

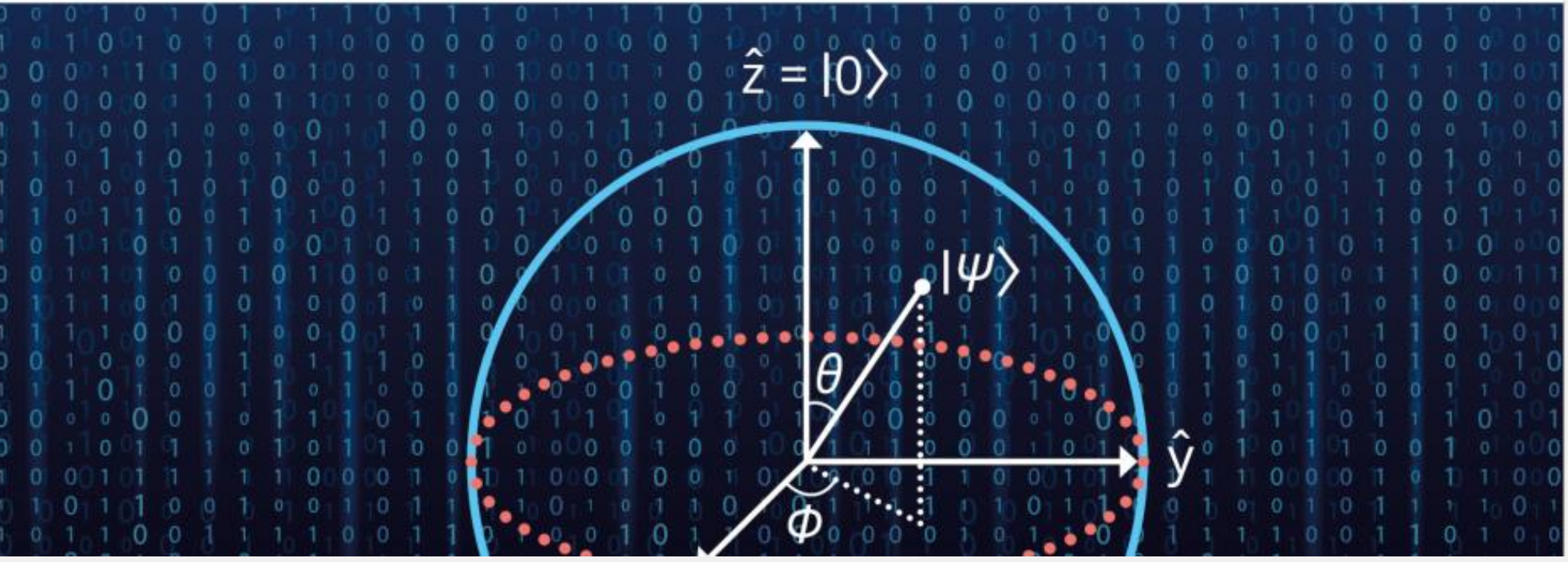
Innovations Eindhoven University of Technology and Academia Sinica

Tanja Lange

Department or Mathematics and Computer Science

Post-Quantum Cryptography: Current state and quantum mitigation

Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing,
Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart.
Evangelos Rekleitis, Angeliki Aktypi, Athanasios-Vasileios Grammatopoulos.



Two ENISA reports

Reports commissioned by ENISA
(European Union Agency for Cybersecuriy)

- Current state and quantum mitigation.

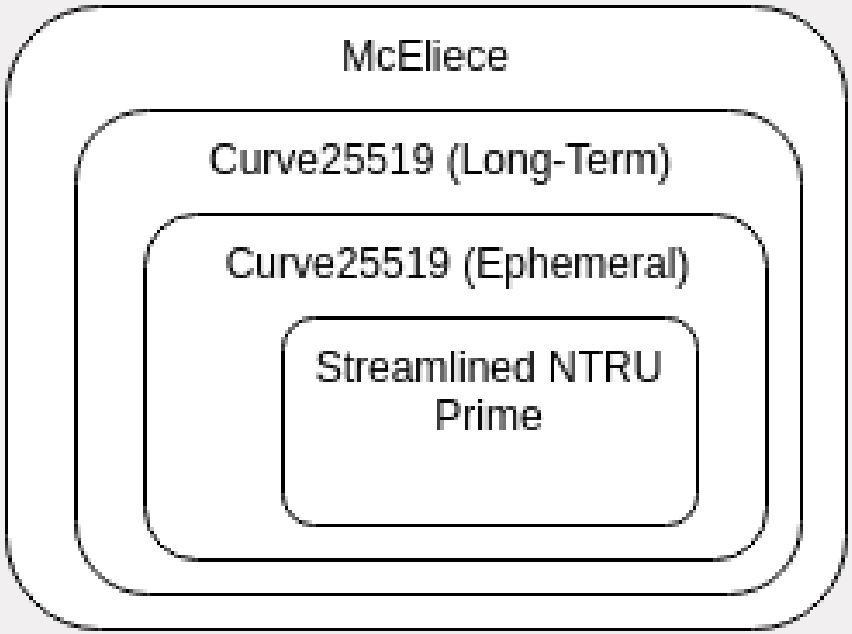
- PQC Integration Study

PQConnect

- Do not patch PQC onto existing network protocols, but add a new layer with superior security.
- Can be gradually deployed.
- Add support for VPN-like tunnels to clients and servers.
- PQConnect is designed for security, handshake and ratcheting proven using Tamarin prover (formal verification tool).
- Use Curve25519 (pre-quantum) and Classic McEliece (conservative PQC) for long-term identity keys.
- Use Curve25519 (pre-quantum) and Streamlined NTRU Prime (PQC) for ephemeral keys.

PQConnect handshake: Nesting schemes

Most conservative system on the outside.



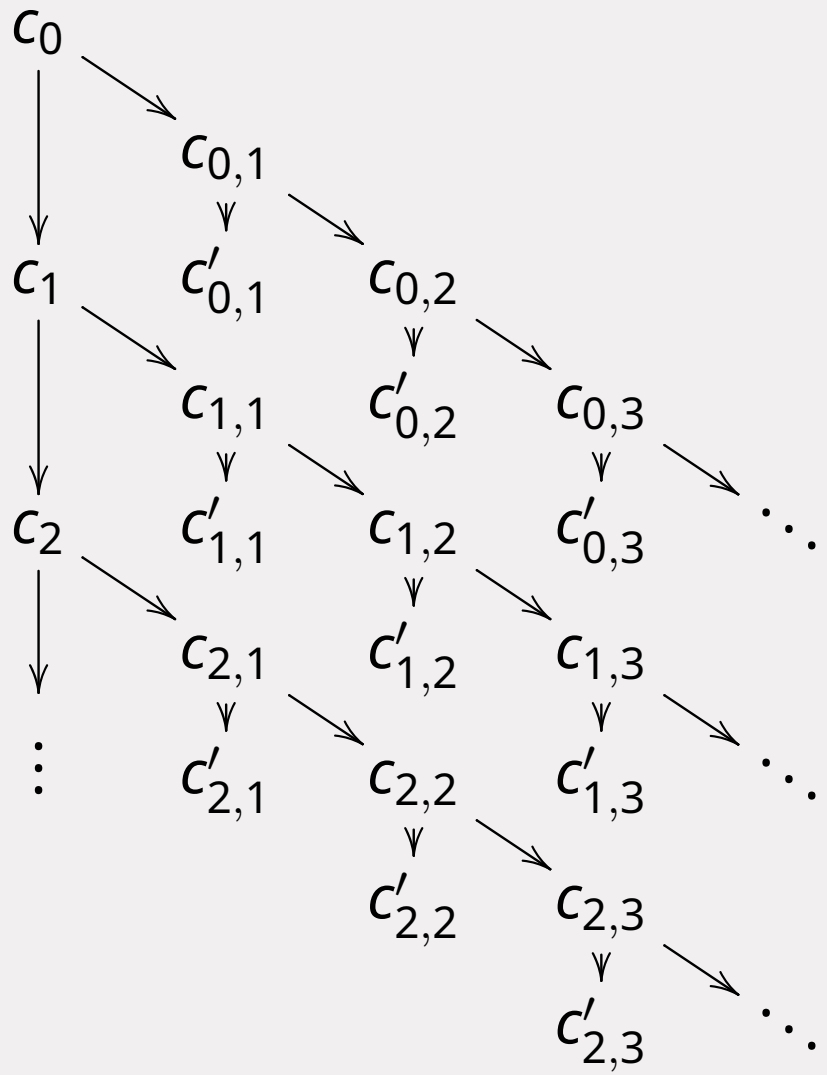
Attacker can see long-term Curve25519 identity key,
can break it with a quantum computer,
but cannot obtain DH value as client's share is wrapped.

Key ratchet advances by message and time

c_0 is the initial key.
Immediately advance ratchet in 3 ways:

- New epoch master key: c_1.
- New branch keys: $c_{0,1}, c_{0,2}$.
- New message key: $c'_{0,1}$.

New epoch every 30 seconds.
Keys erased upon use, or at latest after 2 minutes.
Message keys can deal with delayed transmissions.



NIST PQC submission Classic McEliece

No patents. Shortest ciphertexts.
Fast open-source constant-time software implementations.
Very conservative system, expected to last; has strongest security track record.

Metric	mceliece348864	mceliece460896	mceliece6960119
Public-key size	261120 bytes	524160 bytes	1047319 bytes
Secret-key size	6452 bytes	13568 bytes	13908 bytes
Ciphertext size	128 bytes	188 bytes	226 bytes
Key-generation time	34300491 cycles	109253278 cycles	240091868 cycles
Encapsulation time	44375 cycles	87808 cycles	165500
Decapsulation time	128521 cycles	264058 cycles	291123 cycles

See https://classic.mceliece.org for authors, details & parameters.

NIST submission SPHINCS+

- Signature based on hash functions.
- Requires only a secure hash function, no further assumptions.
- Based on ideas of Lamport (1979) and Merkle (1979).
- Developed starting from SPHINCS with
  - improve multi-signature,
  - smaller keys,
  - Option for shorter signatures (30kB instead of 41kB) if "only" 2^{50} messages signed.
- Selected as winner by NIST.

More info at https://sphincs.org/.

NIST submission NTRU Prime

- Lattice-based encryption systen, shorter keys.
- NTRU Prime exposes less strcture to attackers:
- No decryption errors.

Metric	**Streamlined NTRU Prime** 4591^{761}	**NTRU LPRime** 4591^{761}
Public-key size	1218 bytes	1047 bytes
Secret-key size	1600 bytes	1238 bytes
Ciphertext size	1047 bytes	1175 bytes
Key-generation time	1054992 cycles	44940 cycles
Encapsulation time	44615 cycles	77597 cycles
Decapsulation time	94744 cycles	109283 cycles

More information at https://ntruprime.cr.yp.to/.