White Paper

Designing a Hybrid Path to PQC Built for the Real World

April 2025

Research Institute
of Advanced Technology

2025/04

SoftBank

SANDBOXAQ™

SoftBank and SandboxAQ's Initiative Toward Post-Quantum-Cryptography (PQC) Transition

The emergence of practical quantum computing may bring a significant transformation in cybersecurity, posing immediate risks to existing encryption standards. Encryption technologies such as Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC), which are widely used around the world, are expected to become vulnerable to quantum-powered attacks.

In response, leading organizations — including federal agencies, government supply chain operators, banking sector and financial institutions — are preparing to transition to Post-Quantum Cryptography (PQC), encryption purpose-built to withstand quantum-based attacks.

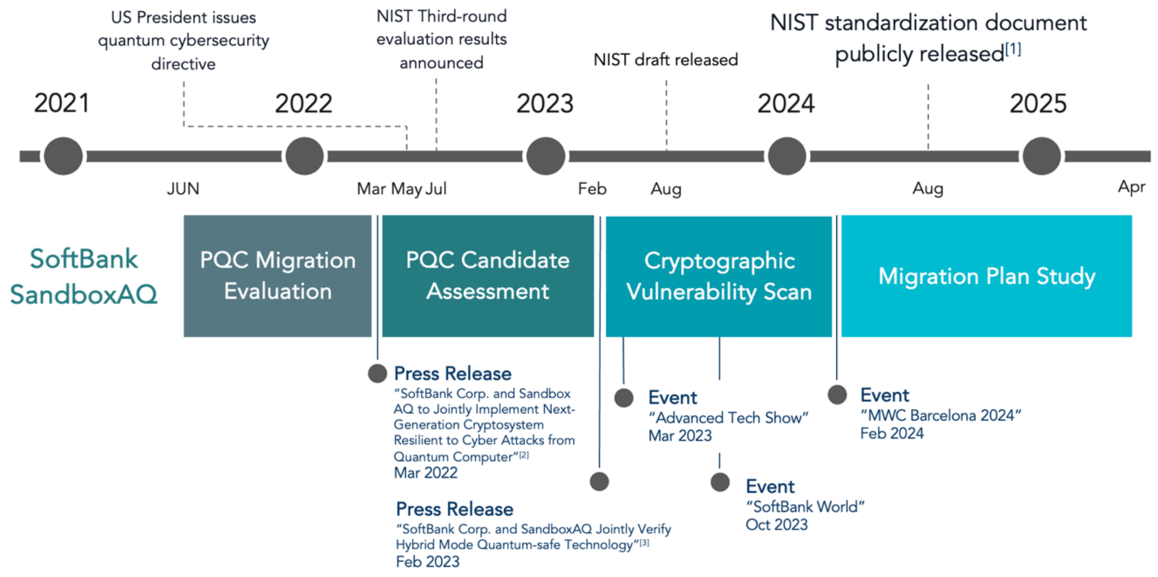

Figure 1. SoftBank and SandboxAQ's Initiative toward PQC transition

SoftBank began collaborating with SandboxAQ on PQC in 2021. Since then, they have closely monitored the standardization trends of PQC algorithms by the US National Institute of Standards and Technology (NIST). Alongside this, SoftBank has been actively engaged in efforts to transition to PQC.

SoftBank and SandboxAQ's study provides insights and preliminary strategies that can be considered for implementation. Recognizing the urgency of protecting sensitive data from "store-now-decrypt-later" attacks, SoftBank and SandboxAQ have validated hybrid cryptographic methods that integrate established classical encryption with robust, quantum-safe solutions. Through comprehensive testing, the technical challenges and potential solutions for organizations navigating this critical transition are outlined. By adopting a hybrid approach to PQC, enterprises can ensure the continuous protection of their digital assets, maintain compliance, and position themselves confidently in the quantum era.

This white paper explains the necessity of hybrid cryptographic schemes and provides details on a proof-of-concept experiment.

The Threat of Quantum Computing

Quantum computers leverage principles from quantum mechanics — such as superposition and entanglement — to perform complex computations far more quickly than traditional computers. These methods rely on mathematical problems — specifically factoring large numbers or computing discrete logarithms — that traditional computers can't efficiently solve. While still emerging, quantum computing capabilities are advancing rapidly, driven by intense research investment globally. This remarkable computational power presents serious risks to today's cybersecurity.

Currently, public key encryption methods such as RSA and ECC protect everything from banking transactions and medical records to national security communications. Public key encryption, also known as asymmetric encryption, uses different keys for encryption and decryption. In public key encryption, the sender encrypts the data using a public key, and the receiver decrypts it using a private key. By design, a third-party attacker can know the public key but cannot decrypt the encrypted data without the private key. Public key encryption is used for key exchange in encrypted communications and for digital signatures to prevent impersonation. Traditional public key encryption methods have ensured security by using mathematical problems such as factoring large numbers or computing discrete logarithms.

However, quantum computers can easily solve these mathematical problems using a powerful algorithm known as Shor's algorithm. Shor's algorithm allows quantum computers to solve problems like factoring large numbers, which would require exponential computational resources on classical computers, by using qubits in a superposition of 0 and 1. This enables quantum computers to efficiently calculate private keys from public key information based on traditional encryption algorithms.

Although the realization of quantum computers is often considered to be in the distant future, governments and companies are already facing their threats. It is anticipated that encrypted communications lacking quantum resistance may be intercepted now and decrypted once quantum computers become practical. Such attacks are known as Store Now Decrypt Later (SNDL) attacks or Harvesting attacks. This risk highlights the urgent need for a transition to quantum-resistant encryption to protect data in the quantum era.

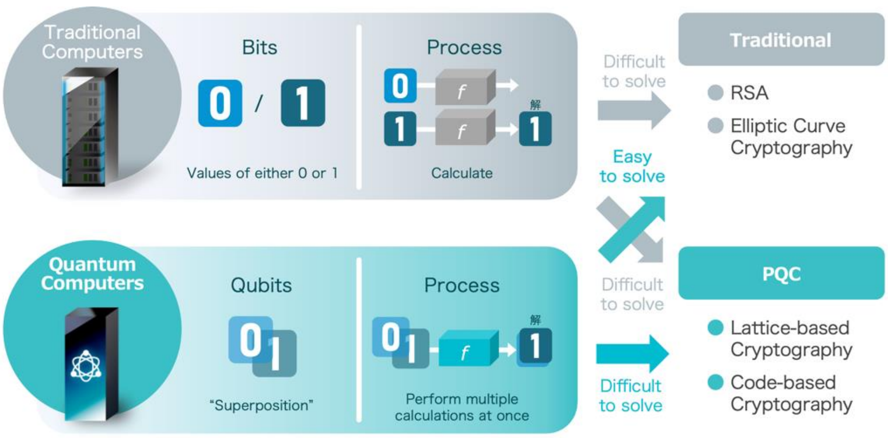

Figure 2. Encryption methods hard to defeat by Traditional and Quantum computing

Understanding Post-Quantum Cryptography

PQC refers to encryption techniques specifically engineered to withstand quantum computing threats.

Unlike RSA and ECC, PQC algorithms are based on mathematical problems that are believed to resist quantum-based attacks. Because they rely on fundamentally different mathematical foundations, quantum computers using algorithms like Shor's can't easily decrypt PQC-secured data.

Several PQC approaches currently exist, and we'll explore each below.

Feature	Structured Lattice	Unstructured Lattice	Isogeny-based	Code-based
Security Strength	High; thoroughly analyzed and trusted	Very High; strong theoretical security	Uncertain; recent vulnerabilities discovered	High; proven resistance
Performance (Speed)	Fast encryption & decryption speeds	Slower; requires significant computational resources	Slow; computationally intensive	Moderate; manageable computational overhead
Key Sizes	Moderate; generally practical and manageable	Large; potentially challenging for widespread adoption	Smallest among PQC algorithms (advantageous)	Very large; can impact storage and bandwidth
Resource Requirements	Moderate; suitable for everyday devices and servers	High; significant processing power required	High; places substantial load on systems	Moderate to High; balanced processing needs
Maturity & Practical Adoption	Mature; widely tested (e.g., Kyber, Dilithium), endorsed by NIST	Less mature; limited adoption due to complexity	Least mature; vulnerabilities have emerged recently	Mature; longstanding research, though less popular due to large keys

Table 1. Comparison of PQC encryption types

Structured Lattice-based Cryptography

This well-regarded approach employs mathematical problems derived from structured lattices — geometric arrangements of points in multidimensional space. Algorithms such as Kyber and Dilithium fall into this category. Structured lattice methods offer excellent efficiency and balanced security and have performed exceptionally in practical demonstrations, receiving a strong endorsement from NIST.

Unstructured Lattice-based Cryptography

This also relies on lattice structures, but there are fewer mathematical structures and symmetries. Although unstructured lattices potentially provide stronger theoretical security, they require significantly larger key sizes and increased computational resources, often making them less suitable for widespread deployment than structured lattice approaches.

Isogeny-based Cryptography

The "isogenies" referenced are complex mathematical structures called elliptic curves and the relationships between them, called isogenies. Isogeny-based algorithms initially appeared promising due to their small key sizes; however, recent vulnerabilities and higher computational demands during encryption have raised concerns regarding their practical security and performance.

Code-based Cryptography

This method uses error-correcting codes that can reliably detect and correct errors within data. While highly resistant to quantum attacks, code-based approaches typically involve larger encryption keys, potentially impacting storage and data transmission efficiency.

NIST standardization

Recognizing the urgency, NIST released official PQC standards in 2024. The standardized algorithms include one key exchange algorithm (FIPS203) and two digital signature algorithms (FIPS204, FIPS205), respectively.

Key Exchange Algorithm

FIPS203: ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)

- ML-KEM is a cryptographic algorithm based on structured lattice problems, unlike traditional RSA or ECC, and relies on problems that are difficult for even quantum computers to solve. Specifically, it ensures security using the shortest vector problem in lattices. It enables efficient key generation and encryption, providing high security with relatively low latency and overhead.

Digital Signature Algorithm

FIPS204: ML-DSA (Module-Lattice-Based Digital Signature Algorithm)

- ML-DSA is also a digital signature algorithm based on structured lattice problems. ML-DSA has fast signature generation and verification speeds, and it is particularly excellent in balancing security and performance.

FIPS205: SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)

- SLH-DSA is a cryptographic technique based on hash functions. It employs a signature method using hash functions and has high security. However, it increases the load on communication bandwidth and storage due to high computational volume and large signature size.

NIST has continuously chosen the additional algorithms which will function as a backup defense in case quantum computers eventually become capable of cracking the lattice-based algorithms.

Key Exchange Algorithm

- HQC
    - HQC is based on error-correcting codes, a mathematical foundation distinct from the structured lattices used in ML-KEM. This diversity in mathematical approaches ensures resilience against potential vulnerabilities in ML-KEM, providing a robust alternative for securing data against quantum attacks.

Digital Signature Algorithm

- FN-DSA (FFT over NTRU-Lattice-Based Digital Signature Algorithm)
    - FN-DSA, known as Falcon, utilizes Fast Fourier Transform (FFT) to achieve efficient and compact digital signatures. This lattice-based scheme offers strong security guarantees against both classical and quantum attacks, making it a robust choice for post-quantum cryptography.

Currently, NIST is in the process of drafting implementation guidelines and detailed technical documents for these algorithms. Organizations are recommended to update their systems based on the new standards once these documents are released.

Hybrid Encryption Scheme Combining Classical Cryptography and PQC

Challenges in Transitioning to Quantum-Safe Encryption

While structured lattice-based cryptography currently leads as a practical solution, transitioning to PQC is a complex, resource-intensive process that requires careful planning. Organizations face multiple challenges in adapting their cryptographic infrastructure to ensure quantum security.

The technical and operational challenges are significant:

- Many organizations' legacy systems are deeply integrated with classical encryption standards, such as RSA and ECC.
- Introducing PQC requires extensive testing to ensure new encryption methods do not disrupt current software, hardware, or third-party integrations.
- Moreover, upgrading encryption standards involves careful coordination between cybersecurity, IT, and compliance teams to prevent data leaks or operational downtime during the transition.
- Since PQC has been standardized only recently, there is a risk that potential vulnerabilities may be discovered. If such vulnerabilities are found after the transition, resources will need to be allocated again for the migration process.

Waiting too long to address these challenges brings substantial risks. Delaying implementation until quantum threats become immediate could expose organizations to data breaches or costly non-compliance penalties.

Sensitive data encrypted with traditional methods that cannot be decrypted today could still become vulnerable in future "store-now-decrypt-later" scenarios. Additionally, regulatory pressure is increasing rapidly, with authorities like NIST moving swiftly toward standardized PQC adoption.

Addressing these transition challenges proactively is essential for organizations aiming to protect data, maintain trust, and avoid potential operational disruptions as quantum computing evolves.

Hybrid Encryption: Bridging Classical and Quantum-Safe Security

Given the complexity of immediately shifting entirely to quantum-resistant methods, organizations require a strategic approach that bridges existing cryptography with new PQC standards.

SoftBank and SandboxAQ advocate for a practical solution known as hybrid encryption, which seamlessly blends traditional cryptography with quantum-resistant algorithms. Hybrid encryption provides an immediate layer of quantum-safe security without forcing organizations into costly infrastructure overhauls.

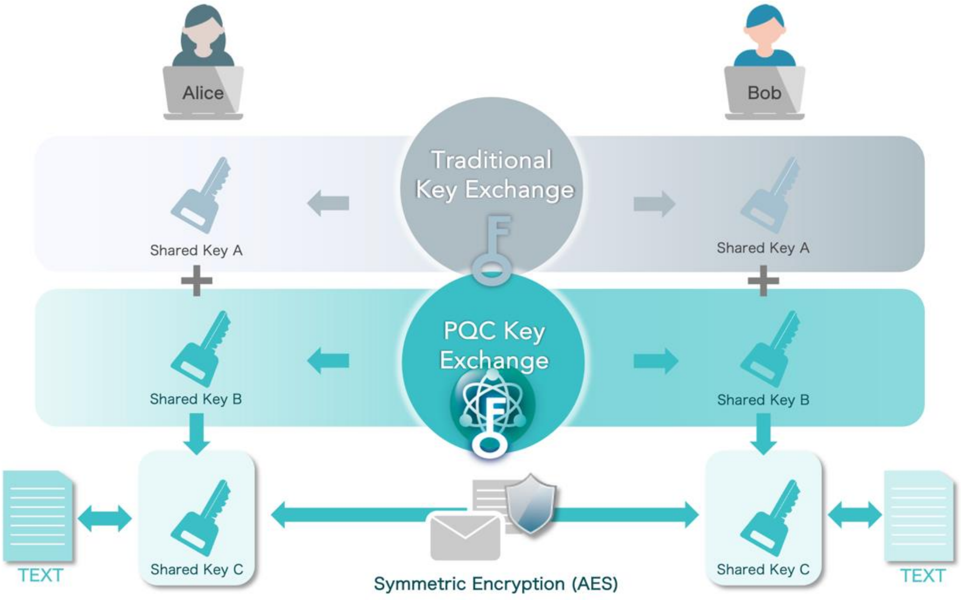

Figure 3. The process of the hybrid key exchange method

Figure 3 illustrates the process of establishing a secure communication channel between two parties, Alice and Bob, using a hybrid key exchange mechanism that incorporates both traditional and PQC. This approach ensures robust security even in the face of potential quantum computing threats.

1. Traditional Key Exchange: Initially, Alice and Bob attempt to establish a shared key (Shared Key A) using a traditional algorithm vulnerable to quantum attacks.

2. PQC Key Exchange: Concurrently, Alice and Bob engage in a PQC key exchange, leveraging their respective PQC key pairs to generate a secure Shared Key B, resistant to quantum attacks.

3. Decryption and Final Key Generation: Bob, possessing the corresponding PQC private key, decrypts the received package to obtain Shared Key A. Both parties now utilize Shared Key A to derive a final symmetric key, Shared Key C.

4. Secure Message Exchange: With Shared Key C in place, Alice encrypts the message ("TEXT") and sends it to Bob, who can then decrypt and read the message securely.

Please note that this method is merely a simplified explanation of the hybrid approach and may differ from actual processing. The implementation of the hybrid method is currently being reviewed in a standardization draft by Internet Engineering Task Force (IETF) as of April 2025.

By simultaneously deploying classical encryption (e.g., ECC) alongside structured lattice-based PQC algorithms, hybrid encryption secures data both today and against future quantum threats. This dual-layer approach allows for the gradual adoption of PQC, minimizing compatibility issues and operational risks.

Key strategic benefits of hybrid encryption include:

- **Immediate Quantum Security:** Immediately protects sensitive data from quantum-enabled attacks.
- **Smooth Compatibility:** Integrating existing infrastructure minimizes disruptions, preventing costly downtime.
- **Regulatory Compliance:** Meets current and anticipated regulatory requirements (e.g., FIPS, PCI-DSS) with minimal adjustments to existing workflows.

Feature	Hybrid Encryption	Pure PQC Encryption
Quantum Resistance	☑ Immediate quantum-safe security	☑ Fully quantum-resistant
Integration Complexity	☑ Minimal; integrates easily into existing infrastructure	ⓘ High; requires significant infrastructure changes
Compatibility with Legacy Systems	☑ High; maintains compatibility with current standards	ⓘ Low; limited compatibility, may require major upgrades
Operational Risk During Transition	☑ Low; phased adoption reduces disruptions	ⓘ Higher; risk of disruption from immediate overhaul
Regulatory Compliance	☑ Easily meets current (e.g., FIPS, PCI-DSS) and future requirements	☑ Meets future quantum-focused standards, but compliance requires immediate, comprehensive updates
Cost and Resource Impact	☑ Moderate; preserves existing investments	ⓘ Higher; requires substantial new resources
Time to Implement	☑ Shorter; phased integration	ⓘ Longer; extensive testing & deployment required

Table 2. Hybrid vs Pure PQC implementation

Real-World PQC Demonstration: SoftBank and SandboxAQ

Recognizing the importance of real-world validation, SoftBank partnered with SandboxAQ to rigorously demonstrate hybrid encryption in authentic user scenarios. The goal was clear: **confirm whether quantum-safe encryption algorithms could provide reliable, practical security without affecting performance in typical day-to-day activities.**

The comprehensive tests simulated various common digital activities, including online gaming, high-definition video streaming, standard web browsing, and secure VPN connections. This approach enabled a realistic assessment of the encryption methods under conditions users regularly experience rather than idealized laboratory setups.

Experimental setup

The experimental setup consisted of a pair of Linux servers, a Cisco WiFi-6 access point and several Android handsets. Generally, an automatic traffic generator would run on the handset and then terminate on the Linux server, with appropriate measurements being taken. To ensure comprehensive coverage, SoftBank tested multiple network technologies widely used in today's global communication landscape, including:

- 5G networks, representing cutting-edge cellular communications
- LTE connections, for widespread mobile data usage
- SmartVPN networks, simulating secure, enterprise-level remote connections
- WiFi environments, typical of both home and office settings

The handsets were running a custom VPN software that would simulate TLS (Transport Layer Security) sessions running in PQC-hybrid mode by re-keying the VPN, using the appropriate cipher suite, each time a TLS HELLO packet was encountered. This would introduce real-world latency to the TLS session emulating the impact of adding PQC key negotiation. Furthermore, traffic shaping was added to simulate congestion and latency which would be experienced in realistic network conditions. The traffic shaping parameters were selected to emulate on-premise WiFi, 5G, LTE and Smart VPN connections.

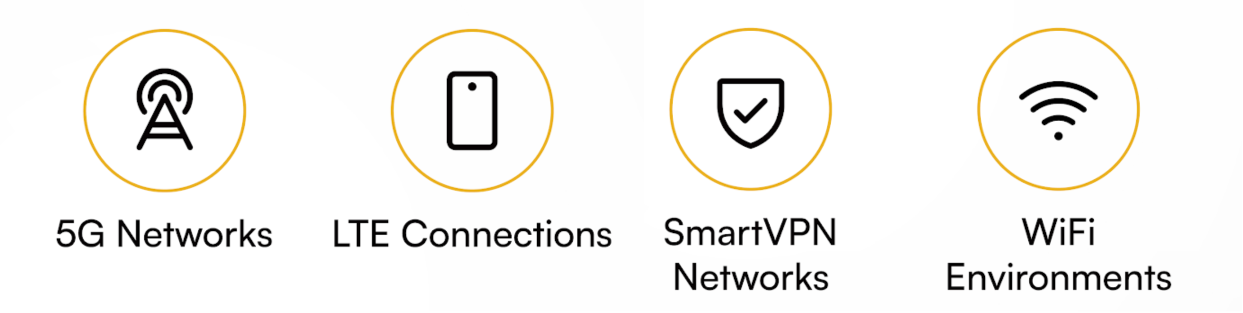

Figure 4. PQC test scenarios

Metrics and algorithms

In each scenario, the study measured critical user-experience metrics:

- **Latency**: Ensuring encryption did not noticeably delay user interactions.
- **Connection Rate**: Confirming connections remained stable and reliable.
- **Device Performance**: Verifying minimal impact on CPU usage and battery life.

Through this testing, we intended to validate the performance of different hybrid encryption methods and show that they wouldn't create obstacles for business and consumer activities.
The algorithms used in the proof-of-concept experiment are listed in the following table, including traditional algorithms and PQC. The selection focused primarily on the algorithms that were still in the third round of the standardization process as of 2022.

Key Exchange

- Traditional Cryptography (Elliptic curve Diffie–Hellman; ECDH)
- Structured Lattice-based Cryptography (ML-KEM, NTRU, Saber)
- Unstructured Lattice-based Cryptography (FrodoKEM)
- Code-based Encryption (BIKE, HQC)
- Isogeny-based Cryptography (SIKE)

Digital Signatures

- Traditional Cryptography (ECDSA)
- Lattice-based Cryptography (ML-DSA, Falcon)

Key Findings and Insights

The real-world testing conducted by SoftBank and SandboxAQ provided clear evidence supporting the practical adoption of hybrid encryption. Structured lattice-based PQC algorithms, particularly ML-KEM and ML-DSA, were highly effective. They had a minimal impact on real-world performance. **Specifically, structured lattice-based algorithms matched traditional encryption methods (such as ECC) across all critical performance areas — including connection latency, CPU load, and reliability.**

These findings underscore the practicality and usability of hybrid PQC in everyday situations. However, not all PQC algorithms performed equally:

- Isogeny-based cryptography, initially considered promising due to smaller key sizes, underperformed significantly.
- It exhibited notably slower connection speeds and higher CPU demands.

- It also suffered from recently identified vulnerabilities, highlighting its limited real-world applicability compared to structured lattices.

For these reasons, isogeny-based cryptography are not included in the standardization process as of April 2025.

Latency

First, we compare the overall latency (time to first byte of the traffic generator request) grouped by PQC algorithm families on a logarithmic scale. As shown in Figure 5, traditional algorithms (ECDH) are the fastest at any security level, followed by structured lattices. This is evident because the center of the top (yellow, 'trad') distribution is the farthest to the left, and the fourth from the top (dark orange, 'struct_lattice') is the next farthest left.

Unstructured lattices (FrodoKEM) do not perform as well but still significantly outperform isogeny-based schemes (SIKE). Code-based schemes (HQC, BIKE) are distributed throughout, but their peak latency is similar to unstructured lattices and isogenies.

Compared to theoretical values from SUPERCOP (System for Unified Performance Evaluation Related to Cryptographic Operations and Primitives), we notice that despite isogenies having much longer computation times than structured lattices, the difference in the figure isn't as obvious. This is because the TTFB latency here includes not only the KEM part but also the rest of the TLS handshake, which uses a Dilithium certificate. Therefore, the performance is offset by a constant overhead of 100-200ms, making the visual difference between KEM parts smaller than expected and resulting in tighter grouping across all families. This dilution of KEM effects reduces differences between KEMs but provides useful context since, in real-world applications, KEMs are just one part of a multi-functional handshaking protocol.

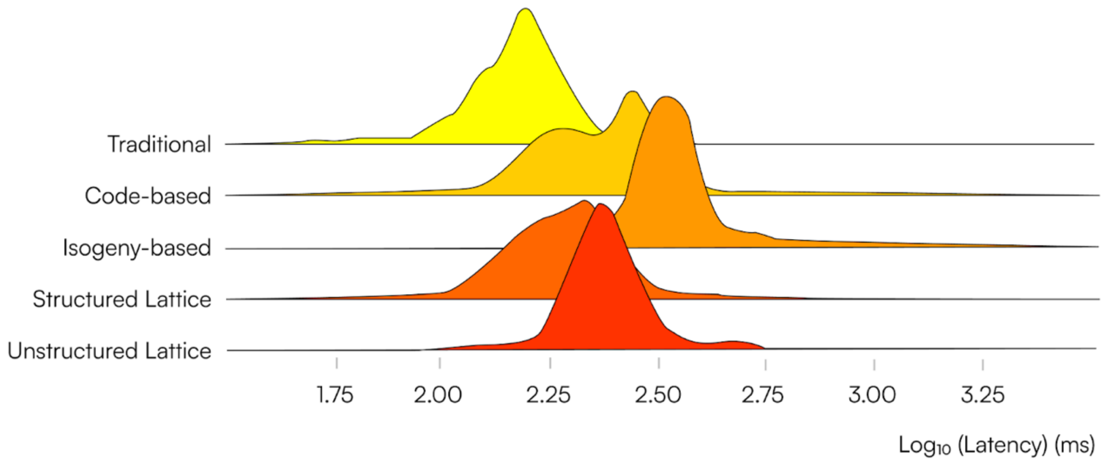

Figure 5. Latency (in ms) of all asymmetric cryptography for WiFi deployment. Distributions are shown on a logarithmic scale in order to group the results and distributions for easy visual comprehension.

Concurrent Connection

We also compared the impact of key exchange algorithms on the allowable number of concurrent connections. As shown in the graph, the hybrid approach with PQC algorithms resulted in a decrease in the number of concurrent connections compared to traditional algorithms. Among them, algorithms based on structured lattice problems (ML-KEM, NTRU, Saber) showed minimal degradation. In contrast, isogeny-based algorithms (SIKE) exhibited significant performance degradation in terms of concurrent connections.

Code-based algorithms, while experiencing some decline in performance, demonstrate greater resilience compared to isogeny and unstructured lattice-based algorithms. This outcome highlights their potential as a viable alternative to structured lattice-based algorithms, which are currently considered the standard for PQC. The superior performance of code-based algorithms suggests that they could play a crucial role in ensuring the security of sensitive data and communications in the era of quantum computing.

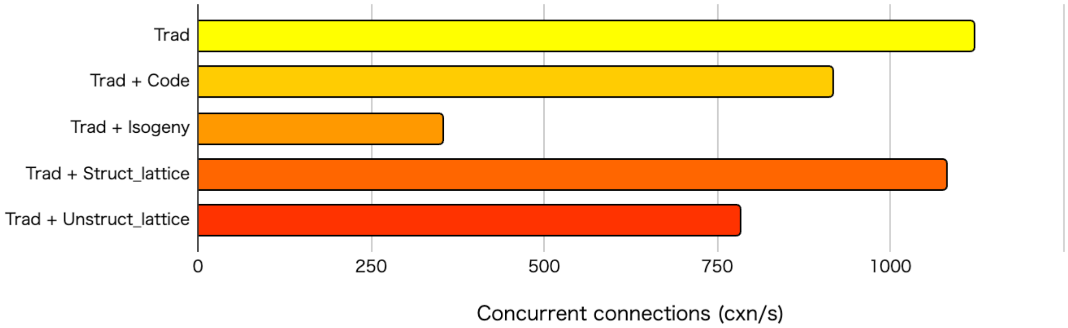

Figure 6. Concurrent connection rate per algorithm

CPU & Memory usage

Figure 7 shows a scatter plot of average CPU and memory usage for each algorithm family. The values are relative to the minimum CPU and memory usage of the server during the multi-day experiment, representing the positive difference in the overall CPU and memory time series. Although isogenies (black points) have low memory requirements due to their small size, they are extremely computationally intensive. This results in larger black points, indicating high latencies caused by the computational load.

On the other hand, unstructured lattices (red points) require less computation than isogenies but have higher memory utilization due to their large sizes. These large key sizes likely result in larger point sizes, as transmitting them over a network with limited bandwidth increases latency. It's important to note that while CPU usage distributions accurately represent different PQC algorithms, memory usage distributions are influenced by the underlying OS memory management behavior.

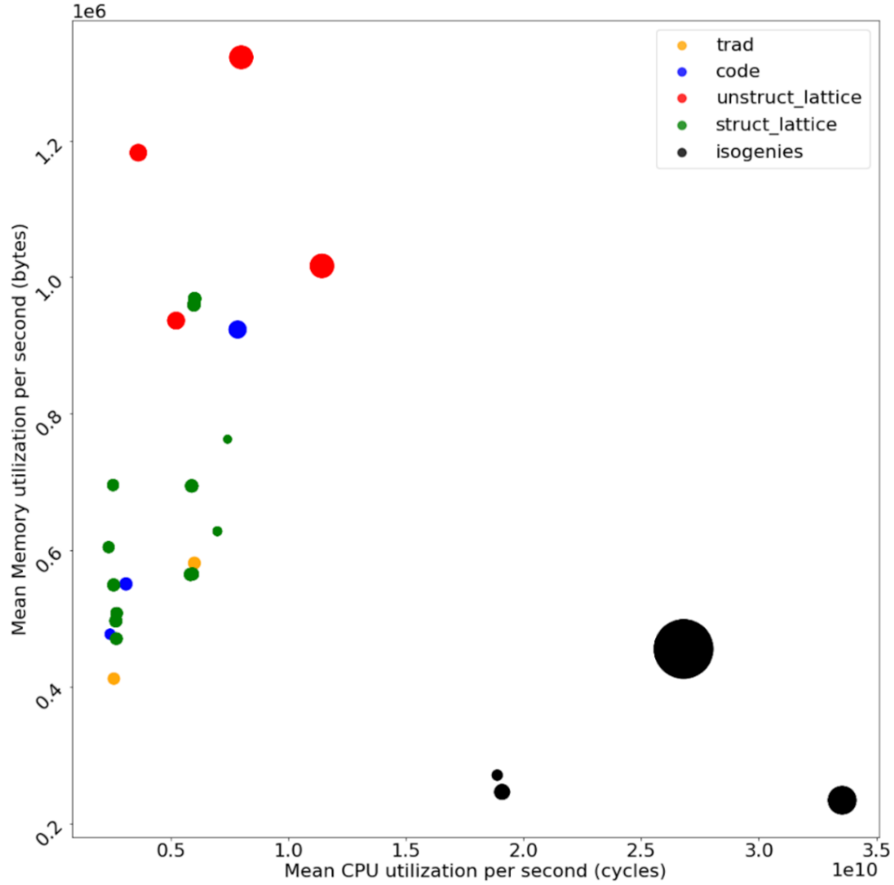

Figure 7. Mean CPU usage (instruction cycles) versus mean memory utilization (bytes) for each algorithm. Colors represent the specific family of algorithms with different security parameters and the size of the spot represents a relative latency in key exchange.

Handshake size for Digital Signature

This figure shows the communication size during the handshake phase of PQC hybrid digital signature algorithms. A traditional algorithm (ECDSA) has a very small communication size, while PQC algorithms based on structured lattices and other approaches have larger sizes. Combining traditional and PQC algorithms increases the communication size further.

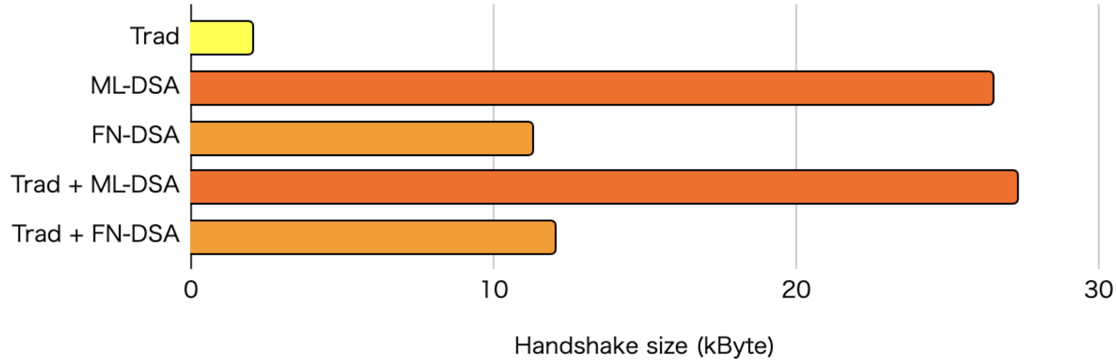

Figure 8. The mean handshake size in kbytes

Latency for Digital Signature

Considering the communication size, implementing digital signature algorithms might seem challenging at first glance. However, from the perspective of latency, it is clear from the figure that PQC (Post-Quantum Cryptography) is highly efficient. Both the time taken for signing and verifying digital signatures show that the latency of PQC algorithms is less than a quarter of that of traditional cryptography. Additionally, for ML-KEM (Machine Learning Key Encapsulation Mechanism), the computation is completed in a very short time, less than 10%.Therefore, it can be seen that the impact on latency is minimal.

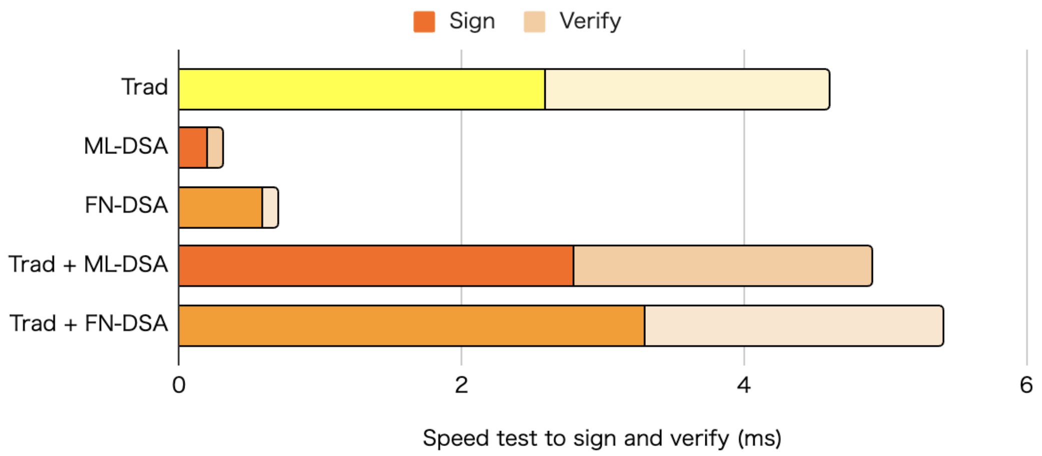

Figure 9. The latency for the digital signature to sign and to verify in ms

Observations

The demonstration revealed that PQC algorithms were rarely the performance bottleneck during stress tests.

- Network conditions — such as bandwidth limitations — proved the most significant factors influencing user experience.
- This finding confirms that structured lattice-based PQC algorithms like Kyber and Dilithium are highly scalable and practical for widespread deployment.

These results position structured lattice-based hybrid encryption as the clear and viable pathway forward for organizations aiming to secure their data effectively against quantum threats.

However, the testing also revealed that in some use cases—such as those involving a large volume of digital signatures—the handshake size may increase when using hybrid signature schemes. While this had minimal impact in our tested scenarios, such effects could become significant in communication environments with heavy signature traffic. Therefore, it is important for organizations to validate PQC integration against their specific network and application requirements.

Actions Toward Early Adoption of PQC

Benefits of Early Adoption of PQC

The demonstration experiment by SoftBank and SandboxAQ clearly showed that hybrid encryption methods are a practical and effective solution for companies preparing for the quantum computing era.

Hybrid encryption methods are a powerful means to protect organizational confidential information against modern cyber threats and prepare for the advancement of quantum computing. On the other hand, it is necessary to carefully select and verify algorithms to ensure they meet requirements, considering factors such as the communication size of signature algorithms and the CPU load due to algorithm performance. This verification not only highlights practicality but also reveals differences and challenges associated with the algorithms.

Taking proactive steps toward quantum-safe encryption positions organizations for sustained security and competitive advantage in an evolving threat landscape.

Immediate adoption of hybrid PQC solutions offers significant benefits:

- **Proactive Data Protection**: Organizations can immediately secure sensitive information from emerging quantum threats, especially protecting data vulnerable to "store-now-decrypt-later" attacks.
- **Compliance Assurance and Risk Reduction**: Regulatory frameworks such as FIPS, PCI-DSS, and GDPR increasingly require robust cryptographic protections. Early adoption of PQC ensures continued compliance, avoiding potential regulatory penalties or reputational damage due to breaches.
- **Cost Efficiency and Investment Protection**: Transitioning proactively reduces the long-term financial and operational burdens associated with rushed, reactive upgrades. Hybrid encryption allows organizations to preserve their existing cryptographic investments while gradually transitioning to PQC standards.
- **Enhanced Trust and Reputation**: By demonstrating forward-thinking security practices, organizations gain credibility with customers, partners, and regulators. Early PQC adoption signals proactive security leadership, enhancing market trust and competitive positioning.

By acting early, businesses mitigate future risks, simplify compliance efforts, and secure their critical data for the long term — positioning themselves confidently ahead of quantum computing developments.

Best Practices for Your Organization's PQC Transition

Successfully transitioning to quantum-safe encryption involves deliberate planning and structured execution. Organizations should follow clear, practical steps to ensure a smooth adoption of PQC.

Step #1: Conduct a Cryptographic Inventory

Begin by thoroughly cataloging all cryptographic systems currently in use. Create detailed documentation outlining precisely which encryption methods (such as RSA, ECC, or digital signatures) protect your sensitive data. Don't overlook embedded cryptography, certificates, key-management processes, hardware security modules, and third-party services.

Step #2: Test and Evaluate Algorithms

Rank your systems based on data sensitivity, regulatory compliance, and vulnerability to future quantum threats. Prioritize critical infrastructures and high-value data, such as financial records, health information, or intellectual property, that require long-term confidentiality. Identify systems requiring more immediate protection or significant resources during a transition.

Step #3: Build Crypto-Agility

Adopting new cryptography often involves technical hurdles. Prepare by creating flexible frameworks capable of integrating new algorithms quickly and seamlessly. Abstraction layers within cryptographic libraries or centralized crypto management services help minimize the effort required when future upgrades or algorithm switches become necessary. You can also adopt frameworks or APIs to support multiple cryptographic standards without major architectural changes.

Step #4: Adopt a Hybrid Encryption Strategy

To safeguard data today and tomorrow, implement hybrid encryption that pairs quantum-safe algorithms with established classical cryptography. You can do this by layering classical encryption (e.g., RSA, ECC) with quantum-safe algorithms.

This dual-layer approach protects your data immediately while providing flexibility to transition gradually to fully quantum-resistant cryptography. This ensures your organization is protected even if some PQC methods encounter vulnerabilities down the line, significantly reducing risk.

Recommendations for Transitioning Based on Demonstrated Results

As quantum computing creates new, urgent threats, the need for quantum-safe encryption solutions has never been clearer. Traditional cryptographic methods like RSA and ECC will be outpaced by the leaps in future fault-tolerant quantum computing, putting sensitive business, consumer, and government data at risk.

Through rigorous real-world testing, SoftBank and SandboxAQ have demonstrated that structured lattice-based **hybrid encryption — combining classical encryption with quantum-resistant algorithms — offers organizations a practical, effective way to address these challenges.**

Early adoption of hybrid encryption provides immediate security, ensures compliance with emerging standards, and safeguards critical information from "store-now-decrypt-later" attacks. Beginning with cryptographic data asset inventorying, organizations must act proactively, testing PQC algorithms and implementing crypto-agility frameworks to strengthen their security posture and avoid the inevitable attempts at data exfiltration.

SoftBank and SandboxAQ's successful demonstrations confirm not only the viability of this approach but also the minimal disruption to user experience and network performance across various network scenarios, including on-premise Wi-Fi stress tests.

By following the best practices outlined here and leveraging insights from SoftBank and SandboxAQ, organizations can confidently navigate the complex transition to quantum-safe encryption, ensuring robust data protection today and readiness for tomorrow's security landscape.

Moving forward, SoftBank and SandboxAQ remain committed to developing solutions that help organizations transition to PQC and to accelerating its adoption across industries.

Reference

[1]

"NIST Releases First 3 Finalized Post-Quantum Encryption Standards." National Institute of Standards and Technology, August 2024, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[2]

"SoftBank Corp. and Sandbox AQ to Jointly Implement Next-Generation Cryptosystem Resilient to Cyber Attacks from Quantum Computers." SoftBank Corp, 23 March 2022, https://www.softbank.jp/en/corp/news/press/sbkk/2022/20220323_01/.

[3]

"SoftBank Corp. and SandboxAQ Jointly Verify Hybrid Mode Quantum-safe Technology." SoftBank Corp, 28 February 2023, https://www.softbank.jp/en/corp/news/press/sbkk/2023/20230228_01/.