Review

# A Comparative Analysis of Security Margins and Practical Deployment Readiness of NIST Round 3 Finalist Post-Quantum Cryptographic Algorithms

Janaka Ishan Senarathna * and Janaka Ishan Senarathna

Posted Date: 12 May 2025

doi: 10.20944/preprints202505.0762.v1

Keywords: post-quantum cryptography; NIST Round 3 Finalist Algorithms; CRYSTALS-Kyber; CRYSTALS-Dilithium; FALCON; SPHINCS+, security margins; deployment readiness

*Review*

# A Comparative Analysis of Security Margins and Practical Deployment Readiness of NIST Round 3 Finalist Post-Quantum Cryptographic Algorithms

**Janaka Ishan Senarathna**

Department of Computer and Data Science, NSBM Green University, Mahenwatta, Pitipana, Homagama, Sri Lanka; janakaishansenarathna0169@gmail.com or djisenarathna@students.nsbm.ac.lk

**Abstract:** The National Institute of Standards and Technology (NIST) has recently concluded the third round of its Post-Quantum Cryptography Standardization Process, selecting four finalist algorithms for standardization: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. These algorithms are designed to withstand attacks from both classical and quantum computers, ensuring the long-term security of digital communications. This paper presents a comprehensive comparative analysis of the security margins and practical deployment readiness of these finalist algorithms. CRYSTALS-Kyber, a key encapsulation mechanism based on the hardness of the Module Learning With Errors problem, offers strong security and efficient performance. CRYSTALS-Dilithium, a digital signature algorithm based on module lattices, provides robust security guarantees and relatively straightforward implementation. FALCON, a lattice-based digital signature algorithm utilizing the Fast Fourier Transform, offers compact signatures and fast verification but faces implementation challenges due to its reliance on floating-point arithmetic. SPHINCS+, a hash-based signature scheme, stands out as a conservative choice with security based solely on the well-established security of hash functions. The analysis reveals that while each algorithm has its strengths, they also face unique challenges in terms of side-channel vulnerabilities, formal security proofs, and performance trade-offs. The practical deployment of these algorithms requires careful consideration of specific security requirements, performance needs, and resource constraints. Ongoing research efforts aim to enhance the algorithms' resistance against advanced attacks, optimize their performance across diverse platforms, and develop standardized and secure hybrid cryptographic systems. The transition to post-quantum cryptography will involve challenges such as interoperability with legacy systems, the need for clear standards and regulatory guidance, and the costs associated with software and hardware updates. Continued engagement with the cryptographic community and monitoring of the evolving security landscape will be crucial for ensuring a secure and effective migration to post-quantum cryptography.

**Keywords:** post-quantum cryptography; NIST Round 3 Finalist Algorithms; CRYSTALS-Kyber; CRYSTALS-Dilithium; FALCON; SPHINCS+, security margins; deployment readiness

## 1. Introduction

The advent of quantum computing presents a significant and evolving threat to the landscape of digital security. Theoretically, quantum computers possess the computational power to efficiently break many of the current public-key cryptography algorithms, such as RSA and Elliptic Curve Cryptography (ECC), which underpin much of our modern digital infrastructure.[1] This vulnerability arises from Shor's algorithm, a quantum algorithm capable of factoring large numbers and solving discrete logarithm problems in polynomial time, tasks that are computationally intractable for classical computers.[3] The potential compromise of these widely used cryptographic methods necessitates a proactive transition to post-quantum cryptography (PQC), which aims to develop cryptographic algorithms secure against both classical and quantum computers.[1] The urgency of this transition is amplified by the "harvest now, decrypt later" threat, where malicious actors may be collecting encrypted data today with the intention of decrypting it in the future when sufficiently powerful quantum computers become available.[5] This long-term risk underscores the immediate need for organizations to begin planning and implementing quantum-resistant solutions for data with extended confidentiality requirements.[7]

Recognizing this impending cryptographic disruption, the National Institute of Standards and Technology (NIST) initiated a Post-Quantum Cryptography Standardization Process in 2016.[1] This multi-year, multi-round competition aimed to identify and standardize quantum-safe algorithms through a rigorous evaluation process involving global experts.[9] The evaluation criteria encompassed security, performance, and various other algorithm characteristics.[11] In 2022, NIST announced the first set of algorithms selected for standardization, marking a significant milestone in the global effort to secure digital communications against the quantum threat.[13] This proactive approach by NIST reflects a widespread acknowledgment of the quantum risk and offers a structured pathway for the adoption of quantum-resistant cryptography.[10]

This paper aims to provide a comprehensive and comparative analysis of the security margins and practical deployment readiness of the NIST Round 3 finalist algorithms selected for standardization at the conclusion of the third round of this rigorous process.[11] These algorithms are CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+.[9] Understanding the trade-offs between the security assurances offered by these algorithms and their practicality for real-world deployment is crucial for guiding their adoption across various applications and industries.

## 2. Overview of NIST Round 3 Finalist Algorithms

### *2.1. CRYSTALS-Kyber (ML-KEM)*

CRYSTALS-Kyber, also known as ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), is a key encapsulation mechanism based on the mathematical problem of Module Learning With Errors (MLWE) over module lattices.[13] This problem is believed to remain computationally hard even for quantum computers.[15] NIST selected CRYSTALS-Kyber as the primary algorithm for general encryption and key exchange due to its strong security properties and efficient performance.[10] The algorithm offers different parameter sets, namely Kyber-512, Kyber-768, and Kyber-1024, which are designed to meet varying security levels roughly equivalent to AES-128, AES-192, and AES-256, respectively.[13]

### *2.2. CRYSTALS-Dilithium (ML-DSA)*

CRYSTALS-Dilithium, or ML-DSA (Module-Lattice-Based Digital Signature Algorithm), is a digital signature algorithm that derives its security from the difficulty of lattice problems over module lattices.[16] It employs the Fiat-Shamir with Aborts technique to achieve compact and secure signatures.[18] NIST recommends CRYSTALS-Dilithium as the primary digital signature algorithm for most use cases, highlighting its efficiency and relatively straightforward implementation compared to other lattice-based candidates.[10]

### *2.3. FALCON (FN-DSA)*

FALCON, or FN-DSA (FFT NTRU-based Digital Signature Algorithm), is another lattice-based digital signature algorithm that utilizes the "hash-and-sign" paradigm over NTRU lattices.[10] It employs Fast Fourier Sampling for efficient signature generation and verification.[20] NIST selected FALCON for standardization as a complement to CRYSTALS-Dilithium, particularly for applications where smaller signature sizes are advantageous.[9] While FALCON offers compactness and fast verification, its implementation is more complex due to its reliance on floating-point arithmetic.[3]

### *2.4. SPHINCS+ (SLH-DSA)*

SPHINCS+, also known as SLH-DSA (Stateless Hash-Based Digital Signature Algorithm), stands apart as a stateless hash-based signature scheme.[4] Its security is based solely on the well-understood security of cryptographic hash functions, such as SHA-256, SHAKE-256, and Haraka.[22] NIST chose SPHINCS+ primarily as a cryptographic backup option in the event that lattice-based schemes are found to be vulnerable to future attacks.[9] While offering a very conservative security posture, SPHINCS+ generally exhibits larger signature sizes and slower performance compared to the lattice-based finalists.[23]

## 3. Comparative Analysis of Security Margins

### *3.1. CRYSTALS-Kyber*

The security of CRYSTALS-Kyber is rooted in the Module Learning With Errors (MLWE) problem, a lattice-based problem considered hard even for quantum computers.[13] NIST has specified three security levels for Kyber, aiming for security roughly equivalent to AES-128, AES-192, and AES-256 with its Kyber-512, Kyber-768, and Kyber-1024 parameter sets, respectively.[15] For applications demanding high security, the Kyber team recommends using the Kyber-768 parameter set, which is conservatively estimated to provide more than 128 bits of security against known classical and quantum attacks.[15] Despite its strong theoretical foundations, CRYSTALS-Kyber has been subject to security analysis, revealing potential vulnerabilities. Side-channel attacks, such as the recently disclosed KyberSlash attacks, have demonstrated the possibility of recovering secret keys by exploiting timing-based flaws in specific implementations.[24] These attacks highlight the critical importance of secure implementation practices.[13] Furthermore, ongoing research has questioned the concrete security level provided by Kyber's parameter choices, with some analyses suggesting that the actual security margin might be lower than initially claimed, particularly for Kyber-512.[26] The "Core-SVP" metric, often used to estimate the security of lattice-based schemes, has been a subject of debate regarding its accuracy in reflecting real-world attack costs against Kyber.[27]

### *3.2. CRYSTALS-Dilithium*

CRYSTALS-Dilithium offers strong security guarantees against chosen message attacks, relying on the hardness of lattice problems over module lattices.[18] The Dilithium team recommends using the Dilithium3 parameter set, which, according to a conservative analysis, achieves more than 128 bits of security against known classical and quantum attacks.[18] The security of Dilithium is based on the Module Learning With Errors (MLWE), Module Short Integer Solution (MSIS), and SelfTargetMSIS problems.[17] While MLWE and MSIS are well-established and believed to be secure, the quantum hardness of SelfTargetMSIS, a novel problem specific to Dilithium, has been an area of active research. Recent work has provided the first proof of the hardness of SelfTargetMSIS in the Quantum Random Oracle Model (QROM), bolstering confidence in Dilithium's resistance to quantum adversaries.[28] Similar to other post-quantum algorithms, CRYSTALS-Dilithium is susceptible to side-channel attacks. Power analysis attacks have been demonstrated to recover secret key coefficients by targeting polynomial multiplication operations and exploiting randomness leakage during the signing process.[30] These findings underscore the need for robust side-channel countermeasures in practical implementations of Dilithium.[32]

### *3.3. FALCON*

FALCON is designed to provide strong security under chosen message attacks, with its security based on the Short Integer Solution (SIS) problem over NTRU lattices.[19] The algorithm employs a true Gaussian sampler internally, which is intended to guarantee negligible leakage of information about the secret key, even after a very large number of signatures.[19] In terms of classical security, FALCON-512 is considered roughly equivalent to RSA-2048.[19] The security of FALCON has been analyzed within the Quantum Random Oracle Model (QROM), providing a theoretical basis for its quantum resistance.[20] Despite these security features, FALCON has faced scrutiny regarding its formal security proof and susceptibility to side-channel attacks. Initial analyses revealed that the original parameter choices for FALCON did not align with the standard security proofs for the underlying GPV framework.[34] However, recent work has addressed this by proposing minor modifications to FALCON that allow for the first formal security proof of the scheme in the random oracle model, although achieving strong unforgeability remains a challenge for certain parameter sets.[34] Furthermore, FALCON's reliance on floating-point arithmetic in its key generation and signing processes makes it potentially vulnerable to side-channel attacks, particularly those targeting the Gaussian sampler and FFT operations.[3] Electromagnetic analysis attacks have successfully extracted secret signing keys from FALCON implementations, highlighting the need for effective countermeasures.[3]

### *3.4. SPHINCS+*

SPHINCS+ distinguishes itself by relying solely on the security of well-established cryptographic hash functions, such as SHA-256, SHAKE-256, and Haraka, making it a very conservative choice for post-quantum digital signatures.[21] NIST views SPHINCS+ as an extremely conservative option and a valuable backup in case lattice-based schemes encounter unforeseen vulnerabilities.[14] The algorithm offers both simple and robust variants, providing trade-offs between signature size and signing speed.[35] While its reliance on hash functions provides a strong theoretical security foundation against quantum attacks, SPHINCS+ has been found to be vulnerable to fault injection attacks during the signature generation process.[36] These attacks can potentially lead to universal forgeries, emphasizing the importance of implementing appropriate countermeasures, especially in environments where physical access to devices might be possible.[37] Although SPHINCS+ is designed to limit the number of signatures per key pair to 2^64 to maintain security, the security degrades gracefully if this limit is exceeded.[23] The original tight security proof for SPHINCS+ was found to have flaws, but these have since been addressed with a new tight security proof.[38]

## 4. Comparative Analysis of Practical Deployment Readiness

To facilitate a direct comparison of the practical deployment readiness of the NIST Round 3 finalist algorithms, the following tables summarize their performance and resource requirements based on the available research.

**Table 1.** Performance Comparison of NIST PQC Round 3 Finalists.

| Algorithm | Security Level | Operation | Metric | Value (Approx.) | Platform | Source |
|---|---|---|---|---|---|---|
| Kyber-512 | AES-128 | Key Generation | Cycles (Haswell) | 122,684 | Intel i7-4770K | [15] |
| Kyber-512 | AES-128 | Encryption | Cycles (Haswell) | 154,524 | Intel i7-4770K | [15] |
| Kyber-512 | AES-128 | Decryption | Cycles (Haswell) | 187,960 | Intel i7-4770K | [15] |

| | | | | | | |
|---|---|---|---|---|---|---|
| Kyber-768 | AES-192 | Key Generation | Cycles (Haswell) | 199,408 | Intel i7-4770K | [15] |
| Kyber-768 | AES-192 | Encryption | Cycles (Haswell) | 235,260 | Intel i7-4770K | [15] |
| Kyber-768 | AES-192 | Decryption | Cycles (Haswell) | 274,900 | Intel i7-4770K | [15] |
| Dilithium2 | NIST 2 | Key Generation | Cycles (Skylake) | 300,751 | Intel i7-6600U | [18] |
| Dilithium2 | NIST 2 | Signing | Cycles (Skylake) | 1,355,434 | Intel i7-6600U | [18] |
| Dilithium2 | NIST 2 | Verification | Cycles (Skylake) | 327,362 | Intel i7-6600U | [18] |
| Dilithium3 | NIST 3 | Key Generation | Cycles (Skylake) | 544,232 | Intel i7-6600U | [18] |
| Dilithium3 | NIST 3 | Signing | Cycles (Skylake) | 2,348,703 | Intel i7-6600U | [18] |
| Dilithium3 | NIST 3 | Verification | Cycles (Skylake) | 522,267 | Intel i7-6600U | [18] |
| Falcon-512 | NIST 1 | Key Generation | ms | 8.64 | Intel i5-8259U | [19] |
| Falcon-512 | NIST 1 | Signing | Sign/sec | 5948.1 | Intel i5-8259U | [19] |

| | | | | | | |
|---|---|---|---|---|---|---|
| Falcon-512 | NIST 1 | Verification | Verify/sec | 27933.0 | Intel i5-8259U | [19] |
| Falcon-1024 | NIST 5 | Key Generation | ms | 27.45 | Intel i5-8259U | [19] |
| Falcon-1024 | NIST 5 | Signing | Sign/sec | 2913.0 | Intel i5-8259U | [19] |
| Falcon-1024 | NIST 5 | Verification | Verify/sec | 13650.0 | Intel i5-8259U | [19] |
| SPHINCS+-128f-simple | NIST 1 | Signing | Cycles (AVX2) | ~10^8 | Intel | [39] |
| SPHINCS+-128f-simple | NIST 1 | Verification | Cycles (AVX2) | ~10^7 | Intel | [39] |

**Table 2.** Resource Requirements of NIST PQC Round 3 Finalists.

| **Algorithm** | **Security Level** | **Public Key Size (Bytes)** | **Private Key Size (Bytes)** | **Signature/Ciphertext Size (Bytes)** | **RAM Usage (KB)** | **Source** |
|---|---|---|---|---|---|---|
| Kyber-512 | AES-128 | 800 | 1632 | 768 (Ciphertext) | - | [15] |
| Kyber-768 | AES-192 | 1184 | 2400 | 1088 (Ciphertext) | - | [15] |
| Kyber-1024 | AES-256 | 1568 | 3168 | 1568 (Ciphertext) | - | [15] |
| Dilithium2 | NIST 2 | 1312 | 2528 | 2420 (Signature) | ~10 | [18] |
| Dilithium3 | NIST 3 | 1952 | 4000 | 3293 (Signature) | ~61 | [18] |

| | | | | | | |
|---|---|---|---|---|---|---|
| Dilithium5 | NIST 5 | 2592 | 4864 | 4595 (Signature) | ~98 | [18] |
| Falcon-512 | NIST 1 | 897 | ~1998 | 666 (Signature) | ~14 | [19] |
| Falcon-1024 | NIST 5 | 1793 | ~3840 | 1280 (Signature) | ~29 | [19] |
| SPHINCS+-128s-simple | NIST 1 | 32 | 64 | 7856 (Signature) | - | [42] |
| SPHINCS+-128f-simple | NIST 1 | 32 | 64 | 17088 (Signature) | - | [42] |

The practical deployment of these algorithms presents several challenges and considerations. The increased computational demands and larger key/signature sizes of PQC algorithms compared to classical cryptography can impact the performance of existing infrastructure, particularly in resource-constrained environments.[7] Interoperability with legacy systems will be a critical aspect of the transition, likely requiring hybrid cryptographic approaches that combine classical and post-quantum algorithms.[44] While NIST has finalized the first PQC standards, broader adoption hinges on the development of international standards and clear regulatory guidance.[46] Implementing these novel algorithms securely, especially to mitigate side-channel attacks, demands specialized expertise.[7] The transition will also involve costs associated with software and hardware updates, testing, and personnel training.[7]

Each algorithm has its own set of implementation libraries and ongoing pilot projects. CRYSTALS-Kyber has reference and optimized implementations in C, with third-party libraries available in various languages and integration with frameworks like liboqs.[47] It is being explored in pilot projects for secure key exchange.[48] CRYSTALS-Dilithium also has C implementations and third-party libraries in multiple languages, with ongoing efforts in hardware implementation.[50] FALCON has C and Python reference implementations, with integration into liboqs and hardware implementations under development.[19] SPHINCS+ has C implementations for different hash functions and parameter sets, along with third-party libraries and ongoing research into hardware implementations and memory optimization for constrained devices.[52]

## 5. Conclusion and Recommendations

The NIST Round 3 finalist post-quantum cryptographic algorithms represent a significant step towards securing digital systems against the future threat of quantum computers. Each algorithm offers a unique profile in terms of security margins and practical deployment readiness. CRYSTALS-Kyber stands out as an efficient and promising KEM for general encryption, though ongoing security analysis and implementation vulnerabilities warrant careful consideration. CRYSTALS-Dilithium provides a strong and efficient digital signature algorithm suitable for a wide range of applications, with a growing body of security analysis. FALCON offers the advantages of compact signatures and fast verification, making it attractive for bandwidth-constrained scenarios, but its implementation complexity and side-channel vulnerability require attention. SPHINCS+ provides the most conservative security guarantees through its reliance on hash functions, but its larger signature sizes and slower signing speeds might limit its applicability in performance-critical contexts.

For organizations embarking on the transition to post-quantum cryptography, a thorough evaluation of their specific security requirements, performance needs, and resource constraints is essential. A hybrid approach, combining traditional and post-quantum algorithms, may be a prudent strategy during the initial phases of migration to ensure interoperability and maintain a degree of security even if one of the new algorithms faces unforeseen vulnerabilities. Further research is crucial in areas such as enhancing the resistance of these algorithms against advanced side-channel and fault attacks, optimizing their performance across diverse hardware and software platforms, and developing standardized and secure hybrid cryptographic systems. Continued engagement with the cryptographic community and monitoring the ongoing analysis of these algorithms will be vital for ensuring a secure and effective transition to a post-quantum future.

## References

1. "NIST Post-Quantum Competition: The Round 3 Finalists," Cloud Security Alliance, accessed on May 11, 2025. [Online]. Available: https://cloudsecurityalliance.org/articles/nist-post-quantum-competition-and-the-round-3-finalists-are
2. "SPHINCS+ | Post-Quantum Cryptography," DigiCert Insights, accessed on May 11, 2025. [Online]. Available: https://www.digicert.com/insights/post-quantum-cryptography/sphincs
3. "FALCON Down: Breaking FALCON Post-Quantum Signature Scheme through Side-Channel Attacks," in Proc. Fourth PQC Standardization Conference, 2022. [Online]. Available: https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/falcon-down-pqc2022.pdf
4. "Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms," Univ. Colorado Colorado Springs, Colorado Springs, CO, USA, 2021. [Online]. Available: https://cwssp.uccs.edu/sites/g/files/kjihxj2466/files/2021-09/1_Security%20Comparisons%20and%20Performance%20Analyses%20of%20Post-Quantum%20Signature%20Algorithms.pdf
5. "NIST Post-Quantum Cryptography Update," in Proc. PQC Conference, Austin, TX, USA, 2025. [Online]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_PLENARY_1000_Bill-N_Andrew-R_NIST-PQ-Crypto-Update.pdf
6. "PQC Adoption Challenges Outlined by NIST," Quantum Xchange Blog, accessed on May 11, 2025. [Online]. Available: https://quantumxc.com/blog/how-quantum-xchange-solves-for-the-pqc-adoption-challenges-outlined-by-nist/
7. "Challenges of Upgrading to Post-Quantum Cryptography (PQC)," Post-Quantum, accessed on May 11, 2025. [Online]. Available: https://postquantum.com/post-quantum/pqc-challenges/
8. "NIST PQC: The Road Ahead," NIST Computer Security Resource Center, accessed on May 11, 2025. [Online]. Available: https://csrc.nist.gov/csrc/media/Presentations/2025/nist-pqc-the-road-ahead/images-media/rwcpqc-march2025-moody.pdf
9. "NIST Unveils Post-Quantum Cryptography (PQC) Standards," Post-Quantum, accessed on May 11, 2025. [Online]. Available: https://postquantum.com/industry-news/nist-pqc-standards/
10. "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," NIST, Gaithersburg, MD, USA, NIST IR 8413, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf
11. "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," accessed on May 11, 2025.
12. "Post-Quantum Cryptography | Evaluation Criteria," NIST Computer Security Resource Center, accessed on May 11, 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)

13. "Decoding the CRYSTALS-Kyber attack using artificial intelligence: Examination and strategies for resilience," in Proc. CEUR Workshop, 2025. [Online]. Available: https://ceur-ws.org/Vol-3826/short26.pdf
14. "Announcement: The End of the 3rd Round - the First PQC Algorithms to be Standardized," Google Groups, accessed on May 11, 2025. [Online]. Available: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/G0DoD7lkGPk/m/f3Hl0sh3AgAJ
15. "Kyber," CRYSTALS, accessed on May 11, 2025. [Online]. Available: https://pq-crystals.org/kyber/
16. "Efficiency Analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for Digital Signatures in Various Environments," ResearchGate, accessed on May 11, 2025. [Online]. Available: https://www.researchgate.net/publication/387483277_Efficiency_Analysis_of_NIST-Standardized_Post-Quantum_Cryptographic_Algorithms_for_Digital_Signatures_in_Various_Environments
17. "Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model," NIST, Gaithersburg, MD, USA, 2025. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=956883
18. "Dilithium," CRYSTALS, accessed on May 11, 2025. [Online]. Available: https://pq-crystals.org/dilithium/
19. "Falcon," Falcon Project, accessed on May 11, 2025. [Online]. Available: https://falcon-sign.info/
20. "Falcon (signature scheme)," Wikipedia, accessed on May 11, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Falcon_(signature_scheme)
21. "SPHINCS: practical stateless hash-based signatures," in Proc. Workshop on Cybersecurity in a Post-Quantum World, 2015. [Online]. Available: https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/papers/session5-bernstein-paper.pdf
22. "SPHINCS+ Introduction," di-mgt.com.au, accessed on May 11, 2025. [Online]. Available: https://www.di-mgt.com.au/pqc-07-sphincsplus-intro.html
23. "A note on SPHINCS+ parameter sets," in Proc. Fifth PQC Standardization Conference, 2024. [Online]. Available: https://csrc.nist.gov/csrc/media/Events/2024/fifth-pqc-standardization-conference/documents/papers/a-note-on-sphincs-plus-parameter-sets.pdf
24. "Root Causes 354: CyberSlash Attack Against CRYSTALS-Kyber," Sectigo Official, accessed on May 11, 2025. [Online]. Available: https://www.sectigo.com/resource-library/root-causes-354-cyberslash-attack-against-crystals-kyber
25. "How to Avoid KyberSlash Attacks and Others," QuantumXC Blog, accessed on May 11, 2025. [Online]. Available: https://quantumxc.com/blog/kyberslash-attacks-crystals-kyber-flaws/
26. "Overview and Discussion of Attacks on CRYSTALS-Kyber," Cryptology ePrint Archive, 2023. [Online]. Available: https://eprint.iacr.org/2023/1952.pdf
27. "2023.11.25: Another way to botch the security analysis of Kyber-512," cr.yp.to Blog, accessed on May 11, 2025. [Online]. Available: https://blog.cr.yp.to/20231125-kyber.html
28. "Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model," arXiv preprint arXiv:2312.16619, 2023. [Online]. Available: https://arxiv.org/abs/2312.16619
29. "Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model," Cryptology ePrint Archive, 2023. [Online]. Available: https://eprint.iacr.org/2023/1968
30. "A Novel Power Analysis Attack against CRYSTALS-Dilithium Implementation," Cryptology ePrint Archive, 2024. [Online]. Available: https://eprint.iacr.org/2024/111
31. "Practical Public Template Attack Attacks on CRYSTALS-Dilithium With Randomness Leakages," IEEE Signal Processing Society, accessed on May 11, 2025. [Online]. Available: https://signalprocessingsociety.org/publications-resources/ieee-transactions-information-forensics-and-security/practical-public
32. "An Efficient Non-Profiled Side-Channel Attack on the CRYSTALS-Dilithium Post-Quantum Signature," ECE Research, North Carolina State Univ., Raleigh, NC, USA, 2025. [Online]. Available: https://research.ece.ncsu.edu/wp-content/uploads/sites/8/Dilithium_SCA_cameraready.pdf
33. "Falcon - A Post-Quantum Signature Scheme," PQShield, accessed on May 11, 2025. [Online]. Available: https://pqshield.com/falcon-a-post-quantum-signature-scheme/
34. "A Closer Look at Falcon," Cryptology ePrint Archive, 2024. [Online]. Available: https://eprint.iacr.org/2024/1769.pdf

35. "SPHINCS+," SPHINCS+, accessed on May 11, 2025. [Online]. Available: https://sphincs.org/
36. "eShard Expert Review no. 3 - Fault Attacks on SPHINCS+," PQShield, accessed on May 11, 2025. [Online]. Available: https://pqshield.com/eshard-expert-review-no-3-fault-attacks-on-sphincs/
37. "CHES 2023 blog: Protecting your future credit card! (Fault attacks on SPHINCS+)," COSIC - KU Leuven, accessed on May 11, 2025. [Online]. Available: https://www.esat.kuleuven.be/cosic/blog/ches-2023-blog-protecting-your-future-credit-card-fault-attacks-on-sphincs/
38. "A Tight Security Proof for SPHINCS+, Formally Verified," Cryptology ePrint Archive, 2024. [Online]. Available: https://eprint.iacr.org/2024/910.pdf
39. "Optimization for SPHINCS+ using Intel® Secure Hash Algorithm Extensions," in Proc. Fourth PQC Standardization Conference, 2022. [Online]. Available: https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/optimizatin-for-sphinc-plus-using-intel-pqc2022.pdf
40. "Dilithium for Memory Constrained Devices," Cryptology ePrint Archive, 2022. [Online]. Available: https://eprint.iacr.org/2022/323.pdf
41. "Benchmarking and Analysing the NIST PQC Lattice-Based Signature Schemes Standards on the ARM Cortex M7," Cryptology ePrint Archive, 2022. [Online]. Available: https://eprint.iacr.org/2022/405.pdf
42. Argyle-Software, "sphincsplus," GitHub repository, accessed on May 11, 2025. [Online]. Available: https://github.com/Argyle-Software/sphincsplus/
43. "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms," arXiv preprint arXiv:2503.12952, 2025. [Online]. Available: https://arxiv.org/html/2503.12952v1
44. "NIST Outlines Strategies for Crypto Agility as PQC Migration Stalls, Available for Public Comment," The Quantum Insider, accessed on May 11, 2025. [Online]. Available: https://thequantuminsider.com/2025/03/07/nist-outlines-strategies-for-crypto-agility-as-pqc-migration-stalls-available-for-public-comment/
45. "Next steps in preparing for post-quantum cryptography," NCSC.GOV.UK, accessed on May 11, 2025. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
46. "Post-Quantum Cryptography PQC Challenges," Post-Quantum, accessed on May 11, 2025. [Online]. Available: https://postquantum.com/post-quantum/post-quantum-pqc-challenges/
47. "Kyber – Software," CRYSTALS, accessed on May 11, 2025. [Online]. Available: https://pq-crystals.org/kyber/software.shtml
48. "WISeKey and OISTE.ORG Generate and Launch a Post-Quantum Cryptography Root Key to Defend Against Quantum Cyber Threats," GlobeNewswire, accessed on May 11, 2025. [Online]. Available: https://www.globenewswire.com/news-release/2025/05/07/3075725/0/en/WISeKey-and-OISTE-ORG-Generate-and-Launch-a-Post-Quantum-Cryptography-Root-Key-to-Defend-Against-Quantum-Cyber-Threats.html
49. "crystals-kyber," GitHub Topics, accessed on May 11, 2025. [Online]. Available: https://github.com/topics/crystals-kyber?o=desc&s=updated
50. "Dilithium – Software," CRYSTALS, accessed on May 11, 2025. [Online]. Available: https://pq-crystals.org/dilithium/software.shtml
51. "Falcon," TQ42 Cryptography Library, GitHub Pages, accessed on May 11, 2025. [Online]. Available: https://terra-quantum-public.github.io/tq42-pqc-oss/post_quantum_algs/digital_signature/falcon.html
52. sphincs, "sphincsplus," GitHub repository, accessed on May 11, 2025. [Online]. Available: https://github.com/sphincs/sphincsplus
53. "Streaming SPHINCS+ for Embedded Devices using the Example of TPMs," Cryptology ePrint Archive, 2021. [Online]. Available: https://eprint.iacr.org/2021/1072.pdf
54. "Overview of NIST Round 3 Post-Quantum cryptography Candidates," PQSecure Technologies, 2020. [Online]. Available: https://www.pqsecurity.com/wp-content/uploads/2020/07/Round-3.pdf
55. "KyberSlash attacks put quantum encryption projects at risk," Bleeping Computer, accessed on May 11, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/kyberslash-attacks-put-quantum-encryption-projects-at-risk/

56. "An Improved Two-Step Attack on CRYSTALS-Kyber," arXiv preprint arXiv:2407.06942, 2024. [Online]. Available: https://arxiv.org/html/2407.06942v1
57. "SPHINCS+ - Step by Step," er4hn Blog, accessed on May 11, 2025. [Online]. Available: https://er4hn.info/blog/2023.12.16-sphincs_plus-step-by-step/
58. "SPHINCS+: stateless hash-based digital signature," Telsy, accessed on May 11, 2025. [Online]. Available: https://www.telsy.com/en/sphincs-stateless-hash-based-digital-signature/
59. "ML-DSA | Post-Quantum Cryptography," DigiCert Insights, accessed on May 11, 2025. [Online]. Available: https://www.digicert.com/insights/post-quantum-cryptography/dilithium
60. "CRYSTALS-Dilithium," CRYSTALS, accessed on May 11, 2025. [Online]. Available: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf
61. "SHIFT SNARE: Uncovering Secret Keys in FALCON via Single-Trace Analysis," arXiv preprint arXiv:2504.00320, 2025. [Online]. Available: https://arxiv.org/pdf/2504.00320
62. "Post-Quantum Cryptography," NIST Computer Security Resource Center, accessed on May 11, 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
63. "CRYSTALS – Dilithium: Digital Signatures from Module Lattices," Peter Schwabe, 2017. [Online]. Available: https://cryptojedi.org/papers/dilithium-20170627.pdf
64. "SPHINCS+ becomes a standard in post quantum technology – SDU Professor plays key role," SDU, accessed on May 11, 2025. [Online]. Available: https://www.sdu.dk/en/om-sdu/institutter-centre/imada_matematik_og_datalogi/nyt_fra_imada/sphincs
65. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," NIST, accessed on May 11, 2025. [Online]. Available: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
66. "CRYSTALS-Kyber Algorithm Specifications And Supporting Documentation," CRYSTALS, accessed on May 11, 2025. [Online]. Available: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210131.pdf
67. "A look at the latest post-quantum signature standardization candidates," The Cloudflare Blog, accessed on May 11, 2025. [Online]. Available: https://blog.cloudflare.com/another-look-at-pq-signatures/
68. "Quantum Computing Threat: The First NIST Post-Quantum Cryptographic Standards," PQShield, 2022. [Online]. Available: https://pqshield.com/wp-content/uploads/2021/02/PQShield-Quantum-Threat-2-The-First-NIST-Post-Quantum-Cryptographic-Standards-July-2022.pdf
69. "SPHINCS+," SPHINCS+, accessed on May 11, 2025. [Online]. Available: https://sphincs.org/data/sphincs+-paper.pdf

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.