# PKI and Post-Quantum Cryptography

David Cooper

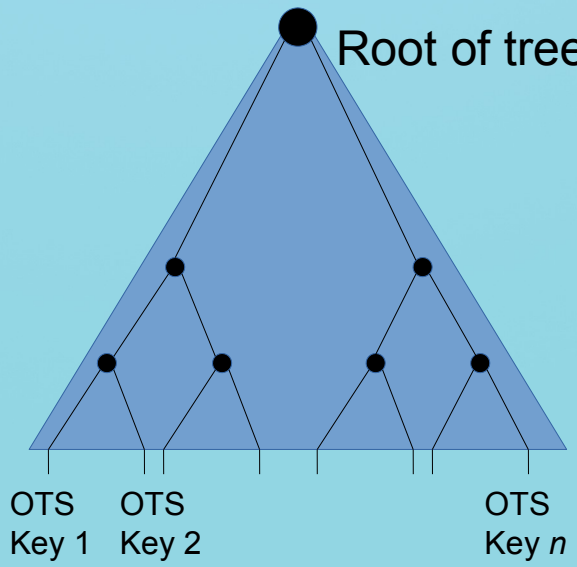
March 5, 2019

# Post-Quantum Algorithms

- Stateless cryptographic algorithms
  - NIST Post-Quantum Cryptography Standardization Process
  - https://csrc.nist.gov/projects/post-quantum-cryptography
  - pqc-comments@nist.gov
- Stateful hash-based signatures
  - Internet Research Task Force (IRTF) Crypto Forum Research Group (CFRG)
  - https://csrc.nist.gov/Projects/Stateful-Hash-Based-Signatures
  - https://csrc.nist.gov/News/2019/stateful-hbs-request-for-public-comments

# Stateful Hash-Based Signatures

- Two options, XMSS/XMSS$^{MT}$ and LMS/HSS, specified by CFRG.
- Create large number of one-time signature (OTS) keys
- Publish root of a tree of these keys



# Stateful Hash-Based Signatures

- Very small public key ~ 60 bytes
- Moderate signature size ~ 2.5 to 8 KB
- Secure if hash function is secure (pre-image resistant), *if used correctly*.
- Smaller and faster signatures than stateless hash-based signatures (e.g., SPHINCS+).
- Significant risk from one-time key reuse!

# Candidate Post-Quantum Algorithms

## Signature Algorithms

- CRYSTALS-DILITHIUM
- FALCON
- GeMSS
- LUOV
- MQDSS
- Picnic
- qTESLA
- Rainbow
- SPHINCS+

## Key Encapsulation Mechanisms

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC
- LEDAcrypt (merger of LEDAkem/LEDApkc)
- NewHope
- NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
- NTRU Prime
- NTS-KEM
- ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
- Round5 (merger of Hila5/Round2)
- RQC
- SABER
- SIKE
- Three Bears

# Candidate Signature Algorithms

| Algorithm | Type | Public Key (bytes) | Signature (bytes) |
|---|---|---|---|
| CRYSTALS-DILITHIUM | Lattice | 1184 | 2044 |
| FALCON | Lattice | 897 | 690 |
| qTESLA | Lattice | 1504 | 3104 |
| LUOV | Multivariate | 7536 | 1746 |

- Fast (or not too slow) signing and verification
- Moderate key and signature sizes

# Candidate Signature Algorithms

| Algorithm | Type | Public Key (bytes) | Signature (bytes) |
|---|---|---|---|
| GeMSS | Multivariate | 417,408 | 48 |
| Rainbow | Multivariate | 152,097 | 64 |

- Large (huge) public keys
- Very small signatures
- Performance:
  - GeMMS: fast verification; very slow signatures
  - Rainbow: fast signing and verification
- Maybe useful for applications such as Certificate Transparency?

# Candidate Signature Algorithms

| Algorithm | Type | Public Key (bytes) | Signature (bytes) |
|---|---|---|---|
| Picnic | symmetric-key | 32 | 13,786 |
| SPHINCS+ | Hash-based | 32 | 8,080 |
| MQDSS | Multivariate | 62 | 32,882 |

- Very small public keys
- Large signatures
- Performance:
  - Picnic: somewhat slow signing and verification
  - SPHINCS+: very slow signing, moderate verification
  - MQDSS: slow signing and verification

# PKI

- LAMPS – Limited Additional Mechanisms for PKIX and SMIME
  - *Algorithm Identifiers for HSS and XMSS for Use in the Internet X.509 Public Key Infrastructure* - draft-vangeest-x509-hash-sigs
  - *Multiple Public-Key Algorithm X.509 Certificates* – draft-truskovsky-lamps-pq-hybrid-x509
    - Include second (post-quantum) public-key in non-critical extension
    - Include second (post-quantum) signature in non-critical extension

# What to do now?

- Don’t rush:
  - https://spectrum.ieee.org/tech-talk/computing/hardware/the-us-national-academies-reports-on-the-prospects-for-quantum-computing
  - Issuing PQ certificates can wait until client software can process it.
  - Don’t know which algorithms will be standardized and/or implemented.
  - Don’t know whether clients will support multi-algorithm certificates.