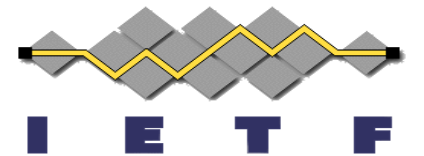


Signature Authentication in the IKEv2 using PQC

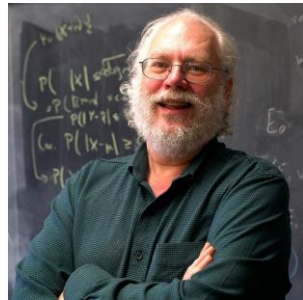
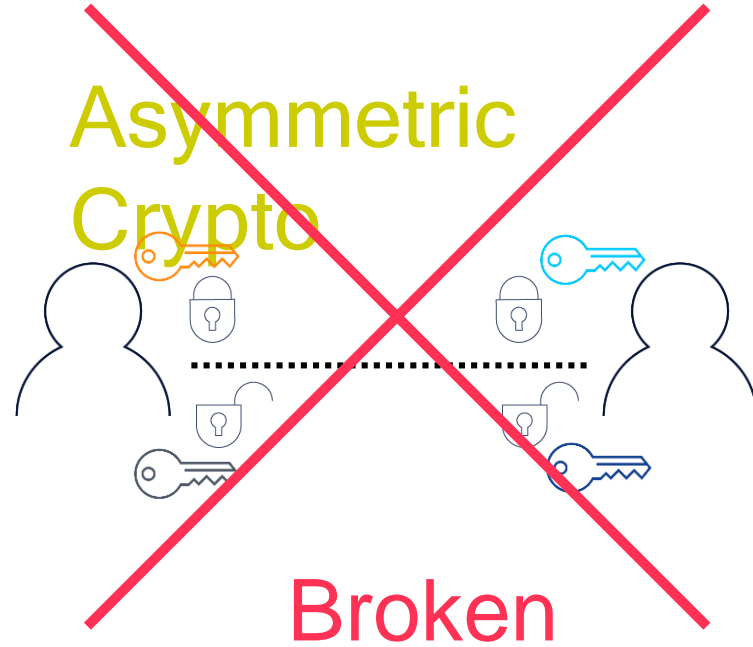
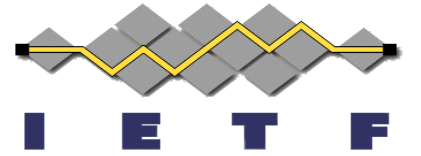
[draft-reddy-ipsecme-ikev2-pqc-auth](#)

Tirumaleswar Reddy, **Valery Smyslov**, Scott Fluhrer

IETF 120, Vancouver

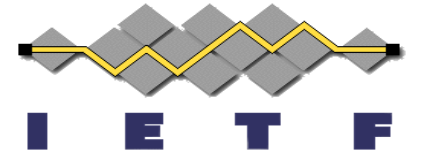


Impact of Quantum Computers in Cryptography



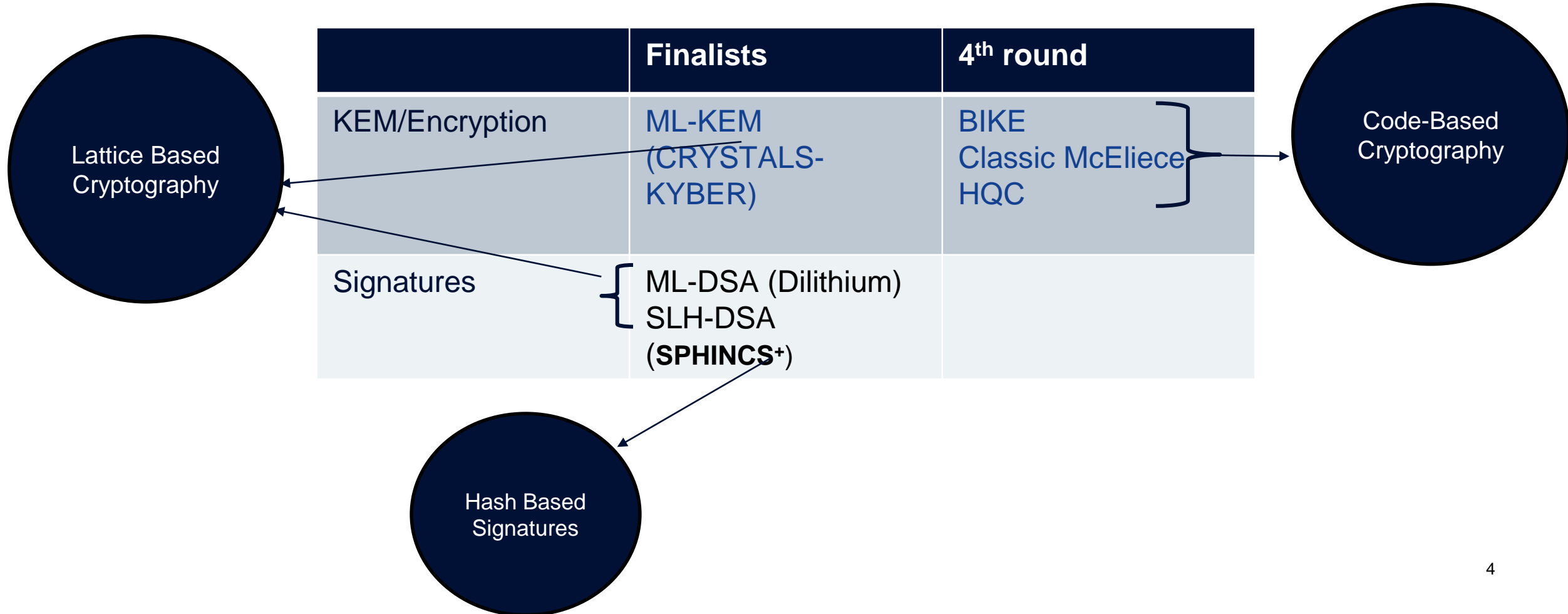
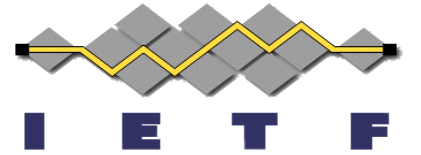
Peter Shor
Algorithm for prime
factorization of large
integers

PQC Auth in IKEv2

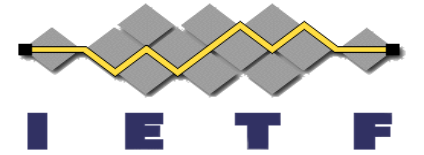


- IKEv2 relies on traditional algorithms vulnerable to quantum attacks, like RSA and ECDSA.
- Introduce PQC signatures for authentication in IKEv2.
 - Enhance security against potential future cryptographically relevant quantum computer attack that could break current asymmetric cryptographic algorithms.

NIST Candidates Selected for Standardization

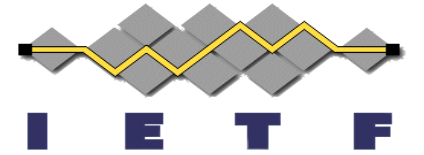


ML-DSA in IKEv2



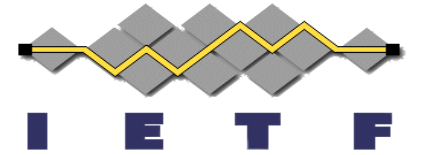
- ML-DSA in X.509 certificates is defined in <https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/>
- ML-DSA algorithm in IKEv2 at three PQ security levels:
 - ML-DSA-44:
 - PQ Security Level: 2
 - AES/SHA Hardness: Comparable to SHA-256/SHA3-256 (collision search)
 - ML-DSA-65 :
 - PQ Security Level: 3
 - AES/SHA Hardness: Comparable to AES-192 (exhaustive key recovery)
 - ML-DSA-87 :
 - PQ Security Level: 5
 - AES/SHA Hardness: Comparable to AES-256 (exhaustive key recovery)
- ML-DSA can be used in both deterministic and randomized signing mode.

SLH-DSA in IKEv2



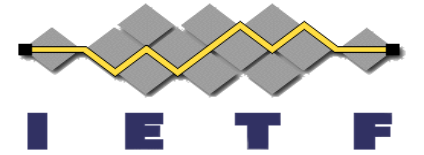
- SLH-DSA in X.509 certificates is defined in <https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-sphincs-plus/>
- SLH-DSA algorithm in IKEv2 at three security levels.
 - It includes the small (S) or fast (F) versions of the algorithm
 - Use of either SHA-256 or SHAKE256 as the hash function.
- SLH-DSA algorithm in IKEv2 at three security levels:
 - SLH-DSA-128{S,F}-{SHA2,SHAKE}
 - SLH-DSA-192{S,F}-{SHA2,SHAKE}
 - SLH-DSA-256{S,F}-{SHA2,SHAKE}
- SLH-DSA can be used in both deterministic and randomized signing mode.

Signaling support for PQC signatures



- The initiator could indicate in the Certificate Request payload that it trusts a CA certificate signed by an ML-DSA or SLH-DSA key.
- Leverage ipsecme-ikev2-auth-announce that allows peers to announce their supported authentication methods.

Next Steps



- Comments and suggestions are welcome
- Consider for WG adoption