Lecture 10

zaterdag 10 december 2022 19:43

post-quantum cryptography → cryptography under assumption attacker has quantum computer

Shor's algorithm → period finding
↓ integer factorization, ↘ discrete log

categories of signatures:

- code-based: enc
- hash-based: sign
- isogeny-based: enc
- lattice-based: enc, sign
- multivariate quadratic: sign

stateful hash-based signatures → problem on VM: need to be restored from backup, also issues in cluster

one-time signature

↳ for many messages: key generation

hash-based

secret = hash(random)
public = hash(secret)

1-bit message: sign with first or last 32-bits of 64-bit secret (if bit=0 / if bit=1)

4-bit message: more of the same

signing more than one message: side channels ⇒ forgeries

256-bits: induction ...

downside: large keys

publish $H^{16}(SK)$

reveal $S = H^m(SK)$ a signature for message m

to verify, check whether $PK = H^{16-m}(SK)$

Eve can sign with $H(3)$ for message $m+1$

Solution: Use key chains in two directions; knowing both sides is only possible if both are known (allow "shortcuts")

fast Winternitz: sign message & checksum of message

Merkle tree: binary tree, every node contains hash of combination of nodes below