Hybrid Post-Quantum Secure Authentication Using Quantum-Generated One-Time Tokens: A Comparative Analysis with Classical Authentication Systems

Author1
Dipika S. Harode ,
Assistant Professor
Department of Computer Science
Vidya Bharati Mahavidyalaya Amravati.
dipikaharode11@gmail.com

Author 2
Vedanti U. Deshmukh
Assistant Professor
Department of Computer Science
Vidya Bharati Mahavidyalaya Amravati.
vedantideshmukh76@gmail.com

.

ABSTRACT

The rapid advancement of quantum computing poses a serious threat to classical authentication mechanisms that rely on computational hardness assumptions and software-based randomness. Traditional authentication systems such as passwords, one-time passwords (OTPs), and public-key cryptography depend heavily on pseudorandom number generators (PRNGs) and classical cryptographic algorithms, many of which are vulnerable to future quantum attacks. This paper proposes and analyzes a Hybrid Post-Quantum Secure Authentication system using Quantum-Generated One-Time Tokens (Q-OTT)**.** The proposed approach combines true quantum randomness obtained from Quantum Random Number Generators (QRNGs) with post-quantum cryptographic (PQC) algorithms for token protection and verification. A detailed comparison between classical authentication systems and the hybrid Q-OTT approach is presented in terms of randomness, security, entropy, and quantum resistance. The study demonstrates that hybrid Q-OTT systems offer significantly enhanced security against both classical and quantum adversaries, at the cost of moderate infrastructure requirements.

Keywords

Post-Quantum Cryptography, Quantum Random Number Generator, One-Time Token, Authentication Systems, Quantum Security, Hybrid Authentication

1. INTRODUCTION

Authentication plays a crucial role in ensuring the security of modern digital systems by verifying the identity of users, devices, and services before granting access to sensitive resources. It serves as the first line of defense against unauthorized access in a wide range of applications, including cloud computing, financial transactions, healthcare systems, Internet of Things (IoT) environments, and critical infrastructure networks. As digital services continue to expand in scale and complexity, the demand for robust, reliable, and future-proof authentication mechanisms has become increasingly important.

Over the years, classical authentication techniques such as passwords, one-time passwords (OTPs), and public-key–based digital signatures have become standard due to their straightforward implementation, low computational overhead, and wide compatibility across platforms. These mechanisms typically rely on well-established cryptographic primitives and software-based pseudo-random number generators. While such approaches have been effective against classical adversaries, they are fundamentally built on computational hardness assumptions and deterministic processes that introduce inherent security limitations. Weak passwords, token reuse, predictable randomness, and key-management challenges continue to expose classical authentication systems to brute-force attacks, replay attacks, phishing, and credential compromise.

Recent advancements in quantum computing have raised serious concerns about the long-term reliability of existing authentication mechanisms. In particular, powerful quantum algorithms such as Shor's algorithm pose a significant threat to widely deployed public-key cryptographic schemes, including RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA), by enabling efficient factorization and discrete logarithm computations. As large-scale quantum computers become more practical, authentication systems that rely on these classical primitives are expected to become increasingly vulnerable. Furthermore, software-based pseudo-random number generators used in traditional authentication frameworks may produce predictable or biased outputs under certain conditions, increasing the risk of token-prediction, impersonation, and replay attacks—especially in high-frequency or resource-constrained environments.

To address these emerging challenges, post-quantum cryptography has been proposed as a promising solution, offering cryptographic algorithms designed to resist quantum attacks. However, many post-quantum authentication methods still depend on classical sources of randomness for key generation and token creation, leaving potential weaknesses in entropy and unpredictability. This limitation highlights the need for authentication mechanisms that not only rely on quantum-resistant algorithms but also incorporate fundamentally stronger sources of randomness.

In response to these concerns, this paper investigates a Hybrid Post-Quantum Secure Authentication approach that combines Quantum-Generated One-Time Tokens (Q-OTT) with post-quantum cryptographic techniques. By leveraging the inherent unpredictability and true randomness provided by quantum processes alongside quantum-resistant cryptographic protections, the proposed framework aims to enhance authentication robustness and mitigate both classical and quantum-enabled attacks. This hybrid model seeks to bridge the gap between theoretical quantum security and practical deployability, offering a forward-looking authentication solution capable of maintaining security guarantees in the post-quantum era.

2. LITERATURE REVIEW

Authentication mechanisms have been the linchpin of digital security for decades. With the rise of quantum computing and its threat to classical cryptography, recent research has shifted toward quantum-safe authentication methods. This literature review covers seminal works and recent developments relevant to the proposed hybrid system that uses quantum-generated randomness and post-quantum cryptographic safeguards.

2.1 Classical Authentication Systems

2.1.1 Passwords and PIN-Based Authentication

Passwords and PINs are the oldest and most prevalent forms of authentication.Diffie & Hellman (1976) highlighted the fundamental importance of secure authentication in networked environments and introduced protocols to prevent replay attacks.Florêncio & Herley (2007) analyzed user-chosen passwords and documented their inherent weaknesses such as predictability and reuse, which make them vulnerable to brute-force and social engineering attacks. These classical studies confirm that reliance on human-generated or software-derived secrets remains fundamentally weak and forms the baseline vulnerability of traditional systems.

2.1.2 One-Time Passwords (OTPs) & Time-Based Schemes

OTPs were introduced as a mitigation strategy for static password attacks.RFC 2289 (Haller, 1998) formalized OTP generation using hash chains.RFC 6238 (M'Raihi et al., 2011) introduced TOTP, using a shared secret and time as inputs.RFC 4226 (M'Raihi et al., 2005) defined HOTP, based on an HMAC-based counter.These works focus on protocol design and synchronization but rely on software PRNGs and shared secrets, leaving them susceptible to seed theft and prediction. Subsequent studies demonstrated how weak entropy in PRNGs compromises OTP unpredictability.

2.2 Public-Key Authentication and Its Limitations

Classical public-key authentication underpins secure sessions and identity verification.Rivest, Shamir, & Adleman (1978) introduced RSA, foundational for digital signatures.NIST & SECG (2000s) standardized elliptic-curve cryptography (ECC) leading to widespread use of ECDSA.However, these are based on computational hardness (factoring, discrete log) — not guaranteed secure against quantum attacks. Shor's quantum factoring algorithm (1994) theoretically breaks RSA/ECC in polynomial time, creating urgency for quantum-safe alternatives.

2.3 Post-Quantum Cryptography (PQC)

PQC aims to replace classical cryptography with algorithms resilient against both classical and quantum attacks. Bernstein et al. (Post-Quantum Cryptography, 2008) provided one of the earliest comprehensive surveys.NIST PQC Standardization Project (2016–ongoing) evaluated submissions for quantum-safe encryption and signatures. Notable selected algorithms include:CRYSTALS-Kyber (NIST PQC KEM standard) — secure key exchange CRYSTALS-Dilithium (NIST PQC signature standard) — digital signatures FALCON, SPHINCS+ — alternative post-quantum signaturesNIST's PQC process formalizes security proofs against quantum adversaries and standards for practical deployment.

3. METHODOLOGY

This study adopts a comparative system analysis methodology to evaluate the proposed Hybrid Post-Quantum Secure Authentication system using Quantum-Generated One-Time Tokens (Q-OTT) against widely deployed classical authentication systems. The comparison is conducted at the system architecture and security property level, focusing on randomness generation, token construction, cryptographic protection, verification mechanisms, and resistance to quantum threats. A common evaluation framework is used to ensure consistency and fairness, enabling a structured assessment of the strengths and limitations of classical authentication approaches relative to the proposed hybrid Q-OTT system.

3.1 Overview of system under Comparison

Based on the defined comparative framework, this study considers two categories of authentication systems: classical authentication mechanisms and the proposed hybrid post-quantum authentication system. Classical authentication systems include password-based authentication, software-generated one-time password mechanisms such as Time-Based One-Time Passwords (TOTP) and HMAC-Based One-Time Passwords (HOTP), and public-key-based authentication schemes using classical cryptographic algorithms such as RSA and ECDSA. These systems represent the most widely deployed authentication approaches in current digital infrastructures and rely on software-based randomness and classical computational hardness assumptions.

In contrast, the proposed hybrid post-quantum authentication system integrates quantum-generated randomness obtained from a Quantum Random Number Generator (QRNG) with a one-time token construction mechanism based on quantum entropy. The generated tokens are protected using post-quantum cryptographic algorithms, such as CRYSTALS-Dilithium for digital signatures and CRYSTALS-Kyber for secure key establishment, ensuring resistance against both classical and quantum adversaries.

This structured comparison evaluates both classical and hybrid authentication approaches at the system design and security property level, rather than focusing on implementation-specific or hardware-dependent details. Such an approach enables a clear assessment of architectural differences, security guarantees, and future readiness of authentication systems in the post-quantum era.

3.2 Architecture Overview of Hybrid Post-Quantum Secure Authentication Using Quantum-Generated One-Time Tokens:

The proposed authentication system follows a hybrid architecture consisting of four main components: Client Device**,** Quantum Random Number Generator (QRNG)**,** Post-Quantum Cryptographic Module and Authentication Server**.** The client device interacts with a QRNG source to generate true random values. These values are used to construct a one-time authentication token, which is then protected using post-quantum cryptographic algorithms before being transmitted to the server for verification

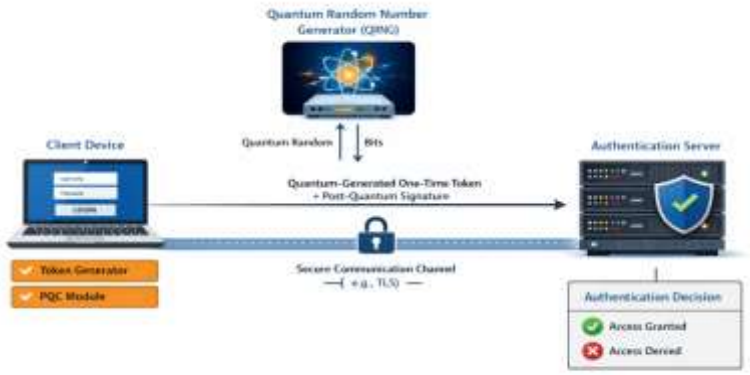

Fig 1: Architecture of Hybrid Post-Quantum Secure Authentication Using Quantum-Generated One-Time Tokens

3.2.1 Client-Side Authentication Module

The client-side module is responsible for initiating the authentication process. It includes the interface through which the user requests authentication and manages local token generation. This module interacts with the quantum randomness source to obtain high-entropy random values and constructs the one-time authentication token. It also hosts the post-quantum cryptographic functions required to protect the token before transmission.

3.2.2 Quantum Random Number Generator (QRNG)

The QRNG serves as the primary entropy source in the architecture. It generates truly random bits based on inherent quantum phenomena, ensuring non-deterministic and unpredictable output. The QRNG may be implemented as a hardware component embedded within the client device or accessed through a trusted external service. The generated quantum randomness forms the foundation of the one-time token, significantly strengthening security compared to software-based randomness.

3.2.3 Post-Quantum Cryptographic Protection Module

The Post-Quantum Cryptographic Module is responsible for securing the generated one-time authentication token. Once the token is constructed using quantum-generated randomness, it is protected using post-quantum cryptographic algorithms, such as quantum-safe digital signature or key encapsulation schemes. This module ensures the integrity and authenticity of the token, even in the presence of quantum-capable adversaries.

3.2.4 Authentication Server

the Authentication Server receives the protected authentication token from the client device and performs verification operations. The server validates the post-quantum cryptographic protection, checks token freshness and correctness, and makes the final authentication decision. Only tokens that successfully pass all verification checks are accepted.

3.3 Working Overview of Hybrid Post-Quantum Secure Authentication Using Quantum-Generated One-Time Tokens:

The proposed Hybrid Post-Quantum Secure Authentication system operates by combining quantum-generated randomness with post-quantum cryptographic protection to generate and verify one-time authentication tokens. The working of the system is designed to ensure high unpredictability, resistance to replay attacks, and security against both classical and quantum adversaries.

3.3.1 QRNG-Based Entropy Source

Unlike classical authentication systems that rely on software-based pseudorandom number generators (PRNGs), the proposed system employs a Quantum Random Number Generator (QRNG) as the primary entropy source. QRNGs exploit inherent quantum phenomena such as photon emission or quantum noise, ensuring that the generated bits are fundamentally unpredictable. The QRNG output provides high-entropy random bits denoted as:

$Rq=\{r1,r2,\ldots,rn\}$

where each bit is generated through a quantum physical process, making prediction or reproduction computationally infeasible.

3.3.2 One Tine Token Structure

The one-time authentication token is constructed by concatenating multiple fields as follows:

Q-OTT= Rq || Ts || N || UID

Where:

Rq = Quantum-generated random bits, Ts = Timestamp indicating token generation time, **N**= Nonce for replay attack prevention , UID= Unique user identifier.

3.3.3 Token Freshness and Replay Protection

The timestamp ensures that the token remains valid only within a predefined time window.The nonce guarantees uniqueness, preventing reuse of tokens even within the same session.This design ensures that each authentication attempt uses a fresh and non-reusable token**.**

3.3.4 Post-Quantum Signature Scheme

To protect the integrity and authenticity of the generated token, the Q-OTT is digitally signed using post-quantum cryptographic (PQC) algorithms, such as: CRYSTALS-Dilithium for digital signatures ,CRYSTALS-Kyber for secure key encapsulation (optional for session establishment).The signing process is defined as:

$\sigma = SignPQC(Q\text{-}OTT,SK)$

where SK represents the post-quantum private signing key.

3.3.5 Security Against Quantum Adversaries

PQC algorithms are designed to resist known quantum attacks, including those based on Shor's and Grover's algorithms. As a result, even a quantum-capable adversary cannot forge or manipulate authentication tokens.

3.3.6 Authentication Request Generation

Once the token is generated and signed, the authentication request transmitted to the server contains:

Auth_Request ={ Q-OTT,σ}

This request is sent over a classical communication channel (e.g., HTTPS), without requiring quantum communication infrastructure.

3.3.7 Server Side Signature Verification

Upon receiving the authentication request, the server verifies the post-quantum signature using the corresponding public key:

VerifyPQC(Q-OTT,σ,PK)

If verification fails, the authentication request is immediately rejected.

3.3.8 Server SideToken Validation Checks

If the signature is valid, the server performs the following checks:Timestamp Validation – Ensures token freshness,Nonce Validation – Prevents replay attacks,User ID Validation – Confirms user authenticity .Only tokens that pass all validation checks are accepted.

4. RESULT & DISCUSSION

This section presents the results of the comparative system-level analysis between classical authentication systems and the proposed Hybrid Post-Quantum Secure Authentication using Quantum-Generated One-Time Tokens (Q-OTT). Since the study is analytical in nature, results are derived from architectural evaluation, security property analysis, and threat resistance assessment, rather than empirical deployment.

4.1 Comparative Analysis Results

The analysis reveals clear differences between classical authentication mechanisms and the proposed hybrid Q-OTT system across multiple dimensions, including randomness quality, cryptographic strength, quantum resistance, and system robustness.

4.1.1 Randomness and Entropy

Classical authentication systems rely on software-based pseudorandom number generators (PRNGs) for generating passwords or one-time tokens. While efficient, PRNGs are deterministic and depend on seed secrecy. If the seed or internal state is compromised, token predictability becomes possible.

In contrast, the proposed hybrid system employs a Quantum Random Number Generator (QRNG), which produces randomness based on inherent quantum phenomena. This results in true, non-deterministic entropy, making token prediction computationally and physically infeasible . Comparing Both System The hybrid Q-OTT system demonstrates significantly higher entropy and unpredictability compared to classical systems.

4.1.2 Token Security and Forgery Resistance

In classical OTP systems, token security depends on the secrecy of shared keys and the strength of classical cryptographic algorithms. Similarly, public-key authentication using RSA or ECDSA is vulnerable to future quantum attacks.

The hybrid Q-OTT system secures tokens using post-quantum cryptographic (PQC) algorithms, such as CRYSTALS-Dilithium and CRYSTALS-Kyber. These algorithms are designed to resist both classical and quantum cryptanalytic techniques.
Hybrid Q-OTT tokens provide strong resistance to forgery, even under quantum adversary models, whereas classical tokens do not offer long-term security guarantees.

4.1.3 Resistance to Quantum Attacks

Classical public-key authentication schemes are known to be vulnerable to Shor's algorithm, which can efficiently break RSA and ECC once large-scale quantum computers become practical.

The proposed system replaces classical cryptographic primitives with quantum-safe alternatives, ensuring that authentication security remains intact even in a post-quantum environment.In conclusion Classical systems show no quantum resistance, while the hybrid Q-OTT system exhibits high quantum resilience by design.

4.1.4 Replay and Freshness Protection

Both classical OTP systems and the proposed hybrid system employ timestamps or counters to mitigate replay attacks. However, in classical systems, replay protection can be weakened if token generation or verification logic is compromised.

In the hybrid system, replay protection is reinforced through Quantum-generated randomness, Nonce-based uniqueness, Post-quantum signature validation. The hybrid Q-OTT system offers stronger replay attack resistance due to combined cryptographic and randomness-based safeguards.

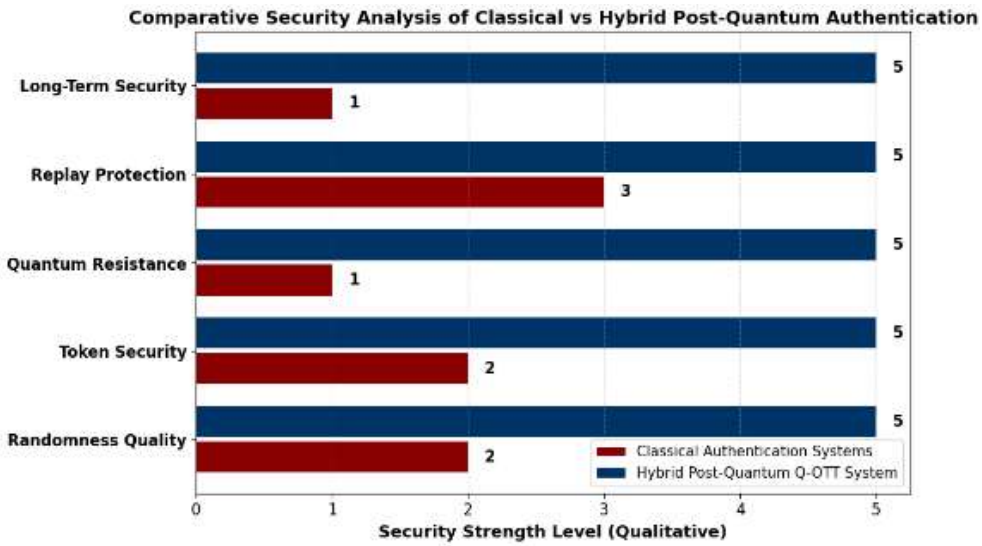

Fig 2: Graph Comparing Classical vs Hybrid Post-Quantum Authentication

4.2 Discussion

The results of the comparative analysis highlight that classical authentication systems are increasingly inadequate in the context of emerging quantum threats. Their reliance on deterministic randomness and classical cryptographic

assumptions makes them vulnerable to both present-day attacks and future quantum adversaries.The proposed hybrid Q-OTT system addresses these limitations by combining true quantum randomness with post-quantum cryptographic protection, thereby strengthening authentication security at both the entropy and cryptographic levels. Although the hybrid approach introduces additional infrastructure requirements, such as QRNG integration and PQC computation, these costs are justified for applications requiring long-term security and quantum resilience.Furthermore, the system's ability to operate over classical communication channels ensures practical deployability without the need for quantum networking infrastructure. This makes the proposed architecture suitable for real-world applications such as banking systems, cloud authentication services, critical infrastructure, and government systems.Overall, the discussion confirms that the hybrid Q-OTT approach represents a **balanced and forward-looking authentication solution**, offering significantly improved security guarantees compared to classical methods while remaining compatible with existing network environments.

5. CONCLUSION

This study presented a comparative system-level analysis of classical authentication mechanisms and a Hybrid Post-Quantum Secure Authentication system using Quantum-Generated One-Time Tokens (Q-OTT). The analysis focused on architectural design, randomness generation, cryptographic protection, and resistance to quantum-era security threats. The findings clearly demonstrate that while classical authentication systems remain widely deployed due to their simplicity and low infrastructure requirements, they exhibit significant limitations in terms of randomness quality, long-term security, and resilience against quantum attacks. The proposed hybrid authentication approach addresses these limitations by integrating true quantum-generated randomness through a Quantum Random Number Generator (QRNG) with post-quantum cryptographic algorithms for token protection and verification. This combination significantly enhances token unpredictability, forgery resistance, and overall authentication robustness, even under advanced quantum adversary models. The comparative results highlight that the hybrid Q-OTT system consistently outperforms classical methods across key security parameters, particularly in quantum resistance and long-term security. Although the hybrid system introduces moderate infrastructure complexity due to QRNG integration and post-quantum computation, the security benefits outweigh these challenges for applications requiring future-proof authentication. Importantly, the proposed architecture operates over classical communication channels, making it practical for real-world deployment without the need for quantum networking infrastructure.

In conclusion, the Hybrid Post-Quantum Secure Authentication using Quantum-Generated One-Time Tokens represents a viable and forward-looking solution for securing authentication systems in the post-quantum era. As quantum computing capabilities continue to advance, adopting such hybrid authentication frameworks will be essential for ensuring long-term security in critical digital infrastructures.

Refrences

1. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing, 26*(5), 1484–1509.
2. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. *NIST Internal Report 8105*. National Institute of Standards and Technology.
3. National Institute of Standards and Technology. (2024). Post-quantum cryptography standardization.
4. Lyubashevsky, V., Ducas, L., Kiltz, E., Lepoint, T., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: Digital signatures from module lattices. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 238–255).
5. Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., & Stehlé, D. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *Proceedings of the IEEE European Symposium on Security and Privacy* (pp. 353–367).

6. Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics, 89*(1), 015004.
7. Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016). Quantum random number generation. *npj Quantum Information, 2*, 16021.
8. M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). TOTP: Time-based one-time password algorithm. *IETF RFC 6238*.
9. M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). HOTP: An HMAC-based one-time password algorithm. *IETF RFC 4226*.
10. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120–126.
11. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.
12. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41.
13. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y. K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Jordan, S. (2022). Status report on the second round of the NIST post-quantum cryptography standardization process. *NIST Internal Report 8309*.
14. Buchmann, J., Dahmen, E., & Hülsing, A. (2014). Hash-based digital signature schemes. In J. Buchmann & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 35–93). Springer.
15. Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum, 5*, 433.
16. Singh, S., & Kumar, A. (2022). A survey on authentication mechanisms for secure systems. *Journal of Information Security and Applications, 66*, 103145.
17. Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics, 89*(1), 015004.
18. Lyubashevsky, V., et al. (2018). CRYSTALS-Dilithium: Digital signatures from module lattices. *IEEE Symposium on Security and Privacy*, 238–255.
19. Bos, J. W., et al. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. *IEEE European Symposium on Security and Privacy*, 353–367.
20. Ma, X., et al. (2016). Quantum random number generation. *npj Quantum Information, 2*, 16021.