announce the standardized quantum-resistant algorithms by 2024.[6]

When postquantum cryptography is fully developed and standardized, organizations can upgrade their existing public-key cryptography systems. One report from the World Economic Forum estimates that 20 billion digital devices will need to be upgraded or replaced with postquantum cryptography in the next 20 years.[7]

This is not a simple switch or patch because cryptography is entrenched across the enterprise, including in physically remote systems. For example, migrating to postquantum cryptography will affect the performance requirements of microprocessors that are embedded in ATM machines, TV set-top boxes, point-of-sale systems, smartphones, and a host of other devices and systems. As a result, algorithm replacement can be extremely disruptive and take decades to complete, and typically requires upgrading or replacing components of the cryptographic infrastructure.[8]

Parallel to its standardization efforts, NIST is developing practices and recommendations aimed at simplifying the migration from current public-key cryptography algorithms to quantum-resistant algorithms.[9] NIST aims to develop a migration playbook with recommendations and practices that help organizations address the challenges of algorithm replacement. In its initial stages, the NIST migration playbook's goal is to demonstrate automated discovery tools to help organizations determine where and how public-key cryptography is being used in hardware, firmware, operating systems, communication protocols, cryptographic libraries, and applications. Then the focus of the initiative will be on prioritizing those components and assets for migration.



Similarly, the World Economic Forum has called for the development of a quantum security coalition to promote the adoption of secure quantum solutions and develop global governance principles and models.[10]

How to prepare for postquantum cryptography

In addition to leveraging the NIST standards and migration recommendations, business leaders can take several actions to ready their organizations for the security implications of quantum computing.

1. **Build awareness of quantum's security risks.** Understand the risk quantum computing poses to existing cryptographic and encryption systems. Extend this awareness to other business leaders at the board and C-suite level to gain support for investing in a quantum-safe cryptography infrastructure.

2. **Take a fresh approach to cryptographic governance.** Preparing cryptographic systems for the quantum computing era is a major technical challenge, one that may require organizations to change their view of the cryptographic infrastructure as rigid and static. In the same way that Agile software delivery practices help create more adaptable technology organizations, so can a more agile approach to cryptographic governance create more flexible businesses that can quickly pivot and reprioritize in response to evolving security threats, including those related to quantum computing. This mindset shift can result in a flexible, dynamic cryptographic infrastructure that's more capable of fluidly evolving with enterprise, industry, and technology security challenges and requirements.

3. **Assess the enterprise's readiness to become crypto-agile.** A refreshed approach to cryptography can enable a more crypto-agile organization—that is, one that can efficiently update cryptographic algorithms, parameters, processes, and technologies to better respond to new protocols, standards, and security threats, including those leveraging quantum computing methods. To assess organizational readiness for crypto-agility, review the following and consider potential migration strategies:

   - **Data and cryptographic assets:** To help respond to systemic changes—such as new algorithms—it can help to provide an accounting of data assets to understand how they're cryptographically protected. Inventory and prioritize cryptographically protected data, transactions, and other assets and understand their retention requirements and location. For example, are they on-premises or in the cloud?

   - **Cryptographic keys:** To identify and prioritize future vulnerabilities, review the types of cryptographic keys being used, their characteristics, and their location in existing computer and communications hardware, operating systems, application programs, communications protocols, key infrastructures, and access control mechanisms.

   - **Infrastructure limitations:** Quantum-safe cryptography may use substantially more processing power than current cryptographic methods, which could require infrastructure upgrades. As NIST standards develop, understand how they will impact system infrastructure. Identify potential future infrastructure shortcomings such as bandwidth, latency, memory, and computing power and develop a plan for addressing these limitations.

4. **Engage with the quantum security ecosystem.** Monitor the development of NIST's postquantum cryptography standards and solutions and understand and evaluate the recommended migration approaches. Develop crypto governance based on a framework such as the NIST Cybersecurity Framework, which outlines practices and processes for managing cybersecurity risk. Finally, engage in public-private and industry ecosystem relationships to stay aware of technology developments in quantum computing, quantum-resistant cryptography, and crypto-agility.

5. **Practice good cyber hygiene.** As always, be proactive about managing and reducing cybersecurity risks. Establish and maintain strong foundational cybersecurity principles and practices and situational awareness of data, infrastructure, and other assets.

While the path to postquantum cryptography may be lengthy and complicated, enterprises can see the quantum threat coming, which makes the decision to prepare a simple one. You may be familiar with the American adage, "an ounce of prevention is worth a pound of cure." In the case of tackling crypto-agility, however daunting the prevention may seem, it would be infinitely more tolerable than the crisis that could result from a collapse of public-key encryption.

Endnotes

1. See, for example, Inside Quantum Technology, "Sundar Pichai warns Davos that quantum computers will be able to break encryption in five years," January 23, 2020; Drs. Michele Mosca and Marco Piani, *Quantum threat timeline*, Global Risk Institute, October 3, 2019.
2. Lov K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, July 1,1996.
3. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," IEEE Xplore, August 6, 2002.
4. Drs. Michele Mosca and Marco Pianis, *Quantum threat timeline report 2020*, Global Risk Institute, January 27, 2021.
5. Inside Quantum Technology, "Sundar Pichai warns Davos that quantum computers will be able to break encryption in five years"; Drs. Mosca and Pianis, *Quantum threat timeline*.
6. NIST, "Post-Quantum Cryptography," June 14, 2021.
7. Catherine P. Foley et al., "Is your cybersecurity ready to take the quantum leap?," World Economic Forum, May 7, 2021.
8. William Barker, William Polk, and Murugiah Souppaya, *Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms*, NIST, April 28, 2021.
9. William Barker and Murugiah Souppaya, "Crypto agility: Considerations for migrating to post-quantum cryptographic algorithms," NCCoE and NIST, June 2021.
10. Vikram Sharma and William Dixon, "We need to build a quantum security coalition. Here's why," World Economic Forum, August 11, 2020.

Acknowledgments

The authors would like to thank **Emily Mossburg, Marc Verdonk, Stefanie Heng, Maria Wright, Aaron Gano, Mary Hughes, Tracey Parry, Cheylin Parker,** and **Shelley Pfaendler** for their contributions to this article.

About the authors

Deborah Golden | debgolden@deloitte.com

Deborah Golden, a principal at Deloitte & Touche LLP, is the US Cyber & Strategic Risk leader for Deloitte Risk & Financial Advisory. She has more than 25 years of cross-industry experience, focused predominantly within government, life sciences and health care, and financial services industries. Golden primarily helps commercial organizations and government agencies navigate multifaceted cyber problems and transform business or mission strategies and operations. Recognizing the ubiquitous, sophisticated nature of cyber, she uses a values-driven approach to help clients align cybersecurity imperatives with cyber risk and strategic business priorities to strengthen cyber resilience.

Colin Soutar | csoutar@deloitte.com

Dr. Colin Soutar is a managing director in Deloitte Risk & Financial Advisory. He is the Government & Public Services Cyber & Strategic Risk Products and Technology leader, and helps government organizations develop and execute their cybersecurity risk management strategies. Soutar has more than 25 years of experience in biometrics, digital identity, and cybersecurity technologies and was previously the CTO of a public company in Toronto, Canada. He currently serves on the World Economic Forum Global Future Council for Cybersecurity.

Itan Barmes | ibarmes@deloitte.nl

Itan Barmes is a member of the cryptography team at Deloitte's cyber risk services department. He has broad experience in both academia and industry and holds a PhD in experimental physics. Currently, Barmes is focusing on the intersection between physics and cybersecurity and works on advising organizations on how to manage their risks in the advent of quantum computers.

Scott Buchholz | sbuchholz@deloitte.com

Scott Buchholz is a managing director with Deloitte Consulting LLP and serves as the Government & Public Services chief technology officer and the national emerging tech research director. A leader and visionary with more than 25 years of experience, he advises clients on how to navigate the future using existing and emerging technologies. Buchholz also leads Deloitte's efforts to explore quantum computing and quantum technologies.

Caroline Brown | carolbrown@deloitte.com

Caroline Brown is a senior writer with Deloitte Consulting LLP, where she writes research reports, articles, and other content about emerging technologies and technology leadership. She specializes in enterprise technologies, technology and industry trends, IT capabilities and competencies, organizational culture, and business processes.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Deborah Golden
US Cyber & Strategic Risk leader | Deloitte Risk & Financial Advisory | Deloitte & Touche LLP
+1 571 882 5106 | debgolden@deloitte.com

Colin Soutar
US GPS Cyber & Strategic Risk Products & Technology leader | Managing director, Cyber & Strategic Risk
Deloitte Risk & Financial Advisory | Deloitte & Touche LLP
+1 571 858 1933 | csoutar@deloitte.com

Itan Barmes, PhD
Manager, Cyber Risk Services | Deloitte Risk Advisory BV
+31 (6) 500 98 170 | ibarmes@deloitte.nl

Scott Buchholz
US Quantum leader | Emerging technology research director
Government & Public Services chief technology officer | Deloitte Consulting LLP
+1 571 814 7110 | sbuchholz@deloitte.com

Quantum technologies, and their heady promise, are in the news. With the promise of breakthrough innovations in drug development, financial modeling, climate change, traffic optimization, machine learning, batteries, and more, is now the time to invest? By the same token, how much concern is warranted about quantum computing's future ability to break today's encryption standards? As business and technology leaders strive to make thoughtful choices for today and tomorrow, what needs to be done to get ready for a quantum-enabled future? What future risks need to be considered—and potentially mitigated—starting today?

Contact the authors for more information or read more about our quantum computing services on Deloitte.com.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Andy Bayiates, Hannah Bachman, Dilip Poddar, and Nairita Gangopadhyay
Creative: Kevin Weier and Anoushriya S Rao
Audience development: Aditya Prasad
Cover artwork: Kevin Weier

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.