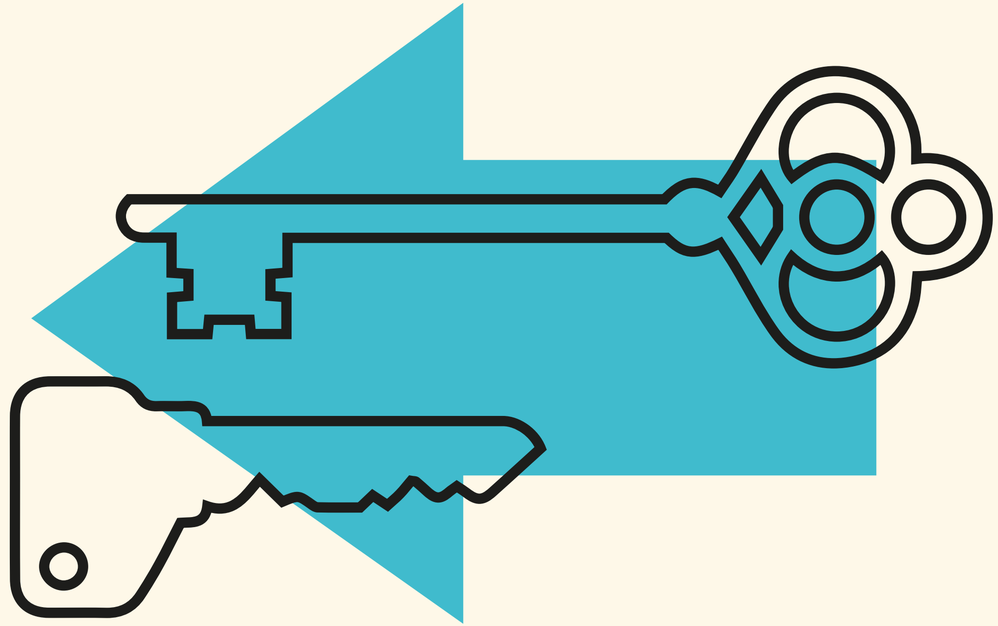
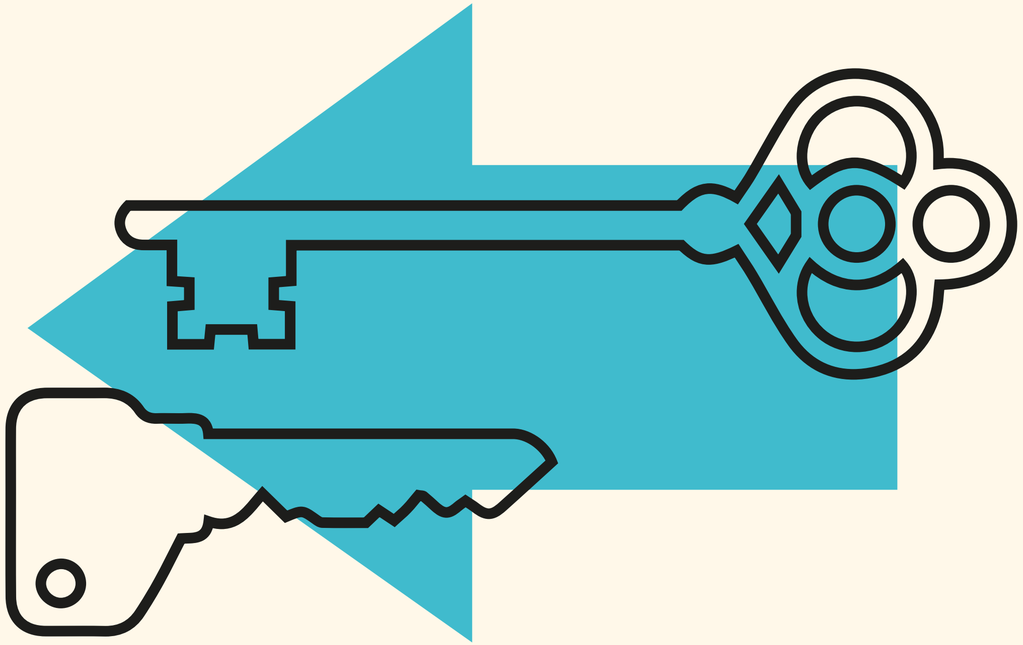
POST-QUANTUM TLS

THOM WIGGERS

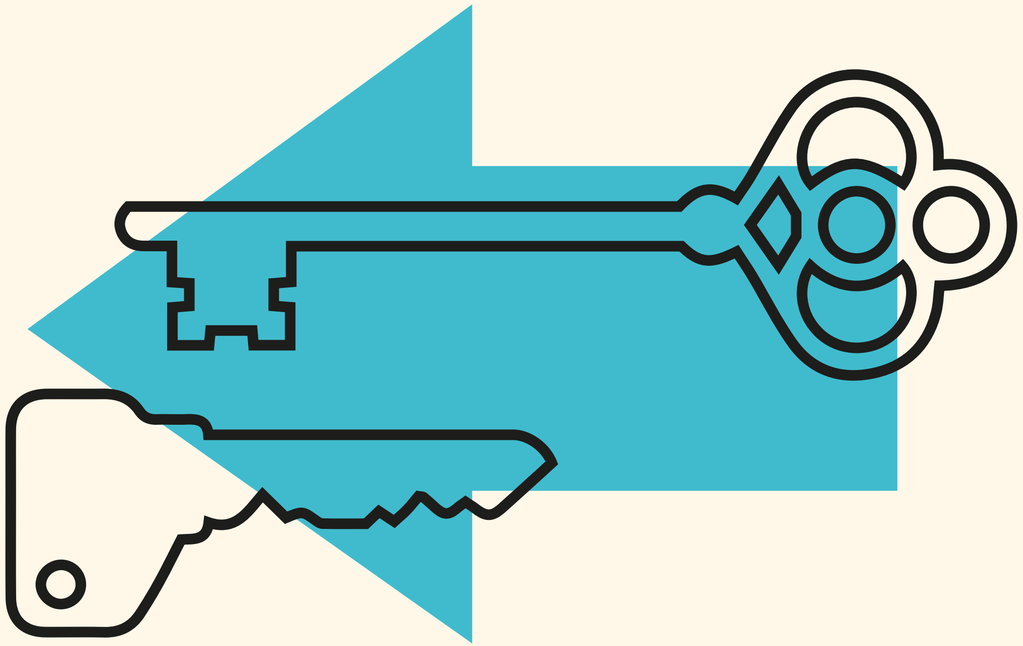


PhD Defense 2024-01-09 14.30

POST-QUANTUM TLS

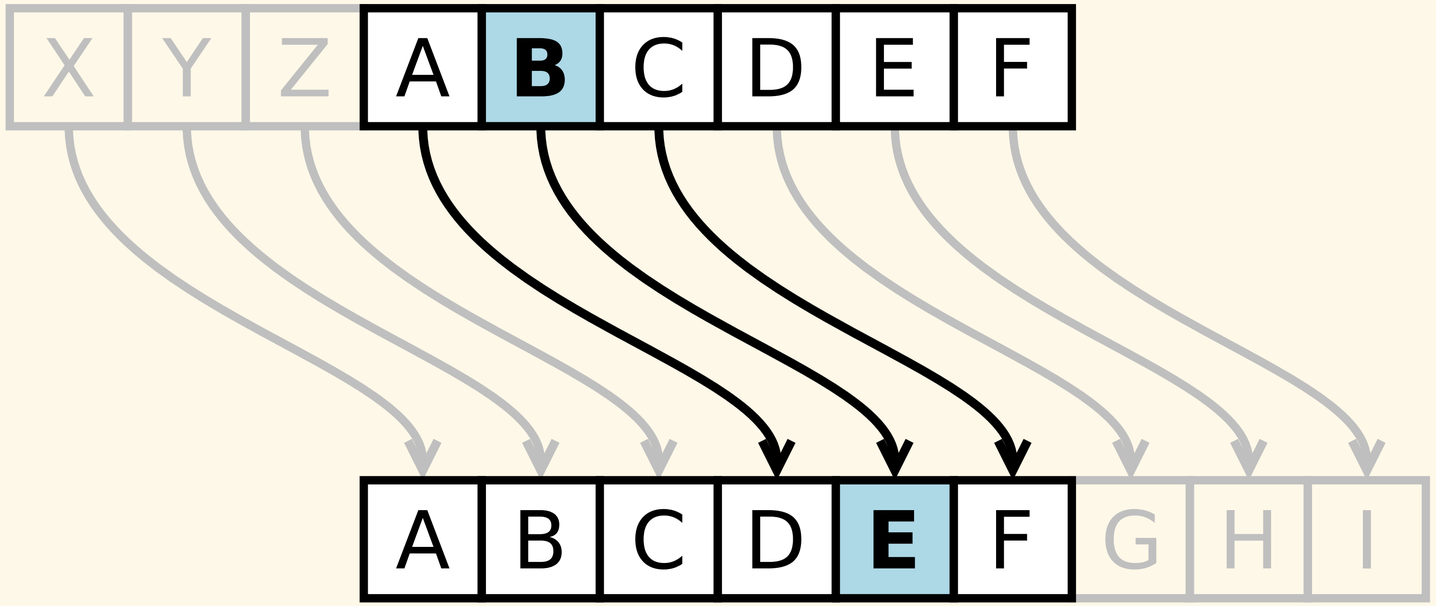


POST-QUANTUM TLS

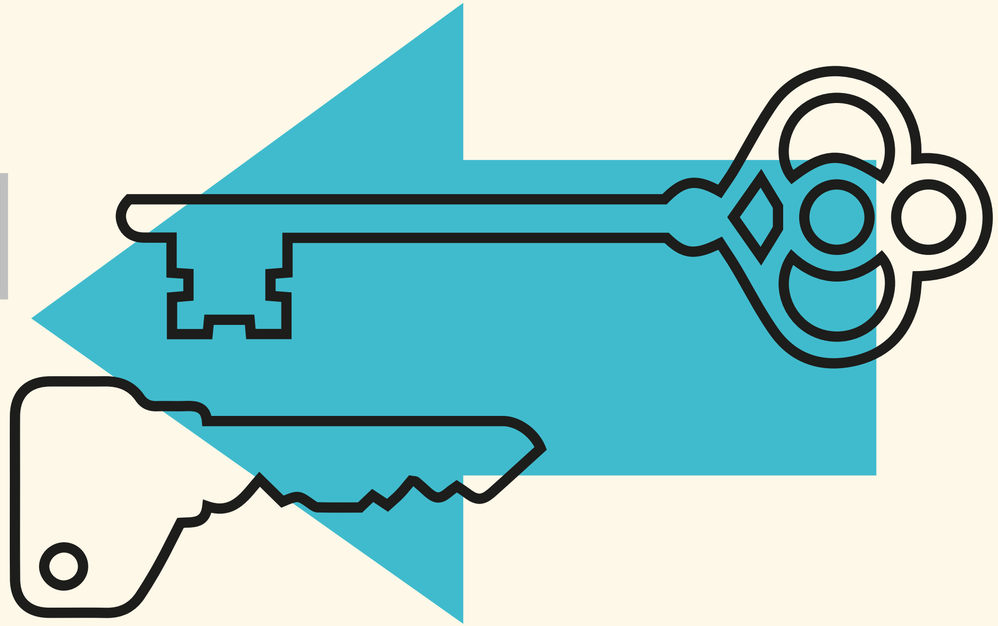


Cryptografie

De sleutels



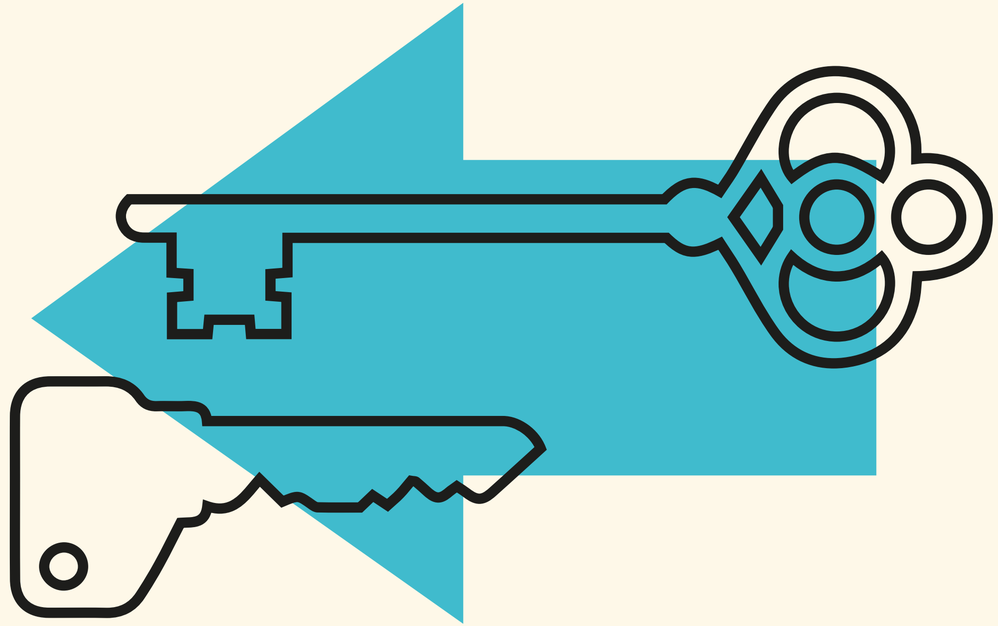
Julius Caesar’s versleuteling



Cryptografie

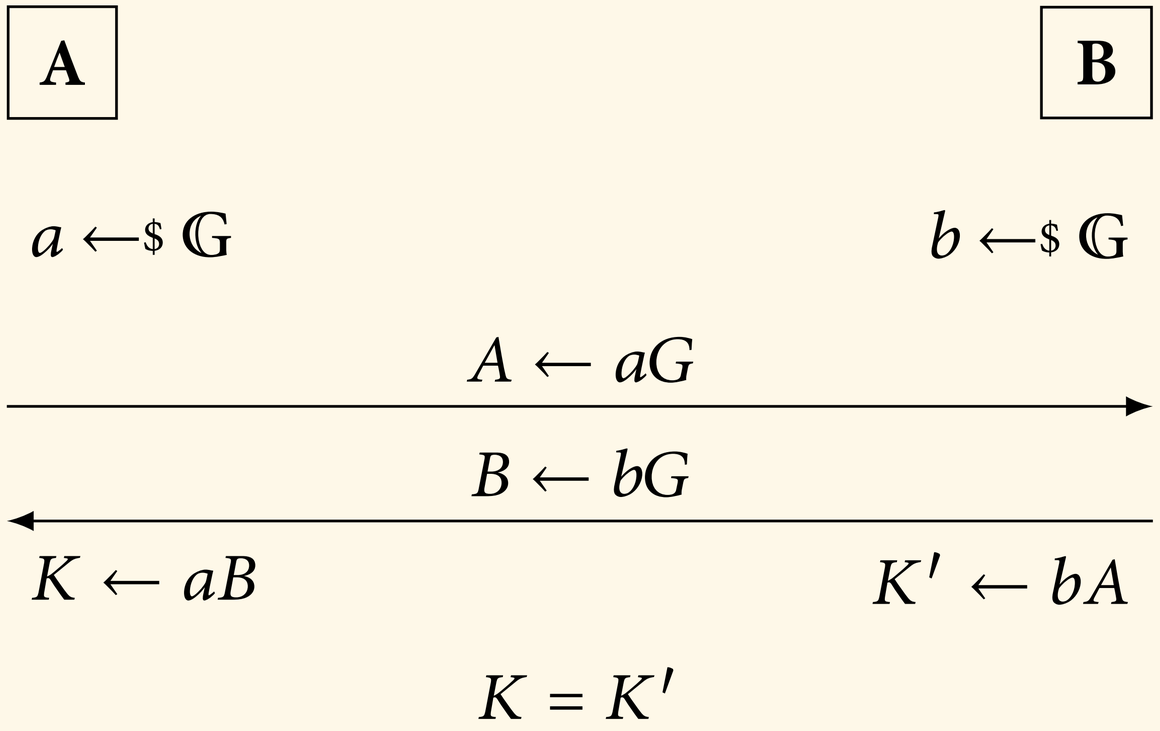
De sleutels

Duitse *Enigma* (~1930-1940s)

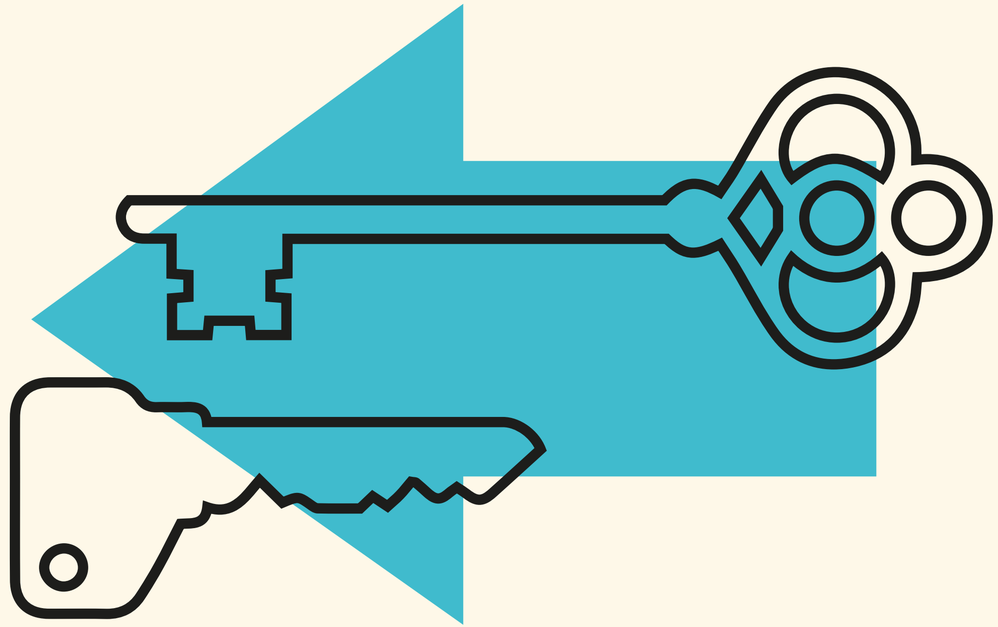


Cryptografie

De sleutels



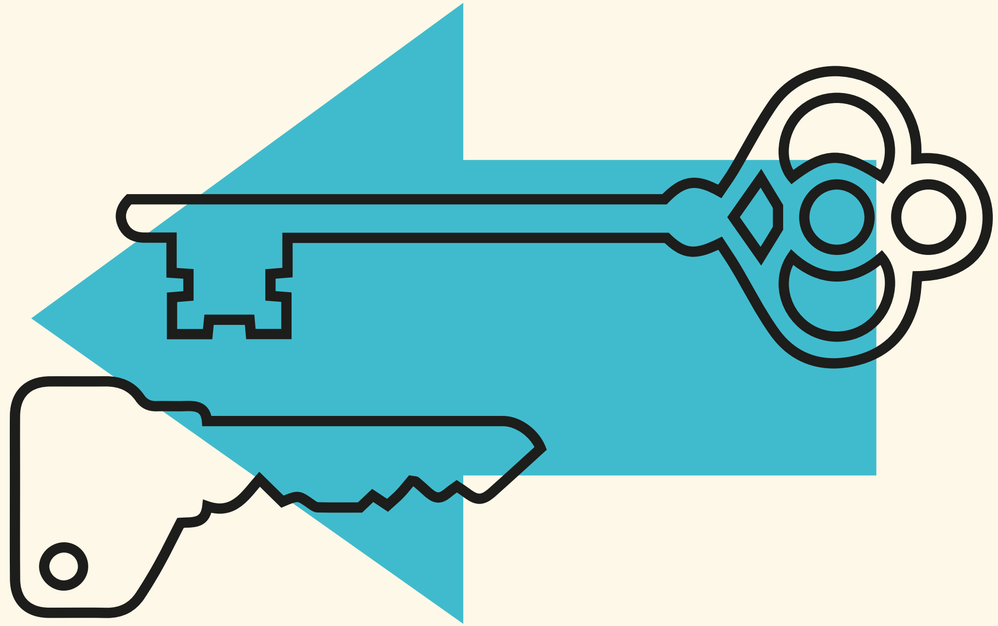
Diffie–Hellman (1976)



Cryptografie

De sleutels

- Gebruiken om informatie te beveiligen (“confidentialiteit”)
  - Staatsgeheimen,
  - Internetbankieren,
  - Online shoppen, …
- Maar ook bijvoorbeeld bewijzen wie je bent (“authenticatie”)
  - Pinpas,
  - OV-chipkaart, …



POST-

QUANTUM

TLS

Quantum

Quantum

Met Olivier

- “Klassieke” computers: bits zijn 0 en 1

“Quantum Computing” by Chris Ferrie and Whurley

Quantum

Met Olivier

- “Klassieke” computers: bits zijn 0 en 1
- Bepaalde wiskunde is moeilijk voor klassieke computers

“Quantum Computing” by Chris Ferrie and Whurley

Quantum

Met Olivier

- “Klassieke” computers: bits zijn 0 en 1
- Bepaalde wiskunde is moeilijk voor klassieke computers
- Kwantum-bits kunnen alles tussen 0 en 1 zijn

“Quantum Computing” by Chris Ferrie and Whurley

Quantum

Met Olivier

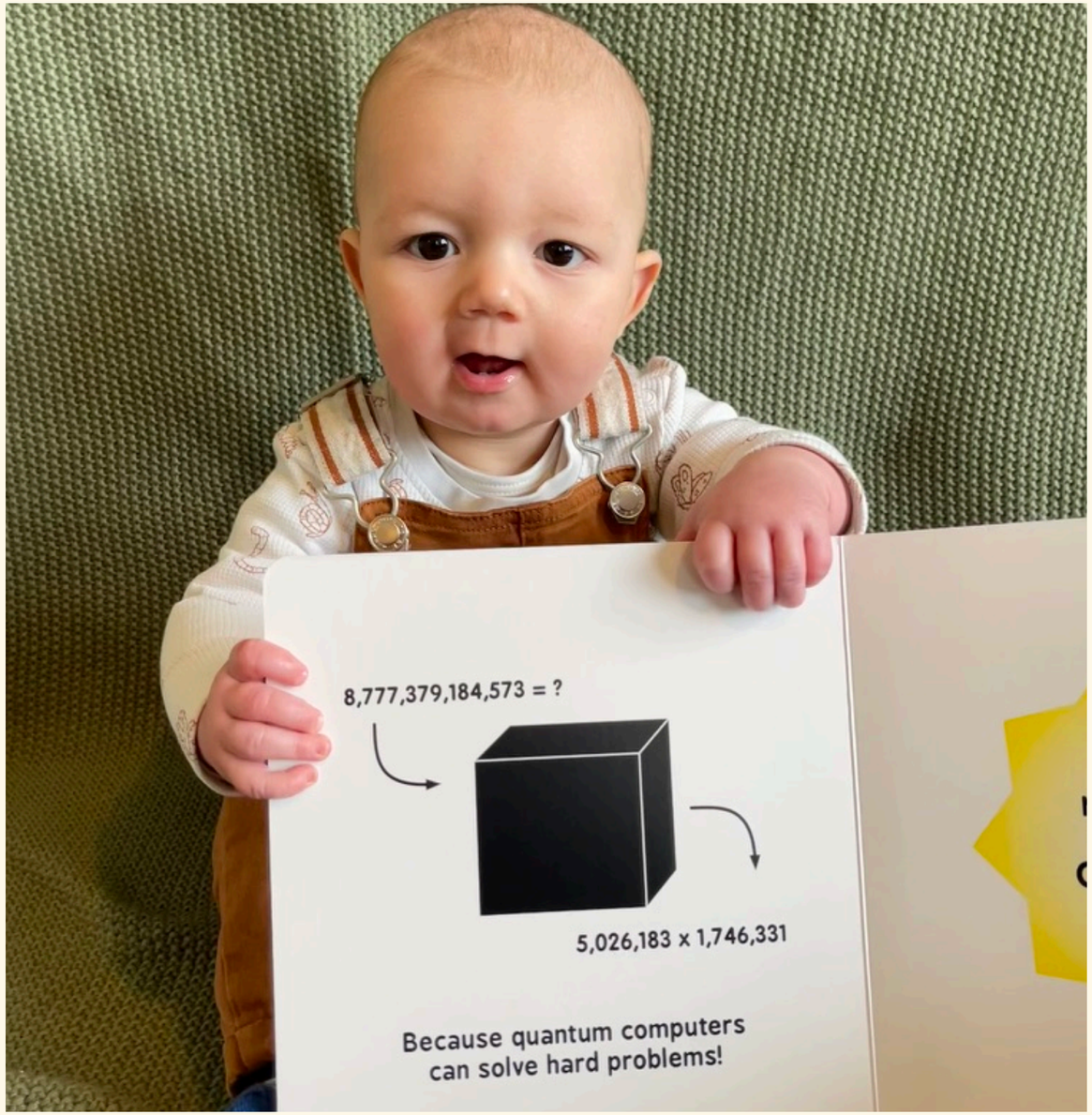
- “Klassieke” computers: bits zijn 0 en 1
- Bepaalde wiskunde is moeilijk voor klassieke computers
- Kwantum-bits kunnen alles tussen 0 en 1 zijn: kwantum-computer

“Quantum Computing” by Chris Ferrie and Whurley

Quantum

Met Olivier

- “Klassieke” computers: bits zijn 0 en 1
- Bepaalde wiskunde is moeilijk voor klassieke computers
- Kwantum-bits kunnen alles tussen 0 en 1 zijn: kwantum-computer
- Kwantum-computers kunnen *sommige* van die moeilijke berekeningen wél snel doen

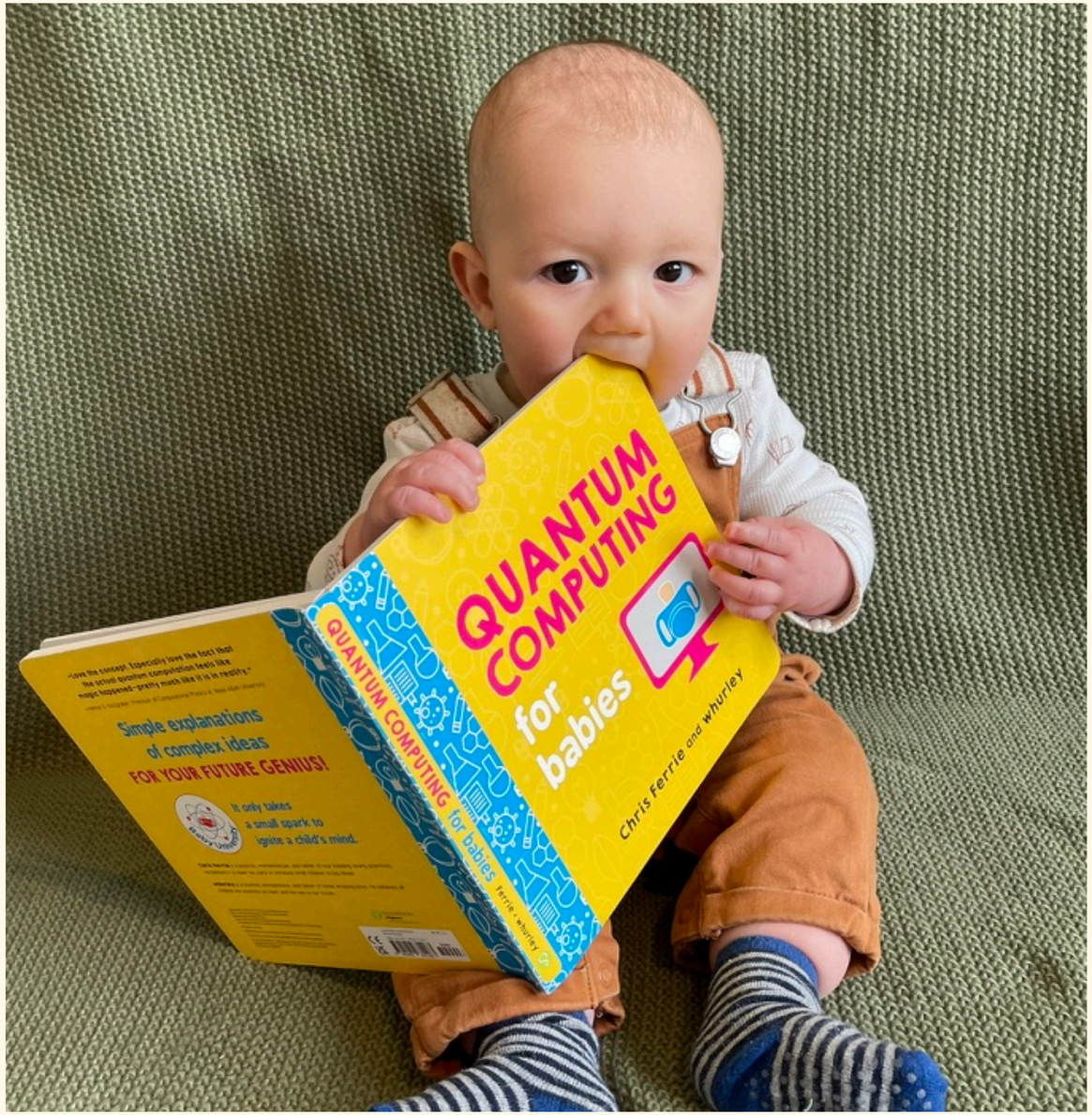


“Quantum Computing” by Chris Ferrie and Whurley

Quantum

Met Olivier

- “Klassieke” computers: bits zijn 0 en 1
- Bepaalde wiskunde is moeilijk voor klassieke computers
- Kwantum-bits kunnen alles tussen 0 en 1 zijn: kwantum-computer
- Kwantum-computers kunnen *sommige* van die moeilijke berekeningen wél snel doen

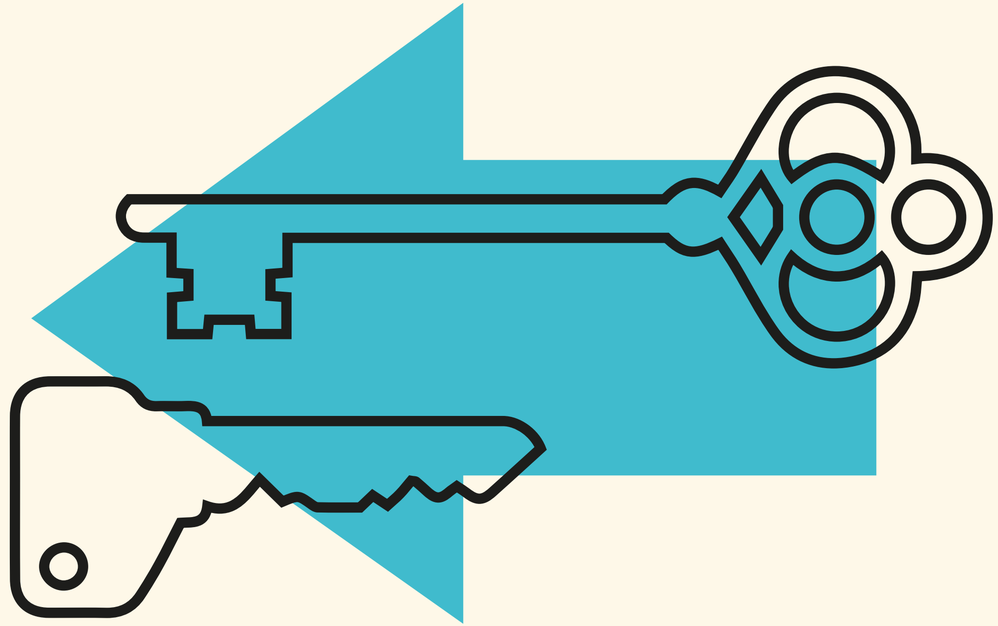


POST-QUANTUM TLS

Post-quantum cryptografie

“Na-kwantum”

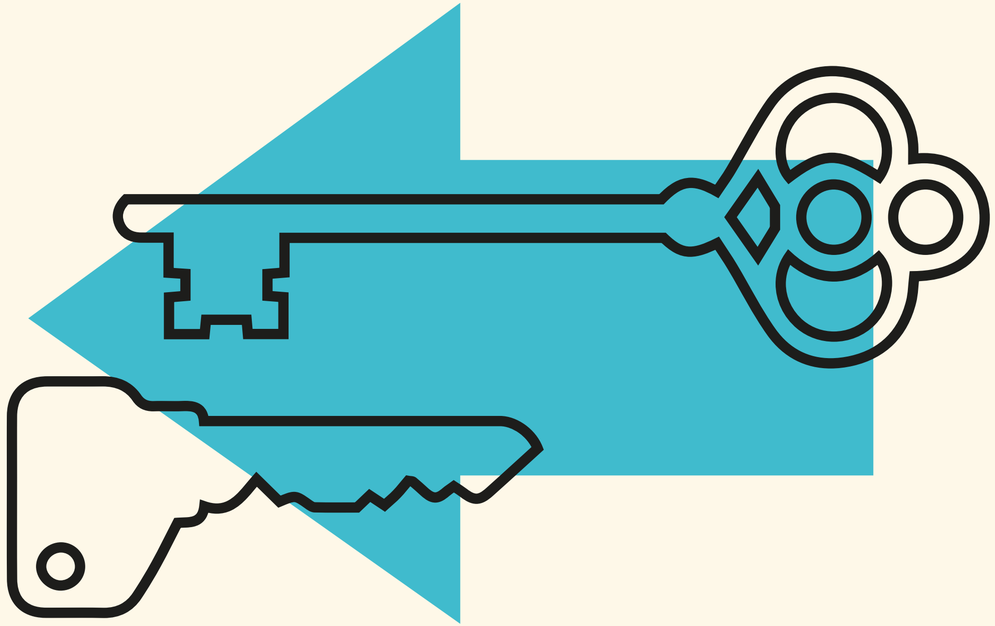
- Cryptografie die gebruik maakt van wiskunde die kwantumcomputers niet “snel” oplossen
- Andere eigenschappen dan we gewend zijn:
  - Groter (meer data) en/of
  - Langzamer (langer rekenen)
- Authenticatie en versleuteling niet meer bijna hetzelfde



Post-quantum cryptografie

“Na-kwantum”

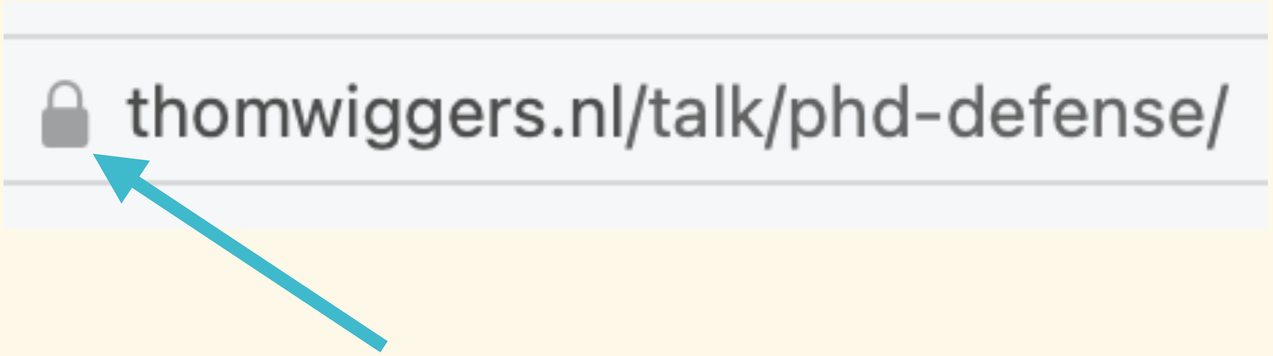
- Er zijn nog geen (grote) kwantum-computers
- Maar er wordt hard aan gewerkt
- Wanneer? 5 jaar? 50 jaar?
- Maar stel je voor dat je ineens niet meer kunt pinnen en internetbankieren: alle winkels ineens stuk
- Nú het moment om de omschakeling te maken



POST-QUANTUM TLS

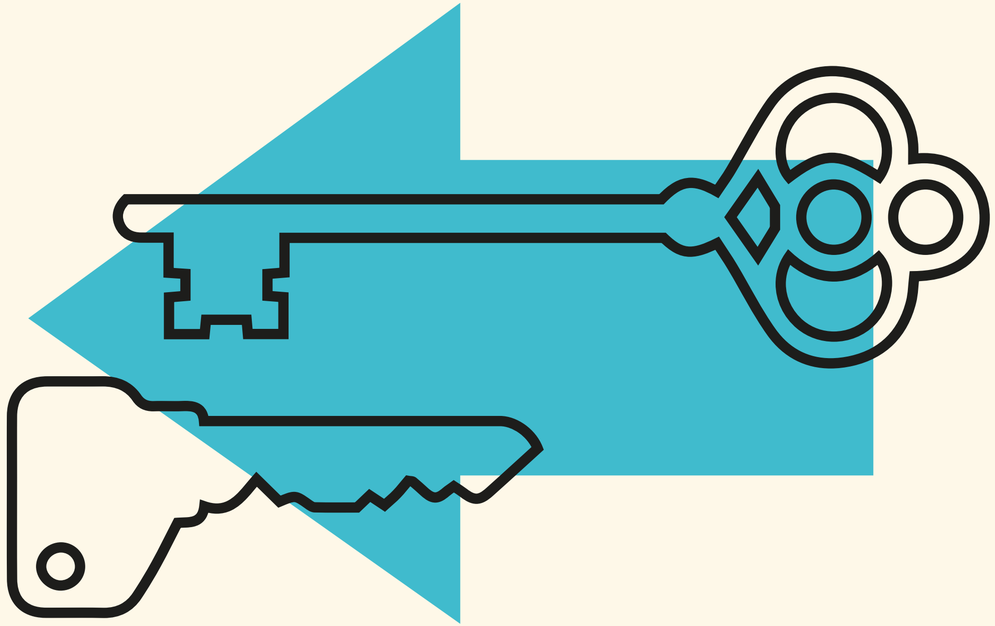
TLS

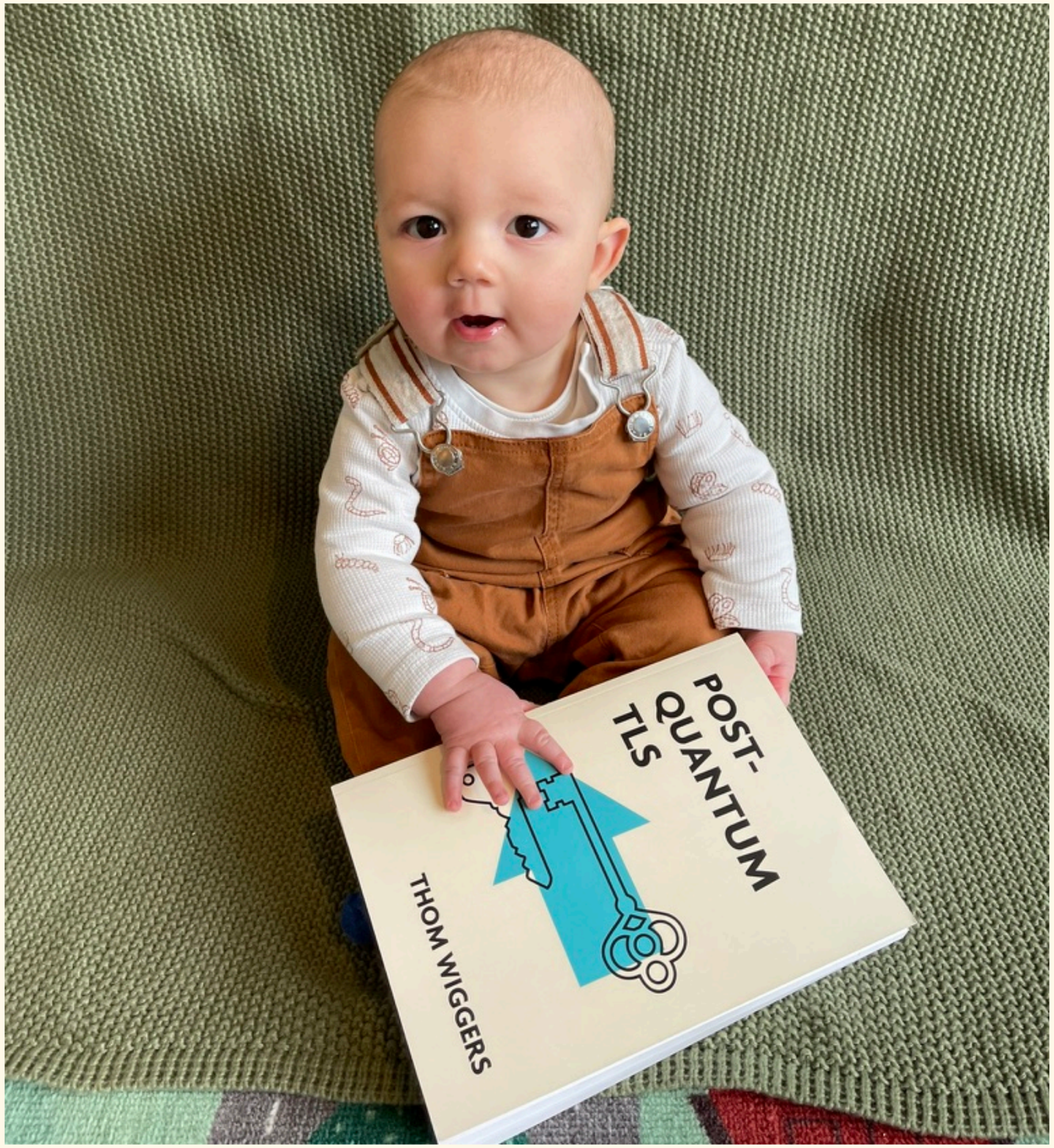
“Het slot in je internetbrowser”



>93%

van de websites op het internet gebruikt TLS



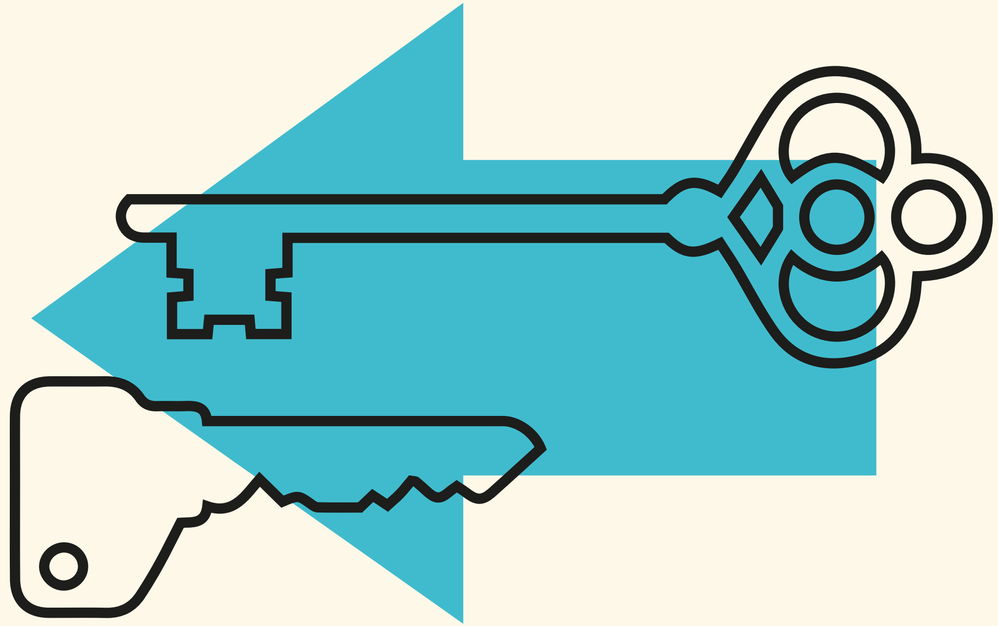

POST-
QUANTUM
TLS
THOM WIGGERS

Mijn proefschrift

Waar gaan die vragen straks over

- Hoofdstuk 3: **Wat is het huidige voorstel voor post-quantum TLS**
- Hoofdstuk 4: **Zou het oude voorstel “OPTLS” efficiënter kunnen zijn?**
- Hoofdstuk 5: **Een betere en snellere TLS-sleuteluitwisseling gebaseerd op KEMs: “KEMTLS”**
- Hoofdstuk 6: **Een variant van KEMTLS die sneller is bij wat extra aannames (KEMTLS-PDK)**

- Deel II: **Hoe veilig is KEMTLS?**
- Deel III: **Hoe snel zijn de varianten van TLS?**



Conclusies

Waar is dit goed voor

- **TLS** beveiligen tegen kwantumcomputers is te doen, maar zonder aanpassingen is de **impact groot**.
- **KEMTLS**, mijn voorstel voor een verbetering van TLS, kan helpen met de **impact verminderen**.
- KEMTLS **is veilig**.
- KEMTLS wordt nu besproken bij de internet-standaardenorganisatie IETF, die over het TLS-protocol gaat