JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# A SURVEY ON POST-QUANTUM CRYPTOGRAPHY APPROACHES FOR SECURE PASSWORD MANAGEMENT

**[1]Adyuth V, [2]Nidhi Narayan, [3]Pranav Neelkanth Hugar, [4]Dr Pallavi Kulkarni**

[1]Student, [2]Student, [3]Student, [4]Assistant Professor
Department of Computer Science & Engineering (Cyber Security),
Dayananda Sagar College of Engineering, Bengaluru, India

***Abstract :*** As better quantum computers are being developed, them breaking classical cryptography in polynomial time is now a looming threat. Shor's algorithm proves mathematically that current encryption standards are not secure against the computing power of quantum computers. Currently popular Post Quantum Cryptography (PQC) algorithms are compute-intensive, also requiring large key sizes. This hinders the adoption of PQC algorithms in real-world digital security systems. There exists a gap in the case of password managers, where adoption of PQC practices is scarce. This survey focuses on the possible PQC primitives, their drawbacks and methods to possibly overcome these drawbacks. This information will be used to determine efficient approaches for building a PQC-based Password Manager. The survey will also consider their mathematical base, their security level and also how efficient they are. The performance trade-offs when PQC algorithms are used are also mentioned in the survey. It also justifies why we need solutions that are scalable, secure and also practical in the post-quantum era.

***Index Terms*** **- Post-Quantum Cryptography (PQC), Password Managers, ML-KEM, ML-DSA, Quantum Computing, Lattice-based Cryptography, Cryptographic Transition, Hybrid Encryption.**

## I. INTRODUCTION

The backbone of digital security is modern cryptography. It protects data, network and applications. The current digital landscape is fully exposed to malicious actors without it. The advancement from classical computing to quantum computing has increased the processing power of computers by a large extent [14]. This processing power allows users to solve complex problems significantly faster, which also poses a threat on the security of the current traditional encryption methods. Attackers can collect and store encrypted data now, which can be decrypted once quantum computers are available. This is known as the "store now, decrypt later" attack. Additionally, Shor's algorithm also proves that a sufficiently powered quantum computer can crack the cryptographic systems that are based on the factorization of large prime numbers like RSA and ECC in polynomial time [13]. Classical cryptographic techniques such as ECC are still widely used in secure communication models [19], but these approaches are expected to become vulnerable in the quantum era, reinforcing the need for PQC. Post-quantum cryptographic practices can be the solution to these threats. Post quantum cryptography (PQC) focuses on developing algorithms which are secure in terms of classical as well as quantum cryptography. PQC uses mathematical problems (eg, lattice-based problems) which cannot be brute-forced by quantum computers. The National Institute of Standards and Technology (NIST) is making efforts to standardise PQC practices. In 2022, NIST announced its first set of standardised PQC algorithms. They are CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium(ML-DSA), SPHINCS+ and FALCON. This survey will mainly look into ML-KEM and ML-DSA. The survey addresses the need for a collective outlook on the most popular PQC algorithms pertaining to Key Encapsulation and Digital Signature mechanisms.

## II. LITERATURE SURVEY

While significant progress is being made with regard to post-quantum cryptography (PQC) development in terms of both standardization and deployment in practical applications; Moody et al. (2024) published the first official NIST PQC transition roadmap which outlined a phased migration path that includes approval of three quantum-resistant standards (ML-KEM, ML-DSA, SLH-DSA). The roadmap also outlines an approval process for deprecation of all classical schemes (RSA & ECDSA) with full prohibition expected by 2035. In doing so, the roadmap established a definitive timeline for migration by industry while also accounting for hybrid transition complexities and related implementation burdens. Vos et al. (2025) propose a hybrid Password-Authenticated Key Exchange (PAKE) protocol that integrates classical cryptography and post-quantum primitives within the random oracle model that enables a smoother migration to quantum-safe authentication [8].

Most research concerning fundamental PQC primitives has focused on lattice-based construction (such as CRYSTALS-Kyber [ML-KEM] and CRYSTALS-Dilithium [ML-DSA]) that offer excellent combinations of security and computational efficiency based upon the Learning With Errors (LWE) problem. Avanzi et al. (2021) and Shi Bai et al. (2021) are examples of studies that

validated the trade-off between the security and performance of these two leading candidate constructions for encryption and digital signature use cases. More recently, Wai-Kong Lee et al. (2022) and Zhou et al. (2024) proposed several optimizations including GPU-based acceleration for improving throughput in real-time environments and optimizing parameters to improve throughput in resource-constrained environments.

There have also been numerous investigations into practical PQC integration in the context of password management and authentication systems. Specifically, Aremu, Tonyalı, and K¨ose (2022) published the results of their investigation into the first password manager based on PQC (using Kyber and Dilithium). While they concluded that it was feasible to protect credentials via PQC, they also noted several limitations including memory snooping and lack of hybrid interoperability. Building on the findings of Aremu, Tonyalı, and K¨ose, Meeran Hassan et al. (2024) integrated multiple PQC schemes (including MLDSA, ML-KEM, and risk-based authentication) with a vector database driven single sign-on (SSO) system that achieved higher than 90% detection accuracy and faster authentication times. Jurkiewicz (2025) introduces a key lifecycle management scheme that is lattice-based password-authenticated and features periodic key updates to achieve forward security against quantum adversaries [9]. Meanwhile, Vos et al. (2025) investigated hybrid PQC-classical password authenticated key exchange protocols to support the transition of existing legacy systems to future quantum computing systems while maintaining adequate levels of cryptographic strength. Stebila and Wilson (2024) illustrate WebAuthn frameworks that use latticebased signatures for securing account-recovery flows within and provide a practical path for integrating PQC into modern authentication recovery systems [10]. Zhou, Zhang, and Li (2024) analyze the effects of tuning implementation constraints on the performance of the CRYSTALS-Kyber (ML-KEM) algorithm across hardware and software environments. It also offers insights into achieving balanced efficiency in practical PQC deployments [18].

**Table 1. Summary of Key Papers on PQC, Authentication, and Password Security**

| Year | Author(s) | Paper Name / Problem Addressed | Contribution / Key Findings | Limitations |
|---|---|---|---|---|
| 2024 | M. Hassan *et al.* | Quantum-safe authentication using PQC + SSO + vector DB + RBA | 98% threat detection; faster PQC-based SSO tokens; secure ML-DSA/ML-KEM workflow | High CPU/RAM usage in vector databases |
| 2022 | O.R. Aremu, S. Tonyalı, A. Ko¨se | PQC-enabled password manager using Kyber-512 & Dilithium-2 | Shows PQC feasible for practical password managers; secure client-side encryption/signing | Vulnerable to memory snooping |
| 2021 | Roberto Avanzi *et al.* | CRYSTALS-Kyber KEM design (Module-LWE) | Fast, secure KEM with low failure rates; widely adopted PQC standard | Side-channel vulnerabilities; non-tight reduction |
| 2020 | V. Lyubashevsky *et al.* | CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation | Standardized Dilithium signature scheme for PQC; focuses on lattice-based security. | Signature size and computation cost higher than classical algorithms. |
| 2024 | H. Li, B. Wang | LWE-based Secure Remote Password (SRP) protocol | Quantum-safe mutual authentication using lattice primitives | Higher computational load |
| 2022 | W. K. Lee *et al.* | DPCrypto: Acceleration of Post-Quantum Cryptography Using Dot-Product Instructions on GPUs | 4.37× throughput (FrodoKEM) and Saber acceleration using GPU dot-product ops | GPU overhead and warp divergence issues |
| 2025 | A. A. Favour, A. Henry, and J. Badmus | Hardware Acceleration of PQC Using ML-Based Optimizers | Introduced ML-based optimization for faster PQC hardware implementations. | Experimental validation required; lacks real-world benchmark data. |
| 2025 | J. Vos *et al.* | A Hybrid Asymmetric PAKE in the Random Oracle Model | Smooth migration path for hybrid authentication; secure PAKE design | Draft stage; not tested in deployments |
| 2025 | M. Jurkiewicz | Forward-secure password lifecycle scheme | Lattice-based evolving keys ensure long-term forward secrecy | Theoretical design; lacks real implementation |
| 2024 | D. Stebila and S. Wilson | Post-quantum WebAuthn account recovery | Dilithium-based signatures for PQ recovery; practical demonstration | Limited to WebAuthn ecosystem |
| 2024 | P. Ravi *et al.* | “Information injection” technique enhances adaptive/timing attack resistance | Provided an in-depth survey of side-channel and fault-injection attacks on lattice-based PQC schemes. | Focused on software implementations; lacks mitigation framework. |
| 2025 | D. Ramakrishna, M. A. Shaik | Thermal/EM side-channel detection for PQC | Real-time dual-layer detection for PQ cryptographic operations | Adds performance and scalability overhead |

| | | | | |
|---|---|---|---|---|
| 2015 | M. Jones, J. Bradley, N. Sakimura | JSON Web Token (JWT) claims representation | Compact signed/encrypted token framework for authentication | Weaker security guarantees than SAML |
| 1999 | P. W. Shor | Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer | Presented the first efficient quantum algorithm to break RSA and discrete-log systems. | Requires scalable quantum hardware; not practical with current quantum systems. |
| 1996 | A. Ekert and R. Jozsa | Quantum Computation and Shor's Factoring Algorithm | Provided theoretical foundations linking quantum mechanics with computation (Shor's algorithm). | Conceptual focus; no experimental verification at that time. |

## III. Some PQC Approaches For Password Managers

### 3.1 Post Quantum Cryptographic (PQC) Primitives

Post-quantum cryptography (PQC) supports the new primitives that are resistant to quantum attacks. These algorithms are built using hard mathematical problems like the learning with errors (LWE) problem [5], which is the foundation for many lattice-based problems. Among these many lattice-based constructions, the NIST-recommended standard algorithms are ML-KEM and ML-DSA. ML-KEM is a Key Encapsulation Mechanism algorithm that provides efficient and secure key exchange with practical performance [3]. ML-DSA serves as a Digital Signature Algorithm confirming authenticity and integrity [4]. Another stateless hash-based signature scheme which provides post-quantum security without using the lattice structure is SPHINCS+ [17].

### 3.2 Module Lattice-Key Encapsulation Mechanism (ML-KEM)

ML-KEM (called CRYSTALS-Kyber before standardisation) is lattice-based and built upon the learning with errors (LWE) problem [3]. This makes it secure against classical and quantum adversaries. The algorithm uses a module lattice structure to encapsulate and decapsulate keys. This results in a reduction of key sizes as compared to other post-quantum schemes. The performance of ML-KEM can be improved by implementing GPU-based Dot-Product instructions which will accelerate the matrix computations [6]. The exploration of ML-KEM application in Single Sign-On solutions [2] has exhibited the multifaceted capabilities of the algorithm other than key exchange.

### 3.3 Module Lattice Digital Signature Algorithm (ML-DSA)

ML-DSA (called CRYSTALS-Dilithium before standardisation) is one of the most advanced digital signature schemes built using the learning with errors (LWE) and Short Integer Solution (SIS) problems [4]. It provides strong security against classical and quantum attacks without requiring a large key size. The efficiency of this algorithm too can be optimized through GPU and ML-based approaches [6] [7] and hence is applicable in Single Sign-On solutions [2].

### 3.4 Transition From Classical to Post-Quantum Cryptography

The transition from classical cryptography like RSA and ECC to PQC is not a choice but a requirement now, as we advance into the quantum computing era. As replacing the current infrastructure entirely is not possible, we should follow a hybrid cryptographic model and combine the classical and PQC algorithms to ensure security during migration. This hybrid model maintains security while complying with legacy systems. Research shows the use of these hybrid frameworks in projects as demonstrated in the works of Aremu et al. (2022) and Hassan et al. (2024). The NIST.IR-8547 report gives us a migration strategy which guides organisations through the post-quantum transition.

### 3.5 Security of a Classical Password Manager

Traditional Password Managers utilize several Architectural Paradigms that each implement their own technologies and methods for deployment.

- Vault-Based Architecture The most common type of architecture stores encrypted passwords either locally or in the Cloud utilizing a Master Password. A classic example of this is LastPass and KeePass. LastPass and KeePass use AES-256 to encrypt data and PBKDF2 and Argon2d to derive strong encryption keys from the Master Password entered by users.
- Generative Approaches Rather than store users' passwords, generative methods generate a new, site-specific password at the time of login using Device-Enhanced Password Authenticated Key Exchange (DE-PAKE) and Oblivious Pseudo-Random Functions (OPRF). This eliminates the risk of losing all user passwords if one of the systems is compromised.
- Distributed Systems Distributed Systems provide credential shares across multiple devices using Shamir's Secret Sharing to ensure no single device has access to the full set of credentials and thus provides redundancy in case of system failure.
- Hardware Integration In addition to the above methods, some password managers also include Hardware-based Security Features using Physically Unclonable Functions (PUFs) or USB Keys to physically bind users' credentials to a specific device providing an additional layer of security.
- Advanced Cryptographic Techniques Innovative Methods are being developed that will make it even more difficult to gain unauthorized access to a User's Credentials. For instance, using Steganography to conceal encrypted credentials inside images and Privacy-Preserving Biometric Authentication with Privacy Protected Templates. [16]

### 3.6 Bridging Classical Password Managers and Post-Quantum Cryptography

Although RSA and ECC are widely used by classical password managers for password protection, they can be broken with a quantum computer using Shor's algorithm. Although the National Institute of Standards and Technology (NIST) has developed quantum-resistant encryption methods, such as MLKEM and ML-DSA and standardized them through NIST.IR-8547, there have

been no implementations of these quantum-resistant algorithms in password managers. As outlined in NIST.IR-8547, a hybrid approach will enable the gradual transition to post-quantum primitives while ensuring that the overall system is still compatible with classical systems

**Table 2. Comparison of Password Manager Implementations**

| Password Manager | Encryption Standard | Quantum Vulnerability |
|---|---|---|
| LastPass | AES-256 + RSA | Vulnerable to Shor's algorithm |
| 1Password | AES-256 + ECC | Vulnerable to Shor's algorithm |
| Bitwarden | AES-256 + RSA | Vulnerable to Shor's algorithm |
| KeePass (Local) | AES-256 | Vulnerable if user de- vice compromised |
| Dashlane | AES-256 + ECC | Vulnerable to Shor's algorithm |

## IV. Comparative Analysis And Trade Offs

### 4.1 PQC vs RSA

**Table 3. Token Generation Performance Comparison (RSA vs PQC)**

| Algorithm | Mean Time (µs) | Improvement |
|---|---|---|
| RSA | 820.98 | – |
| ML-DSA (PQC) | 201.61 | ≈4× faster |

The results from Hassan et al. (2024) demonstrate PQC's advantage in performance in terms of token generation. The authentication tokens referenced in this study conform to the JSON Web Token (JWT) standard, a widely used format for secure token-based communication [12]. RSA TAKES 821 µ s to generate the token as compared to ML-DSA which takes 201 µ s [2]. Hence ML-DSA is almost 4 times faster to generate a token than RSA. In token verification, competitive speed is maintained by PQC relative to RSA. RSA takes 29 µ s whereas ML-DSA takes 32 µ s which is only a 13% difference [2].

**Table 4. Token Verification Performance Comparison (RSA vs PQC)**

| Algorithm | Mean Time (µs) | Difference |
|---|---|---|
| RSA | 28.65 | – |
| ML-DSA (PQC) | 32.49 | 13% slower |

**Table 5. Memory Usage Comparison between RSA and PQC**

| Algorithm | Mean Memory (KB) | Improvement |
|---|---|---|
| RSA | 292 | – |
| ML-DSA (PQC) | 171 | 40% less memory |

Another area is Memory Efficiency where PQC demonstrates superiority. The mean memory usage in RSA is 292KB, while ML-DSA's is 171KB. This represents a 40% reduction in resource consumption [2]. Lower memory requirements are a factor that improves both scalability and performance for PQC, especially when operating in resource-constrained or distributed settings. When combined with the benefits of security and computation, these lower memory requirements make PQC algorithms viable and sustainable options to replace RSA in post-quantum secure systems.

### 4.2 Vector DB vs SQL DB (Key Storage Performance)

When comparing vector and relational SQL databases, we can see how using an optimized PQC key storage has resulted in enhanced performance capabilities. In Hassan et al. (2024) it was demonstrated that when using a vector database, there is a significant advantage in terms of write speed, where the average time per operation for writing 10,000 records is approximately 0.060 milliseconds; while writing 90,000 records takes about 0.100 ms; as compared to the relational SQL database's time of approximately 0.33 ms per operation. The advantages in relation to data-write capability are approximately 331% [2]. These advantages result in improved performance (lower latency) and faster handling of cryptographic keys. Thus, in terms of scalability and ease of use (i.e., faster data and key retrieval), vector databases may be considered more suitable for large-scale, post-quantum-ready systems.

**Table 4. Comparison of PQC Key Storage Performance: Vector DB vs SQL DB**

| Number of Entries | Vector DB Write Time (ms) | SQL DB Write Time (ms) |
|---|---|---|
| 10,000 | 0.060 | 0.332 |
| 50,000 | 0.080 | 0.331 |
| 90,000 | 0.100 | 0.333 |

## V. Comparative Analysis And Trade Offs

With the advanced development of PQC, numerous challenges exist that currently limit implementation across platforms. An example of some of these challenges include the fact that lattice-based algorithms such as ML-KEM and MLDSA require increased

Key and Signature size(s), which lead to an increase in Data Storage and Transmission requirements, thereby motivating future research into Key Compression, and Parameters for Improving Practicality [3] Dilithium2020. Additionally, another major obstacle to the successful deployment of PQC is the computational overhead associated with its operation; however, using hardware Accelerators (eg, GPUs)and Machine Learning (ML)-based Optimizers has demonstrated significant improvement in operational efficiency [6] [7]. There also remains a growing concern regarding emerging Side Channel Attack threats [11], as a result, Hybrid Architectures are currently under design to provide both Real Time Monitoring and Techniques to counter these Threats for Secure Implementation [15]. Lastly, The Slow Pace of Industry Adoption of PQC is still largely attributed to Integration Complexity; however, this can be alleviated through the use of Hybrid Transition Models which combine Classical and PQ Algorithms for Compatibility and Gradual Deployment [1], eg, NIST.IR-8547.As a result, the continuation of Research and Standardization to address the Challenges listed above will be essential to the development of Efficient, Scalable, and Quantum-Resistant Cryptographic Systems.

The emergence of highly effective quantum computers may eventually be a significant threat to our present-day encryption technologies, including RSA and AES, both of which can be broken by quantum computers in an amount of time that is proportional to the input size (polynomial time) via Shor’ s algorithm. In order to mitigate this risk, we believe it is necessary to rapidly adopt Post-Quantum Cryptography (PQC). As such, integrating PQC into existing critical digital security systems, such as password managers, is urgently needed; however, PQC is relatively absent from these applications at this time. Our survey focuses on lattice-based primitives, specifically the NIST standardized primitives MLKEM and ML-DSA. These primitives utilize the LWE problem and other related difficult mathematical problems to provide security against quantum computers. The research indicates that these primitives have been used successfully in practical password manager applications and demonstrate the feasibility of utilizing them in password manager applications. Additionally, the research demonstrated several advantages over classical systems, particularly with respect to performance, as shown by the fact that the time required for generating tokens was much less for ML-DSA than for RSA and, further, the memory usage associated with ML-DSA was also less than that associated with RSA. Therefore, to address the inevitable transition from classical systems to systems that will use PQC, it is essential to implement a secure hybrid cryptographic system that utilizes both classical cryptography and PQC, as indicated in the guidelines provided by NIST. However, while the implementation of hybrid systems may alleviate some of the issues associated with transitioning to PQC, there are still additional issues associated with the use of PQC that include, but are not limited to, larger key and signature sizes that result in greater data storage and transmission requirements, the increased computational overhead, and the persistent concerns about side-channel attacks. Ultimately, addressing the complexity of integrating PQC into practical cryptographic systems will require continuing research into alternative methods that can be utilized to compress keys, to accelerate computations via hardware accelerators (such as GPUs), and to develop hybrid transition models. It is only by continuing to conduct research into these alternatives that we will be able to create cryptographic systems that are efficient, scalable, and resistant to quantum computers in the post-quantum world.

## VI. Conclusion

The emergence of highly effective quantum computers may eventually be a significant threat to our present-day encryption technologies, including RSA and AES, both of which can be broken by quantum computers in an amount of time that is proportional to the input size (polynomial time) via Shor’ s algorithm. In order to mitigate this risk, we believe it is necessary to rapidly adopt Post-Quantum Cryptography (PQC). As such, integrating PQC into existing critical digital security systems, such as password managers, is urgently needed; however, PQC is relatively absent from these applications at this time. Our survey focuses on lattice-based primitives, specifically the NIST standardized primitives MLKEM and ML-DSA. These primitives utilize the LWE problem and other related difficult mathematical problems to provide security against quantum computers. The research indicates that these primitives have been used successfully in practical password manager applications and demonstrate the feasibility of utilizing them in password manager applications.

Additionally, the research demonstrated several advantages over classical systems, particularly with respect to performance, as shown by the fact that the time required for generating tokens was much less for ML-DSA than for RSA and, further, the memory usage associated with ML-DSA was also less than that associated with RSA.

Therefore, to address the inevitable transition from classical systems to systems that will use PQC, it is essential to implement a secure hybrid cryptographic system that utilizes both classical cryptography and PQC, as indicated in the guidelines provided by NIST.

However, while the implementation of hybrid systems may alleviate some of the issues associated with transitioning to PQC, there are still additional issues associated with the use of PQC that include, but are not limited to, larger key and signature sizes that result in greater data storage and transmission requirements, the increased computational overhead, and the persistent concerns about side-channel attacks.

Ultimately, addressing the complexity of integrating PQC into practical cryptographic systems will require continuing research into alternative methods that can be utilized to compress keys, to accelerate computations via hardware accelerators (such as GPUs), and to develop hybrid transition models. It is only by continuing to conduct research into these alternatives that we will be able to create cryptographic systems that are efficient, scalable, and resistant to quantum computers in the post-quantum world.

## VII. Acknowledgment

We gratefully acknowledge Dayananda Sagar College of Engineering for offering an enriching academic and research environment. Our special thanks go to Dr Mohammed Tajuddin, our Head of Department, for his constant support; and to the faculty members whose encouragement has been instrumental in the completion of this work.

## References

**[1]** O. R. Aremu, S. Tonyalı, and A. K¨ose, “A Password Manager for Post-Quantum Era,” in Proc. 2nd Int. Conf. Cyber Secur. Digit. Forensics (ICONSEC’ 22), Fethiye, Turkey, Sept. 7 – 11, 2022.

**[2]** M. Hassan, R. Nimsara, R. Dharmawardhane, V. Basnagoda, K. Y. Abeywardena, and D. Siriwardana, "Post-Quantum Single Sign-On Solution," in Proc. 2024 Int. Conf. Comput. Appl. (ICCA), Malabe, Sri Lanka, Dec. 2024, pp. 1 – 6, doi: 10.1109/ICCA62237.2024.10927943.

**[3]** R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehl´e, "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation," NIST PQC Round 2 Submission, pp. 143, 2019.

**[4]** V. Lyubashevsky et al., "CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation," 2020.

**[5]** H. Li and B. Wang, "A Secure Remote Password Protocol From the Learning With Errors Problem," in Proc. 2022 IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), 2022, pp. 1084 – 1090.

**[6]** W. K. Lee, H. Seo, S. O. Hwang, R. Achar, A. Karmakar, and J. M. B. Mera, "DPCrypto: Acceleration of Post-Quantum Cryptography Using Dot-Product Instructions on GPUs," IEEE Trans. Circuits Syst. I: Regul. Pap., vol. 69, no. 9, pp. 3591 – 3604, 2022, doi: 10.1109/TCSI.2022.3176966.

**[7]** A. A. Favour, A. Henry, and J. Badmus, "Hardware Acceleration of PQC Using ML-Based Optimizers," 2025.

**[8]** J. Vos, S. Jarecki, C. A. Wood, C. Yun, S. Myers, and Y. Sierra, "A Hybrid Asymmetric Password-Authenticated Key Exchange in the Random Oracle Model," IACR Cryptol. ePrint Arch., Paper 2025/1343, 2025. [Online]. Available: https://eprint.iacr.org/2025/1343

**[9]** M. Jurkiewicz, "Quantum-Safe Forward Secure Password Authenticated Key Life-Cycle Management Scheme with Key Update Mechanism," Int. J. Electron. Telecommun., vol. 71, no. 1, pp. 61 – 68, 2025.

**[10]** D. Stebila and S. Wilson, "Quantum-Safe Account Recovery for WebAuthn," in Proc. 19th ACM Asia Conf. Comput. Commun. Secur. (ASIACCS), 2024, pp. 1814 – 1830.

**[11]** P. Ravi, A. Chattopadhyay, J. P. D'Anvers, and A. Baksi, "Side-Channel and Fault-Injection Attacks over Lattice-Based Post-Quantum Schemes (Kyber, Dilithium): Survey and New Results," ACM Trans. Embed. Comput. Syst., vol. 23, no. 2, Art. no. 35, pp. 1 – 54, Mar. 2024, doi: 10.1145/3603170.

**[12]** M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," Tech. Rep., 2015.

**[13]** P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Rev., vol. 41, no. 2, pp. 303 – 332, 1999, doi: 10.1137/S0036144598347011.

**[14]** A. Ekert and R. Jozsa, "Quantum Computation and Shor's Factoring Algorithm," Rev. Mod. Phys., vol. 68, no. 3, pp. 733 – 753, Jul. 1996, doi: 10.1103/RevModPhys.68.733.

**[15]** D. Ramakrishna and M. A. Shaik, "PSESV: A Hybrid Post-Quantum Encryption Framework with Real-Time Thermal and EM Side-Channel Attack Detection," Information Technology and Control, vol. 54, no. 2, pp. 251 – 268, 2025.

**[16]** H. A. Saleh, "Password Managers: A Critical Review of Security, Usability, and Innovative Designs," Journal of Computer Sciences Institute, vol. 36, pp. 328 – 335, Sep. 2025, doi: 10.35784/jcsi.7725.

**[17]** D. J. Bernstein, A. H¨ulsing, S. K¨olbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ Signature Framework," in Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS'19), London, United Kingdom, 2019, pp. 2129 – 2146, doi: 10.1145/3319535.3363229.

**[18]** M. Zhou, K. Zhang, and F. Li, "Evaluating constraint tuning effects on CRYSTALS-KEM performance across hardware and software implementations," J. Syst. Archit., vol. 156, p. 103295, Dec. 2024.

**[19]** V. S. Vagdevi and V. S. Deepthi, "APHEC: Attribute Policy Homomorphic Encryption and an Elliptic Curve Cryptography based Attack Classification Model for MANET Security," Design Engineering (Toronto), vol. 2021, no. 9, pp. 8955–8976, 2021.