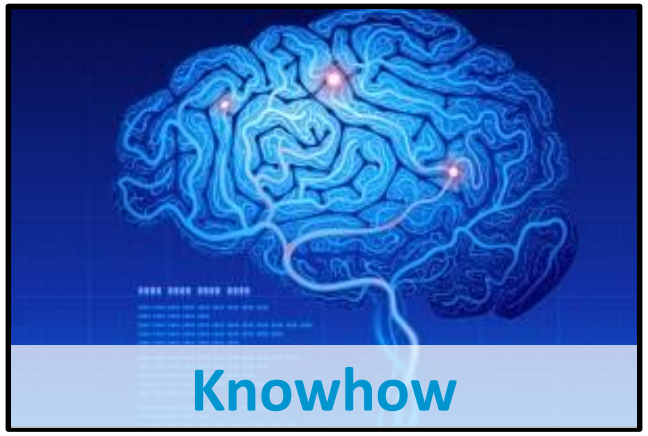
Kwantumcomputers Vs. Cryptografie

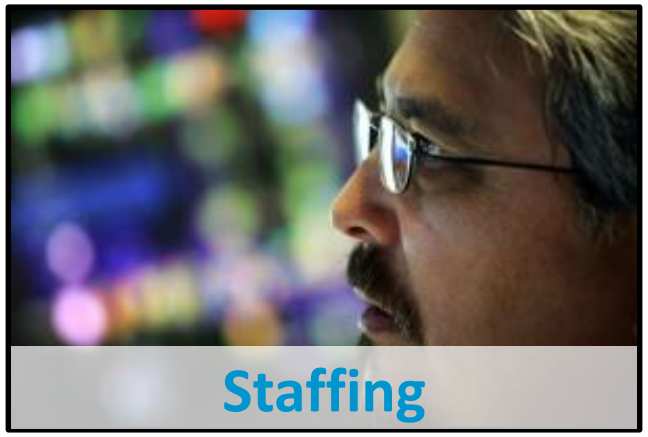
Kristof Verslype
Cryptographer, PhD
Smals Research

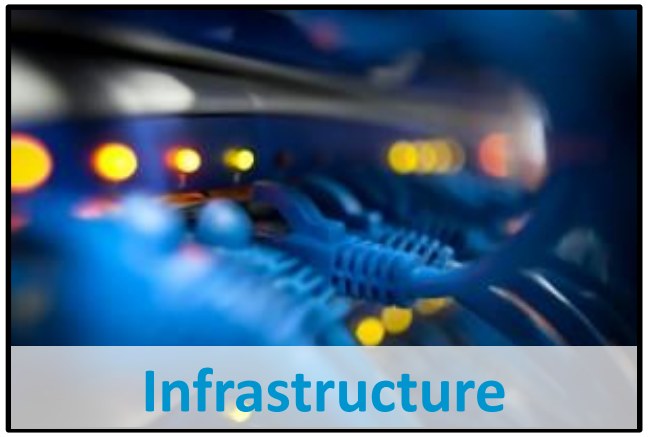
Smals
ICT for society

Smals
ICT for society

SUPPORT FOR E-GOVERNMENT







g-cloud

top EMPLOYER BELGIË BELGIQUE
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

WWW.SMALS.BE

Smals
ICT for society

Smals Research 2022

Innovation with new technologies

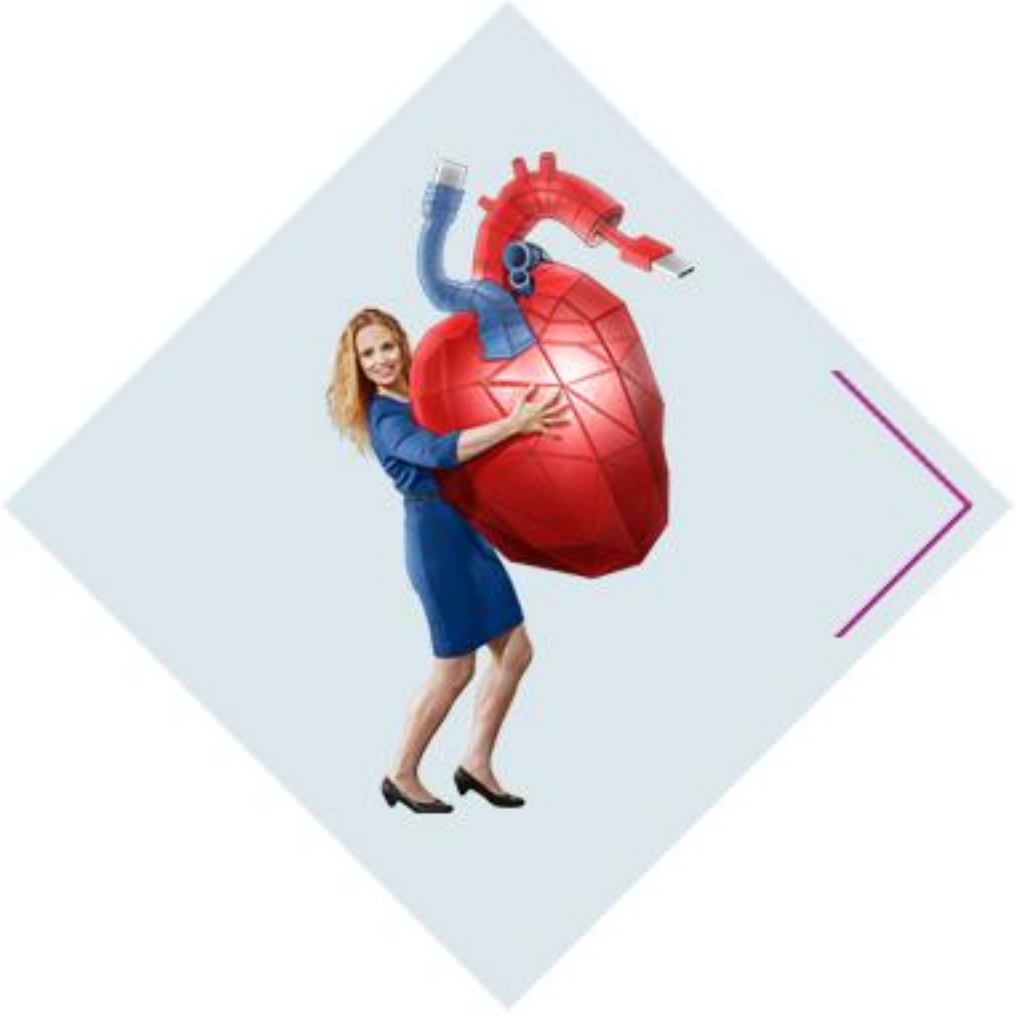
Consultancy & expertise

Internal & external knowledge transfer

Support for going live

2022

- Low Code Development
- AI-Augmented Software Development
- Resilient Application Architectures
- On-premise Cloud: Anthos
- GIS for Analytics
- Near real time Translation
- Passwordless Authentication using FIDO
- Flexible Authorization Management
- Recommender Systems
- Named Entity Recognition Service
- Approach for detecting AI Cases
- Pseudonymization Service
- Format-Preserving Encryption Service
- Synthetic Data



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 kwantumcomputerlab in Nederland

De Nederlandse koning Willem-Alexander tijdens de opening van het Microsoft Quantum Lab in Delft. Beeld EPA

Vandaag opent de Nederlandse koning Willem-Alexander in Delft het gloednieuwe Microsoft Quantum Lab. Daar werkt

nature
International journal of science

Smals
ICT for society

Google claimt quantum supremacy

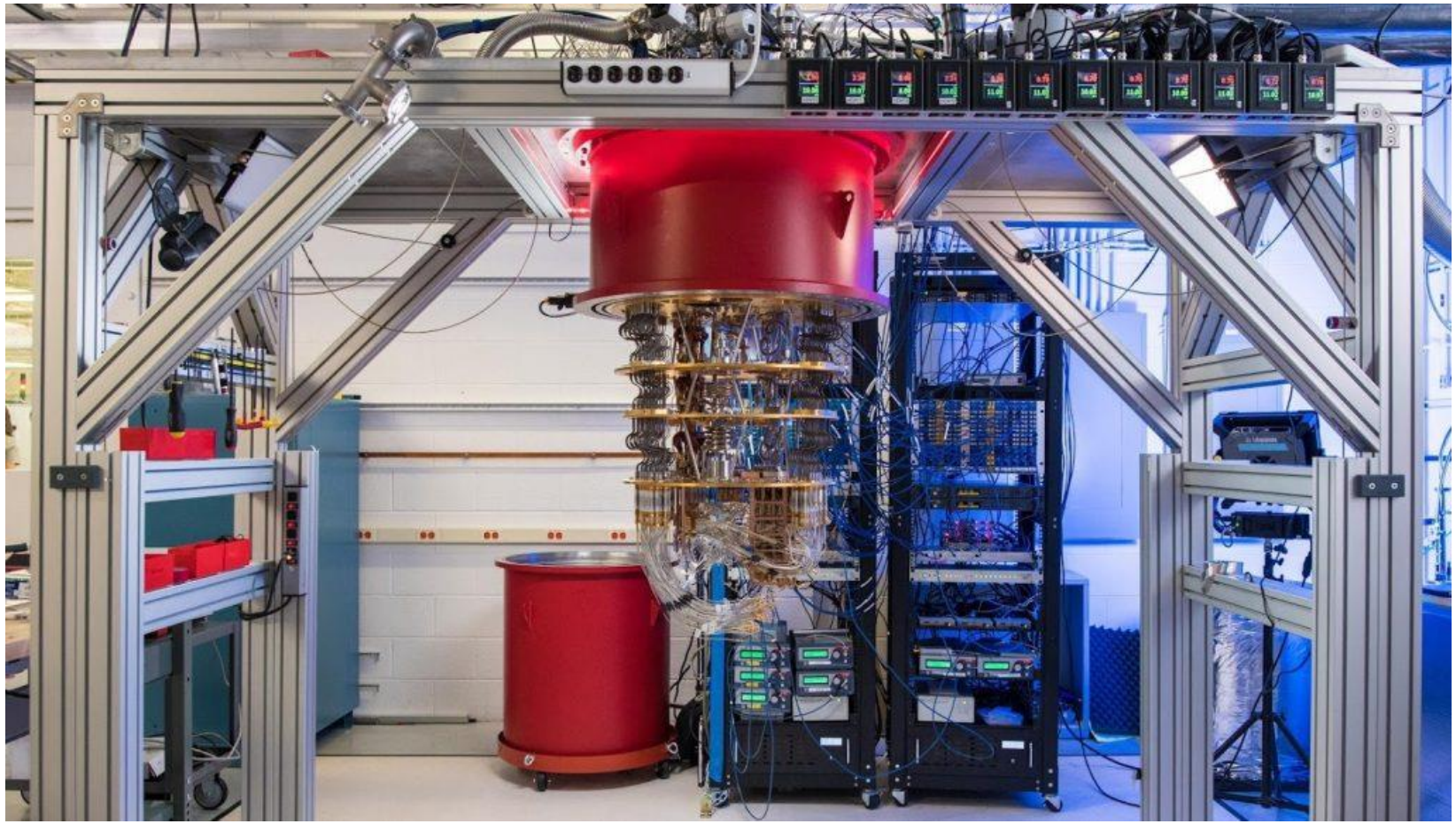
23 oktober 2019

Google

Article

Quantum supremacy using a programmable superconducting processor

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 individual quantum computers. Both have published the details of their work in the journal *Physical Review Letters*.

Smals ICT for society

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,

Smals
ICT for society

Is het kwantumleger in sneltempo aan het oprukken?

Smals
ICT for society

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

"Een kwantumcomputer, 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

Niettemin wordt er wereldwijd fors geïnvesteerd in quantum computing, met nu en dan significante doorbraken (maar de weg is nog lang)

Smals ICT for society

Google claimt quantum supremacy

23 oktober 2019

Google

Article

Quantum supremacy using a programmable superconducting processor

nature
International journal of science

Quantum supremacy / Primacy

Kwantumcomputer kan probleem oplossen dat in de praktijk **onmogelijk** is voor een klassieke computer.

Eén, in de praktijk nutteloos probleem, volstaat!

John Preskill, 2012

Niettemin is bouwen van kwantumomputer met 53 qubits zeer sterke prestatie

Het probleem

- Willekeurig kiezen getallen volgens specifieke distributie
- Op lijf geschreven van kwantumcomputer
- Niet echt nuttig

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**
  Hoofd Quantum Computer Architectures Lab, TU Delft
  "Simpelweg niet waar"

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 individual quantum computers. Both have published the details of their work in the journal *Physical Review Letters*.

Het probleem

- Simulatie voor berekenen waarschijnlijkheden output circuit met fotonen (kwantumeffecten)
- Op lijf geschreven van kwantumcomputer.
- Niet echt nuttig

De claim

"10^{23} x sneller dan een klassieke supercomputer"

De reactie

- Wordt niet gecontesteerd
- Deze keer lijkt quantum supremacy / primacy wel bereikt

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

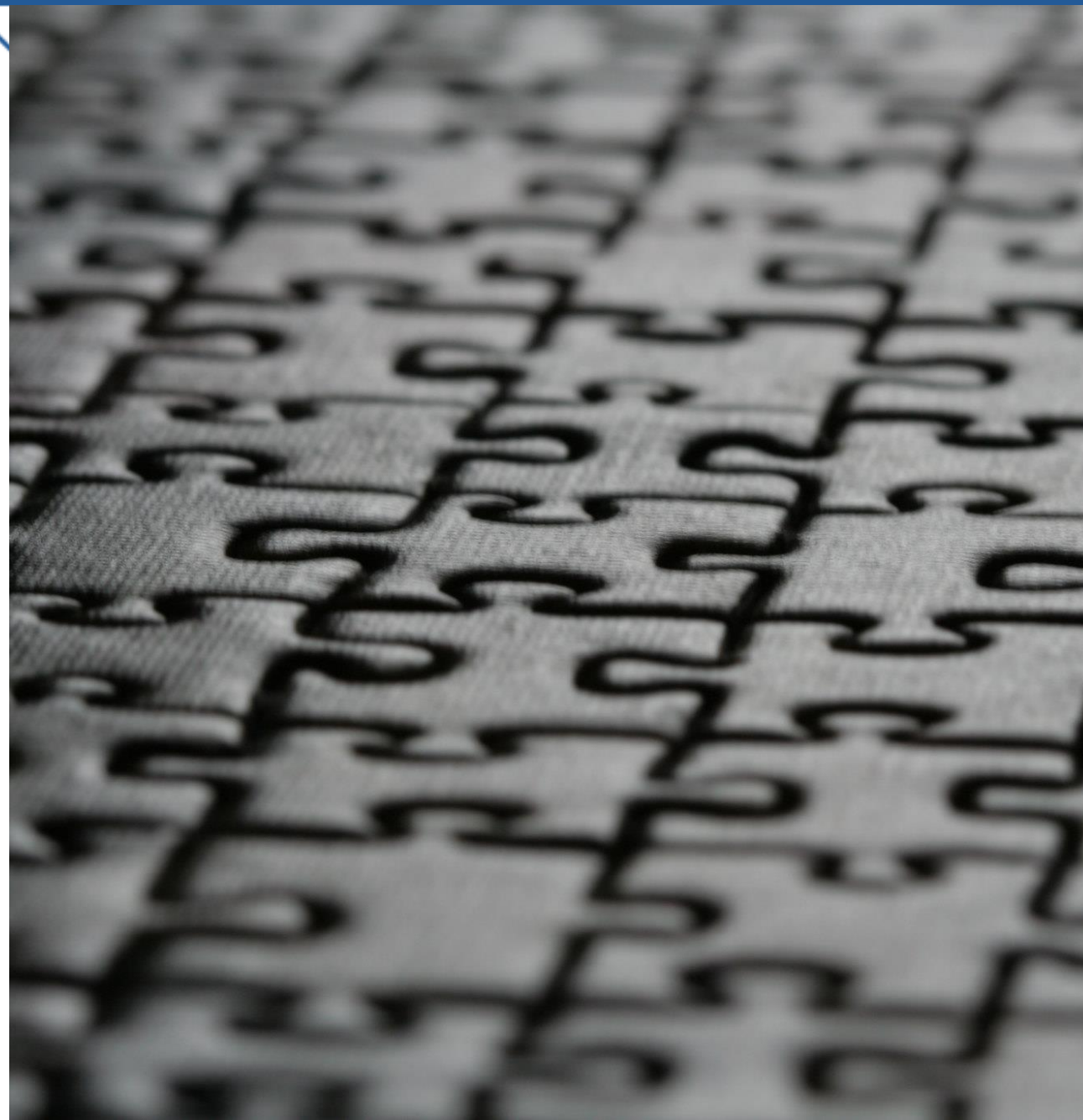
De theoretische kracht van kwantumcomputers

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

Misvatting
“Kwantumcomputers zullen alle problemen kunnen oplossen die moeilijk (of zelfs onmogelijk) zijn voor klassieke computers.”

Afhankelijk van probleem

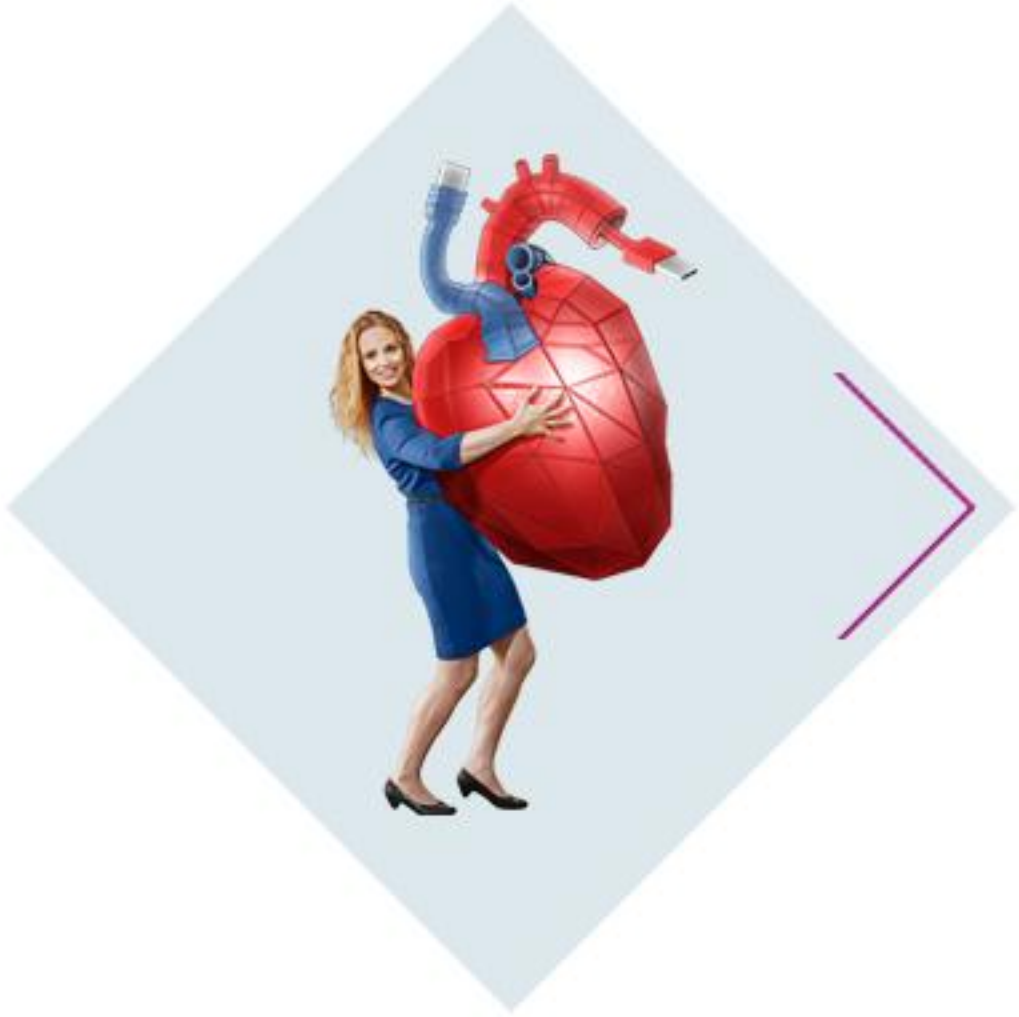
- Waarschijnlijk geen noemenswaardige meerwaarde
  Vb. Combinatorische zoekproblemen zoals traveling salesman problem)
- Mogelijks *meerwaarde*
  Vb. Deep learning
- Duidelijke meerwaarde
  Vb. Simulaties natuurlijke processen
  Vb. Breken moderne cryptografie



THE BYTE.

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,

Smals ICT for society



Agenda

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

Kwantumtoestand

- **Superpositie**
  Waarde qubit onbepaald tot op moment van meting
- **Verstrengeling (entanglement)**
  Meting ene qubit heeft impact op uitkomst meting andere qubit

Kwantumtoestand

Smals
ICT for society

Historiek & State of the art

1e helft 20e eeuw
Ontwikkeling
Kwantummechanica

1980-1982
Idee kwantumcomputer
(Benioff, Feynman, Manin)

1998
Eerste kwantumcomputer
2 qubits

11/2017
IBM Q 20 Tokyo
20 qubits

3/2018
Google Bristlecone
72 qubits

7/2019
Google Sycamore
54 qubits (53 effectief)

9/2020
D-Wave Advantage
5000 qubits

11/2021
Jiuzhang 2
60 qubits

1/2017
D-Wave 2000Q
2048 qubits

D-Wave

- Vereist minder verstrengeling
- Maar wel meer qubits
- Oorspronkelijk gericht op optimalisatievraagstukken
- Theoretisch zelfde mogelijkheden als circuit-based kwantumcomputer
- Laten we verder buiten beschouwing

11/2021
IBM EAGLE
127 qubits

uantum_processors

Smals
ICT for society

Een kwantumcomputer bouwen

Waarom is het bouwen van een kwantumcomputer zo complex?

- Isolatie
- Foutencorrectie
- Schaalbaarheid

Uitdaging 1: Isolatie

Interferentie

- Kwantumtoestand enorm gevoelig voor interferentie buitenaf
- Temperaturen dicht tegen absolute nulpunt (-273,15° C)
- Afgeschermd van trillingen, licht & magnetische straling

Coherence time

- Uitdaging: voldoende lang coherent houden kwantumtoestand
- Googles Sycamore: tienden of honderdsten van een microseconde

Manipuleren

- Kwantum logische poorten zijn foutgevoelig
- Uitlezen

Evolutie

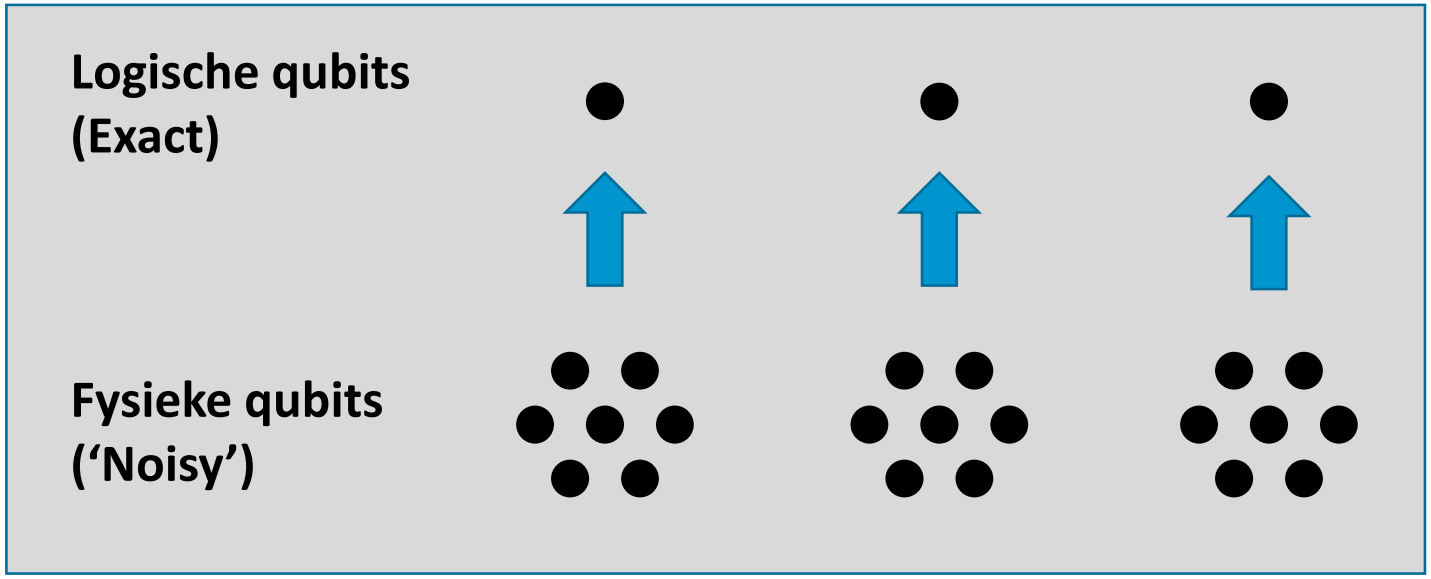
- Veel vooruitgang geboekt voorbije jaren
- Toch fouten wellicht onvermijdelijk

Smals
ICT for society

Uitdaging 2: Foutencorrectie

Fouten wellicht onvermijdelijk → foutencorrectie noodzakelijk

Meerdere fysieke qubits vormen samen 1 logische qubit



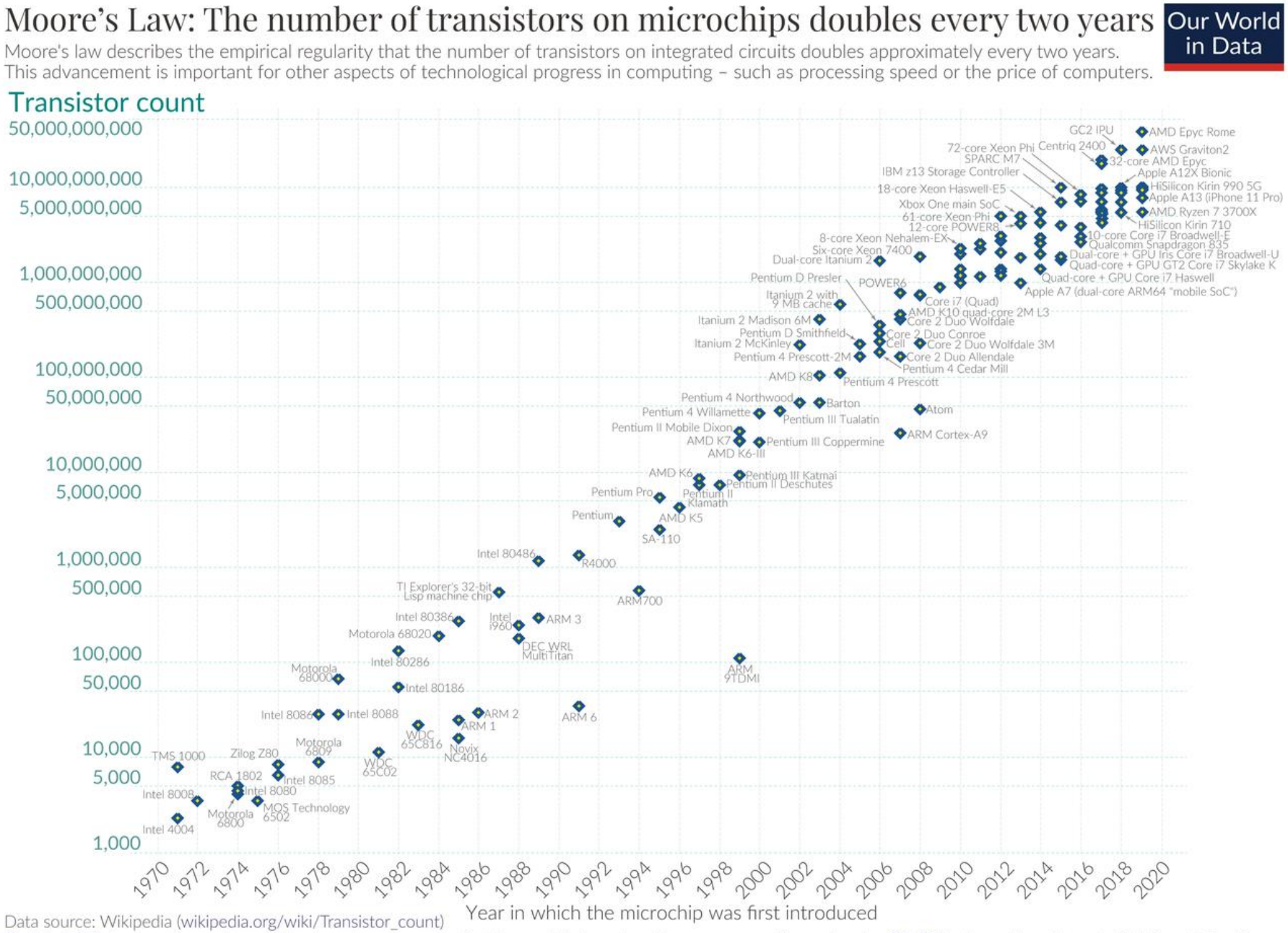
Evolutie

- Jaren '80 en '90: "*onmogelijk!*"
- Theoretisch mogelijk
- Nog geen experimenten

Vereisten

- Vereist voldoende lange coherence time
- Schattingen: 1000 tot 100 000 fysieke qubits per logische
  - Noise fysieke qubits
  - Lengte van het circuit

Uitdaging 3: Schaalbaarheid



Klassieke computer

- Aantal transistors op een chip verdubbelt elke x (12, 18, 24) maand

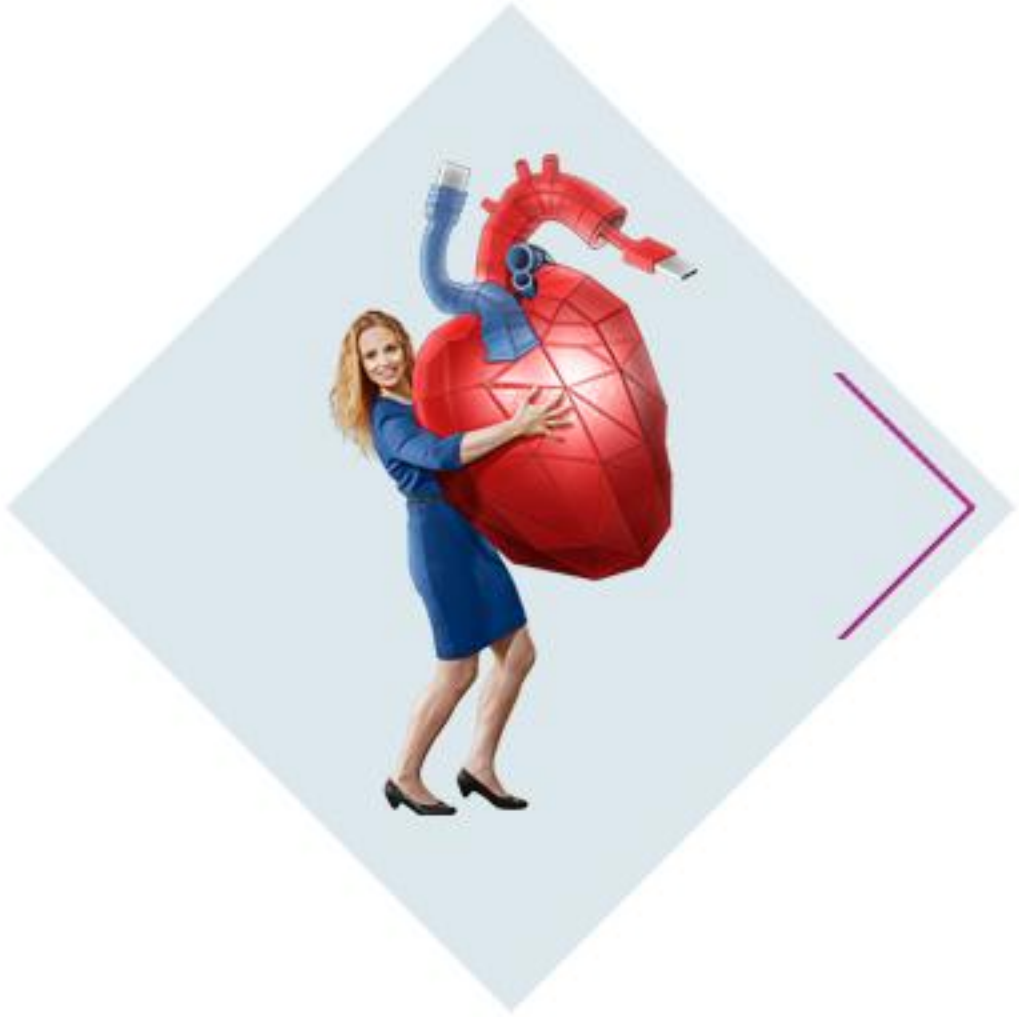
Kwantumcomputer

- $O(10) \longrightarrow O(107)$
- Zal eveneens een exponentïele groei nodig hebben
- Die voldoende lang aangehouden moet worden

Waarom is het bouwen van een kwantumcomputer zo complex?

- Isolatie
- Foutencorrectie
- Schaalbaarheid

De uitdagingen zijn astronomisch!



Agenda

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

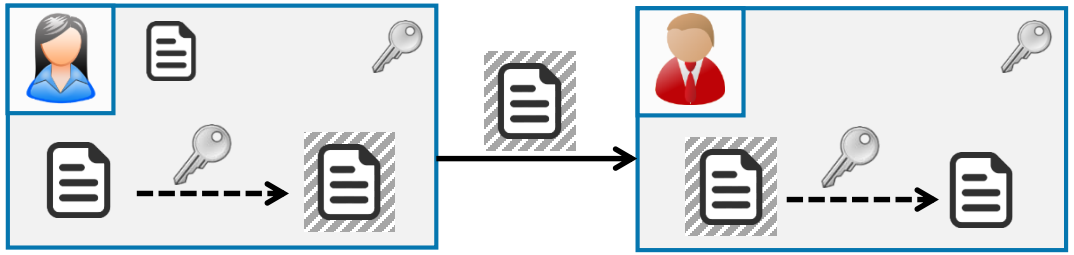
Impact kwantumcomputers op moderne cryptografie?

Symmetrische cryptografie

Publieke sleutelcryptografie

Symmetrische vercijfering

- Encryptie en decryptie met dezelfde sleutel
- AES



Kraken = vinden sleutel

Toy klassieke computer

- Sleutellengte = ~~6 bits~~ 128 bits
- $8^2 = 2^6 = 64$ mogelijke sleutels (= de zoekruimte)
- Veiligheid = 6 bit
- Beste aanval is ± één na één aflopen van de sleutels
- Gemiddeld wordt sleutel gevonden na 32 pogingen

Toy kwantumcomputer

- Belooft kwadratische versnelling:
  Zoekruimte verkleint van 64 naar $\sqrt{64} = 8$
- Veiligheid daalt tot 3 bit, want $8 = 2^3$
- Gemiddeld wordt sleutel gevonden na 4 pogingen

Toy maatregel

128 → 256 bits

- Verdubbelen sleutellengte: ~~6 → 12 bits~~
- $2^{12} = 64^2 = 4096$ mogelijke sleutels
- Zoekruimte voor kwantumcomputers: $\sqrt{4096} = 64$

Zoekruimte

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Smals ICT for society

Algoritme van Grover op kwantumcomputer

Aantal vereiste LOGISCHE qubits

- AES-128: 2953,
- AES-192: 4449
- AES-256: 6681
- **Verstrengeld**

Caveat

Eerst moet een “kwantum orakel” gebouwd worden. Deze stap doet de performantiewinst van Grover’s algorithm mogelijk teniet

Zoekruimte

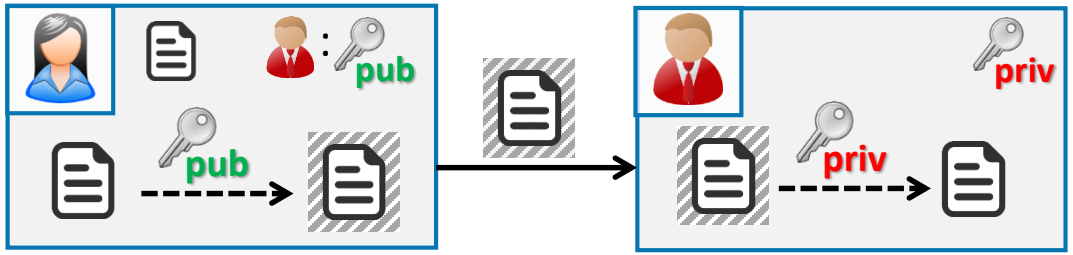
0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Krachtige kwantumcomputers vormen geen bedreiging voor symmetrische cryptografie

(Uit voorzorg wel voldoende lange sleutels nemen)

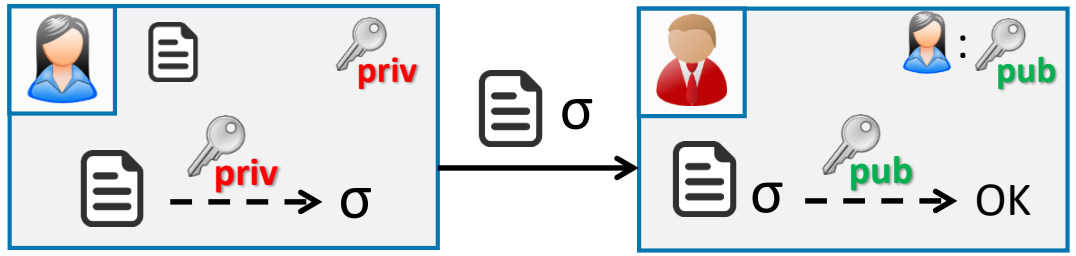
Publieke sleutel encryptie

- Confidentialiteit
- Encryptie en decryptie met verschillende sleutel



Digitale handtekeningen

- Integriteit, authenticiteit
- Vb. BE eID



Ook authenticatie & opzetten veilige kanalen (TLS)

Meest courante systemen gebaseerd op
RSA of elliptische krommen

Priemgetal

Natuurlijk getal enkel deelbaar door 1 en zichzelf
Vb. 2, 3, 5, 7, 11, 13, 17, 19, 23, …

Getal factoriseren

Ontbinden in priemfactoren
vb. $12 = 2^2 * 3$

RSA aanname

Er bestaat geen efficiënt algoritme om een getal dat het product is van twee grote priemgetallen, te factoriseren. In de praktijk onhaalbaar wanneer voldoende grote priemgetallen gekozen.

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

Voorbeeld

RSA-250 (829 bits) gepubliceerd in 1991

21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979377

=

64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367

×

33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711

Werd in februari 2020 door klassieke computers gefactoriseerd

Publieke sleutelcryptografie – Factorisatie

Grootste RSA getal gefactoriseerd door klassieke computer
RSA-250 (829 bits)
21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979371

(in 2020, 2700 core-years)

Grootste RSA getal gefactoriseerd met algoritme Shor door kwantumcomputer…
21
(in 2012)

Disclaimer: Kwantumcomputers factoriseerden reeds grotere, zeer specifiek gekozen getallen zonder het algoritme van Shor.

RSA-2048 (2048 bits)
25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404536402352738195137863656439121201039712282212072035 7

Algoritme van Shor (1994)

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

RSA

Algoritme	# bits security	# logische qubits	# fysieke qubits
*RSA-**1024***	80	± 2048	
*RSA-**2048***	112	± 4096	**20 miljoen** (8 uur, 2019)
*RSA-**3072***	128	± 6144	
*RSA-**7680***	192	± 15360	
*RSA-**15360***	256	± 30720	

x2

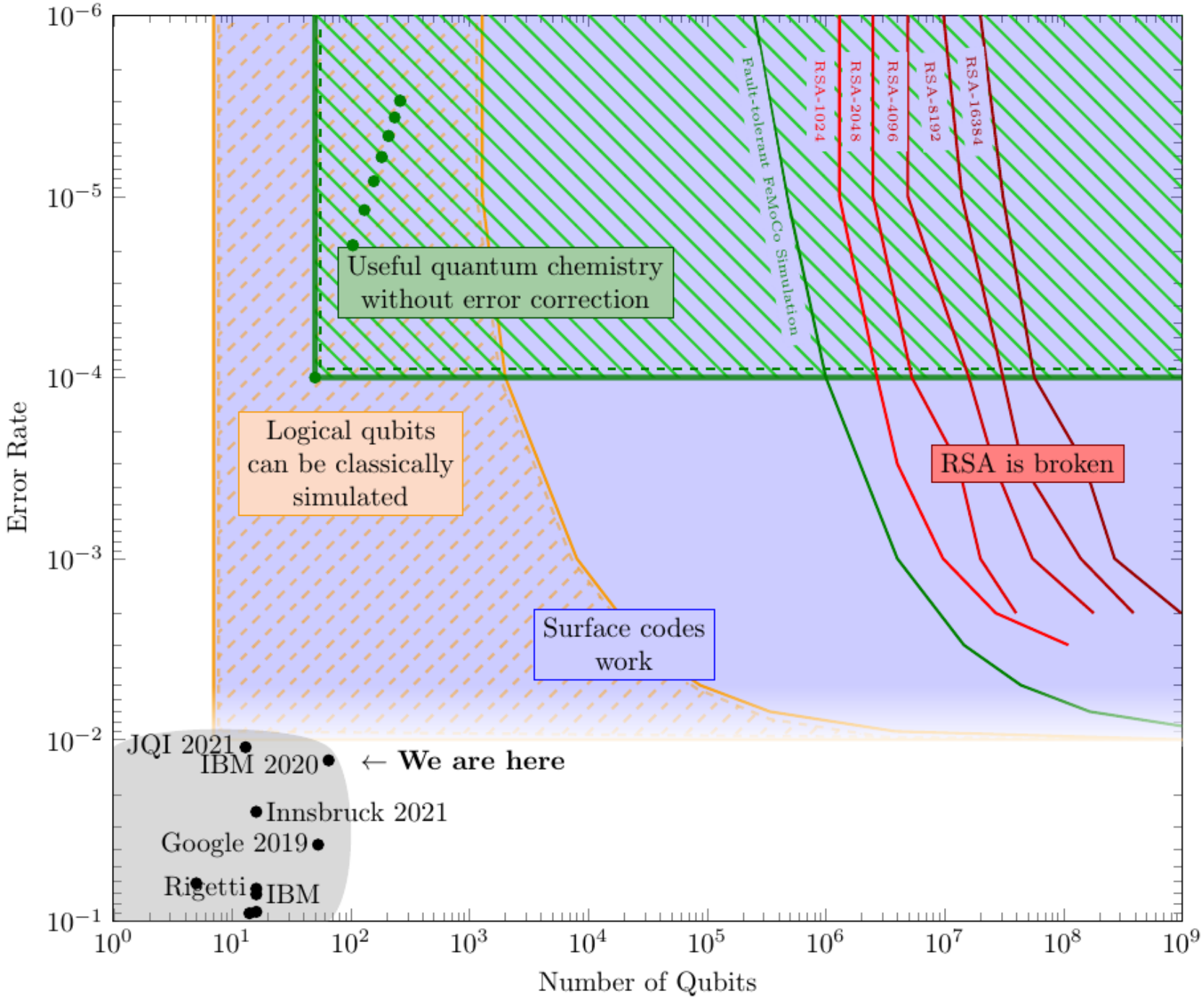
Elliptische krommen

Algoritme	# bits security	# logische qubits	# fysieke qubits
*P-**256** = secp256r1*	128	± 1536	**13 miljoen** (24 uur, 2022)
*P-**384** = secp384r1*	192	± 2304	
*P-**521** = secp521r1*	256	± 3126	

x6

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

(Maar daar zijn we nog niet)

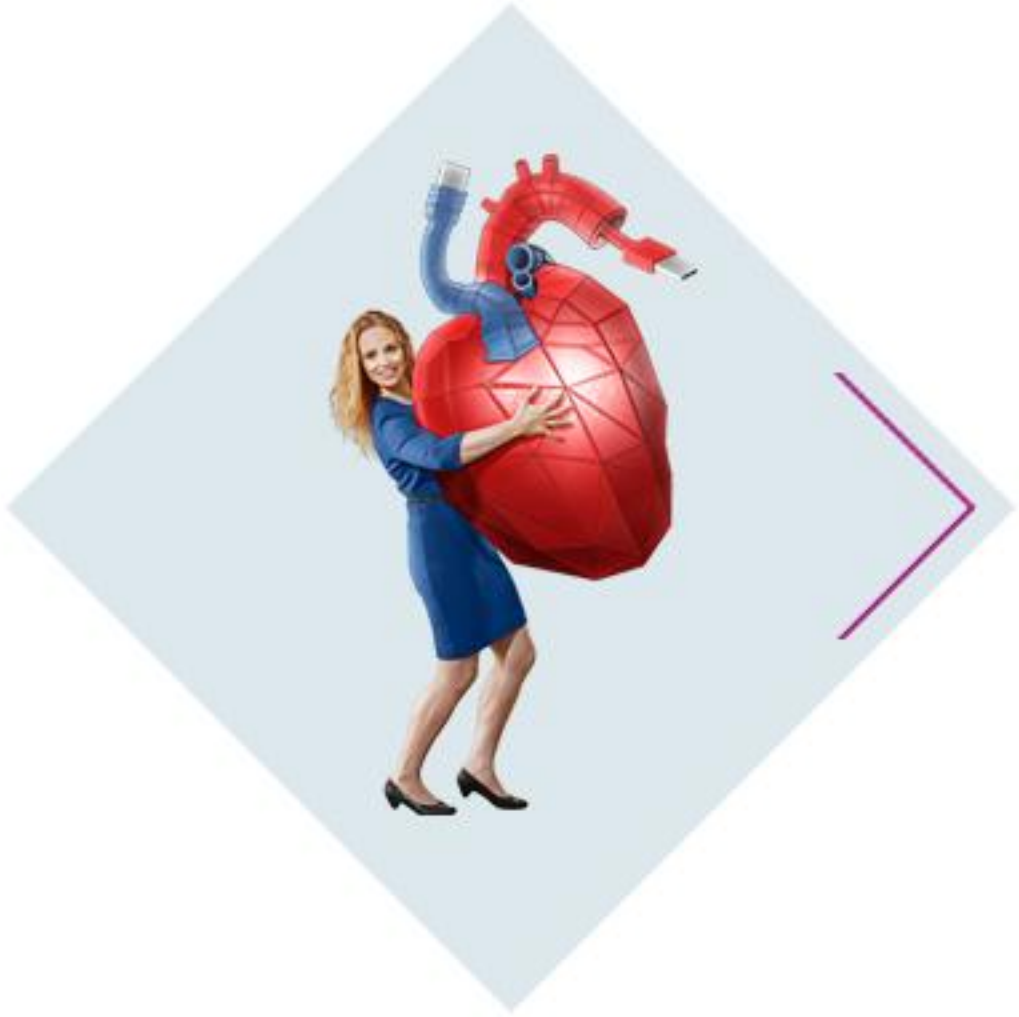


Surface codes = error correction

"Longer algorithm's like Shor's algorithm (to break RSA) likely require more than 1000 physical qubits per logical qubit."

"We need Moore's-law type scaling for quantum computers to ever be useful"

By Samuel Jaques,
University of Oxford, 2021
https://sam-jaques.appspot.com/quantum_landscape



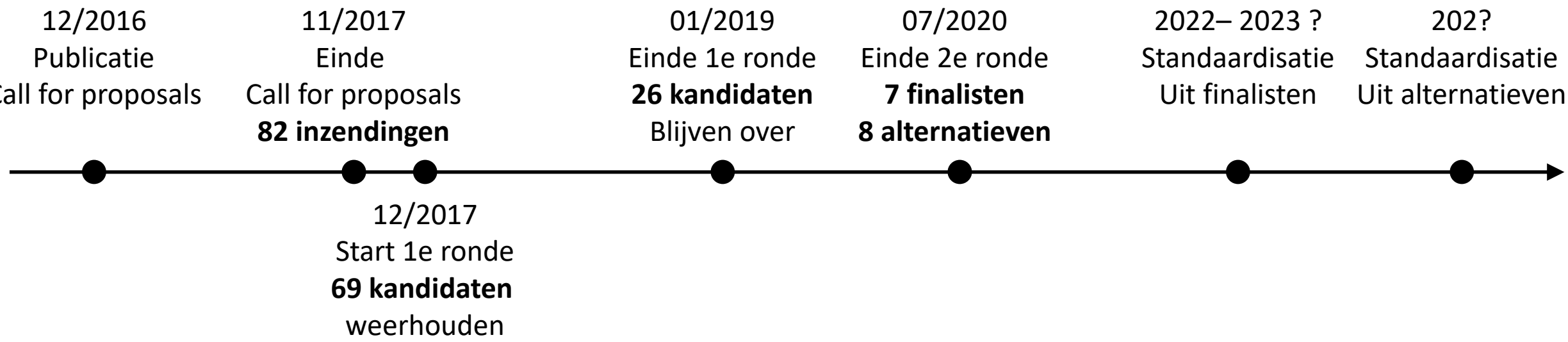
Agenda

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

Twee luiken

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

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



Doorheen procedure **nieuwe zwakheden ontdekt**, waardoor kandidaten afvielen

Algoritmes **uit te voeren op klassieke computer**. Vb. Met QOS (Quantum Open Safe) library

Niet alles in NIST procedure
Meer gevanceerde cryptografische bouwblokken

Smals ICT for society

Kwantumresistente cryptografie – NIST standaardisatieprocedure

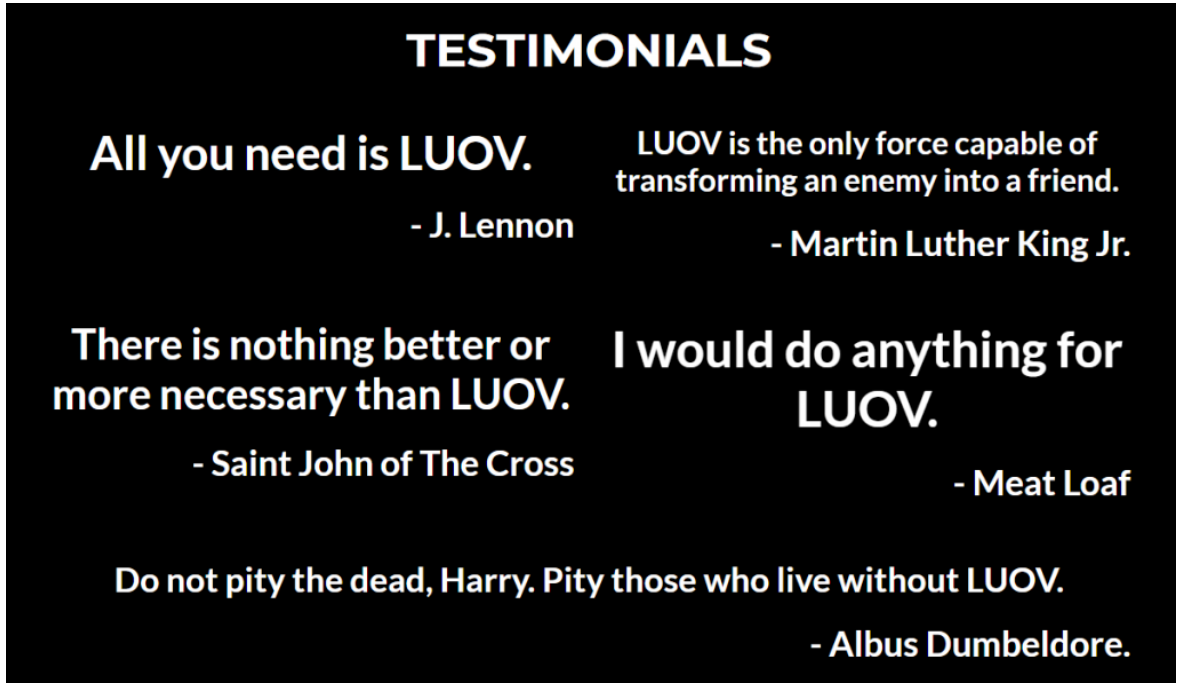
KU LEUVEN

COSIC

SABER
Public-key Encryption and Key-establishment Algorithms

LUOV
Digital Signature Algorithms

Behoort tot de groep
“Lattice-based cryptografie”
(grootste groep
inzendingen & finalisten)



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

- RSA en EC voor informatie tot niveau top-secret
- Indien je nog niet overgeschakeld bent van RSA naar EC, wacht je beter op kwantumresistente standaard

2020

- Kwantumresistente cryptografie essentieel voor verdediging van de natie
- Vertrouwen in lattice-based cryptografie (en hash-based signatures)

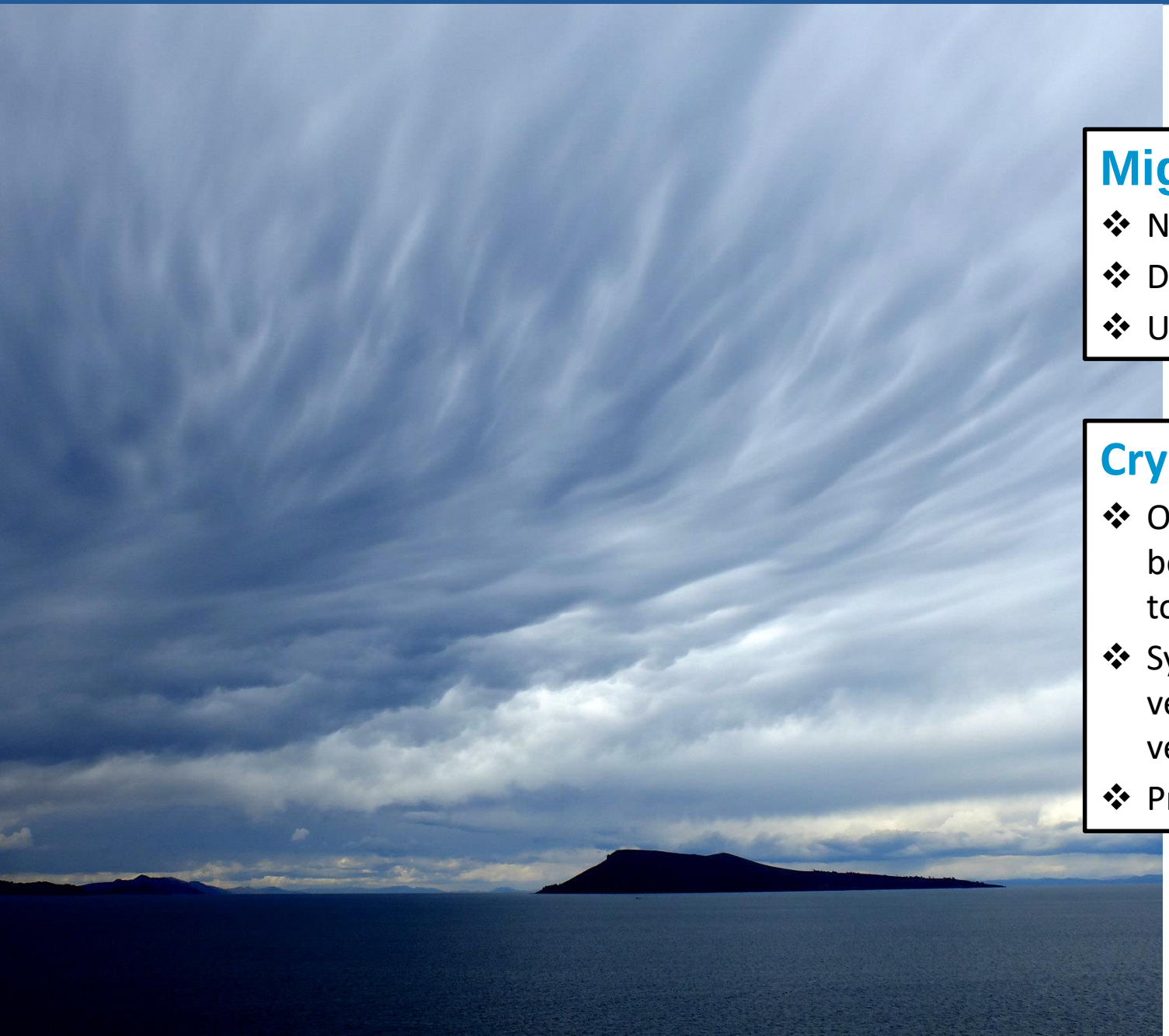
2021 FAQ

- “Cryptographically Relevant Quantum Computer” (CRQC)
- NSA does not know when or even if a [CRQC] will exist
- The cryptographic systems that NSA produces, certifies, and supports often have very long lifecycles. NSA has to produce requirements today for systems that will be used for many decades in the future
- New cryptography can take 20 years or more to be fully deployed to all National Security Systems

“Unfortunately, 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



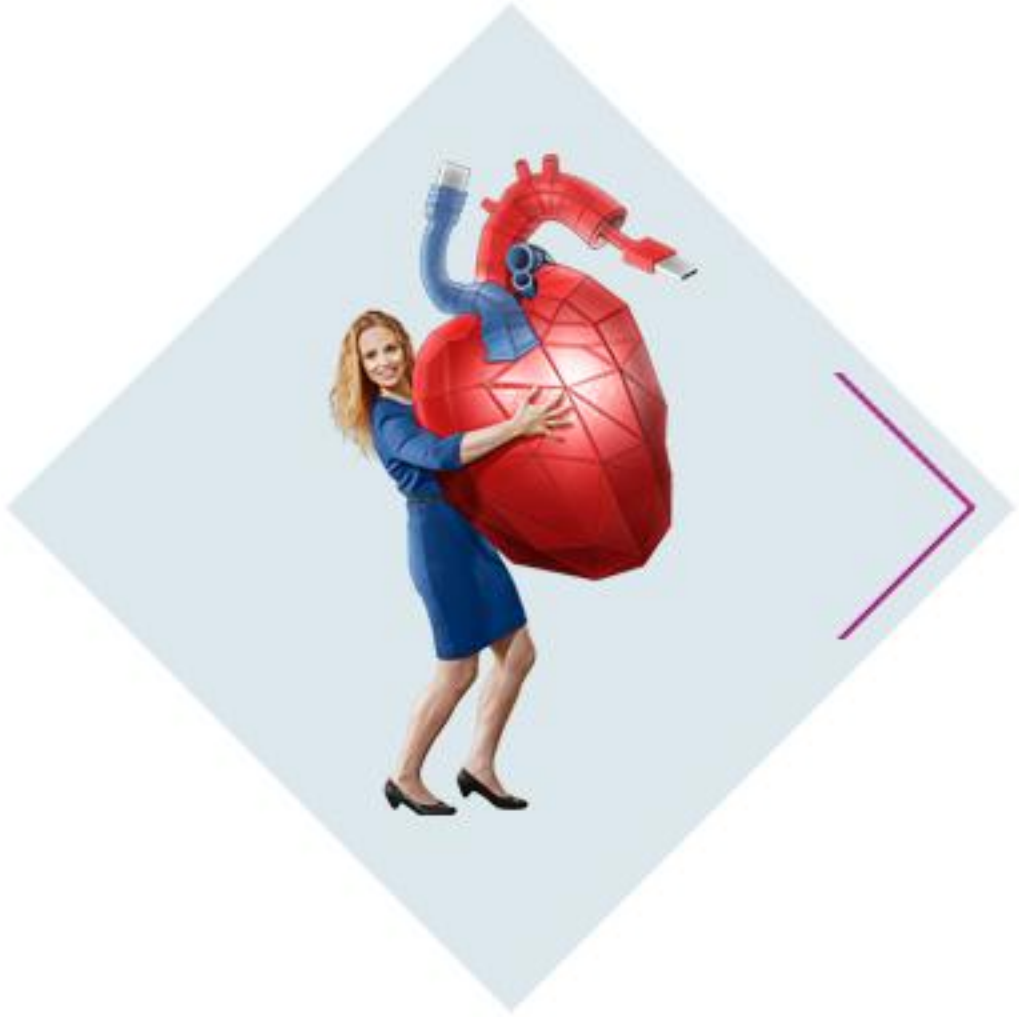
Migratie

- NIST standaardisatieprocedure loopt
- Daarna migreren
- Urgentie hangt af van risicoinschatting

Crypto agility ter voorbereiding

- Overzicht: welke cryptografische bouwblokken en sleutels waar (en waarom) toegepast
- Systemen voldoende flexibel bouwen om vervangen cryptografische bouwblokken te vergemakkelijken
- Processen ter migratie uitwerken

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

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

Thanks for listening!

Smals
ICT for society

Referenties

- F. ARUTE, K. ARYA, […] J. MARTINIS. *Quantum supremacy using a programmable superconducting processor*. Nature, 23 October 2019 https://www.nature.com/articles/s41586-019-1666-5
- *Post-Quantum Cryptography – Project overview*. NIST. https://csrc.nist.gov/projects/post-quantum-cryptography
- *Commercial National Security Algorithm Suite*. NSA. https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm
- *Post-Quantum Cybersecurity Resources*. NSA. https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/
- S. DAS SARMA. *Quantum computing has a hype problem. MIT Technology Review*. 22 Maart 2022 https://www.technologyreview.com/2022/03/28/1048355/quantum-computing-has-a-hype-problem/
- M. GRASS, B. LANGENBERG, M. ROETTELER, R. STEINWANDT. *Applying Grover's algorithm to AES: quantum resource estimates*. Post-Quantum Cryptography, Springer, Cham, 2016. https://arxiv.org/pdf/1512.04965.pdf
- C. GIDNEY, M. EKERA. *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. arXiv preprint arXiv:1905.09749, 2019. https://arxiv.org/abs/1905.09749
- M. DYAKONOV. *The Case Against Quantum Computing*. EEE Spectrum 56.3, 15 November 2018. https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing
- H. HELSMOORTEL, W. DE MAESENEER. *Vlaamse topwetenschappers blikken vooruit: Staat er in 2030 een kwantumcomputer in onze woonkamer?* VRT Nieuws, 15 January 2020, https://www.vrt.be/vrtnws/nl/2019/12/24/vlaamse-topwetenschappers-blikken-vooruit-naar-2030-kwantumcomp/
- D. MASLOV, J. GAMBETTA. On "Quantum Supremacy". IBM Research Blog, 21 October 2019. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/
- V. MAVROEIDIS, K. VISHI, M. Zych, A Jøsang. *The impact of quantum computing on present cryptography*. arXiv preprint arXiv:1804.00200, 2018 Mar 31. https://arxiv.org/pdf/1804.00200.pdf
- 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

- IBM. Q System One quantum. https://www.ibm.com/quantum-computing/systems/
- Andrew Magill. JTAG board 1 https://flickr.com/photos/amagill/2877921712/
- Max Roser – Transistor count. https://ourworldindata.org/uploads/2019/05/Transistor-Count-over-time-to-2018.png
- Alex Does Physics. Polarization http://alexdoesphysics.blogspot.com/2018/11/mathematical-description-of-polarization.html
- Orren Jack Turner. Einstein in 1947 https://en.wikipedia.org/wiki/Albert_Einstein#/media/File:Albert_Einstein_Head.jpg
- INTVGene. Puzzle. https://www.flickr.com/photos/intvgene/370973576/
- Nature. Layout Sycamore processor. https://www.nature.com/articles/s41586-019-1666-5
- D-Wave Systems. D-Wave 2000Q Quantum Computer. https://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order
- Quantum computing https://www.roche.com/quantum-computing.htm
- Pixabay. Jug Thermos Hot Cold Drink Coffee https://pixabay.com/photos/jug-thermos-hot-cold-drink-coffee-3638398
- Marcus Gripe, Garv... (writing) https://flickr.com/photos/neoeinstein/4503776883
- Willian Clifford. This is as close as you get. (fingerprint) https://www.flickr.com/photos/williac/2503890509/
- Birthday paradox https://commons.wikimedia.org/w/index.php?curid=10784025
- Natascha. Keys. https://www.flickr.com/photos/tasj/5207744064
- Kristof Verslype. Threatening clouds above Lake Titicaca, Peru. https://www.flickr.com/photos/verslype/23928588621

Smals ICT for society