PQC Internet

Arne Ansper

arne@cyber.ee

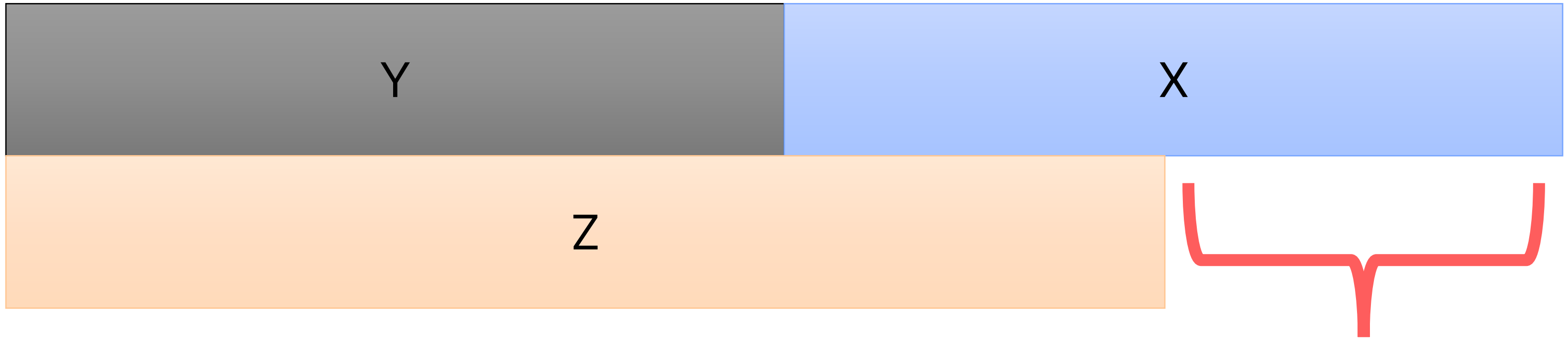
CYBERNETICA

What IETF is doing regarding PQC?

- Involved working groups
  - pquip – Post-Quantum Use In Protocols
  - cfrg - Crypto Forum RG
  - tls – Transport Layer Security
  - ipsecme – IP Security Maintenance and Extensions
  - lamps – Limited Additional Mechanisms for PKIX and SMIME
  - cose – CBOR Object Signing and Encryption
  - mls – Messaging Layer Security
  - openpgp – Open Specification for Pretty Good Privacy

Mosca theorem

- "Harvest today, decrypt tomorrow" attack



Urgent problem

IETF Approach

- Most of the work is done in parallel in the existing working groups
- Huge tasks are split into smaller tasks that are prioritized
  - There will be many intermediary standards towards the full PQC Internet
- Confidentiality problem is the most urgent and is dealt first
  - Fortunately it's also the simplest
  - Standards that are needed to ensure the long-term confidentiality are most mature
- Work is also performed for authentication and PKI
  - More complex
  - Less mature
  - More external dependencies

What needs to be done for each protocol?

- Finalized algorithms – secure, stable, standardized
- Protocols that are capable of accepting new algorithms
  - Sizing of messages, performance of algorithms, mandatory information flows
- Encoding of the keys, signatures, cryptograms etc.
- Identifiers for algorithms
- Security proofs of protocols
  - You just can't plug PQC algorithm into existing protocol and declare that it is secure

Why it takes so long?

- Nature of the IETF standardization process
- Even simple things are complex to do securely
- Readiness of the algorithms
- Politics. Mostly about the usage of PQ/T hybrid algorithms
  - BSI, ANSSI: required
  - ETSI, ENISA: allowed
  - NSA, NCSC, CSR: discouraged
- But: most of the drafts have been implemented

"Confidentiality" Protocols

- HPKE
- IPsec/IKE
- TLS
- CMS
- SSH

Hybrid Public Key Encryption RFC 9180

- Not "this hybrid" but the "original hybrid"
- Comprehensive solution to the public-key encryption – traditional or PQC
  - key establishment
  - key derivation
  - encryption
  - standardized and safe APIs
- Vision
  - PQC should be incorporated into protocols by applying HPKE or its parts

HPKE Security Proofs for Post-Quantum

- Security of HPKE has proven for DHKEM
- A full proof of post-quantum security would need to take appropriate security models and assumptions into account, in addition to simply using a post-quantum KEM
- HPKE Auth mode is provably secure with post-quantum-secure authenticated KEM
    - We don't have post-quantum-secure authenticated KEM

X25519 + ML-KEM-768

- Hybrid KEM that combines X25519 with ML-KEM-768
- X-Wing
  - https://datatracker.ietf.org/doc/draft-connolly-cfrg-xwing-kem/
- For HPKE (expired)
  - https://datatracker.ietf.org/doc/draft-westerbaan-cfrg-hpke-xyber768d00/
- For TLS (expired)
  - https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/

IPsec/IKE

- Focus is on ensuring the confidentiality
- Packet encryption is PQC secure, key exchange is not
- RFC 8784 – reintroduce DH-less pre-shared symmetric key mode to IKE
  - Supported by e.g. Cisco and Juniper
  - ... but most likely will be updated
- RFC 9370 – up to 7 layers of additional KEM-s
  - RFC 9242 – solves the problem of the large keys of the PQC algorithms
  - ... but there are more drafts

IKE KEMs

- ML-KEM
  - https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/
- ML-KEM and Frodo KEM
  - https://datatracker.ietf.org/doc/draft-wang-hybrid-kem-ikev2-frodo/

TLS

- RFC 8773 – short-term solution, support for additional preshared keys
- Hybrid key exchange
  - https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
- ML-KEM usage in TLS
  - https://datatracker.ietf.org/doc/draft-connolly-tls-mlkem-key-agreement/
- X25519 + ML-KEM-768 (expired)
  - https://datatracker.ietf.org/doc/draft-tls-westerbaan-xyber768d00/

Messaging Layer Security (MLS) RFC 9420

- End-to-end secure messaging
- Uses HPKE
- Short-term solution: X-Wing usage in MLS
  - https://datatracker.ietf.org/doc/draft-mahy-mls-xwing/
- Different long-term solutions proposed
  - Parallel sessions
  - Separate KEMs at protocol level that can be used selectively

CMS

- RFC 8696 – pre-shared keys in CMS
- Using KEMs in CMS
  - https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kemri/
- Using ML-KEM in CMS
  - https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kyber/

SSH

- No active WG for SSH
- Only expired drafts
- Kyber
  - https://datatracker.ietf.org/doc/draft-kampanakis-curdle-ssh-pq-ke/
- NTRU
  - https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-ssh/

PQC PKI

- Three options
  - Parallel PKIs
  - Combined algorithms/keys in certificates
  - Multiple algorithms/keys in certificates
- More complex problem

Other protocols

- DNSSEC
- JOSE/COSE
- OpenPGP

References

- Summary of IETF activities
  - https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc
- Post-Quantum Cryptography for Engineers
  - https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/
- Terminology for Post-Quantum Traditional Hybrid Schemes
  - https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/

Thank you!

https://cyber.ee/

info@cyber.ee

cybernetica

CyberneticaAS

cybernetica_ee

Cybernetica