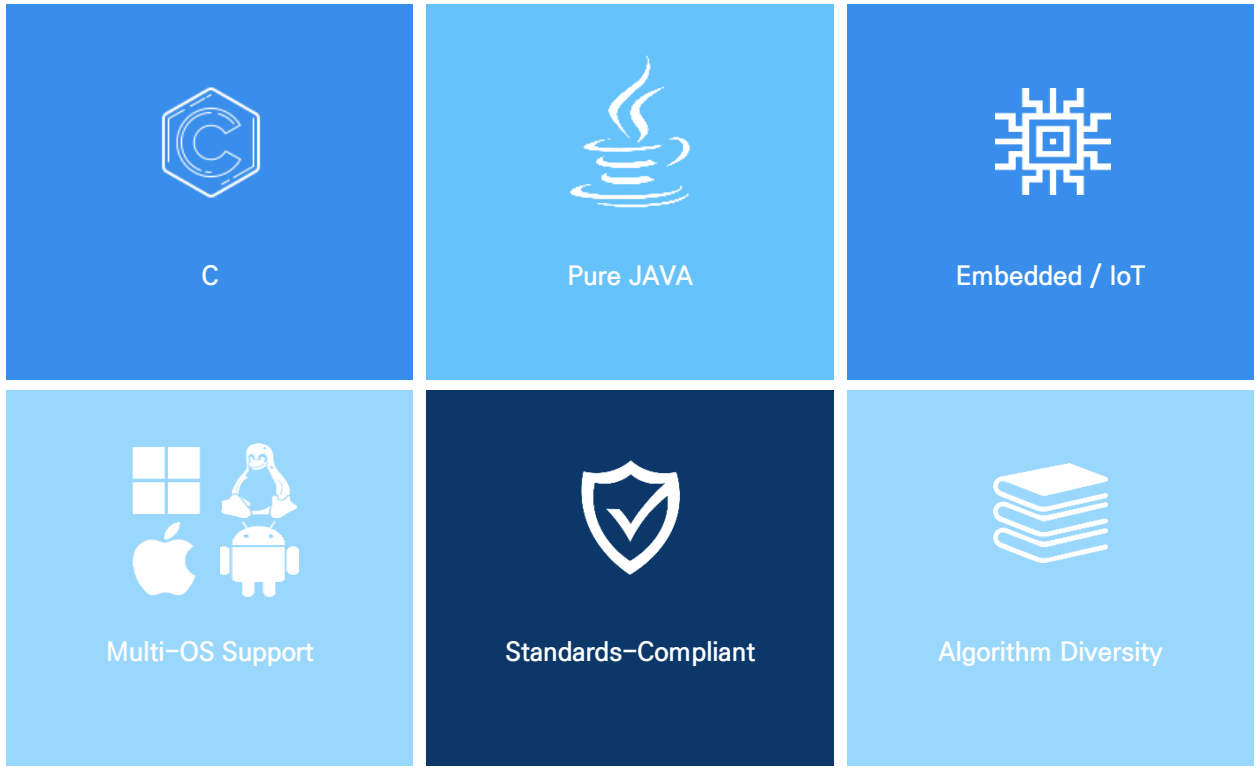
ypqc

Next-Gen PQC Security Module Against Quantum Threats



Next Authentication Platform
Whykeykey

What is Quantum computer?

- Principle: Utilizes quantum mechanics phenomena of 'superposition' and 'entanglement' for ultra-high-speed computation.
- Characteristics: Achieves computational capabilities far superior to traditional supercomputers.
- Applications: Set to revolutionize diverse industries including Artificial Intelligence (AI), defense, drug development, and aerospace.

The Advent of the Quantum Computing Era

- CES 2025 Focus: Highlighted as a key future technology connecting AI and semiconductors.
- Rapid Technological Progress: Significant achievements anticipated within the next three years.
- Major Players' Commercialization Goals:
  - Google: Presented a six-stage commercialization roadmap targeting usability by 2031.
  - IBM: Aims to implement error-corrected quantum computers by 2029 for commercialization.
  - Microsoft: Pursuing R&D in collaboration with partners like IonQ, Honeywell, and Atom Computing.
- Domestic Landscape (South Korea): Launched the Public-Private Quantum Strategy Committee in March 2025.
- Outlook: Accelerated quantum computing development driven by competition among big tech companies
  → Expected to shorten the timeline for quantum computer commercialization.

Threats of Quantum Computing

Quantum computers pose an imminent threat to current cryptographic systems, necessitating the urgent development of quantum-resistant solutions to protect global e-commerce, national security, and cryptocurrencies.

1 Collapse of Current Cryptography

- Vulnerability: Shor's Algorithm* on quantum computers can easily break existing cryptographic standards like RSA and ECC (used in most e-commerce).
- Impact: Poses significant risks to current e-commerce security and national security.
- Urgency: Mosca's Inequality** highlights the need for pre-emptive action before quantum computers become widely available.
- Cryptocurrency Alert: Major changes anticipated for cryptocurrencies like Bitcoin and Ethereum.

2 Quantum Computing Threat Analysis

Feature	RSA2048 (Classical)	ECDSA(P256) (Classical)	Quantum Computing (Shor's Algorithm)
Underlying Principle	Factorization	Discrete Logarithm	Quantum Fourier Transform (QFT)
Time Complexity	$O\left(e^{\sqrt[3]{\frac{64}{9}(\log n)(\log^2 n)^2}}\right)$ (Exponential)	$O(\sqrt{n})$ (Exponential)	$O\left((\log n)^3\right)$ (Polynomial)
Feasibility	Infeasible	Infeasible	Feasible

* Shor's Algorithm: A quantum algorithm that can quickly factor large numbers. It can solve integer factorization and discrete logarithm problems in polynomial time without a private key.

** Mosca's Inequality (Store Now, Decrypt Later – SNDL): Quantum computers enable "Store Now, Decrypt Later" attacks. This means past transaction keys recorded on blockchains could be decrypted and exploited. Therefore, quantum-resistant cryptography must be developed years before decryption technology becomes widespread.

Background

- Threat: The advancement of quantum computing technology (Peter Shor's Algorithm) jeopardizes existing public-key cryptography.
- Urgency: Mosca's Inequality states that while quantum computer commercialization is unpredictable, Post-Quantum Cryptography (PQC) must be prepared in advance.

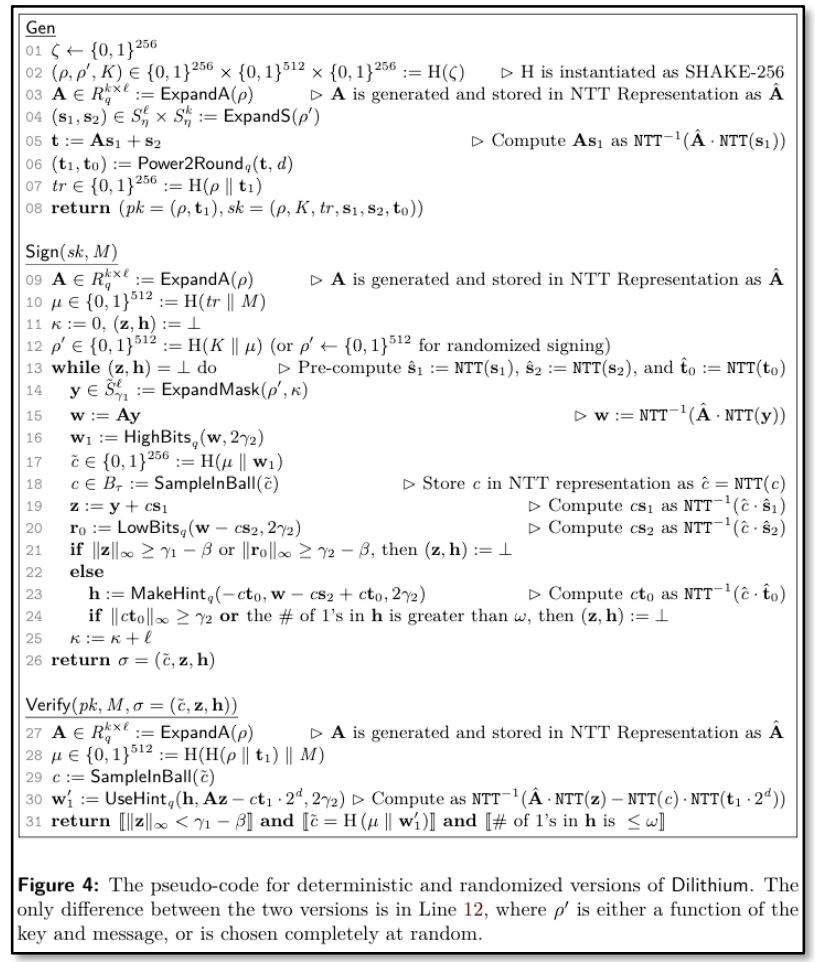
What is PQC?

- A new public-key cryptography designed to withstand decryption threats in a quantum computing environment.
- Lattice-based cryptography is being standardized domestically (TTA, HIMQ/RLizard).

Ypqc

- WhykeykeySoft Technology Research Institute is the first in Korea to develop and test both the Korean TTA standard (RLizard.CCA) and international standard algorithms (MLDSA / MLKEM) in C and Java languages, respectively. Based on this, we have launched Ypqc, our post-quantum cryptography module.

Example of lattice-based algorithm



Gen
01 $\zeta \leftarrow \{0,1\}^{256}$
02 $(\rho, \rho', K) \in \{0,1\}^{256} \times \{0,1\}^{512} \times \{0,1\}^{256} := \mathrm{H}(\zeta)$ ▷ H is instantiated as SHAKE-256
03 $\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
04 $(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^\ell \times S_\eta^k := \mathsf{ExpandS}(\rho')$
05 $\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ ▷ Compute $\mathbf{A}\mathbf{s}_1$ as $\mathtt{NTT}^{-1}(\hat{\mathbf{A}} \cdot \mathtt{NTT}(\mathbf{s}_1))$
06 $(\mathbf{t}_1, \mathbf{t}_0) := \mathsf{Power2Round}_q(\mathbf{t}, d)$
07 $tr \in \{0,1\}^{256} := \mathrm{H}(\rho \,\|\, \mathbf{t}_1)$
08 **return** $(pk = (\rho, \mathbf{t}_1), sk = (\rho, K, tr, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0))$

Sign(sk, M)
09 $\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
10 $\mu \in \{0,1\}^{512} := \mathrm{H}(tr \,\|\, M)$
11 $\kappa := 0$, $(\mathbf{z}, \mathbf{h}) := \perp$
12 $\rho' \in \{0,1\}^{512} := \mathrm{H}(K \,\|\, \mu)$ (or $\rho' \leftarrow \{0,1\}^{512}$ for randomized signing)
13 **while** $(\mathbf{z}, \mathbf{h}) = \perp$ do ▷ Pre-compute $\hat{\mathbf{s}}_1 := \mathtt{NTT}(\mathbf{s}_1)$, $\hat{\mathbf{s}}_2 := \mathtt{NTT}(\mathbf{s}_2)$, and $\hat{\mathbf{t}}_0 := \mathtt{NTT}(\mathbf{t}_0)$
14 $\quad \mathbf{y} \in \tilde{S}_{\gamma_1}^\ell := \mathsf{ExpandMask}(\rho', \kappa)$
15 $\quad \mathbf{w} := \mathbf{A}\mathbf{y}$ ▷ $\mathbf{w} := \mathtt{NTT}^{-1}(\hat{\mathbf{A}} \cdot \mathtt{NTT}(\mathbf{y}))$
16 $\quad \mathbf{w}_1 := \mathsf{HighBits}_q(\mathbf{w}, 2\gamma_2)$
17 $\quad \tilde{c} \in \{0,1\}^{256} := \mathrm{H}(\mu \,\|\, \mathbf{w}_1)$
18 $\quad c \in B_\tau := \mathsf{SampleInBall}(\tilde{c})$ ▷ Store c in NTT representation as $\hat{c} = \mathtt{NTT}(c)$
19 $\quad \mathbf{z} := \mathbf{y} + c\mathbf{s}_1$ ▷ Compute $c\mathbf{s}_1$ as $\mathtt{NTT}^{-1}(\hat{c} \cdot \hat{\mathbf{s}}_1)$
20 $\quad \mathbf{r}_0 := \mathsf{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma_2)$ ▷ Compute $c\mathbf{s}_2$ as $\mathtt{NTT}^{-1}(\hat{c} \cdot \hat{\mathbf{s}}_2)$
21 $\quad$ **if** $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ or $\|\mathbf{r}_0\|_\infty \geq \gamma_2 - \beta$, then $(\mathbf{z}, \mathbf{h}) := \perp$
22 $\quad$ **else**
23 $\quad\quad \mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{w} - c\mathbf{s}_2 + c\mathbf{t}_0, 2\gamma_2)$ ▷ Compute $c\mathbf{t}_0$ as $\mathtt{NTT}^{-1}(\hat{c} \cdot \hat{\mathbf{t}}_0)$
24 $\quad\quad$ **if** $\|c\mathbf{t}_0\|_\infty \geq \gamma_2$ **or** the # of 1's in $\mathbf{h}$ is greater than ω, then $(\mathbf{z}, \mathbf{h}) := \perp$
25 $\quad \kappa := \kappa + \ell$
26 **return** $\sigma = (\tilde{c}, \mathbf{z}, \mathbf{h})$

Verify$(pk, M, \sigma = (\tilde{c}, \mathbf{z}, \mathbf{h}))$
27 $\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
28 $\mu \in \{0,1\}^{512} := \mathrm{H}(\mathrm{H}(\rho \,\|\, \mathbf{t}_1) \,\|\, M)$
29 $c := \mathsf{SampleInBall}(\tilde{c})$
30 $\mathbf{w}_1' := \mathsf{UseHint}_q(\mathbf{h}, \mathbf{A}\mathbf{z} - c\mathbf{t}_1 \cdot 2^d, 2\gamma_2)$ ▷ Compute as $\mathtt{NTT}^{-1}(\hat{\mathbf{A}} \cdot \mathtt{NTT}(\mathbf{z}) - \mathtt{NTT}(c) \cdot \mathtt{NTT}(\mathbf{t}_1 \cdot 2^d))$
31 **return** $[\![\|\mathbf{z}\|_\infty < \gamma_1 - \beta]\!]$ **and** $[\![\tilde{c} = \mathrm{H}(\mu \,\|\, \mathbf{w}_1')]\!]$ **and** $[\![\#$ of 1's in $\mathbf{h}$ is $\leq \omega]\!]$

Figure 4: The pseudo-code for deterministic and randomized versions of Dilithium. The only difference between the two versions is in Line 12, where ρ' is either a function of the key and message, or is chosen completely at random.

Post Quantum Cryptography Standard Algorithm

Standards Development Organization (SDO)	Algorithm	Note
NIST (USA)	**ML-KEM (CRYSTALS-KYBER)**	Encryption (lattice-based)
NIST (USA)	**ML-DSA (CRYSTALS-DILITHIUM)**	Digital Signature (lattice-based)
NIST (USA)	SLH-DSA (SPHINCS+)	Digital Signature (hash-based)
TTA (Korea)	**Ring-Lizard**	Encryption (lattice-based)
TTA (Kore)	HiMQ	Digital Signature (multivariate quadratic-based)
KpqC contest	AiMer	Digital Signature (hash-based)

Algorithm Standardization

- NIST (U.S. National Institute of Standards and Technology): Published three standard algorithms.
- TTA (Korea Telecommunications Technology Association): Announced two algorithms (for encryption and digital signatures).

NIST National Institute of Standards and Technology

TTA

Security Industry Initiatives

- Samsung SDS: Developed the hash-based digital signature algorithm AiMer in collaboration with KAIST.
- RaonSecure: Incorporated some PQC elements into its products.
- Dream Security: Developed a post-quantum cryptography module.
- CryptoLab: Engaged in algorithm standardization and consulting.

SAMSUNG SDS

HEAAN CRYPTO LAB

Government Policy Actions

- Considering PQC algorithms for KCMVP (Korean Cryptographic Module Validation Program) certification.
- Launched a project to build a national infrastructure for issuing PQC certificates.
- Movement toward adopting PQC in defense and public-sector organizations.

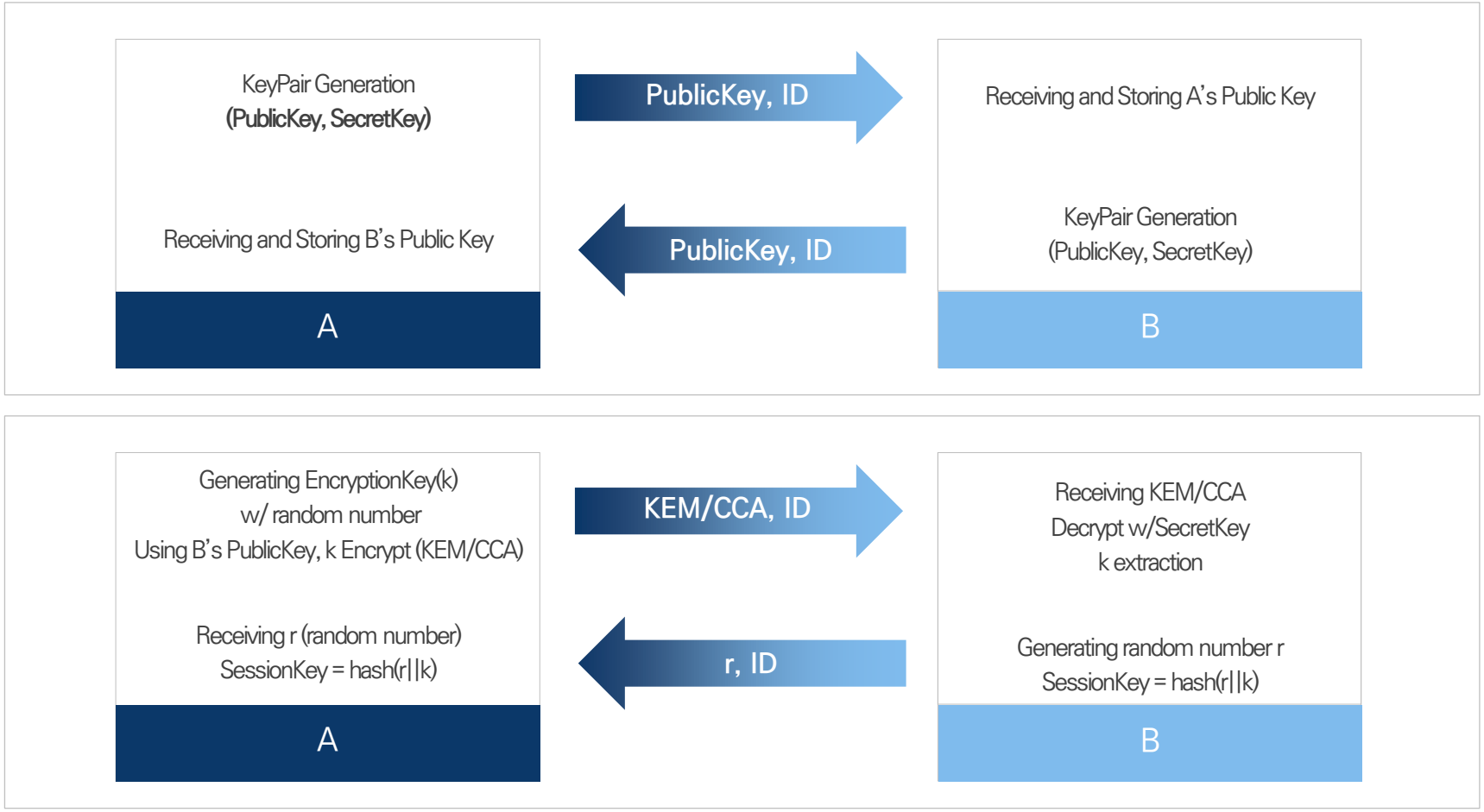
PQC Communication Method – Key Sharing Process

Public Key Exchange

- MLKEM / RLizard Method
- The same applies to MLDSA.
- The generated private key is stored in a secure repository.
- The counterpart's public key is stored in a separate database.
- Optionally delivered in the form of a certificate.
- Mutual key exchange (optional).
- Security parameters are agreed upon in advance.

Encryption Key Exchange

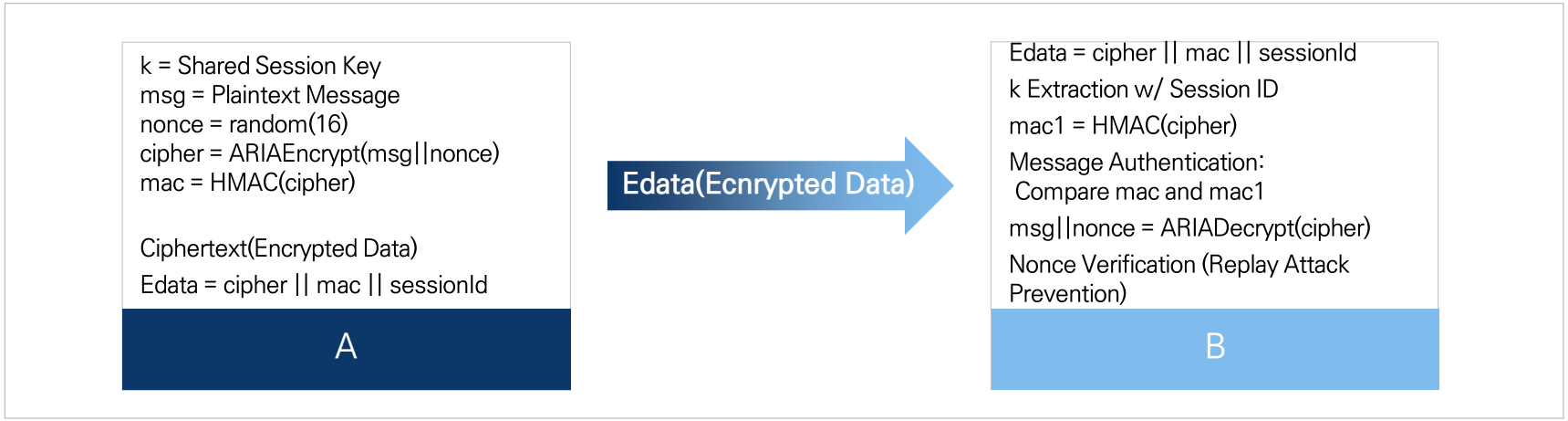
- MLKEM / RLizard Method Encrypts the encryption key using the recipient's public key.
- Generates additional random numbers and a session key.
- The session key consists of a symmetric key, IV (initialization vector), and MAC key.
- Subsequent encrypted communication uses the session key.



PQC Communication Method – E2EE, Digital Signature

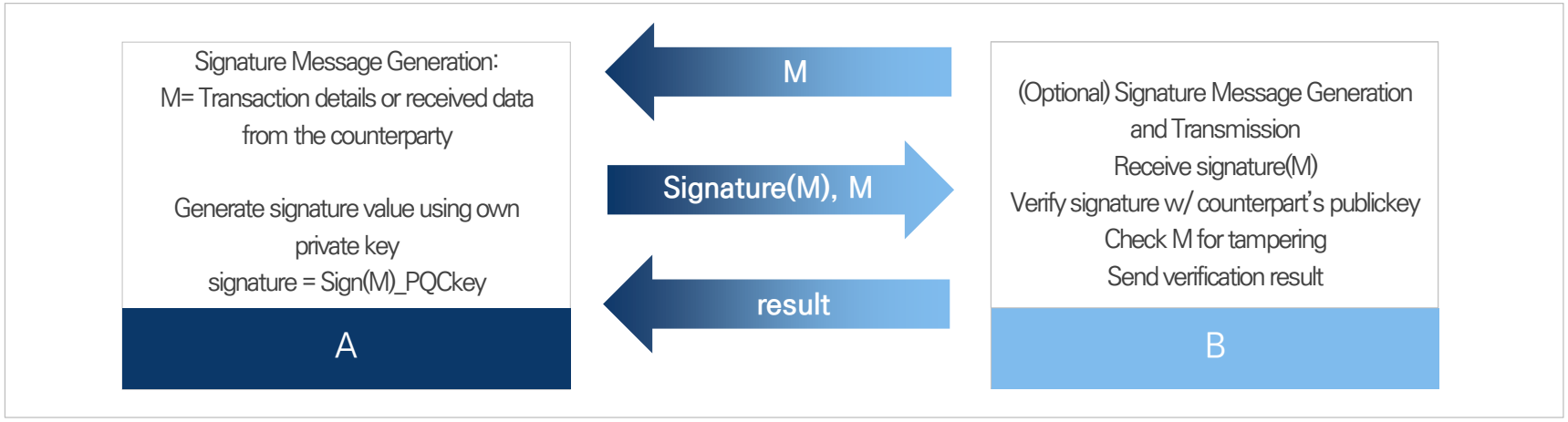
End-to-end encryption (E2EE)

- MLKEM / RLizard
- Use the shared session key to encrypt and decrypt communication data.
- Apply a message authentication code (MAC).
- Prevent replay attacks.
- Both A and B generate and transmit ciphertext in the same way.



Digital Signature

- MLDSA
- Generate and transmit a digital signature using one's private key.
- Verify the digital signature using the recipient's public key.
- Challenge-response method can be applied for transaction verification.
- For future transaction proof, it is recommended to store the signature separately.
- Use of a certificate is optional if needed.



Global standardization and national roadmaps indicate that enterprises must begin transitioning to post-quantum cryptography now to ensure secure adoption by 2028 and beyond.

Commercialization Timeline

Timeline

- Considering the current pace of quantum computing development, major national institutions recommend accelerating the adoption of post-quantum cryptography (PQC).
- The U.S. National Institute of Standards and Technology (NIST) recommends that major enterprises adopt PQC by 2028.
- The UK's National Cyber Security Centre (NCSC), in its recent guidance, recommends that enterprises:
  - Identify vulnerable systems by 2028
  - Prioritize critical upgrades by 2031
  - Fully transition to PQC by 2035

Algorithm Standardization

Standardization

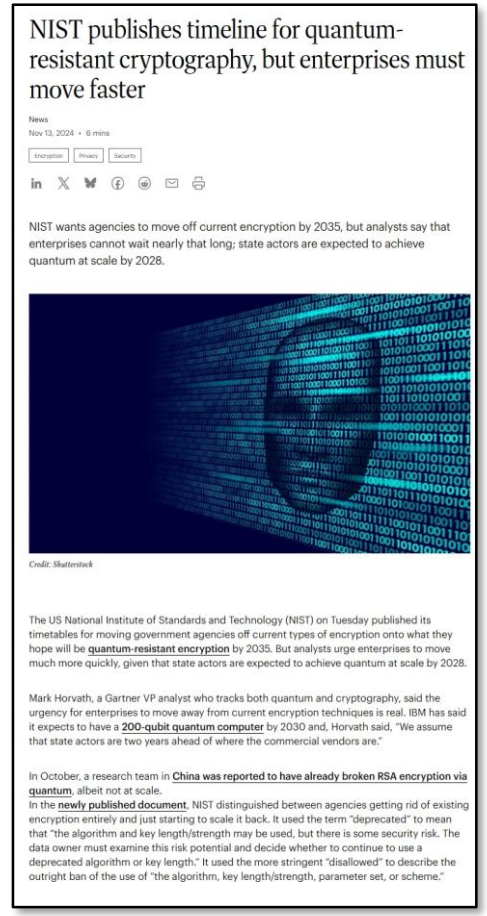
- Standardization efforts are currently led by the United States:
  - ML-KEM : Module-lattice-based standard encryption algorithm (FIPS 203)
  - ML-DSA : Module-lattice-based standard digital signature algorithm (FIPS 204)
  - SLH-DSA : Hash-based standard digital signature algorithm (FIPS 205)
- Hash-based algorithms are expected to be used for special purposes due to their large key and signature sizes.
- Existing domestic standard algorithms (RLizard / HiMQ) are outdated and are expected to be replaced by four new algorithms.

WhykeykeySoft Development Status & Outlook

WhykeykeySoft

- Currently focusing on the development of three major standard algorithms:
  - Encryption : ML-KEM, RLizard.CCA
  - Digital Signature: ML-DSA
- Ongoing work on stability and performance, develop other algorithms

Related Article (Source : CSO)



NIST publishes timeline for quantum-resistant cryptography, but enterprises must move faster

News
Nov 13, 2024 • 6 mins

Encryption | Privacy | Security

NIST wants agencies to move off current encryption by 2035, but analysts say that enterprises cannot wait nearly that long; state actors are expected to achieve quantum at scale by 2028.

Credit: Shutterstock

The US National Institute of Standards and Technology (NIST) on Tuesday published its timetables for moving government agencies off current types of encryption onto what they hope will be quantum-resistant encryption by 2035. But analysts urge enterprises to move much more quickly, given that state actors are expected to achieve quantum at scale by 2028.

Mark Horvath, a Gartner VP analyst who tracks both quantum and cryptography, said the urgency for enterprises to move away from current encryption techniques is real. IBM has said it expects to have a 200-qubit quantum computer by 2030 and, Horvath said, "We assume that state actors are two years ahead of where the commercial vendors are."

In October, a research team in China was reported to have already broken RSA encryption via quantum, albeit not at scale.
In the newly published document, NIST distinguished between agencies getting rid of existing encryption entirely and just starting to scale it back. It used the term "deprecated" to mean that "the algorithm and key length/strength may be used, but there is some security risk. The data owner must examine this risk potential and decide whether to continue to use a deprecated algorithm or key length." It used the more stringent "disallowed" to describe the outright ban of the use of "the algorithm, key length/strength, parameter set, or scheme."

By combining growing market demand, active industry adoption, and consulting-driven technology transfer, we aim to accelerate PQC commercialization.

〈 Consulting Business Direction 〉

Provide technology transfer and consulting services to domestic companies requiring PQC.
Commercialize PQC modules for TLS, widely used in e-commerce and web services.
Establish a recurring revenue model through continuous module updates.

Background

- As post-quantum cryptography (PQC) technologies gain attention, interest among domestic security and web service providers is rapidly increasing.
- As of 2024, there are **814 domestic information security companies**, many of which face difficulties in internalizing PQC technology due to high costs and technical complexity.

Market Trends

- Major domestic security-listed companies such as **Hancom Secure, Dream Security, and Raon Secure** are actively developing PQC solutions.
- **Samsung Electronics** – Integrated PQC features into the Galaxy S25 series to protect user data.
- **SK Telecom** – Launched the first commercial global VPN service with PQC in Korea.

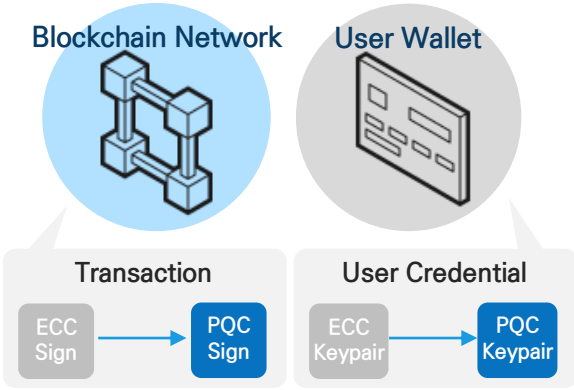
Market Size

- Target: domestic security companies requiring PQC technology transfer and consulting
- Approx. **800 companies × USD 25,000 ≈ USD 20 million**.
- Additional recurring cash flow expected through continuous PQC module updates

With proven blockchain expertise and growing urgency for PQC adoption, we aim to pioneer a secure PQC-based environment to safeguard the future of digital assets.

〈 Blockchain Business Direction 〉

Develop alternative technologies for transaction signatures and wallet schemes in blockchain.
Build a PQC-based blockchain mainnet.



Background

- Most cryptocurrencies currently rely on **public-key cryptography (ECC-based)**.
- Quantum computers could extract private keys, leading to **transaction forgery** and **double-spending attacks**.

Technology Trends

- Some, including Jensen Huang, predict that it will take around **20 years** before useful quantum computers appear, suggesting that applying PQC now is premature.
- Others argue that quantum computers may emerge **before 2030**, and based on **Mosca's Inequality**, immediate PQC adoption is more appropriate.

Blockchain Development Capabilities

- Experience in:
  - ▸ Operating a **white-label-based exchange**
  - ▸ Researching **wallet structures**
  - ▸ Developing **private blockchains (Hyperledger Fabric)**
- Ability to form a **mainnet development team and network**, contingent upon investment.

Core Strengths of Ypqc

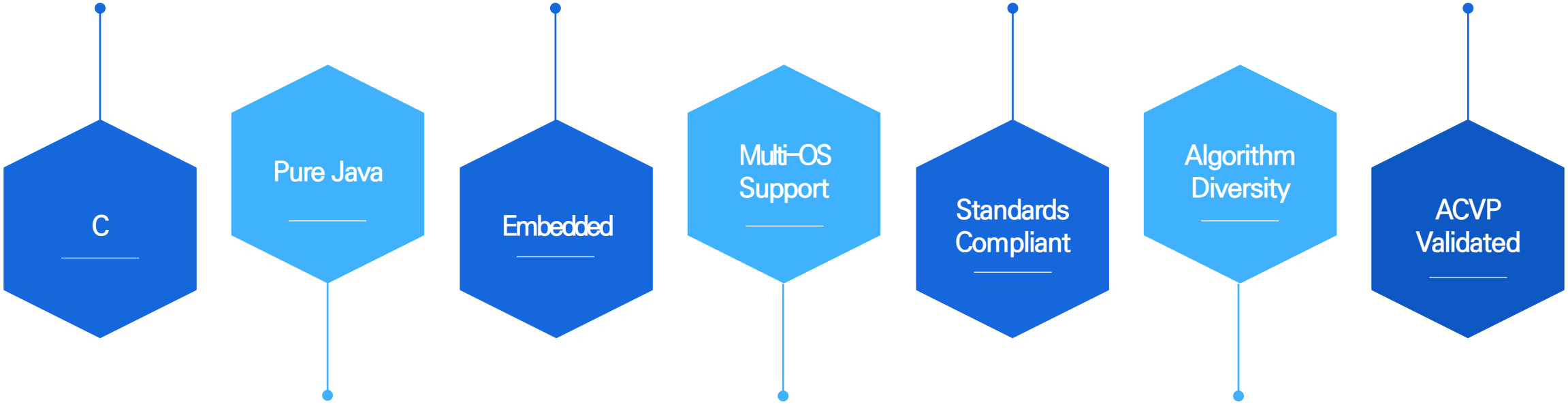
Delivering the most versatile, standards-compliant, and future-ready PQC module.

Pure C codebase, highly portable and efficient across platforms.

Designed for constrained environments with minimal memory footprint.

Fully aligned with NIST PQC standards and cryptographic best practices.

Validated through the NIST ACVP process to ensure reliability and interoperability.



Fully implemented in Java without JNI, ensuring portability and ease of integration

Compatible across major operating systems for seamless adoption.

Supports multiple PQC algorithms including ML-KEM, ML-DSA, and RLizard.

Backed by rigorous development, public validation, and verifiable results.

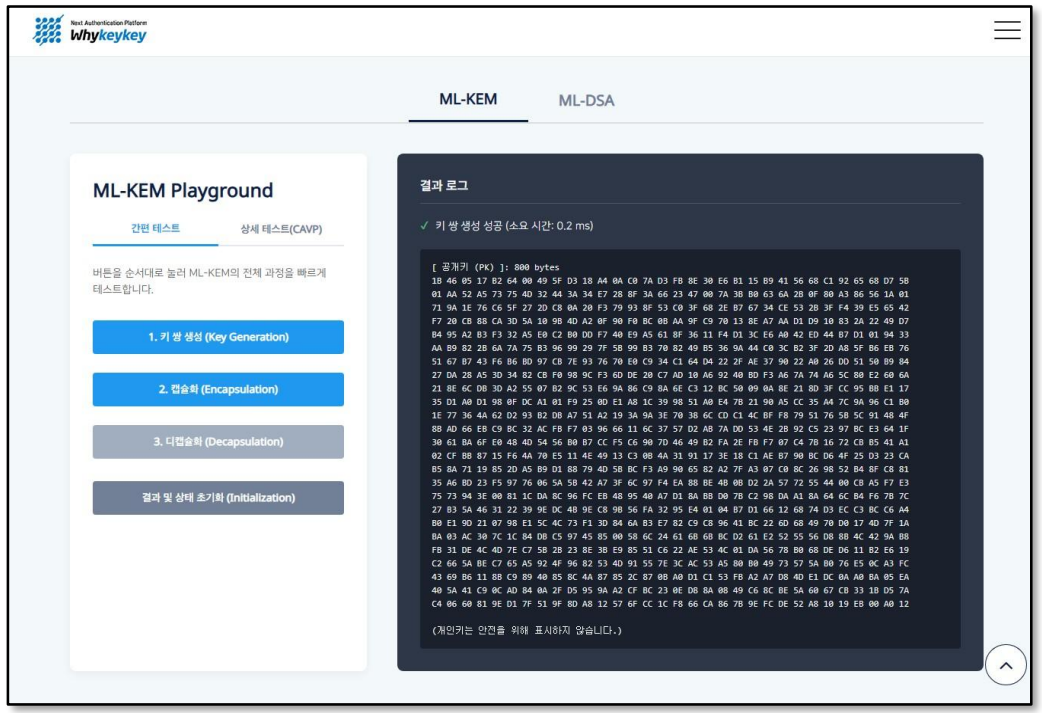
Algorithm Development (Completed)

- Two international standard algorithms: ML-KEM (encryption), ML-DSA (digital signature).
- One domestic standard algorithm: RLizard (encryption)
- ▸ First and only in Korea to be developed simultaneously in both C and Java languages.

Universal Testing Environment (Playground)

- A public webpage where anyone can test the consistency of their own algorithm.
- Shows computation times to evaluate performance.

WhykeykeySoft PQC Playground (Click image to try)



Roadmap to Quantum-Resistant Future

Building on our unique expertise as a foundational PQC developer, we are engineering a future-proof cryptographic engine designed to meet emerging global standards and achieve the most stringent security certifications.

01 Technology Roadmap

Continuous Innovation

- Expanding Algorithm Portfolio
  - ▸ Currently developing/reviewing four additional algorithms for KpqC (Korean PQC standard)
  - ▸ This ensures we remain at the forefront of both domestic and international standardization.
- Enhanced Performance & Features
  - ▸ Ongoing R&D for performance optimization and integration with emerging technologies (e.g., IoT, Blockchain).

02 Market Strategy

Securing Leadership

- Targeting KCMVP Certification
  - ▸ Actively preparing for KCMVP (Korea Cryptographic Module Validation Program) certification immediately following the final algorithm announcement.
- Market Expansion & Dominance
  - ▸ Public Sector : Ancitipating mandatory PQC adoption for public institutions, creating a significant market opportunity. KpqC readiness positions us as a primary suuplier.
  - ▸ Private Sector : Providing a seamless upgrade path for all existing security products to become quantum-resistant.

03 Unique Edge

Unmatched Expertise

- Fundamental Technology Ownership
  - ▸ WhykeykeySoft is the only company in Korea to have independently developed post-quantum cryptography from the ground up, based on our own core principles.
  - ▸ This deep expertise guarantees superior flexibility, support, and long-term reliability for our clients.

Next Authentication Platform
Whykeykey

A. 55, Seongsuil-ro 8-gil, Seongdong-gu, Seoul, Korea

T. +82 2-576-4746

W. www.whykeykey.com

THANK YOU