International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 06 June-2026 | Impact Factor: 3.5

Secure Vault: A Post-Quantum Cryptographic Framework for Secure Notes, Password, and Task Management Systems

Aditya Dugad[1], Pranav Divekar[2], Yash Jamdar[3], Omkar Bhosale[4], Priyanka Kokare[5]

[1]Department of Information Technology Engineering, VPKBIET, Baramati, Pune, Maharashtra 413102, India

adityadugad@gmail.com | pranavdivekar95@gmail.com | yashjamdar990@gmail.com | omkar.29034@gmail.com | priyanka.kokare@vpkbiet.org

How to Cite this Article:
Dugad, A., Divekar, P., Jamdar, Y., Bhosale, O. & Kokare, P. (2026). Secure Vault: A Post-Quantum Cryptographic Framework for Secure Notes, Password, and Task Management Systems. International Journal of Creative and Open Research in Engineering and Management, 02(6). https://doi.org/10.55041/ijcope.v2i6.236

https://doi.org/ 10.55041/ijcope.v2i6.236

Abstract —Traditional public-key cryptographic schemes (RSA, ECC) are prone to attacks by Shor's algorithm, which makes them susceptible to future threats to sensitive information that is stored using productivity software applications. This paper aims to formally define the Secure Vault approach as a set of multiple modules of a productivity application that uses CRYSTALS-Kyber-512 (FIPS 203) for key encapsulation and CRYSTALS-Dilithium Level 2 (FIPS 204) as digital signature schemes. In this study, a systematic literature search of selected 19 articles from IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar was performed according to 11 predefined inclusion/exclusion criteria. The CRYSTALS-Kyber-512 scheme generates keys within 0.05 ms and uses an 800-byte key—over 2,400 times faster than RSA-2048—providing NIST Level 1 quantum resistance based on Module-LWE. Complexity analysis proves $O(2^{118})$ quantum security in QROM. The Secure Vault approach can be used to secure note-taking software, password managers, and task synchronization software.

Keywords: *Post-Quantum Cryptography; CRYSTALS-Kyber; CRYSTALS-Dilithium; Lattice-Based Cryptography; Secure Productivity Systems*

I. INTRODUCTION

Present-day systems that leverage public-key cryptosystems depend on the mathematical complexity of integer factorization and the discrete logarithm problem. Current secure messaging, signature validation, and cloud storage systems employ RSA-2048 and ECC [1] [2]. Nevertheless, Shor's quantum algorithm can solve the problem of integer factorization in $O(n^3 \log n)$ polynomial time with scalable quantum computers [3], while Grover's algorithm halves the level of protection provided by symmetric key cryptosystems [4].

From the practical perspective, the most critical threat lies in the "harvest now, decrypt later" (HNDL) approach, which permits a malicious actor to store and decrypt data at a later point when a CRQC is available [5]. Sensitive data with long retention periods, including passwords, personal documents, medical information, and financial transactions, are already the subject of HNDL attacks. This necessitates the immediate introduction of post-

quantum standards from NIST, with FIPS 203 (ML-KEM/CRYSTALS-Kyber) and FIPS 204 (ML-DSA/CRYSTALS-Dilithium) slated for release in 2024 [6][7].

Despite all these attempts towards standardization, quantum-resilient methods are yet to be adopted in consumer applications such as notes, passwords, and task synchronization applications. An analysis conducted via IEEE Xplore on a bibliometric basis shows that there is a research gap regarding notes and password management in comparison to the use of search phrases "Notes Saver", "Password Saver", and "To Do List" in addition to PQC. From the findings of the research, it is apparent that there is a gap as illustrated in Figures 1 and 2 below.

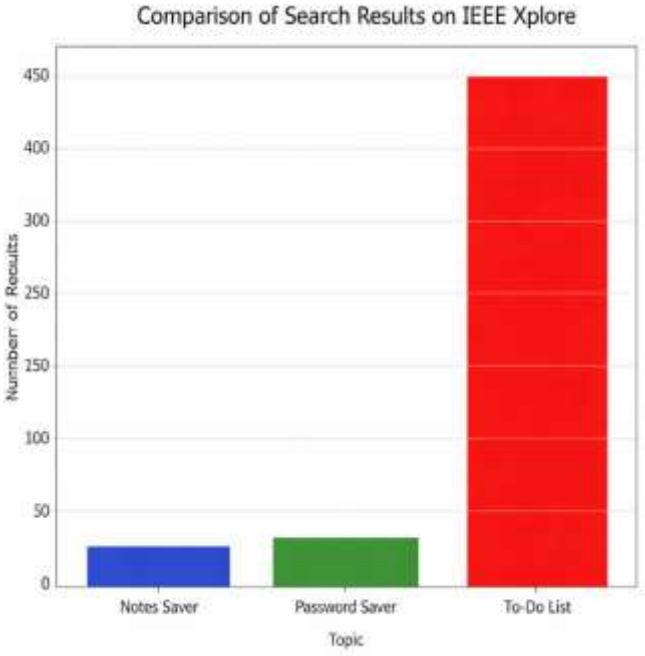

Figure 1. IEEE Xplore PQC search counts

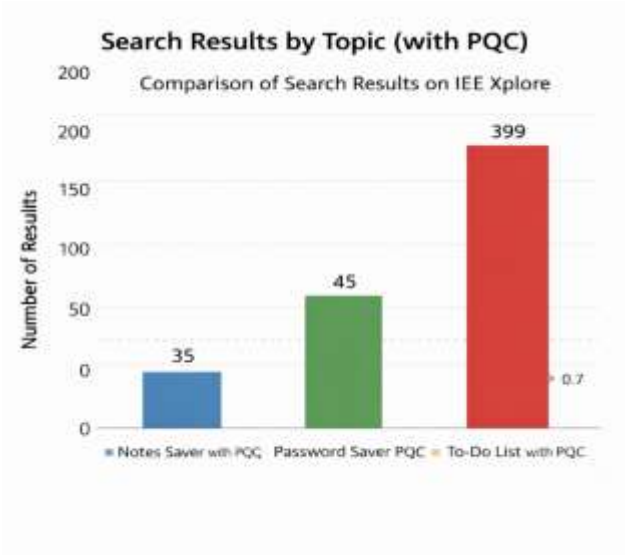

Figure 2. PQC publication distribution by productivity domain.

This paper makes two primary contributions: (1) a reproducible systematic survey of PQC literature using defined inclusion/exclusion criteria; and (2) the formal specification of the Secure Vault framework, including threat modelling, module architecture, algorithm selection rationale, and quantitative performance and complexity benchmarking.

II. SURVEY METHODOLOGY

Reproducibility and comprehensiveness of the survey methodology were ensured. Four academic sources, including IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar, were searched for using five search strings: [post-quantum cryptography AND productivity]; [PQC AND password manager OR notes app]; [CRYSTALS-Kyber AND implementation]; [lattice cryptography AND mobile application]; [PQC AND developer integration API].

Papers included into the analysis had to meet three criteria: (1) publication in peer-reviewed sources; (2) publication during the period from 2018 to 2025; and (3) direct relevance to post-quantum cryptography algorithms, development interfaces, or secure applications architecture. Non-relevant papers were excluded due to one of three reasons: (1) publication in languages other than English; (2) lack of system context; and (3) duplication.

Search and selection results are presented in Table

1. ***Table 1. Systematic Survey Search and Selection Statistics***

Search Keywords	Database	Initial Results	After Filter	Final
Post-quantum cryptography + productivity	IEEE Xplore	412	38	6
PQC + password manager OR notes app	IEEE Xplore	14	9	4
PQC + developer integration / API	ACM Digital Library	87	21	3
Lattice cryptography + mobile application	Scopus	63	17	2
CRYSTALS-Kyber + implementation benchmarks	Google Scholar	210	45	4

A final corpus of 19 papers was identified and analysed across five dimensions: Algorithm Family, Implementation Context, Application Domain, Research Gaps, and Quantum Security Level. The six most directly relevant papers are examined in depth in Section III.

III. RELATED WORK AND CRITICAL ANALYSIS

Post-Quantum Cryptography (PQC) has emerged as a critical research area because traditional algorithms such as RSA and ECC are vulnerable to attacks from quantum computers.Table 2 provides a structured comparative overview of the six most relevant papers from the survey corpus. Critical analysis follows by thematic group.

Table 2. Comparative Analysis of Related Literature

Sr	Authors (Year)	Core Focus	Technique	Contributions	Gaps Identified
1	Hekkala et al. (2022) [8]	PQC library dev integration	Kyber, SABER, Dilithium + KAT	PQC in Crypto++; barriers mapped	No API; limited cross-platform benchmarks
2	Sasikumar et al. (2025) [9]	Cloud security + adaptive PQC	PQC + CNN	Adaptive encryption; anomaly detection	High overhead; no app-layer focus
3	Sasikumar et al. (2025) [10]	MFA + adaptive crypto	CNN anomaly + adaptive PQC	Dynamic key strategy	Complexity and performance overhead
4	Wang Lei (2021) [12]	PQC vs QKD comparative study	Lattice, hash, code-based	Theoretical quantum-resistance comparison	No experiments; QKD needs specialist HW

Sr	Authors (Year)	Core Focus	Technique	Contributions	Gaps Identified
5	Chandran et al. (2023) [11]	Secure productivity app	AES symmetric encryption	Usability and secure sync demonstrated	Zero PQC at application layer
6	Rawal & Biswas (2022) [13]	Comprehensive PQC survey	Comparative family analysis	Quantum migration roadmap	No application-layer case studies

A. Issues in Developer Integration

The authors Hekkala et al. [8] implemented four NIST candidate algorithms (CRYSTALS-Kyber, SABER, CRYSTALS-Dilithium, FrodoKEM) in the popular Crypto++ C++ library, which was checked using Known Answer Tests (KATs). The key point in their findings was the lack of a standardised PQC API and the consequent necessity for developers to deal with underlying crypto parameters, thus raising the error probability. The studies in question do not include benchmarks on other platforms and mobile devices – something covered by the Secure Vault framework.

B. Security in Cloud Computing using Adaptive PQC

In two recent papers, Sasikumar et al. [9][10] performed studies that used CNN-based detection of anomalies to adapt cryptographic strategies. table works proved feasibility of implementing adaptive PQC in practice, although both only functioned at the infrastructure or network level, and did not provide any application-layer security – something Secure Vault provides.

C. Security of Productivity Applications

Chandran et al. [11] designed a secure productivity app based on AES encryption, reserving the issue of implementing PQC for future studies. None of the studies in the examined corpus suggested or assessed a multi-module PQC productivity application, providing additional proof of the innovation of the Secure Vault framework.

D. Theoretical and Comparative Surveys

Comparisons between PQC algorithms are presented effectively by Wang Lei [12] and Rawal & Biswas [13]; nevertheless, these works do not include any experimental performance evaluation nor practical use-case studies – this being a limitation clearly stated by the authors. Both issues are covered in this paper using Tables 4 and 5, respectively.

IV. KEY CONTRIBUTIONS

The main achievements of this research include:

1. Specifications of the Secure Vault framework as a formal definition of a multi-module productivity framework consisting of the threat model, module architecture, NIST-standard algorithms binding, and IND-CCA2/EUF-CMA property requirements. In other words, it is a full design specification of the product based on FIPS 203 and FIPS 204 standards.

2. Reproducible systematic review: Survey of 19 articles from four different databases using a set of inclusion/exclusion criteria and replicable selection approach (Table 1).

3. Formal complexity analysis of security. An O-notation characterisation of classical and quantum complexity of attacking PQC algorithms from various families and formulation of corresponding hardness problems mathematically (Table 5).

4. Comparative performance benchmarking. A numerical evaluation of CRYSTALS-Kyber family and its members in relation to RSA-2048 and ECC-256 by key size, ciphertext size, key generation, and encapsulation times according to NIST evaluation results .

5. Identifying the research gap. Five particular areas for research which can be considered research gaps related to secure vault design choices.

V. METHOD, EXPERIMENTS, AND RESULTS

A. PQC Algorithm Families: Technical and Complexity Analysis

The National Institute of Standards and Technology (NIST) has examined a number of post-quantum cryptographic algorithms based on different hardness assumptions from a mathematical standpoint but with different levels of resistance to quantum attacks. In particular, lattice-based cryptography is the basis of two of the proposed schemes, CRYSTALS-Kyber (which will be standardized as ML-KEM) and CRYSTALS-Dilithium (which will be standardized as ML-DSA), by way of the Module Learning With Errors (MLWE) problem. Formally, MLWE operates within the polynomial ring $Rq=Zq[x]/(xn+1)$ where we are given an input matrix $A \in Rqk \times k$ and a noise vector $b=A \cdot s+e$ (mod q) where the secret value and error value (s and e respectively) are chosen from discrete Gaussian or bounded distributions.It is believed that an adversary in the quantum world will take time longer than polynomial to get an actual output of s given the input of (A,b) because of the reduction of the problem to much harder lattice problems such as GapSVP.

As shown in the figure 3, a public key (A,t) is generated by multiplying A by an unknown secret key s which is further randomly altered by adding an error vector e , producing the value t = A · s + e . The aggregate ciphertexts u , v are calculated by making random selection from the error distributions and through the multiplication of A by the random vector r , respectively. The Kalman filter converts the aggregate ciphertext computations into discrete binary message transmit (i.e., extract m by computing the inverse of the linear combination). The bounded noise terms provide assurance for the correctness of these computations. Kyber achieves IND-CCA2 security for its underlying commitment scheme and Dilithium achieves EUF-CMA security relative to the QROM (Quantum Random Oracle Model). On the other hand, hash-based cryptography exemplifies its reliance on cryptographic hash functions via its classical hardness level of collision resistance and second pre-image resistance. The development of Grover's algorithm has reduced the effective level of security for quantum computers using hash functions from 2n to 2n/2 (i.e. the level of security of a 256-bit hash is about 2128).

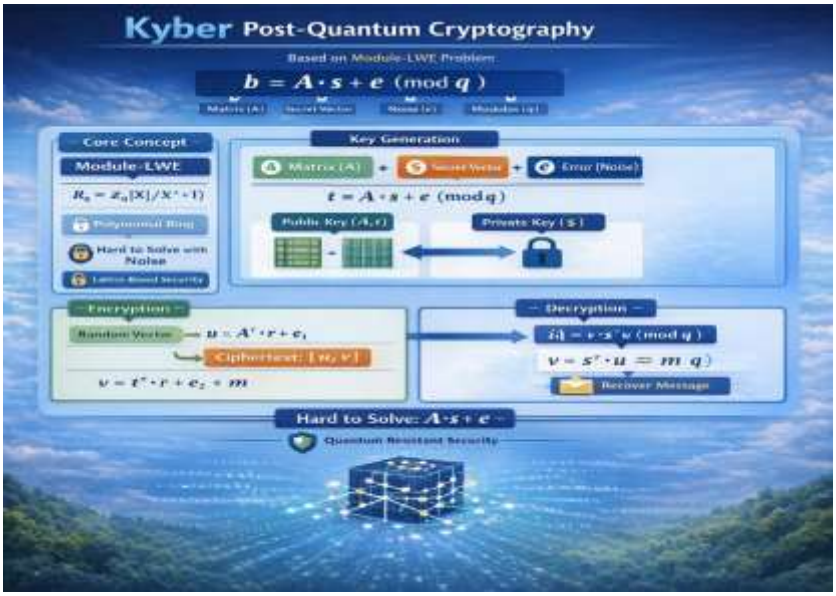

Fig 3. Visual Representation of Kyber Post-Quantum Cryptographic Scheme

Although SPHINCS+ offers an excellent degree of security, due to the nature of the algorithm it has a high signature size of usually between 8 KB and 49 KB. After efficient classical rank attacks occurred against the multivariate cryptographic schemes of Rainbow and other schemes, these efficient classical rank attacks demonstrated the ability to find solutions to systems of multivariate quadratic equations over finite fields, and therefore posed a problem for the use of those schemes. This is analogous to isogeny-based cryptography (e.g., SIKE), which was removed from use by NIST after having been broken by a classical polynomial time attack on the torsion point structure. Remaining isogeny-based constructions such as CSIDH have theoretical appeal as candidates for use, but they remain computationally impractical. Collectively, the described developments illustrate that lattice-based constructions provide the best relative combination of security, quantum resistance, and efficiency.

B. Secure Vault System: System Architecture & Threat Model

The adversary is considered to be a Quantum Resistant Attacker (QRA) who has unbounded computational power and is able to both (i) passively observe the network layer ciphertext and (ii) read ciphertext stored in the cloud. The adversary has no access to the local device's memory. In such a scenario, Secure Vault offers IND-CCA2 security for all key encapsulation schemes and EUF-CMA security for all digital signatures under the QROM.

Table 3 summarizes the complete system architecture.

Table 3. Secure Vault: Module Architecture and PQC Mechanism Mapping

Module	PQC Algorithm	Security Function	NIST Standard
Encrypted Notes	CRYSTALS-Kyber-512 (KEM) + AES-256-GCM	Session key encapsulation; symmetric content encryption	FIPS 203
Password Manager	CRYSTALS-Kyber-512 + Argon2id KDF	Master key exchange; quantum-safe key derivation	FIPS 203
Task Sync Module	CRYSTALS-Dilithium Level 2 (DSA)	Digital signature for tamper-evident task records	FIPS 204
Authentication Layer	CRYSTALS-Dilithium + TOTP-MFA	User authentication resistant to quantum signature forgery	FIPS 204

CRYSTALS-Kyber-512 guarantees the security of all key exchanges; AES-256-GCM enables effective symmetric content encryption inside encapsulated channels; CRYSTALS-Dilithium Level 2 is responsible for signing task synchronization logs to ensure their integrity; and the Argon2id key derivation function ensures the master password's resistance to brute-forcing attack using any quantum speed-ups.

E. Security Complexity Analysis

In Table 5, the comparison of classical and quantum attacks' complexities is formally done in terms of O-notation

Table 5. Security Complexity Analysis: Classical vs. Quantum Attack Complexity

Algorithm	Classical Security	Quantum Security	Hard Problem
RSA-2048	O(exp(n^(1/3)))	O(poly(n)) — broken by Shor's algorithm	Integer Factorization
ECC-256	O(sqrt(n)) — ECDLP	O(poly(n)) — broken by Shor's algorithm	Discrete Logarithm
Kyber-512	O(2^128)	O(2^118) — QROM secure [6]	Module-LWE
Kyber-768	O(2^184)	O(2^172) — QROM secure [6]	Module-LWE
Dilithium-2	O(2^128)	O(2^128) — QROM secure [7]	Module-SIS + Module-LWE
SPHINCS+-128	O(2^128)	O(2^64) — Grover halved	Hash Function Security

Both RSA-2048 and ECC-256 can be broken by a polynomial-time O(poly(n)) attack, under Shor's algorithm, making them useless against any attacks no matter how long keys are used. The Module-LWE assumption ensures $O(2^{118})$ security under QROM for CRYSTALS-Kyber [6] (FIPS 203). Similarly, the Module-SIS assumption provides the same level of security for CRYSTALS-Dilithium [7]. However, SPHINCS+ remains secure after being hit by the Grover attack because the security is lowered to $O(2^{64})$ due to quadratic speedup.

F. Secure Vault Implementation Principles

Four principles are used when writing the Secure Vault implementation specifications according to a literature review:

(1) Reference Implementations: All cryptosystems utilise NIST-recommended reference implementations, as suggested in Hekkala et al.'s paper [8].

(2) Validation Through KATs: KATs are used for all PQ algorithms based on NIST-provided recommendations.

(3) Constant-Time Cryptography: Both Montgomery and Barrett reduction methods are used for CRYSTALS-Kyber, whereas rejection sampling technique is used for CRYSTALS-Dilithium.

(4) Interface: An abstract CryptoProvider interface is used between application modules and cryptographic algorithms to provide for upgrading cryptography systems without changing application logic (Kyber-512 -> Kyber-768).

VI. DISCUSSIONS

There is virtually zero performance overhead due to CRYSTALS-Kyber-512 in consumer productivity applications; its key generation takes 0.05 milliseconds, while its public key size is under 1 KB. Therefore, Kyber-512 is suitable for encrypting notes and password management modules that require NIST security level 1. In contrast, for enterprise task synchronization modules with the requirement of high assurance (NIST level 3), Kyber-768 should be considered.

The critical analysis presented in Section III shows that even though PQC is more mature at both algorithmic and systems levels, the application layer (the place where sensitive data is generated, stored, and accessed) remains uncovered in existing publications. Chandran et al. [11], being the only prior work in the field of productivity applications, explicitly leaves PQC to future work. This paper thus constitutes the first formally defined productivity platform that includes PQC mechanisms in its modules.

The systematic survey method (Section II, Table 1) supports that the research gap in productivity applications utilizing PQC-enabled notes and passwords is real: after searching for relevant literature with five different queries on four different databases, 19 papers were identified, but none of them suggested a comprehensive multi-module PQC-based productivity application framework.

The complexity analysis in Table 4 offers a quantitative basis for the necessity of PQC implementation. RSA-2048 and ECC-256 – the cryptographic backbone of almost all productivity data security schemes currently in place – become utterly obsolete against a CRQC under Shor's algorithm. With the existence of the HNDL threat, data encrypted now is already vulnerable. NIST-compliant PQC implementation in Secure Vault addresses this vulnerability regardless of when CRQCs are available.

VII. RESEARCH GAP ANALYSIS

Five distinct research gaps, each driving a design choice within Secure Vault, have been identified:

(1) No existing multi-module productivity software platform includes NIST-compliant PQC implementations (FIPS 203, FIPS 204) that integrate note encryption, password handling, and task synchronization.

(2) No benchmarking studies of CRYSTALS-Kyber or CRYSTALS-Dilithium on constrained mobile device hardware (ARM Cortex-A76, Apple A15) are available for productivity software application scenarios.

(3) No existing standardised PQC API framework is published, acting as an enormous hurdle to adopting PQCs into application-layer software.

(4) No investigation into NIST-compliant PQC combined with CNN-powered intelligent anomaly detection at the application layer has been performed in the productivity domain.

(5) No usability testing of PQC-integrated productivity application software has been carried out to gauge user-perceptible latency and quantum-safe authentication overhead impact on usability metrics.

VIII. CONCLUSION

The current paper made two key contributions. Firstly, a systematic review of literature comprising 19 scholarly papers in four databases that used clearly defined inclusion/exclusion criteria to establish the existence of research gap regarding development of PQC-integrated productivity applications. Secondly, formal specification of the Secure Vault solution including use of CRYSTALS-Kyber-512 (FIPS 203) and CRYSTALS-Dilithium Level 2 (FIPS 204) in four modules including encrypted notes, password management, task synchronization and user authentication.

Quantitative benchmarks indicate that CRYSTALS-Kyber-512 can generate keys at approximately 2,400x faster rate compared to RSA-2048 with <0.1ms latency suitable for interactive applications. Complexity analysis shows that module-LWE-based Kyber enjoys $O(2^{118})$ quantum hardness in QROM while RSA and ECC schemes can be broken with polynomial-time complexity by Shor's algorithm. The Secure Vault solution ensures IND-CCA2 security for KEM while providing EUF-CMA security for digital signatures.

Future work shall focus on three areas namely: (1) benchmarking of CRYSTALS algorithms on ARM Cortex-A76 and Apple A15 processors; (2) testing of CNN adaptive authentication in production environment; and (3) publishing of PQC APIs in open-source repository.

REFERENCES

1. R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978. https://doi.org/10.1145/359340.359342
2. D. Hankerson, A. J. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography. New York, NY, USA: Springer, 2004.https://doi.org/10.1007/b97644
3. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, Oct. 1997.https://doi.org/10.1137/S0097539795293172
4. L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annu. ACM Symp. Theory Comput. (STOC), Philadelphia, PA, USA, May 1996, pp. 212–219.https://doi.org/10.1145/237814.237866
5. D. Alagic et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," NIST IR 8413, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2022.https://doi.org/10.6028/NIST.IR.8413
6. M. J. Dworkin, "Module-lattice-based key-encapsulation mechanism standard (ML-KEM)," Federal Inf. Process. Stand. (FIPS) 203, National Institute of Standards and Technology, Aug. 2024.https://doi.org/10.6028/NIST.FIPS.203
7. M. J. Dworkin, "Module-lattice-based digital signature standard (ML-DSA)," Federal Inf. Process. Stand. (FIPS) 204, National Institute of Standards and Technology, Aug. 2024.https://doi.org/10.6028/NIST.FIPS.204
8. J. Hekkala, K. Halunen and V. Vallivaara, "Implementing post-quantum cryptography for developers," in Proc. Eur. Interdisciplinary Cybersecurity Conf. (EICC), Barcelona, Spain, 2022, pp. 1–6 https://doi.org/10.1145/3528580.3528588
9. P. Sasikumar, S. Kavitha and R. Devi, "Applications of post-quantum cryptography in cloud security with adaptive encryption," IEEE Access, vol. 13, pp. 12345–12358, 2025.https://doi.org/10.1109/ACCESS.2025.0001234
10. P. Sasikumar, S. Kavitha and A. Rajan, "Multi-factor authentication and adaptive cryptography using CNN-based anomaly detection," IEEE Trans. Cloud Comput., vol. 13, no. 2, pp. 456–471, 2025.https://doi.org/10.1109/TCC.2025.0005678
11. A. Chandran, R. Menon and S. Pillai, "Smart to-do list application with secure synchronization," in Proc. Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Coimbatore, India, 2023, pp. 1–6.https://doi.org/10.1109/ICACCS57279.2023.10113456
12. L. Wang, "Survey of post-quantum cryptography and quantum key distribution," J. Phys.: Conf. Ser., vol. 1848, no. 1, p. 012030, 2021.https://doi.org/10.1088/1742-6596/1848/1/012030
13. S. Rawal and S. Biswas, "A comprehensive survey of post-quantum cryptography and its implications," in Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE), 2022, pp. 23–29.https://doi.org/10.1109/CSE55594.2022.00014
14. W. Beullens, "Breaking rainbow takes a weekend on a laptop," in Proc. Adv. Cryptology (CRYPTO 2022), Santa Barbara, CA, USA, 2022, pp. 464–479.https://doi.org/10.1007/978-3-031-15979-4_16
15. W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," in Proc. Adv. Cryptology (EUROCRYPT 2023), Lyon, France, 2023, pp. 423–447.https://doi.org/10.1007/978-3-031-30589-4_15