Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

6th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS

(PKIA 2025)

SEPTEMBER 3-4th, 2025

Post-Quantum Hybrid Digital Signatures: Bridging Classical and Quantum-Resistant

Paper ID:
76

Cryptography

Mr. Jitendra Kumar, Dr. Balaji Rajendran(CDAC Bangalore), Mr. Aashish Banati, Dr. K K Soundra Pandian(Office of CCA), Dr. S D Sudarsan(C-DAC Bangalore)

Background and Motivation

- Quantum Computing threatens traditional cryptographic systems such as RSA and Elliptic Curve(EC) based digital signature schemes
  - The vulnerability exists because the underlying mathematical approach, such as prime integer factorization used in RSA and discrete logarithmic problems used in EC-based cryptography, can be efficiently solved using quantum algorithms
- Post-quantum cryptography (PQC) presents promising quantum-resistant alternatives, but questions about performance, implementation readiness, and trust remain
- The paper will analyze hybrid signature schemes, design their implementation strategies, and compare them
- The primary focus of this study is to indicate that hybrid signatures are a practical and secure transitional solution for digital trust during the impending quantum era

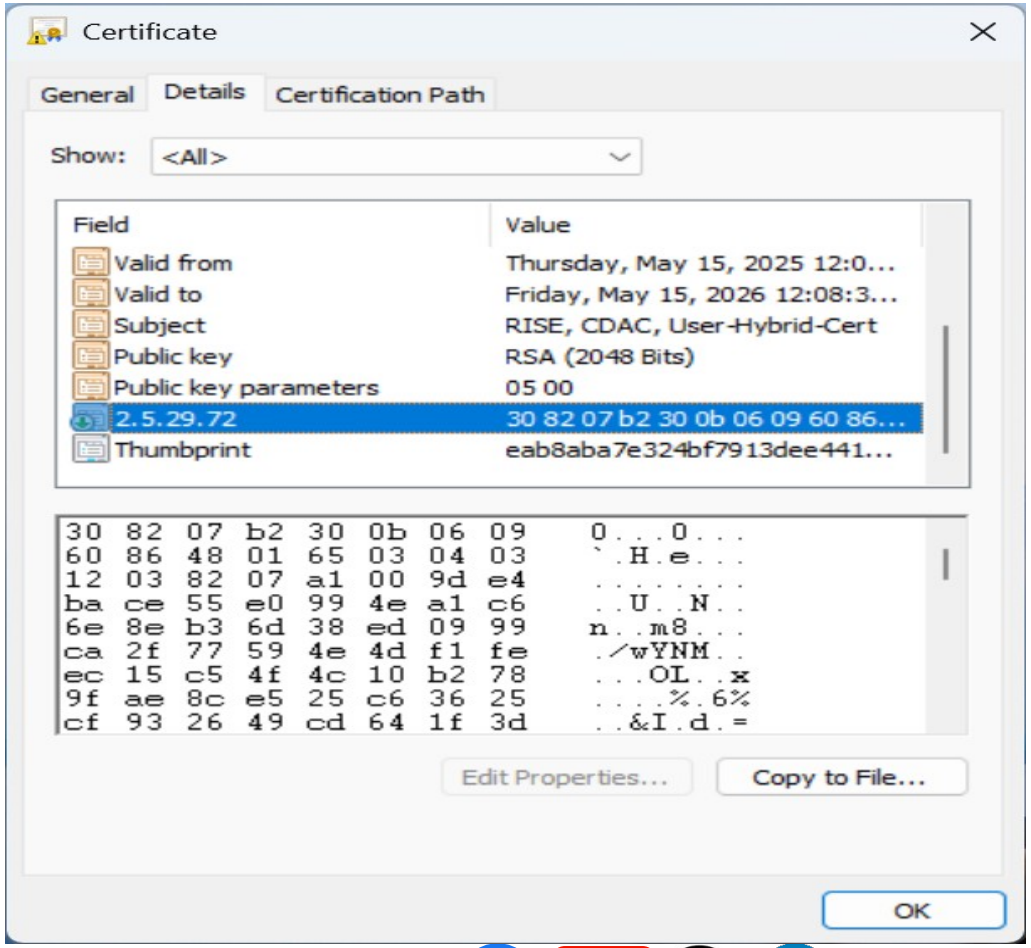
Related Study

- RFC 9794 [1] defines the new terminologies for Post-Quantum Traditional Hybrid Schemes, as the algorithms and standards are still evolving and have not fully matured.
- Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klausner, Scott Fluhrer in the IETF draft [3] have proposed Composite ML-DSA for use in X.509 Public Key Infrastructure and CMS

Hybrid Digital Certificate

- The hybrid digital certificate must include dual public keys, such as classical and post-quantum-based keys.
- The popular digital certificate format, X.509 v3, supports only one public key; hence, the standard should be updated to ensure backward compatibility and support for dual certificates.
- An approach where the hybrid certificate can store ML-DSA public key in the extension "subjectAltPublicKeyInfo"- The support is provided in the Latest Bouncy Castle Library [13]
  - https://www.bouncycastle.org/download/bouncy-castle-java/#latest
  - bcprov-jdk18on-1.81.jar

Hybrid Digital Certificate Example



Hybrid Digital Signature Scheme

- **Parallel Hybrid Signatures: Both signatures are verified independently, but must both validate**
  - **Backward compatibility with legacy systems**
  - **Forward security against future quantum threat**
- **Concatenated Hybrid Signature: Both signatures are generated independently and concatenated**
- **Nested (or Combined) Signing: One signature authenticates the other**
- **Composite Signature: A Composite Hybrid Digital Signature is [3] a combination of multiple cryptographic signature algorithms into a single composite signature structure**
  - **The composite digital signature can utilize the composite keys as a single key for the cryptographic operation**
  - **The scheme can utilize the existing fields in protocols such as PKCS#10 [9], CMP [10], X.509 [11], and CMS [12]**

Symbols Used

M= Original Message

PRrsa=Traditional RSA Private Key

PRml−dsa=Post Quantum ML-DSA Private Key

PUrsa=Traditional RSA Public Key

PUml−dsa=Post Quantum ML-DSA Public Key

H1 = Traditional SHA Hashing Function

H2 = Post Quantum ML-DSA Hashing Function

E1= Traditional Encryption Function

E2= Post Quantum ML-DSA Encryption Function

D1= Traditional RSA Decryption Function

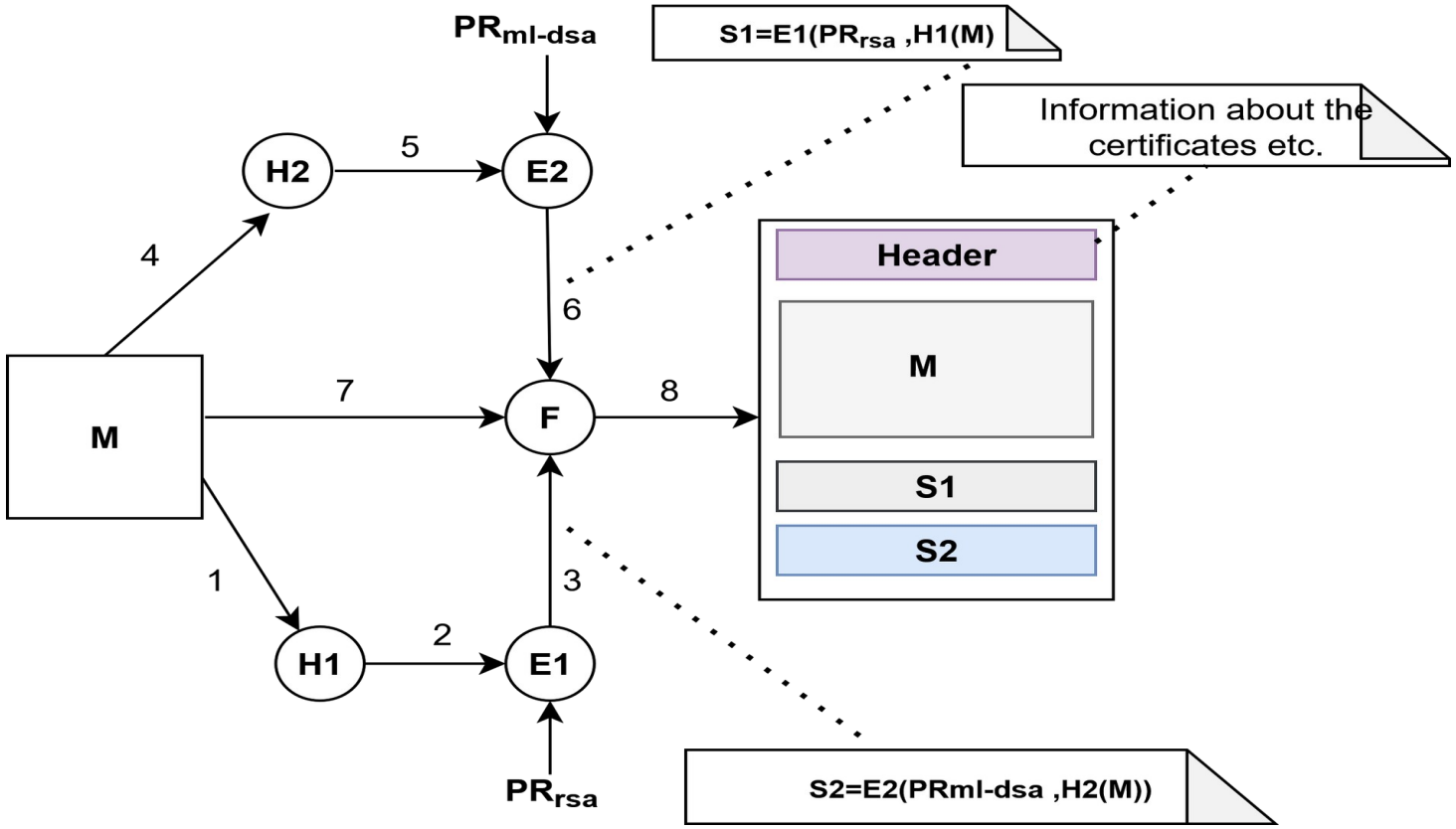
D2= Post Quantum ML-DSA Decryption Function

S1 = Traditional RSA-based Signature

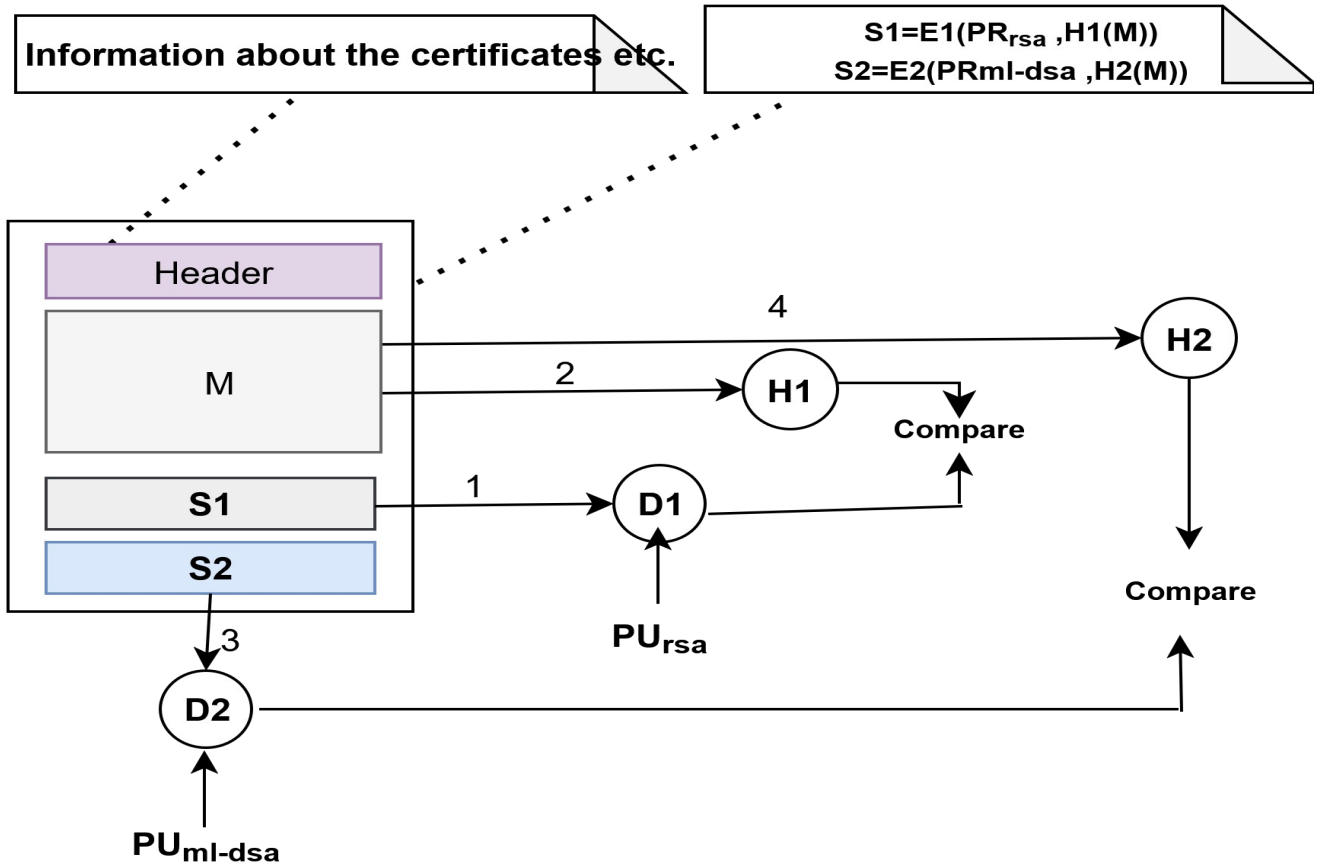
S2= Post Quantum ML-DSA based Signature

F= A Cryptographic Message Syntax (CMS) format function

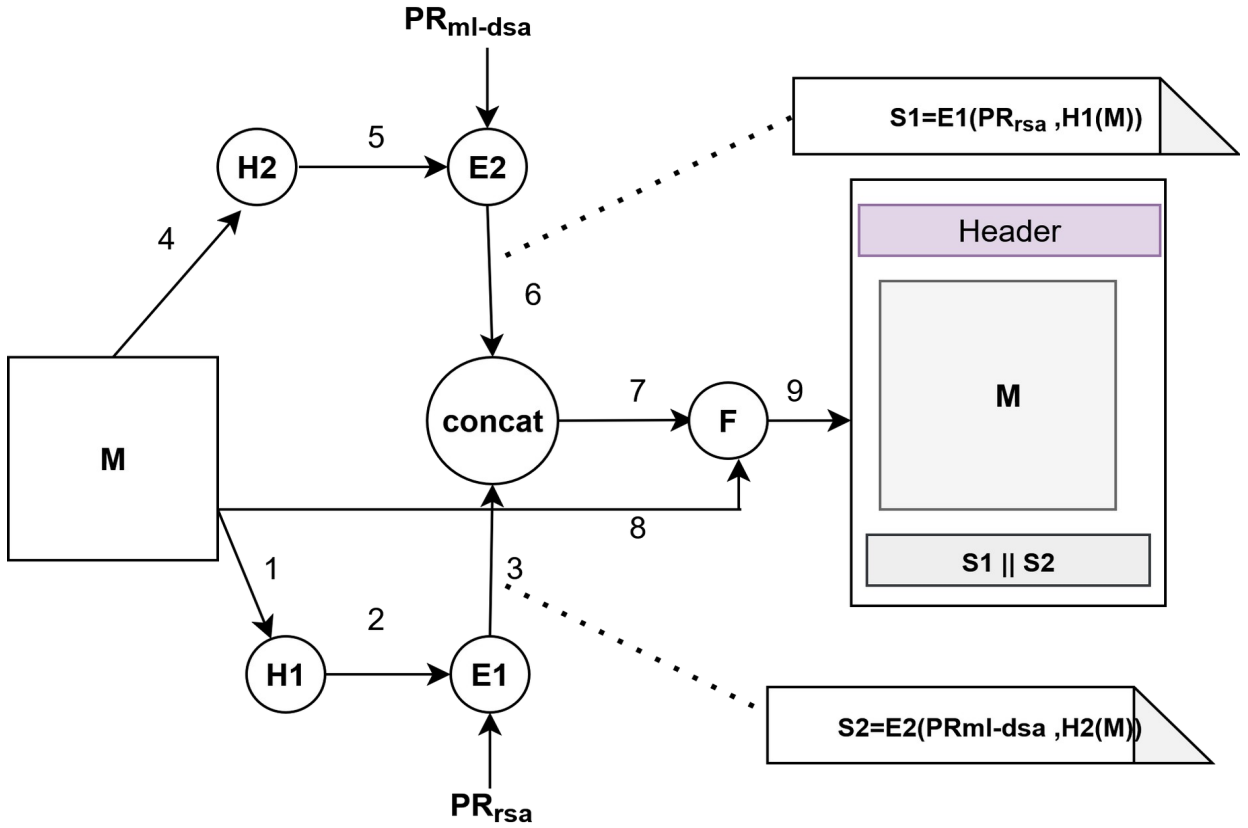
Parallel Hybrid Signature Creation



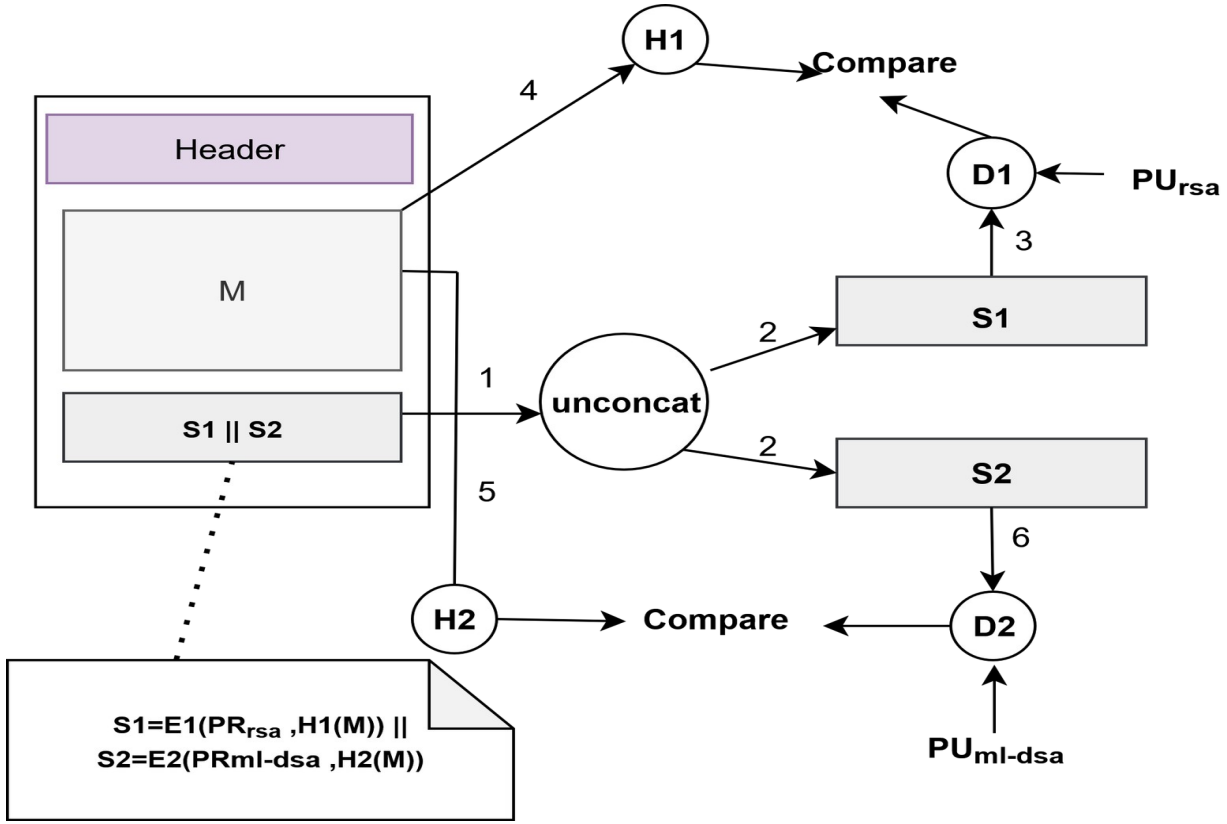
Parallel Hybrid Signature Verification



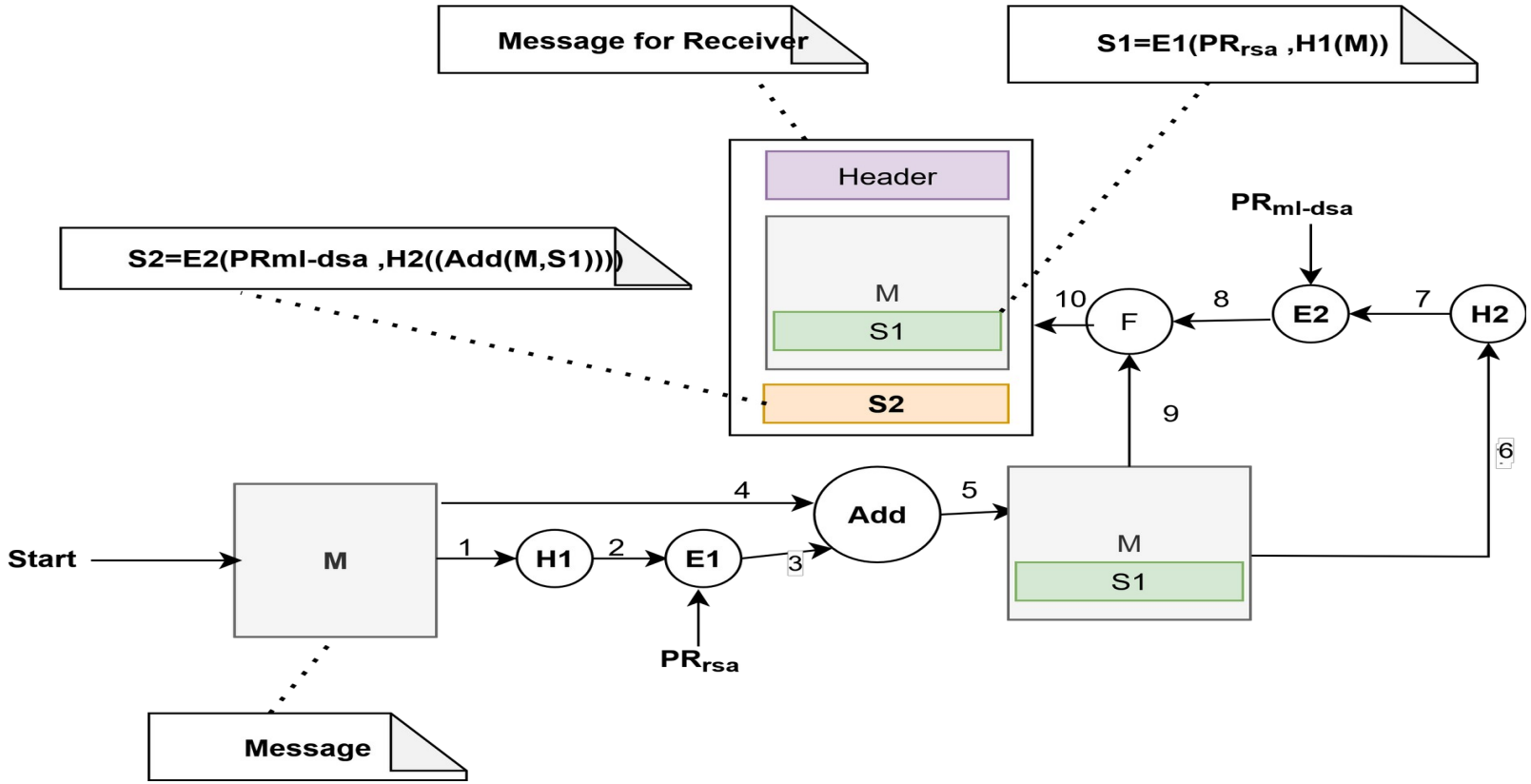
Concatenated Hybrid Signature Creation



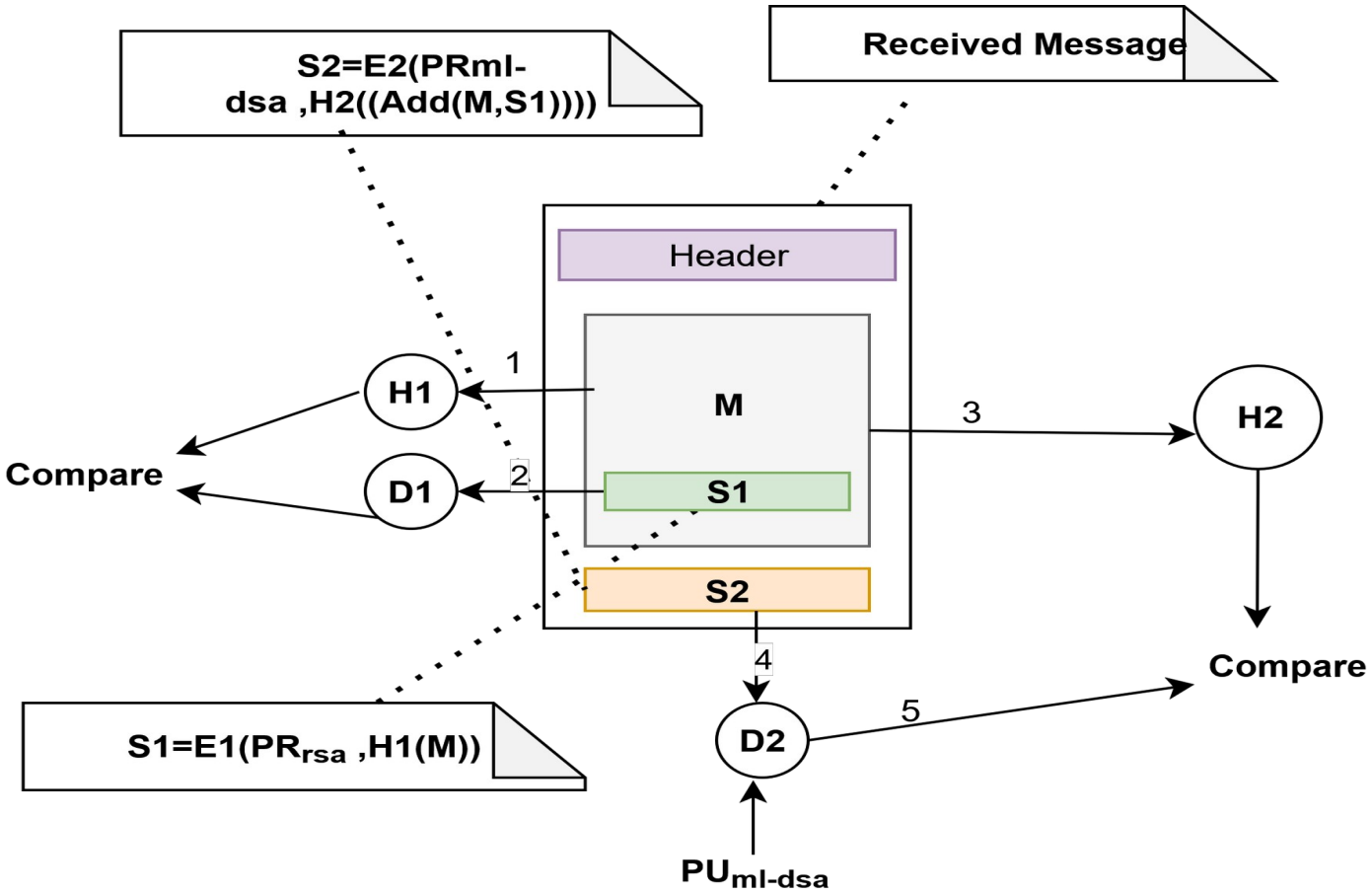
Concatenated Hybrid Signature Verification



Nested Hybrid Signature Creation



Nested Hybrid Signature Verification



PQC Key and Signature Sizes

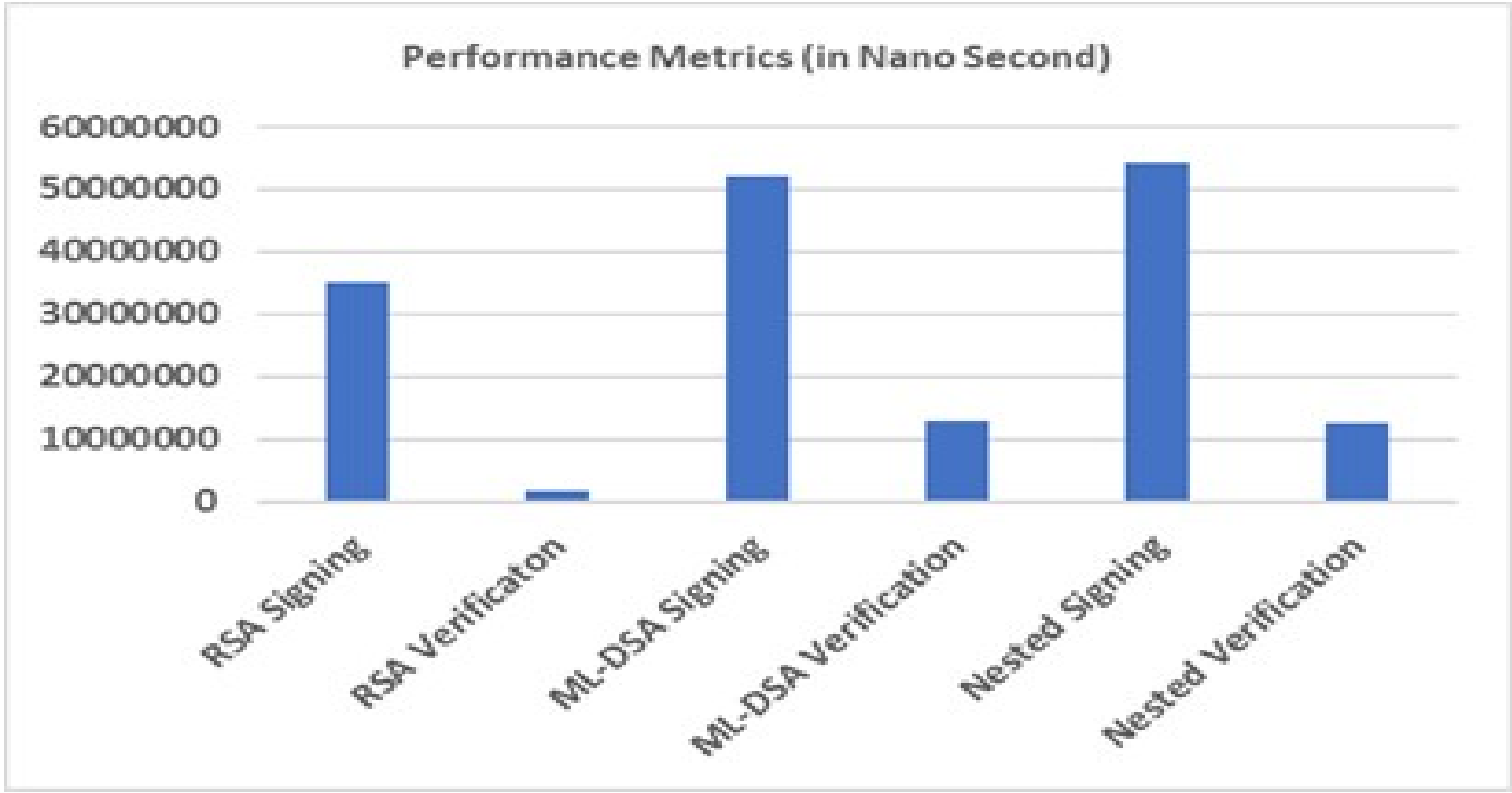
Scheme	Public Key (bytes)	Private Key (bytes)	Signature (bytes)
RSA-2048	256	256	256
ECDSA-P256	**64**	**32**	**256**
ML-DSA-44 (Dilithium2)	**1312**	**2528**	**2420**
ML-DSA-65 (Dilithium3)	**1952**	**4000**	**3293**
ML-DSA-87 (Dilithium5)	**2592**	**4864**	**4595**
FN-DSA-512 (Falcon512)	**897**	**7553**	**666**
FN-DSA-1024 (Falcon1024)	**1793**	**13953**	**1280**

Courtesy: NIST

Performance metrics

Algorithm	Execution Time (In Nano Second)
RSA Signing	35191340
RSA Verification	1773140
ML-DSA Signing	52021300
ML-DSA Verification	12835060
Nested Signing	54368440
Nested Verification	12700860

Performance Metrics



Conclusion

- **The hybrid digital signature can be a practical and transitional solution, combining the strengths of traditional and post-quantum algorithms to ensure long-term security and interoperability.**
- **The paper will present hybrid signature schemes, design their implementation strategies, and compare their performance**
- **The hybrid schemes introduce trade-offs regarding computational efficiency, signature size, and complexity.**
  - **Hence, these aspects must be carefully balanced during design and implementation.**

References

1. Flo D, Michael P, Britta Hale, ”Terminology for Post-Quantum Traditional Hybrid Schemes,” Last Accessed on August. 5, 2025. [Online]. Available: https://datatracker.ietf.org/doc/rfc9794/
2. Sharon Boeyen, Stefan Santesson, Tim Polk, Russ Housley, Stephen Farrell, David Cooper, ”Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280
3. Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, Scott Fluhrer, "Composite ML-DSA for use in X.509 Public Key Infrastructure and CMS," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/
4. Jake Massimo, Panos Kampanakis, Sean Turner, Bas Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/
5. R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

References

6. National Institute of Standards and Technology, “Digital Signature Standard (DSS),” FIPS PUB 186-4, Jul. 2013.
7. L. Ducas et al., “CRYSTALS-Dilithium: Digital Signatures from Module Lattices,” NIST PQC Round 3 Submissions, 2020.
8. Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, "Composite ML-DSA for use in Internet PKI," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ounsworth-pq-composite-sigs-13
9. Magnus Nyström, Burt Kaliski, "PKCS \#10: Certification Request Syntax Specification Version 1.7," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2986
10. Tero Mononen, Tomi Kause, Stephen Farrell, Dr. Carlisle Adams," "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4210

References

11. Sharon Boeyen, Stefan Santesson, Tim Polk, Russ Housley, Stephen Farrell, David Cooper," Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5280

12. Russ Housley," Cryptographic Message Syntax (CMS)," Last Accessed on June. 6, 2025. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5652

13. Bouncy Castle for Java, Last Accessed on August. 20, 2025. [Online]. Available: https://www.bouncycastle.org/download/bouncy-castle-java/

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

THANK YOU

C-DAC

https://
pkiindia.in

Social Media
/pkiindia

IEEE BANGALORE SECTION