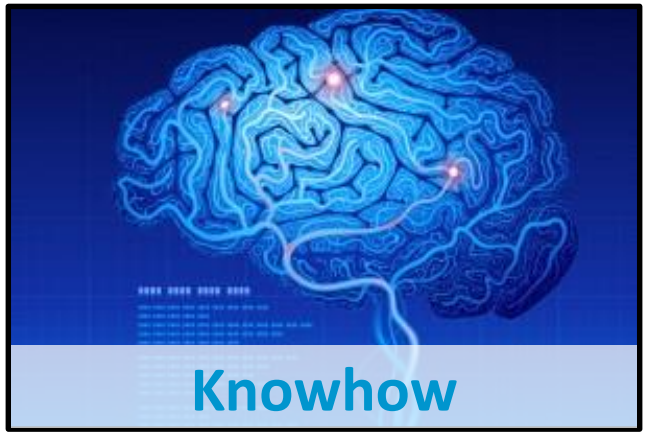
Kwantumcomputers Vs. Cryptografie

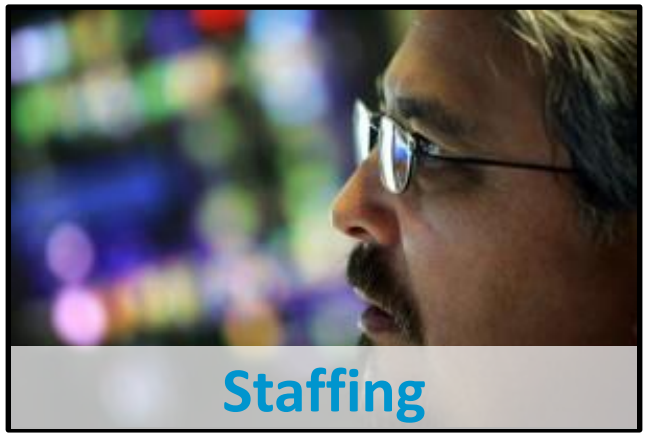
Kristof Verslype
Cryptographer, PhD
Smals Research

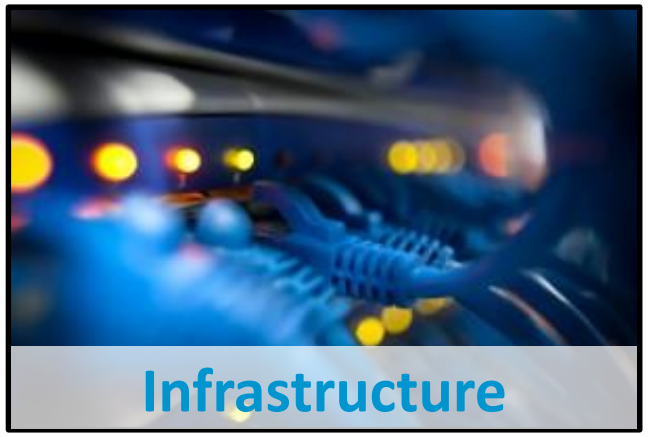
Smals
ICT for society

Smals
ICT for society

SUPPORT FOR E-GOVERNMENT







g-cloud

top EMPLOYER BELGIË BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

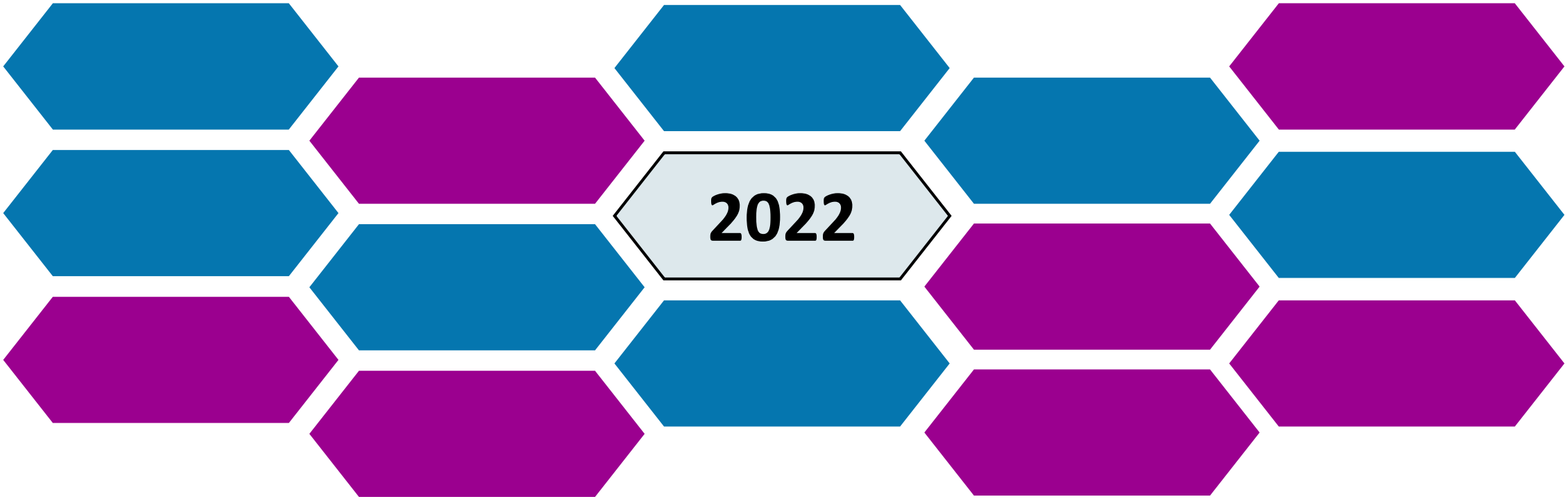
Smals Research 2022

Innovation with new technologies

Consultancy & expertise

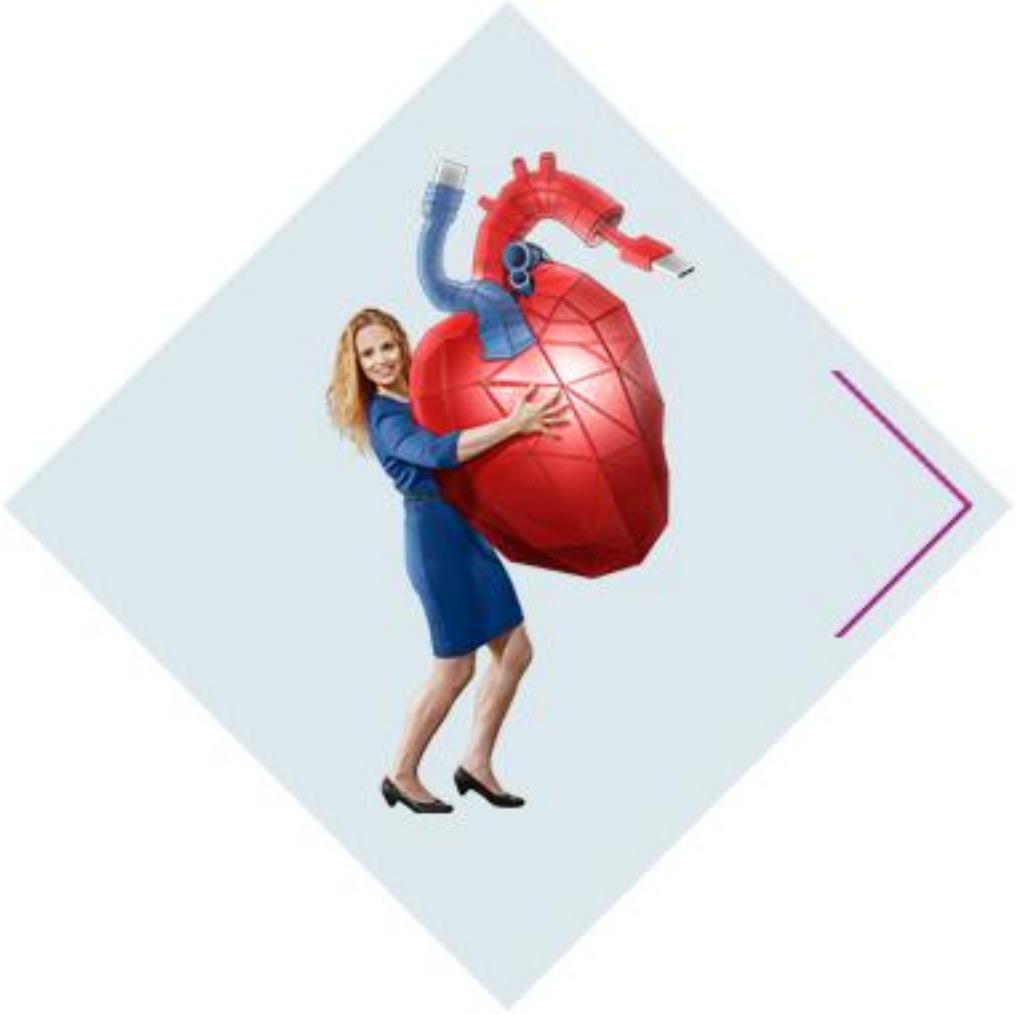
Internal & external knowledge transfer

Support for going live



Smals
ICT for society

www.smalsresearch.be



Agenda

- **In de media**
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- Kwantumresistente cryptografie
- Conclusies

DeMorgen. 21 februari 2019

Waarom Microsoft vol inzet op een kwantu

nature
International journal of science

Smals
ICT for society

Google claimt quantum supremacy

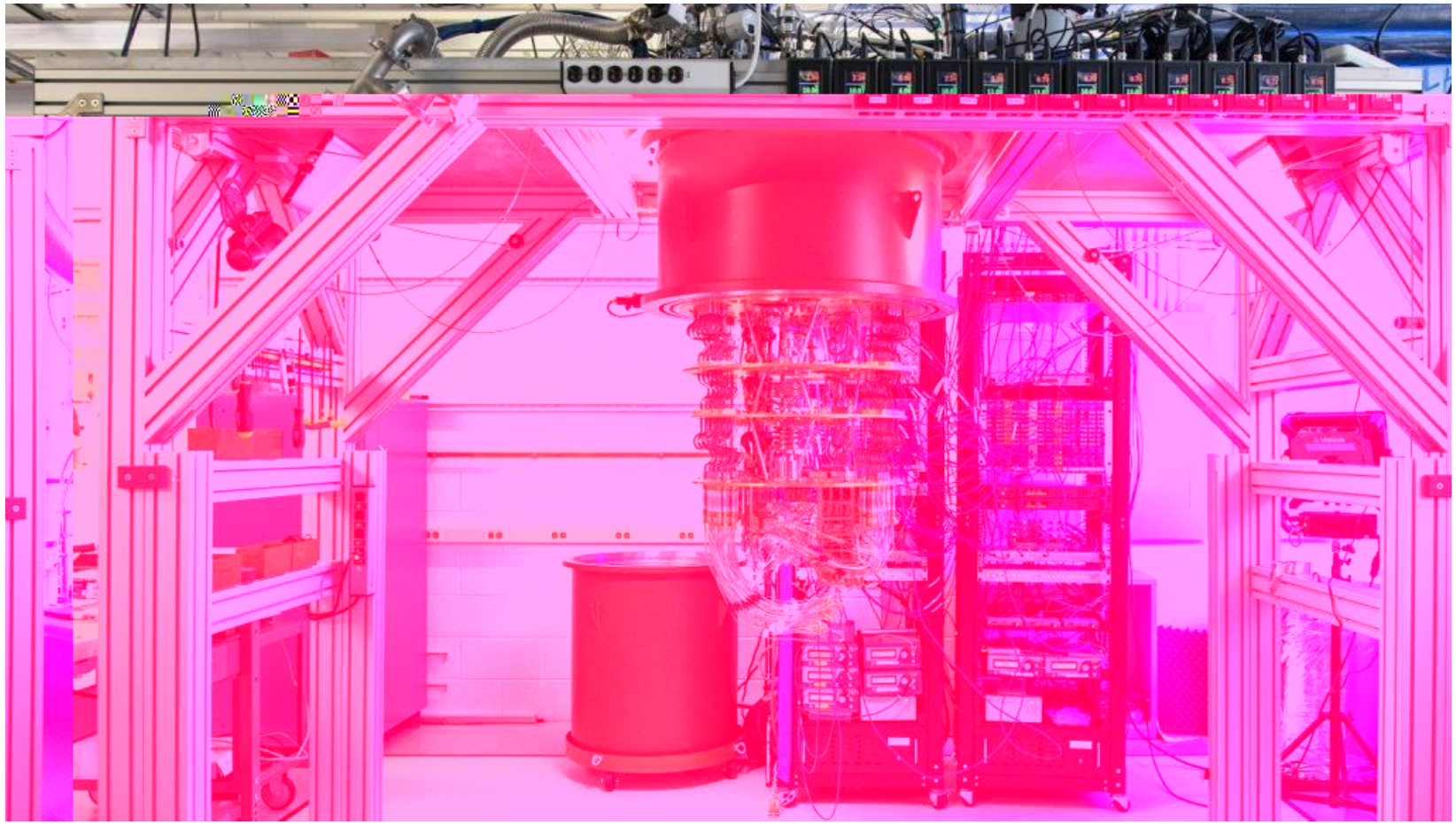
23 oktober 2019

Google

Article

Quantum supremacy using a programmable ng processor supercondictir

nature
International journal of science



Smals
ICT for society

China claimt quantum primacy

27 oktober 2021

PHYS.ORG

Two Chinese teams claim to have reached primacy with quantum computers

by Bob Yirka , Phys.org

The Pan team's optical quantum computer uses a 144-mode interferometer to solve a Gaussian boson

Two teams in China are claiming that they have reached primacy with their individu
quantum computers. Both have published the details of their work in the journal
Physical Review Letters.

Smals
ICT for society

THE BYTE.

27 januari 2022

Experts are warning that quantum computers could eventually overpower conventional **encryption methods**, a potentially dangerous fate for humanity that they're evocatively dubbing the "quantum apocalypse,

Is het kwantumleger in sneltempo aan het oprukken?

Retraction Watch, 24 April 2022

Authors retract second Majorana paper from Nature

A year after retracting a *Nature* paper claiming to find evidence for the elusive Majorana particle that many hope would have paved the way for a quantum computer, a group of researchers have retracted a second paper on the subject from the same journal.

Ettore Majorana

In the August 2017 paper "Epitaxy of advanced nanowire quantum devices," Erik Bakkers of QuTech and Kavli Institute of NanoScience, Delft University of Technology, in The Netherlands, and colleagues claim that

, waar Nederlandse natuurkundigen aan werkten, lijkt verder weg dan ooit. Voor de tweede keer in korte tijd moet de groep wetenschappers een publicatie [in het wetenschappelijk tijdschrift Nature] intrekken omdat er in het onderzoek fouten zijn ontstaan

De Morgen, 25 april 2022

Smals
ICT for society

Google claimt quantum supremacy

23 oktober 2019

Google


Article

premacy using a programmable
ting processor

Quantum sup
superconduc

nature
International journal of science

Quantum supremacy / Primacy

onmogelijk

Eén, in de praktijk nutteloos probleem, volstaat!

Niettemin is bouwen van kwantumomputer met 53 qubits zeer sterke prestatie

Het probleem

De claim

Onze Sycamore kwantumcomputer doet in 200 seconden waar een klassieke computer 10 000 jaar voor nodig heeft.

De reactie

IBM

Conservatief geschat kan dit in 2,5 dagen met een klassieke computer, bovendien met een veel hogere nauwkeurigheid

Koen Bertels

Simpelweg niet waar

als
society

China claimt quantum primacy

27 oktober 2021

PHYS.ORG

Two Chinese teams claim to have reached primacy with quantum computers

by Bob Yirka , Phys.org

The Pan team's optical quantum computer uses a 144-mode interferometer to solve a Gaussian boso

n ...

lual

Two teams in China are claiming that they have reached primacy with their indivic quantum computers. Both have published the details of their work in the journal *Physical Review Letters*.

Het probleem

De claim

10^{23} x sneller dan een klassieke supercomputer

De reactie

Opnieuw zeer sterke prestatie!
(O.a 56-qubit test)

Smals
ICT for society

De theoretische kracht van kwantumcomputers

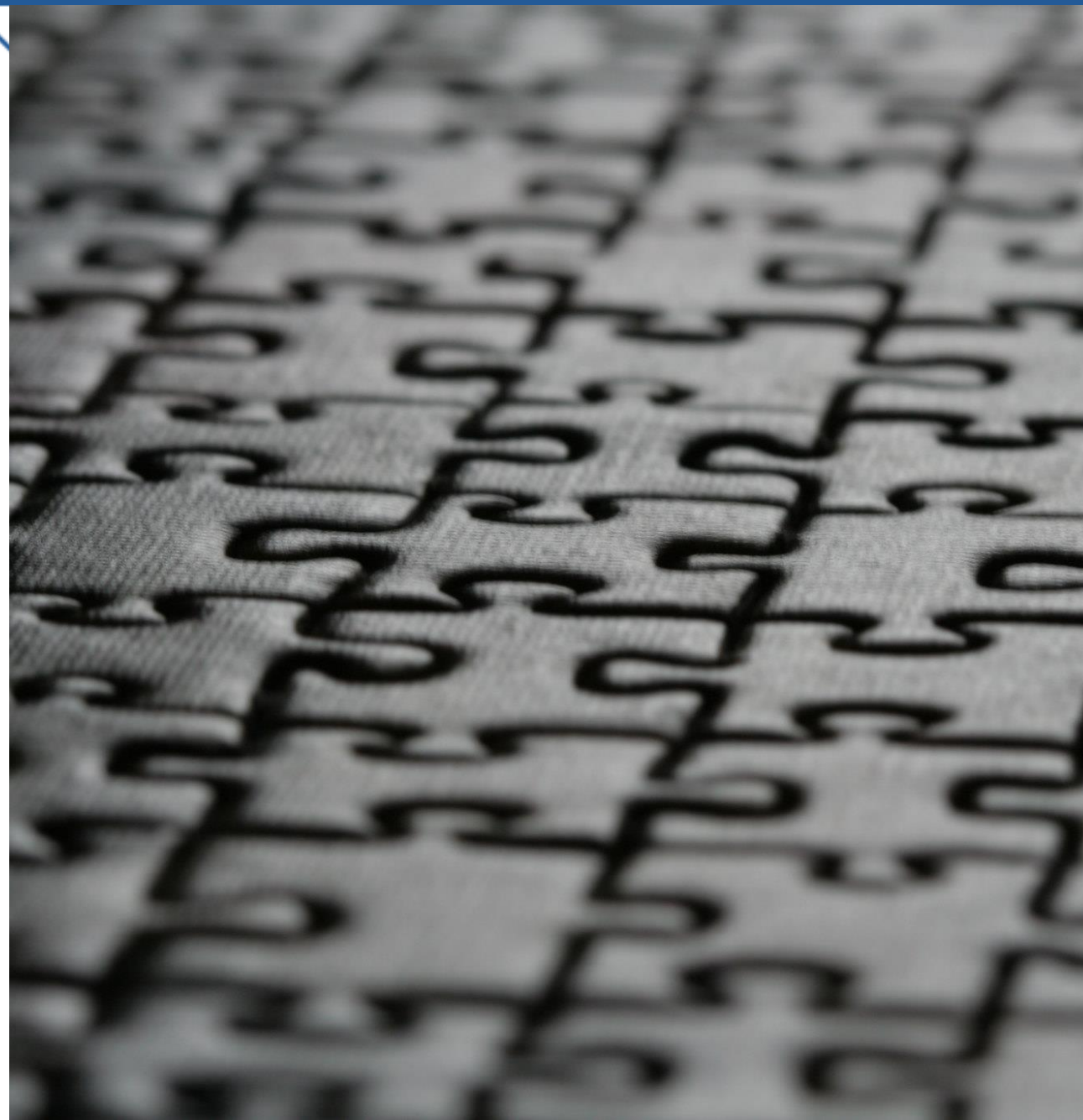
Ervaring
Als mensen iets niet begrijpen, geven ze er mythische eigenschappen aan.

Misvatting

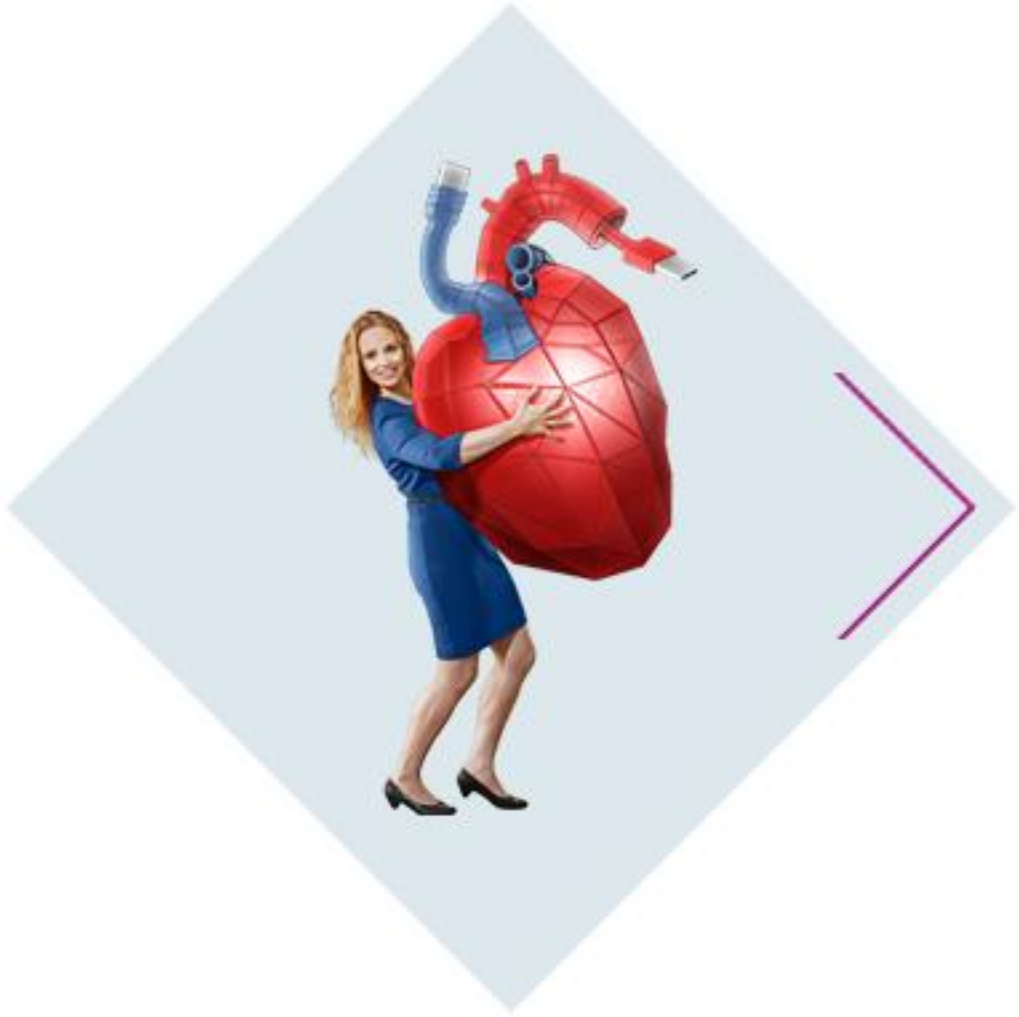
oplossen die moeilijk (of zelfs onmogelijk) zijn voor

Afhankelijk van probleem

- Waarschijnlijk geen noemenswaardige meerwaarde
  Vb. Combinatorische zoekproblemen zoals traveling salesman problem)
- Mogelijks *meerwaarde*
  Vb. Deep learning
- Duidelijke meerwaarde
  Vb. Simulaties natuurlijke processen
  Vb. Breken moderne cryptografie




CLICKBAIT



Agenda

- In de media
- **Kwantumcomputers (niet) in de praktijk**
- De crypto-apocalypse?
- Kwantumresistente cryptografie
- Conclusies

Principes kwantumcomputers

Kwantumtoestand

- **Superpositie**
- **Verstrengeling (entanglement)**

Kwantumtoestand

Smals
ICT for society

Historiek & State of the art

D-Wave

-
-
-
-
-

Een kwantumcomputer bouwen

Smals
ICT for society

Uitdaging 1: Isolatie

Interferentie

-
-
-

Coherence time

-
-

Manipuleren

-
-

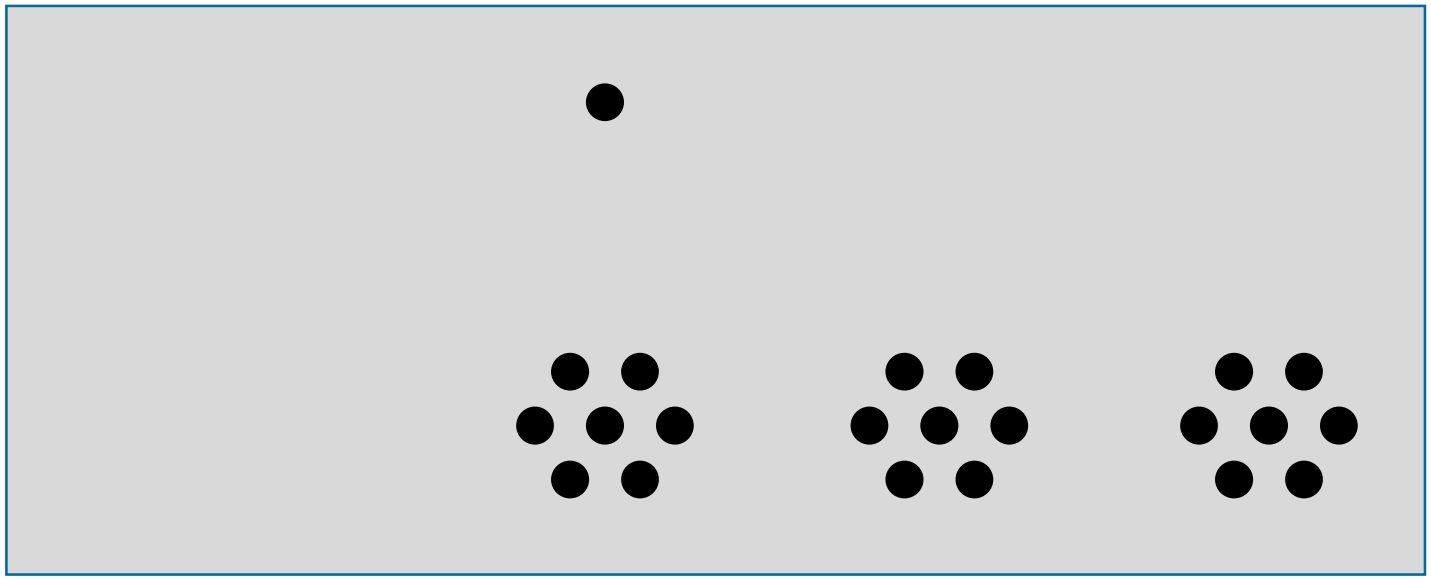
Evolutie

-
-

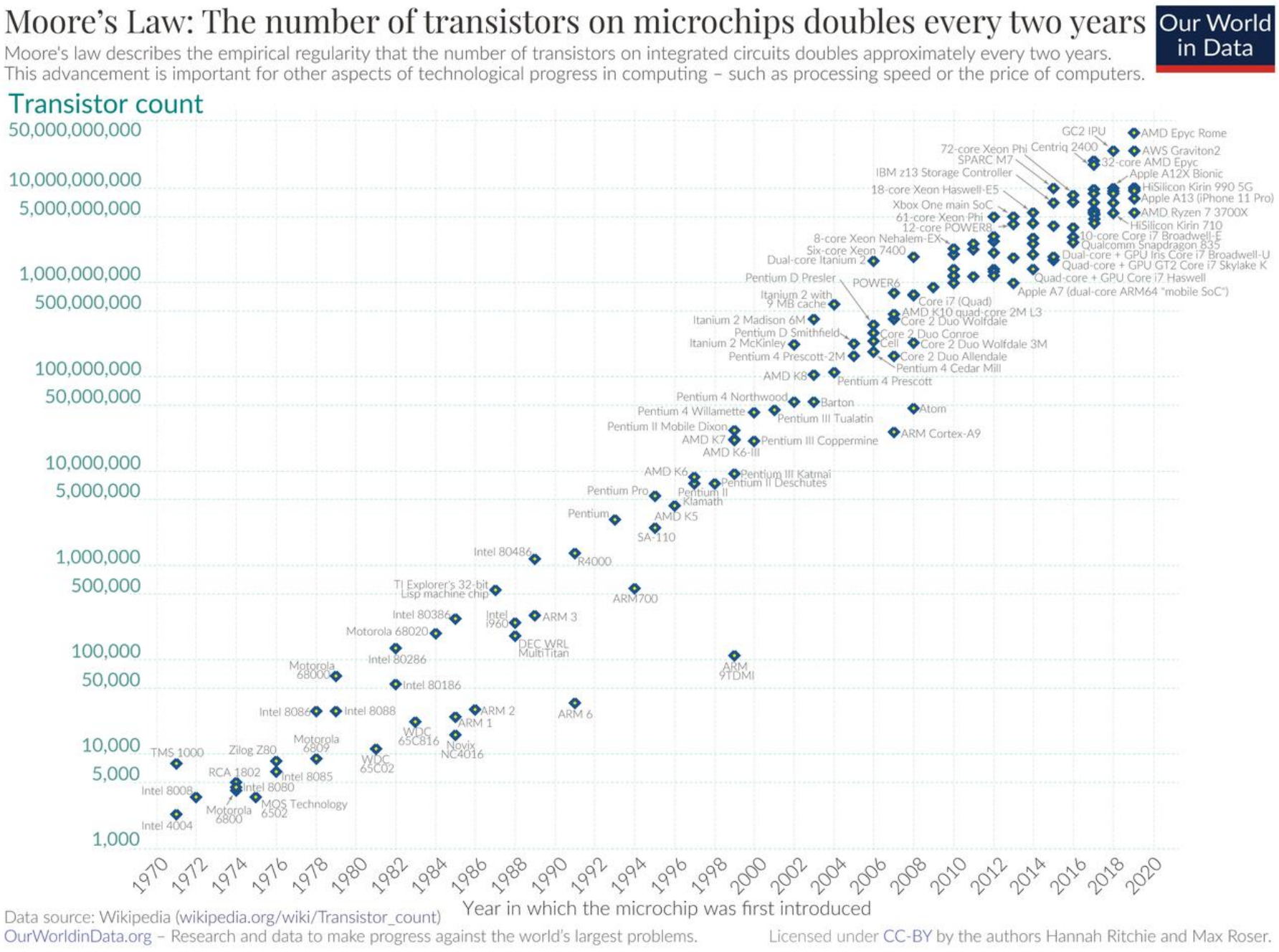
Smals
ICT for society

Uitdaging 2: Foutencorrectie

Fouten wellicht onvermijdelijk → foutencorrectie noodzakelijk



Uitdaging 3: Schaalbaarheid



Klassieke computer

-

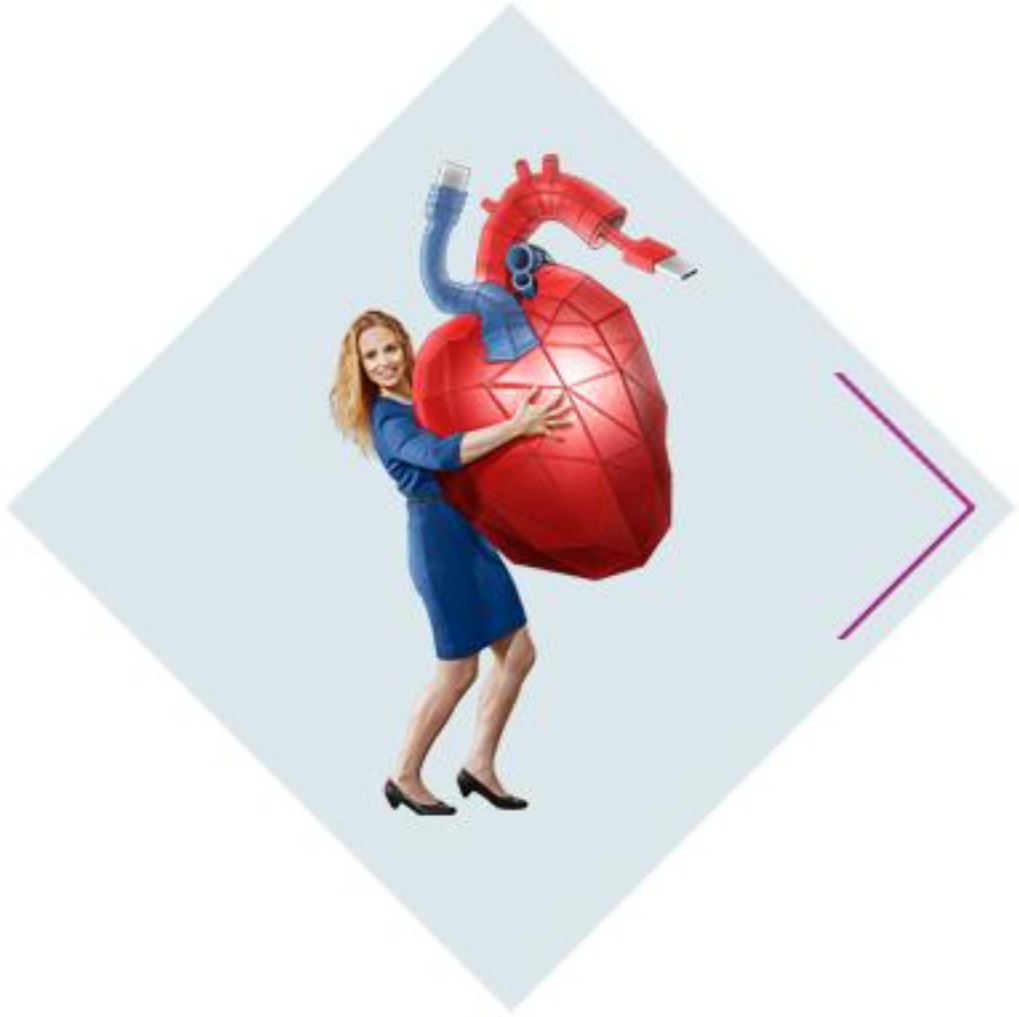
Kwantumcomputer

- $O(10) \longrightarrow O(107)$
-
-

Een kwantumcomputer bouwen

De uitdagingen zijn astronomisch!

Smals
ICT for society



Agenda

- In de media
- Kwantumcomputers (niet) in de praktijk
- **De crypto-apocalypse?**
- Kwantumresistente cryptografie
- Conclusies

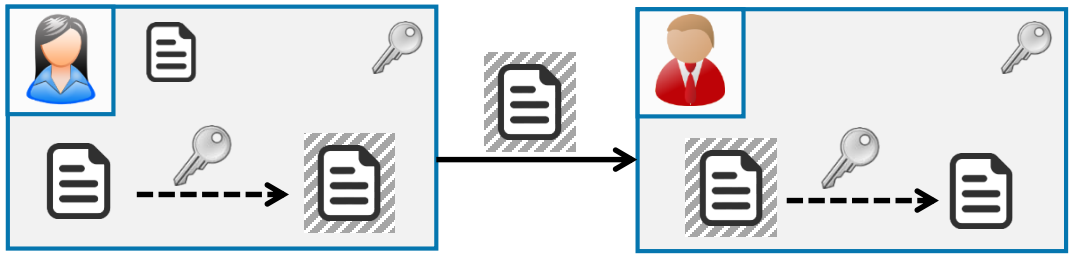
De crypto-apocalypse?

Impact kwantumcomputers op moderne cryptografie?

Smals
ICT for society

Symmetrische vercijfering

-
-



Kraken = vinden sleutel

Toy klassieke computer

-
-
-
- ±
-

Toy kwantumcomputer

-

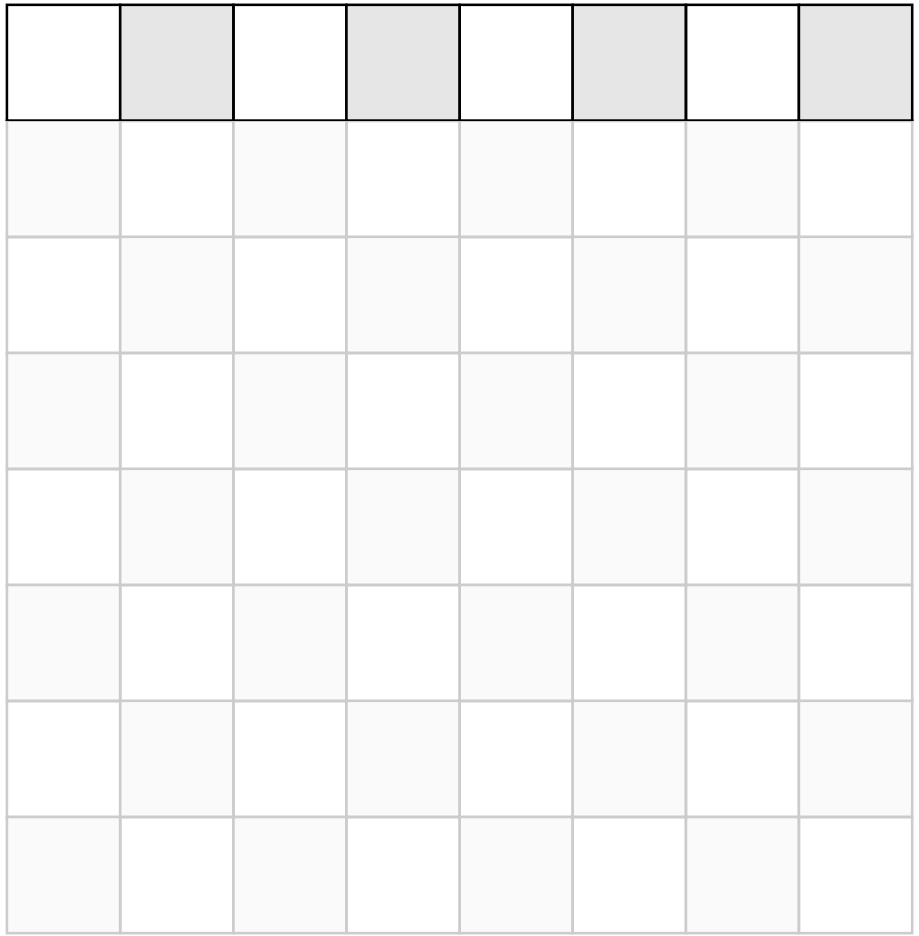
$$\sqrt{64}$$
$$3$$

-
-

Toy maatregel

-
-
- $\sqrt{4096}$

Zoekruimte



Smals
ICT for society

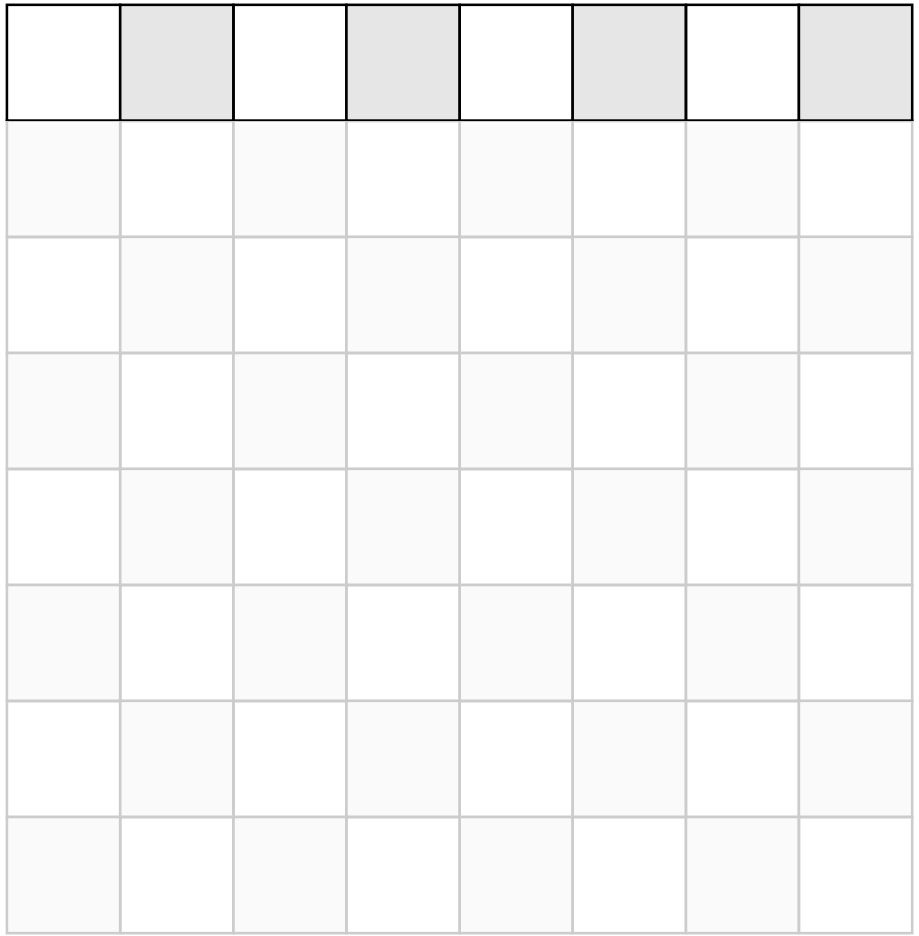
Algoritme van Grover op kwantumcomputer

Aantal vereiste LOGISCHE qubits

- ►
- ►
- ►
- ► **Verstrengeld**

Caveat

Zoekruimte

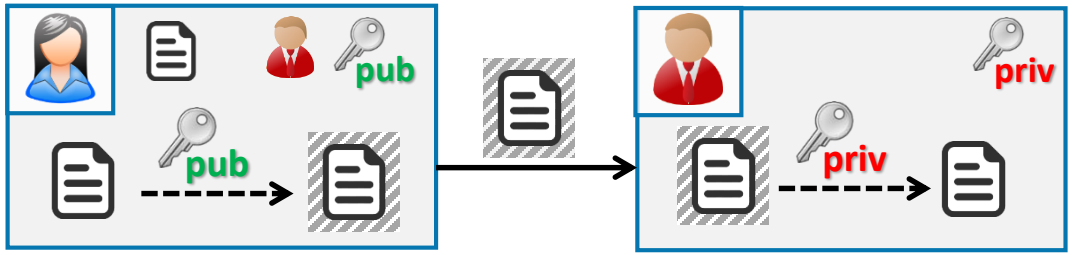


Smals
ICT for society

Krachtige kwantumcomputers vormen geen bedreiging voor symmetrische cryptografie

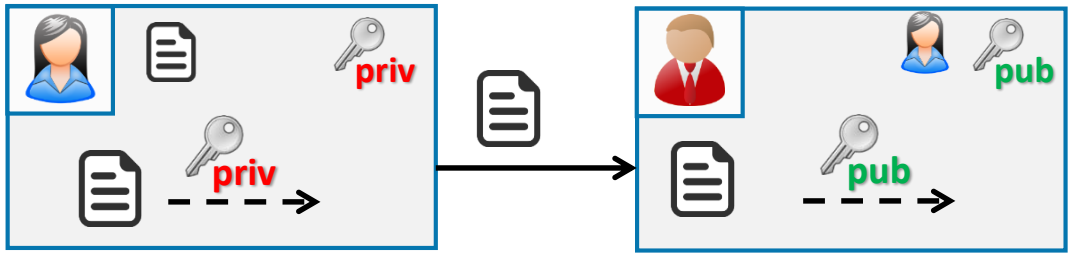
Publieke sleutel encryptie

-
-



Digitale handtekeningen

-
-



Ook authenticatie & opzetten veilige kanalen (TLS)

Priemgetal

Getal factoriseren

RSA aanname

Krachtige kwantumcomputer zou dit wel efficiënt kunnen m.b.v. algoritme van Shor

Voorbeeld

RSA-250 (829 bits) gepubliceerd in 1991

Werd in februari 2020 door klassieke computers gefactoriseerd

Publieke sleutelcryptografie – Factorisatie

Grootste RSA getal gefactoriseerd door klassieke computer
RSA-250 (829 bits)

RSA-2048 (2048 bits)

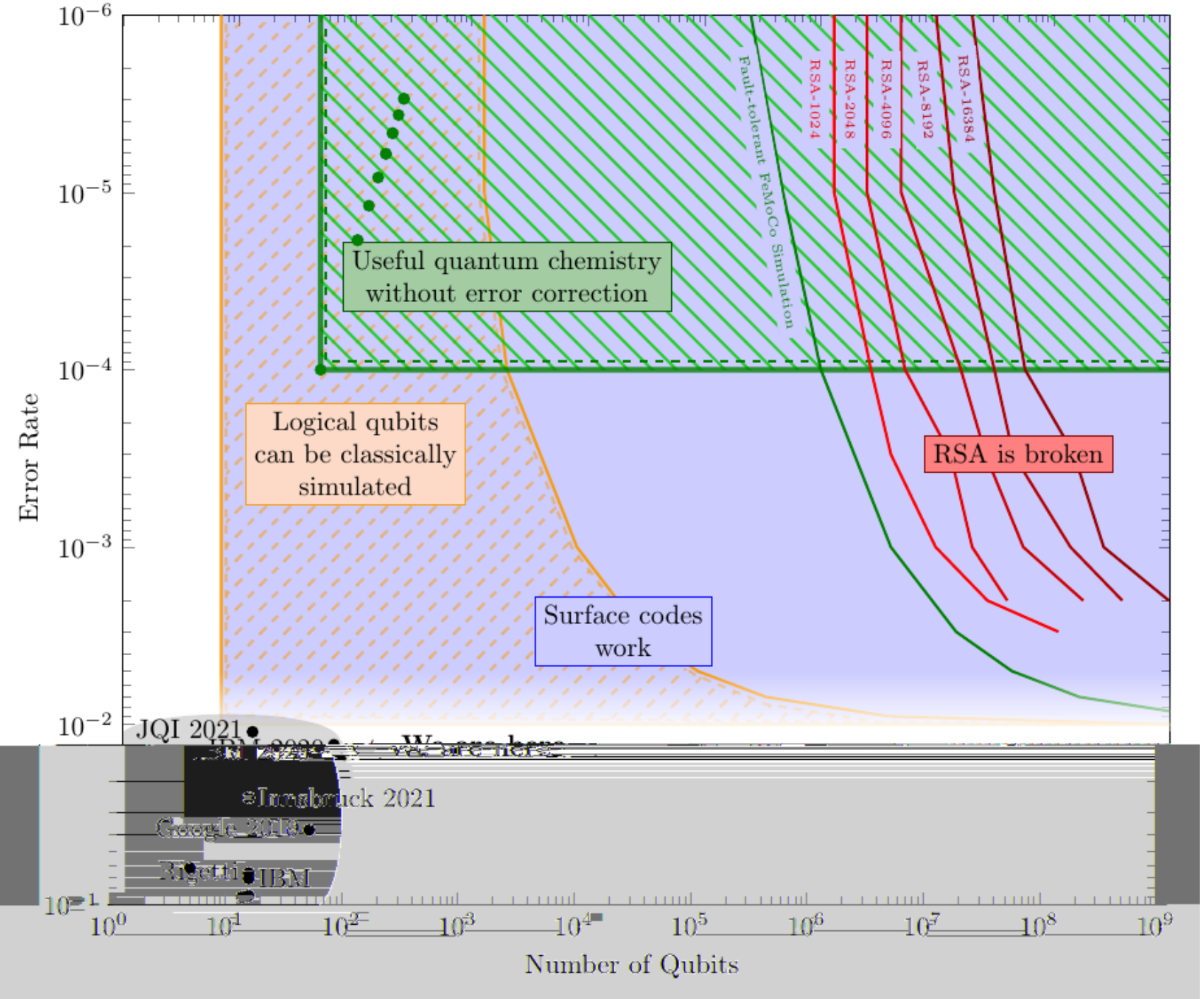
Grootste RSA getal gefactoriseerd met algoritme Shor door kwantumcomputer…

Algoritme van Shor (1994)

- Kwantumalgoritme om getallen te factoriseren (RSA)
- Ook toepasbaar op moderne cryptografie gebaseerd op elliptische

Algoritme	# bits security	# logische qubits	# fysieke qubits
*RSA-**1024***			
*RSA-**2048***			**20 miljoen**
*RSA-**3072***			
*RSA-**7680***			
*RSA-**15360***			

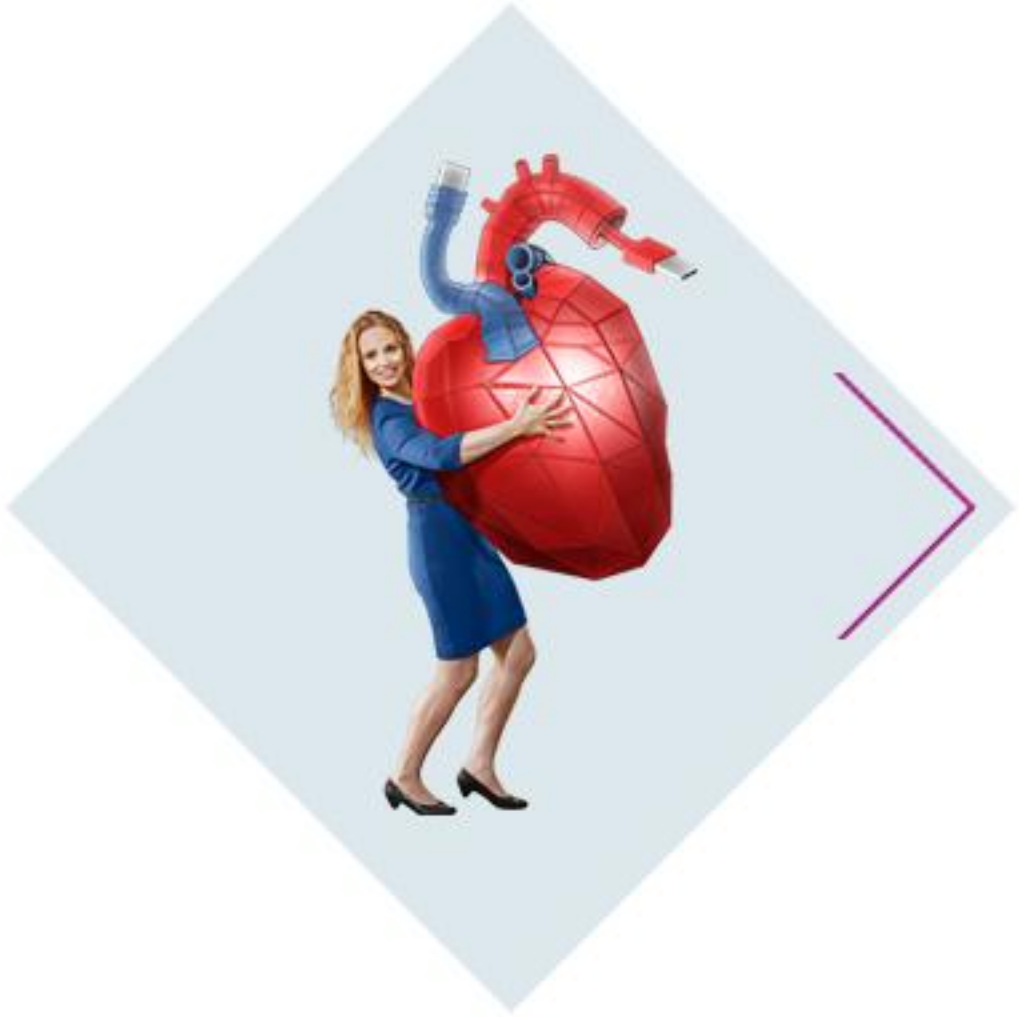
Krachtige kwantumcomputers met tientallen miljoenen fysieke qubits vormen een bedreiging voor publieke sleutelcryptografie



Surface codes = error correction

algorithm (to break RSA) likely require more than 1000 physical qubits per logical qubit

-law type scaling for quantum computers to ever be



Agenda

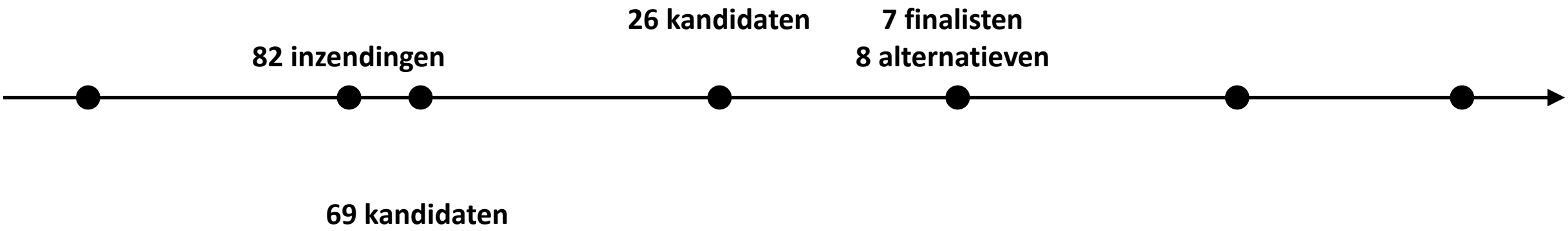
- In de media
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- **Kwantumresistente cryptografie**
- Conclusies

Kwantumresistente cryptografie – NIST standaardisatieprocedure

Twee luiken

- Public-key Encryption and Key-establishment Algorithms
- Digital Signature Algorithms

National Institute of Standards and Technology
U.S. Department of Commerce



nieuwe zwakheden ontdekt

uit te voeren op klassieke computer

Niet alles in NIST procedure

Smals ICT for society

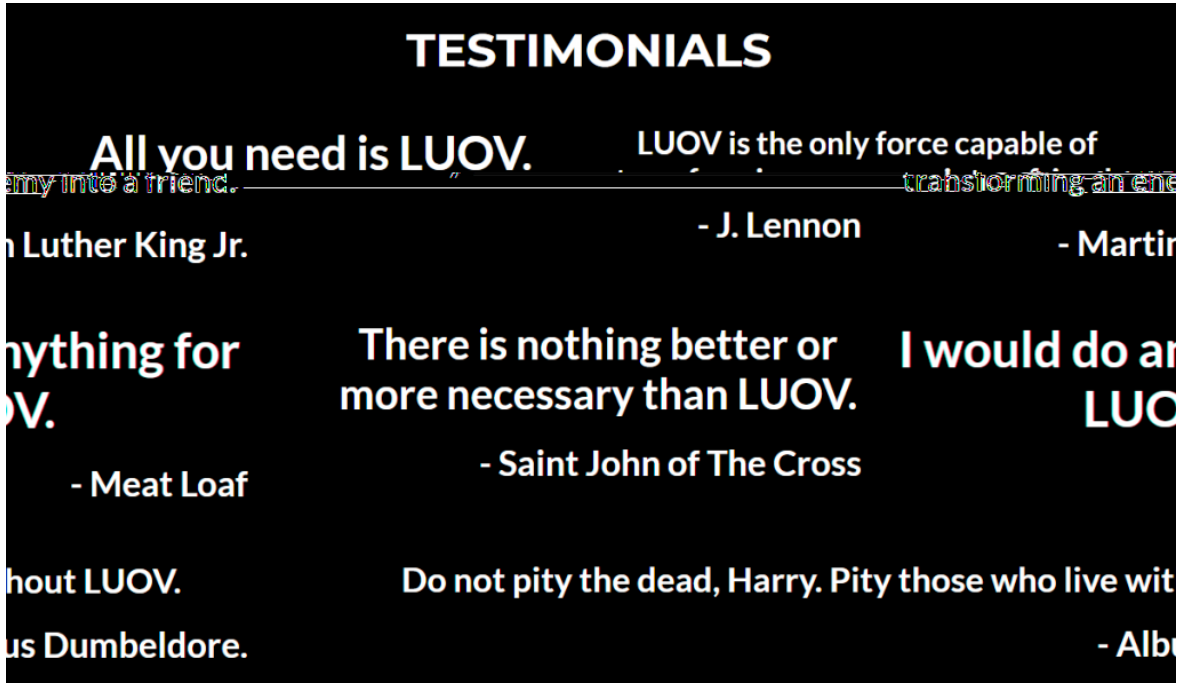
Kwantumresistente cryptografie – NIST standaardisatieprocedure

KU LEUVEN

COSIC

SABER
Public-key Encryption and Key-establishment Algorithms

LUOV
Digital Signature Algorithms



NIST

"Parameter sets of LUOV were significantly affected [by this type of attack]"
"Too new to be incorporated into a standard"

Smals
ICT for society

Kwantumresistente cryptografie – NSA

2015

-
-

2020

-
-

2021 FAQ

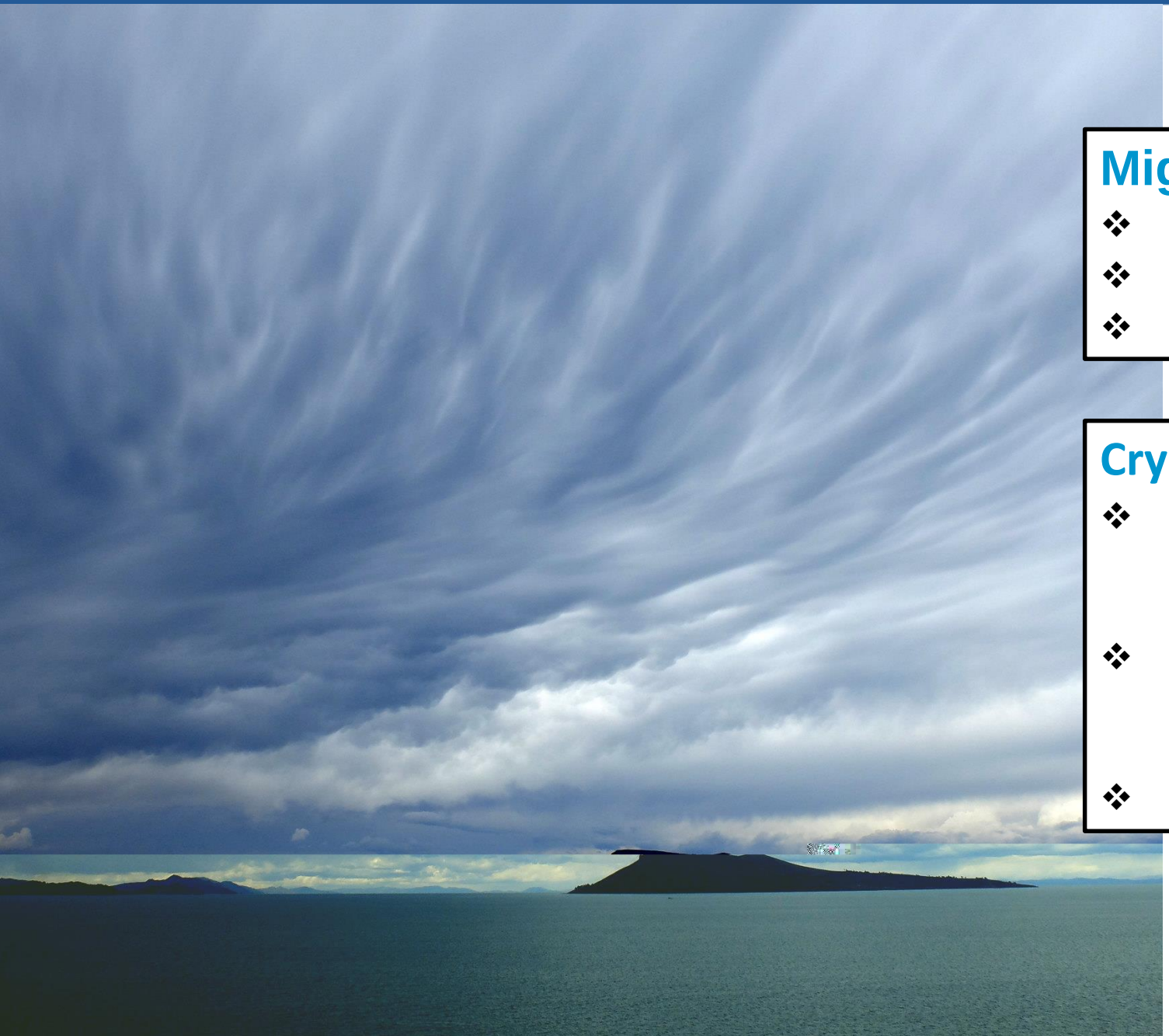
-
-
-

-

, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be.

IAD, defensieve tak NSA, 2015

Kwantumresistente cryptografie – Conclusie



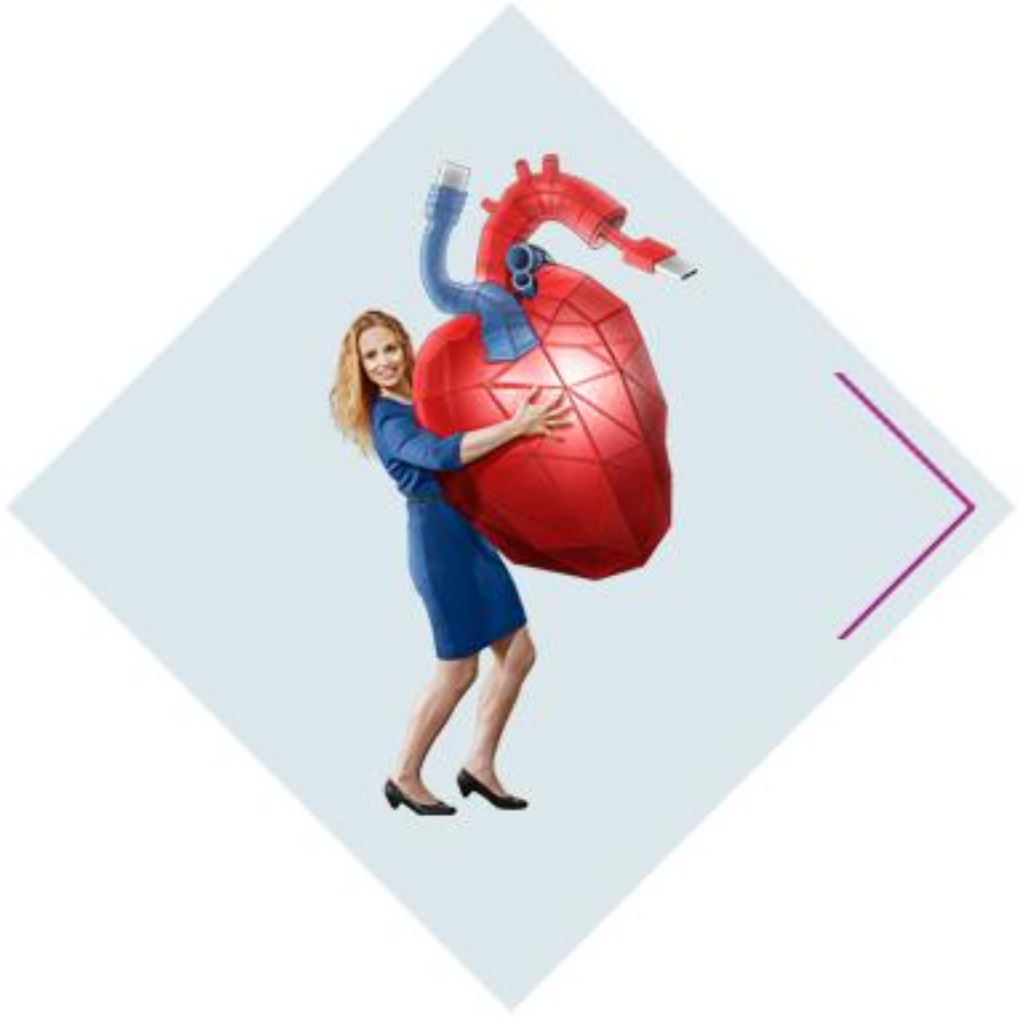
Migratie

-
-
-

Crypto agility ter voorbereiding

-
-
-

Smals
ICT for society



Agenda

- In de media
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- Kwantumresistente cryptografie
- **Conclusies**

Conclusie

Veel vooruitgang, nog veel meer hype

Bouw kwantumcomputers gigantisch complex
(Isolatie, foutencorrectie, schaalbaarheid)

Langere sleutels volstaan voor symmetrische crypto
Miljoen fysieke qubits vereist om publieke sleutelcryprografie te kraken

De NIST standaardistieprocedure loopt

Agenda

- In de media
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- Kwantumresistente cryptografie

That’s all!

Kristof Verslype
Cryptographer, PhD
Smals Research

Smals
ICT for society
Belgian public sector

kristof.verslype@smals.be
+32(0)2 7875376
www.smals.be
www.smalsresearch.be
www.cryptov.net
@KristofVerslype
linkedin.com/in/verslype

Smals
ICT for society

Referenties

Quantum supremacy using a programmable superconducting processor

Post-Quantum Cryptography – Project overview

Commercial National Security Algorithm Suite

Post-Quantum Cybersecurity Resources

Quantum computing has a hype problem. MIT Technology Review

Applying Grover's algorithm to AES: quantum resource estimates

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

The Case Against Quantum Computing

Vlaamse topwetenschappers blikken vooruit: Staat er in 2030 een kwantumcomputer in onze woonkamer?

The impact of quantum computing on present cryptography

- J. Preskill. *Quantum computing in the NISQ era and beyond*. Quantum. 2018 Aug 6;2:79. https://arxiv.org/abs/1801.00862

Smals ICT for society

Externe bronnen foto’s

Smals
ICT for society