PQC Recommendations for Internet Applications

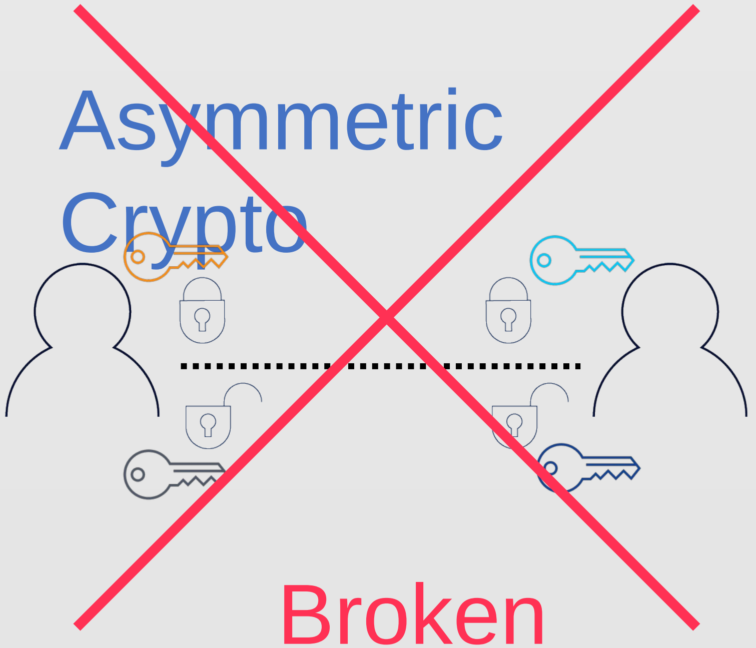
https://datatracker.ietf.org/doc/draft-reddy-uta-pqc-app/

IETF 119

March 2023

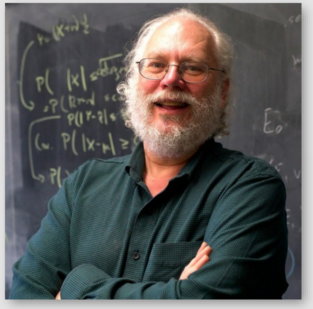
K Tirumaleswar Reddy (Nokia)

Impact of Quantum Computers in Cryptography



Asymmetric Crypto

Broken

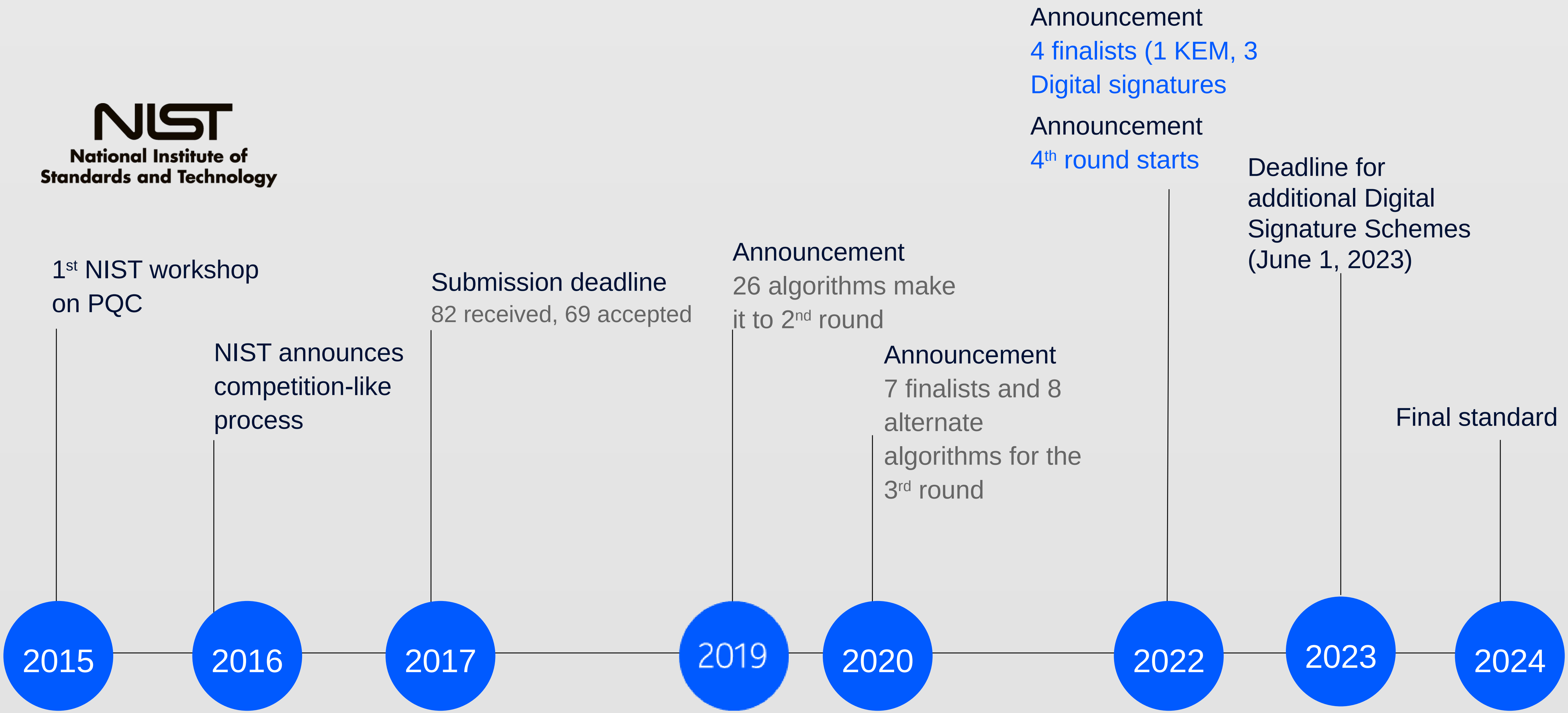


Peter Shor

Algorithm for prime factorization of large integers

PQC standardization timeline

NIST
National Institute of
Standards and Technology



2015

1st NIST workshop on PQC

2016

NIST announces competition-like process

2017

Submission deadline
82 received, 69 accepted

2019

Announcement
26 algorithms make it to 2nd round

2020

Announcement
7 finalists and 8 alternate algorithms for the 3rd round

2022

Announcement
4 finalists (1 KEM, 3 Digital signatures

Announcement
4th round starts

2023

Deadline for additional Digital Signature Schemes (June 1, 2023)

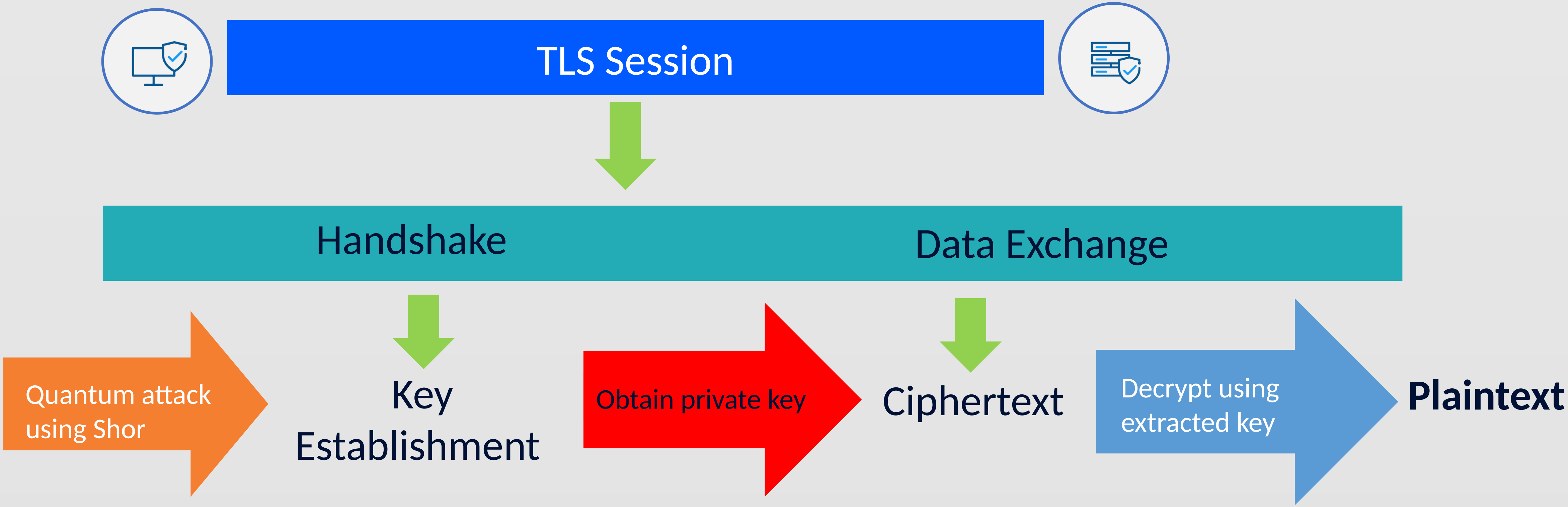
2024

Final standard

Scope of the draft

- This document discusses Quantum-Ready usage profiles for applications using TLS to defend against passive and on-path attacks employing CRQCs.

Data Confidentiality



TLS Session

Handshake

Data Exchange

Quantum attack using Shor

Key Establishment

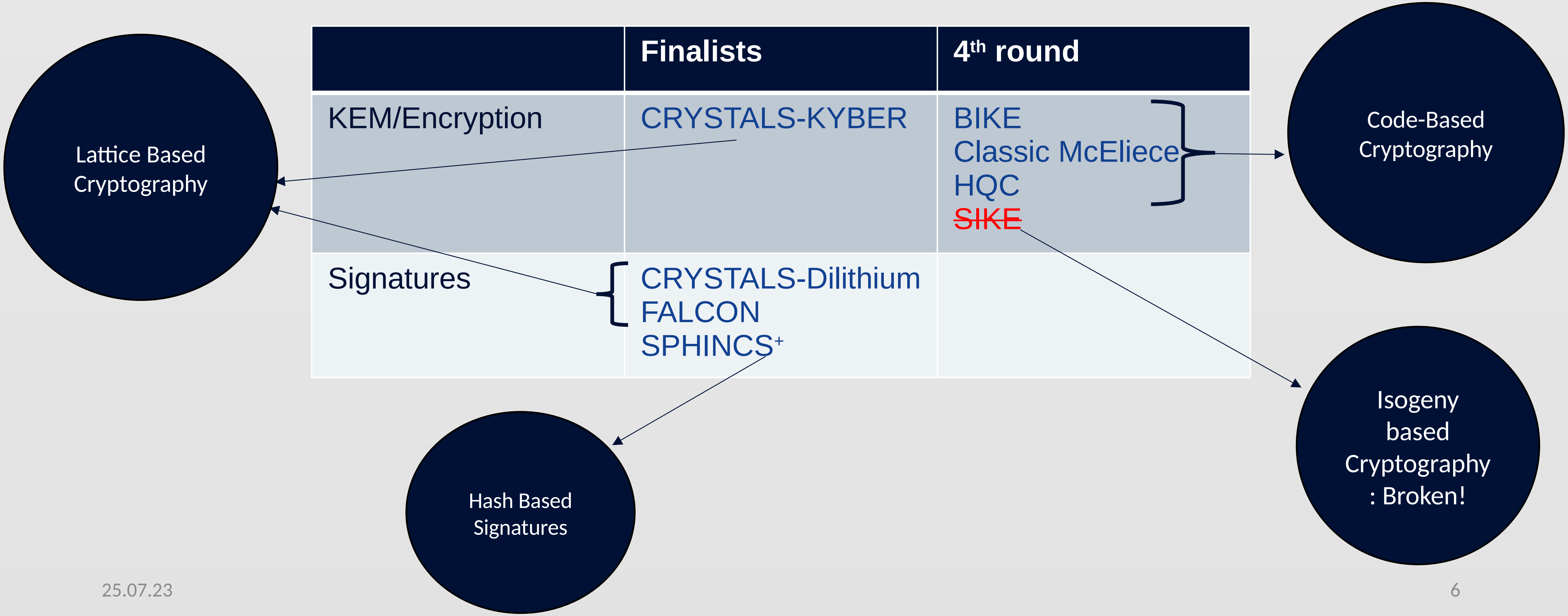
Obtain private key

Ciphertext

Decrypt using extracted key

Plaintext

T Candidates Selected for Standardization/4th Round Candidates



	Finalists	4th round
KEM/Encryption	CRYSTALS-KYBER	BIKE Classic McEliece HQC ~~SIKE~~
Signatures	CRYSTALS-Dilithium FALCON SPHINCS^{+}	

Lattice Based Cryptography
Code-Based Cryptography
Isogeny based Cryptography : Broken!
Hash Based Signatures

Hybrid key exchange in TLS 1.3

- Hybrid key exchange in TLS 1.3 https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - the client’s key_exchange contains two component public keys, one for a post-quantum algorithm and one for a traditional algorithm.
  - the server key_exchange value contains concatenation of the ct output of the PQC KEM Encap and the ECDH ephemeral key share
  - It provides hybrid confidentiality but does not address hybrid authentication or PQ authentication
    - PQ/T hybrid confidentiality: Confidentiality is achieved by a PQ/T hybrid as long as at least one component algorithm that aims to provide this property remains secure.
  - Fairly mature
  - Clients cache server’s preference for key exchange algorithms.
  - Early deployments showing reasonable performance:
    - ✓ Chrome experiments, Cloudflare, Open Quantum Safe and WolfSSL

Hybrid Exchange support and multiple round trips

- Sending Both Traditional and Hybrid Key Exchange Algorithms
  - Size of the hybrid key exchange algorithm key share may exceed the MTU
  - Traditional public key and PQ-KEM ciphertext in ServerHello may exceed the MTU
- Indicate support for Hybrid Key Exchange
  - the client may initially indicate support for hybrid key exchange and send a traditional key exchange algorithm key share in the first ClientHello message
  - HelloRetryRequest to request a hybrid key exchange algorithm key share from the client.
- Avoid duplication of PQ-KEM public key shares in the ClientHello
- [I-D.davidben-tls-key-share-prediction] defines a mechanism for servers to communicate key share preferences in DNS responses. TLS clients can use this information to reduce TLS handshake round-trips.

Authentication

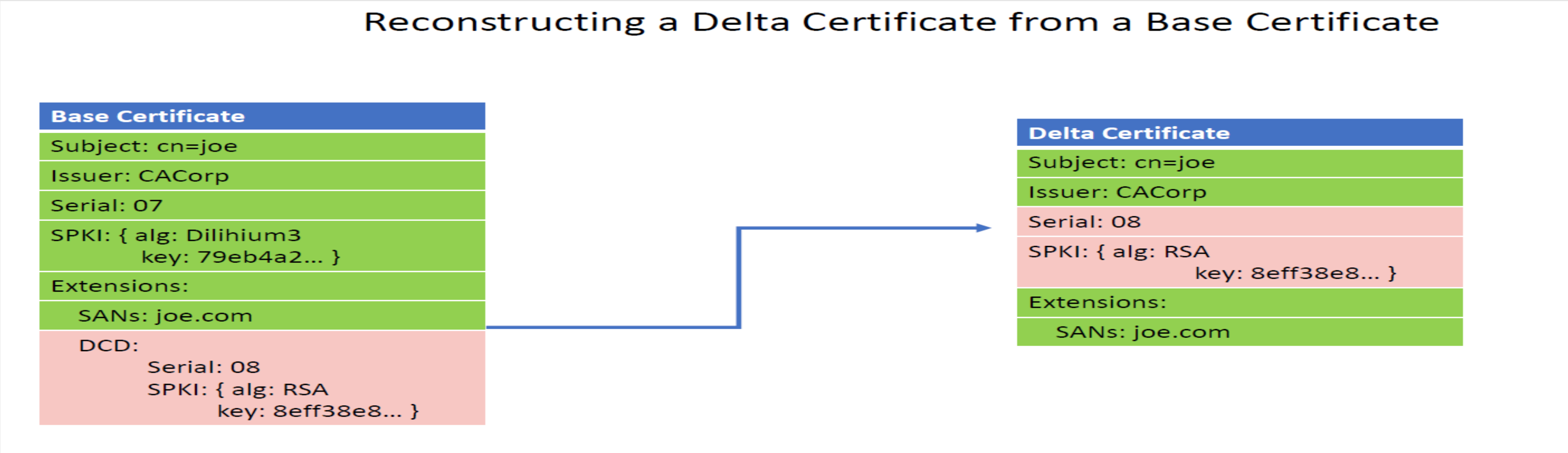
- Protect from on-path attacker using CRQC
- A Post-Quantum X.509 Certificate using Module-Lattice Digital Signature Algorithm (ML-DSA), formerly called Dilithium, is defined in [I-D.ietf-lamps-dilithium-certificates]
- Authentication through a PQ/T hybrid scheme or a PQ/T hybrid protocol, as long as at least one component algorithm remains secure to provide the intended security level.
- The frequency and duration of system upgrades (e.g., root CA) and the time when CRQCs will become widely available need to be weighed in to determine **whether and when to support the PQ/T Hybrid Authentication property**.
- Discussions in LAMPS WG to use PQ/T Hybrid Certificate

PQ/T Hybrid Authentication

- The composite signature contains two signatures in a single atomic container that have been generated using two different cryptographic algorithms. For example, NIST define a dual signature as "two or more signatures on a common message".
  - Composite Signatures For Use In Internet PKI is defined in https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/
- A Mechanism for X.509 Certificate Discovery https://www.ietf.org/id/draft-lamps-okubo-certdiscovery-00.html
  - The Primary Certificate uses a widely adopted cryptographic algorithm while the Secondary Certificate uses the algorithm that is new and not widely adopted yet.
  - Traditional certificates can be exchanged during the TLS handshake and PQ certificates can be exchanged after the session has been established using the mechanism defined in [RFC9261].

PQ/T Hybrid Authentication

- A Mechanism for Encoding Differences in Paired Certificates https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/
  - It allows a relying party to extract information sufficient to construct the paired certificate and perform certification path validation using the constructed certificate.



Reconstructing a Delta Certificate from a Base Certificate

Base Certificate

Subject: cn=joe

Issuer: CACorp

Serial: 07

SPKI: { alg: Dilihium3
key: 79eb4a2... }

Extensions:

SANs: joe.com

DCD:
Serial: 08
SPKI: { alg: RSA
key: 8eff38e8... }

Delta Certificate

Subject: cn=joe

Issuer: CACorp

Serial: 08

SPKI: { alg: RSA
key: 8eff38e8... }

Extensions:

SANs: joe.com

Informing PQC Security Compatibility Issues

- Informing users that the server do not support PQC or hybrid key exchange.
- When the server detects that the client doesn't support PQC or hybrid key exchange, it can send an 'insufficient_security' fatal alert to the client.

Impacted Application Protocols

- Encrypted DNS
- Hybrid public-key encryption (HPKE)
  - ➢ Interaction with Encrypted Client Hello
  - ➢ Oblivious HTTP
  - ➢ MLS
- WebRTC (DTLS)
- HTTPS (Sensitive Data)

Hybrid Key Exchange : Bridging the Gap Between Post-Quantum and Traditional Cryptography

- Post-quantum algorithms selected for standardization are relatively new and they they have not been subject to the same depth of study as traditional algorithms.

- In addition, certain deployments may need to retain traditional algorithms due to regulatory constraints, for example FIPS compliance.

- Hybrid key exchange enables potential security against "Harvest Now, Decrypt Later" attack while not fully abandoning traditional cryptosystems.

Contributing to this document

- Consider for WG adoption
- Comments and Suggestions are welcome
- The document is being collaborated on: https://github.com/tireddy2/pqc_uta