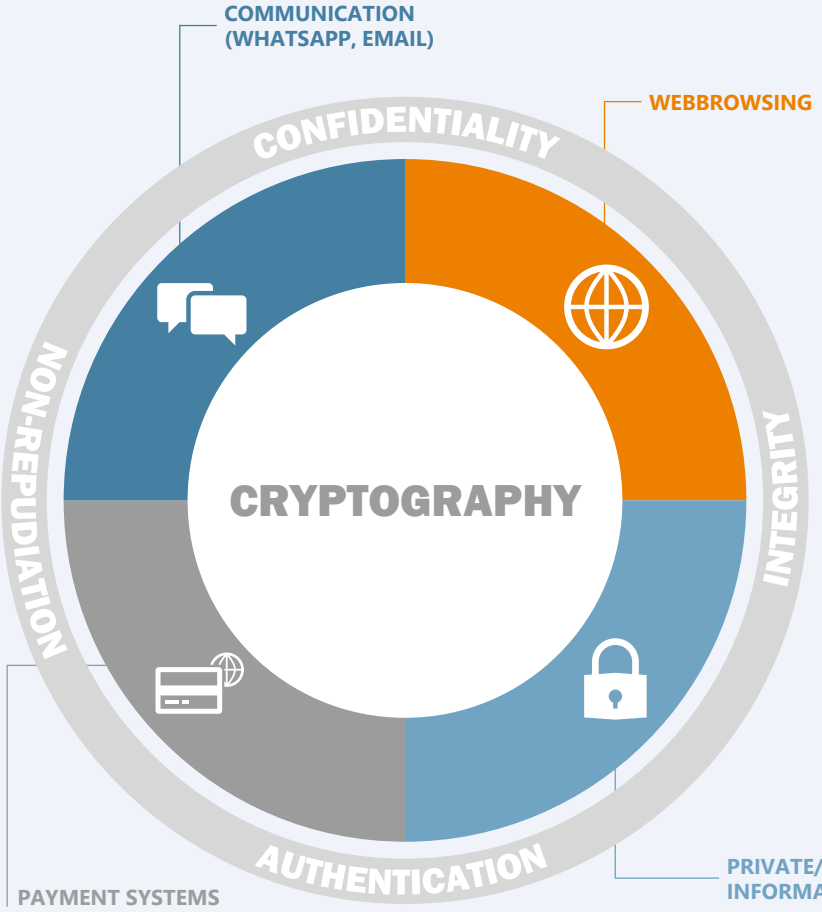
De Dreiging van Quantum Computers

Thomas Attema

25 Maart 2025

Cryptografie is Overal
- Het beschermt onze communicatie kanalen



CODEMAKERS

VS

CODEKRAKERS

NIET-STANDAARD HIËROGLIEFEN

300 AD

1900 BC

CAESAR CIPHER

800 AD

60 BC

VIGENÈRE CIPHER

1863

1553

“LE CHIFFRE INDÉCHIFFRABLE”

ENIGMA-CODE

1945

1923

RSA

HEDEN

1978

SHOR'S QUANTUM ALGORITME

1994

QUANTUM COMPUTER

2030/2040/
2050/???

NU

CODEMAKERS

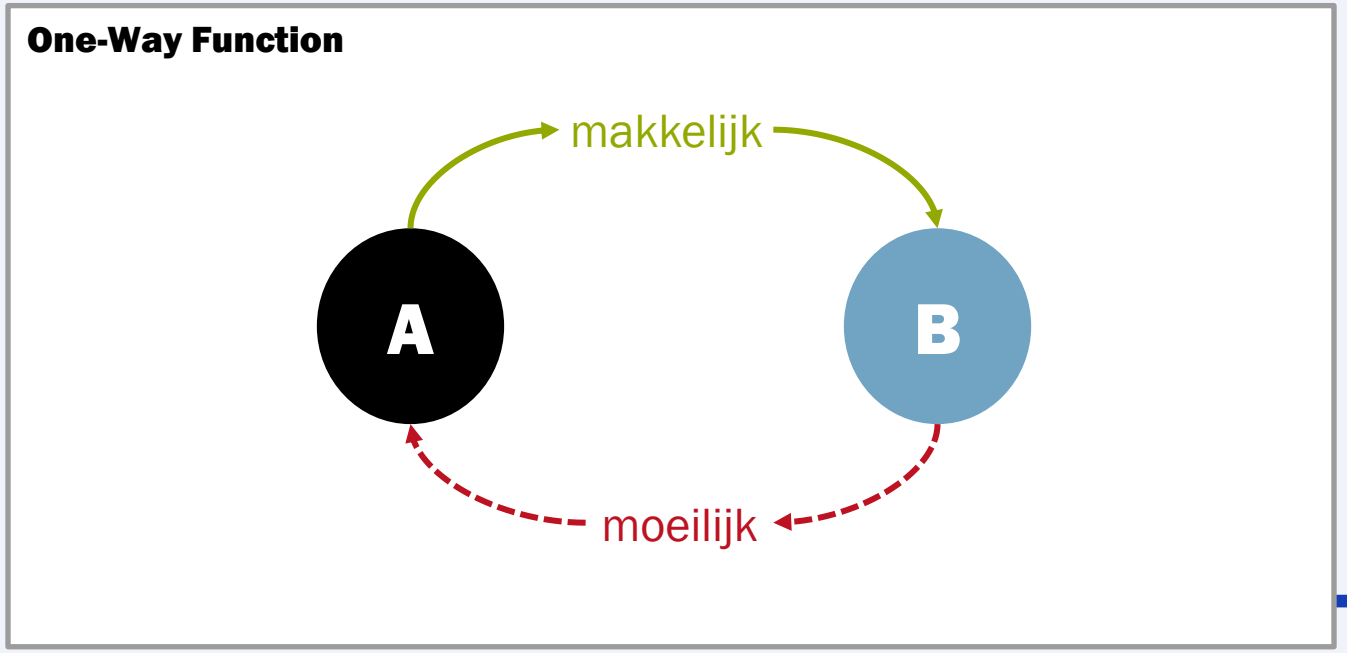
vs

CODEKRAKERS

Het Huidide Hoofdstuk
Post-Quantum Cryptografie

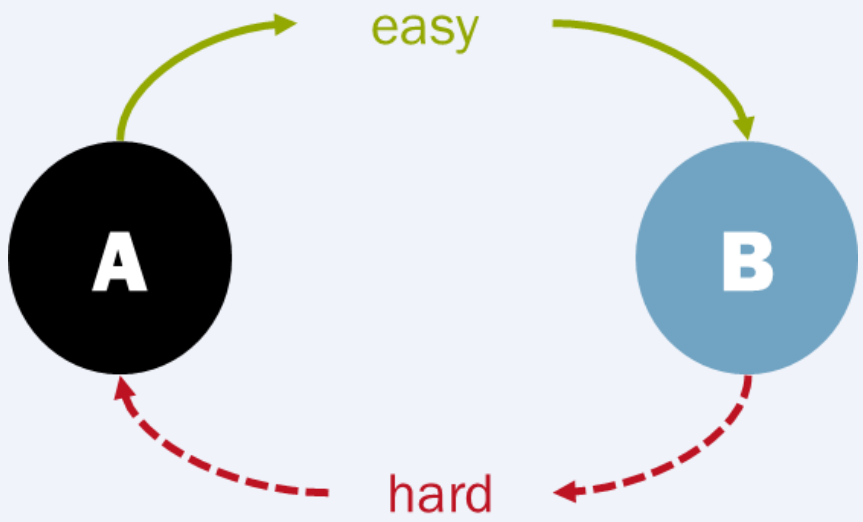
Cryptografische Protocollen Ontwerpen

- Versleutelen moet eenvoudig zijn (efficiënt)
- Ontsleutelen ***met*** de geheime sleutel moet eenvoudig zijn
- Ontsleutelen ***zonder*** de geheime sleutel moet extreem moeilijk zijn



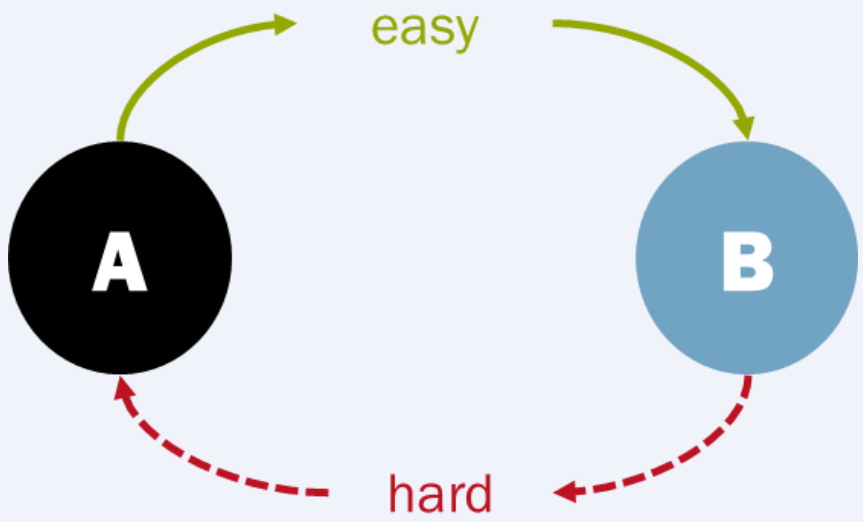
Voorbeeld: Factoriseren

- Vermenigvuldigen is makkelijk:
  - $7 \times 13 = 91$
  - $67 \times 83 = 5561$
  - $27\,277 \times 35\,527 = 969\,069\,979$
- Maar het omgekeerde (factoriseren) is moeilijk:
  - $57 = ? \times ?$



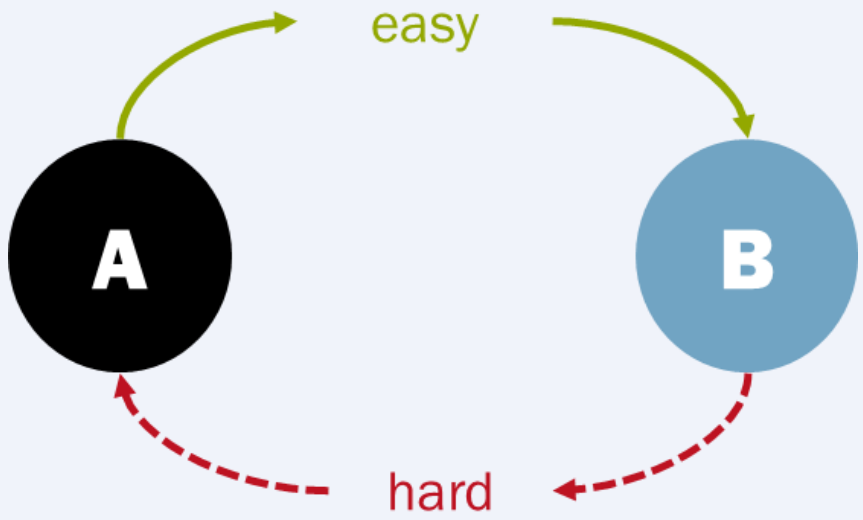
Voorbeeld: Factoriseren

- Vermenigvuldigen is makkelijk:
  - $7 \times 13 = 91$
  - $67 \times 83 = 5561$
  - $27\,277 \times 35\,527 = 969\,069\,979$
- Maar het omgekeerde (factoriseren) is moeilijk:
  - $57 = 3 \times 19$
  - $4171 = ? \times ?$



Voorbeeld: Factoriseren

- Vermenigvuldigen is makkelijk:
  - $7 \times 13 = 91$
  - $67 \times 83 = 5561$
  - $27\,277 \times 35\,527 = 969\,069\,979$
- Maar het omgekeerde (factoriseren) is moeilijk:
  - $57 = 3 \times 19$
  - $4171 = 43 \times 97$
  - $1.370.842.307 = ? \times ?$



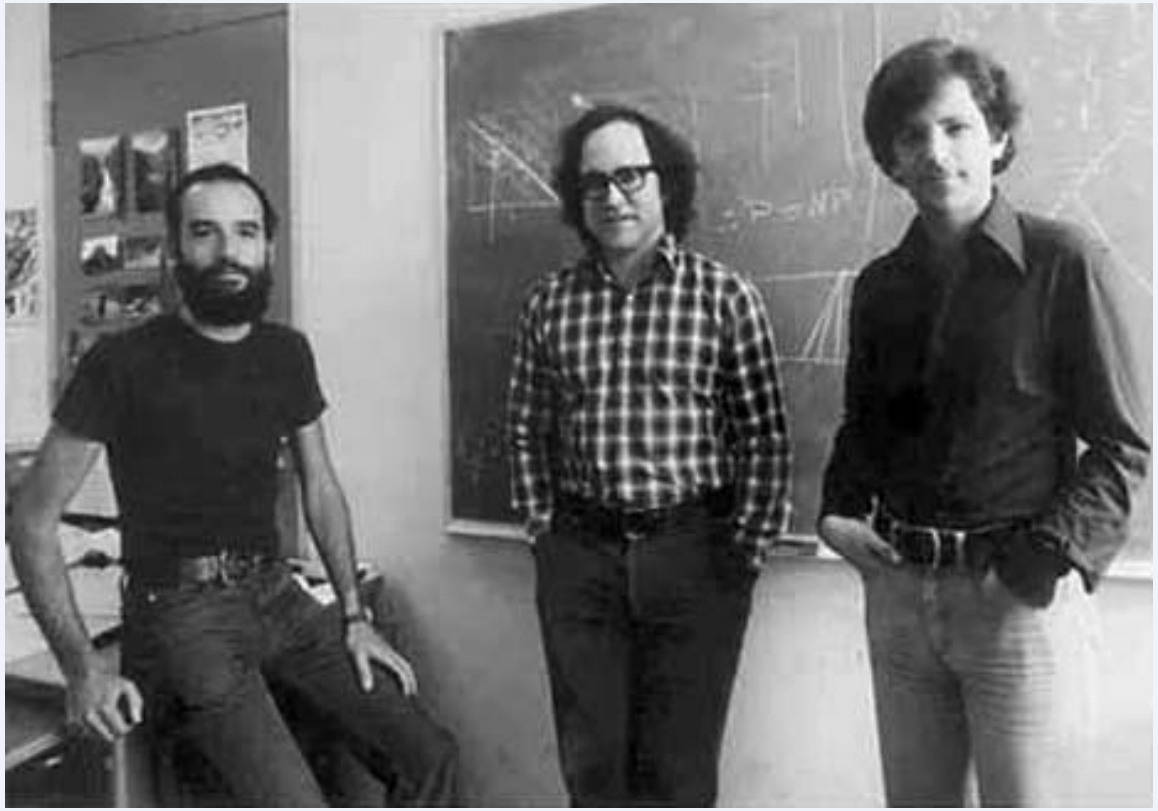
Cryptografische Protocollen Ontwerpen

- RSA versleuteling bouwt op de moeilijkheid van factoriseren (1978)

- Meestal weten we niet hoe we veiligheid kunnen bewijzen
  - Veiligheid is dan een (goed onderbouwde) ***aanname***

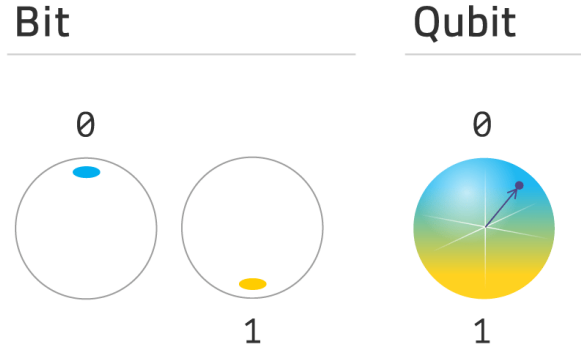
- Daarom is cryptanalyse cruciaal
  - Aannames omver helpen => onveilige schema's identificeren
  - Veiligheid kwantificeren => selecteer sleutelgroottes

- Veel jaren aan cryptanalyse zijn nodig om **vertrouwen** in cryptografie op te bouwen



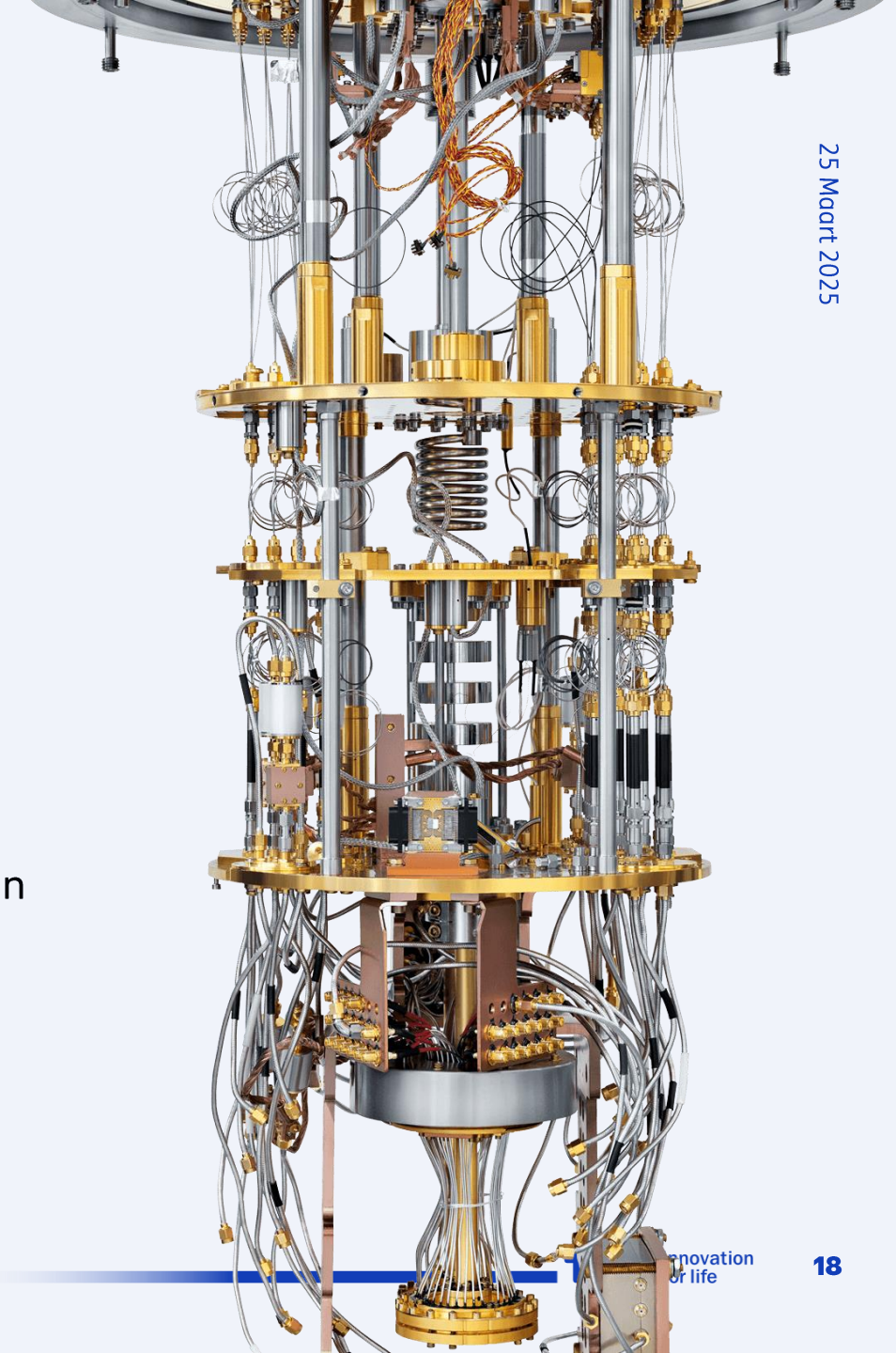
Quantum Computers

- Fundamenteel andere manier van rekenen
- Gebruikt qubits i.p.v. bits



- Verschillende uitdagingen: coherence, stability, scalability, error-correction
- Herdefinieerd welke problemen moeilijk zijn

Quantum computer ≠ Supercomputer



De Quantum Dreiging

Shor's algoritme (1994)

- Gebruikt Quantum Fourier Transformatie om periodes te vinden
- (Sub)exponentiële versnelling t.o.v. klassieke computers
- Breekt publieke sleutel cryptografie met een bepaalde structuur

Factoriseren
&
Discrete Logaritme

Grover's algoritme (1996)

- Ongestructureerd zoeken in databases
- Versnelling van brute force aanvallen

Key Search

Quantum Computing – State of the Art

NEWS | 23 October 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

DECEMBER 9, 2024 Editors' notes

Google's new quantum chip hits error correction target

by Nature Publishing Group

TECH

Satya Nadella explains why Microsoft's quantum 'breakthrough' is so important

Katherine Tangalakis-Lippert Feb 20, 2025, 2:54 AM GMT+1 Share Save

State of the Art – Een Aantal Nuances

Quantum Computing Remains Experimental Despite 2024 Advances: Forrester

By John P. Mello Jr. • January 6, 2025 5:00 AM PT • Email Article

Markets

Practical Use Of Quantum Computers 20 Years Away: Nvidia Chief

January 9, 2025

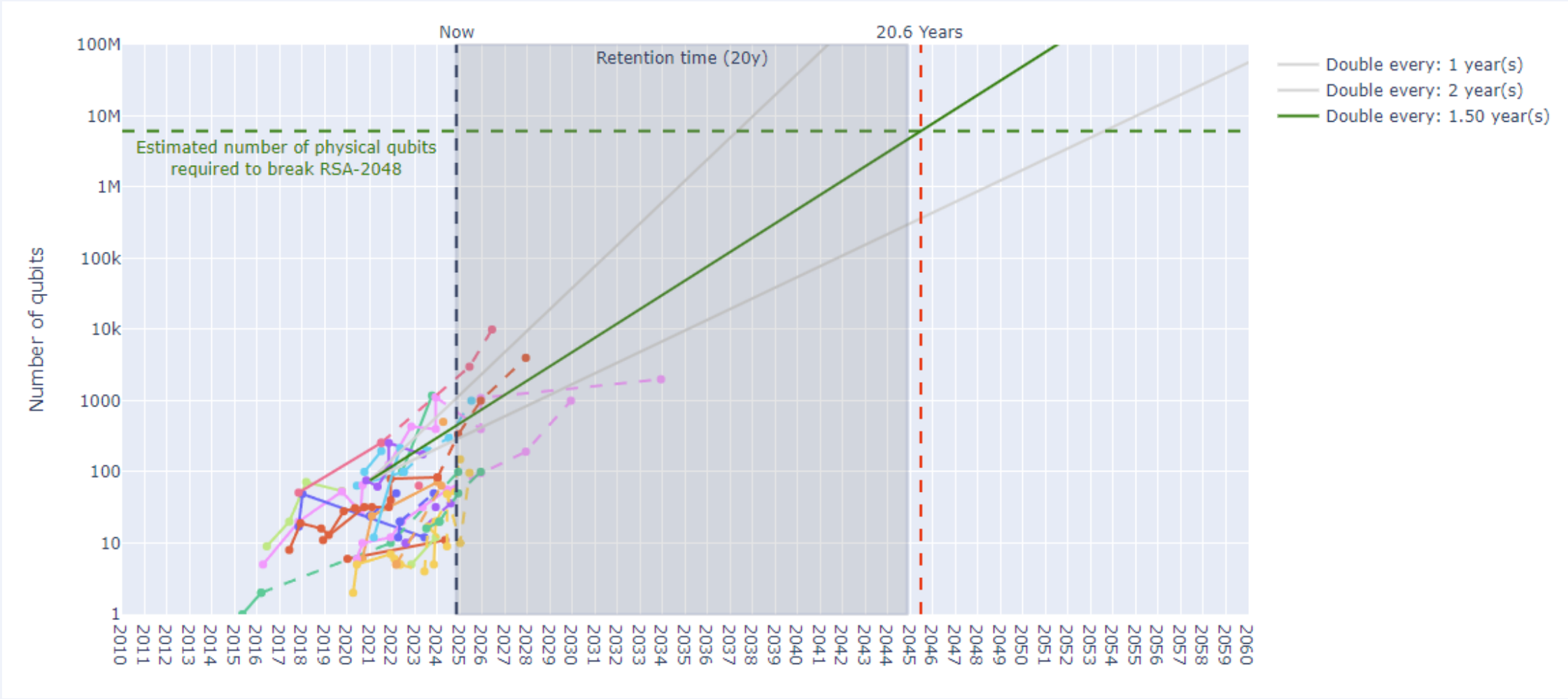
Huang's statements triggered an $8 billion meltdown in the four biggest quantum computing shares in the US

Google CEO: Practical quantum computers likely still a decade away

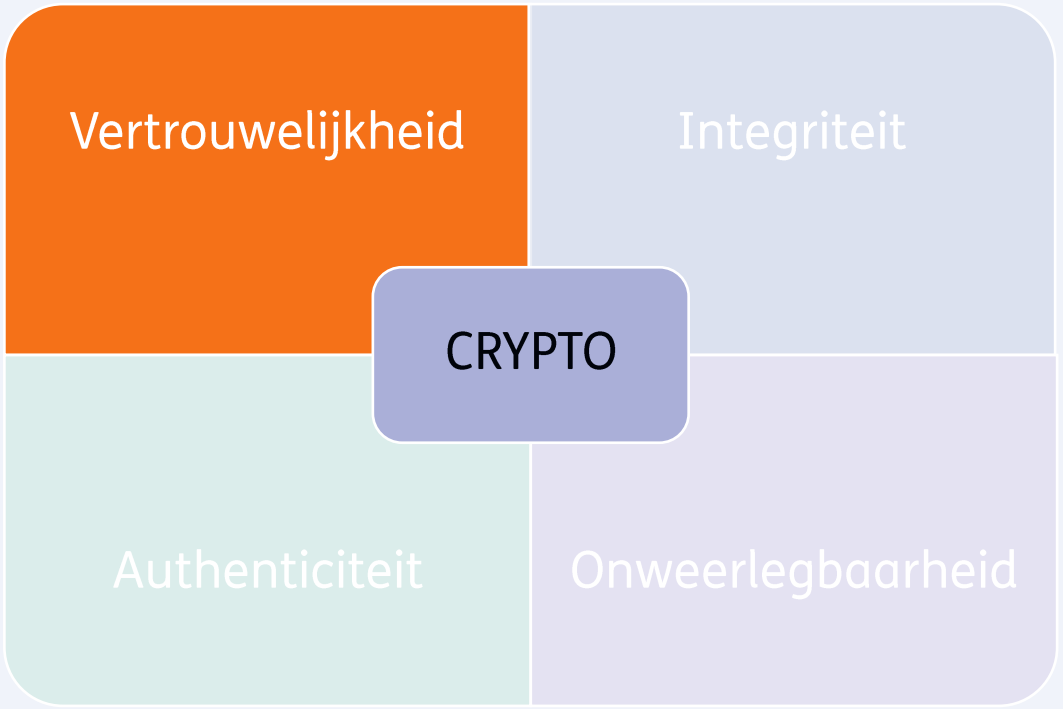
Comments follow debut of Google's Willow quantum chip late last year

February 15, 2025 By: Charlotte Trueman Have your say

Quantum Computing – State of the Art



Urgentie - Store Now Decrypt Later Attack

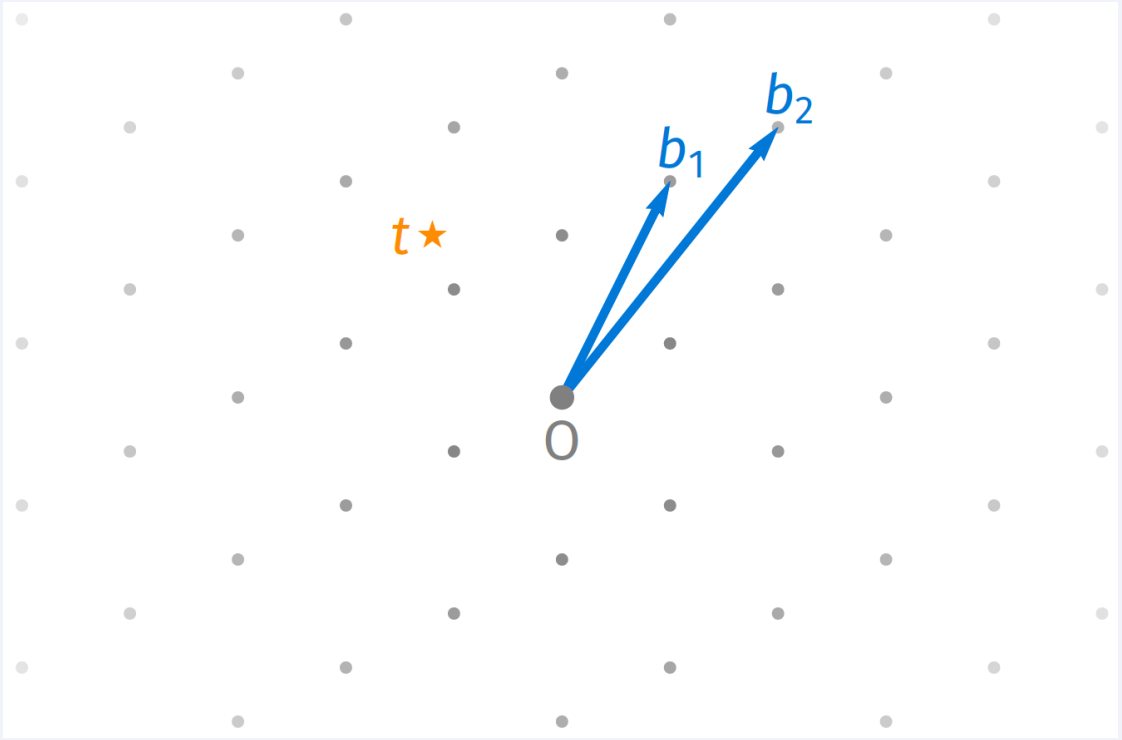


Post-Quantum Cryptografie

- Cryptografie veilig tegen quantum aanvallers

- Gebaseerd op wiskundige problemen
  - (aangenomen) moeilijk zelfs voor quantum computers

- Verschillende wiskundige platforms:
  - Lattices
  - Hash-Based
  - Codes
  - Multivariate
  - Isogenies
  - …



NIST Post-Quantum Standaardisatie Competitie

Tijdslijn (2016 – present)

- **2016:** NIST call geopend
- **2017:** Ronde 1: 69 kandidaten
- **2019:** Ronde 2: 26 kandidaten
- **2020:** Ronde 3: 7 finalisten, 8 alternatieven
- **2022**: Bekendmaking van
  - 4 winnaars (1 KEM, 3 SIG)
  - 4 alternatieven voor Ronde 4 (KEMs)
  - Nieuwe competitie voor aanvullende SIG
- **2023**: Eerste concept standaarden
- **2024**: Eerste standaarden (3 out of 4)
- **Maart 11, 2025**: Alternatieve KEM geselecteerd (HQC)
- **Later:** Vierde digitale handtekening
- **Gaande:** Competitie voor extra digitale handtekening

Standaardisatie: Niet eenvoudig!

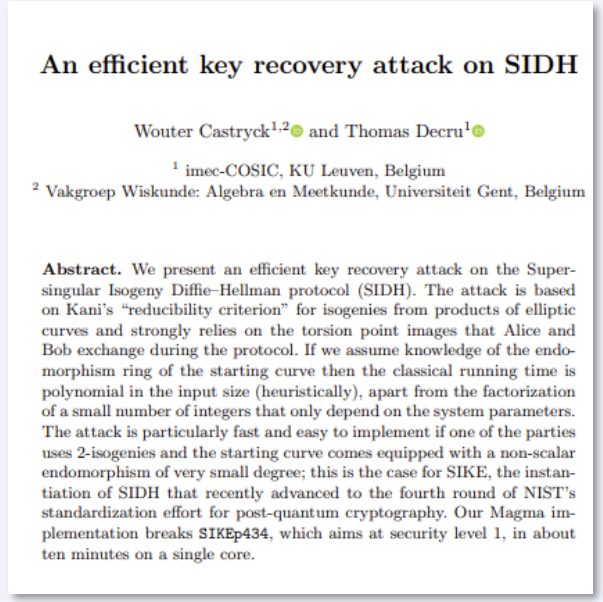
- NIST Standaardisatie startte al in 2016
- Onderzoekers wereldwijd hebben de veiligheid sindsdien bestudeerd, toch:

Juli 2022

- SIKE volledig **gebroken** nadat het in de vierde ronde terecht was gekomen
- Verrassend: 6 jaar (!) na de start van de NIST competitie

December 2023

- *KyberSlash:* Side-channel aanval op Kyber
- Geen fundamentele kwetsbaarheid => implementatie bleek onveilig

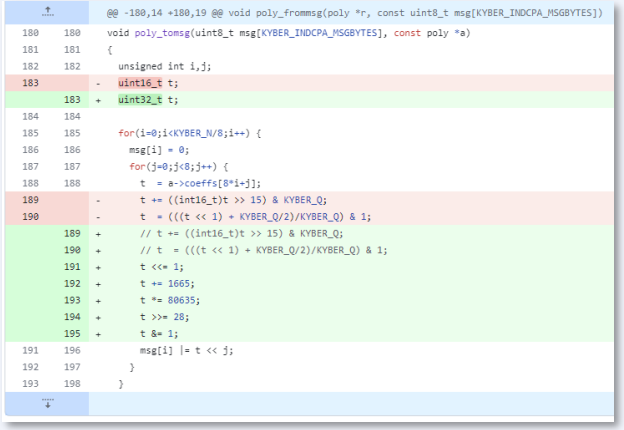


An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

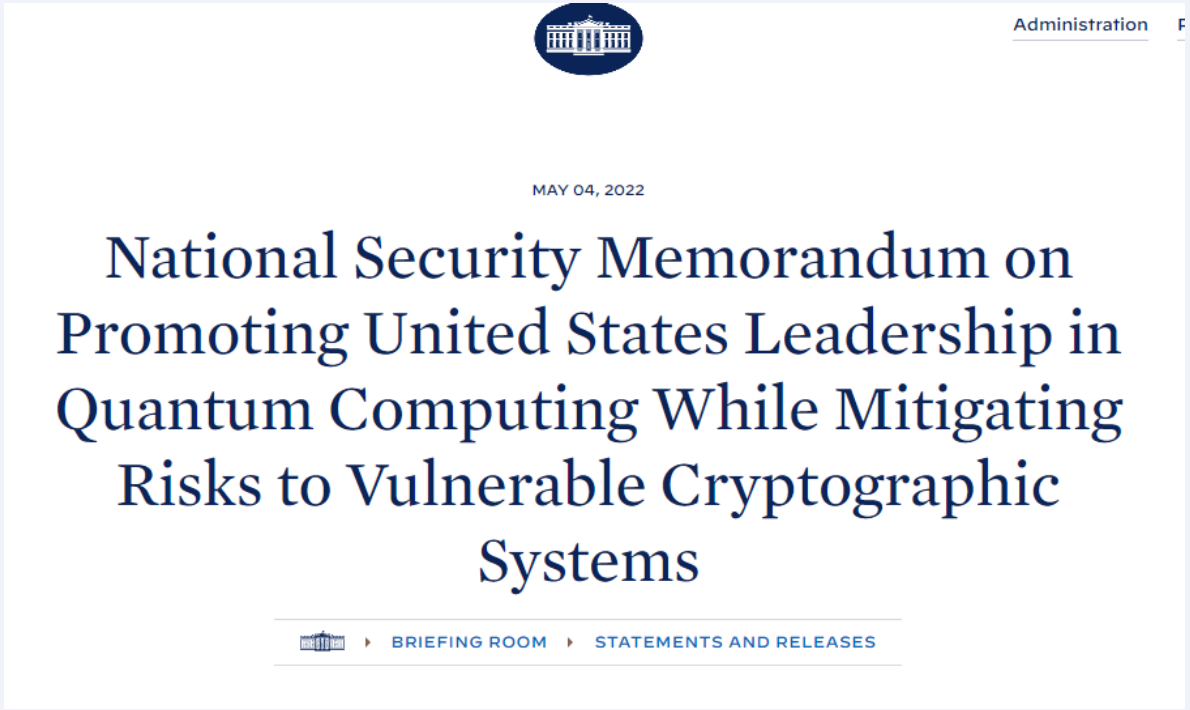
Abstract. We present an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman protocol (SIDH). The attack is based on Kani's "reducibility criterion" for isogenies from products of elliptic curves and strongly relies on the torsion point images that Alice and Bob exchange during the protocol. If we assume knowledge of the endomorphism ring of the starting curve then the classical running time is polynomial in the input size (heuristically), apart from the factorization of a small number of integers that only depend on the system parameters. The attack is particularly fast and easy to implement if one of the parties uses 2-isogenies and the starting curve comes equipped with a non-scalar endomorphism of very small degree; this is the case for SIKE, the instantiation of SIDH that recently advanced to the fourth round of NIST's standardization effort for post-quantum cryptography. Our Magma implementation breaks **SIKEp434**, which aims at security level 1, in about ten minutes on a single core.



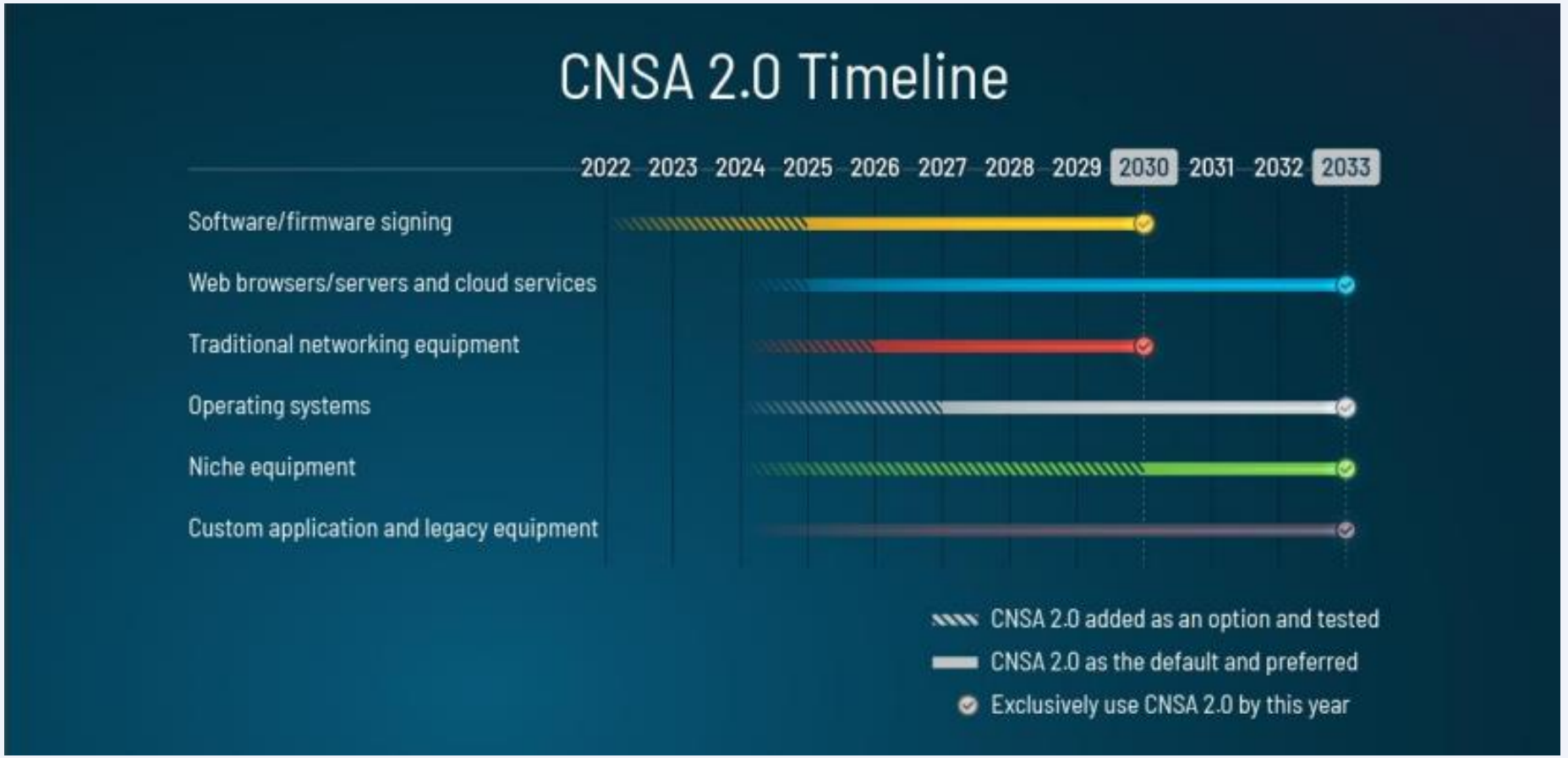
```
@@ -180,14 +180,19 @@ void poly_frommsg(poly *r, const uint8_t msg[KYBER_INDCPA_MSGBYTES])
180 180  void poly_tomsg(uint8_t msg[KYBER_INDCPA_MSGBYTES], const poly *a)
181 181  {
182 182    unsigned int i,j;
183     -  uint16_t t;
    183 +  uint32_t t;
184 184
185 185    for(i=0;i<KYBER_N/8;i++) {
186 186      msg[i] = 0;
187 187      for(j=0;j<8;j++) {
188 188        t  = a->coeffs[8*i+j];
189     -      t += ((int16_t)t >> 15) & KYBER_Q;
190     -      t  = (((t << 1) + KYBER_Q/2)/KYBER_Q) & 1;
    189 +      // t += ((int16_t)t >> 15) & KYBER_Q;
    190 +      // t  = (((t << 1) + KYBER_Q/2)/KYBER_Q) & 1;
    191 +      t <<= 1;
    192 +      t += 1665;
    193 +      t *= 80635;
    194 +      t >>= 28;
    195 +      t &= 1;
191 196        msg[i] |= t << j;
192 197      }
193 198    }
```

Mei 2022: US White-House Memorandum

- *“It directs specific actions for agencies to take as the United States begins the multi-year process of migrating vulnerable computer systems to quantum-resistant cryptography”*



Tijdslijnen voor de PQC-Migratie van “US National Security Systems”



UK National Cyber Security Center – Tijdslijnen voor de PQC-migratie

- Gepubliceerd op 20 Maart, 2025

- Voor UK industrie, overheid en toezichthouders, but voornamelijk:
  - Grote organisaties;
  - Kritieke infra;
  - Bedrijven met ‘custom’ IT oplossingen.

The key milestones are:

By 2028

- Define your migration goals
- Carry out a full discovery exercise (assessing your estate to understand which services and infrastructure that depend on cryptography need to be upgraded to PQC)
- Build an initial plan for migration

By 2031

- Carry out your early, highest-priority PQC migration activities
- Refine your plan so that you have a thorough roadmap for completing migration

By 2035

- Complete migration to PQC of all your systems, services and products

Nederland

Alle systemen quantumveilig voor 2030?

De staatssecretaris wil dat alle systemen voor 2030 quantumveilig zijn, maar veel lokale overheden hebben nog geen idee hoe.

Thijs Doorenbosch 17 maart 2025

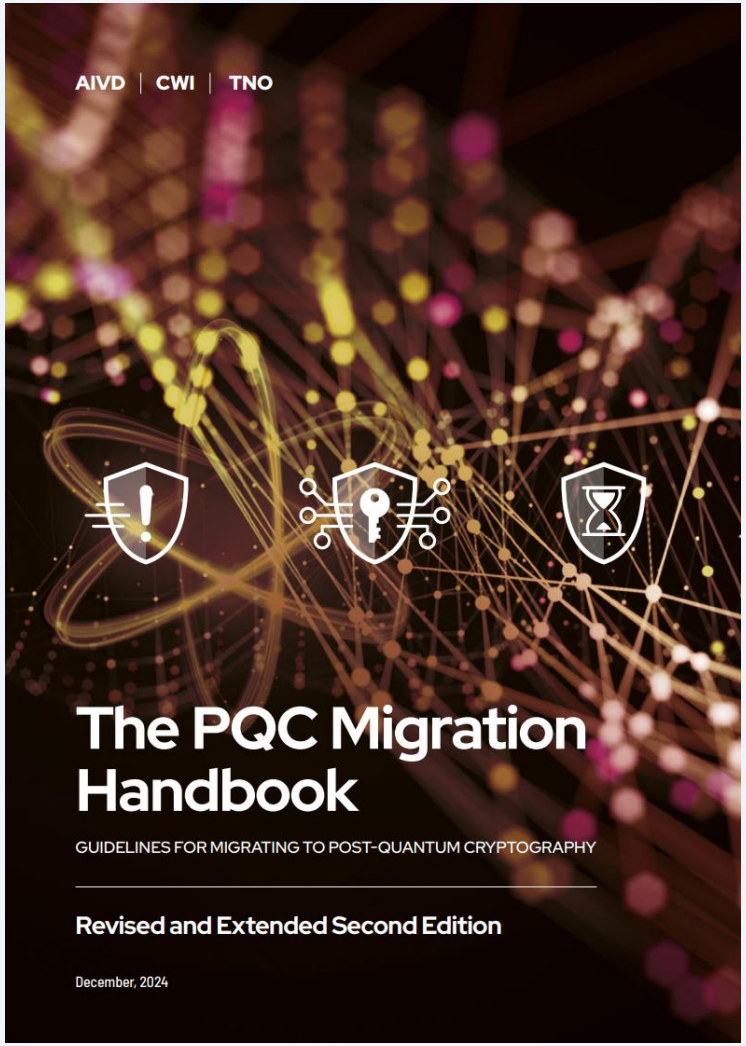
Migreren naar PQC is Uitdagend

Technische uitdagingen:

- **Karakteristieken** - Post-quantum cryptografie is anders
- **Diversiteit** – Meer verschillende crypto om uit te kiezen
- **Risico's –** Wat als nieuwe crypto onveilig blijkt?
- **Wendbaarheid** – Het is waarschijnlijk dat er nog meer migraties komen
- …

Niet-Technische Uitdagingen:

- Juridisch
- Organisatorisch
- Interoperabiliteit
- Supply-chain afhankelijkheden
- …



Een Eerste Stap – Cryptographic Asset Discovery

- Welke cryptografie gebruik je waar? En voor welk doel?

Cryptography is everywhere, e.g.:

- Libraries (applications, OS)
- Middleware (IPsec (VPNs), ..)
- Hosts (IoT, smartcards, applications, printers, routers,..)
- Containers (Docker, VMs)
- Hardware (HSM, smartcards, tokens, servers, laptops, BYOD (onboarding), physical vaults, …)
- Hardware root-of-trust (hardware-fused keys, PUFs, (T)RNG, …)
- Infrastructure (?)
- Networks (end-points, DNS, application servers of specific appliances …)
- Cloud
- Security infra (IDS, firewalls, …)
- Internal communication
  - Email encryption and signatures, VPN
- Application vs infrastructure

PQC Migration – De Drie Stappen van ETSI

1. **Diagnose**
   - Bepaal jouw positie in de PQC Migratie
   - PQC inventarisatie

2. **Planning**
   - Wanneer?
   - Hoe?

3. **Uitvoering**
   - Bepaal migratie per cryptografie toepassing
   - Algemene strategieën zoals hybrides en pre-shared keys
   - Cryptografische wendbaarheid

De Migratie is al Begonnen

Apple Unveils PQ3 Protocol - Post-Quantum Encryption for iMessage

Feb 22, 2024 Newsroom Quantum Computing / Encryption

HARDWARE > QUANTUM | September 22, 2023

Signal adds quantum-resistant encryption to its protocol

The update is available in the latest release of the Signal client and will be a requirement for all chats in the future.

Tuta Mail adds new quantum-resistant encryption to protect email

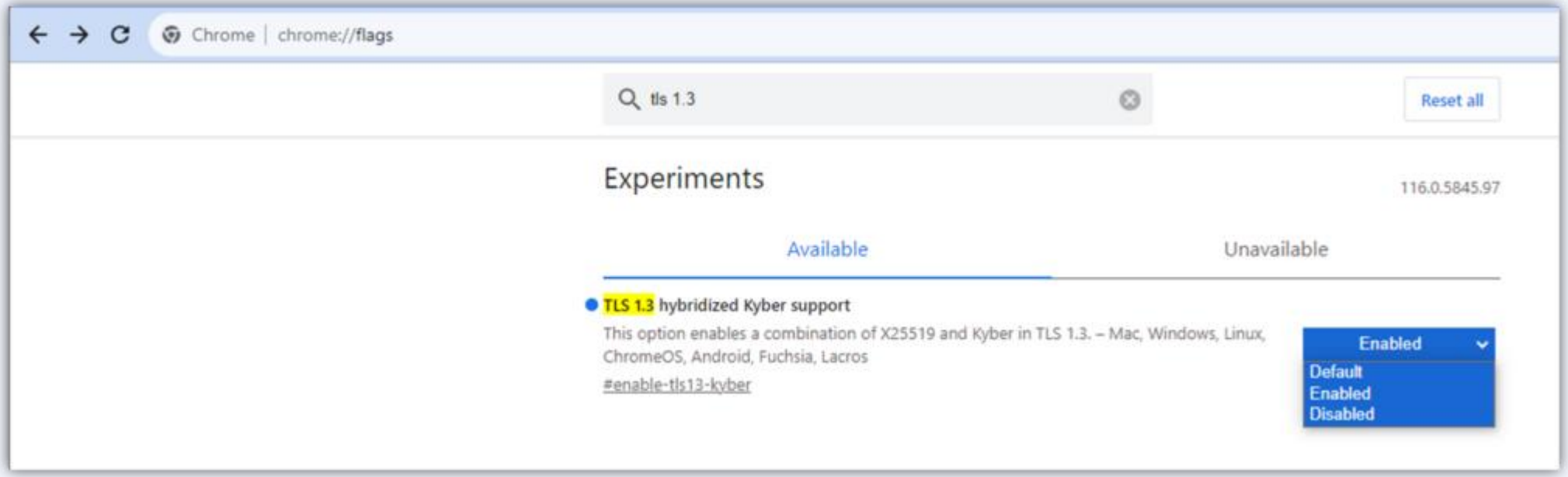
By Bill Toulas March 11, 2024 05:21 PM 2

De Migratie is al Begonnen

Security & Identity

Securing tomorrow today: Why Google now protects its internal communications from quantum threats

November 19, 2022



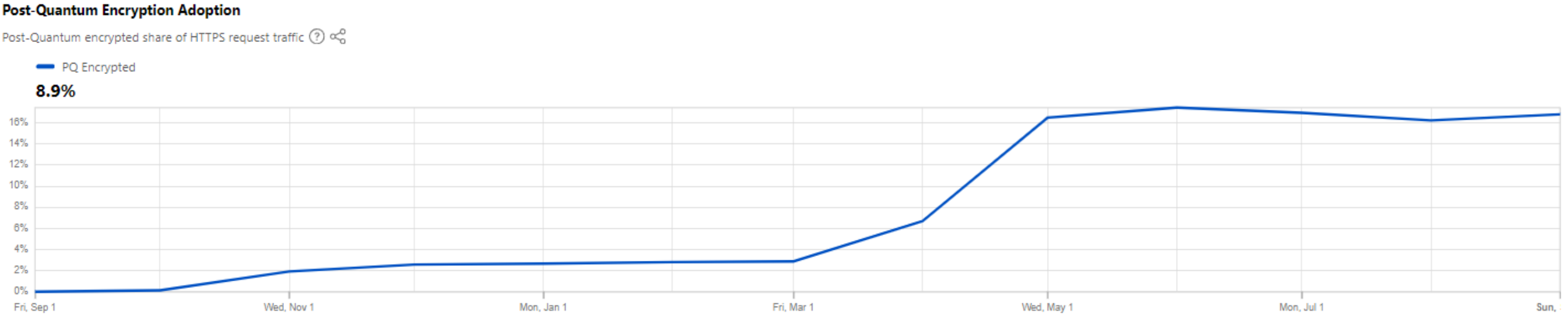
De Migratie is al Begonnen

Defending against future threats: Cloudflare goes post-quantum

10/03/2022


Bas Westerbaan


Cefan Daniel Rubin



Technische Uitdagingen

- PQ digitale handtekeningen zullen waarschijnlijk een grotere performance impact hebben impact
- Implementatie veiligheid
  - E.g., backdoors voorkomen
- Side-channel weerbaarheid
- PQC voor resource constraint omgevingen (e.g., IoT)
- Supply chain veiligheid
- Meer geavanceerde cryptografie
  - E.g., threshold cryptografie

Conclusie

- De PQC Migratie is al begonnen, we kunnen niet achter blijven.
  - Zelfs als je gelooft dat quantum computers nooit crypto zullen breken.

- Een deel van de migratie is makkelijk, e.g., updaten van TLS.
  - Maar er is nog een lange staart aan cryptografische toepassingen die moeilijk te migreren zijn.

- De PQC Migratie biedt de kans om de cryptografische hygiëne te verbeteren.
  - E.g., cryptografische wendbaarheid.

Bedankt!

Vragen?