MIT Technology Review Insights

Produced in collaboration with

TII Technology Innovation Institute

Organizations need to strengthen their cybersecurity now before quantum computing becomes powerful enough to break today's encryptions.

Facing tomorrow's quantum hackers today

Preface

"Facing tomorrow's quantum hackers today" is an MIT Technology Review Insights report developed in collaboration with Abu Dhabi's Technology Innovation Institute. The report is based on interviews with cryptography experts, mathematicians, physicists, and senior executives of quantum computing companies worldwide. The interviews were conducted in February 2022 to evaluate how a quantum computer, when one is fully developed, can threaten today's cybersecurity systems, and what enterprises and organizations can – and should – do today to protect themselves. Poornima Apte was the writer, Kwee Chuan Yeo was the editor, and Nicola Crepaldi was the publisher. The research is editorially independent, and the views expressed are those of MIT Technology Review Insights.

We would like to thank the following individuals for providing their time and insights:

Najwa Aaraj, Chief Researcher, Cryptography Research Center, Technology Innovation Institute, Abu Dhabi (UAE)

Jung Hee Cheon, Professor of Mathematics at Seoul National University, and Director of the Industrial and Mathematical Data Analytics Research Center, Seoul (South Korea)

William Hurley, Chief Executive Officer, Strangeworks (USA)

Duncan Jones, Head of Cybersecurity, Quantinuum, Cambridge (UK)

Dustin Moody, Mathematician; Head, Post-quantum Cryptography Project; National Institute of Standards and Technology, NIST (USA)

Jian-Wei Pan, Professor of Physics, University of Science and Technology of China (China)

Grégoire Ribordy, Co-founder and Chief Executive Officer, ID Quantique, Geneva (Switzerland)

Tony Uttley, President and Chief Operating Officer, Quantinuum (USA)

Foreword

Welcome to this MIT Technology Review Insights report. Developed in collaboration with Abu Dhabi's Technology Innovation Institute, this report analyzes how post-quantum cryptography can serve as an efficient defense against hackers who can one day use quantum computers – when they are fully developed – to attack current cybersecurity systems.

In an era of rapid advances in quantum technology, it's only a matter of time before we see a fully operational quantum computer that can cripple today's public-key cryptography systems, which form the foundation of today's secure digital communications. With the quantum race gathering momentum as tech leaders grapple with tweaking qubits to help achieve quantum supremacy and advantage, it's time to examine and prepare for the ramifications of a post-quantum age. Google and IBM, along with startups such as Rigetti, IonQ, and Xanadu, are building viable quantum-computing systems. In 2019, Google announced that its quantum computer had solved a problem faster than the best existing supercomputers, thus achieving quantum supremacy. In 2020, academic researchers in China also reported that their quantum computers had outperformed conventional computers in working with an algorithm designed for specialized optimization tasks.

Clearly, when a cryptographically relevant quantum computer is operational, some forms of secure encryption will be compromised, leading to an imminent breakdown in security and confidentiality – two hallmarks of today's critical infrastructure systems. There are compelling reasons for enterprises to think about protecting themselves today against the technology of tomorrow. Organizations must make their data and cybersecurity systems resistant to quantum-based attacks, and hybrid solutions are available for those unsure how to proceed with post-quantum cryptography.

Since 2016, the National Institute of Standards and Technology in the US has been working with cryptographers worldwide to develop standardized quantum-resistant algorithms that follow stringent testing criteria. The entity is set to make its final selection public in 2022.

Researchers at Technology Innovation Institute's Cryptography Research Center have developed a post-quantum cryptography library that provides multiple schemes for public-key encryption, key encapsulation, and digital signatures. In addition, these researchers have found a way to simulate the efficiency of quantum computers in breaking cryptographic codes on classical computers. As this race between quantum physicists and cryptographers reaches a tipping point, there is increasing urgency for today's enterprises to make their operations crypto-agile by adopting quantum-resistant algorithms. It's crucial to proactively plan now to meet this looming threat.

We thank all those who contributed their insights to this report, and we hope you enjoy reading this introduction to post-quantum cryptography.

Dr. Ray O. Johnson
Chief Executive Officer, Technology Innovation Institute

CONTENTS

01 Executive summary **5**

Definitions 7

02 Fueling the quantum momentum **8**

03 Bracing for the power of quantum **10**

04 The path to a cryptographically relevant quantum computer **11**

05 The quantum threat to public-key cryptography **12**

06 Developing post-quantum cryptography **14**

Expected challenges 16

A hybrid transition? 17

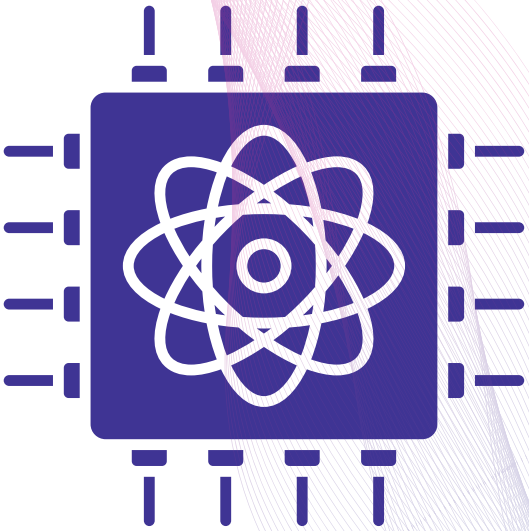
07 Conclusion **18**

What governments can do 18

What the C-Suite can do 19

No better time than now 20

01 Executive summary



When it comes to computing ability, the general rule of thumb is more is better. Quantum computers promise to feed this hunger. Their immense processing power derives from their ability to store and handle significantly larger volumes of data than classical bit-driven computers. As a result, a future quantum computer, in theory, could take minutes to solve problems that take classical computers tens of thousands of years.

The possibilities of such computing power are enormous. Sifting through libraries of molecular combinations to accelerate drug discoveries, tightening logistics planning, boosting computational chemistry, fine-tuning weather forecasting accuracy, and strengthening financial modeling are just a few of the many applications waiting in the wings.

However, one dark cloud lurks on the horizon. As quantum technology continues to advance, hackers can one day use this processing power to break public-key cryptography systems, which form the basis for today's secure interactions over the Internet, as well as other systems such as public-key infrastructure, code-signing systems, secure email, and key-management systems. Experts warn this is a major threat to modern digital security that needs to be tackled now. "It will completely break these crypto systems," says Dustin Moody, a mathematician at US-based National Institute of Standards and Technology (NIST).

Although a full-scale quantum computer has yet to become reality, the danger is imminent. Duncan Jones, head of cybersecurity at a Cambridge- and Colorado-based quantum computing company, Quantinuum, says he's concerned about a particular problem. "If I send you some encrypted data today and somebody records that, they can break into that later on," says Duncan. "They don't need a quantum computer today to break into it. They can just patiently sit on that data and they can then decrypt in the future."

As quantum technology continues to advance, hackers can one day use this processing power to break public-key cryptography systems, which form the basis for today's secure interactions over the Internet.

To defend against such quantum attacks, post-quantum cryptography is emerging as an efficient and effective solution. It refers to a set of new cryptographic algorithms, in particular public-key algorithms, that can be implemented using today's classical computers. There is growing urgency for enterprises of all sizes and across all industries, as well as public institutions and other organizations, to make their systems crypto-agile and adopt such quantum-resistant algorithms in their security frameworks. This report explores what enterprises and public institutions can do today – and how – to help protect against crippling attacks tomorrow.

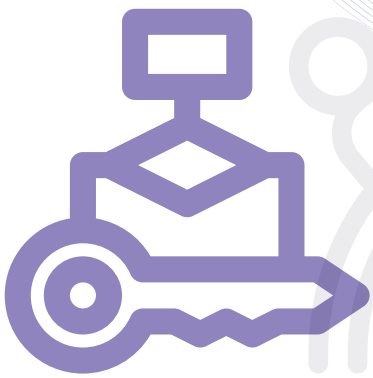
The key findings of this report:

Enterprises and organizations need to make their data and cyber systems resistant to quantum-based attacks now. While a cryptographically relevant quantum computer might still be years away, companies and organizations cannot afford to wait and see how the quantum-computing landscape evolves. Cyber threat actors could harvest sensitive data now and decrypt it later, which means protection needs to kick in today. A quantum-based attack could cripple an enterprise's bottom line. Given the high stakes, a proactive, rather than reactive, stance toward such threats becomes crucial.

A hybrid transition might be a good stepping stone. Enterprises and organizations unsure how to proceed with post-quantum cryptography can opt for a hybrid solution, which layers a quantum-resistant algorithm onto a classical one. Such a test drive allows them to understand how the new crypto framework might fit into their overall processes. A note of caution: while a hybrid approach is a cautious early measure, enterprises and organizations should not rely on it as a permanent safety net. They need to have a clear plan to transition from the hybrid to the post-quantum cryptography model.

It takes a village. Quantum computing involves contributions from various experts – physicists, cryptographers, computer scientists, and mathematicians. Enterprises and organizations need to beef up their quantum expertise by either hiring in-house talent or working with consultants. Recruiting a trusted resource or two to sift through the hype might pay rich dividends in the long run. Companies and organizations need to figure out how to benefit from the riches of quantum computing while protecting their systems from its problems. Expert advice can help them walk this fine line and increase their value propositions safely and securely.

Cyber threat actors could harvest sensitive data now and decrypt it later, which means protection needs to kick in today. A quantum-based attack could cripple an enterprise's bottom line.



Definitions

You will encounter the following terms in the report:

Quantum computing
A computing technique that harnesses the power of quantum mechanics to store data and perform computations hundreds of times faster than the world's best supercomputer.

Quantum cryptography
A type of cybersecurity that bases its security operations on physics, specifically quantum mechanics, to get the job done. Quantum key distribution uses this approach, using light, or rather photons – the particles that make up light – to securely transmit data.

Post-quantum cryptography
A math-based approach to cybersecurity in the quantum age. It's a set of algorithms that can run on classical devices and quantum devices to resist attacks from both classical and quantum computers. Quantum-resistant cryptography is another name for this approach.

Qubit
A subatomic particle like an electron or a photon that can be used to relay data. It is a basic unit in quantum computing, equivalent to a "bit" in classical computing. You can use microwaves or lasers to manipulate qubits. You also need to have sufficiently high numbers of qubits, so that they can deliver significantly more processing power than classical computers and break public-key cryptography.

Superposition, entanglement, and decoherence
Superposition is when a qubit can take on multiple states between just the two binary states that classical bits adopt, 0 and 1. These many states mean that a qubit can simply have more information coded into its DNA. In addition, pairs of qubits can group together – a process known as entanglement. They exist in a single state, so manipulating one will affect the other in a specific way. Such a process leads to an exponential increase in processing power when manipulated. However, qubits are extremely unstable and lose their desired state with the slightest external disturbance.

Quantum advantage and quantum supremacy
Quantum advantage is a milestone achieved in quantum computing when a quantum computer can perform a particular computation significantly faster than the best classical computer. Quantum supremacy is achieved when a quantum computer can develop a solution to a particular problem that no classical computer is able to handle – in a reasonable amount of time.

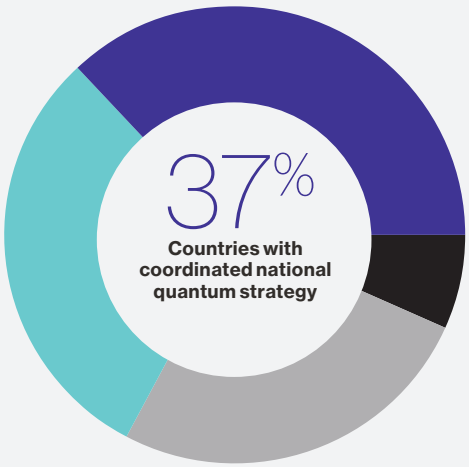
NISQ and CRQC
A noisy intermediate-scale quantum (NISQ) computer is one we have today and works with 50-100 qubits. It is an "intermediate-scale" quantum computer on the path to a full-fledged one. A cryptographically relevant quantum computer (CRQC) is one that poses a threat to public-key cryptographic systems and will need millions of qubits.

02 Fueling the quantum momentum

Quantum computers can store and process large volumes of data, making them capable of handling problems that classical computers cannot in a reasonable amount of time. The difference between a classical computer and quantum computer lies in the way they process or transmit data. A classical computer uses binary bits – either 0 or 1 – which can represent only one of those two values at a time. However, quantum computers use qubits that can simultaneously represent multiple possible states of 1 and 0. Qubits can also influence one another at a distance. As you entangle more and more qubits together, the ability of the system to make calculations increases exponentially, rather than in the linear fashion that characterizes a classical computer. Harnessing the power of quantum mechanics, quantum computing therefore promises to surpass even what today's fastest supercomputers can accomplish.

Figure 1: Quantum-technology R&D policies by country

The proportion of countries with and without coordinated quantum-technology strategies



30.4%
Countries with quantum strategy in development

26.1%
Countries without national strategy, but with significant government or government-endorsed iniatives

6.5%
Countries without significant initiatives but are participants in international quantum partnerships

COORDINATED NATIONAL QUANTUM STRATEGY

Austria	Iran	Slovakia
China	Israel	South Korea
France	Japan	Taiwan
Germany	Netherlands	United Kingdom
Hungary	Russia	United States
India	Singapore	

QUANTUM STARTEGY IN DEVELOPMENT

Canada	South Africa	Thailand

WITHOUT COORDINATED NATIONAL STRATEGY, BUT WITH SIGNIFICANT GOVERNMENT-LED OR ENDORSED INIATIVES

Australia	New Zealand	Switzerland
Denmark	Norway	United Arab
Finland	Portugal	Emirates
Ireland	Spain	
Italy	Sweden	

WITHOUT COORDINATED SIGNIFICANT INITIATIVES BUT ARE PARTICIPANTS IN INTERNATIONAL PARTNERSHIPS

Belgium	Estoria	Poland
Bulgaria	Greece	Romania
Croatia	Latvia	Slovenia
Cyprus	Lithunia	Turkey
Czech Republic	Malta	

Source: The Canadian Institute for Advanced Research, April 2021[1]

Governments and private companies around the world recognize the potential of quantum computing – which could create a "value of $450 billion to $850 billion in the next 15 to 30 years," according to estimates from a 2021 report from Boston Consulting Group[2] – and are working to develop their own quantum strategies and research initiatives. As of January 2021, 17 countries have "some form of national initiative or strategy to support quantum technology research and development" according to a May 2021 report from the Canadian Institute of Advanced Research (see Figure 1, page 8).[3] And private companies in countries like Japan have joined forces to develop their own initiatives. In late 2021, 25 Japanese companies, including Hitachi, Fujitsu, and Toshiba, jointly established a new strategic alliance called the Quantum Strategic Industry Alliance for Revolution (Q-STAR). Its mission is to position Japan as "a quantum technology innovation-oriented nation," according to a statement by Fujitsu on behalf of the group.[4]

In addition to governments, companies across the world have been pouring money into research in quantum technology (see Figure 2). On the private industry side, technology companies like those in the US and Japan – Google, IBM, Microsoft, Honeywell, Hitachi, Fujitsu, and Toshiba – are all invested in the high-stakes race. While quantum technology is still in its initial stages, the past few years have seen significant developments. In November 2021, IBM announced it had created a 127-qubit quantum processor[5], which more than doubled the size of those made by Google and researchers at the University of Science and Technology of China (USTC), and was also touted as the world's largest superconducting quantum processor. IBM's announcement came a few months after USTC said that its 66-qubit Zuchongzhi processor had surpassed Google's 54-qubit Sycamore[6], which the US search engine company announced in 2019 as having achieved "quantum supremacy" – a point at which a quantum computer can solve a problem that a classical computer would find impossible.[7]

Meanwhile, startups have also been hard at work. Canada-based Xanadu Quantum Technologies is developing a type of quantum computer based on the science of light waves; and US-based IonQ aims to commercialize a machine based on atomic particles called trapped ions.[8] Both companies use chips that can function at room temperature, which are different from those at IBM and Google with supercooling requirements. According to Pitchbook, venture capitalists invested $1.02 billion into quantum-computing companies in 2021 (as of September), more than the amount funneled into the industry during the previous three years combined.[9] In February 2022, Canada's D-Wave Systems added itself to the list of quantum computer developers seeking public listing in New York, following in the footsteps of IonQ, which became the first pure-play quantum computing startup to go public in October 2021.[10]

Quantum computing could create a value of $450 billion to $850 billion in the next 15 to 30 years, according to Boston Consulting Group.

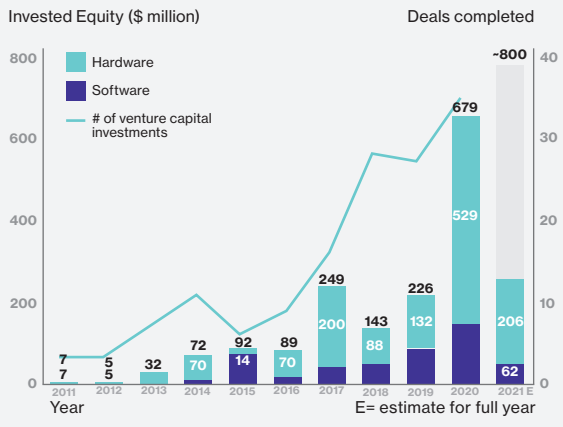
Figure 2: Equity investments in quantum computing

Two-thirds of equity investments in quantum computing were made between 2018 and 2020.

2/3
Two-thirds of all equity investments (~$1.3B) have come since 2018

$800M
Equity investments could reach a single-year record of ~$800M in 2021

73%
Nearly three-fourths of investments since 2018 have been in hardware



Source: Pitchbook (as of June 7, 2021) and Boston Consulting Group, 2021[11]

Bracing for the power of quantum

The arrival of full-scale quantum computing power is not a question of if, but when, as breakthroughs accelerate and investment dollars pour into the industry. Quantum technology has the potential to boost advances in various fields, from materials science to pharmaceuticals research, which companies are hoping to harness. For example, IonQ and South Korean automaker Hyundai Motor announced in early 2022 that they have formed a partnership to focus on using quantum computing to study lithium compounds and battery chemistry.[12]

While enterprises are eager to tap into the new opportunities quantum computers deliver, the emergence of a powerful quantum computer is also a cause for concern because hackers could use one to break the best digital defenses in the world. To understand how, picture a safe that can be cracked if you know the right combination to the lock. You have to systematically try one combination after another. Hackers use computers to find all the combinations faster so they can breach systems more easily.

Fortunately, today's public cybersecurity defenses have extremely hardy locks. Even the most powerful supercomputer today cannot compute how to break them. But quantum computing could eventually change this – today's quantum computers aren't extremely powerful, but they are getting there rapidly. It's possible that in a little more than a decade – and perhaps even sooner – hackers could use the processing power of quantum computers to break today's encryptions that protect all kinds of web-based communications and protocols.

It's possible that in a little more than a decade – and perhaps even sooner – hackers could use the processing power of quantum computers to break today's encryptions that protect all kinds of web-based communications and protocols.

04 The path to a cryptographically relevant quantum computer

A quantum computer powerful enough to pose a threat to today's public-key cryptography systems – used to secure most web-based transactions – is called a cryptographically relevant quantum computer (CRQC). A CRQC needs millions of qubits to work. Such a computer does not yet exist. IBM's 127-qubit quantum computer aside, most quantum computers today are on the noisy intermediate scale quantum (NISQ) level of 50 to100 qubits. They are very sensitive to the environment and susceptible to interference, which makes them unreliable.

Professor Jian-Wei Pan at the University of Science and Technology of China (USTC), points out that the path to a CRQC will be paved with incremental steps. Pan says two quantum computers under his direction, Zuchongzhi and Jiuzhang, have already achieved quantum advantage, which is the point reached when a quantum computer can significantly outperform the best classical computer to process a particular computation.

"The final and most challenging stage is building programmable universal quantum computers, which could have a high impact on cracking classical encryption systems, big-data-set searches, and artificial intelligence," Pan says. Such impact is a concern for cybersecurity teams, although it's still debatable how soon the world will get to such a CRQC. "Given the current state of quantum computing, we hope to achieve the last goal through a 15- to 20-year effort," Pan says. For others, the view is hazier. "There is a lot of progress and a lot of money invested, so because of this it's very difficult to forecast the rate of progress," says Grégoire Ribordy, co-founder and chief executive officer of Geneva-based ID Quantique, a subsidiary of South Korea's wireless carrier SK Telecom that offers commercial quantum-cryptography solutions for data protection.

Both public and private sectors are leaning in on their efforts to build a quantum computer that could deliver promised riches. Against this backdrop, experts say we need to transition to post-quantum cryptography now. "The time to do something about protecting your assets was yesterday," says Tony Uttley, president and chief operating officer at Quantinuum, a quantum computing firm created from a merger between Honeywell Quantum Solutions and Cambridge Quantum. "And if you haven't already done something about it, the next best time to do it is today."

"The final and most challenging stage is building programmable universal quantum computers... given the current state of quantum computing, we hope to achieve the last goal through a 15- to 20-year effort."

Jian-Wei Pan, Professor of Physics, University of Science and Technology of China

05 The quantum threat to public-key cryptography

Cryptography works by using a set of keys in combination with encryption and decryption algorithms to securely send messages. The original message is scrambled with an encryption algorithm, before it's locked with a secret key and sent. When the message reaches the recipient, the message is decoded (unlocked) by using a secret key and a decryption algorithm.

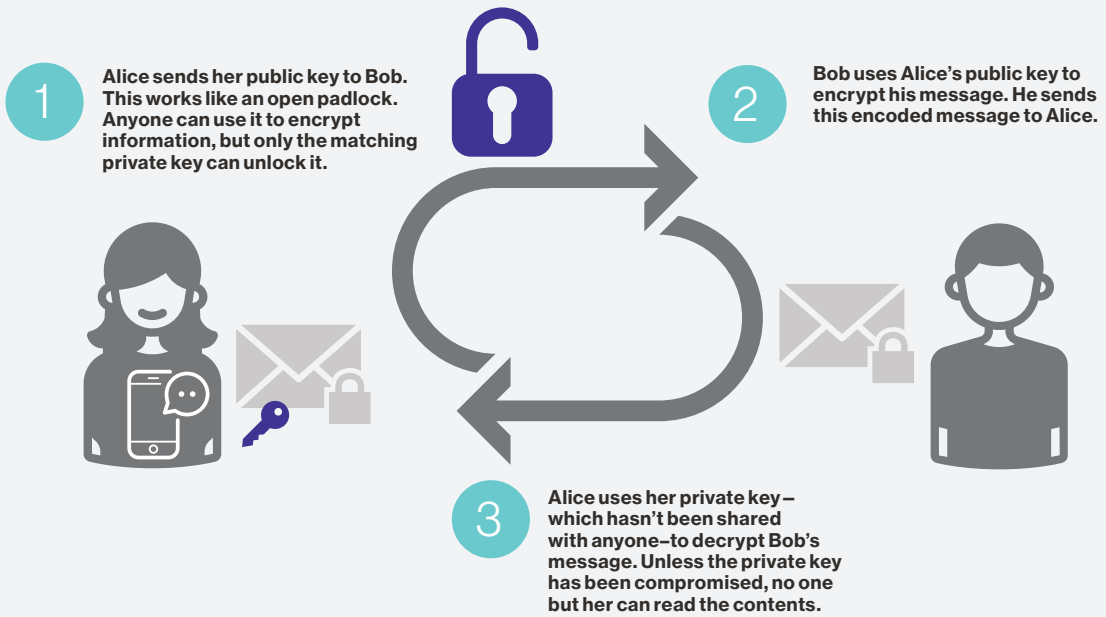
In symmetric encryption, the digital keys for encryption and decryption are identical. In asymmetric encryption, a publicly available key is used to encrypt – this is why this method is also known as public-key cryptography – but the message is decrypted with a private key (see Figure 3, page 13).

Public-key cryptography makes robust authentication, encryption, key exchange, and digital signing possible, and it forms the basis of today's numerous Internet security standards. Standardized algorithms that form the basis of the encryption keys in today's public-key cryptography are widely used and effective. They are usually based on the assumption that the private keys are secure because they are derived from mathematical algorithms that are intractable or impossible to reverse-engineer. The popular Rivest-Shamir-Adleman (RSA) algorithm is one example. It operates on the theory that multiplying two large prime integer numbers to arrive at an answer is easy. But it is difficult to perform this operation in reverse. Which means, given a large number, it is difficult to tell which two prime numbers it would break down into.

Industry professionals are worried that hackers could be able to decipher the "key" to public-key encryption algorithms using quantum computing. Indeed in 1994, mathematician Peter Shor, then working at Bell Labs but currently a professor at Massachusetts Institute of Technology, discovered an algorithm that would effectively cripple RSA. The only condition: It would need to run on a CRQC.

Given the pace of advances and investments in quantum computing, it's only a matter of time before defenses are overpowered. Financial transactions, military strategies, proprietary information, healthcare systems, online shopping, social media apps, and more could be vulnerable once this happens.

Figure 3: How public-key cryptography works



Source: CBInsights, 2021[13]

Although a CRQC has yet to be achieved, cryptography experts warn that today's public-key methods are vulnerable. Given the pace of advances and investments in quantum computing, it's only a matter of time before defenses are overpowered. Financial transactions, military strategies, proprietary information, healthcare systems, online shopping, social media apps, and more could be vulnerable once this happens. For security systems that use public-key cryptography to protect sensitive information, failure to prepare for the advent of a CRQC is like playing with fire. "Given the impact, it is important to prepare not based on an optimistic scenario that a fully capable quantum computer will come late, but by building some margin of security," Ribordy says. The other concern is that threat actors might already be harvesting data now to decrypt it later. Federal agencies store classified information for decades and are vulnerable to the harvest-now-decrypt-later approach.

06 Developing post-quantum cryptography

To achieve hack-proof – or at least hack-resistant – security that will not buckle when attacked by a CRQC, the industry is trying approaches based on physics and mathematics. Quantum cryptography uses quantum mechanics to transmit data securely. A process called quantum key distribution drives this approach. The mathematics-rooted process for security is called quantum-resistant cryptography, or post-quantum cryptography, and relies on a set of robust mathematical algorithms that can withstand quantum-computing attacks.

Much of the attention in post-quantum cryptography has been focused on algorithms that are being culled and standardized in the US by the National Institute of Standards and Technology (NIST). In 2016, NIST launched a public call for quantum-resistant algorithms. Over the years, it has narrowed down the original 69 submissions to 15 and subjected those remaining to additional reviews.

In the first half of 2022, NIST expects to release a first set of standardized algorithms that will proceed to a fourth round of further study. "We have also said that we are going to issue a new call for more public-key signatures because we want to have diversity in our portfolio," says Dustin Moody, a mathematician at NIST, who is leading the institute's post-quantum cryptography project.

While the NIST competition has made headlines in recent years, it's not the only work concentrated on post-quantum cryptography. Companies and public institutions around the world are creating libraries of standardized algorithms that can withstand the threats that advanced quantum

"Standardization ensures that you can use a secure crypto system because you're working with an algorithm that has been evaluated and vetted, and as long as you implement it as the standard says, you can trust its security."

Dustin Moody, Mathematician, National Institute of Standards and Technology

computers pose. In December 2021, Coinbase, the largest US cryptocurrency exchange, announced the launch of an open-source cryptography library that contains tools for developers to help enhance the security of transactions.[14]

In March 2021, the Abu Dhabi-based Technology Innovation Institute (TII) also unveiled the United Arab Emirates' first cryptography library that contains a collection of algorithms to safeguard confidential data and information.[15] TII is also developing a framework with which government entities and enterprises can enable crypto-agility. "Our talent bench comprises mathematicians, software developers, and cryptographers, who design and develop these algorithms internally," says Najwa Aaraj, the chief researcher at TII's Cryptography Research Center. Aaraj says that clients approach the center with their specific post-quantum cryptography needs and TII understands the clients' technology assets before recommending specific algorithms from their library.

In South Korea, telecom company LG Plus, has been focusing on the development of post-quantum cryptography algorithms and The Chinese Association for Cryptologic Research hosted its own competition for quantum-resistant algorithms in 2020.[16,17] China is said to be developing its own set of algorithms under the direction of the Office of State Commercial Cryptography Administration.[15] Experts in Europe too have voiced concerns that the US has taken the lead in post-quantum cryptography and urged the continent to focus its energies in the field.[18]

As the NIST competition draws to a close, the institute's next steps will be to standardize an initial set of quantum-resistant algorithms. Standardization "ensures that you can use a secure crypto system because you're working with an algorithm that has been evaluated and vetted," Moody says, "as long as you implement it as the standard says, you can trust the security of using a good, safe algorithm."

Recipe for a robust quantum-resistant algorithm

What factors make a good quantum-resistant algorithm? Dustin Moody, head of the post-quantum cryptography project at the National Institute of Standards and Technology in the US, checks off the following requirements for a robust quantum-resistant algorithm:

1. Security While this might seem obvious, the ability of an algorithm to constitute a hack-resistant defense against a fully functional quantum computer is a basic requirement.

2. Performance The efficiency of an algorithm will drive the ease of adoption. Key size is an important consideration for efficiency because the bandwidth needed to complete data transmission increases with key size. Today's algorithms are in the low 100s of bytes. NIST's post-quantum finalists are going to be 10 times that size. "Luckily for most applications, that little bit of bigger bandwidth requirement is not going to be a problem," Moody says.

3. Speed Key size also determines speed of data transfer, which is a significant factor that dictates adoption. The larger the key size, the slower the speed of data transmission. Because users prioritize speed, they are likely to settle for faster but less secure options, which would be a concern.

4. Shareability Quantum-resistant algorithms need to be shared freely, but companies are less likely to adopt them if the solutions are bound by intellectual property rights and patent laws.

5. Cost The costs associated with adopting quantum-resistant algorithms might not faze large companies, but present questions of equity. Not all enterprises and government organizations will be able to afford the monetary investments needed to secure their data first, leaving the others vulnerable. A low-cost solution is ideal to decrease this barrier to adoption.

Expected challenges

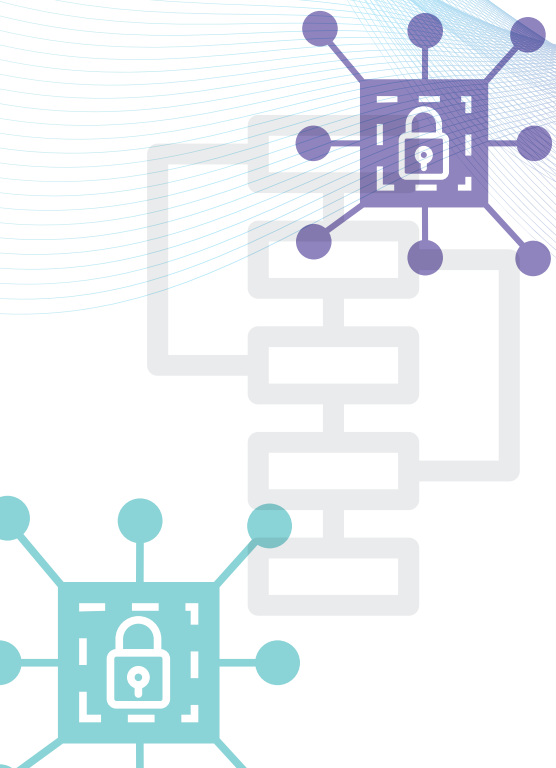
Challenges related to post-quantum cryptography fall into two buckets: those directly related to the development of the algorithms themselves and those related to barriers to widespread adoption.

For one thing, it's difficult to truly measure the strength of a quantum-resistant algorithm without the development of a fully operational quantum computer. Such a catch-22 situation means that until such a computer exists to test robustness, simulations are the next best thing. Indeed, to combat this problem, the development of quantum-resistant algorithms will be iterative and ongoing, Moody predicts. NIST expects to move on with the first round of vetted algorithms and continue standardization in the wake of additional research. "There will be ongoing standardization that occurs in the future as more research happens," he says. "We will standardize other algorithms." That does not mean that enterprises should wait. "These first ones [to be standardized] are the ones that we anticipate will be for primary, general-purpose use. So we want people to start using these but standardization will continue into the future."

Next are adoption headaches. While the NIST-proposed standard for public-key cryptography has been a hit, a similar process for the adoption of quantum-resistant algorithms is far from guaranteed. "The biggest challenge will be to communicate so that people know the threat, know that we have solutions and encourage adoption of standardized algorithms," Moody says.

Switching to a post-quantum cryptography system will be resource-intensive in terms of effort and cost. New algorithms might slow the speed of transactions; networks and supporting infrastructure might have to grow in parallel to accommodate a greater demand on resources without compromising speed. "We need to make it clear that even though there's going to be a cost and it's not going to be easy, that it's a transition that [companies] need to do sooner than later," Moody says. NIST plans to issue guidance for adoption as part of its efforts to address these challenges. Candidates from around the world have participated in the NIST open call for quantum-resistant algorithms, but not all countries will adopt the NIST-standardized algorithms.

Jung Hee Cheon, professor of mathematics at Seoul National University in South Korea, and director of the Industrial and Mathematical Data Analytics Research Center in Seoul, says that a few countries – South Korea, China, and the UAE among them – are following their own paths to a library of quantum-resistant algorithms. It will become a case of letting the best algorithm win, predicts



"A few countries–including South Korea, China, and the UAE–are following their own paths to a library of quantum-resistant algorithms. It will become a case of letting the best algorithm win."

Jung Hee Cheon, Professor of Mathematics, Seoul National University

Cheon, who is also the founder of data-security startup Cryptolab. "I think the market or enterprise can have options to choose from," he says.

In addition, adoption of quantum-resistant algorithms will be challenging because the benefits are not clearly visible, Cheon says. It is a problem related to all cybersecurity – all is fine when systems chug along securely, but everybody complains when something breaks. Despite the lack of visibility, Cheon believes adoption is crucial. "The cost will blow up if it is adopted after quantum computers are established," he cautions.

A hybrid transition?

To ease the move to post-quantum cryptography, industries and governments are eyeing a hybrid approach, layering a quantum-resistant algorithm with one already in use today. The logic is that if one layer of security is compromised, then you can still lean on the other for protection.

Najwa Aaraj, the chief researcher at TII's Cryptography Research Center says we will need a lot of groundwork to prepare for a post-quantum landscape. First, enterprises need to ensure crypto-agility so they can adopt new quantum-resistant algorithms more easily. "Most of the systems [even] today do not have code modularity, which means you cannot simply layer or switch out code," she says. In such cases, transition to post-quantum cryptography will take a lot more groundwork. "Those systems will have to have code bases and libraries refactored for us to be able to replace classical crypto schemes with the hybrids," Aaraj points out.

Enterprises and governments that plan to rely on a hybrid model as a path to quantum-resistant cryptography also need a clear exit strategy to wean themselves off that model. "There will be a phase where companies can adopt hybrid approaches as long as [they] ensure that there is a clear path to moving to post-quantum later on, while maintaining compatibility," Aaraj says. Enterprises should not use classical and insecure algorithms as a safety net for longer than necessary.

> "There will be a phase where companies can adopt hybrid approaches as long as [they] ensure that there is a clear path to moving to post-quantum later on, while maintaining compatibility."
>
> Najwa Aaraj, Chief Researcher, Cryptography Research Center, Technology Innovation Institute

07 Conclusion

Advances in quantum computing are likely to significantly disrupt public-key cryptographic systems. Today's classical devices need to be protected from devastating attacks by hackers who may use quantum technology – when it is fully developed – for their own gains. Proactive security will necessitate a concerted effort from both public and private sectors to develop a rigorous plan to embrace post-quantum cryptography and adopt the standardized algorithm that works for their technology systems.

What governments can do

Governments around the world have realized the necessity of shoring up cybersecurity defenses against advanced quantum computers. Actions they need to carry out follow two tracks:

- Pave the path for legislation related to quantum computing
- Prepare their own networks for the transition to post-quantum cryptography

Aaraj is concerned that many federal entities around the world are underprepared for what's coming and are leaving their critical infrastructure exposed through data that is being stored now and can be decrypted, or attacked, later. The problem is rooted in a lack of thorough knowledge about what assets they even have. "Information governance is missing in a lot of places, so an inventory of information and crypto assets does not exist," Aaraj says. Without a thorough assessment of current inventory, it will be challenging to understand which systems need a heavier lift during the transition. Outlining vulnerable assets is therefore an essential early step in making the switch to post-quantum cryptography. Recognizing this problem, the US White House issued a national security memorandum in January 2022, to give agencies 180 days to conduct an inventory of their encryption systems and report the ones not following quantum-resistant algorithms.[19]

Governments also need to set the stage for advancements in the field by investing in research. While the private sector conducts its own projects in quantum computing, it's important for governments to support the development of quantum computing as well.

In addition to investing in research, governments can encourage legislation. Establishing laws will help governments visibly demonstrate their commitment to the field and provide a much-needed framework to measure progress toward specified goals. Much of the quantum-related federal government activity in the US stems from the National Quantum Initiative Act of 2018, which allocated $1.25 billion in funding over five years to increase the pace of quantum research and development.[20] The National Quantum Coordination Office (NQCO), one of the products of this act, coordinates quantum-information science activities across the US federal government, industry, and academia. The National Defense Authorization Act (NDAA)

Without a thorough assessment of current inventory, it will be challenging to understand which systems need a heavier lift during the transition. Outlining vulnerable assets is therefore an essential early step in making the switch to post-quantum cryptography.

Much like the theory of the weakest link, ensuring that the cybersecurity systems of all countries progress on similar tracks will be key to cybersecurity defenses around the world. Governments should actively share resources and insights.

of 2021, which mandates an evaluation of the threat to national security systems, has also boosted quantum research and provided threat-related funding. Meanwhile, experts say the European Union – already well known for its data-security and privacy law, the General Data and Protection Regulation – should update its laws to include the threat posed by quantum computing.[21]

Much like the theory of the weakest link, ensuring that the cybersecurity systems of all countries progress on similar tracks will be key to cybersecurity defenses around the world. Governments should actively share resources and insights. Agreements in recent years show this is already taking place: in 2019, Japan and the US signed an agreement to collaborate on research in quantum-information science and technology.[22] At the same time, a fair number of governments are setting up their own processes to develop quantum-resistant algorithms. Governments can encourage the adoption of such algorithms through incentives. They can raise awareness of the threats posed by future quantum computers, encourage the transition to post-quantum cryptography, and build trust by leading the transition to standardized quantum-resistant algorithms themselves, Moody says.

What the C-Suite can do

Eighty-nine percent of the more than 3,000 C-suite executives surveyed by IBM Institute for Business Value for a 2021 CEO study didn't see quantum computing as directly relevant to delivering business results in the next two to three years.[23] This stance doesn't place quantum computing and its possibilities in the right context. Businesses need to start now to prepare for what's coming and begin the transition to post-quantum cryptography. Enterprises that work with sensitive and valuable information must act with a sense of urgency, but the problem is not limited to such businesses alone, warns Duncan Jones, head of cybersecurity at Quantinuum. "You can get caught in the crossfires of sophisticated cyberwarfare."

The C-suite needs to stay updated about the latest developments in the field. "Where are we in relation to a cryptographically relevant quantum computer?" "What is the latest in the industry?" These are the questions to keep asking, says William Hurley, chief executive officer of Strangeworks, who describes his startup as one that focuses on humanizing quantum computing and making it accessible to everyone. "The reason is that there is so much happening in quantum right now that what you think is 10 to 20 years away may actually take place in less than three or four years and will create entirely new challenges that we will have to address, challenges we've never before thought of in cybersecurity," he says. For University of Science and Technology of China's professor Pan, the "quantum world is a bizarre one for those of us living in the classical world." Every little bit helps, Pan says. "A moderate familiarity with quantum computing can help one quickly pick up the advances in the cutting-edge field." Enterprises will have to lean on expertise, either through internal hiring or by tapping consultants' expertise.

Much like governments, all private industries need to take stock of their assets and include them in a plan in the transition to post-quantum systems. They also need to evaluate the flow of information to and from enterprise systems. The principle of basic cybersecurity hygiene – you are only as safe as your weakest link – also applies to the transition to post-quantum cryptography. "You can have all the post-quantum cryptography in the world and be 'fully protected' against a quantum attack but if you have a vendor who is not, then it becomes entirely irrelevant," Hurley points out. The solution: ensure quantum adoption beyond your immediate internal enterprise. Set up an exercise to trace how data flows – and from where – and how the company stores it. This applies to data in transit, including processing and transferring data.

Crypto-agility is key, Aaraj says. A company's technology stack needs to be modular and able to accommodate the quantum-resistant algorithms that are coming down the pike. Enterprises need to understand compatibility of both internal crypto assets and the external ones they work with, she says. Understanding these relationships will be crucial to make the transition to post-quantum cryptography.

Enterprises need to choose the scheme that works for their implementation needs. In the library of standardized quantum-resistant algorithms, a few will work for digital signatures, others for true encryption. Sizes of keys and signatures will come into play, as will bandwidth considerations. "Enterprises need to understand the limitations of the systems on which those crypto systems will be deployed and then choose the right candidate," Aaraj says.

Making a clean break will necessitate having a clear life-cycle management policy for algorithms – when to include them, what kind of public-key infrastructure they will need, and when to retire them. This is particularly relevant when considering a hybrid transition. A hybrid model will work if a clear plan for taking the next step to post-quantum cryptography is in place.

Creating a framework to adopt quantum-resistant algorithms today will accelerate the transition to post-quantum cryptography for businesses and public institutions.

No time better than now

Adoption of quantum-resistant algorithms may not happen overnight, but it needs to happen sooner rather than later. The harvest-now-decrypt-later approach that rogue cyber threat actors are adopting to procure sensitive data is real, and enterprises and governments need to prepare accordingly.

Enterprises and organizations can start today by ensuring their security systems are:

- Modular
- Crypto-friendly
- Ready to integrate with post-quantum cryptography

As enterprises familiarize themselves with the lay of the land, a hybrid model to the transition might be a good idea. But companies need a clear plan for when and how to complete the move to post-quantum cryptography. As Aaraj puts it: "Enterprises need to protect themselves today against the technology of tomorrow."

> "There is so much happening in quantum right now that what you think is 10 to 20 years away may actually take place in less than three or four years and will create entirely new challenges that we will have to address, challenges we've never before thought of in cybersecurity."
>
> William Hurley, Chief Executive Officer, Strangeworks

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of *MIT Technology Review,* the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review Global Insights Panel has unparalleled access to senior-level executives, innovators, and thought leaders worldwide for surveys and in-depth interviews.

From the sponsor

The Technology Innovation Institute (TII) aims to become a leading global research center dedicated to pushing the frontiers of knowledge. Our teams of scientists, researchers and engineers work in an open, flexible and agile environment to deliver discovery science and transformative technologies. Our work means we will not only prepare for the future; we will create it. Working together, we are committed to inspiring innovation for a better tomorrow. We are part of Abu Dhabi Government's Advanced Technology Research Council, which oversees technology research in the emirate. As a disrupter in science, we are setting new standards and serve as a catalyst for change.

Illustrations
Cover art and spot illustrations created with Adobe Stock and The Noun Project.

Footnotes

1. Canadian Institute for Advanced Research, "A Quantum Revolution - Report on Global Policies for Quantum Technology," May 2021, p. 12 and p. 13.

2. Jean-François Bobier, Matt Langione, Edward Tao, and Antoine Gourévitch, "What Happens When 'If' Turns to 'When' in Quantum Computing?" Boston Consulting Group, July 21, 2021.

3. Fujitsu, "Establishment of Quantum Strategic Industry Alliance for Revolution (Q-STAR)," September 1, 2021.

4. Canadian Institute for Advanced Research, "A Quantum Revolution - Report on Global Policies for Quantum Technology," May 2021, p. 12 and p. 13.

5. Matthew Sparkes, "IBM creates largest ever superconducting quantum computer," NewScientist, November 15, 2021.

6. Bob Yirka, "Chinese achieve new milestone with 56 qubit computer," Phys.org, July 12, 2021.

7. Elizabeth Gibney, "Hello quantum world! Google publishes landmark quantum supremacy claim," Nature, October 23, 2019.

8. Sara Castellanos, "Xanadu Lands $100 Million as Investments Pour Into Quantum Computing," The Wall Street Journal, May 25, 2021.

9. Marina Temkin, "Investors bet on the technologically unproven field of quantum computing," PitchBook, September 13, 2021.

10. Sean Silcoff, "Canadian quantum computer pioneer D-Wave to go public on NYSE in US$340-million SPAC deal," The Globe and Mail, February 8, 2022.

11. Jean-François Bobier, Matt Langione, Edward Tao, and Antoine Gourévitch, "What Happens When 'If' Turns to 'When' in Quantum Computing?", Boston Consulting Group, July 21, 2021.

12. Paul Smith-Goodson, "Can Quantum Battery Research Extend Electric Vehicle Range? IonQ And Hyundai Intend To Find Out," Forbes, February 9, 2022.

13. CBInsights, "Post-Quantum Cryptography: A Look At How To Withstand Quantum Computer Cyber Attacks," August 25, 2021,

14. Zhiyuan Sun, "Coinbase launches open-source cryptography library Kryptology," Cointelegraph, December 6, 2021.

15. Technology Innovation Institute, "Abu Dhabi's TII Unveils First Post-Quantum Cryptography Library in UAE," March 29, 2021.

16. Han-Gyeol Seon, "Korean telecom firms expand commercial use of quantum cryptography," The Korea Economic Daily, June 9, 2021.

17. Davide Castelvecchi, "The race to save the Internet from quantum hackers," Nature, February 8, 2022.

18. André Loesekrug-Pietri, "It's not too late for Europe to lead the post-quantum cryptography race," Sifted, August 30, 2021.

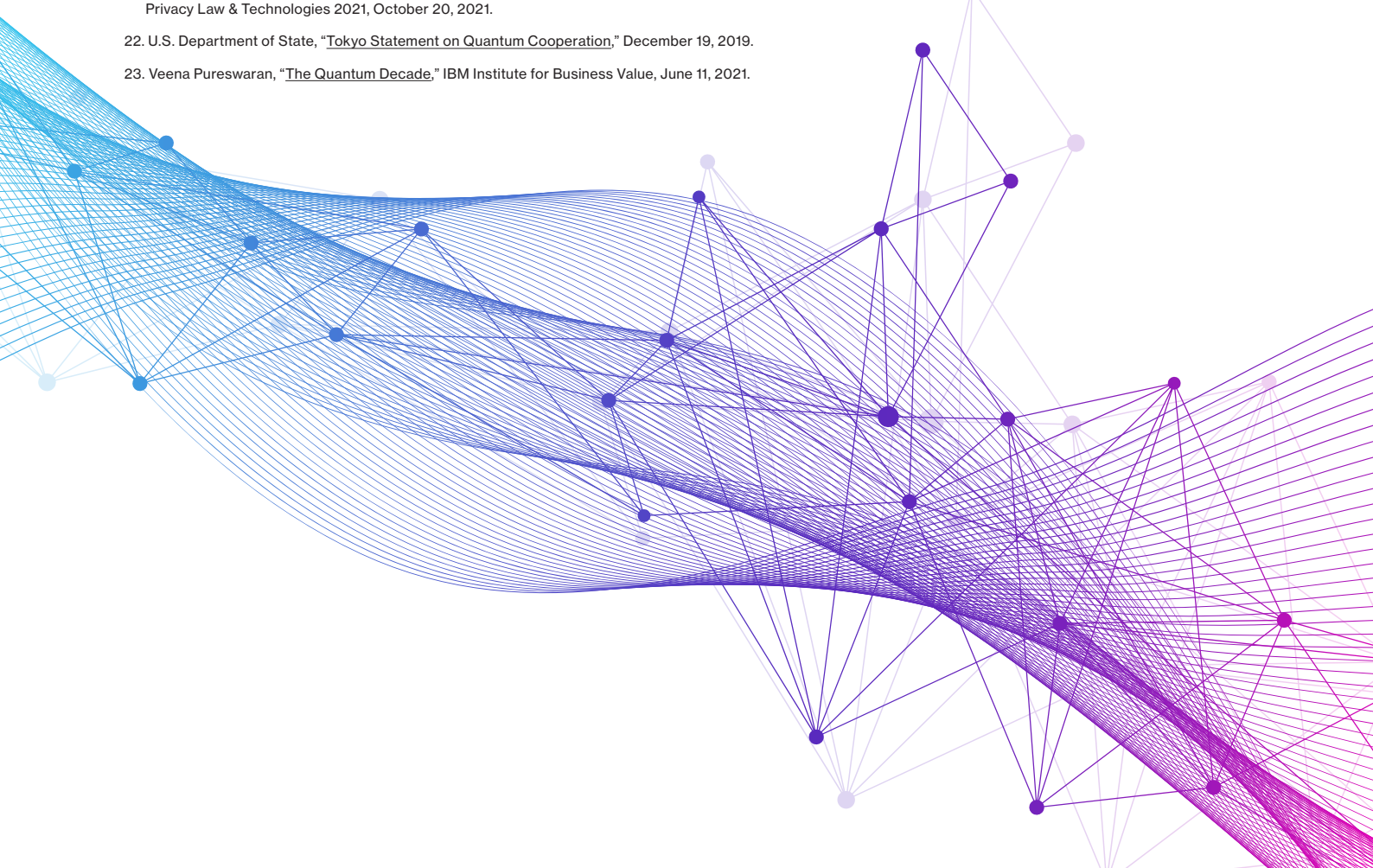
19. The White House, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022.

20. American Institute of Physics, "National Quantum Initiative Act - H.R.6227 / S.3143," December 21, 2018.

21. Luigi Bruno and Isabella Spano, "Post-Quantum Encryption and Privacy Regulation: Can the Law Keep Pace with Technology?," European Journal of Privacy Law & Technologies 2021, October 20, 2021.

22. U.S. Department of State, "Tokyo Statement on Quantum Cooperation," December 19, 2019.

23. Veena Pureswaran, "The Quantum Decade," IBM Institute for Business Value, June 11, 2021.



MIT Technology Review Insights

www.technologyreview.com
@techreview @mit_insights
insights@technologyreview.com