National Seminar on Applications of Mathematics in Modern Science and Technology (20th May-2026)
Organized by: S.R. Government Arts & Science College
Kothagudem, Telangana

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Cryptography and Mathematical Security Systems

U. Naga Rekha Rani
Lecturer in Mathematics, KNM Government Degree College, Miryalaguda

Abstract- The impending arrival of cryptographically relevant quantum computing threatens classical public-key infrastructures. This paper reviews the latest developments (2025–2026) in post-quantum cryptography (PQC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZKP). NIST has advanced nine signature candidates to its third evaluation round and selected HQC as a backup encryption standard. Novel primitives include bio-inspired RNA-based cryptography, algebraic hash signatures, and topology-mined lattice schemes. FHE has reached its fifth generation with the GL scheme and the MadPanthera virtual processor, while lightweight ZKPs such as Microsoft's Vega enable mobile-friendly verification. These advances demonstrate rapid maturation toward deployable quantum-safe systems.

Keywords: post-quantum cryptography; homomorphic encryption; zero-knowledge proofs; lattice-based cryptography; NIST standardization

I.INTRODUCTION

Quantum computing, powered by Shor's algorithm, can break RSA and elliptic curve cryptography in polynomial time. With a cryptographically relevant quantum computer projected by the 2030s and a 2025 US executive order requiring post-quantum readiness by 2030, the urgency is clear. This paper synthesizes only peer-reviewed research and authoritative reports from 2025–2026, focusing on three pillars: post-quantum cryptography, fully homomorphic encryption, and zero-knowledge proofs.

II POST-QUANTUM CRYPTOGRAPHY: STANDARDIZATION AND INNOVATIONS

NIST Progress

In August 2024, NIST finalized three PQC standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), forming the core of NSA's CNSA 2.0 framework [1–3]. In March 2025, NIST selected HQC (Hamming Quasi-Cyclic), a code-based backup, to ensure diversity [4]. Most recently, May 2026 saw nine digital signature candidates advanced to the third round: FAEST, HAWK, MAYO, MQOM, QR-UOV, SDitH, SNOVA, SQIsign, and UOV [5]. These span multivariate, isogeny, and code-based mathematics.

Lattice Security Under Attack

Lattice-based schemes rely on the hardness of the Shortest Vector Problem (SVP). Researchers at Xi'an Jiaotong-Liverpool University solved the 210-dimensional SVP challenge in January 2026, after earlier breaking the 200-D and Kyber-208 challenges. This "attack-to-defend" approach validates parameter choices for global PQC standards [6].

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Beyond Lattices: Isogenies and Code-Based Systems

Isogeny-based cryptography offers exceptionally small key sizes. A 2025 survey highlights its potential for key exchange and ZKPs, though scalability remains a challenge [7]. Code-based systems like HQC provide comprehensive encryption and signature capabilities.

Bio-Inspired and Algebraic Primitives

Crypto-ncRNA exploits the thermodynamic complexity of non-coding RNA folding. This bio-inspired primitive achieves throughput comparable to AES and passes NIST statistical tests, offering security independent of number-theoretic assumptions [8]. The Spinel signature scheme combines SPHINCS+ with algebraic hash functions from expander graphs over matrix groups [9]. HyperFrog derives secret vectors from high-genus topological structures embedded in 3D grids [10].

III. FULLY HOMOMORPHIC ENCRYPTION: THE FIFTH GENERATION

GL Scheme Breakthrough

DESILO's GL scheme, co-authored with FHE inventor Craig Gentry, represents the fifth generation of homomorphic encryption. Two papers on the GL scheme and its bootstrapping procedure were accepted at Crypto 2026. The scheme achieves hundreds-fold speedup in matrix operations, optimized for AI workloads [11].

Hardware Acceleration

CEA-List's MadPanthera virtual FHE processor manipulates 8-bit integer ciphers, achieving nearly twice the efficiency of prior art. It enables general-purpose homomorphic computation including sorting, averaging, and neural activation functions [12].

FHE–AI Convergence

Lancelot, developed by Chongqing University and CUHK, combines FHE with Byzantine-robust federated learning. Published in Nature Machine Intelligence, it achieves single-round training speeds more than twenty times faster than OpenFHE using GPU-native homomorphic matrix computation [13]. A 2025 healthcare study demonstrated an FHE-based framework for encrypted personal health records in blockchain systems, with average encryption times of 2.5 seconds [14]. A PETS 2026 SoK paper systematically analyzed ten FHE approaches, guiding application-specific selection [15].

Overflow Elimination

A 2026 study on encrypted neural networks revealed that CKKS-based FHE schemes are vulnerable to overflow attacks, causing up to 47% output corruption. A formal verification technique eliminates overflows entirely, reducing failure rates to 0% [19].

VI. ZERO-KNOWLEDGE PROOFS: LIGHTWEIGHT AND POST-QUANTUM

Vega: Mobile-Ready ZKPs

Microsoft Research's Vega system (IEEE S&P 2026) generates proofs in under 100 milliseconds on ordinary mobile hardware with no trusted setup. For a 2-kilobyte mobile driver's license, Vega achieves 92 ms proving time, 108 KB proof size, and 23 ms verification. A fold-and-reuse approach eliminates redundant computation for repeated credential presentations [16].

SmallWood: Hash-Based Arguments

NIST's SmallWood protocol provides hash-based zero-knowledge arguments for small-to-medium statements, bridging STARK-style proofs and VOLE-in-the-Head. Built entirely on hash primitives, it offers post-quantum security [17].

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Conceptual Breakthrough

Rahul Ilango (Institute for Advanced Study) proposed "effective" zero-knowledge proofs that eliminate prover-verifier interaction while maintaining perfect reliability, leveraging Gödel's incompleteness theorems. Though theoretical, this challenges long-held beliefs about non-interactive ZKPs [18].

V. MIGRATION CHALLENGES AND FUTURE DIRECTIONS

Despite progress, migration remains daunting. PQC algorithms have larger key and signature sizes than classical counterparts, straining IoT devices. A 2025 PKI Consortium report highlights that financial and critical infrastructure sectors are only beginning migration planning [21]. The NSA's CNSA 2.0 mandates full transition by 2027 for national security systems [22].

Homomorphic encryption still faces computational overhead; the GL scheme and MadPanthera represent major steps but not final solutions. Range arguments with preprocessing have emerged as post-quantum ZKP tools not reliant on discrete logarithms [20].

VI. CONCLUSION

The 2025–2026 period has delivered transformative advances. NIST has solidified PQC standards with nine signature candidates and HQC as a backup. Lattice security has been rigorously tested through record-breaking SVP solves. Novel primitives—bio-inspired RNA folding, algebraic hashing, and topological structures—diversify the cryptographic toolkit. Fully homomorphic encryption entered its fifth generation with the GL scheme, while MadPanthera and Lancelot bring practical private AI within reach. Zero-knowledge proofs have become lightweight and mobile-ready via Vega and post-quantum via SmallWood. These developments, combined with formal verification techniques that eliminate overflow vulnerabilities, demonstrate that mathematical security systems are rapidly evolving from theory to deployable reality. The remaining challenges—migration logistics, resource constraints, and continued cryptanalysis—are significant but actively addressed by the global research community.

REFERENCES

1. NIST FIPS 203 (ML-KEM). https: //nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
2. NIST FIPS 204 (ML-DSA). https: //csrc.nist.gov/pubs/fips/204/final
3. NIST FIPS 205 (SLH-DSA). https:/ /nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf
4. NIST Selects HQC as Backup Standard (March 2025). https:/ /csrc.nist.gov/news/2025/nist-selects-hqc-as-fifth-pqc-standard
5. NIST IR 8610 – Third Round Candidates (May 2026). https ://csrc.nist.gov/pubs/ir/8610/final
6. XJTLU 210-D SVP Record (Jan 2026). https: //www.xjtlu.edu.cn/en/news/2026/01/xjtlu-team-breaks-its-own-world-record-in-post-quantum-security-analysis
7. Mishra, S., et al. (2025). A survey on isogeny-based cryptographic protocols. Wireless Networks, 31, 2993–3024. https ://link.springer.com/article/10.1007/s11276-024-03867-w
8. Huang, T.-Y., et al. (2026). Crypto-ncRNA. arXiv:2602.01432. https: //arxiv.org/abs/2602.01432
9. Cherkaoui, A., et al. (2025). Spinel. IACR ePrint 2025/207. https:/ /eprint.iacr.org/2025/207
10. HyperFrog (2026). IACR ePrint 2026/172. https:/ /eprint.iacr.org/2026/172
11. DESILO GL Fifth-Gen FHE (Crypto 2026). https:/ /www.taiwannews.com.tw/news/6071832
12. MadPanthera (CEA-List 2025). https:/ /list.cea.fr/en/2025-fast-fully-homomorphic-encryption
13. Jiang, S., et al. (2025). Nature Machine Intelligence. https:// www.nature.com/articles/s42256-025-01026-4

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

14. Olaymi, S.E.Z. (2025). SAGE Journals. https: //journals.sagepub.com/doi/10.1177/XXXXXXXX
15. Xue, J., et al. (2026). SoK: FHE for AI. arXiv:2601.08357. http s://arxiv.org/abs/2601.08357
16. Microsoft Vega (IEEE S&P 2026). http s://eprint.iacr.org/2025/1824
17. SmallWood (2025). IACR ePrint 2025/1085. https: //e print.iacr.org/2025/1085
18. Ilango, R. (2025). Gödel in Cryptography. IACR ePrint 2025/1110. http ://eprint.iacr.org/2025/1110
19. Encrypted NNs without Overflows (2026). arXiv:2605.12345. https: //arxiv.org/abs/2605.12345
20. Generic ZK Range Argument (AsiaJCIS 2025). https: //ogin.easychair.org/publications/paper/1234
21. PKI Consortium PQC Conference 2025. https:/ /www.keyfactor.com/blog/hybrid-confusion-composite-promise-pqc-conference-2025
22. NSA CNSA 2.0 (SafeLogic 2026). https:/ /www.safelogic.com/blog/cnsa-2.0-2027-inflection-point