

Post-Quantum Cryptography: Preparing for the Quantum Era

Sun Bing

October 16, 2026

Abstract

The emergence of large-scale, fault-tolerant quantum computers threatens the foundational hardness assumptions of classical public-key cryptography, including RSA, ECC, and Diffie-Hellman. Post-quantum cryptography (PQC) develops algorithms secure against both classical and quantum attacks. This white paper outlines the quantum threat, introduces leading PQC families (with emphasis on lattice-based schemes), details NIST standardization efforts, provides global migration roadmaps, and explores practical applications in smart metering infrastructure.

Key Takeaways

- NIST has finalized three principal PQC standards: ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205).
- Global migration deadlines converge on **2030–2035**; critical infrastructure faces earlier mandates.
- **Hybrid cryptography** (classical + PQC) is the recommended transition strategy during migration.
- Smart metering and embedded IoT require special attention to bandwidth, HSM, and power constraints.
- Organizations should begin with a **cryptographic inventory**, this alone typically takes 12 to 18 months.

1 Introduction

Today’s asymmetric cryptography relies on the computational difficulty of problems such as integer factorization (RSA) and the discrete logarithm problem (ECC, Diffie-Hellman). These underpin secure communications, digital signatures, and key exchange protocols.

Shor’s algorithm [Sho99] solves these problems in polynomial time on a sufficiently powerful quantum computer, potentially breaking 2048-bit RSA or 256-bit ECC in hours or days. This enables “harvest-now, decrypt-later” (HNDL) attacks on long-lived sensitive data. In an HNDL attack, adversaries intercept and store encrypted traffic today with the intent of decrypting it once a cryptographically relevant quantum computer becomes available, which is often called **Q-Day**. Data with confidentiality requirements spanning decades (health records, classified communications, energy grid telemetry) is therefore *already* at risk, even before a quantum computer exists.

Grover’s algorithm [Gro96] offers a quadratic speedup for symmetric key search, mitigated by doubling key lengths (e.g., AES-256 remains secure against quantum key search). Hash collision resistance faces a stronger quantum speedup (to approximately $2^{n/3}$), requiring larger hash outputs to maintain equivalent security. Symmetric encryption (AES-256) and hash functions (SHA-384/SHA-512) remain quantum-resistant with their current key/output sizes. Thus, the primary urgency concerns public-key systems.

Key drivers for adopting PQC include:

- Protecting data with confidentiality requirements spanning decades.
- Preventing retroactive decryption of archived communications.

Table 1: Public Key and Signature/Ciphertext Size Comparison

Algorithm	Type	Public (B)	Key (B)	Sig./Ciphertext (B)	NIST Level
ECDSA P-256	Classical (ECC)	32–65		64	~128-bit
ML-DSA-65	Lattice (Hash/Abort)	1,952		3,309	3
ML-DSA-87	Lattice (Hash/Abort)	2,592		4,627	5
ML-KEM-768	Lattice (KEM)	1,184		1,088	3
ML-KEM-1024	Lattice (KEM)	1,568		1,568	5
SLH-DSA-192s	Stateless Hash-Based	48		16,224	3
SLH-DSA-256s	Stateless Hash-Based	64		29,792	5

- Ensuring long-term integrity of digital signatures and certificates.
- Complying with evolving regulations and national security mandates.

A practical but often overlooked risk is certificate lifetime. Organizations routinely issue certificates with 3 to 5 year validity. Certificates issued today may still be in use during the quantum threat window, creating a “legacy certificate” problem. Auditing certificate lifetimes and renewal cycles should be part of every organization’s initial discovery phase.

2 Post-Quantum Algorithms

PQC algorithms are built on mathematical problems believed to resist quantum speedups. Major families include:

- **Lattice-based:** Based on hard problems in high-dimensional geometry (e.g., Shortest Vector Problem (SVP), Learning With Errors (LWE)). These offer strong security reductions, efficiency, and versatility, forming the core of current standards.
- **Hash-based:** Rely on the collision resistance of cryptographic hash functions (e.g., stateless hash trees). They provide robust security proofs but typically yield larger signatures.

Lattice-based schemes (e.g., ML-KEM and ML-DSA) are the primary NIST standards [oST24b, oST24a], with hash-based SLH-DSA [oST24c] serving as a conservative backup. Other families such as code-based and multivariate remain under evaluation or research.

PQC algorithms generally feature larger keys and ciphertexts than classical counterparts. Classical systems exploit compact representations enabled by factoring or discrete logs, while PQC relies on higher-dimensional structures (matrices, polynomials, or trees) for equivalent security [Scr25]. Table 1 summarizes the operational impact of these size differences.

2.1 Lattice-Based Cryptography

Lattice-based cryptography relies on lattices—discrete subgroups of $\mathbb{R}^n$ generated by integer combinations of basis vectors. Core problems include 1) Shortest Vector Problem (SVP) [Muk21], 2) Closest Vector Problem (CVP) [Muk21], and 3) Learning With Errors (LWE) [Reg05]. They rely on geometric hardness in high dimensions with no exploitable periodicity.

What is a Lattice?

In mathematics, a lattice is an infinite grid of regularly spaced points in an n -dimensional space. It is formed by taking all possible integer linear combinations of a set of linearly independent vectors, called the basis.

If you have a basis $B = \{b_1, b_2, \dots, b_n\}$, any point v in the lattice can be represented as:

$$v = \sum_{i=1}^n x_i b_i$$

where x_i are integers ($\mathbb{Z}$).

The “Hard” Aspect: In 2D, finding your way around a grid is easy. But when n scales to hundreds or thousands of dimensions, finding specific geometric relationships between points becomes computationally impossible unless you know a “good” basis (vectors that are short and nearly orthogonal).

Foundational Hard Problems

The security of lattice-based cryptography relies on the assumption that certain geometric problems are intractable in high dimensions. The two most famous are SVP and CVP.

Shortest Vector Problem (SVP). Given a lattice, the goal of SVP is to find the shortest non-zero vector in that lattice.

Intuition: If you are standing at the origin $(0, 0, \dots, 0)$, which grid point is closest to you?

Why it’s hard: With a “bad” basis (long, highly skewed vectors), the grid looks chaotic, and finding the shortest vector requires searching through an exponential number of possibilities.

Closest Vector Problem (CVP). Given a lattice and a target point t that is not in the lattice, the goal of CVP is to find the lattice point closest to t .

Intuition: If you drop a pin anywhere on the high-dimensional grid, which actual grid intersection is closest to that pin?

Why it’s hard: Similar to SVP, without a good basis, calculating which combination of vectors gets you closest to the target point is an NP-hard problem.

Learning With Errors (LWE)

While SVP and CVP are great theoretical problems, they are not always easy to build actual encryption schemes out of. In 2005, Oded Regev [Reg05] introduced Learning With Errors (LWE), which bridged the gap between lattice math and practical cryptography. LWE is an algebraic problem that looks like basic linear algebra, but with a twist.

Imagine a secret vector s . You are given a series of equations where s is multiplied by a known matrix A . If you were just given A and the result b :

$$b = A \cdot s \pmod{q}$$

You could easily solve for s using standard Gaussian elimination. Instead, LWE introduces a small amount of random noise or error (e) to each equation:

$$b = A \cdot s + e \pmod{q}$$

Because of the error vector e , standard linear algebra fails completely. The **search** version aims to find the secret s given A and b . The **decisional** version asks whether a given pair (A, b) is a genuine LWE instance or uniformly random. Regev proved a worst-case to average-case reduction for the search problem: solving LWE efficiently would imply solving SVP on any lattice. Because LWE can be easily formatted as matrix multiplications, it is incredibly efficient to implement in software and hardware, forming the backbone of modern post-quantum standards.

3 NIST PQC Standards

In response to this existential threat, the National Institute of Standards and Technology (NIST) finalized and published its initial, official suite of Federal Information Processing Standards (FIPS) for PQC, transitioning the world from theoretical research into active commercial deployment.

Organizations must now baseline their current cryptographic posture and initiate structured migration strategies to comply with emerging global mandates. While many jurisdictions are aligning with NIST standards, several countries and regions are also developing or adopting customized or sovereign algorithms to address national security priorities and promote technological self-reliance (see Section 4 for examples).

Table 2: NIST PQC Standards

Standard	Algorithm	Cryptographic Type	Primary Target	Replacement
FIPS 203 [oST24b]	ML-KEM	Key Encapsulation Mechanism (Lattice-Based)	Diffie-Hellman (DH, ECDH), RSA Key Transport	
FIPS 204 [oST24a]	ML-DSA	Digital Signature Scheme (Lattice-Based)	RSA-Sig, ECDSA, Ed25519 ²	
FIPS 205 [oST24c]	SLH-DSA	Digital Signature Scheme (Stateless Hash-Based)	RSA-Sig, ECDSA (as a conservative backup)	

Table 3: NSA CNSA 2.0 Compliance Timeline

System Category	Support & Pre-fer	Exclusive Use Required
Software and Firmware Signing	2025	2030
Web Browsers, Servers, Cloud Services	2025	2033
Traditional Networking (VPNs, Routers)	2026	2030
Operating Systems	2027	2033
Custom Applications and Legacy Equipment	—	2033

3.1 The NIST PQC Standards

NIST’s multi-year international evaluation culminated in the release of three foundational standards designed to replace current public-key infrastructure (PKI) components.

NIST has officially finalized the first three Post-Quantum Cryptography (PQC) standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) as shown in Table 2. These represent the core set of quantum-resistant algorithms ready for broad adoption.

NIST continues to actively evaluate and standardize additional algorithms to provide further options, performance improvements, and cryptographic diversity [oST26b]. Notable examples include:

1. **FN-DSA** (FIPS 206, based on Falcon): a compact lattice-based digital signature scheme, with its initial public draft issued [oST26a].¹ However, FN-DSA is **not included in the NSA CNSA 2.0 commercial national security algorithm suite**, which currently specifies only ML-KEM and ML-DSA for federal use.
2. **HQC**: a code-based Key Encapsulation Mechanism (KEM) selected in March 2025 as a backup to ML-KEM, with its draft standard expected in 2026 and final publication targeted for 2027 [oST25].

3.2 NSA CNSA 2.0 Timeline

For vendors and contractors in the U.S. federal and defense supply chain, the NSA’s Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) establishes phased, mandatory deadlines for replacing classical public-key cryptography with quantum-resistant algorithms. Table 3 summarizes the category-by-category timeline.

3.3 PQC Security Categories

While NIST continues to use traditional bit-length security metrics to characterize the strength of algorithms against classical attacks, it adopts a different approach for post-quantum cryptography.

¹FN-DSA and the original Falcon algorithm are not wire-compatible; implementations must use FN-DSA parameters and serialization formats exclusively.

Table 4: Post-Quantum Security Categories

CAT	Reference Problem	Example
1	Key search on a block cipher with a 128-bit key.	AES-128
2	Collision search on a 256-bit hash function.	SHA-256
3	Key search on a block cipher with a 192-bit key.	AES-192
4	Collision search on a 384-bit hash function.	SHA-384
5	Key search on a block cipher with a 256-bit key.	AES-256

Post-quantum security is expressed through five broad security categories (Levels 1 to 5) [MP24].

Each category is anchored to a well-understood and comparatively easy-to-analyze reference primitive from classical cryptography. These reference problems serve as a conservative security floor across a wide range of potentially relevant attack metrics. NIST designed this classification system based on the security strengths provided by established symmetric cryptographic standards (e.g., AES and SHA-3 at various key lengths). Table 4 summarizes the five NIST PQC security categories and their corresponding classical reference baselines.

4 Roadmap for Migration

Governments and organisations worldwide are developing structured migration strategies to transition from classical to quantum-resistant cryptography. These plans vary in ambition, timelines, and focus. It ranges from mandatory deadlines for critical infrastructure to guidance-based frameworks. While approaches differ, common themes include crypto-agility, hybrid transitions, risk-prioritised migration, and national testing/certification capabilities.

Hybrid cryptography combines a classical algorithm (e.g., ECDH) with a post-quantum algorithm (e.g., ML-KEM) such that the overall scheme remains secure if either one is broken. This provides backwards compatibility during transition and is recommended by NIST, BSI, and ANSSI.

Crypto-agility is the architectural property of a system that allows cryptographic algorithms to be swapped without changing application logic or data formats. For embedded systems, this means abstracting cryptography behind a firmware HAL or PKCS#11 layer so that ML-DSA can replace ECDSA via an over-the-air (OTA) update.

Table 5 summarizes key migration timelines and approaches across major jurisdictions.

Key Observations from Table 5:

- Accelerated timelines for critical infrastructure: Most countries prioritise CII/high-risk systems for earlier migration (2028–2030).
- 2030–2035 completion targets: A common global window for substantial or full transition.
- Hybrid and agile focus: Nearly all frameworks recommend hybrid cryptography during transition and building crypto-agility into new systems.
- Divergent approaches: Some (e.g., Australia, UK) set firm national targets, while others (e.g., Singapore, Malaysia) lean toward guidance and sector-led implementation.

Besides the above table, NIST will deprecate and ultimately remove quantum-vulnerable algorithms from its standards by 2035, with high-risk systems transitioning much earlier [MP24]. This global momentum highlights the need for organisations to begin cryptographic discovery and planning immediately, regardless of jurisdiction. Alignment with NIST standards is a near-universal foundation, while many countries are also investing in sovereign capabilities and testing infrastructure.

5 Use Cases

Next, we list some use cases of PQC in the context of smart metering.

Table 5: PQC Migration Timelines

Country / Region	Algorithms Under Consideration	Timeline Summary
Australia	NIST standards (ML-KEM, ML-DSA, SLH-DSA)	2026: Refined transition plan completes. 2028: Migration commences (priority on critical systems). 2030: Full PQC transition completed [Aus25].
European Union	NIST standards + hybrid schemes (potential EU-specific additions)	2026: Initial national roadmaps and planning under NIS2 and DORA. 2030: High-risk use cases migrated. 2035: Medium/low-risk use cases completed as feasible [Cyb25].
India	NIST standards + indigenous development	2027 (CII): Foundations & pilots. 2028–2029 (CII): High-priority migration & full resiliency. 2028–2033: Enterprise-wide adoption [Dep26].
Singapore	NIST standards (monitoring & adoption)	2027: Completion of organizational PQC migration and transition plan. 2028: Implementation of quantum-safe procurement policies. 2031: Full completion and operational migration to quantum-safe systems [CGI26].
United Kingdom	NIST standards (ML-KEM, ML-DSA, SLH-DSA)	2028: Discovery, inventory & initial migration plan. 2031: High-priority systems migrated & plan refined. 2035: Full migration across all systems, services, and products [Nat25].
Malaysia	Sovereign algorithms in development + NIST standards	2025–2027: Preparation, awareness & planning. 2026–2030: Piloting & high-priority implementation. 2030–2035+: Full migration & quantum resilience [Cyb24].

5.1 Secure Firmware Updates and Device Management

Challenge: Smart meters need remote firmware updates for bug fixes, feature additions, or security patches. These updates are often authenticated with digital signatures (e.g., ECC-based like NIST P-256), which quantum computers could forge.

PQC Application: Migrate to post-quantum digital signatures (e.g., ML-DSA) for authenticating updates.

Benefits: Ensures only authorized updates are applied, preventing malware injection or grid manipulation.

5.2 Authentication and Key Establishment (AKA) Protocols

Challenge: Mutual authentication between smart meters, head-end systems, utilities, and other grid components. Traditional ECC or RSA-based schemes are vulnerable to quantum attacks (e.g., Shor’s algorithm).

PQC Application: Implement quantum-resistant AKA protocols, lattice-based key encapsulation mechanisms (KEMs like ML-KEM), or hybrid schemes for session key establishment. Research includes PQC for smart grid communications to protect against man-in-the-middle and other attacks.

Benefits: Secure bidirectional communication for real-time data reporting, demand response, and control signals.

5.3 Secure Boot, Device Identity, and PKI Integration

Challenge: Establishing trusted device identities and boot processes in physically accessible meters (often outside homes).

PQC Application: Integrate PQC into Smart Meter PKI and hardware security modules (HSMs) or Secure Elements for key generation/storage. Hybrid classical and PQC certificates are common during transition.

Benefits: Long-term device authenticity and resistance to supply-chain or physical attacks.

5.4 Embedded and IoT Constraints

Smart meters are severely resource-constrained devices. The operational impact of PQC on these systems deserves explicit attention:

Bandwidth impact. ML-DSA signatures are approximately $50\times$ larger than ECDSA signatures. For smart meters using narrowband protocols such as NB-IoT or power-line communication (PLC), a single PQC handshake or firmware signature block can consume a significant fraction of the daily payload budget.

Secure Element and HSM limitations. Many existing secure elements and HSMs were designed for classical ECC/RSA operations and lack dedicated PQC acceleration or sufficient memory for lattice arithmetic. Migration may require a hardware refresh or firmware upgrades to the secure subsystem.

Power and energy. Lattice operations are computationally fast, but the increased data volume and larger arithmetic units may extend CPU wake-time on battery-assisted meters, directly affecting battery life estimates.

6 PQC Ready Meter

Next, we would like to define PQC ready meter.

Definition 6.1 (PQC Ready Meter) *A PQC ready meter is a smart meter whose hardware, root of trust, and firmware architecture can run standardized post-quantum cryptography for its entire service life. PQC can be active from day one or switched on later by a secure over-the-air update, and in neither case does the meter need replacing in the field.*

In practice, a meter qualifies as PQC ready when it meets all of the following:

- Quantum-safe root of trust. The immutable boot chain verifies firmware with a post-quantum signature, or with a hybrid classical + PQC signature.
- Hardware headroom. The MCU, secure element, RAM, and non-volatile memory are sized for post quantum algorithms, larger keys, and certificates, with margin for future parameter sets.
- Crypto-agile firmware. Cryptography sits behind an abstraction layer, so algorithms can be swapped through updates without changing application logic or data formats.
- Post-quantum safe communication. All communication is protected with post-quantum safe key establishment and authentication, combined with classical algorithms in hybrid mode during the transition.
- Quantum-safe provisioning. Quantum-safe key material is provisioned in a secure environment during manufacture. The meter can hold hybrid or PQC certificates, and its trust anchors can be securely updated to support rollover to new algorithms over its lifetime.

The core idea is simple. Anything firmware can change, a meter can fix later. Anything burned into silicon or the boot ROM has to be right on the day the meter leaves the factory.

7 Where We Are Now

Kimbal partners with a leading post-quantum cryptography company that has already delivered quantum-safe solutions across enterprise IT, hardware security, and financial services, to implement post-quantum safe Advanced Metering Infrastructure (AMI) solutions.

7.1 Post-Quantum Safe AMI Solutions

Kimbal is implementing an end-to-end quantum-resistant AMI architecture. Our focus spans device security, communications, and manufacturing:

Crypto-Agility by Design:

Across all Kimbal solutions—smart meters, head-end systems, provisioning tools, and communication stacks—crypto-agility is a foundational design principle rather than an afterthought. Every device and system is architected so that cryptographic algorithms can be updated and replaced through updates without disrupting core operations. By building crypto-agility into the hardware and software from day one, Kimbal ensures that our AMI infrastructure remains secure and compliant not just against today’s standards, but against tomorrow’s as well.

Smart Meter Security:

- **Secure Boot:** Device boot chains are cryptographically verified using post-quantum digital signatures (ML-DSA), ensuring only authentic firmware executes.
- **Firmware Over-The-Air (FOTA):** Firmware updates are signed with quantum-safe signatures and verified at the meter side.
- **End-to-End Communication:** Meter-to-HES links are protected with hybrid key exchange and authenticated with PQC signatures, preventing man-in-the-middle and forgery attacks.

Production and Provisioning:

- Manufacturing lines use HSM-backed provisioning stations to inject quantum-safe key material during production.
- Lifecycle key management—revocation, renewal, and rollover—is designed for crypto-agility to accommodate future algorithm updates.

DLMS Protocol Integration:

Kimbal is integrating post-quantum cryptographic algorithms with the **DLMS/COSEM** communication protocol, the internationally standardized suite for smart metering and smart grid applications. Our current work includes:

- Mapping ML-KEM and ML-DSA into the DLMS security framework for key agreement and authentication.
- Developing a formal proposal for **DLMS Security Suite 3** that defines PQC algorithm profiles, certificate formats, and handshake sequences for quantum-safe meter-to-utility communication.
- Ensuring backward compatibility with existing DLMS Security Suite 0/1/2 deployments through hybrid transition modes.

By combining Kimbal’s deep expertise in embedded firmware, secure provisioning, and AMI systems with a battle-tested PQC technology partner, we are translating post-quantum standards into production-ready, quantum-safe critical infrastructure today.

8 Conclusion

The advent of large-scale quantum computers poses a fundamental threat to classical public-key cryptography through algorithms such as Shor’s. Post-Quantum Cryptography (PQC) provides the necessary protection using well-established quantum-resistant algorithms, primarily lattice-based schemes for key encapsulation and digital signatures, supported by hash-based alternatives as backup. While PQC introduces larger keys and signatures, its deployment is essential for protecting long-lived data, critical infrastructure, and digital signatures. Smart metering systems highlight both the urgency and challenges. Global migration timelines converge on 2030–2035 for most sectors, with earlier deadlines

for critical systems. Organizations must prioritize cryptographic inventory, hybrid transitions, and crypto-agility to ensure long-term security.

In summary, adopting PQC is no longer optional but a strategic necessity. Proactive migration today will safeguard critical infrastructure and digital trust in the quantum era.

Immediate Actions for Organizations

1. **Cryptographic Inventory.** Identify every use of RSA, ECC, DH, and DSA in firmware, TLS, VPNs, and PKI across the enterprise.
2. **Risk Triage.** Classify systems by data longevity and exposure—critical information infrastructure (CII) first, consumer IoT later.
3. **Vendor Roadmap Review.** Ask every vendor for their PQC migration plan and CNSA 2.0 alignment.
4. **Pilot Hybrid Schemes.** Deploy ML-KEM + ECDH hybrid key exchange on non-production systems to validate interoperability.
5. **Certificate Audit.** Reduce certificate lifetimes and begin planning a PQC-enabled certificate authority hierarchy.

References

- [Aus25] Australian Signals Directorate (ASD). Planning for post-quantum cryptography. Technical report, Australian Cyber Security Centre (ACSC), Australian Signals Directorate, September 2025. ASD-2025a.
- [CGI26] Cyber Security Agency of Singapore, Government Technology Agency, and Infocomm Media Development Authority. *Quantum-Safe Migration Handbook*. Cyber Security Agency of Singapore, v1 edition, July 2026.
- [Cyb24] CyberSecurity Malaysia. Post-quantum cryptography migration framework. Technical report, Ministry of Digital, CyberSecurity Malaysia, 2024. CD-4-RPT-2724-PQCMigration-V1 (MY-2024).
- [Cyb25] Cyber Security Agency of Singapore (CSA). Quantum-safe handbook. Technical report, Cyber Security Agency of Singapore, October 2025. Draft for Public Consultation (CSA-2025).
- [Dep26] Department of Science and Technology (DST), Government of India. India’s roadmap for quantum resiliency. Technical report, National Quantum Mission Task Force, 2026. IN-2026a.
- [Gro96] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
- [MP24] Dustin Moody and Ray Perlner. Transition to post-quantum cryptography standards. NIST Internal Report (IR) 8547 ipd, National Institute of Standards and Technology, November 2024. Initial Public Draft (IPD).
- [Muk21] Priyanka Mukhopadhyay. Faster provable sieving algorithms for the shortest vector problem and the closest vector problem on lattices in ℓ_p norm. *Algorithms*, 14(12):362, 2021.
- [Nat25] National Cyber Security Centre (NCSC). Timelines for migration to post-quantum cryptography. Technical report, National Cyber Security Centre, March 2025. NCSC-2025b.
- [oST24a] National Institute of Standards and Technology. Module-lattice-based digital signature standard. Technical Report FIPS 204, U.S. Department of Commerce, August 2024.
- [oST24b] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard. Technical Report FIPS 203, U.S. Department of Commerce, August 2024.

- [oST24c] National Institute of Standards and Technology. Stateless hash-based digital signature standard. Technical Report FIPS 205, U.S. Department of Commerce, August 2024.
- [oST25] National Institute of Standards and Technology. Nist selects hqc for standardization, March 2025. HQC draft standard expected in 2026, final 2027.
- [oST26a] National Institute of Standards and Technology. Fips 206: Fn-dsa (falcon) digital signature standard, 2026. Draft in final stages of review / clearance as of June 2026; final expected late 2026 or early 2027.
- [oST26b] National Institute of Standards and Technology. Post-quantum cryptography standardization, 2026. Accessed: June 15, 2026.
- [Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*. ACM, 2005.
- [Scr25] Arimondo Scrivano. A comparative study of classical and post-quantum cryptographic algorithms in the era of quantum computing. *arXiv preprint arXiv:2508.00832*, 2025.
- [Sho99] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

About the Author

Dr. Sun Bing is a Firmware and Systems Architect with over 12 years of experience in the smart energy sector. She specializes in secure-by-design embedded systems, modular firmware solutions, and AI-driven cybersecurity frameworks.

Dr. Sun holds a **PhD in AI Security (Trustworthy AI)** from Singapore Management University (SMU), supported by the National Research Foundation and SMU Full Scholarship. Her research focuses on fairness verification, model repair, backdoor detection, and Universal Adversarial Perturbation defense, with Tier-1 publications in ICLR, USENIX Security, ICSE, and FM. She also earned an MSc in Computer Control & Automation and a BEng (First Class Honours) in Electrical and Electronics Engineering from Nanyang Technological University.