NTNU | Norwegian University of Science and Technology

Kvantesikkerhet: Fremtidssikker kommunikasjon og personvern

Tjerand Silde @ Webinar Kvantetrusselen

Introduksjon

Førsteamanuensis i kryptologi ved NTNU

Institutt for informasjonssikkerhet og kommunikasjonsteknologi og CCIS

Leder NTNU Applied Cryptology Lab

Kvantesikker kryptografi og personvern

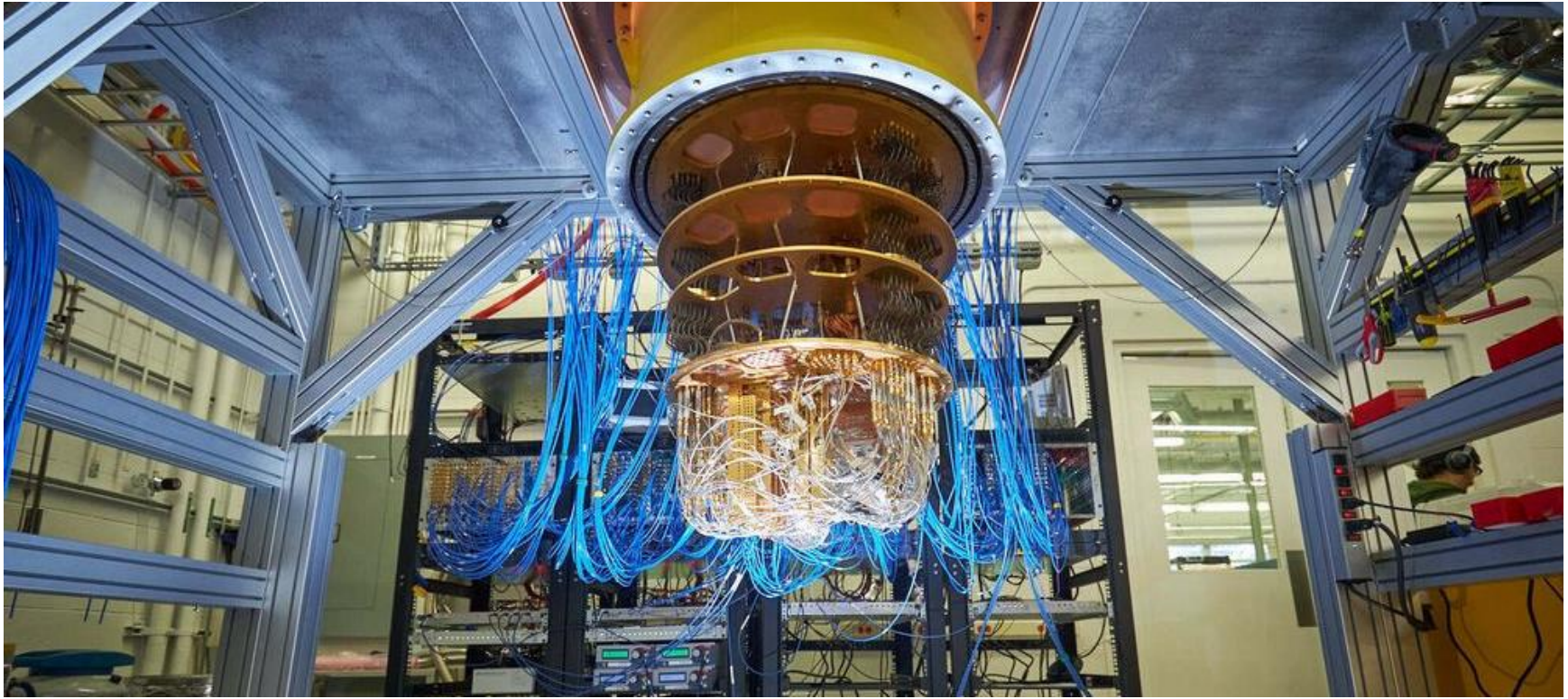
Kryptoekspert i PONE Biometrics

Kryptografi i dag

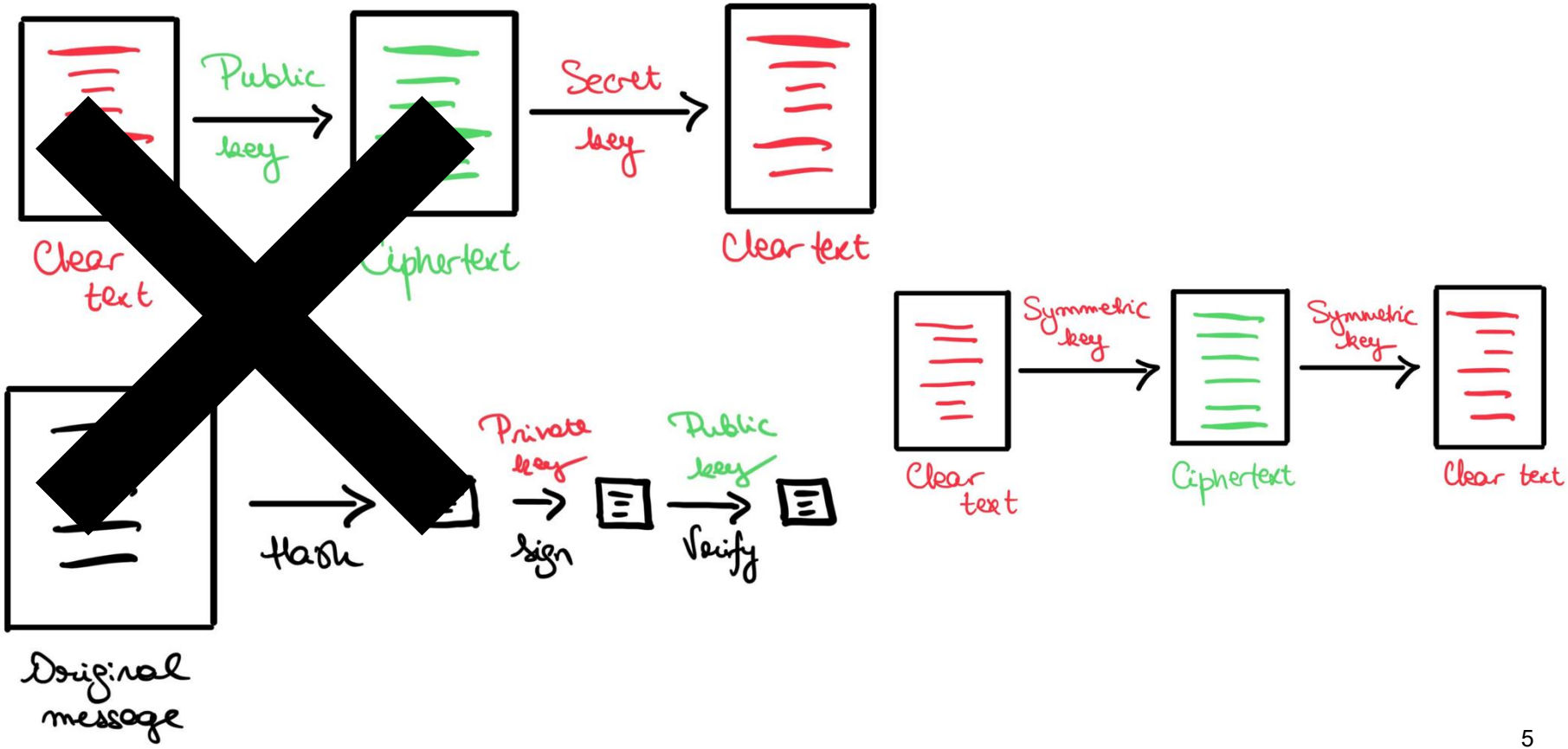
Sikker kommunikasjon:	Signal, WhatsApp, iMessage,…
Sikker tilkobling:	TLS, SSH, IPsec,…
Digital autentisering:	FIDO, Bank ID, EU Wallet,…
Betaling:	PayPal, VISA / Mastercard, Apple / Google Pay, Venmo,…

Vil disse tjenestene være sikre i fremtiden?

Kvantedatamaskiner



Kryptografi i morgen



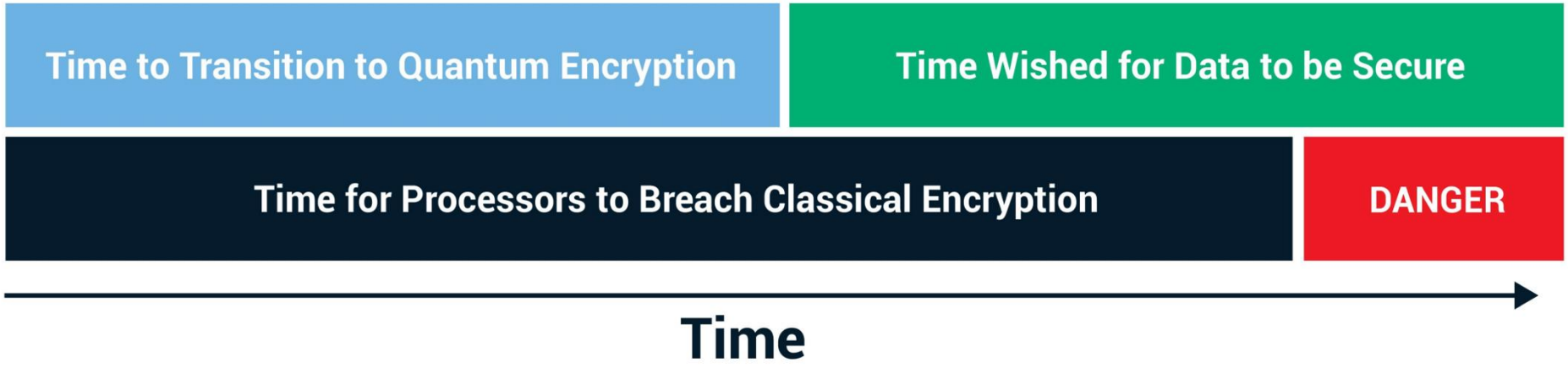
Kvantetrusselen

Kvantedatamaskiner er ikke nødvendigvis bedre; de er forskjellige fra hva vi har i dag og gjør noen ting bedre

De kan i teorien knekke offentlig-nøkkel kryptering og digitale signaturer basert på faktorisering og dlog

Det er mange nylige gjennombrudd innen kvanteberegninger

Urgency: Mosca's Inequality



Don't wait - upgrade your encryption now!

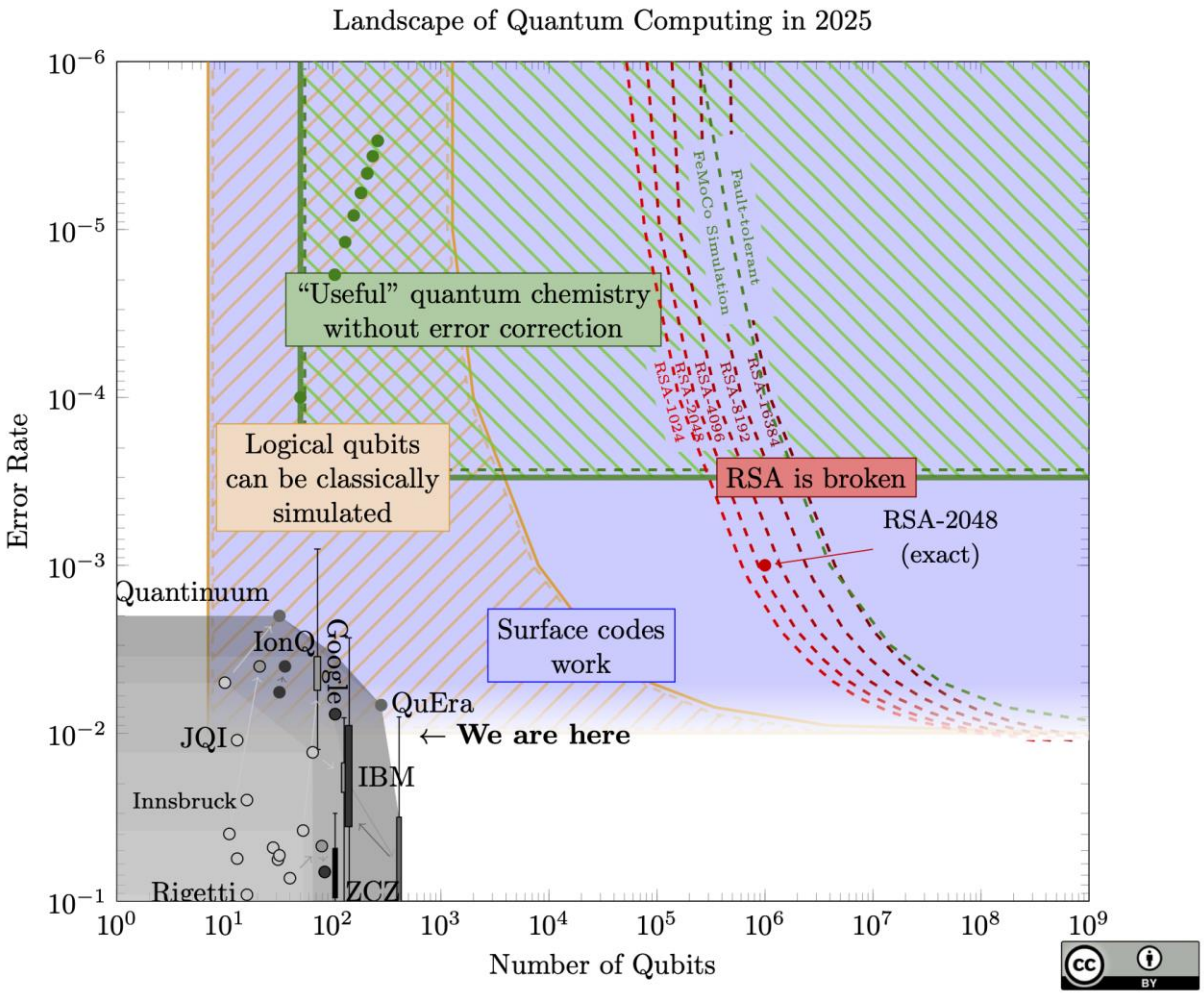
How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.


Landscape of Quantum Computing in 2025
Error Rate
Number of Qubits
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
10^{8}
10^{9}
"Useful" quantum chemistry without error correction
Logical qubits can be classically simulated
Surface codes work
RSA is broken
RSA-2048 (exact)
FeMoCo Simulation
Fault-tolerant
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
Quantinuum
IonQ
Google
QuEra
← We are here
JQI
IBM
Innsbruck
Rigetti
ZCZ

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

FIPS 204

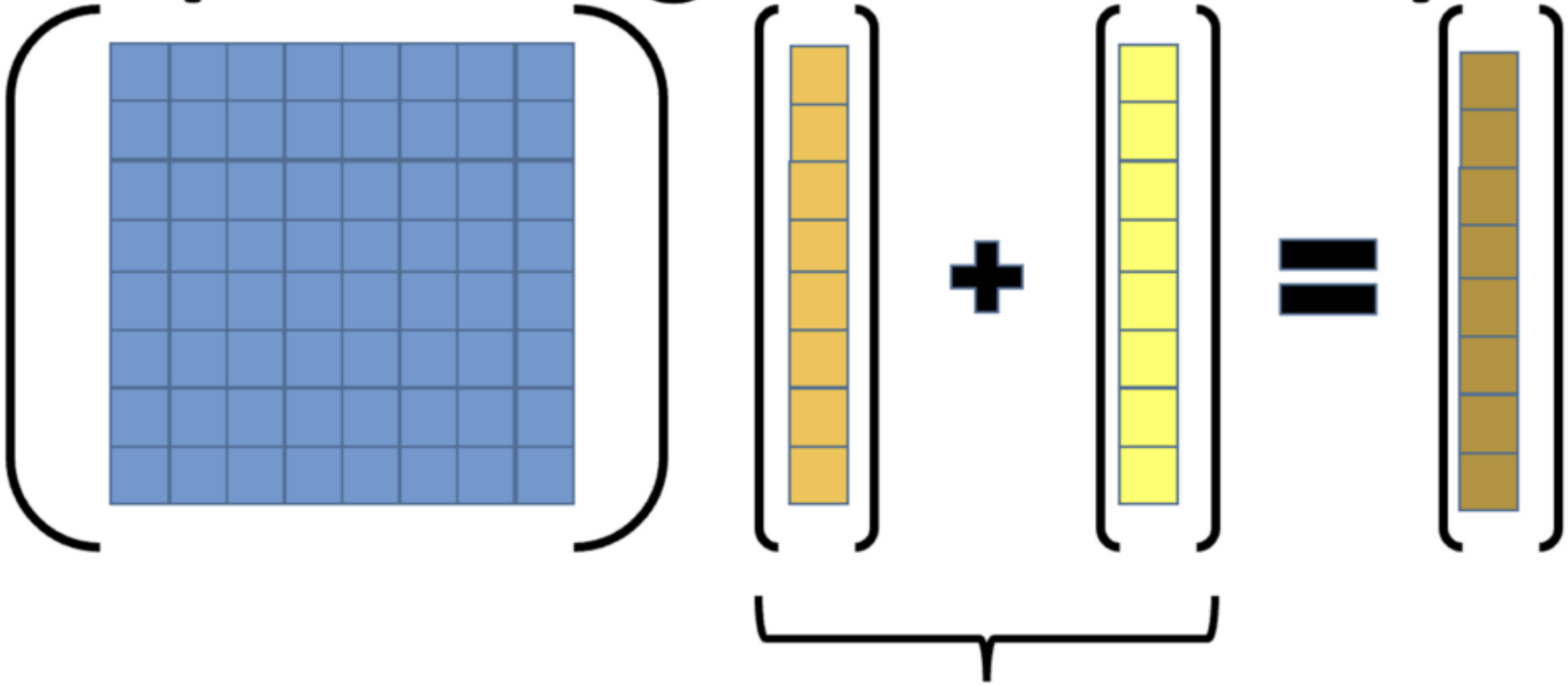
Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

(Learning With Errors)



Small coefficients to enforce uniqueness

Adoption & Usage

Worldwide

Last 7 days

Post-quantum encryption adoption

Post-quantum encrypted share of HTTPS request traffic

Traffic type: Exclude bots

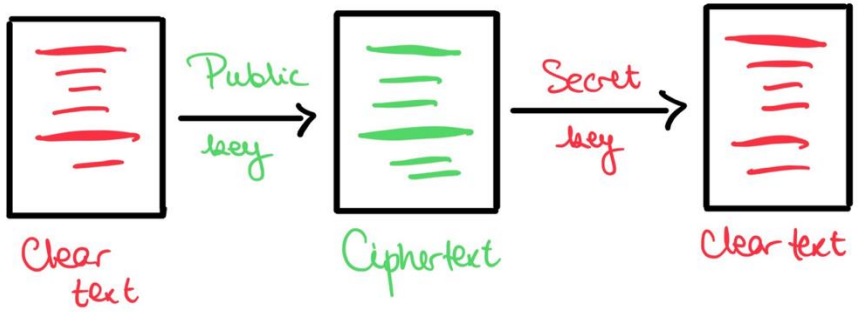
Browser support

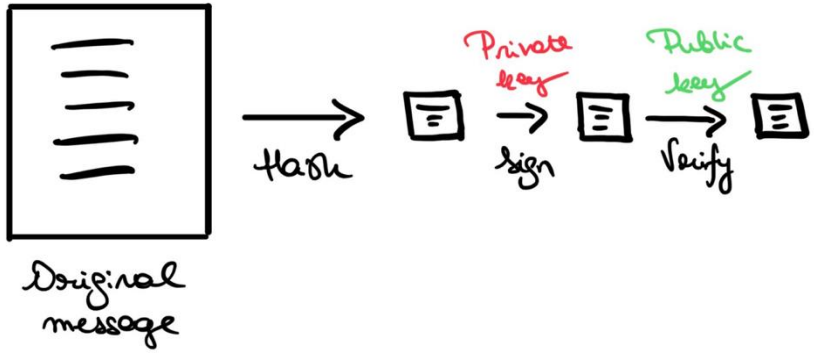
Check your browser for post-quantum encryption support

✓ PQ Your browser is connecting using the *X25519MLKEM768* key agreement, which is post-quantum secure.

Avansert kryptografi

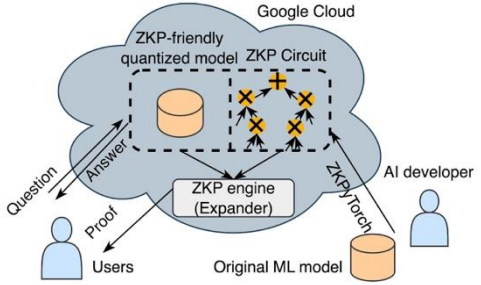
- Nå kan vi erstatte kryptering og signaturer
- Kryptografi benyttes andre steder også!
- Er de kvantesikre?





Personvernapplikasjoner

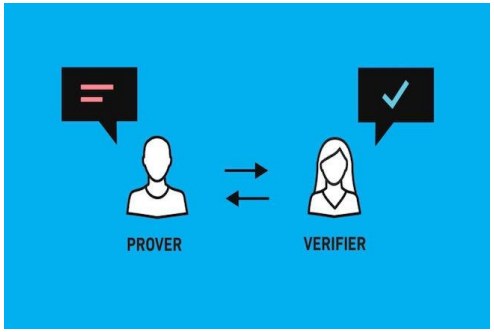
- Anonym smittesporing
- Attribut-basert autentisering
- Konfidensielle transaksjoner
- Personvernbevarende KI
- Verifiserbare beregninger
- Elektronisk valg



Disruptive Personvernteknikker

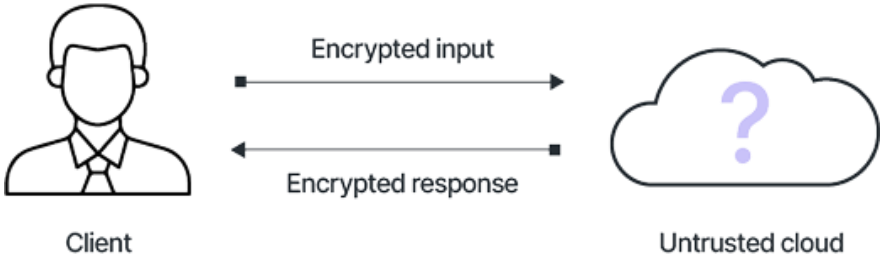
Zero-Knowledge Proofs

- Tillater at man kan **bevise** påstander uten å dele sensitiv informasjon



Homomorfisk Kryptering

- Tillater **beregning** på kryptert informasjon, uten å dele innhold eller nøkkel



Kvantesikkerhet?

Zero-Knowledge Proofs

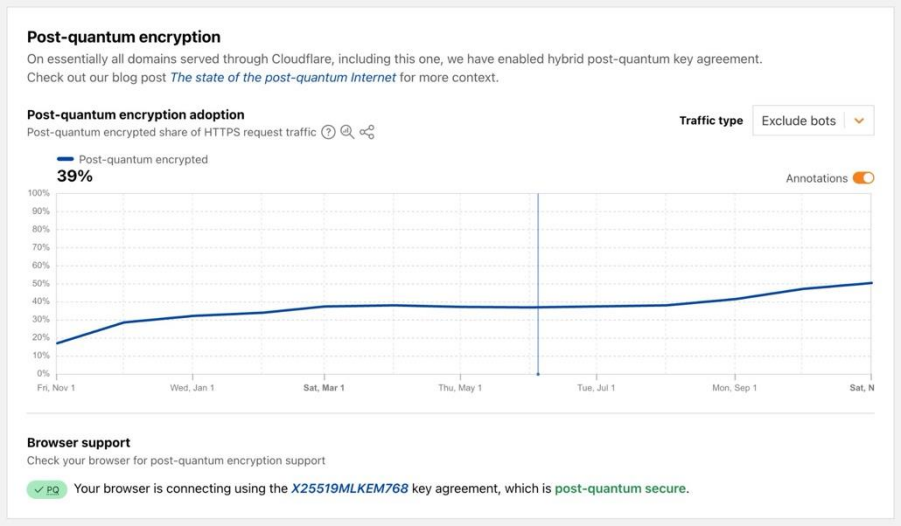
- Kan bygges fra latticer, samme matematiske problemer som nye kvantesikre standarder
- Er mer komplekse enn dagens ZK-systemer

Homomorfisk Kryptering

- Kan (tilfeldigvis) bare bygges fra latticer, som allerede er kvantesikre
- Finnes flere startups, og åpen kildekode begynner å bli klar for produksjon

Veien videre

- Symmetrisk kryptering
- Offentlig-nøkkel krypto
- Avanserte primitiver



- En stor jobb å bytte til kvantesikre algoritmer
- Må videreutvikle de avanserte primitivene
- PQC >> QKD