CRYPTO

Cryptografie en Quantum Security

- Sander Dorigo
- Security Architect @ Fox-IT

- 27 november 2024, FreshMinds

Fox Crypto

OPENVPN™

Old school security

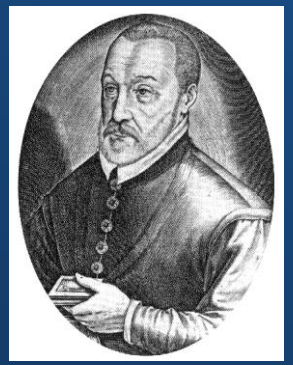
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

FRE**S**HMIND**S** -> IUH**V**KPLQG**V**

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

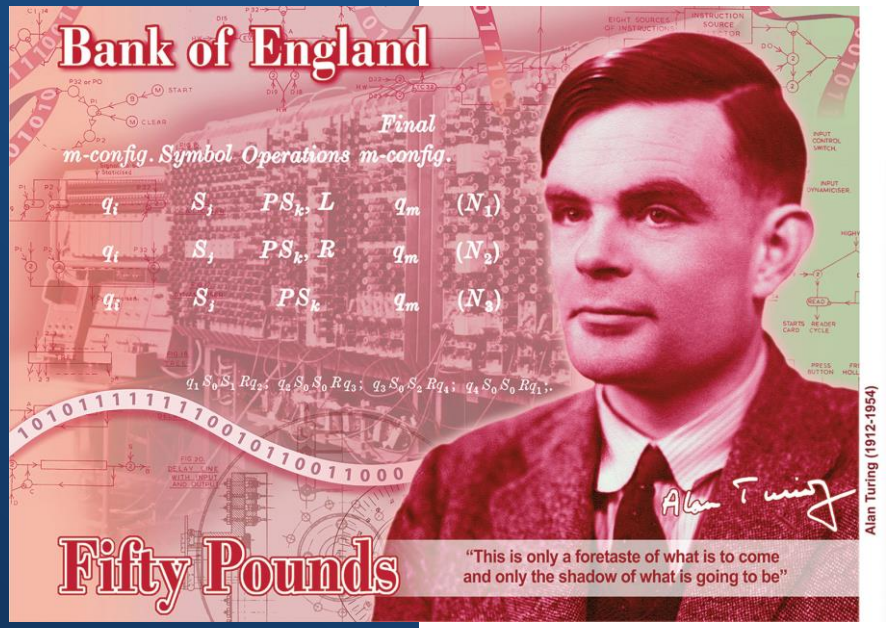
S	A	N	D	E	R	I	S	C	**O**	**O**	L
F	R	E	S	H	M	I	N	D	S	F	R
X	**R**	**R**	V	L	D	Q	F	F	G	T	C



lets minder old school security

Enigma

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



Philips Crypto

- De Aroflex
- Cryptomodule
- “Beroflex”

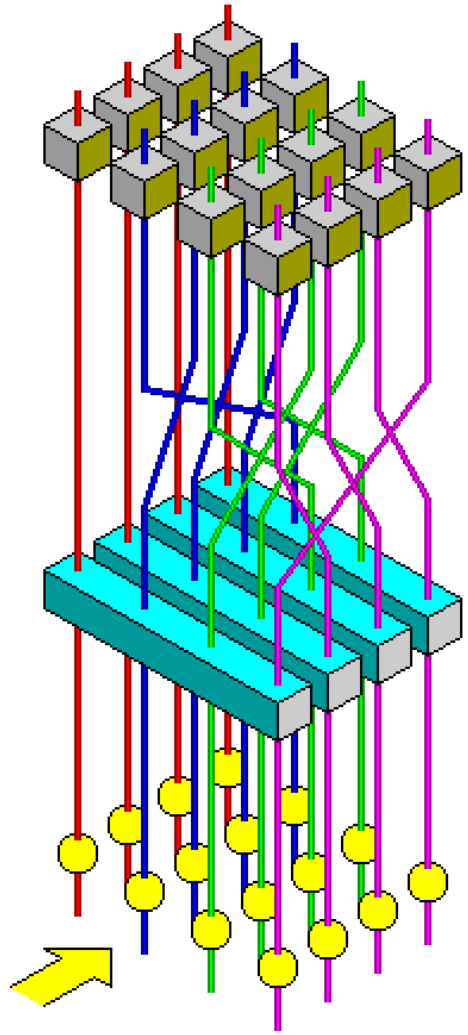
Lessons learned

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

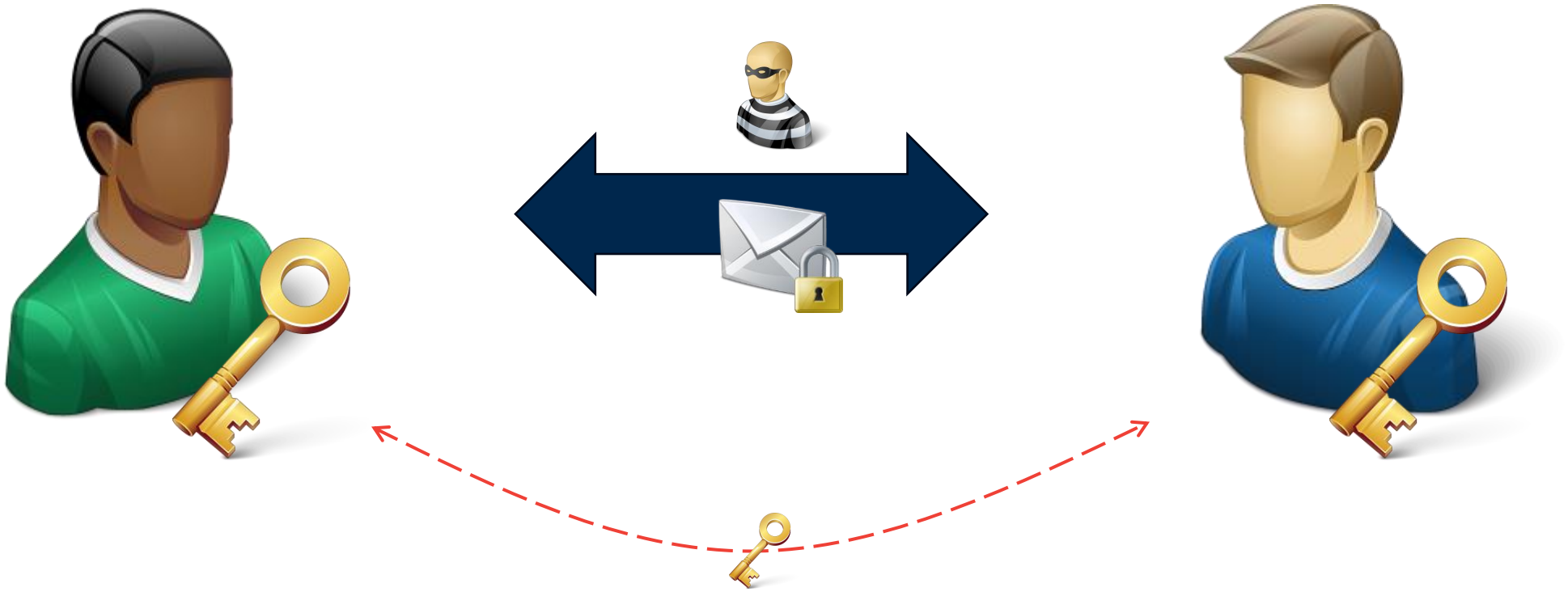
Auguste Kerckhoffs

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”



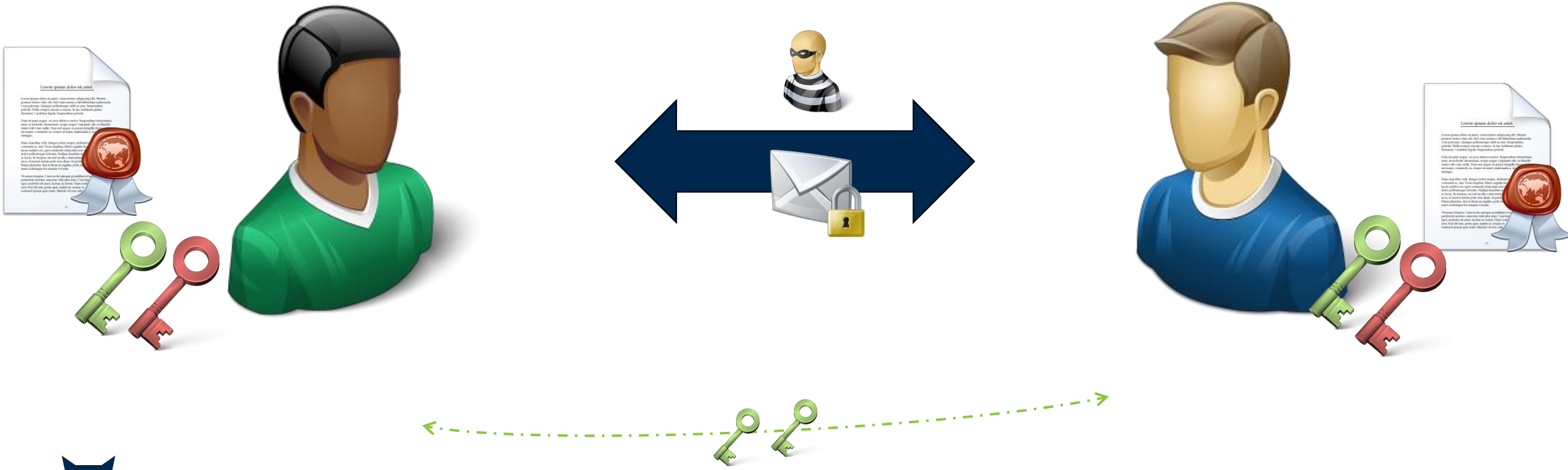
Symmetrische cryptografie



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



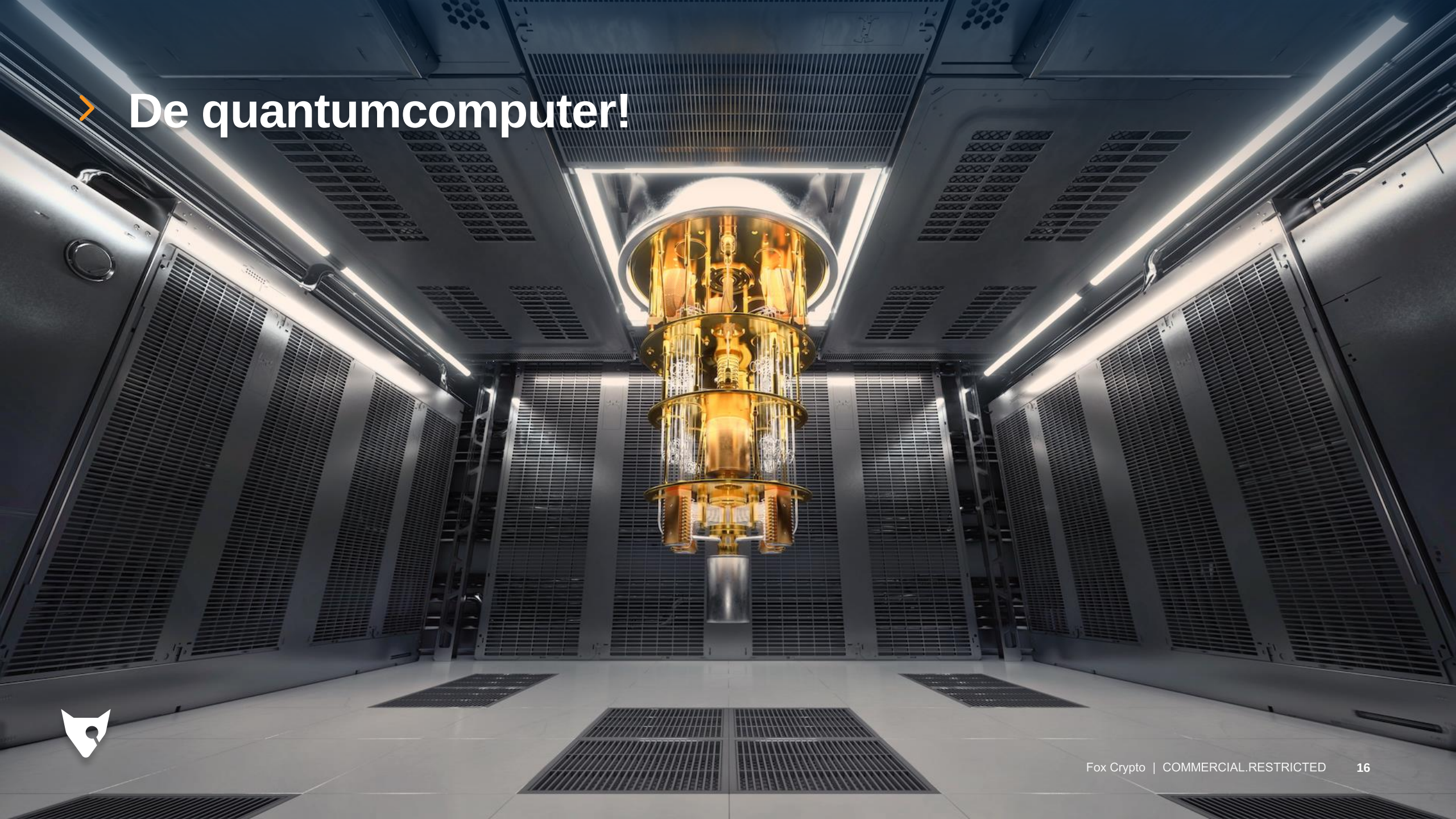
(A)Symmetric cryptography

Where is (a)symmetric cryptography used?

- HTTPS traffic
  - Browser uses asymmetric crypt… …ecure symmetric connection.
  - Let's Encrypt, TLS …
- Signal and Wh…
  - Use a … certificates
  - C… every message
- Dec… …ections (VPN, military)
  - Usu… …tificates and symmetric keys

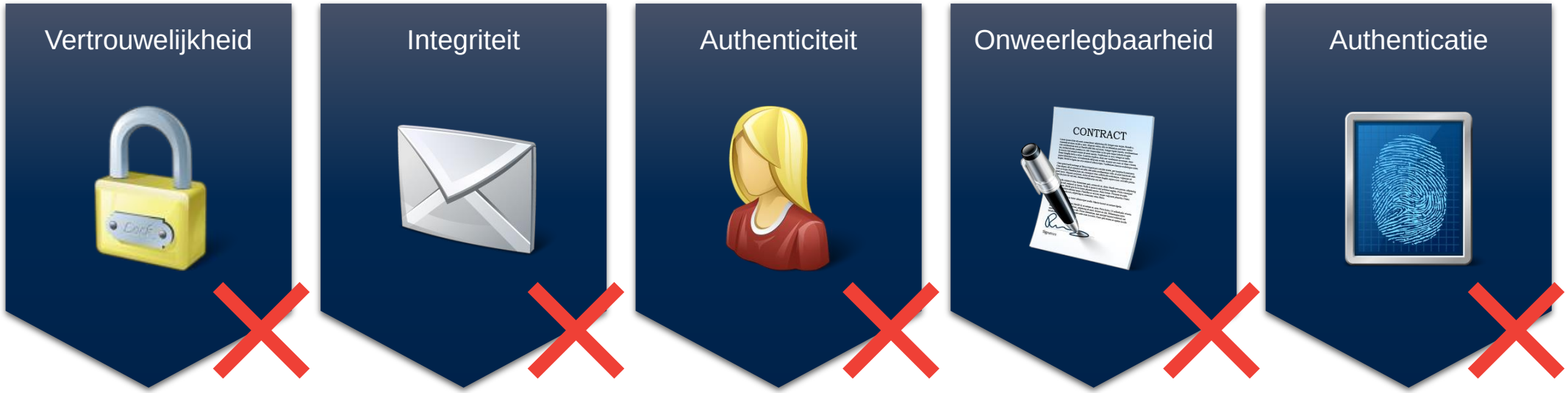
VULNERABLE

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

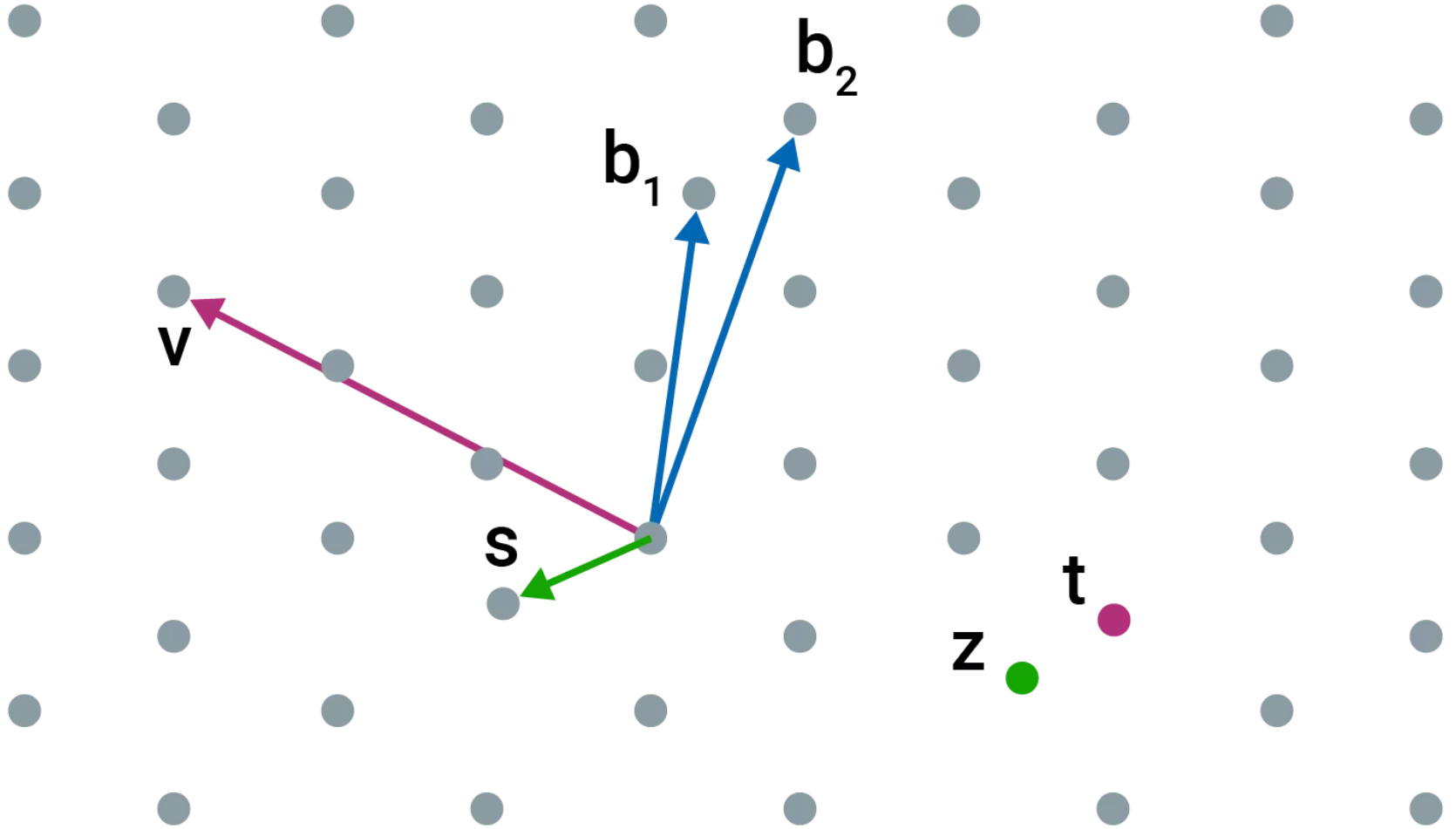
Later?

RSA (old)

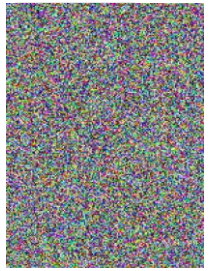
- Think of two very large prime numbers, *p* and *q*
  - This is the secret key
- Multiply them, resulting in *n*
  - *n* is the public key

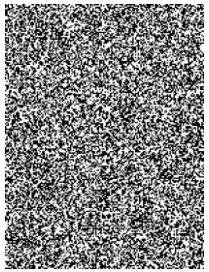
- Calculating *n* from *p*q* is very simple.
- Calculating *p* and *q* if you only know *n* is very hard

Lattice based cryptography (new!)

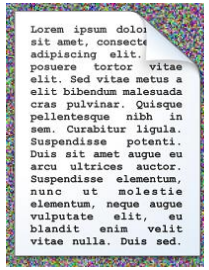


Code based cryptography (new!)



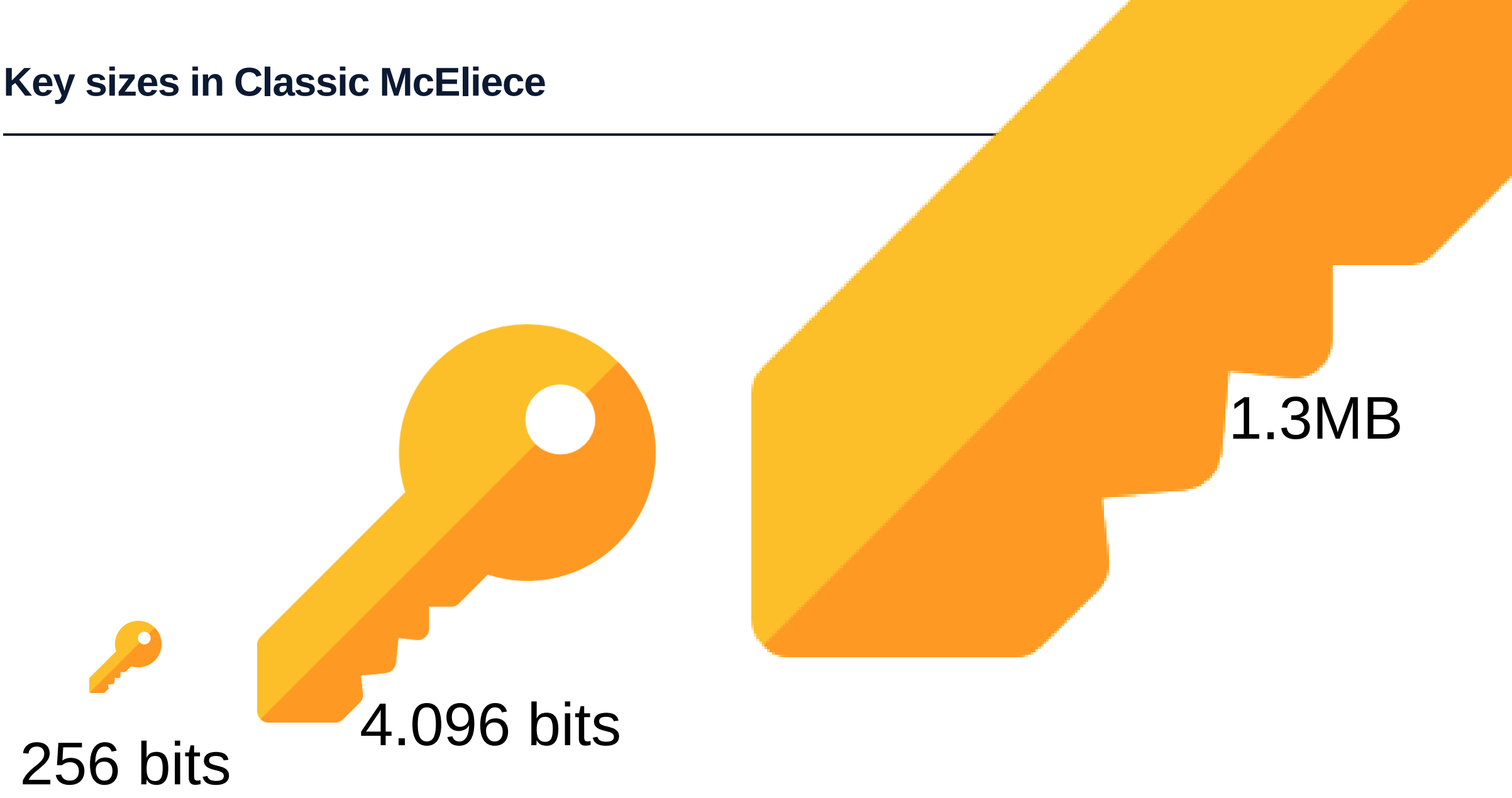


1. Generate random data with a public key
2. Apply data to file, making the content unreadable

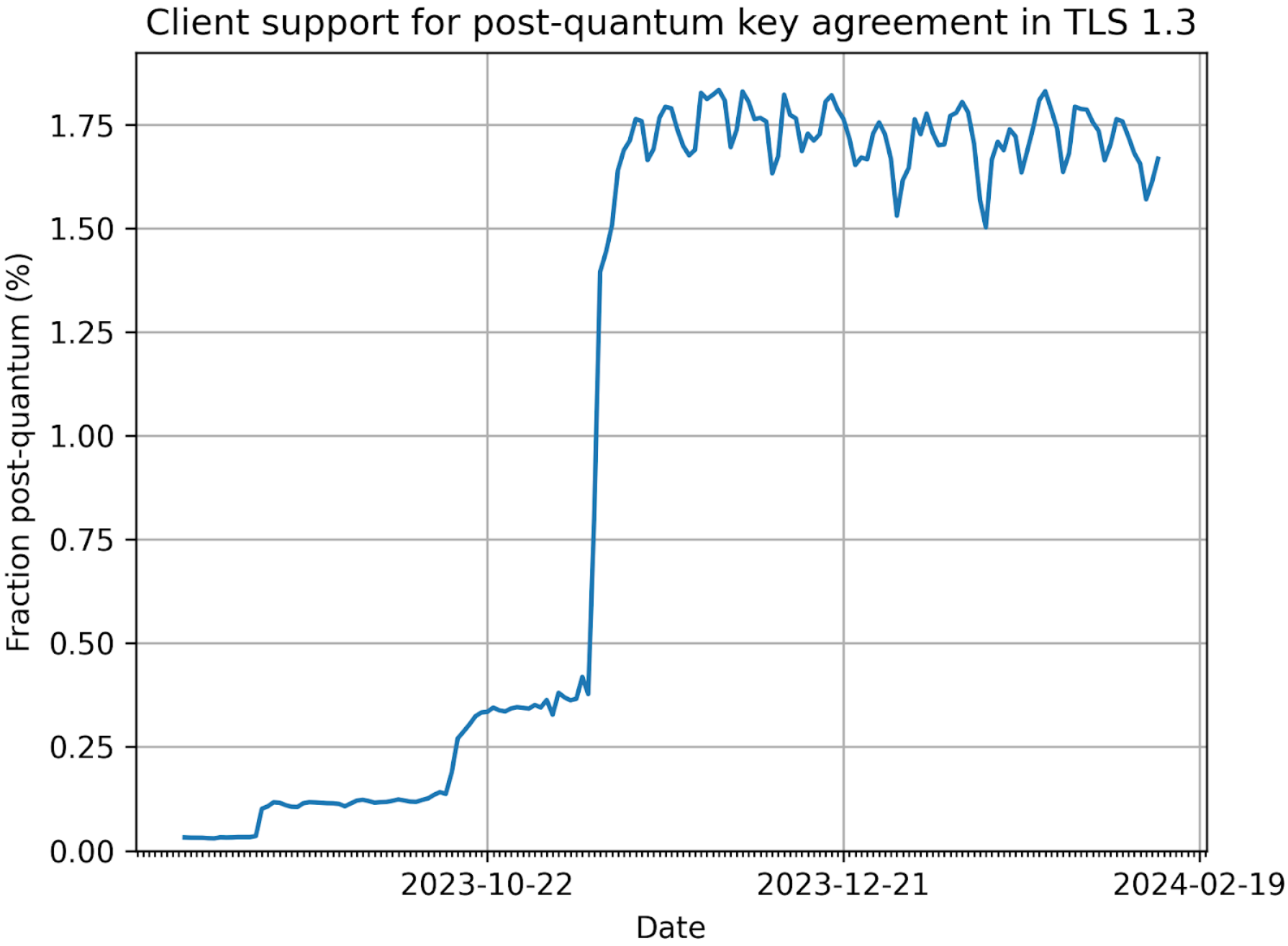


3. Unscramble the random data by applying the private key

Key sizes in Classic McEliece

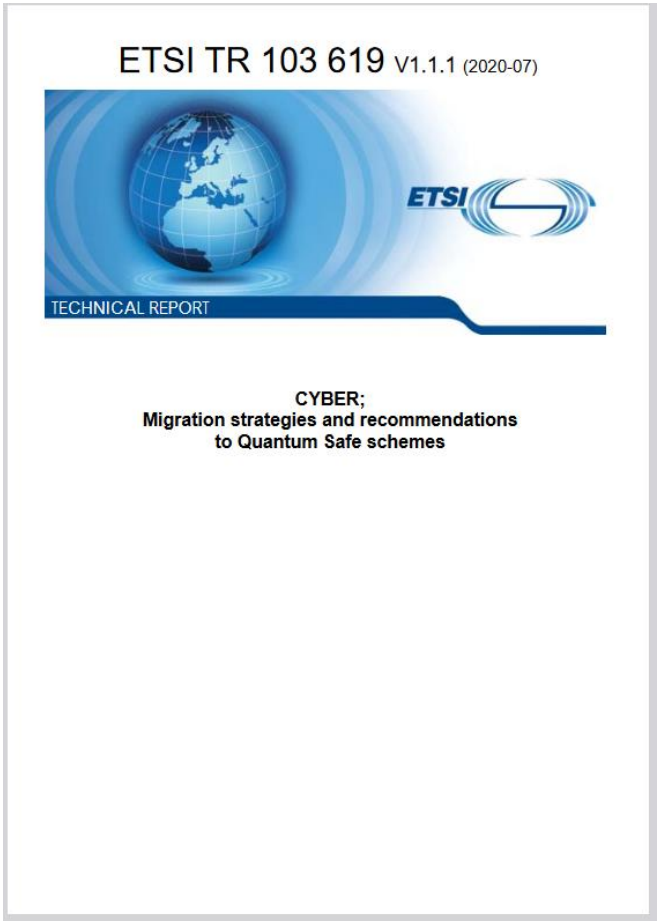


Protocollen


Client support for post-quantum key agreement in TLS 1.3
Fraction post-quantum (%)
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
2023-10-22
2023-12-21
2024-02-19
Date

Migratiehandleidingen

Migratiehandleidingen



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 “lijmlaag” 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