POST-QUANTUM CRYPTOGRAPHY EXPLAINED

for security professionals

PQC

DEPLOYMENTS

ALFRED MENEZES

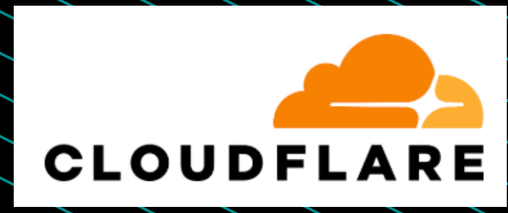
INTRODUCTION

- Upgrading communication protocols to support post-quantum cryptography is challenging.
- Both ends of the communication channel must support the upgrade.
    - For example, when migrating TLS 1.3, both the client and server must support the new cryptographic algorithms.
- Migration is easiest in environments where a single organization controls both endpoints.

HYBRID DEPLOYMENT

- Traditional elliptic-curve key agreement (ECDH) is combined with a quantum-safe key establishment mechanism such as ML-KEM (Kyber).
    - The final shared secret key is derived by concatenating the secrets from both algorithms and passing them through a key derivation function.
    - Protects against Harvest-Now, Decrypt-Later (HNDL) attacks.
- Most migrations today have not upgraded digital signatures.
    - Quantum-secure signatures are generally not necessary until Q-day, when large-scale quantum computers become available.

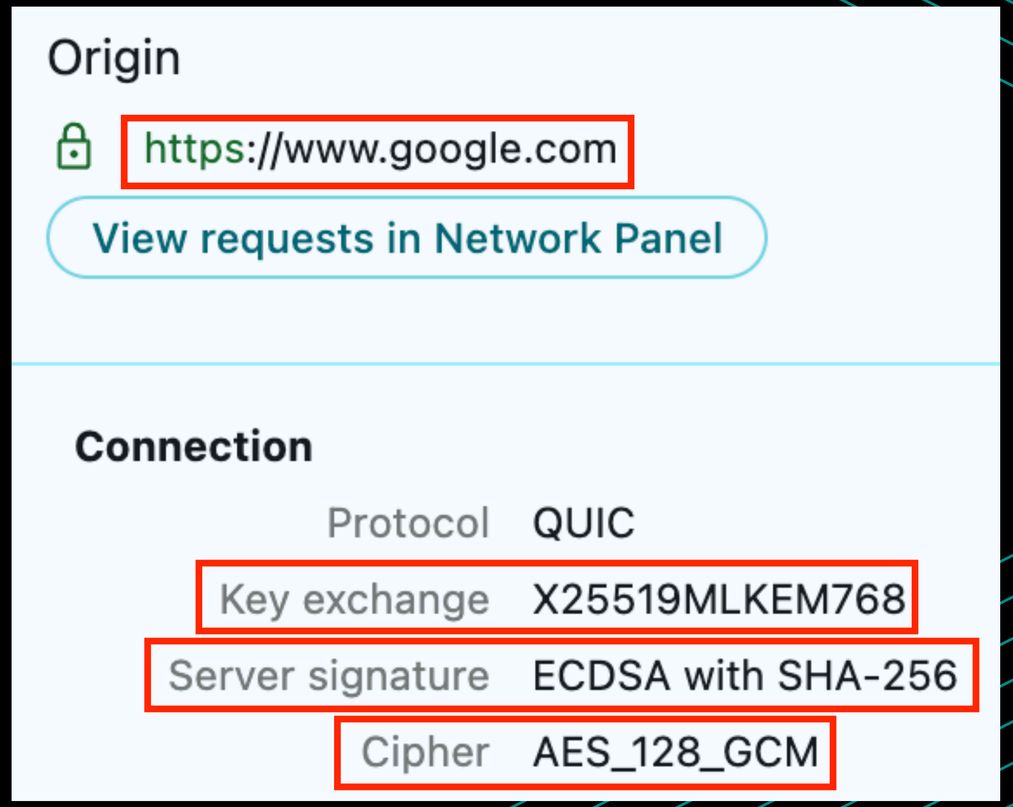
CLOUDFLARE



- Cloudflare provides content delivery and security services for roughly 20% of all websites.
- Began experimenting with PQC in TLS in 2019.
- 2022: Hybrid ML-KEM/ECDH enabled by default for connections between browsers and the Cloudflare network.
- October 2025: Over 50% of all human-initiated traffic with Cloudflare uses PQC.
- Source: blog.cloudflare.com/pq-2025/

GOOGLE

- Integrated hybrid PQC key establishment into both the Chrome browser and the QUIC transport protocol.
- QUIC connection to google.com secured using:
  - Hybrid ECDH (with Curve25519) and ML-KEM (with the ML-KEM-768 parameter set) for key establishment.
  - ECDSA to sign the handshake public keys.
  - AES-GCM to encrypt/authenticate session data.
- Source: cloud.google.com/security/resources/post-quantum-cryptography



AMAZON WEB SERVICES

- Dec 2024: AWS released a comprehensive migration roadmap.
    - Hybrid ECDH-Kyber key establishment is deployed to defend against Harvest Now, Decrypt Later threats.
- June 2025: Progress toward enabling quantum-safe authentication.
    - Integration of ML-DSA (Dilithium) signatures into KMS.
- Nov 2025: ML-DSA included in Private Certificate Authority (Private CA).
- Source: aws.amazon.com/security/post-quantum-cryptography/

SIGNAL

- Signal was the first to deploy post-quantum key agreement for end-to-end encrypted messaging.
- (2023) PQXDH: Post-Quantum Extended Diffie-Hellman.
  - Protection against Harvest Now, Decrypt Later attacks.
- (2025) SPQR: Sparse Post-Quantum Ratchet.
  - Provides both forward secrecy and post-compromise security even against quantum attackers.
- Sources: signal.org/blog/pqxdh
  signal.org/blog/spqr/

APPLE iMESSAGE

- In February 2024, Apple deployed PQC in iMessage.
- PQ3: a new protocol that introduces hybrid post-quantum key establishment.
    - For both initial key establishment and ongoing rekeying.
- Authentication still depends on ECDSA signatures, so is not quantum-safe.
- Source: security.apple.com/blog/imessage-pq3

EMBEDDED SYSTEMS CHALLENGES

- Embedded environments face a unique set of constraints:
  - very long lifetimes.
  - limited CPU power and memory.
  - restricted communication bandwidth.
  - infrequent of impossible update mechanisms.

- Embedded systems requiring PQC migration are everywhere:
  - Automotive systems.
  - Aerospace and satellite systems.
  - Critical infrastructure systems: power grids.
  - Medical devices: implanted devices, hospital equipment.
  - Large-scale IoT deployments: smart meters, home automation devices, sensor networks.
  - Secure hardware: credit cards, bank cards, hardware security modules.

CLOSING

- Large-scale PQC deployment is already underway across the internet.
- Most deployments use hybrid classical-plus-post-quantum cryptography.
- Upgrading key establishment is happening much faster than upgrading digital signatures.
- The most difficult migration challenges lie ahead in embedded and long-lived systems.