



# CRYPTO

## Cryptografie en Quantum Security

- > Sander Dorigo
- > Security Architect @ Fox-IT
- > 27 november 2024, FreshMinds

## > Fox Crypto



## > Old school security

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

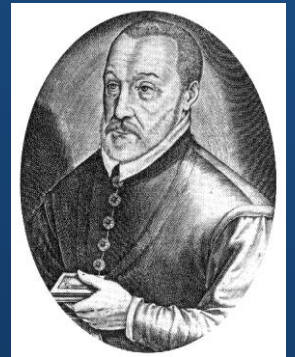
FRESHMINDS -> IUHVKPLQGV



# > lets minder old school security

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

S	A	N	D	E	R	I	S	C	O	O	L
F	R	E	S	H	M	I	N	D	S	F	R
X	R	R	V	L	D	Q	F	F	G	T	C

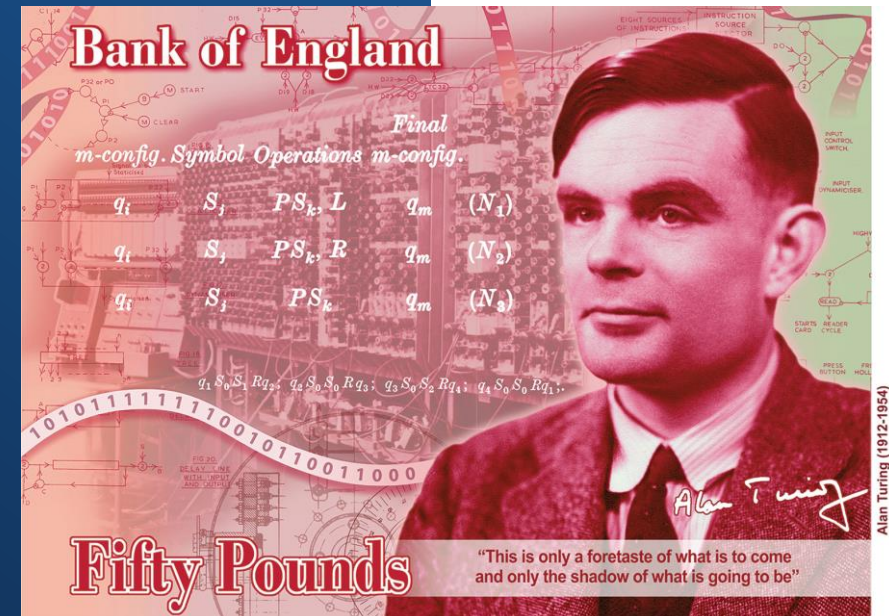


➤ lets minder old school security



## > Enigma

- Duitse uitvinding
- Fransen, Polen en Engelsen
- Alan Turing



## > Philips Crypto

- De Aroflex
- Cryptomodule
- “Beroflex”



## > Lessons learned

- Het moet praktisch onkraakbaar zijn
- Het design is “openbaar”, de sleutel is het geheim
- Het moet makkelijk en stressvrij te gebruiken zijn

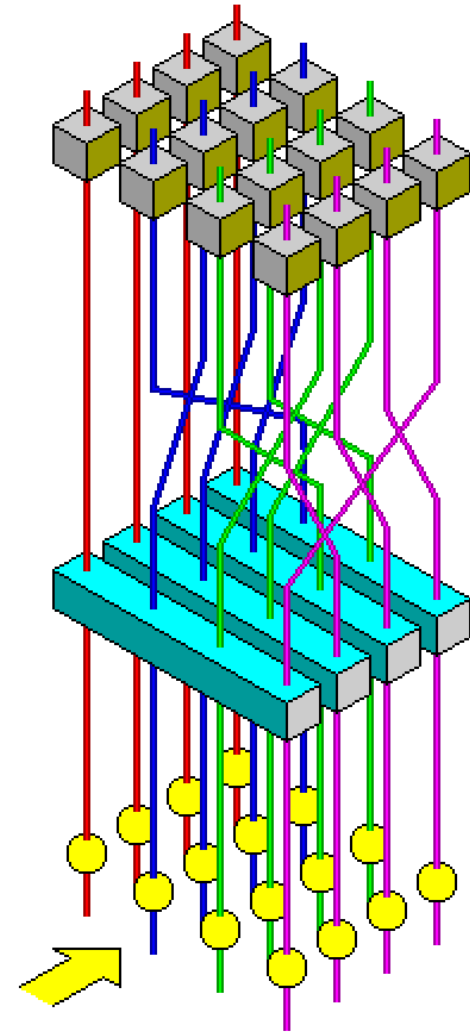


Auguste Kerckhoffs

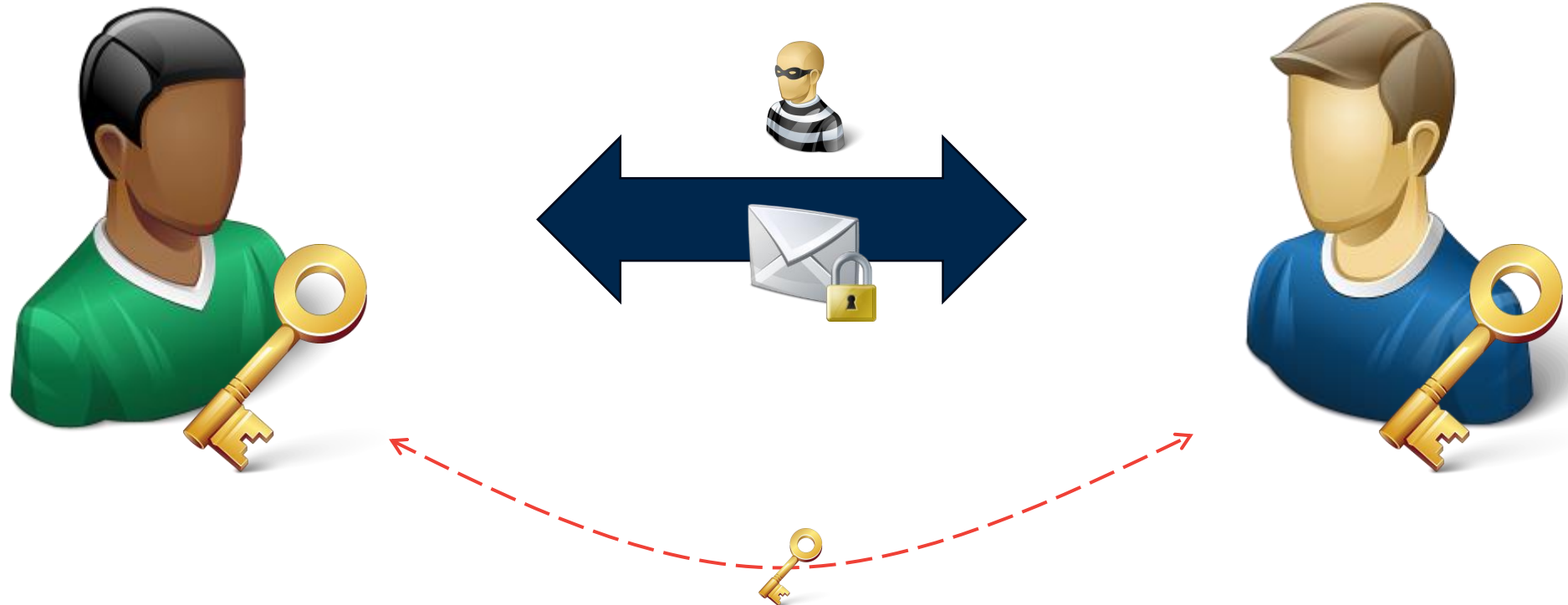


## > DES, triple DES en AES: moderne cryptografie

- De intrede van de computer
  - Data Encryption Standard (1977)
  - Advanced Encryption Standard (2001)
- Sleutels worden langer, het algoritme complexer
  - “Secret key cryptografie”



## > Symmetrische cryptografie

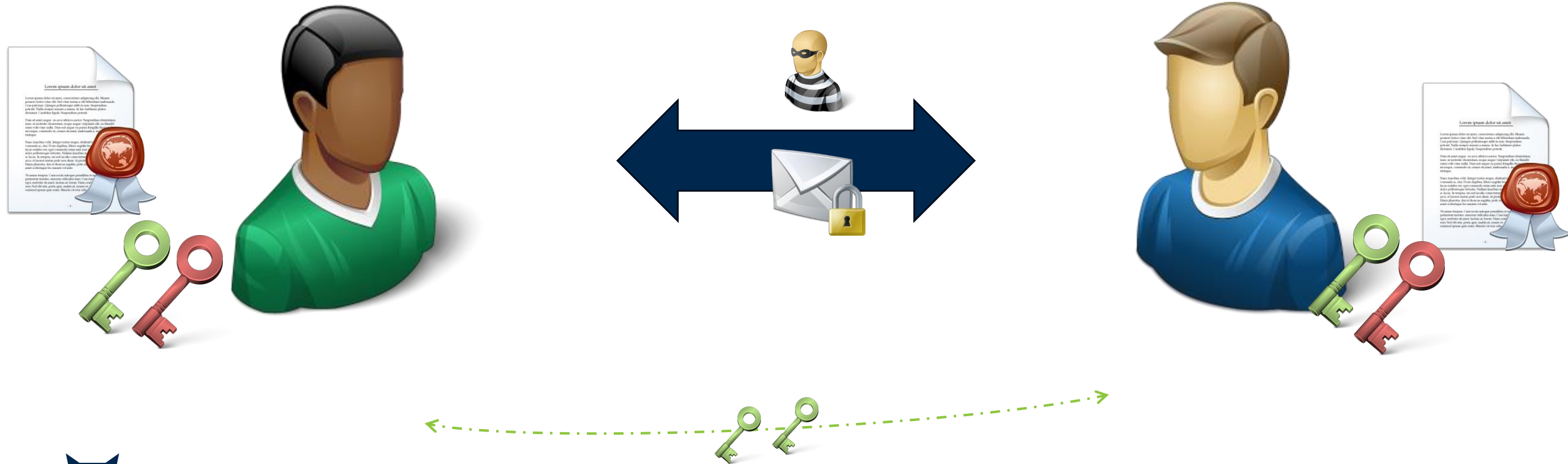


## > Hoe krijg je nou zo'n “veilig kanaal”?

- Niet heel duurzaam of veilig:
  - Sleutels overvliegen
  - Codeboeken maken van rijstpapier
  - Sleutels gebaseerd op de datum of de tijd
- Een sleutelpaar
  - Eén sleutel om te versleutelen
  - Een andere sleutel om te ontcijferen



# > Asymmetrische cryptografie



# (A) Symmetric cryptography

---



## Where is (a)symmetric cryptography used?

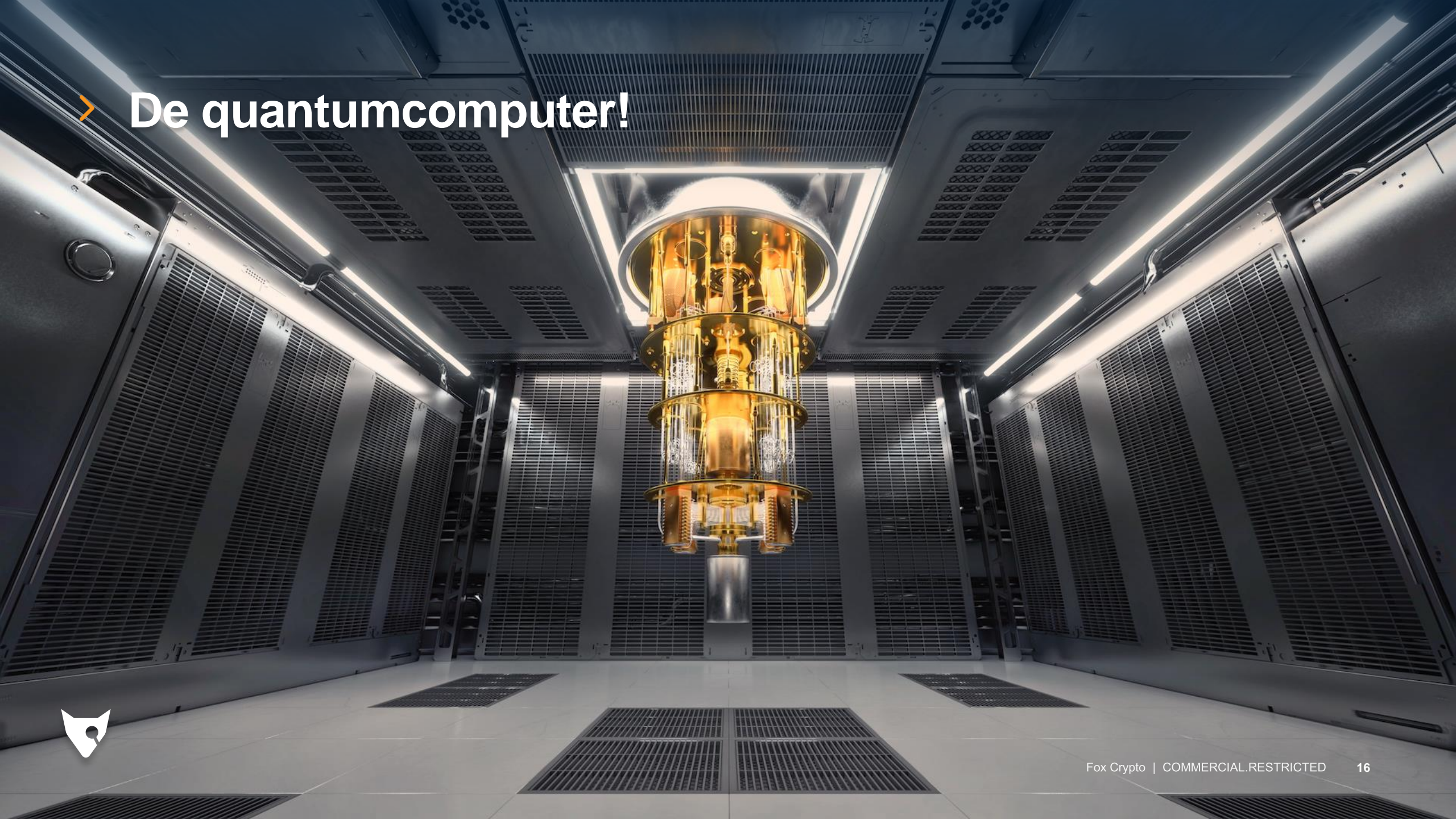
---

- HTTPS traffic
  - Browser uses asymmetric crypt to establish secure symmetric connection.
  - Let's Encrypt, TLS certificates
- Signal and WhatsApp
  - Use asymmetric crypt and certificates
  - Encrypt every message
- Decentralized networks (VPN, military)
  - Use asymmetric crypt and symmetric keys

**VULNERABLE**



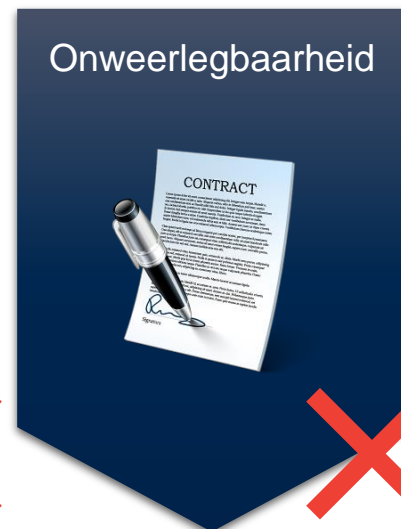
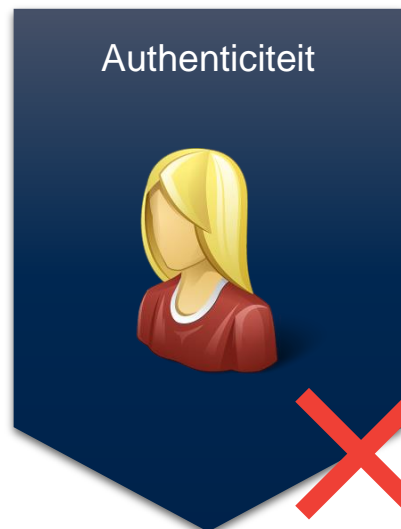
# > De quantumcomputer!



➤ It's not important to know how a quantum computer works



## > Maar wat betekent dat dan?



> Store now, decrypt later



## > Reactie

- Software en kennis
- Migratiehandleidingen
- Protocollen
- Algoritmes



# > Algoritmes



# Nieuwe algoritmes

---

## Now

- RSA
- Diffie–Hellman
- ECC Diffie–Hellman



PUBLIC

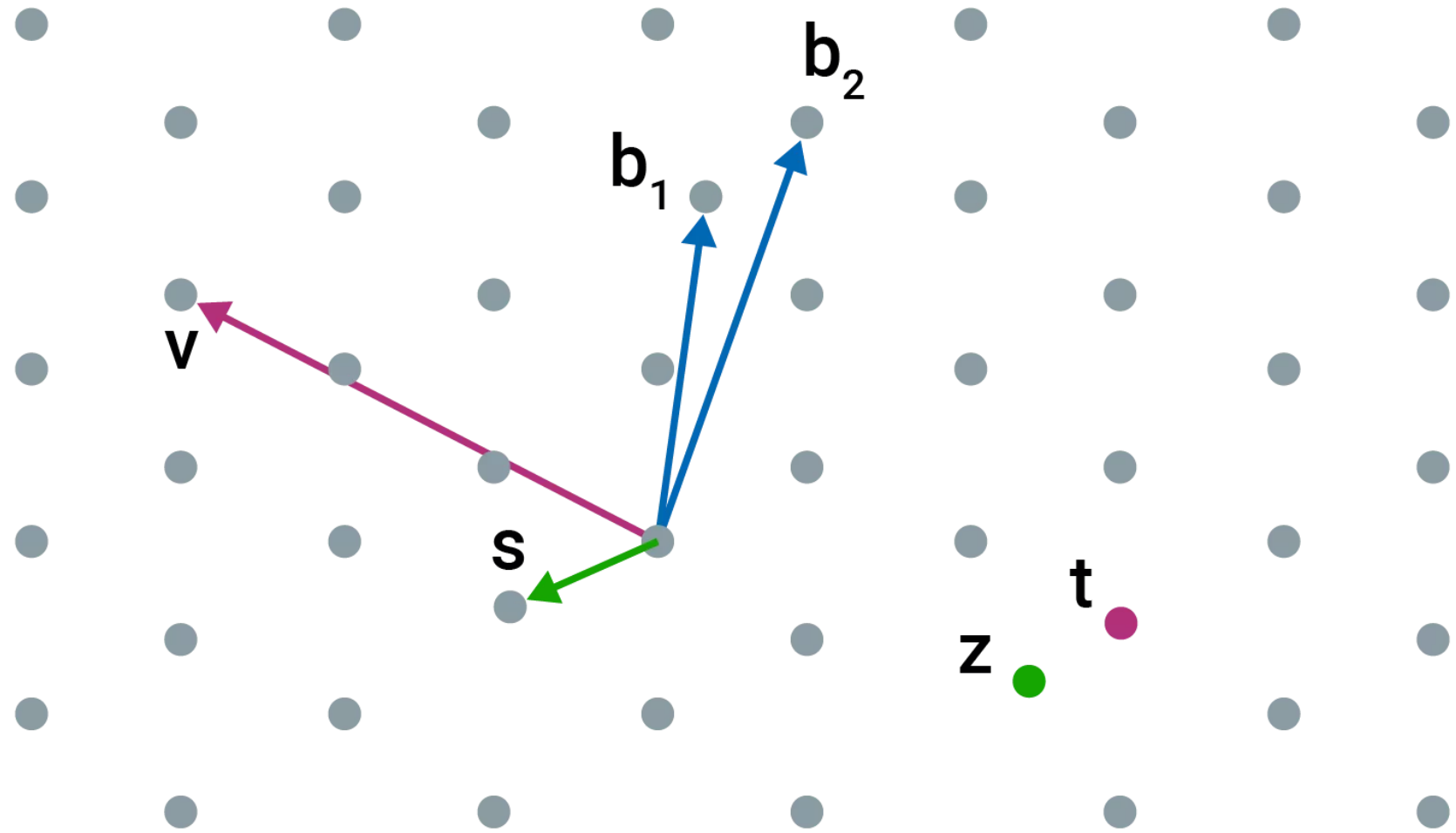
## RSA (old)

---

- Think of two very large prime numbers,  $p$  and  $q$ 
  - This is the secret key
- Multiply them, resulting in  $n$ 
  - $n$  is the public key
  
- Calculating  $n$  from  $p * q$  is very simple.
- Calculating  $p$  and  $q$  if you only know  $n$  is very hard

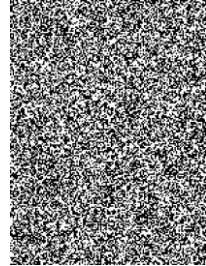
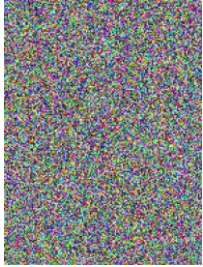
# Lattice based cryptography (new!)

---

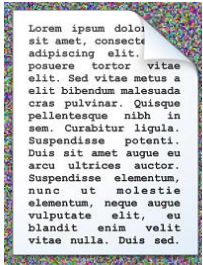


# Code based cryptography (new!)

---



1. Generate random data with a public key
2. Apply data to file, making the content unreadable



3. Unscramble the random data by applying the private key

## Key sizes in Classic McEliece

---



256 bits



4.096 bits

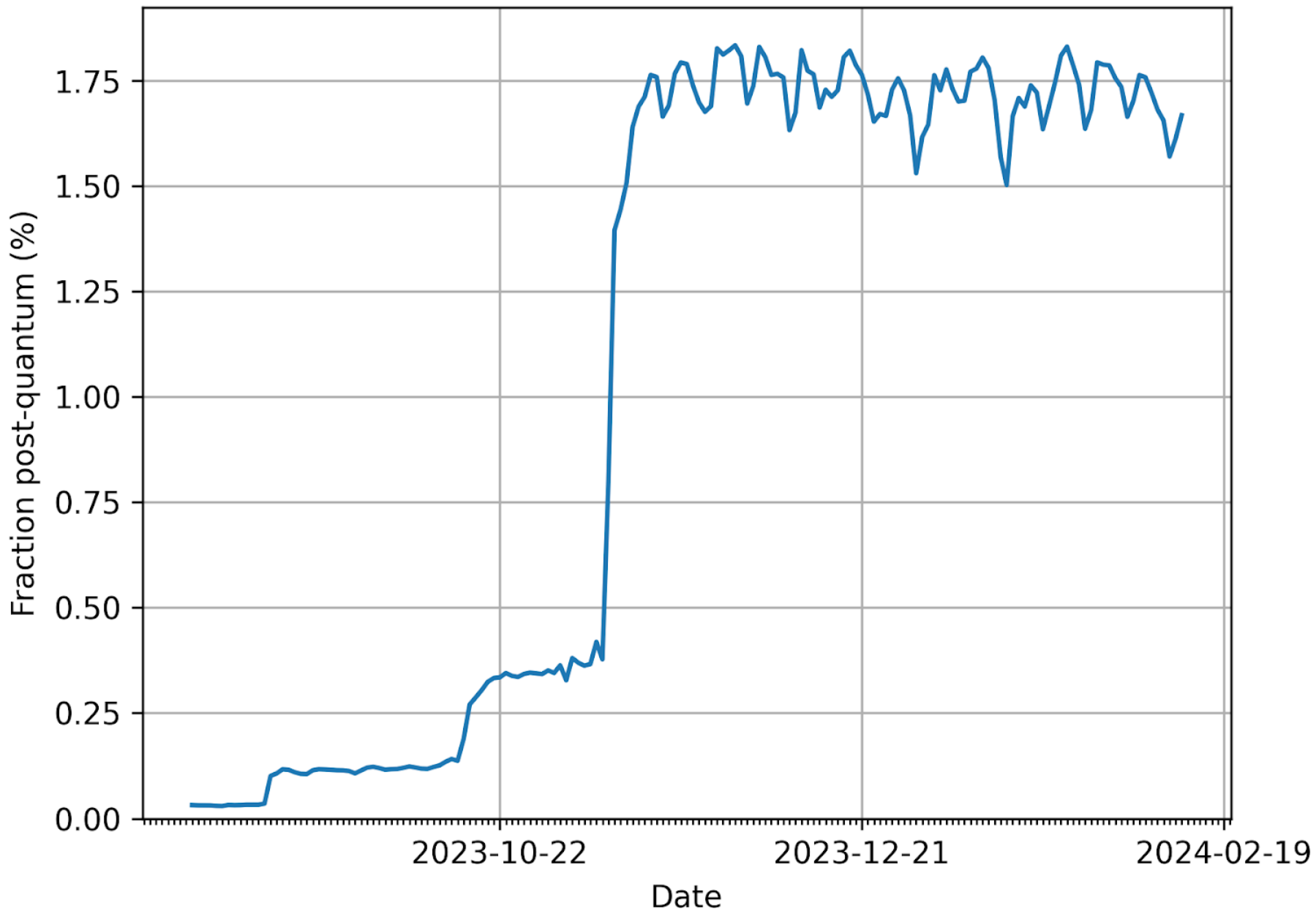


1.3MB

# > Protocollen



# Client support for post-quantum key agreement in TLS 1.3



## > Migratiehandleidingen



# Migratiehandleidingen

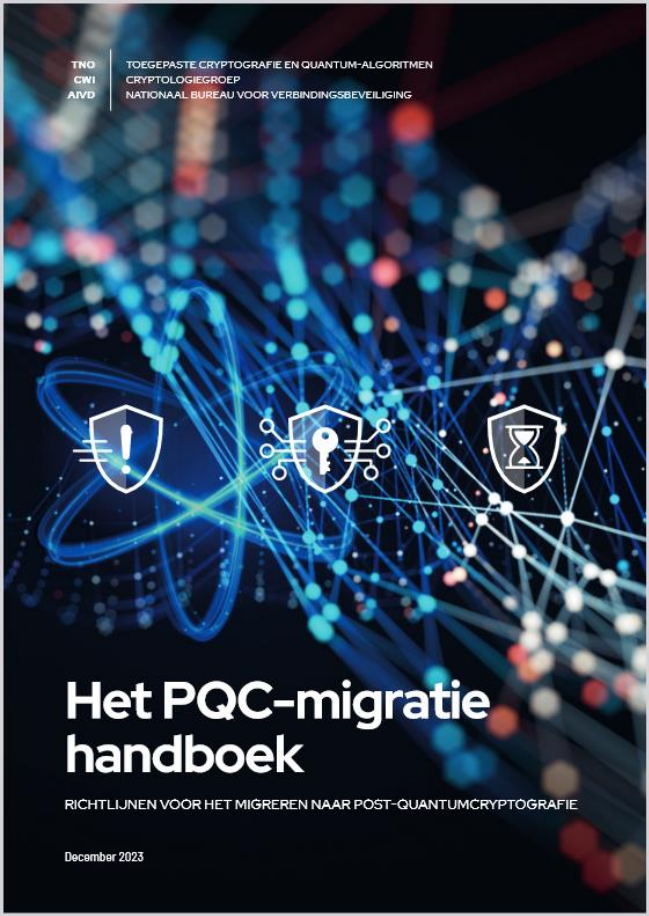




## Maak je organisatie quantumveilig

Een handreiking voor het maken van een risicoanalyse en migratieplanning

The cover features a photograph of a complex quantum device with numerous copper-colored components and thin wires.



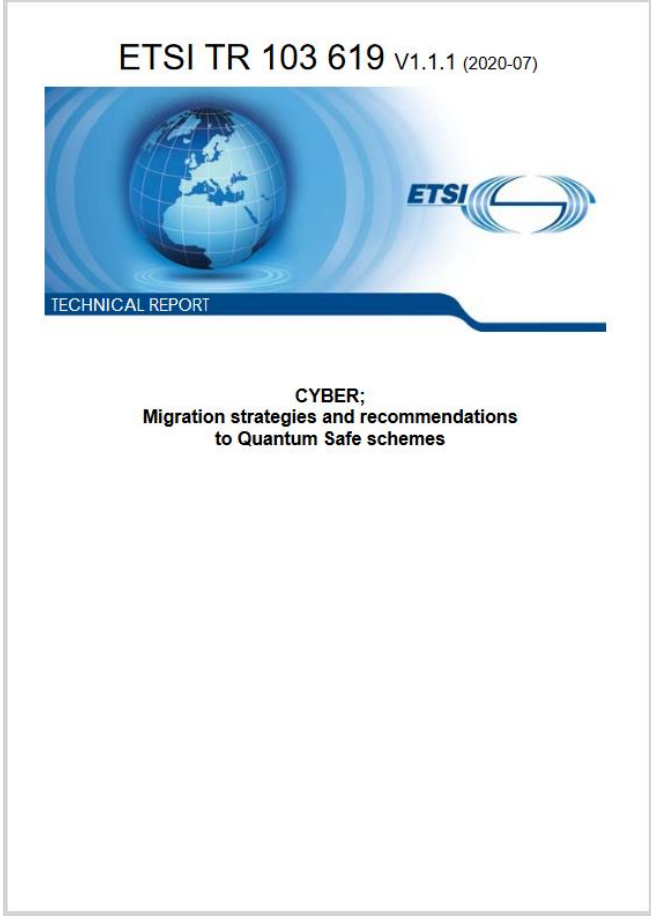
TNO TOEGEPASTE CRYPTOGRAFIE EN QUANTUM-ALGORITMEN  
CW1 CRYPTOLOGIEGROEP  
AIVD NATIONAAL BUREAU VOOR VERBINDINGSBEVEILIGING

## Het PQC-migratie handboek


RICHTLIJNEN VOOR HET MIGREREN NAAR POST-QUANTUMCRYPTOGRAFIE

December 2023

The cover features a blue-toned network visualization with nodes and connecting lines, overlaid with three shield icons containing symbols for warning, a key, and a timer.



ETSI TR 103 619 V1.1.1 (2020-07)



TECHNICAL REPORT

### CYBER; Migration strategies and recommendations to Quantum Safe schemes

The cover features a blue globe with the ETSI logo to its right. Below the globe, the text 'TECHNICAL REPORT' is written in a blue bar.

## > Software en kennis



## > Software en kennis

- De Nationale Quantumcursus
- Quantum Inspire
- Het Crypto Agility monster van NCSC
- Open Quantum Safe
- Explainer video van “Veritasium”
- Azure Quantum “katas”
- Qiskit



## > Reactie

- **Algoritmes**
  - Zorgen voor de onderliggende basis, de wiskundige bouwstenen voor nieuwe cryptografie
- **Protocollen**
  - Zijn de “lijm laag” tussen applicaties
- **Migratiehandleidingen**
  - Geven houvast voor de vraag “ja maar hoe dan?”
- **Software en kennis**
  - Bouwt op al het voorstaande concrete oplossingen en zorgt voor invulling



## > Vragen en antwoorden



Sander Dorigo

sander.dorigo@fox-it.com



**CRYPTO**  
Part of fox-IT