Post-Quantum Cryptography: A Comprehensive Review of Past Technologies and Current Advances

Bhavya Jain
Department of Computer Science & Engg.,
B. M. Institute of Engineering and Technology,
GGSIP University, Delhi, India
jbhavya876@gmail.com

Dr Harish Kumar Mittal
Principal and Head, Department of CSE,
B. M. Institute of Engineering and Technology,
Delhi-NCR, India
mittalberi@gmail.com

Abstract— Quantum computing poses an unprecedented threat to the cryptographic foundations that secure our digital civilisation! This paper presents a comprehensive examination of post-quantum cryptography (PQC), tracing the revolutionary transition from classical to quantum-resistant cryptographic systems. We analyse the mathematical foundations underlying major PQC families, including lattice-based, code-based, hash-based, multivariate, and isogeny-based approaches. The paper evaluates the groundbreaking NIST PQC standardisation process and its transformative impact on cryptographic development, while examining implementation challenges across diverse platforms. Performance metrics and security analyses reveal the fascinating trade-offs between different approaches. We conclude by exploring emerging research directions and challenges in securing digital infrastructure against the quantum revolution.

Index Terms—Post-quantum cryptography, quantum computing, lattice-based cryptography, code-based cryptography, multivariate cryptography, hash-based signatures, isogeny-based cryptography, NIST standardisation, cryptanalysis.

INTRODUCTION

Modern public-key cryptosystems—such as RSA, Diffie-Hellman and elliptic-curve cryptography—rely on the presumed intractability of certain mathematical problems for classical computers. However, Shor's algorithm, when executed on a sufficiently capable quantum computer, would render these schemes entirely vulnerable [1],[2]. Consequently, adversaries can employ a "harvest now, decrypt later" strategy, collecting encrypted communications today and decrypting them retroactively once quantum resources become available, thereby compromising long-term confidentiality. In response, the cryptographic community has embarked on a concerted effort to devise quantum-resilient alternatives. Google's CECPQ2 experiment within Chrome demonstrated the feasibility of hybrid classical–quantum key exchange [3], and, since 2016, NIST's post-quantum cryptography standardisation process has driven the evaluation and selection of algorithms suitable for widespread adoption [4]. Post-quantum cryptography (PQC) encompasses a range of mathematical paradigms—including lattice-based, code-based, hash-based, multivariate-polynomial and isogeny-based constructions—that are designed to resist both classical and quantum attacks without recourse to quantum hardware [5].

This comprehensive review achieves the following objectives:

1. **Quantum Threat Assessment**: Analyse the timeline and impact of quantum computing on current cryptographic infrastructures.
2. **PQC Family Analysis**: Examine the mathematical foundations, security assumptions, and practical characteristics of major post-quantum approaches.
3. **Standardisation Impact**: Evaluate NIST's groundbreaking standardisation process and its influence on cryptographic development.
4. **Implementation Reality**: Assess performance metrics, deployment challenges, and real-world adoption across diverse platforms.
5. **Future Directions**: Explore emerging research frontiers and advanced cryptographic functionalities in the post-quantum era.

II. QUANTUM COMPUTING AND THE CRYPTOGRAPHIC THREAT MODEL

A. Quantum Computing Fundamentals

Quantum computers harness the mind-bending principles of quantum mechanics to perform computations that would bring classical computers to their knees! These revolutionary machines exploit quantum phenomena, including superposition, entanglement, and interference, to achieve computational capabilities that seem almost magical [6]. The fundamental unit of quantum computation, the qubit, exists in a superposition of both 0 and 1 states simultaneously until measured. This quantum parallelism enables exponential scaling of computational power - a system with n qubits can represent 2^n states simultaneously! Major technology companies have achieved remarkable milestones: Google's 70-qubit Sycamore processor demonstrated "quantum supremacy" in 2019 [7], while IBM's roadmap targets 1000+ qubit systems by 2025.

B. Algorithmic Weapons of Quantum Destruction

Shor's Algorithm [2] represents the ultimate cryptographic apocalypse, efficiently factoring large integers and computing discrete logarithms in polynomial time on quantum computers. **Grover's Algorithm** [8] provides a quadratic speedup for searching unsorted databases, effectively halving the security of symmetric cryptographic systems.

Table I: Impact of Quantum Algorithms on Classical Cryptographic Schemes

Scheme	Problem	Classical Security	Quantum Security	Algorithm
RSA	Integer Factorization	Exponential	Polynomial	Shor's
DSA	Discrete Logarithm	Exponential	Polynomial	Shor's

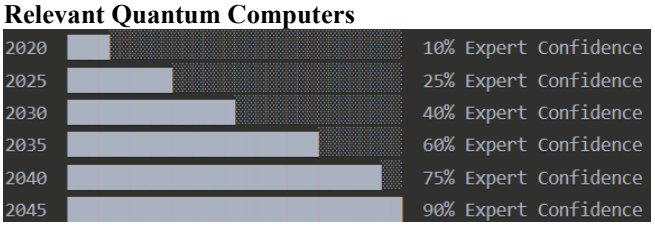
ISBN: 978-93-343-1044-3

ECDSA	Elliptic Curve DLP	Exponential	Polynomial	Shor's
Diffie-Hellman	Discrete Logarithm	Exponential	Polynomial	Shor's
AES-128	Symmetric Encryption	128 bits	64 bits	Grover's
SHA-256	Hash Function	256 bits	128 bits	Grover's

C. Timeline of Quantum Threat Realisation

The timeline for cryptographically relevant quantum computers involves significant uncertainty, but expert consensus suggests we're racing against time! Conservative estimates place the quantum cryptographic threat within 10-20 years, while optimistic quantum computing development could accelerate this timeline dramatically [9].

Figure 1: Expert Projections for Cryptographically Relevant Quantum Computers



III. CLASSICAL CRYPTOGRAPHIC SYSTEMS UNDER SIEGE

A. Symmetric Key Cryptography: The Resilient Survivors

Symmetric key algorithms demonstrate remarkable resilience against quantum attacks! These systems use identical keys for encryption and decryption, maintaining their core security properties even in the quantum era. However, Grover's algorithm delivers a devastating blow by effectively halving their security levels [10].

Table II: Post-Quantum Security Levels for Symmetric Algorithms

Algorithm	Key Size (bits)	Classical Security (bits)	Quantum Security (bits)	Real-World Usage
AES-128	128	128	64	TLS 1.3, VPNs, Wi-Fi WPA3
AES-192	192	192	96	Government systems, Banking
AES-256	256	256	128	Military, Classified data
ChaCha20	256	256	128	Mobile devices, Web browsers

B. Asymmetric Key Cryptography: The Quantum Casualties

Asymmetric cryptography enables the digital trust infrastructure that powers our interconnected world, but faces complete annihilation from quantum attacks! These systems support secure communications without prior key exchange and enable digital signatures that authenticate the digital identities we rely upon daily.

Current Asymmetric Families Facing Quantum Extinction:

1. **Integer Factorisation Cryptography (RSA):** Deployed across SSL/TLS connections securing web traffic, email encryption (PGP/GPG), and digital certificates. RSA's ubiquity makes its quantum vulnerability particularly catastrophic - billions of devices and systems worldwide depend on RSA security [11].
2. **Discrete Logarithm Cryptography (DSA/DH):** Powers key exchange protocols in SSH, IPsec VPNs, and legacy TLS implementations. The Diffie-Hellman key exchange revolutionized secure communications but faces complete compromise from Shor's algorithm.
3. **Elliptic Curve Cryptography (ECC):** Provides compact security for mobile devices, IoT systems, and modern TLS implementations. ECDSA signatures secure Bitcoin transactions, while ECDH key exchange protects messaging applications like WhatsApp and Signal.

Systems Currently Being Phased Out:

- Legacy SSL/TLS implementations using RSA key exchange.
- DSA-based government systems (FIPS 186-4 deprecation).
- Older Bitcoin wallet implementations used weak curve parameters.
- Industrial control systems with embedded RSA modules.

IV. POST-QUANTUM CRYPTOGRAPHIC APPROACHES: THE MATHEMATICAL ARSENAL

Table III: Post-Quantum Cryptographic Family Comparison

PQC	Security Form	Key Size	Performance	Quantum Resistance	Standard Status
Lattice-based	SVP, LWE	Medium	High	Excellent	NIST Selected
Code-based	Syndrome Decoding	Large	High	Excellent	NIST Alternative
Hash-based	Hash Functions	Small	Medium	Conservative	NIST Selected
Multivariate	MQ Problem	Large	Medium	Moderate	Under Review
Isogeny-based	Isogeny Finding	Small	Low	Compromised	Withdrawn

A. Lattice-based Cryptography: The Mathematical Marvel

Lattice-based cryptography represents the crown jewel of post-quantum security! These systems base their security on the computational hardness of lattice problems such as the Shortest Vector Problem (SVP) and the Learning With Errors

ISBN: 978-93-343-1044-3

(LWE) problem, which remain intractable even for quantum computers [12].

Revolutionary Advantages:

- Provable Security: Security reductions to worst-case hardness assumptions provide unprecedented confidence
- Versatile Functionality: Supports advanced features including fully homomorphic encryption and functional encryption
- Balanced Performance: Achieves excellent speed-to-security ratios across diverse platforms
- Reasonable Sizes: Offers manageable key and signature sizes compared to other post-quantum alternatives.

Leading Lattice-based Champions:

- **CRYSTALS-Kyber:** This module, an LWE-based key encapsulation mechanism, achieved NIST standardisation as the primary post-quantum key establishment algorithm! Kyber's balanced security, performance, and key size make it the go-to choice for most applications [13].
- **CRYSTALS-Dilithium:** Selected as NIST's primary digital signature standard, Dilithium provides fast signing and verification with moderate signature sizes. Based on module-LWE and module-SIS problems, it offers an excellent security-performance balance [14].
- **FALCON:** This NTRU lattice-based signature scheme achieves the smallest signature sizes among NIST selections at the cost of implementation complexity. FALCON's compact signatures make it ideal for bandwidth-constrained applications [15].

Real-World Deployment: Google's CECPQ2 experiment successfully integrated Kyber into Chrome browser connections, demonstrating practical feasibility for global deployment!

B. Code-based Cryptography: The Veteran Survivor

Code-based cryptography, pioneered by McEliece in 1978, represents the longest-tested post-quantum approach! These systems base security on the NP-hard problem of decoding random linear codes, withstanding four decades of intensive cryptanalytic assault [16].

Next-Generation Code-based Systems:

- BIKE (Bit Flipping Key Encapsulation): Reduces key sizes through quasi-cyclic structures.
- HQC (Hamming Quasi-Cyclic): Provides balanced performance with moderate key sizes.

Deployment Example: Quantum-safe VPN implementations have successfully integrated Classic McEliece for ultra-conservative security requirements in government communications.

C. Hash-based Signatures: The Conservative Fortress

Hash-based signature schemes provide the most conservative approach to post-quantum security, relying solely on cryptographic hash functions like SHA-256 that resist quantum attacks with sufficient output sizes [17].

NIST Standardised Hash-based Signatures:

- **XMSS (eXtended Merkle Signature Scheme):** Stateful signatures with tree-based key management [18]
- **LMS (Leighton-Micali Signature):** Alternative stateful approach with similar security properties [19]
- **SPHINCS+:** Stateless hash-based signatures selected as NIST alternate standard, eliminating state management complexity [20]

Deployment Example: Software update systems increasingly adopt SPHINCS+ for firmware signing, leveraging its conservative security assumptions and stateless operation.

D. Multivariate Cryptography: The Algebraic Challenger

Multivariate cryptography bases security on solving systems of multivariate quadratic equations over finite fields, an NP-hard problem. These systems excel at producing compact signatures but suffer from large public keys and recent cryptanalytic breakthroughs.

Deployment Challenge: The spectacular Rainbow signature scheme break in 2022 highlighted the evolving cryptanalytic landscape for multivariate systems [21].

E. Isogeny-based Cryptography: The Fallen Champion

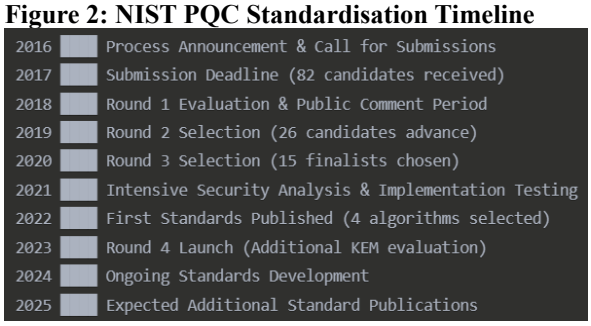
Isogeny-based cryptography once promised compact key sizes through the hardness of finding isogenies between supersingular elliptic curves. However, the dramatic SIKE cryptosystem break in 2022 using classical number-theoretic techniques effectively eliminated this family from practical consideration [22].

V. NIST POST-QUANTUM STANDARDIZATION PROCESS: THE CRYPTOGRAPHIC OLYMPICS

The NIST Post-Quantum Cryptography Standardisation Process represents the most comprehensive cryptographic evaluation in history! This rigorous multi-year competition has systematically assessed cryptographic algorithms through unprecedented global collaboration.

A. Process Timeline and Methodology

Figure 2: NIST PQC Standardisation Timeline



B. Selected Algorithms and Selection Rationale

NIST's 2022 Standardisation Decisions:

1. **Primary Key Establishment: CRYSTALS-Kyber**
    - Selection Rationale: Optimal balance of security, performance, and key sizes across diverse platforms

2. **Primary Digital Signatures: CRYSTALS-Dilithium**

ISBN: 978-93-343-1044-3

- Selection Rationale: Fast operations with strong security foundations and reasonable signature sizes

3. **Alternate Digital Signatures: FALCON**
   - Selection Rationale: Smallest signature sizes for bandwidth-constrained applications

4. **Conservative Signatures: SPHINCS+**
   - Selection Rationale: Maximum security confidence through hash-function-only design.

5. **Alternate Key Establishment: Classic McEliece**
   - Selection Rationale: Longest cryptanalytic history providing maximum security confidence.

C. Implementation and Adoption Considerations

The transition to post-quantum cryptography presents extraordinary engineering challenges across the entire cryptographic ecosystem:

Algorithm Agility Requirements: Systems must seamlessly transition between cryptographic algorithms as standards evolve and threats emerge. This demands sophisticated cryptographic abstraction layers and automated algorithm negotiation protocols.

Hybrid Security Approaches: During the transition period, hybrid schemes combining classical and post-quantum algorithms provide prudent security strategies. These systems remain secure as long as either the classical or post-quantum component resists attack.

Resource Constraint Management: Embedded systems and IoT devices with limited computational resources and memory face significant challenges implementing resource-intensive post-quantum algorithms.

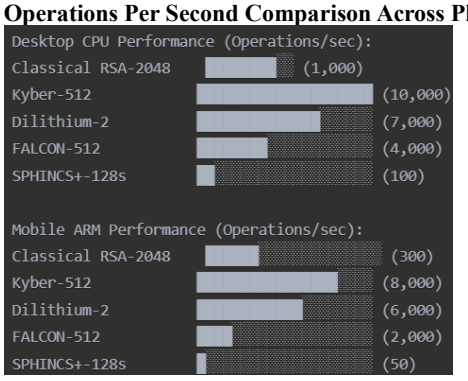
Cryptographic Library Integration: Major libraries, including OpenSSL, BoringSSL, and libsodium, have begun comprehensive integration of NIST post-quantum standards, facilitating ecosystem-wide adoption.

VI. PERFORMANCE ANALYSIS AND IMPLEMENTATION BENCHMARKS

A. Computational Performance Characteristics

Post-quantum algorithms exhibit dramatically different performance profiles compared to classical cryptographic systems! The computational efficiency varies significantly across algorithm families and hardware platforms.

Figure 3: Operations Per Second Comparison Across Platforms



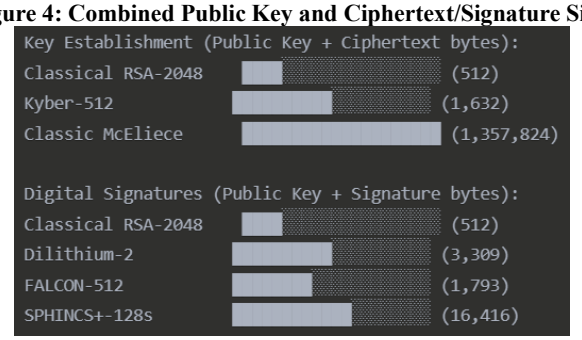
Performance Insights:

- Lattice-based schemes (Kyber, Dilithium) significantly outperform classical RSA across all platforms
- Hash-based signatures (SPHINCS+) provide excellent verification speed, but slower signing operations
- FALCON offers competitive performance with the smallest signature sizes.
- Code-based schemes excel in encryption/decryption speed despite large key sizes.

B. Size Metrics and Storage Requirements

Key and signature sizes represent critical considerations for bandwidth-constrained applications and storage-limited devices.

Figure 4: Combined Public Key and Ciphertext/Signature Sizes



C. Implementation Security Considerations

Implementing post-quantum cryptography securely presents unique challenges beyond algorithmic correctness:

Table IV: Implementation Security Analysis

PQC Family	Side-Channel Vulnerability	Memory Require	Complexity	Hardware Potential
Lattice-based	Medium-High	Medium	Medium	High
Code-based	Medium	High	Medium	Medium
Hash-based	Low	Low-Medium	Low	High
Multivariate	Medium	High	High	Medium

Critical Implementation Challenges:

1. **Side-channel Resistance**: Lattice-based schemes require careful implementation to prevent timing attacks and power analysis vulnerabilities [23].
2. **Constant-time Operation**: Ensuring operations execute in constant time, regardless of secret data, prevents timing-based information leakage.
3. **Fault Attack Mitigation**: Some post-quantum implementations require specific countermeasures against fault injection attacks.
4. **Memory Management**: Larger key sizes and intermediate values create memory management challenges, particularly in constrained environments.

VII. SECURITY ANALYSIS AND CRYPTANALYTIC DEVELOPMENTS

ISBN: 978-93-343-1044-3

A. Security Assumptions and Mathematical Foundations

Post-quantum cryptographic algorithms rely on diverse mathematical problems believed to resist quantum computational attacks. This diversity provides crucial resilience against algorithmic breakthroughs!

B. Recent Cryptanalytic Developments

The post-quantum cryptanalytic landscape continues evolving with remarkable discoveries that reshape our understanding of algorithmic security:

Major Cryptanalytic Breakthroughs:

1. **Rainbow Signature Scheme Break (2022)**: Beullens' algebraic attack completely broke the Rainbow multivariate signature scheme, demonstrating how unexpected mathematical insights can devastate seemingly secure systems [21].
2. **SIKE Isogeny System Collapse (2022)**: Castryck and Decru's classical attack using techniques from algebraic number theory completely compromised SIKE, eliminating isogeny-based cryptography from practical consideration [22].
3. **Lattice Cryptanalysis Advances**: Improvements in sieving algorithms and quantum lattice attack analyses have refined parameter selections for lattice-based schemes without fundamentally threatening their security [24].

C. Quantum Cryptanalytic Frontiers

Beyond Shor's and Grover's algorithms, researchers actively explore quantum computational techniques that might impact post-quantum security:

Quantum Algorithm Development Areas:

1. **Quantum Lattice Algorithms**: Quantum approaches to shortest vector problems could potentially impact lattice-based schemes, though current techniques don't threaten practical security parameters [25].
2. **Quantum Hidden Subgroup Methods**: Generalisations of Shor's algorithm to non-abelian groups continue generating research interest for potential cryptanalytic applications.
3. **Quantum Machine Learning Attacks**: Quantum machine learning might accelerate certain cryptanalytic techniques, though concrete threats remain speculative.

VIII. REAL-WORLD DEPLOYMENTS AND INDUSTRY ADOPTION

Industry Sector	Adoption	Primary Drivers	Key Applications	Timeline
Financial Services	Early Testing	Regulatory compliance, data longevity	Secure transactions, customer data	2025-2027
Healthcare	Pilot Programs	Patient privacy, record integrity	Medical records, device security	2026-2028
Automotive	Development	Vehicle lifespan, safety-critical systems	V2V/V2I communications	2025-2030
Government/Military	Aggressive Deployment	National security, classified data	Secure communications, intelligence	2024-2026
Technology	Production Integration	Competitive advantage, user privacy	Cloud services, consumer devices	2024-2025

Industry-Specific Case Studies:

1. **Financial Services Leadership:** JPMorgan Chase has implemented post-quantum cryptography testing for high-value financial transactions, emphasising long-term data confidentiality requirements. The Federal Reserve has issued guidance for post-quantum readiness across the banking sector.
2. **Healthcare Data Protection:** Epic Systems, the major electronic health record provider, has begun evaluating post-quantum signatures for patient record integrity, addressing decades-long medical data retention requirements.
3. **Automotive Security Evolution:** Tesla and other connected vehicle manufacturers are integrating post-quantum cryptography into vehicle-to-vehicle and vehicle-to-infrastructure communication protocols, recognising 15+ year automotive service lifecycles.
4. **Government Security Mandates:** The U.S. Department of Defence has established aggressive post-quantum transition timelines for classified systems, while NIST has issued federal guidance requiring post-quantum readiness planning across government agencies.

IX. EMERGING RESEARCH DIRECTIONS AND ADVANCED FUNCTIONALITIES

A. Advanced Post-Quantum Cryptographic Primitives

Breakthrough Research Areas:

1. **Post-Quantum Zero-Knowledge Proofs:** These systems enable privacy-preserving authentication and confidential transactions without revealing underlying sensitive data! Lattice-based constructions like [26] demonstrate practical zero-knowledge proofs resistant to quantum attacks.
2. **Post-Quantum Fully Homomorphic Encryption (FHE):** Quantum-resistant FHE allows computation on encrypted data without decryption, revolutionising cloud computing privacy! Microsoft's SEAL library and IBM's HElib demonstrate practical lattice-based FHE implementations [27], enabling secure cloud analytics.
3. **Post-Quantum Multi-Party Computation:** Secure multi-party computation enables multiple parties to jointly compute functions while maintaining input privacy. Research focuses on efficient post-quantum protocols for distributed cryptographic operations [28].
4. **Post-Quantum Anonymous Credentials:** Privacy-preserving attribute-based authentication systems resistant to quantum attacks support anonymous

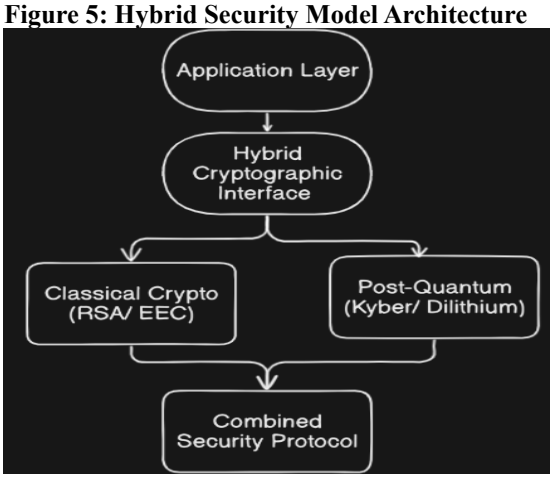
ISBN: 978-93-343-1044-3

access control and selective disclosure of credentials [29].

B. Hybrid Cryptographic System Design

During the post-quantum transition, hybrid approaches combining classical and quantum-resistant algorithms provide optimal security strategies:

Figure 5: Hybrid Security Model Architecture



C. Lightweight Post-Quantum Cryptography for Constrained Environments

The deployment of post-quantum algorithms in resource-constrained environments presents extraordinary challenges requiring innovative solutions:

Internet of Things (IoT) Challenges: Resource-constrained IoT devices often have severe computational and memory limitations, making standard post-quantum algorithms impractical. Research focuses on algorithm parameter optimisation, specialised hardware acceleration, and novel mathematical approaches tailored to constrained environments [30].

X. CONCLUSION

Through meticulous analysis of five revolutionary post-quantum cryptographic families, NIST's methodical standardisation initiative has forged an extraordinary defensive arsenal featuring CRYSTALS-Kyber's lattice-based key encapsulation brilliance, CRYSTALS-Dilithium and FALCON's signature authentication prowess, SPHINCS+ for uncompromising hash-based security applications, and Classic McEliece's code-based ultra-conservative key establishment mechanisms. The practical deployment landscape reveals that lattice-based cryptographic schemes achieve the most spectacular equilibrium between computational efficiency, security robustness, and cross-platform compatibility, while successful real-world implementation demands an unwavering commitment to side-channel attack mitigation, perpetual cryptanalytic scrutiny, and resource-optimised algorithmic engineering. The cryptographic frontier extends magnificently beyond fundamental primitives into advanced zero-knowledge proof systems, fully homomorphic encryption architectures, and secure multi-party computational frameworks, with lightweight post-quantum solutions for IoT and embedded infrastructure representing the most critical developmental imperative as quantum-vulnerable devices infiltrate essential societal systems. Strategic organisational transformation requires agile hybrid cryptographic protocols that seamlessly integrate classical and quantum-resistant algorithms throughout the transitional epoch, supported by unprecedented collaborative synergy between academic research institutions, industrial innovation centres, and governmental security agencies to accelerate quantum-resistant solution maturation and deployment velocity.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978, doi: 10.1145/359340.359342.
[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, Oct. 1997, doi: 10.1137/S0097539795293172.
[3] D. Stebila et al., "Measuring TLS key exchange with post-quantum KEM," in *Proc. 2020 ACM SIGSAC Conference on Computer and Communications Security*, Virtual Event, USA, Nov. 2020, pp. 1808-1821, doi: 10.1145/3372297.3423350.
[4] L. Chen et al., "Report on post-quantum cryptography," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8105, Apr. 2016, doi: 10.6028/NIST.IR.8105.
[5] D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., *Post-Quantum Cryptography*. Berlin, Germany: Springer-Verlag, 2009, doi: 10.1007/978-3-540-88702-7.
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed. Cambridge, UK: Cambridge University Press, 2010.
[7] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505-510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.
[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annual ACM Symposium on Theory of Computing*, Philadelphia, PA, USA, May 1996, pp. 212-219, doi: 10.1145/237814.237866.
[9] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, Sep./Oct. 2018, doi: 10.1109/MSP.2018.3761723.
[10] D. J. Bernstein, "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?" in *Proc. Special-Purpose Hardware for Attacking Cryptographic Systems (SHARCS)*, Vienna, Austria, Sep. 2009, pp. 105-116.
[11] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188-194, Sep. 2017, doi: 10.1038/nature23461.
[12] C. Peikert, "A decade of lattice cryptography," *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283-424, Mar. 2016, doi: 10.1561/0400000074.
[13] R. Avanzi et al., "CRYSTALS-Kyber algorithm specifications and supporting documentation," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2020. [Online]. Available: https://pq-crystals.org/kyber/
[14] L. Ducas et al., "CRYSTALS-Dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, pp. 238-268, Feb. 2018, doi: 10.13154/tches.v2018.i1.238-268.
[15] P.-A. Fouque et al., "FALCON: Fast-Fourier lattice-based compact signatures over NTRU," Submission to the NIST Post-Quantum Cryptography Standardization Process, 2020. [Online]. Available: https://falcon-sign.info/
[16] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," The Deep Space Network Progress Report 42-44, Jet Propulsion Laboratory, Pasadena, CA, USA, Tech. Rep., Jan. 1978, pp. 114-116.
[17] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS - A practical forward secure signature scheme based on minimal security assumptions," in *Proc. 4th International Workshop on Post-Quantum Cryptography*, Taipei, Taiwan, Nov. 2011, pp. 117-129, doi: 10.1007/978-3-642-25405-5_8.
[18] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle signature scheme," Internet Engineering Task Force, RFC 8391, May 2018, doi: 10.17487/RFC8391.
[19] D. McGrew, M. Curcio, and S. Fluhrer, "Leighton-Micali hash-based signatures," Internet Engineering Task Force, RFC 8554, Apr. 2019, doi: 10.17487/RFC8554.
[20] J.-P. Aumasson et al., "SPHINCS+: Submission to the NIST post-quantum cryptography project," National Institute of Standards and

ISBN: 978-93-343-1044-3

Technology, Gaithersburg, MD, USA, Tech. Rep., 2020. [Online]. Available: https://sphincs.org/
[21] W. Beullens, "Breaking Rainbow takes a weekend on a laptop," in *Proc. 42nd Annual International Cryptology Conference (CRYPTO 2022)*, Santa Barbara, CA, USA, Aug. 2022, pp. 464-479, doi: 10.1007/978-3-031-15979-4_16.
[22] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH (preliminary version)," *IACR Cryptology ePrint Archive*, Paper 2022/975, Aug. 2022. [Online]. Available: https://eprint.iacr.org/2022/975
[23] P. Pessl, "Analyzing the shuffling side-channel countermeasure for lattice-based signatures," in *Proc. 17th International Conference on Cryptology in India (INDOCRYPT 2016)*, Kolkata, India, Dec. 2016, pp. 153-170, doi: 10.1007/978-3-319-49890-4_9.
[24] M. R. Albrecht et al., "Estimate all the {LWE, NTRU} schemes!" in *Proc. 14th International Conference on Security and Cryptography for Networks*, Amalfi, Italy, Sep. 2018, pp. 351-367, doi: 10.1007/978-3-319-98113-0_19.
[25] Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange, "Provably weak instances of Ring-LWE," in *Proc. 35th Annual International Cryptology Conference (CRYPTO 2015)*, Santa Barbara, CA, USA, Aug. 2015, pp. 63-92, doi: 10.1007/978-3-662-47989-6_4.
[26] M. del Pino, V. Lyubashevsky, and G. Seiler, "Lattice-based group signatures and zero-knowledge proofs of automorphism stability," in *Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto, ON, Canada, Oct. 2018, pp. 574-591, doi: 10.1145/3243734.3243852.
[27] H. Chen, K. Laine, and R. Player, "Simple encrypted arithmetic library - SEAL v2.1," in *Proc. 6th International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, Feb. 2017, pp. 3-18, doi: 10.1007/978-3-319-70278-0_1.
[28] R. Cramer, I. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge, UK: Cambridge University Press, 2015, doi: 10.1017/CBO9781107337756.
[29] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques*, Innsbruck, Austria, May 2001, pp. 93-118, doi: 10.1007/3-540-44987-6_7.
[30] J. Buchmann, F. Göpfert, A. Hülsing, T. Lange, P. Nitaj, and T. Schneider, "Post-quantum cryptography: State of the art," in *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, P. Y. A. Ryan, D. Naccache, and J.-J. Quisquater, Eds. Berlin, Germany: Springer-Verlag, 2016, pp. 88-108, doi: 10.1007/978-3-662-49301-4_6.

ISBN: 978-93-343-1044-3