Headline

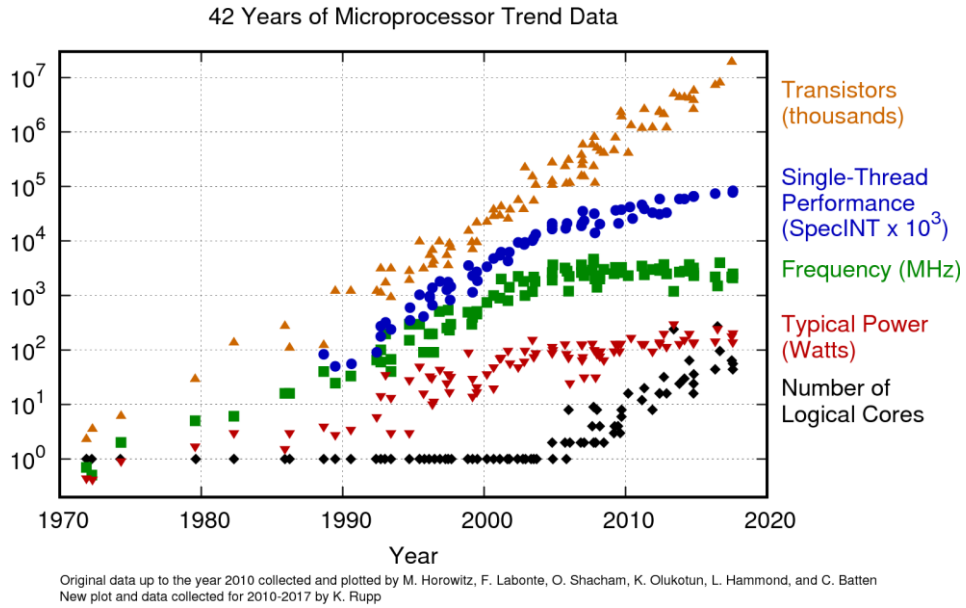
Security threats and response plans to address the advancement of quantum computing technology

Yeong-taek Yu / EQST Financial Business Team Senior Consultant

■ Overview

In 1936, Alan Turing proposed the Turing machine in his paper "On Computable Numbers, with an Application to the Entscheidungsproblem," suggesting a way to solve mathematical problems mechanically. Based on this theoretical model that became the foundation of computer science, the first general-purpose electronic computer, ENIAC (Electronic Numerical Integrator and Computer), was born in 1945. It could perform mathematical calculations quickly for the US military using thousands of vacuum tubes.

Afterward, in 1947, transistors with the advantages of small size, low power consumption, and high durability were invented, replacing vacuum tubes. Computer performance has increased dramatically, leading to today's tremendous performance advancements since transistors became the basis for integrated circuits (ICs).

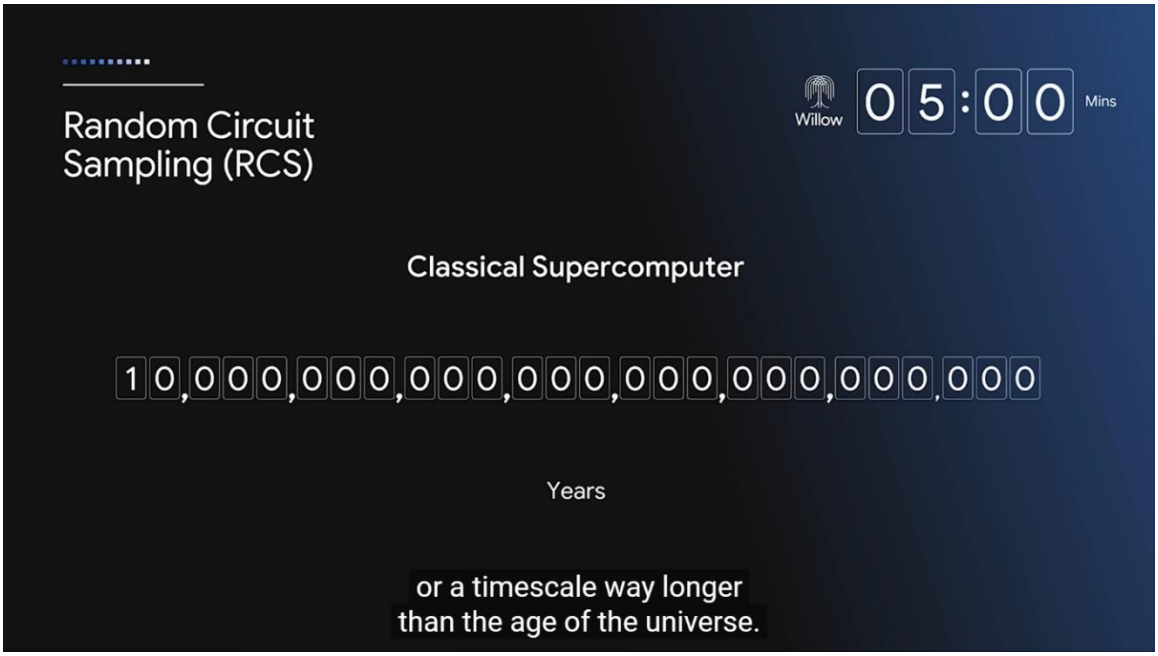


* Source: https://www.karlrupp.net/wp-content/uploads/2018/02/42-years-processor-trend.png

Figure 1. 42 Years of Microprocessor Trend Data

Driven by advances in hardware, AI based on cloud and deep learning has been driving the greatest innovation in human civilization in recent years. However, today's computers have reached the limits of transistor integration and performance and are facing various technological challenges, such as technological limitations in fine processes, power consumption and heat generation issues, and limitations in parallel processing. Humanity stands at the doorstep of another huge innovation: the development of quantum computers, as one way to overcome these problems.

On December 10, 2024, Google Quantum AI Lab introduced the quantum chip Willow and announced that Willow could perform the RCS (Random Circuit Sampling) benchmark calculation, which takes the fastest supercomputer in existence, 10 septillion years, in less than 5 minutes.



* Source: https://www.youtube.com/watch?v=W7ppd_RY-UE&ab_channel=GoogleQuantumAI

Figure 2. Willow Chip's RCS benchmark

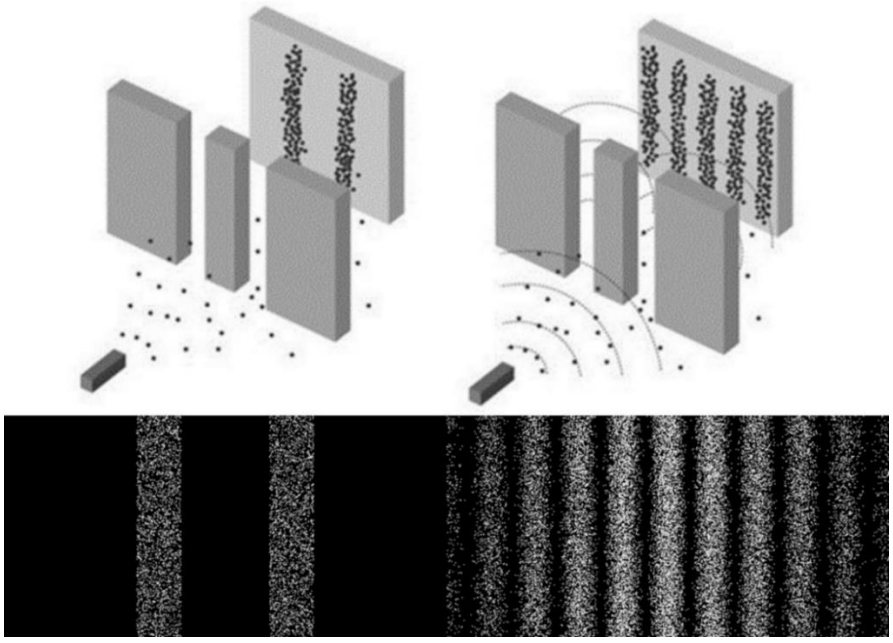
Although a fully commercialized quantum computer has not yet been developed, much progress is being made now. Therefore, issues regarding security threats arising from the development of quantum computers have recently emerged worldwide.

■ What is a quantum computer?

In 1981, American theoretical physicist Richard Feynman argued that classical computers have limitations in accurately modeling the laws of nature. He said that since nature follows the laws of quantum mechanics, we need to create a quantum computer that behaves in the same way as nature. Classical computers handle binary data 0 and 1 by controlling the ON state when current flows and the OFF state when there is little or no current. Therefore, the basic unit is a bit, which is always in one of two states: 0 and 1. On the other hand, quantum computers use quantum bits (qubits) that utilize quantum superposition and quantum entanglement, which are the basic principles of quantum mechanics.

- Quantum Superposition

Quantum superposition is the property that allows a quantum state to exist in multiple states simultaneously. In classical physics (macroscopic world), an object cannot exist in multiple locations at the same time and has only one state. However, in the microscopic world, multiple states exist probabilistically in a single quantum, and the exact state cannot be known until measurement is made. In other words, the condition is determined when a measurement is made. This phenomenon can be observed in the "double-slit experiment" of electrons, which is the trigger for thinking about quantum superposition.



(Left) When observation was made (Right) When no observation was made

* Source: https://m.blog.naver.com/iotsensor/222929618559, wikimedia

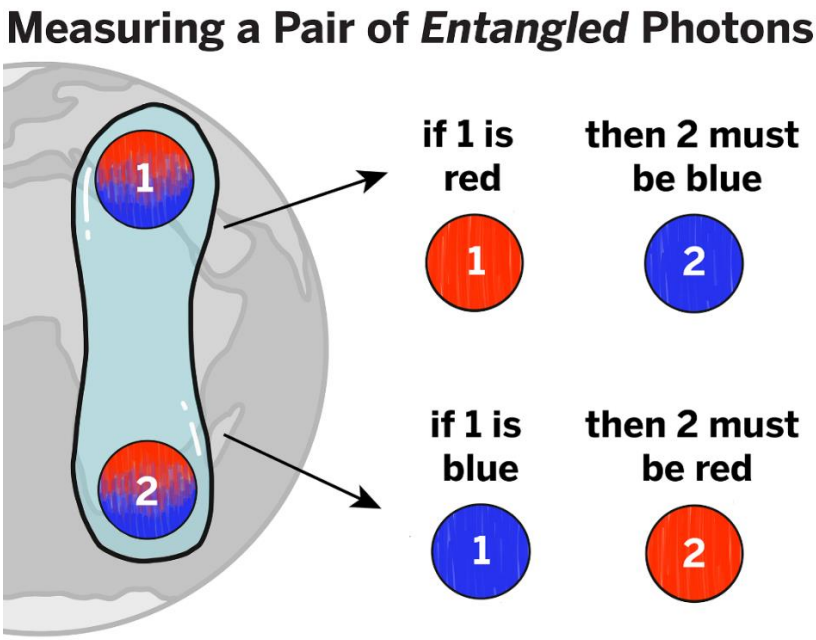
Figure 3. Double-slit experiment

When firing electrons into the double slits one by one randomly, if observed, only two lines appear on the screen, as in the two slits on the left. It is a result that common people can easily understand. However, if not observed, an interference pattern appears, like a wave of water or light, as shown on the right.

This result means that the electrons passed through both slits at the same time, like a wave of light or water, and that one electron exists in two places at the same time. In conclusion, an electron can exist simultaneously in every place. This phenomenon is called quantum superposition.

- Quantum entanglement

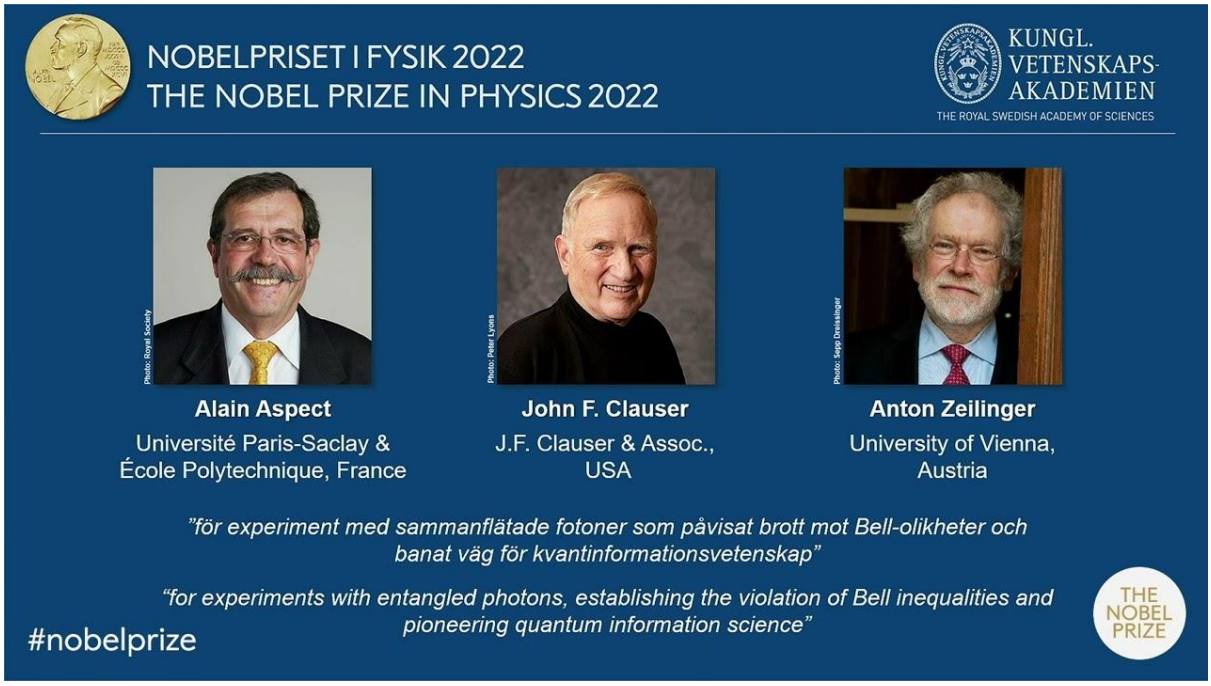
When two unmeasured (in the quantum superposition state) particles are spatially separated, quantum entanglement refers to the phenomenon in which when the quantum state of one particle is measured and determined, the other particle's state is also determined simultaneously. If two particles are in a state of quantum entanglement, if the spin state of one particle is determined to be up, the spin state of the other particle is determined to be down no matter how far apart they are. In nature, there are also cases where a pair of photons are produced simultaneously, and the two photons are in an entangled state with different polarization directions(horizontal and vertical). When two photons are in a superposition state with their polarization directions being vertical or horizontal, if the polarization direction of one photon is determined to be horizontal through measurement, the polarization direction of the other photon is immediately determined to be vertical.



* Source: https://quantumatlas.umd.edu/entry/entanglement/

Figure 4. Quantum superposition

Alain Aspect, John F. Clauser, and Anton Zeilinger were awarded the 2022 Nobel Prize in Physics for their contributions to demonstrating the phenomenon of quantum entanglement and ushering in the era of quantum technology.



* Source: https://www.nobelprize.org/prizes/physics/2022/prize-announcement/

Figure 5. Alain Aspect (left), John F. Clauser (center), and Anton Zeilinger (right)

Qubits with these properties of quantum superposition and quantum entanglement are in a superposition state where 0 and 1 exist simultaneously, and the two states can be calculated in parallel at the same time. If a quantum computer uses three qubits, it can simultaneously compute 2^3=8 states at once. In contrast, a classical computer would need to perform eight separate operations to achieve the same computation. Moreover, when two or more qubits are linked by quantum entanglement, measuring the state of one qubit determines the state of the other instantly. This enables parallel processing and drastically enhances the performance of quantum algorithms.[1]

[1] Quantum algorithm: A computational method for solving problems using the qubits and *quantum gates of a quantum computer (*quantum gate: Performs operations to transform quantum bits, like logic gates (AND, OR, NOT) in classical computers.

Impact of Quantum Computer

A developed quantum computer does not necessarily process all problems faster than classical computers. Tasks that do not leverage parallelism, such as word processing, spreadsheet calculations, and sorting algorithms, may even perform worse on quantum computers than on classical ones. So, what areas will this bring innovation to?

1. Changes in Cryptography

Most modern cryptography techniques rely on algebraic problems. However, quantum computers can quickly solve these problems, potentially rendering current cryptography techniques obsolete. Public-key encryption, widely used in Internet banking, e-commerce, digital signatures, and authentication, relies on the difficulty of prime factorization. Leading public-key encryption methods include RSA, Diffie-Hellman key exchange, and Elliptic Curve Cryptography (ECC).

Using Shor's quantum algorithm, prime factorization that would take classical computers decades can be completed in seconds, and it poses significant security risks in banking transactions, confidential communications, and personal information protection. Symmetric-key encryption is also affected. Symmetric key encryption can find keys as much as a square root faster than a classical computer using Grover's algorithm. For example, in an n-bit symmetric key encryption system, a classical computer would require 2^n attempts to crack the key, but a quantum computer using Grover's algorithm could do so in 2^(n/2) attempts. It effectively halves the encryption key length.

2. Revolutionizing Drug Development and Medicine

While classical computers have limitations in accurately modeling molecular interactions. quantum computers can precisely simulate molecular structures and chemical reactions, significantly accelerating the new drug development process. Moreover, they enable highly sophisticated, personalized medical services through advanced genetic analysis.

3. Solving Optimization Problems

Quantum computers are excellent at solving optimization problems. They can efficiently solve complex optimization challenges in logistics, finance, automotive design, and traffic management. For example, they can optimize traffic flow in real time to reduce congestion and enable the development of efficient urban transportation networks. In industries and businesses, they can optimize logistics and supply chain optimization, reducing costs and improving time efficiency.

4. Advancement of Artificial Intelligence

Quantum computers are expected to maximize AI performance. Machine learning and deep learning models rely on finding optimal parameters from data. Optimization algorithms such as gradient descent require extensive computations, and processing complex datasets can be time-consuming. Quantum optimization techniques, including quantum annealing and quantum variational algorithms, allow for faster identification of optimal parameters. Moreover, AI models must process large datasets for training and validation, and quantum parallel processing enables rapid data handling, significantly improving efficiency. Additionally, it can process matrix multiplication operations performed in deep learning structures such as CNN (convolutional neural network) much faster, which can dramatically improve the learning speed of deep learning.

Post-Quantum Cryptography

Prime factorization requires exponential time in classical algorithms. However, in 1994, Peter Shor developed a quantum algorithm that utilizes quantum superposition and the quantum Fourier transform (QFT) to solve prime factorization in polynomial time. As a result, in a quantum computing environment, existing public-key cryptographic systems face the threat of being decrypted. To counter this, new public-key encryption methods resistant to quantum attacks are being developed, known as post-quantum cryptography (PQC).

Algorithm	Description	Type
Lattice-based Algorithms	- Lattice-based cryptography solves the problem of mathematical lattice structure based on lattice theory. Algorithms for solving problems arising from lattice structures - Currently most used PQC candidate	Kyber NTRU Dilithium FALCON
Code-based Cryptography	- Cryptography technology based on error-correcting codes - Error-correcting code is a mathematical algorithm for correcting errors that occur during transmission, and this principle is applied to cryptography to protect data. - The security of this technology is based on code theory and the difficulty of decrypting grammatically incorrect messages.	McEliece Niederreiter
Multivariate Quadratic Polynomials	- A multivariate quadratic polynomial contains quadratic and linear terms for polynomial expressions. - It is a cryptographic algorithm that finds solutions to multivariate quadratic equations.	Rainbow SFLASH
Hash-based Signatures	- The algorithm utilizes collision resistance, where the probability of two different messages having the same hash value is very low by using a hash function. - It provides secure signatures against threats from quantum computers.	XMSS SPHINCS+
Isogeny-based Cryptography	- Isogeny is a function between elliptic curves, mapping points on one elliptic curve to points on another. - The algorithm is based on the difficulty of finding isogeny between two elliptic curves with the same order.	SIDH SIKE

Table 1. Post-quantum cryptographic algorithm

Security agencies and academic institutions worldwide are striving to develop and standardize post-quantum cryptographic systems before quantum computers become widely available. In 2016, the US National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography Standardization Project, inviting cryptographers from around the world to design encryption methods resistant to quantum attacks. The project aimed to select the most suitable algorithms from the submitted candidates and establish new encryption standards. Throughout four rounds of candidate submissions, NIST announced four finalist algorithms for standardization in May 2022.

Algorithm	Development Agency (Joint Effort of Multiple Agencies)	Base Problem	Usage
CRYSTALS-KYBER	CRYSTALS Team Peter Schwabe, MPI-SP & Radboud University and 10 others https://pq-crystals.org/	Lattice-based algorithm	Public key encryption, key exchange
CRYSTALS-Dilithium	CRYSTALS Team Vadim Lyubashevsky, IBM Research Zurich and 7 others https://pq-crystals.org/	Lattice-based algorithm	Electronic signature
FALCON	Thomas Prest, PQShield and 9 others https://falcon-sign.info/	Lattice-based algorithm	Electronic signature
SPHINCS+	SPHINCS+ Team Andreas Hülsing, Eindhoven University of Technology & SandboxAQ and 17 others https://sphincs.org/	Hash-based	Electronic signature

Table 2. PQC Algorithms Selected by NIST in 2022

NIST selected CRYSTALS-Kyber as the standard for public-key encryption (PKE), key encapsulation mechanisms (KEMs), and CRYSTALS-Dilithium for the digital signature algorithm. FALCON and SPHINCS+ are also planned to be standardized as digital signature algorithms.

In Korea, R&D on post-quantum cryptography is ongoing. Four algorithms were developed and submitted to NIST in 2017. The HimQ and Lizard algorithms have been registered as standard documents by Korea's Telecommunications Technology Association (TTA).

Algorithm	Development Institution	Base Problem	Usage
EMBLEM and R.EMBLEM	Korea University	Lattice-based algorithm	Public key encryption
pqsigRM	KpqC	Code-based algorithm	Electronic signature
HimQ	National Institute of Mathematical Sciences	Multivariate quadratic polynomials	Electronic signature
Lizard	Seoul National University KISA (Korea Internet & Security Agency)	Lattice-based algorithm	Key exchange

Table 3. Post-quantum Algorithms Developed in Korea

■ Application of PQC

Post-quantum cryptography (PQC) can be applied to all areas where encryption is used, especially those relying on public-key cryptography. The part that uses public key encryption should use PQC, quantum-resistant encryption, and the part that uses symmetric keys must use AES 256-bit or higher keys. Additionally, SHA-2 and SHA-3 must also use keys of at least 256 bits. (As technology advances and vulnerabilities are discovered, security standards for symmetric-key encryption will continue to evolve.)

TLS(HTTPS)

For example, the TLS (HTTPS) protocol, which is widely used on the Internet, is one of the most critical areas requiring PQC. Once the key exchange is completed, the symmetric encryption keys used for packet encryption should be at least 256 bits in length.

Client	Server	
Browser	Webserver	WAS
Applying PQC key exchange	Applying PQC key exchange	Public key for data protection between webserver <-> WAS PQC key exchange is required for encryption.

Table 4. TLS PQC Transition

VPN(Virtual Private Network)

VPN exchanges symmetric keys using a public key method and facilitates secured communication by creating an encrypted tunnel using the symmetric key. As with TLS, the public key encryption method used for key exchange must be switched to PQC, and the exchanged symmetric keys must be at least 256 bits.

Middlebox

A middlebox is a network device that filters, alters, and manipulates packets in a network device or system. The main equipment includes a firewall, NAT (Network Address Translation), load balancer, and IDS/IPS (Intrusion Detection/Prevention System).

PQC mainly belongs to the application layer (Layer 7), and middleboxes mainly operate on the network layer (Layer 3) and transport layer (Layer 4). Therefore, since middleboxes play a role in transmitting or inspecting encrypted data, their operations may not change significantly even after PQC is implemented. However, the following features can be used only when PQC is applied to the middlebox as well.

TLS/SSL inspection and termination: decrypts encrypted traffic and forwards it to the internal network.

Encryption inspection: Decrypt encrypted traffic and inspects it.

Internet of Things (IoT)

IoT networks consist of numerous interconnected devices, and secure communication typically involves exchanging keys using public-key cryptography, followed by symmetric-key encryption for data transmission. Therefore, key exchange methods must switch to PQC, but IoT devices often have resource constraints, making it difficult actually to implement PQC. For low-power IoT devices, lightweight PQC is necessary as it requires lower computational costs, minimal memory usage, and reduced bandwidth.

Financial Transaction/Cloud Environment

Mobile financial transactions and cloud environments incorporate all of the aforementioned TLS, VPN, and middlebox content. Additionally, user authentication and digital signatures play a critical role.

For mobile financial services, transactions and user authentication rely on digital signatures using public-key encryption, such as financial and joint authentication certificates. Thus, it is necessary to adopt PQC-based financial and joint authentication certificates.

Similarly, in cloud services, a PQC-type electronic signature is required because a public key-type electronic signature is used for user authentication and access control. Moreover, since symmetric-key encryption is used for data storage in the cloud and is managed via public-key cryptography encryption, PQC must also be applied in this context to ensure secure key management.

Blockchain/Bitcoin

Blockchain relies on both public-key cryptography and hash functions to ensure transaction integrity. Since Bitcoin uses SHA-256 as its hashing mechanism, it is considered secure against quantum computer attacks.

However, Bitcoin’s electronic wallets are not as secure. Bitcoin employs ECDSA (Elliptic Curve Digital Signature Algorithm) for public-key encryption. In the early days, Bitcoin used Pay-to-PubKey (P2PK), where the public key itself served as the wallet address. It made it possible for quantum computers to identify the private and public keys. Since 2010, Bitcoin has adopted Pay-to-PubKey-Hash (P2PKH), in which the user's public key is converted into SHA-256 hash and RIPEMD-160 hash to be used as the address. It prevents the private key from being found using only the wallet address. However, when a transaction occurs, the public key becomes visible to the other party, making it vulnerable to quantum attacks. Therefore, it is necessary to convert the ECDSA to PQC.

Update and Patch Integrity Verification

Critical files such as firmware, system updates, and patches are electronically signed to verify their integrity. Files are signed using a private key, and their integrity is verified using a public key. Once quantum computers are developed, they can identify private keys from public keys, allowing attackers to embed malware in update files, sign them again, and bypass integrity verification. To prevent it, PQC-based electronic signatures must be adopted. As supply chain attacks[2] have become more frequent, ensuring the integrity of update and patch files is more critical than ever. Therefore, the PQC application is essential in this field.

■ Current State of Quantum Computer

How advanced will quantum computers have to be before they pose a threat to current cryptography? It is considered that thousands of qubits are needed to attack a quantum computer using public key cryptography.

Public key cryptography algorithm	Number of qubits required for attack
RSA-1024	About 2,000
RSA-2048	4,000 to 5,000
RSA-3072	7,000 or more
ECC-256	2,000 to 2,500
ECC-512	About 4,000

* Source: "Quantum Computing for Computer Scientists" (Noson S. Yanofsky and Mirco A. Mannucci

Table 5. Number of Qubits Required to Attack Current Public Key Cryptosystems

The leading developers of quantum computers are IBM and Google, with around 100 qubits.

Company	Base Technology	Number of Qubits	Others
IBM Quantum	Superconducting	127 (Eagle)	https://www.ibm.com/quantum
GoogleQuantumAI	Superconducting	105 (willow)	https://quantumai.google
IonQ	Ion Trap	35	https://ionq.com
Microsoft Azure Quantum	Topological Qubit	In development	https://quantum.microsoft.com
D-Wave	Quantum Annealing	5000[3]	https://www.dwavesys.com

[2] It is the case of attackers infiltrating an enterprise's supply chain to distribute malware or compromise systems.

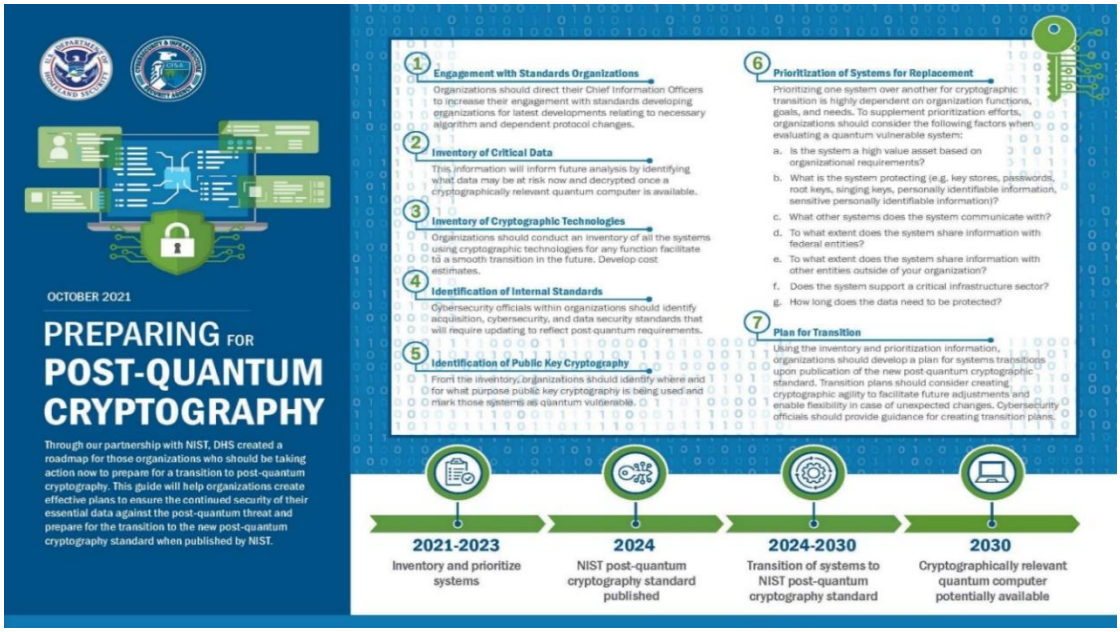
[3] The number of qubits appears to be large because of the nature and implementation of quantum annealing. As it is a quantum computer specialized in solving specific problems quickly, its number of qubits cannot be compared with that of other general-purpose quantum computers.

Table 6. Development of Quantum Computer Development by Company

The quantum computing and quantum cryptography industry forecast that quantum computers will pose a real threat to public-key cryptography systems by 2030.

Conclusion

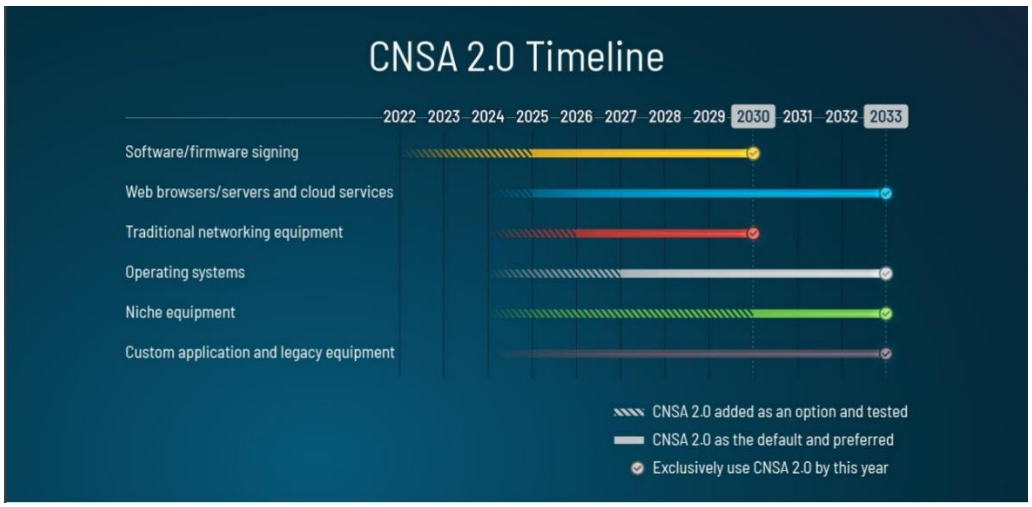
The US government has released its National Cybersecurity Strategy (NSM-10) to transition to PQC by May 2022.



* Source: US National Security Council (NSC)

Figure 7. Cybersecurity Strategy NSM-10 in the United States

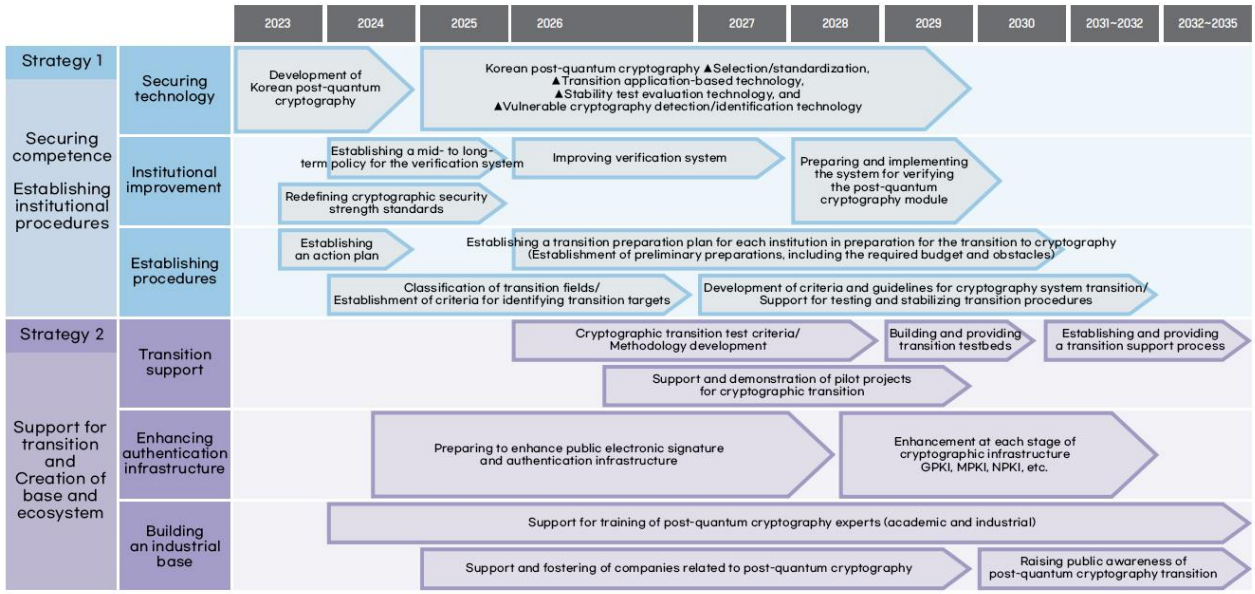
In September, the Cyber Security Advisory of the US National Security Agency (NSA) released the Commercial National Security Algorithm Suite (CNSA) 2.0 Timeline that outlines its plan to begin implementing PQC in software and firmware by 2025 and complete the transition across all sectors, including servers and cloud systems, by 2033.



* Source: NSA National Security Agency

Figure 8. NSA CNSA 2.0 Timeline

In Korea, the National Intelligence Service (NIS) and the Ministry of Science and ICT announced the Master Plan for Post-Quantum Cryptography to transition the entire national cryptographic infrastructure to PQC by 2035. They formulated a detailed implementation plan for each sector last year and plan to establish a legal and regulatory framework by 2030 to support the PQC transition. The plan is to develop related technologies and support necessary policies, such as establishing and operating a cryptographic system transition test bed and integrated support center by 2035.



* Source: NIS

Figure 9. Korea's Master Plan for Post-Quantum Cryptography

Quantum computers are regarded as strategic assets in the global power race. Intelligence agencies worldwide are expected to develop quantum computers in secrecy, without public disclosure, to decrypt classified government and industrial information from other nations. Therefore, in preparation for such threats, a thorough transition to PQC is imperative.