POLITECNICO DI MILANO

Engineering of post-quantum cryptosystems

Gerardo Pelosi

DLT Workshop 2025 - 28 November 2025

The post-quantum transition

State and expectations

- The transition to post-quantum cryptosystems has begun
  - Standards from NIST: FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA)
    - FIPS 206 (FN-DSA), FIPS 207 (HQC-KEM) under development
  - Security agencies from some EU states provided recommendations
- Transition plans, in both cases aim at completing transition by 2030 for critical systems and applications

Migration priority

- High: key establishment methods to avoid *store now-decrypt later* attacks
- Moderate: signatures on data at rest which are expected to retain validity for a long time
- (Relatively) low: signatures for interactive authentication (cannot anticausally break them)

An outlook on cryptographic primitives

Session key establishment

- No post-quantum Diffie Hellman key agreement alternative (yet?)
- Forward secrecy [Schwabe et al., 2020], ratcheting [Juaneda et al., 2025] done with KEMs

Digital Signatures

- Achieving RSA-like efficiency in hash-and-sign approaches is challenging
  - Similarly for ZKID+Fiat-Shamir style alternatives (Schnorr-style signatures)
- From an engineering perspective we can get any two goals among: small PubKey, small Signature, fast signature/verification

Symmetric ciphers and hash functions

- Conservative: 256b security yields at least a 128b-equivalent security even after Grover
- Concrete: 128b security likely ok too - overheads and sequentiality of Grover [Jaques, 2024]

The transition forerunners - SSH and instant messaging

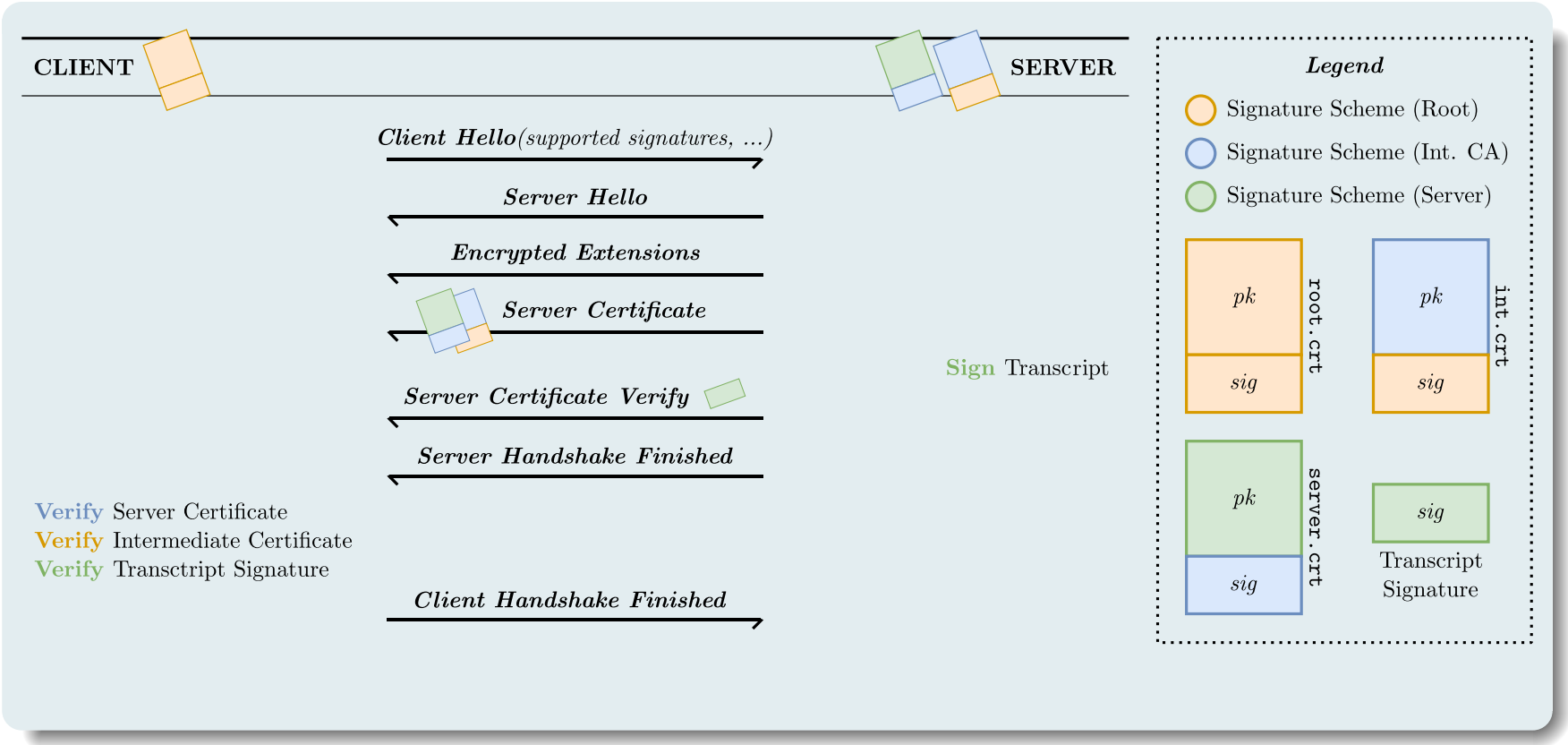
OpenSSH

- OpenSSH was the first widely employed implementation to start transitioning to PQ
  - Friendly protocol and environment: usually runs on high-end hardware, no bandwidth concerns or MTU issues
- Transition started in 2022-04 with Streamlined NTRU Prime+X25519 hybrid
- From 2025-04 ML-KEM-768+X25519 hybrid is the default key establishment
- Currently no PQ signatures for authentication (planned, but deemed less critical)

Instant messaging

- IM apps have many computational resources and little latency concerns
- Signal released PQXDH on 2023-09-19 (Kyber-1024+X25519 hybrid)
- iMessage designs and deploys PQ3 on 2024-02-21 (same hybrid as Signal)

TLS - Overview



Caveats in transitioning TLS

On key establishment

- TLS 1.3 removed the last KEM (RSA-KEM) from the options . . . add them back
- Drop-in forward secrecy requires at least one KEM with fast key generation

On signatures

- TLS certificate verify message is limited to 64 kiB by standard
  - Any PQ signature without $\leq$ 64 kiB signature size is cut out
- The certificate chain (2PubKeys+2Sigs) is limited to 16 MiB by standard
  - Common implementations (OpenSSL) have a far lower bound (few tens of kiBs)
  - PubKey size + Sig size should be limited to avoid malfunctioning
- Client does computes at least 3 verifications, server computes 1 signature
  - Fast verification algorithms will not benefit the server load

DNSSec - structure and constraints

- DNS runs over 53/UDP and is a single request-response pair communication
- DNS traffic is latency critical, network level fragmentation is an issue
  - IPv4 allows for a large transported PDU (64kiB) but may fragment
  - IPv6 does not fragment but established MTU by repeated trials
- DNS server required to sign each response: potential bandwith amplification DoS

Practical cryptographic object size limits

- Ethernet Maximum Transfer Unit: 1500 B
- Minimum required PDU size for IPv6 support: 1280 B
- Conservative PDU payload for DNS extension: 1232 B
  - 1280 B (IPv6 minimum MTU) - 40 B (IPv6 Header) - 8 B (UDP Header)

DNSSec - Viability

Try to squeeze signatures in

- RIPE90 - 2025-05-14: tested a couple PQ candidates from NIST's 4th round+ Falcon (NIST selected as FN-DSA for the smallest signatures)
- Most PQ signatures either do not fit into size constraints, or are too slow
- Hawk (improved Falcon) fits the bill with reduced parameters,

Change the approach

- Observation: authentication in DNSSec is interactive: signatures not mandatory
- SignatureLess-DNSSec [Rawat and Jhanwar, 2025] (2025-08-25)
  - Use a PQ KEM to encapsulate a key per query, compute a MAC tag on the response
  - Fast, uses less bandwith than Falcon-signed DNSSec
  - Transmitter sends more data than responder: no bandwith amplification DoS

Virtual Private Networks

IPSec and OpenVPN

- IPSec: working implementation (StrongSWAN), no issues, given an X.509 library supporting PQ algorithm
- OpenVPN: current FIPS standards supported, relying on a recent OpenSSL

Wireguard

- Single UDP PDU size constraints to DNS make it difficult to use PQ KEMs
  - Stopgap measure: pre-shared symmetric keys can be added to session secret
  - Classic McEliece fits in the constraints without modifications
  - Recent work which modifies slightly protocol, formally verifies security properties and uses McEliece+Kyber hybrid [Lafourcade et al., 2025]

Blockchain Technologies

Pre- and Post-quantum digital signatures

- signature sizes: 65 B (ECDSA); 64 B (Ed25519) – 32 B public keys for 128-bit security.
  - Currently, an Ethereum **"full node"** requires $> 500GB$; an **"archive node"** $\approx 3TB$
  - On a smartphone, block verification: $\approx$ from 2 to 6 hours
- 2,420 B (ML-DSA); 7,856 B (SLH-DSA); 666 (FN-DSA) – 1,016 B; 32 B; 8,97 B public key size for 128-bit security
  - Some newer blockchain architectures or scaling solutions might be able to handle larger signatures more efficiently or use alternative proof systems

Memory and energy constrained devices

- Microcontroller environments have tight memory requirements
    - e.g. STM32L4R5ZI, high end Cortex-M4 has 640kiB SRAM, 2 MiB Flash
- Memory, more than computation latency is often a stopgap

Current NIST standards and fitness on a microcontroller

- Current NIST standard schemes all fit on the above μC
- Additional call signatures are memory constrained:
    - Out of 14, only 10 fit on a high end Cortex-M4 [Kannwischer et al., 2024] (CROSS, HAWK, Mirath, MQOM, PERK, RYDE, MAYO, SNOVA, UOV, FAEST)
- The main roadblock is often the runtime memory consumption
    - Fiat-Shamir transform requires committments to be kept in memory
    - MPCitH derives a significant amount of pseudorandom bytes at runtime

Concluding remarks

- Transitioning to post-quantum cryptography has begun
- Concrete solutions are already available for widely used protocols
  - Some are just drop-in changes (SSH)
  - Some alter the protocol logic (Signature Less - DNSSec, TLS KEM)
- Transitioning requires cryptographic agility
  - No single "silver bullet" solution, a portfolio of algorithms may be required
  - Gain agility now, and keep it for future improvements in cryptosystems

Questions?

Thank you for the attention!

gerardo.pelosi@polimi.it

Bibliography I


Jaques, S. (2024).
Quantum Attacks on AES.


Juaneda, J., Dehez-Clementi, M., Deneuville, J.-C., and Lacan, J. (2025).
RHQC: post-quantum ratcheted key exchange from coding assumptions.
Cryptology ePrint Archive, Paper 2025/481.


Kannwischer, M. J., Krausz, M., Petri, R., and Yang, S.-Y. (2024).
pqm4: Benchmarking nist additional post-quantum signature schemes on microcontrollers.
IACR Cryptol. ePrint Arch., 2024:112.


Lafourcade, P., Mahmoud, D., Ruhault, S., and Taleb, A. R. (2025).
A tale of two worlds, a formal story of WireGuard hybridization.
Cryptology ePrint Archive, Paper 2025/1179.


Rawat, A. S. and Jhanwar, M. P. (2025).
Quantum-safe signatureless dnssec.
In *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '25, page 267–282, New York, NY, USA. Association for Computing Machinery.


Schwabe, P., Stebila, D., and Wiggers, T. (2020).
Post-quantum TLS without handshake signatures.
In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, page 1461–1480, New York, NY, USA. Association for Computing Machinery.

PQC research at PoliMi - Software

Key Encapsulation Methods

- Co-designer and implementation lead of LEDAcrypt
  - Tailored and optimized modular polynomial inversion techniques for AVX2 ISA ext.s
  - Constant time, constant weight encoding algorithm design

Signatures

- Member of CROSS team and implementation lead (2º NIST on-ramp for signatures)
  - Contributed to choice of arithmetics and parameters
  - Realized optimized AVX2 implementation - end-to-end TLS latency tests successful
  - Co-implementation of Cortex-M4 in collaboration with TUM
- Member of LESS team (2º NIST on-ramp for signatures)
  - Contributed to reference and AVX-2 optimized codebase

PQC research at PoliMi - Hardware

Key Encapsulation Methods

- First HDL implementation of HQC-KEM as a dedicated standalone accelerator
  - Designed algorithmic improvement now included in HQC-KEM official specification
  - Largely sub-ms latencies on a low-end Xilinx Artix-A7 FPGA
- NTRU/NTRUPrime/Kyber unified arithmetic accelerators
  - Leverages similarities in the operational description of modular multiplications
  - Cryptographic agility with very small overhead and no performance penalty

Signatures

- CROSS standalone accelerator design - In collaboration with TU Munich
  - Efficiency oriented design: throughput can be scaled easily via parallelization

PQC research at PoliMi - Further directions

Code based cryptography design

- Provided accurate DFR estimation technique for 3-iterations QC-MDPC decoders
  - Allows parameterization of LEDAcrypt/BIKE improving efficiency at no security loss
- Proved computational equivalence of hard problems underlying LEDAcrypt/BIKE
  - Allows public key size vs. ciphertext size tradeoffs w/o security losses

Side channel attacks and countermeasures

- 15+ years of experience in side channel attacks and countermeasures
  - Introduced new countermeasure paradigms (code morphing, chaffing)
  - Currently looking into side channel protection for PQ signatures