NTNU | Norwegian University of Science and Technology

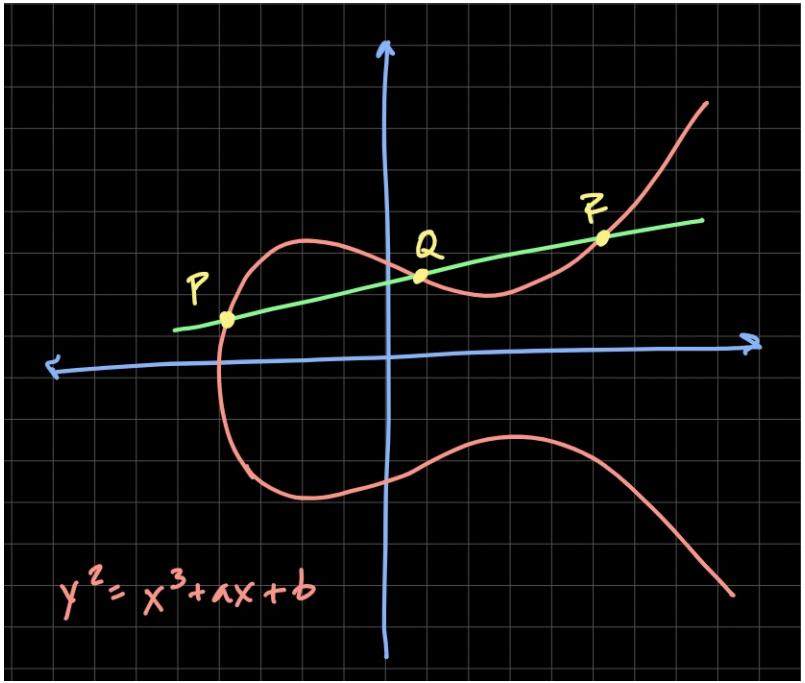
Kvantesikker Kryptografi 1: Slutten på Starten

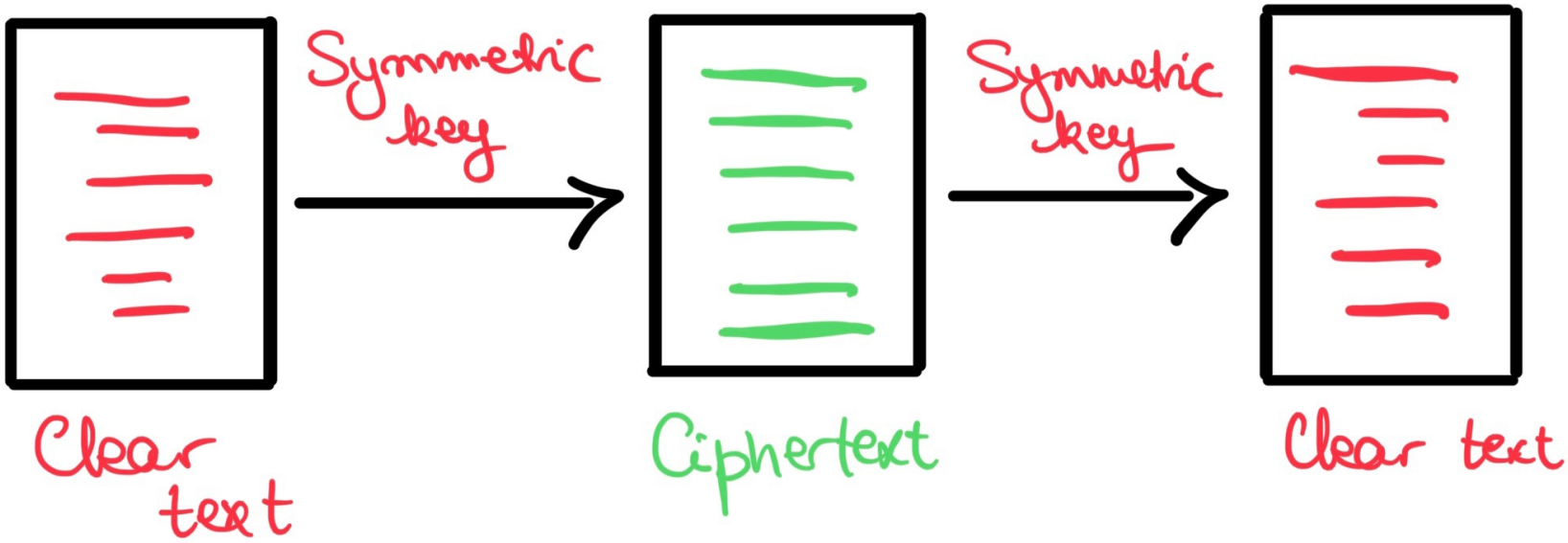
Tjerand Silde – Sikkerhetsfestivalen 2023

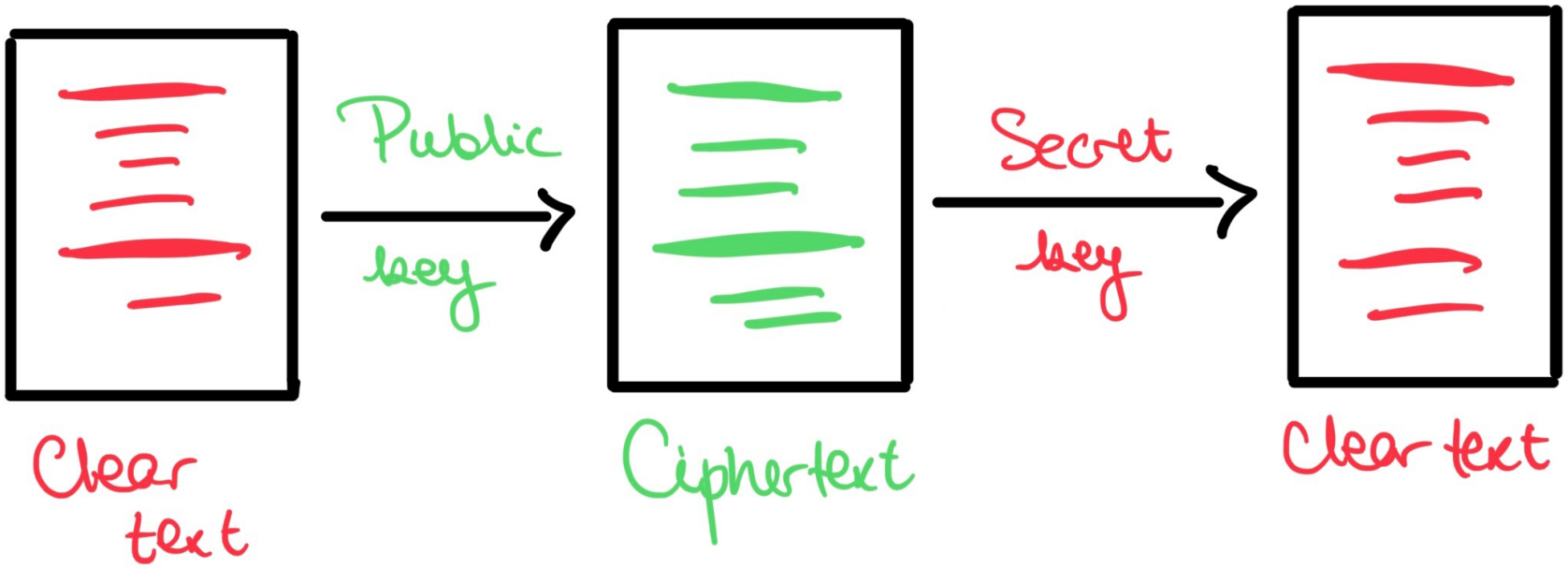
Dagens kryptografi

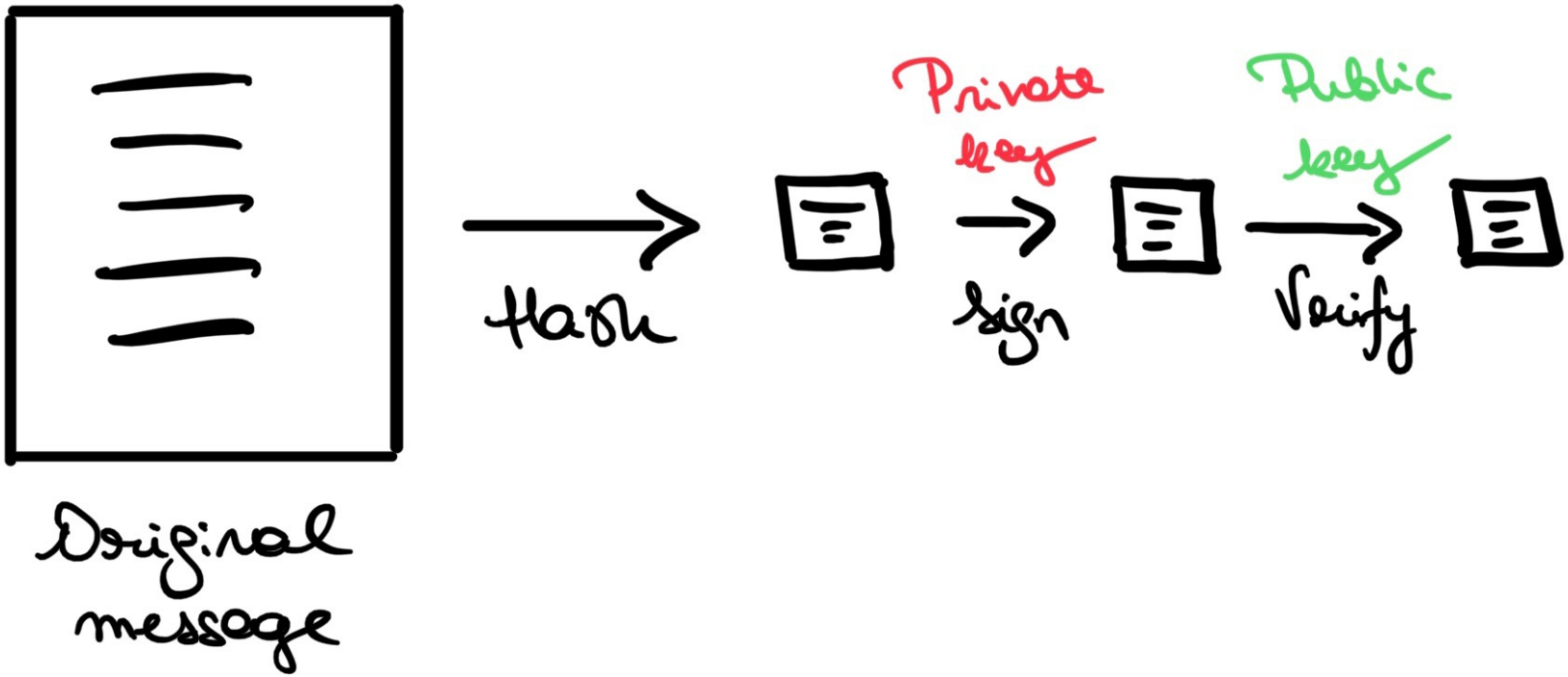
Symmetrisk-nøkkel krypto:
AES-128 og SHA-256

Offentlig-nøkkel krypto:
RSA, Diffie-Hellman (DH),
Elliptiske kurver (ECDH,
ECDSA,...)




Symmetric key
Symmetric key
Clear text
Ciphertext
Clear text


Public
key
Secret
key
Clear
text
Ciphertext
Clear text


Private key
Public key
Hash
Sign
Verify
Original message

Kvantedatamaskiner

Svekker AES-128 og SHA-256, men har AES-256 og SHA-512 (💪💪)

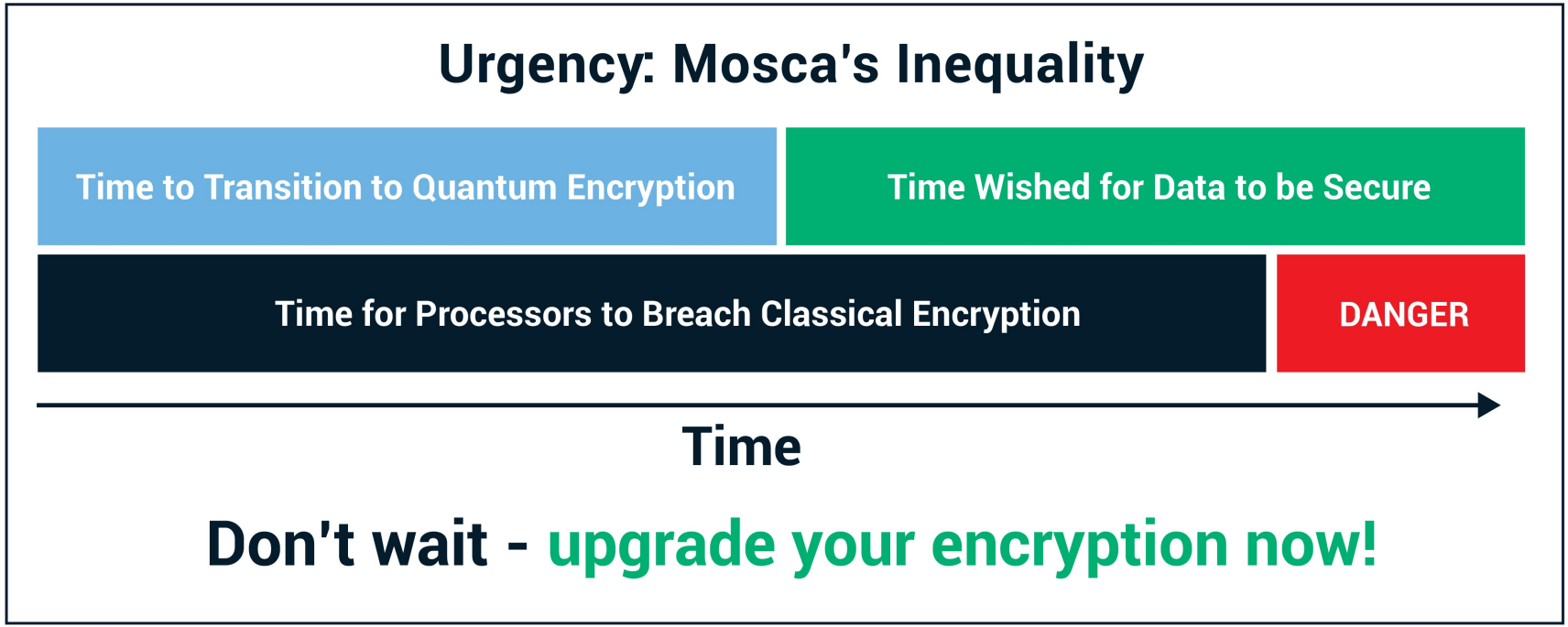
Kan faktorisere (RSA ☠) og beregne (EC) diskrete logaritmer (DH, ECDH, ECDSA ☠☠☠)

Kvantesikker kryptografi

Dagens kryptografi er bygget på vanskelige matematiske problemer vi ikke kan knekke i dag.

Dersom kvantedatamaskiner kan knekke disse problemene så må vi finne nye vanskelige matematiske problemer å bygge kryptografi på.

Hvorfor bryr vi oss i dag?



NIST-standardisering

Moody, Dustin (Fed) 24. aug. 2023, 14:22:37 (for 3 døgn siden) ☆

til pqc-forum

We are very happy to announce that the draft PQC standards are now available!

Dustin Moody
NIST PQC

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

NIST requests comments on the initial public drafts of three Federal Information Processing Standards (FIPS):

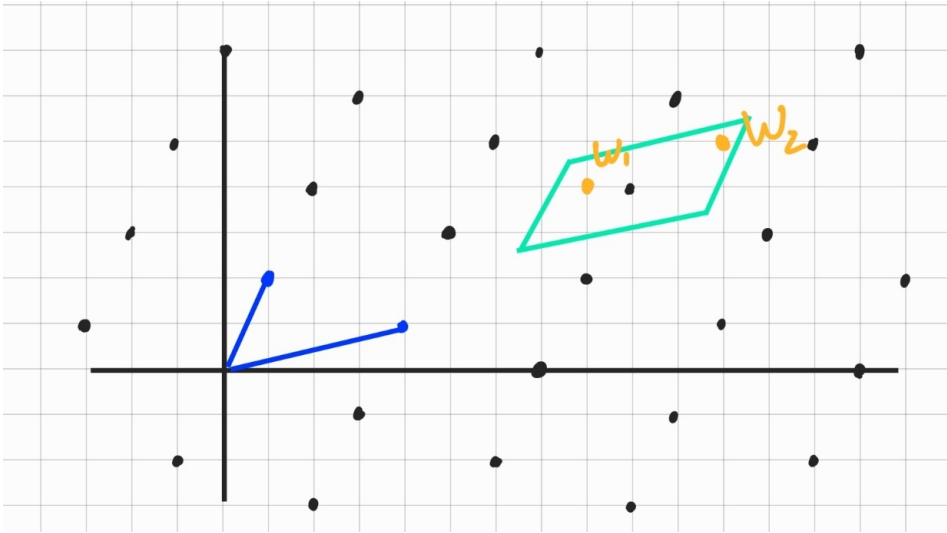
1. FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
2. FIPS 204, *Module-Lattice-Based Digital Signature Standard*
3. FIPS 205, *Stateless Hash-Based Digital Signature Standard*

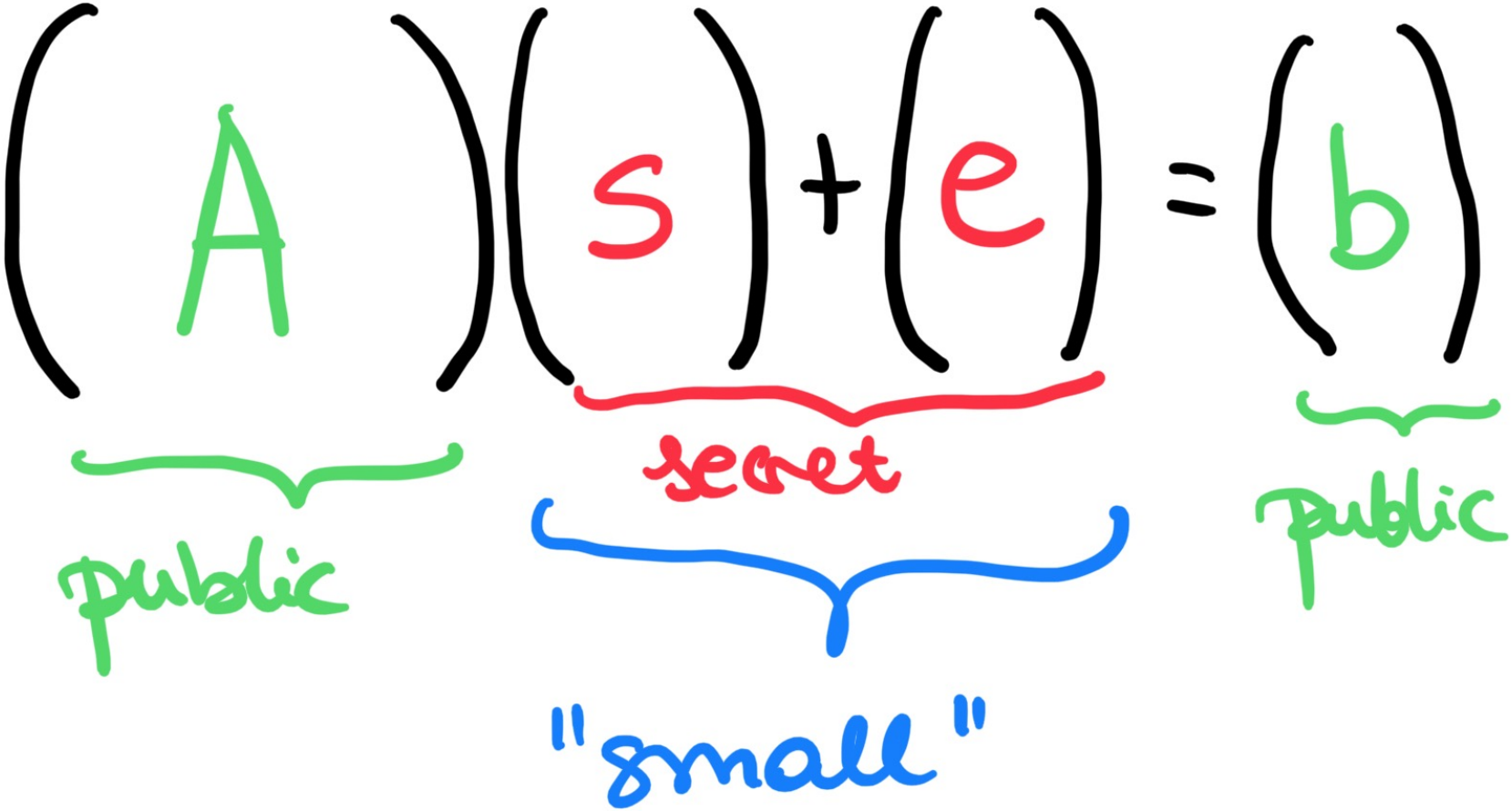
Gitter-basert kryptografi

Nye (2005) vanskelige matematiske problemer

Gir oss sikre og effektive protokoller

Basis: lineær algebra




A
s
+
e
=
b
public
secret
public
"small"

Størrelser

	encapsulation key	decapsulation key	ciphertext	shared secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

Table 3. Sizes (in bytes) of keys and ciphertexts of ML-KEM

nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf

Størrelser

	Private Key	Public Key	Signature Size
ML-DSA-44	2528	1312	2420
ML-DSA-65	4000	1952	3293
ML-DSA-87	4864	2592	4595

Table 2. Sizes (in bytes) of keys and signatures of ML-DSA.

nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf

Størrelser

		Size keyshares(in bytes)		Ops/sec (higher is better)	
Algorithm	PQ	**Client**	**Server**	**Client**	**Server**
Kyber512	✅	800	768	50,000	100,000
Kyber768	✅	1,184	1,088	31,000	70,000
X25519	❌	32	32	17,000	17,000

blog.cloudflare.com/post-quantum-for-all

Størrelser

		Size (bytes)		CPU time (lower is better)	
	PQ	Public key	Signature	Signing	Verification
Ed25519	❌	32	64	1 (baseline)	1 (baseline)
RSA-2048	❌	256	256	70	0.3
Dilithium2	✅	1,312	2,420	4.8	0.5
Falcon512	✅	897	666	8*	0.5
SPHINCS⁺128s	✅	32	7,856	8,000	2.8
SPHINCS⁺128f	✅	32	17,088	550	7

blog.cloudflare.com/nist-post-quantum-surprise

Hybride protokoller

En måte å migrere til kvantesikker kryptografi er å kombinere dagens klassiske algoritmer med morgendagens kvantesikre algoritmer.

Dette anbefales blant annet fra franske og tyske myndigheter. USA erstatter algoritmene direkte.

Veien videre

Nå har vi standardisert de nye kvantesikre algoritmene. Men dette er bare første steg....

Neste foredrag handler om hva vi gjør videre :)

Takk! Spørsmål?

Epost: tjerand.silde@ntnu.no

Nettside: tjerandsilde.no