Kwantumcomputers & Cryptografie

Kristof Verslype
Cryptographer, PhD
Smals Research

Smals
ICT for society

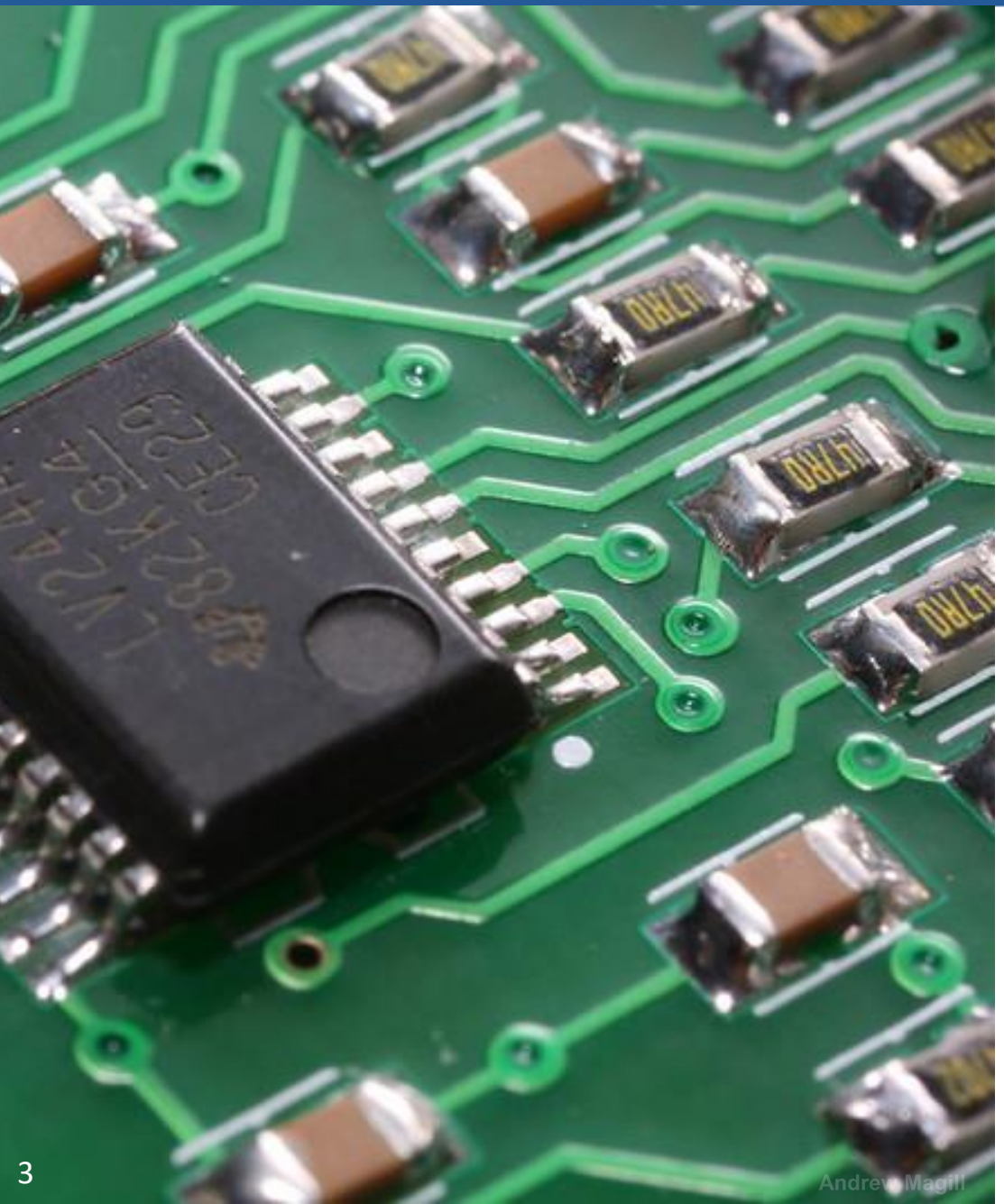
Smals Research 2020




- NewSQL Databases
- Anomalies & Transaction Management
- Conversational Interfaces
- Near-real-time Translation
- Web Scraping for Analytics
- GIS for Analytics
- Augmented Reality
- Graph Analytics Visualisation
- AI Cases & Deployment
- Robotic Process Automation
- Crypto Cases
- European Blockchain Infrastructure
- Knowledge Graphs
- Advanced Cryptography
- Quantum Computing & Cryptography
- FIDO2 / Web Authentication

Smals
ICT for society

Moderne cryptografie



- Sinds intrede computer (Jaren 1970)
- Open algoritmes, geheime sleutels
- Veiligheid gebaseerd op assumpties
- Meer dan geheim houden van communicatie

DES, AES, ElGamal, RSA, …

RSA, DSA, Schnorr, …

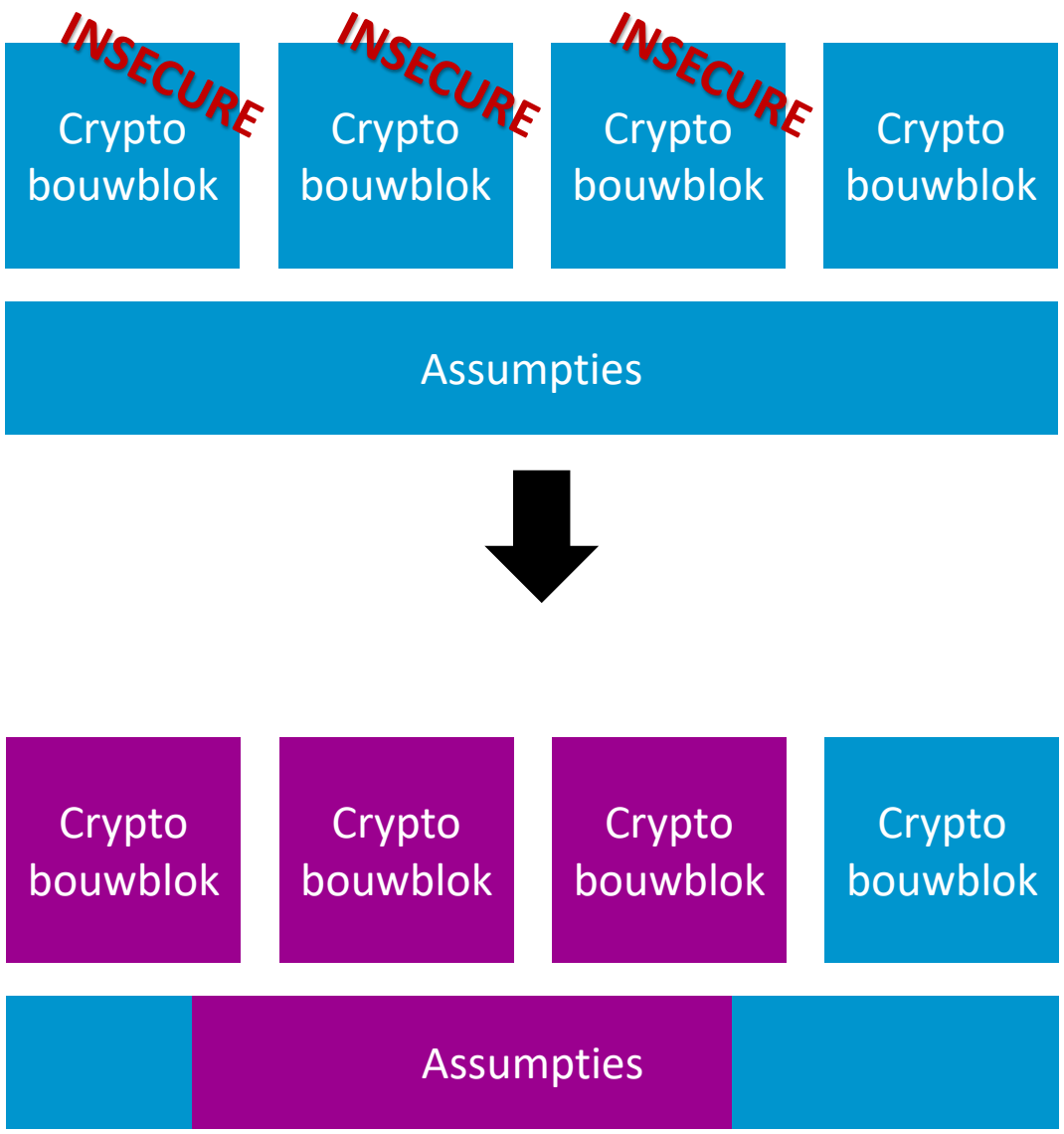
SSH, CHAP, …

MD5, RipeMD, SHA-1, SHA-2, SHA-3

Diffie–Hellman, …

HMAC, …

Crypto assumpties & kwantumcomputers

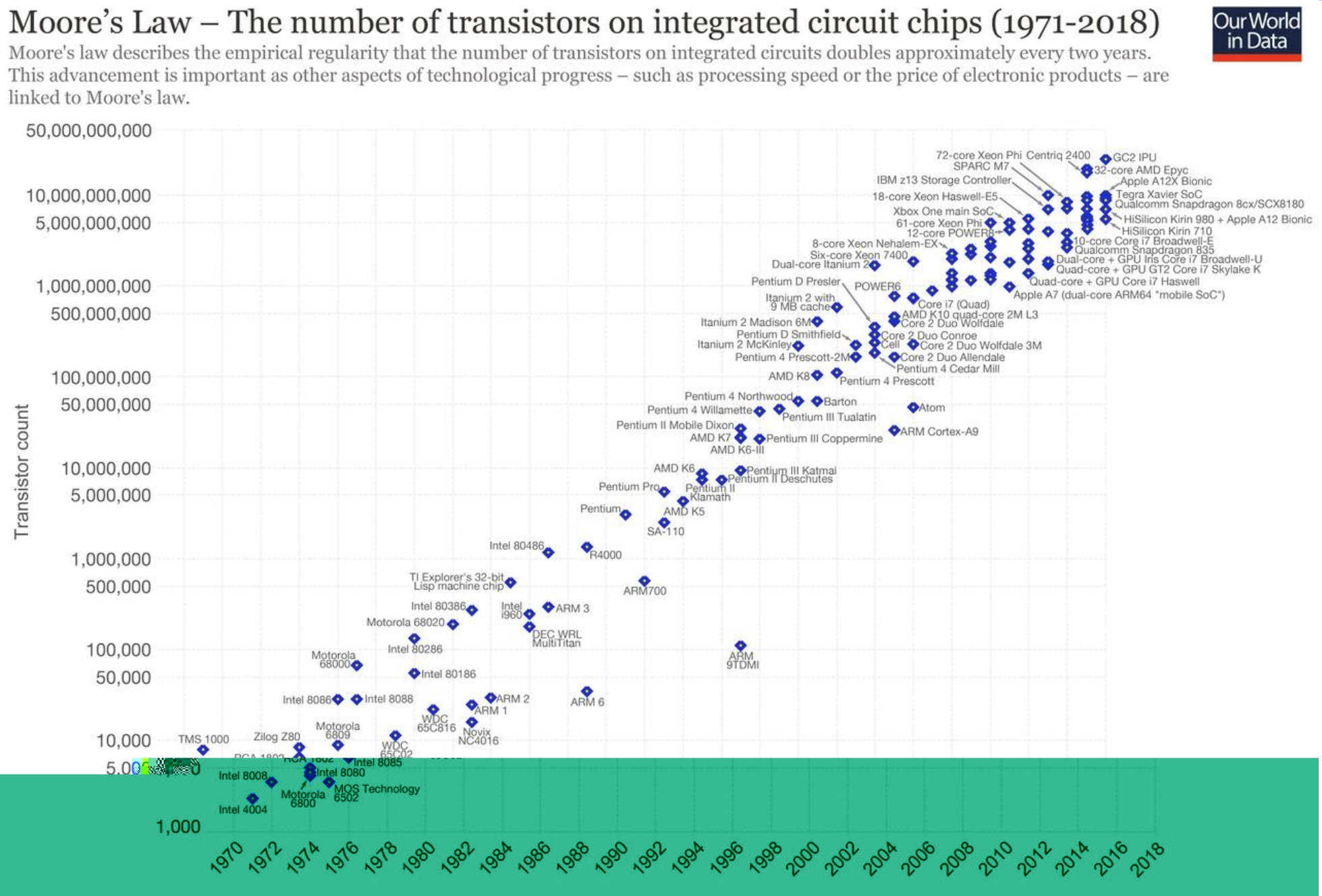


Agenda

Agenda

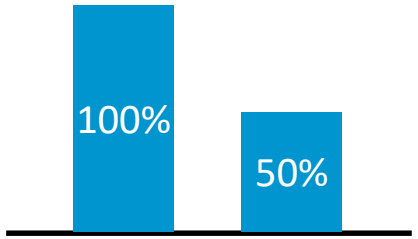
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- Kwantumresistente cryptografie
- Conclusies

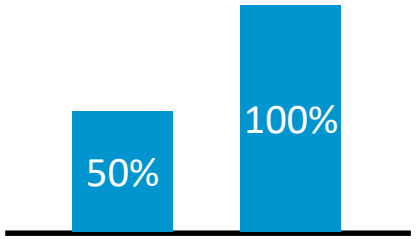
Wet van Moore



- Extrapolatie
- Aantal transistors op een chip verdubbelt elke x (12, 18, 24) maand
- Verwachting: Wet van Moore zal ophouden omstreeks 2025
- Bots met wetten van de Newtoniaanse fysica
- Krachtigere klassieke computers wordt meer en meer een uitdaging
- Naar ander paradigma? Gebaseerd op Kwantumfysica?

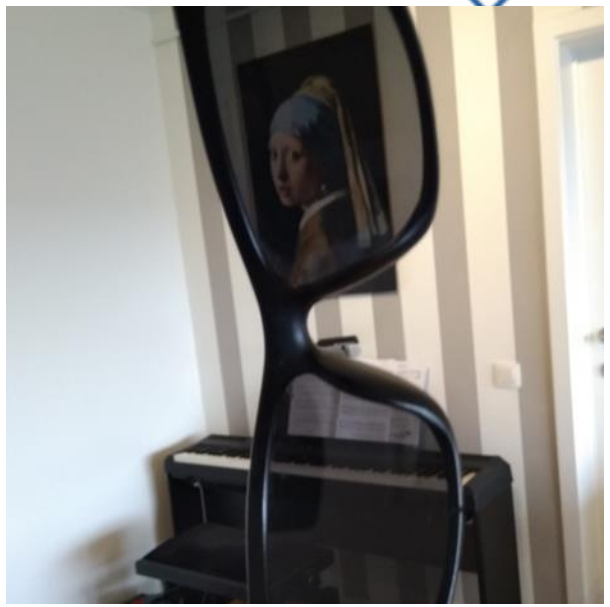
Superpositie

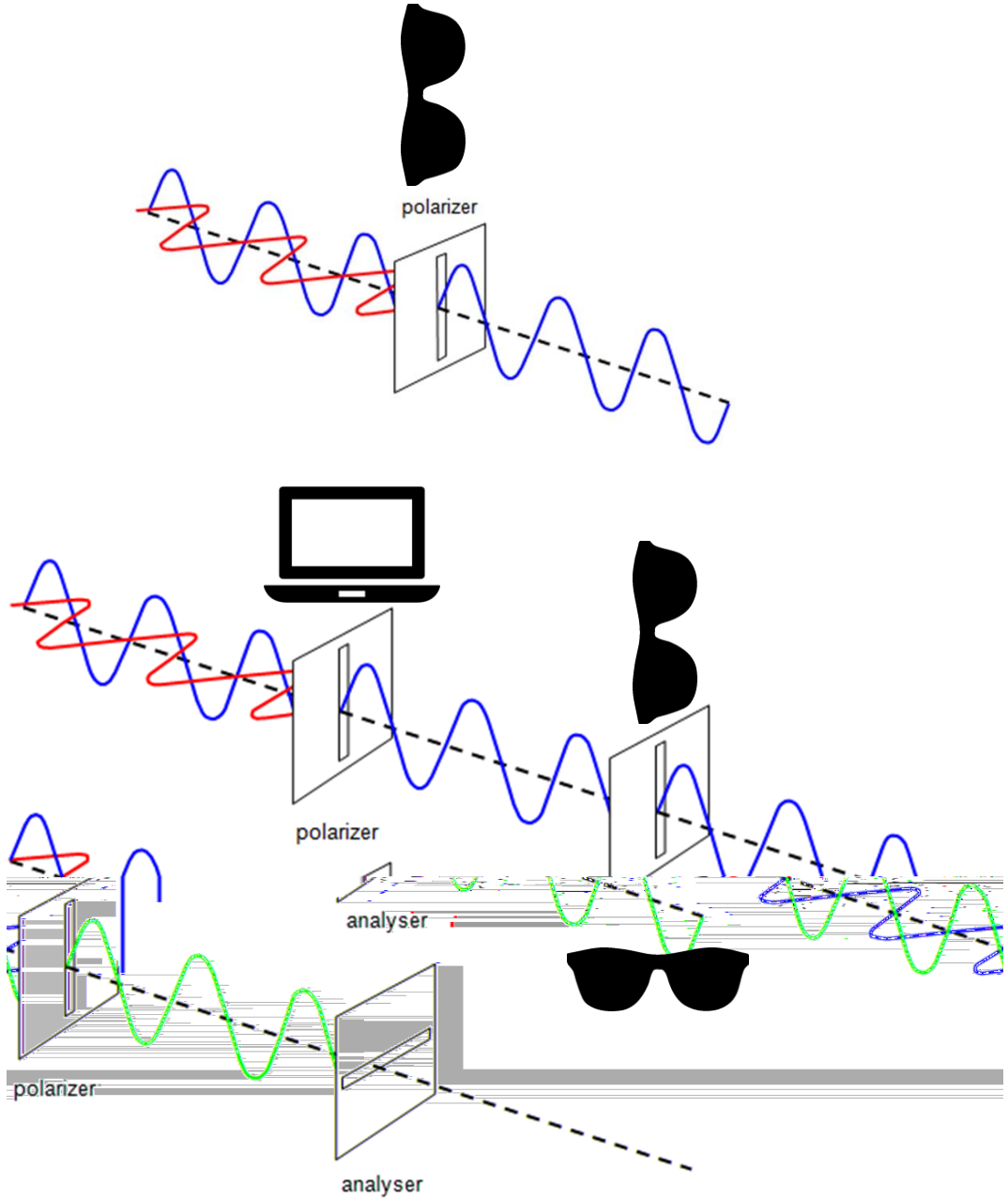




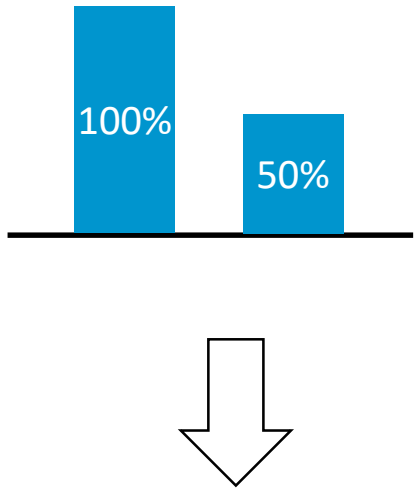
Elektrische lading	Waarde ligt al vast van voor de meting	Meting geen impact op toestand bit	(Sub)atomair ‘deeltje’ (vb. Foton, elektron)	Waarde onbepaald (uitgesmeerd) tot op moment van meting	Meting vernietigt kwantumtoestand: Het mogelijke wordt een concrete waarde

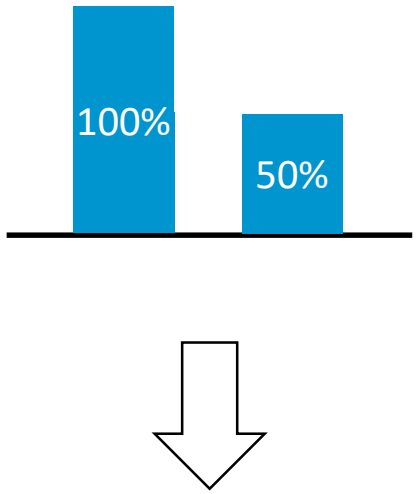
Polarisatie van fotonen – Zonnebrilexperiment

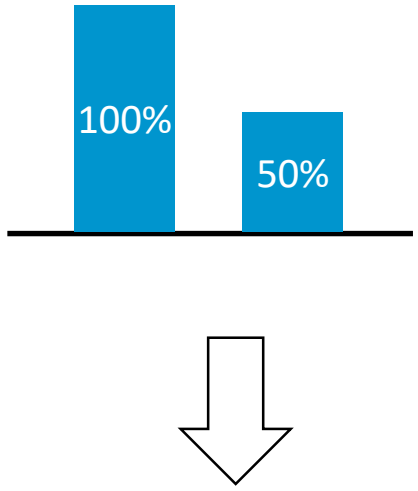


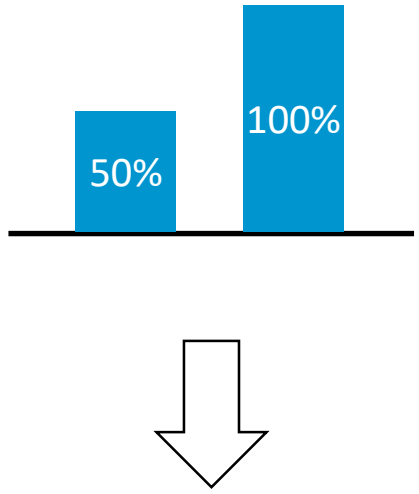


Verstrengeling (entanglement)









Correlatie tussen metingen van verwante deeltjes

Meting ene qubit volstaat om resultaat andere te kennen

Onafhankelijk van onderlinge afstand qubits (↔ Newtoniaanse fysica)

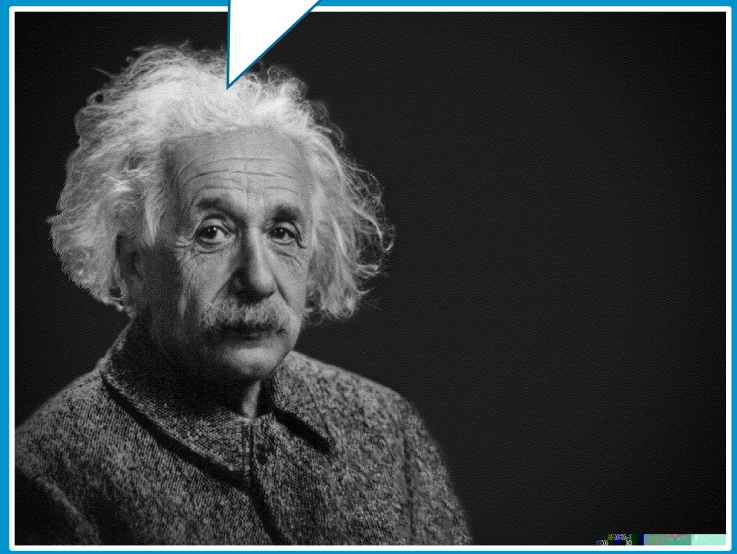
Verstrengeling van meer dan 2 qubits kan ook

Verstrengeling (entanglement)

Waarde is onbepaald tot op het moment van meting

Meting ene qubit heeft impact op uitkomst meting andere qubit

Spukhafte Fernwirkung!
(Spookachtige werking op afstand!)

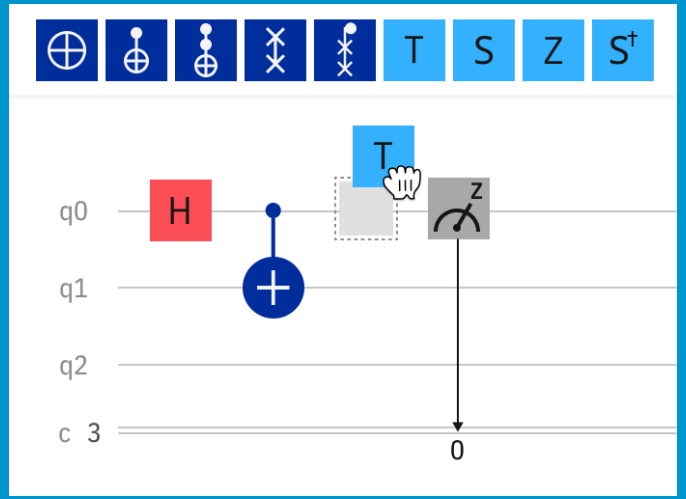


Met hoge waarschijnlijkheid bevestigd door experimenten (vb. Bell test experiments)

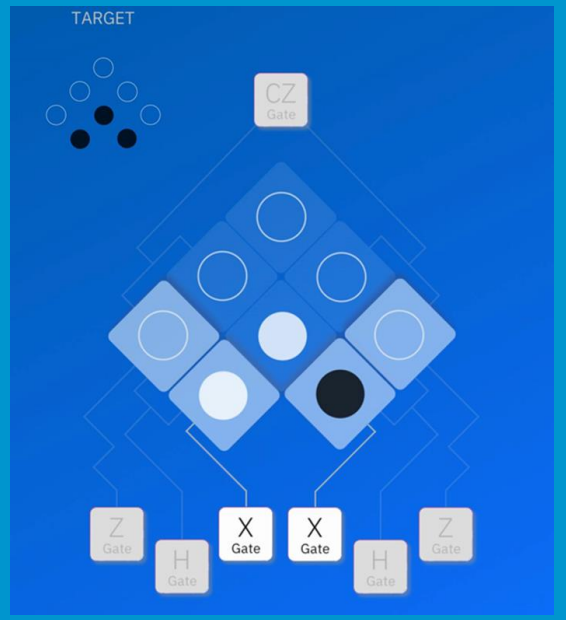
Kwantumberekeningen

Logische poorten:
AND, NOT, OR, XOR, …

Kwantum logische poorten:
Pauli-X, Hadamard, SWAP, …



- Omzetten algoritmes naar instructies voor kwantumprocessor
  vb. Quil, OpenQASM
- Tools om kwantum programma's te creëren & manipuleren
  vb. Qiskit, ProjectQ, Forest
  Vaak uitbreidingen op bestaande programmeertalen
- Quantum Computation Language (QCL), Q#, Q language



De kracht van kwantumberekeningen

Misvatting

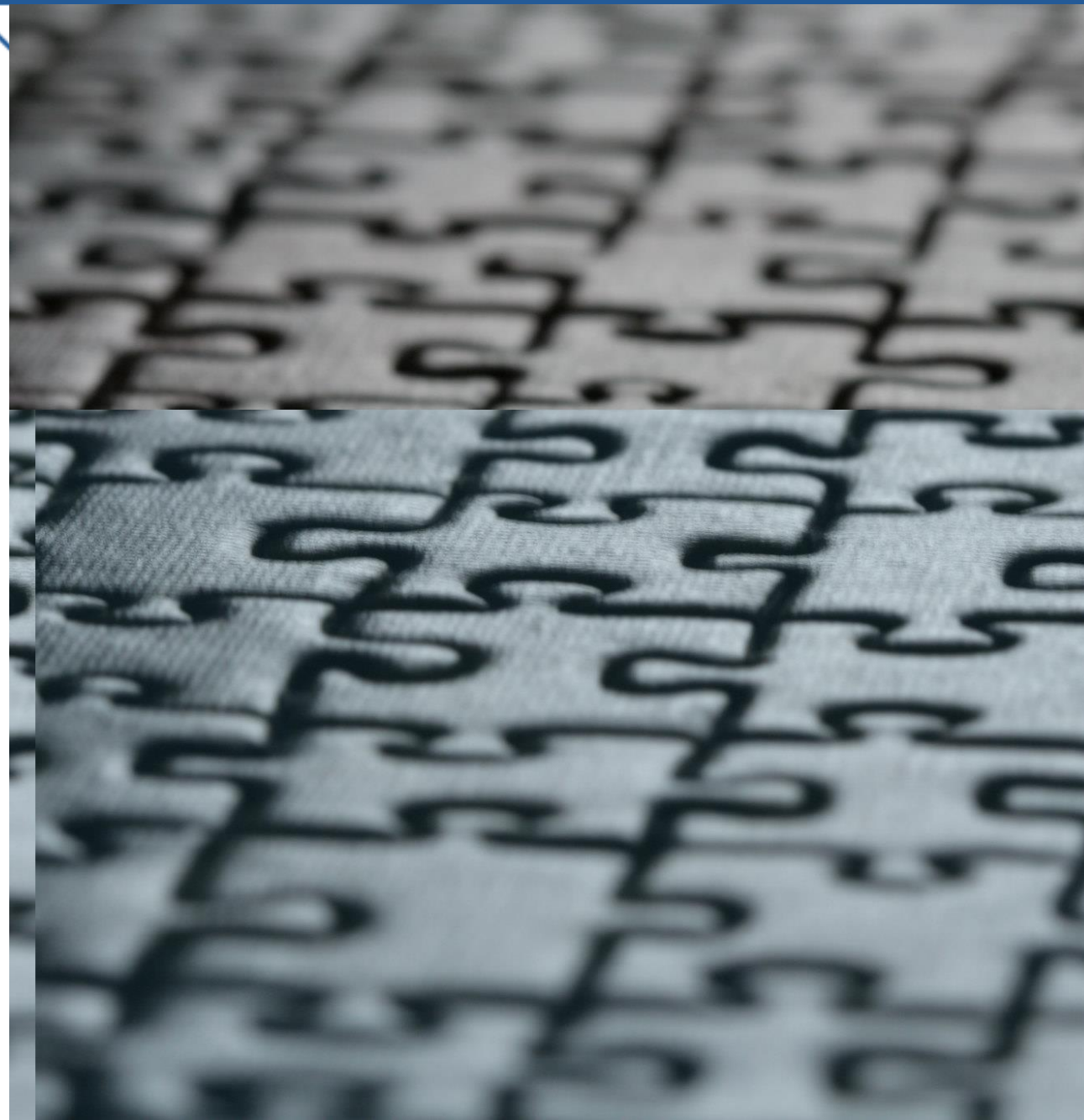
“Kwantumcomputers zullen alle problemen kunnen oplossen die moeilijk (of zelfs onmogelijk) zijn voor klassieke computers.”

Correcter

- Beperkte, maar zeer interessante, categorie van problemen waar kwantumcomputers in excelleren
- Daaronder problemen die moeilijk moeten blijven om moderne cryptografie veilig te houden

Wapenwedloop

- Investeringen van grootmachten zoals Duitsland, China en VS in de techologie
- 2019: 88 miljard dollar wereldwijd (quantum tech)
- Groei van 29%/jaar tot 2026

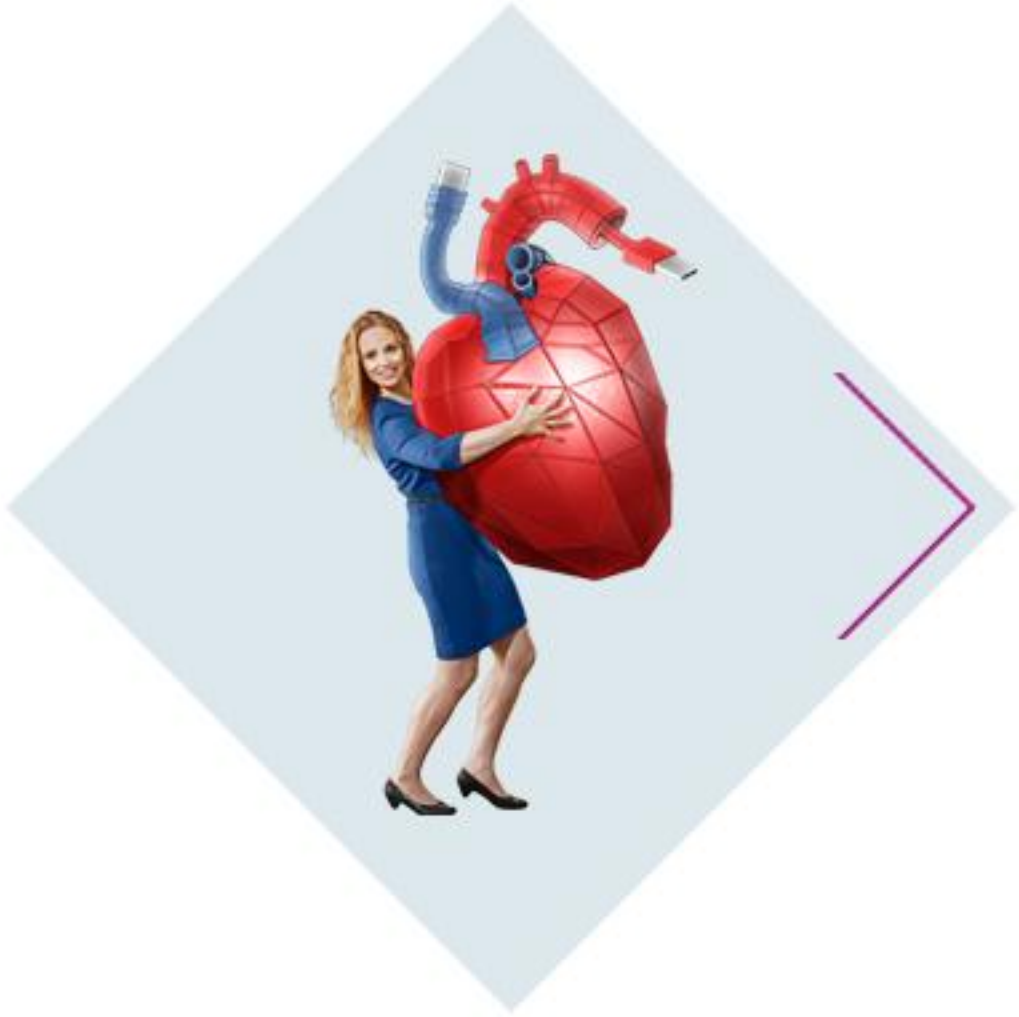


Kwantum- Vs. klassieke computer - Conclusie

- Steunen op weinig intuïtieve principes zoals verstrengeling en superpositie
- Hebben Qubits – (sub)atomaire deeltjes / golven – als kleinste opslag- en rekeneenheid
- Berekening gebeuren op fundamenteel andere wijze dan bij klassieke computers
- Zijn – op papier – krachtig voor een beperkte groep van problemen

"Hoeveel keer sneller [kwantumcomputers zullen zijn] is echter nog koffiedik kijken. Misschien 10 keer, misschien 100 keer. Sommigen hebben het zelfs over 100 miljoen keer sneller."

Belgische professor aan de TU Delft
Hoofd Quantum Computer Architectures Lab TU Delft



Agenda

- Kwantum- Vs. klassieke computer
- De crypto-apocalypse?
- Kwantumresistente cryptografie
- Conclusies

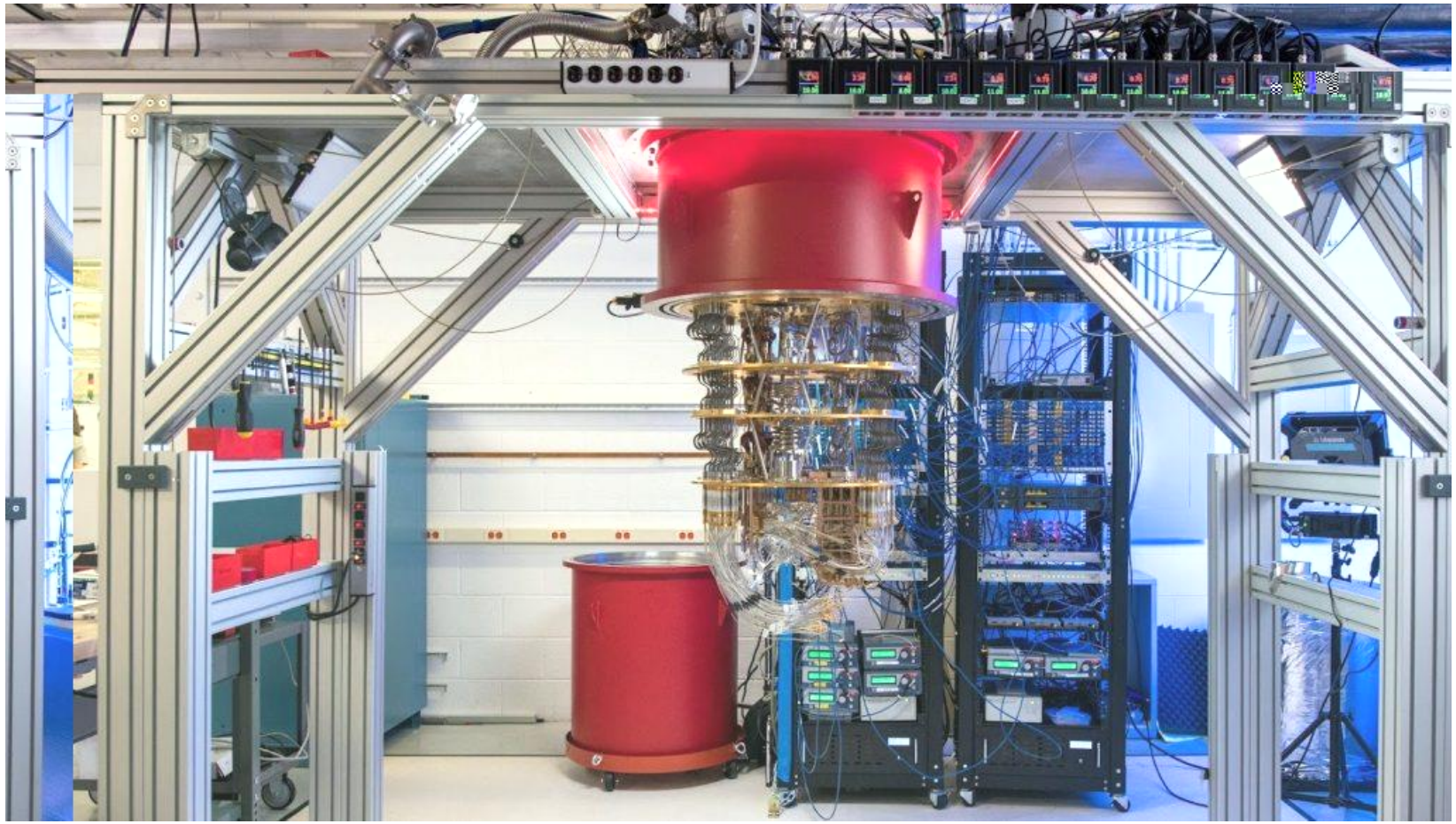
Google claimt quantum supremacy (kwantumsuperioriteit)

Google

Article

Quantum supremacy using a programmable superconducting processor

nature
International journal of science



Smals
ICT for society

Google claimt quantum supremacy (kwantumsuperioriteit)

Google

Article

Quantum supremacy using a programmable superconducting processor

nature
International journal of science

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

John Preskill, 2012

Generen willekeurige gekozen getallen volgens een zeer specifieke distributie op het lijf geschreven van kwantumcomputers

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

- *"Conservatief geschat kan dit in 2,5 dagen met een klassieke computer, bovendien met een veel hogere nauwkeurigheid"*
- Hoofd Quantum Computer Architectures Lab, TU Delft
  "Simpelweg niet waar"

Smals
ICT for society

Google claimt quantum supremacy (kwantumsuperioriteit)

Google

Article

Quantum supremacy using a programmable

[illegible] processor [illegible]supe

nature
International journal of science

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

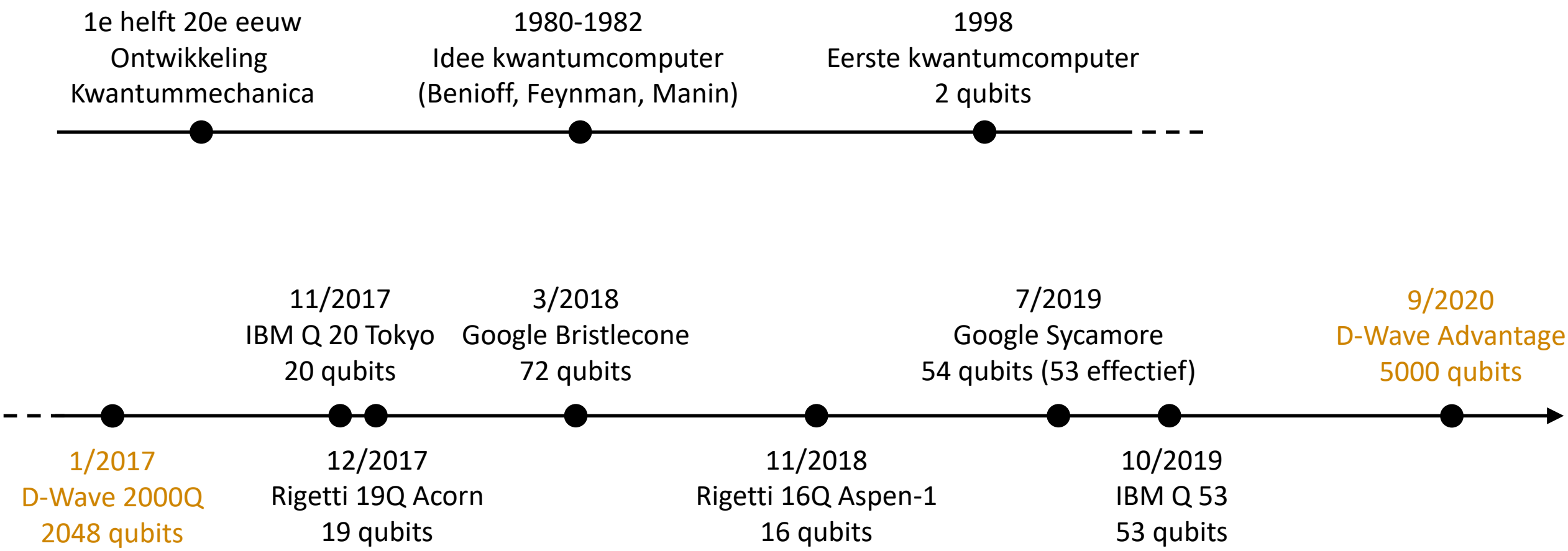
John Preskill, 2012

Kwantumcomputer kan probleem sneller oplossen dan een klassieke computer

- Geen quantum supremacy
- Hoogstens quantum advantage
- Ook dat is betwistbaar
- Blijft sterke prestatie van Google

Smals
ICT for society

Historiek & State of the art



Voor uitgebreidere timeline https://en.wikipedia.org/wiki/List_of_quantum_processors

Adiabatische kwantumcomputers

- Vereist minder verstengeling
- Maar wel meer qubits
- Oorspronkelijk gericht op optimalisatievraagstukken
- Theoretisch zelfde mogelijkheden als universele kwantumcomputer
- Machines worden verkocht
- Nog geen quantum advantage

Smals ICT for society

State of the art

- Universele (Rigetti, Google, IBM)
- Adiabatische (D-Wave)

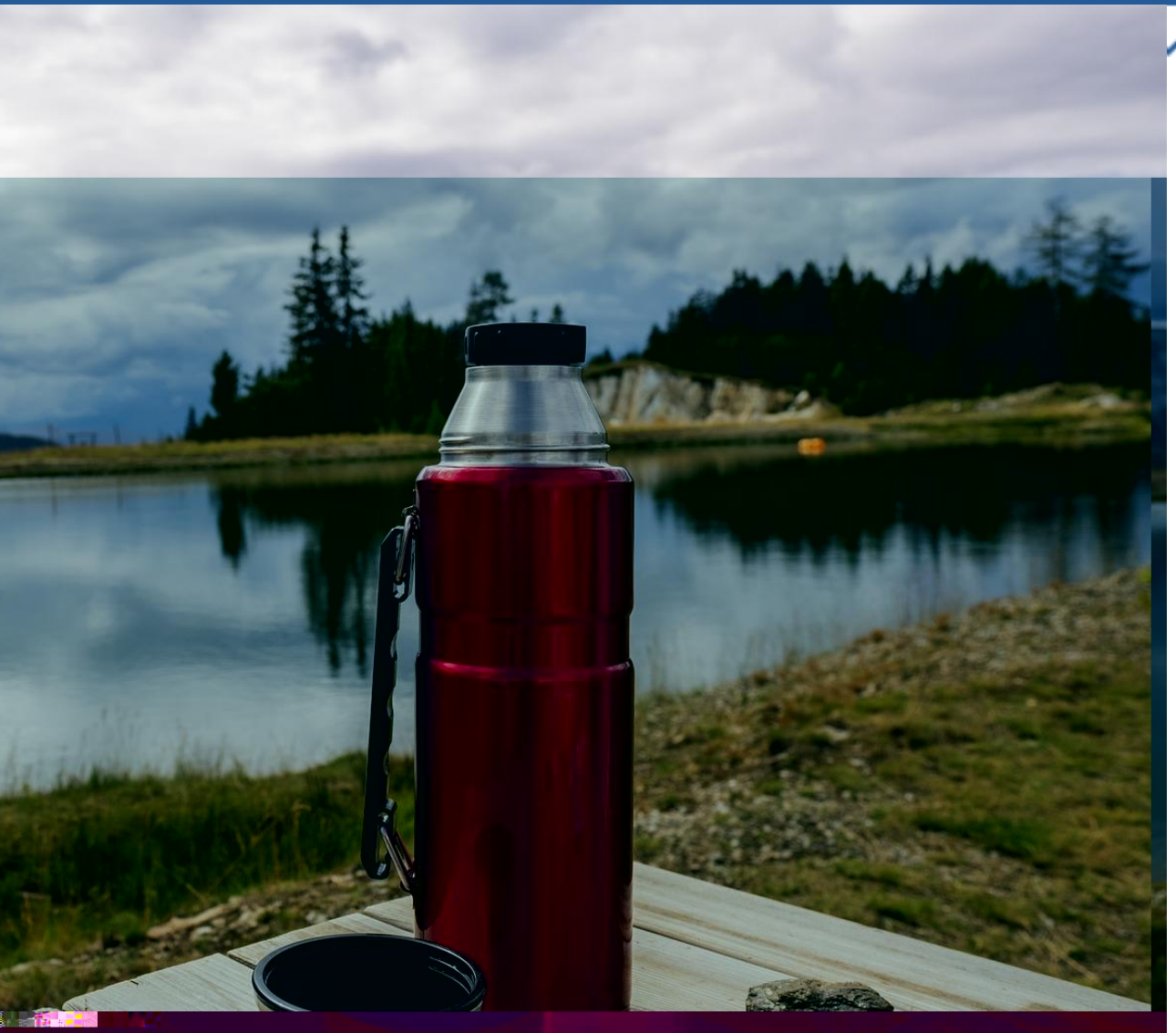
→ IBM prefereert de term ***Quantum Volume***
→ Vergelijken niet evident. Bedrijven niet steeds transparent over inner workings & specs

Smals
ICT for society

Waarom is het bouwen van een kwantumcomputer zo complex?

- Isolatie
- Foutencorrectie
- Schaalbaarheid
- Topologie

Uitdaging 1: Isolatie



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

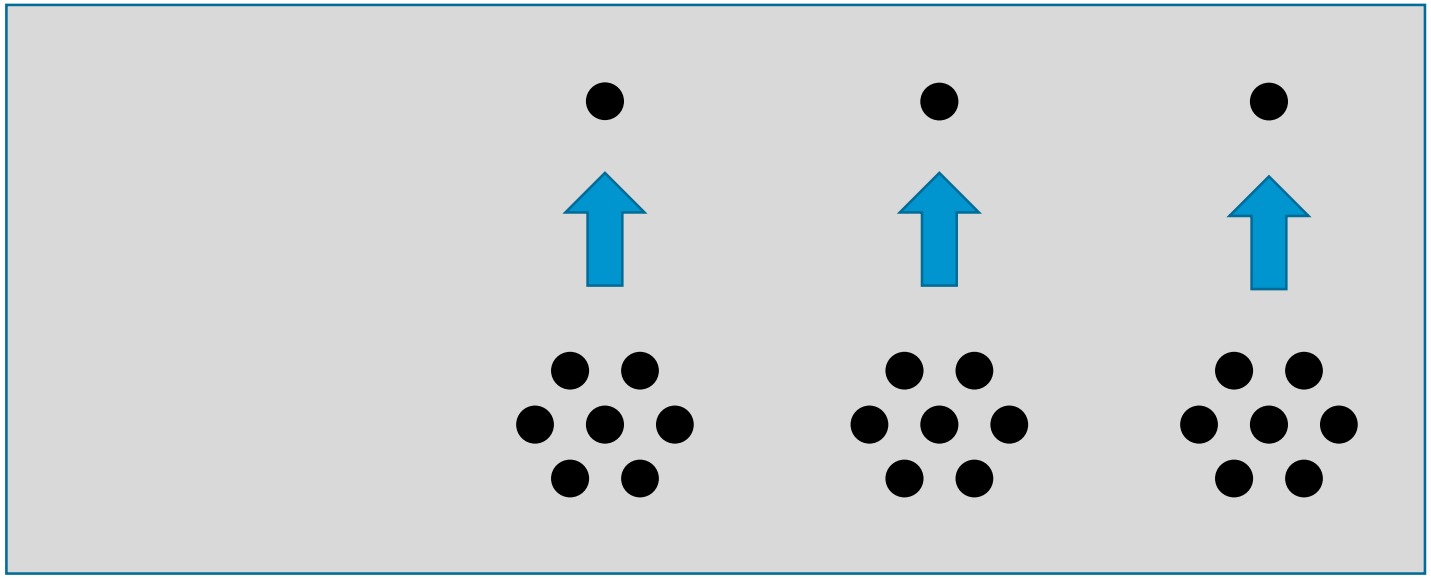
- Nooit volledig vrij van interferentie
- Uitdaging: voldoende lang coherent houden kwantumtoestand
- Googles Sycamore: tienden of honderdsten van een microseconde

- Veel vooruitgang geboekt voorbije jaren
- Toch fouten wellicht onvermijdelijk

Smals
ICT for society

Uitdaging 2: Foutencorrectie

Meerdere fysieke qubits vormen samen 1 logische qubit



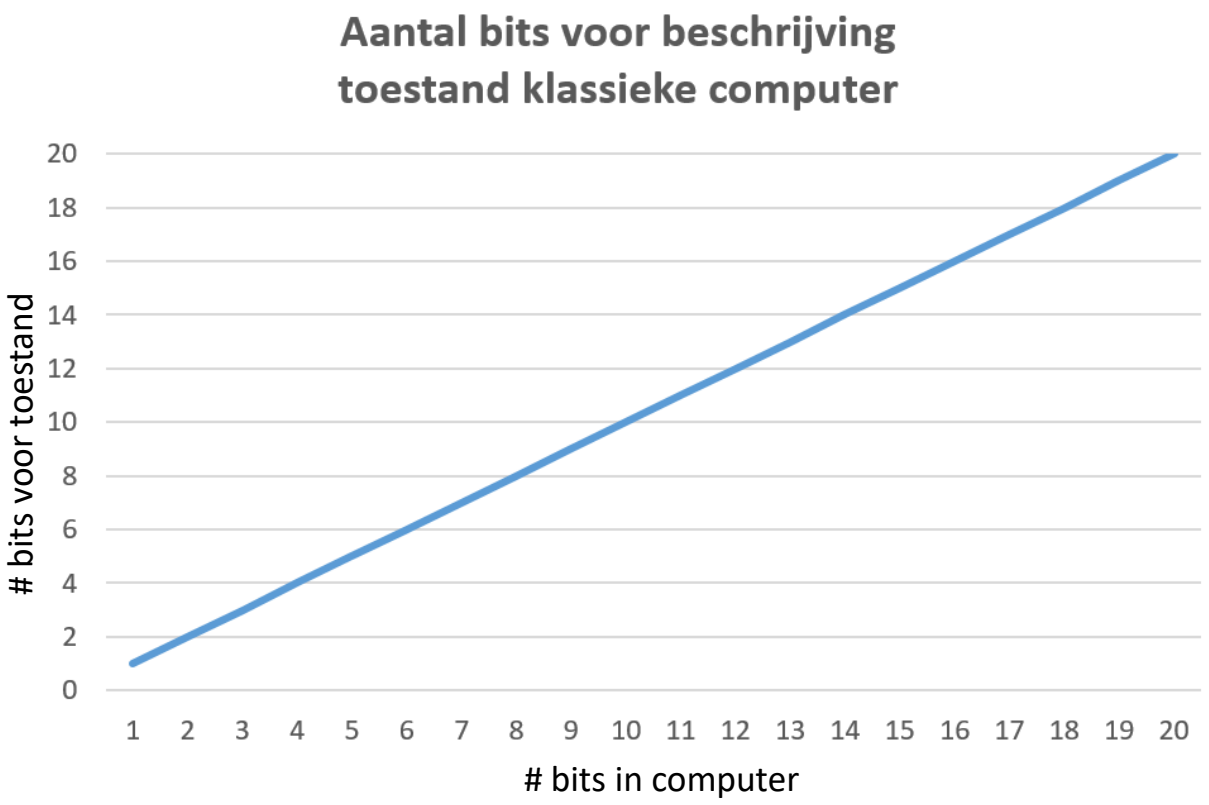
Evolutie

- Jaren ‘80 en ’90: “*onmogelijk!*”
- Theoretisch mogelijk
- Nog geen experimenten (in de praktijk mogelijk?)

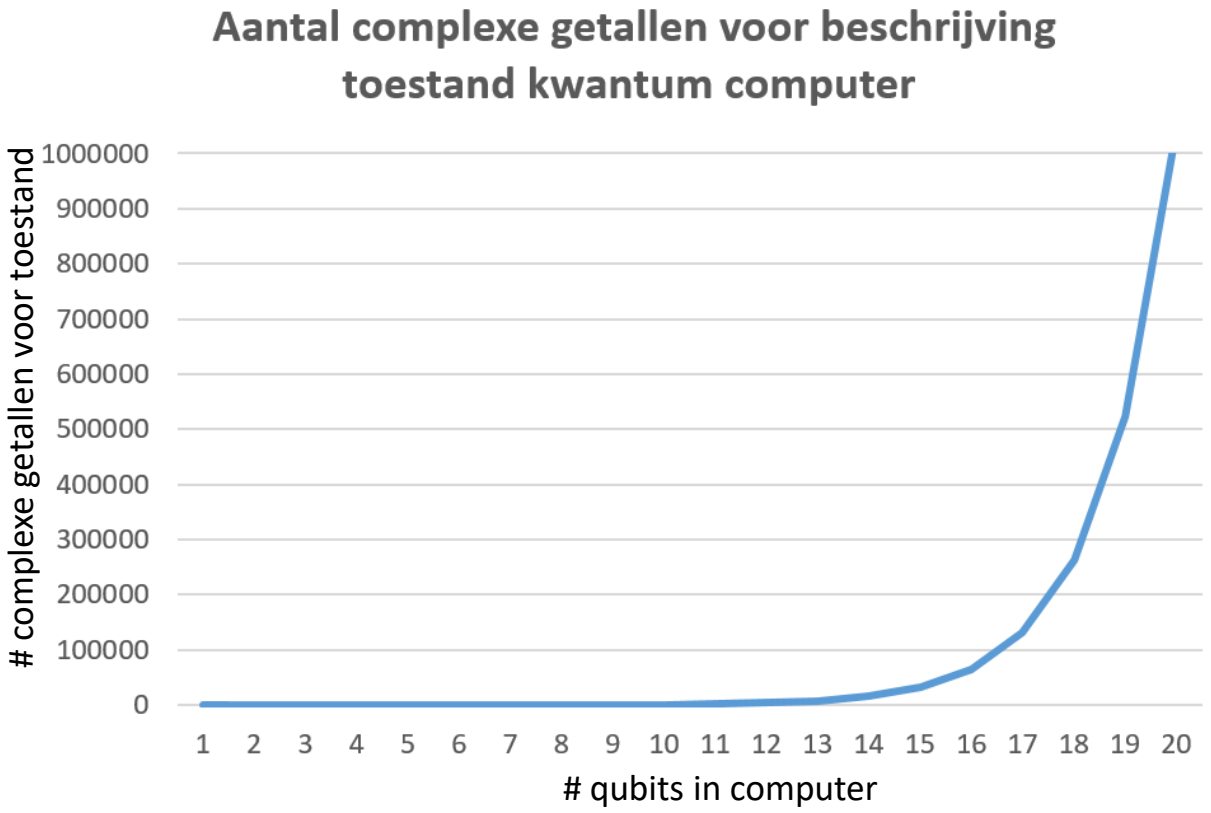
Vereisten

- Meer fouten bij fysieke qubits → meer fysieke qubits per logische
- Schattingen: 1000 tot 100 000 fysieke qubits per logische
- Vereist voldoende lange decoherence time (op zich al een enorme uitdaging)

Uitdaging 3: Schaalbaarheid



Verdubbeling complexiteit bij verdubbeling aantal bits

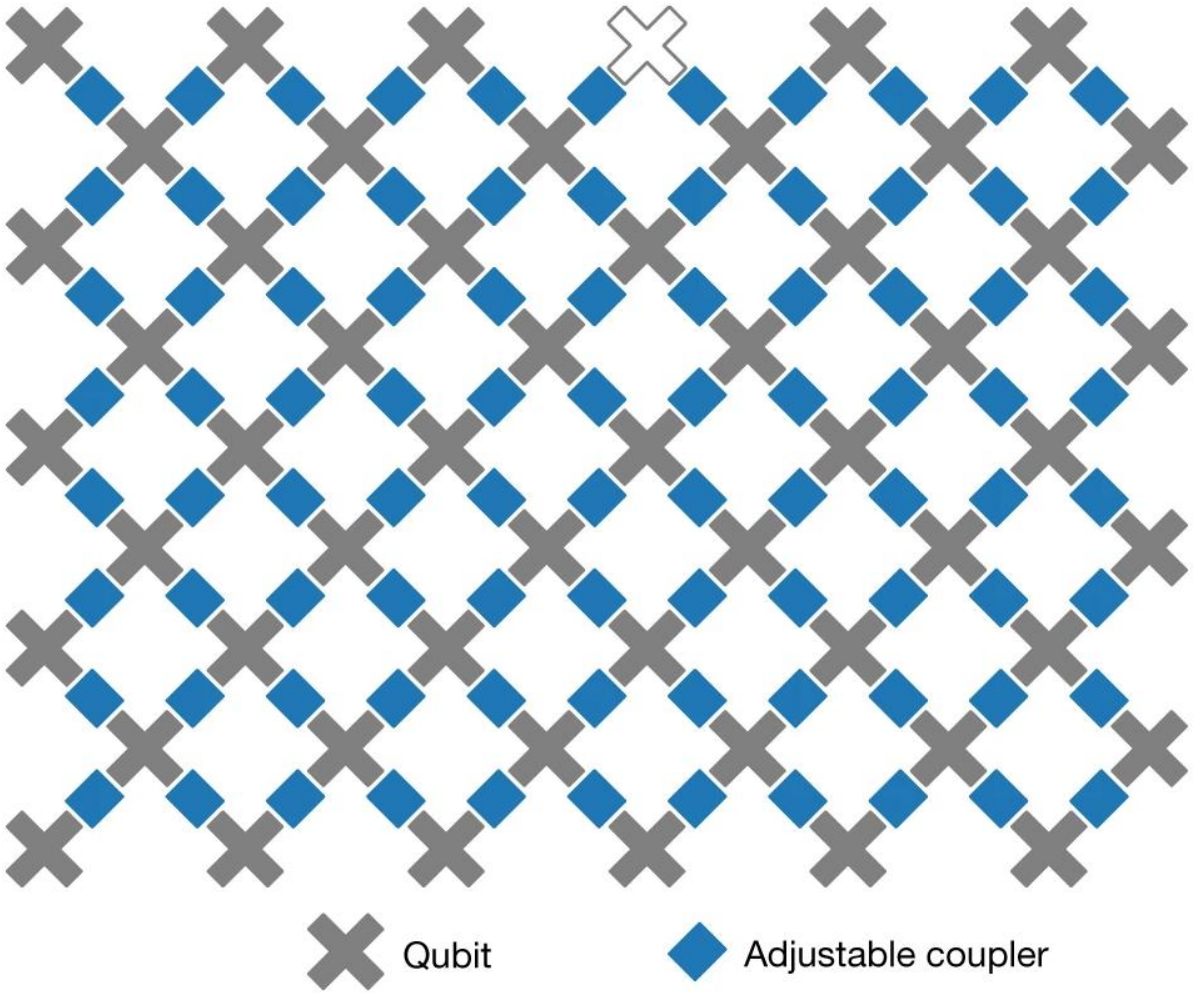


Complexiteit verdubbeld per extra qubit

- 2^{1000} (ongeveer 10^{300}) complexe getallen
- Er zijn minder subatomaire deeltjes in het door ons gekende universum

Uitdaging 4: Topologie (layout) processor

- Operaties mogelijk op data (vb. in RAM)
- Onafhankelijk van de onderlinge positie van die data



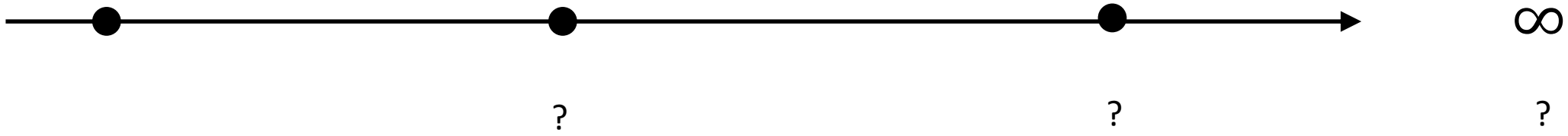
Smals
ICT for society

Waarom is het bouwen van een kwantumcomputer zo complex?

- Isolatie
- Foutencorrectie
- Schaalbaarheid
- Topologie

Kwantumcomputers (niet) in de praktijk: Conclusie

- Experimenten getuigen van enorme vooruitgang
- Beloftevolle initiatieven
- Kwantumcomputers in kinderschoenen
- Luide claims soms overtrokken



Nieuwe inventieve benadering kan veel deuren doen opengaan

Nuttig ≠ in staat moderne cryptografie te breken

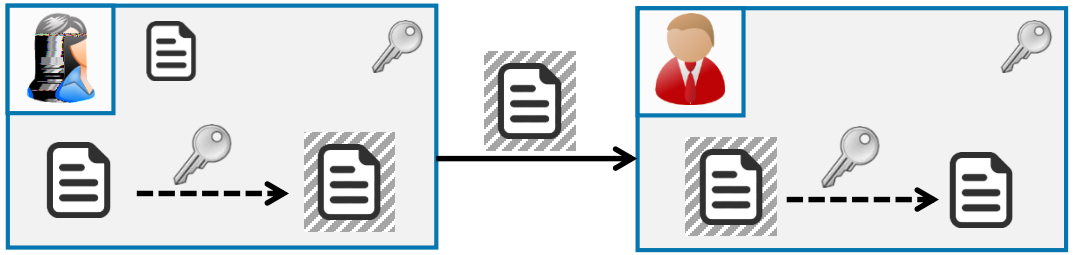
Agenda

Impact kwantumcomputers op moderne cryptografie?

- Symmetrische cryptografie
- Cryptografische hashfuncties
- Publieke sleutelcryptografie

Symmetrische cryptografie

Encryptie en decryptie met dezelfde sleutel
vb. DES (verouderd), AES



Symmetrische cryptografie – Toy example

Sleutellengte = ~~6 bits~~ 256 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

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

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

256 → 512 bits

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

Symmetrische cryptografie – Algoritme van Grover

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

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

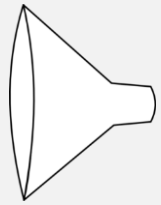
Smals
ICT for society

Symmetrische cryptografie - Conclusie

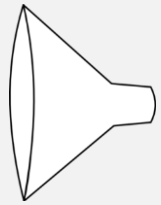
(Zorg wel voor voldoende lange sleutels)

Cryptografische hashfunctie

Integriteit
Zeer courant gebruikt (vb. elektronische handtekeningen, bestanden, blockchain)
Vb. SHA1, SHA2, RIPE-MD

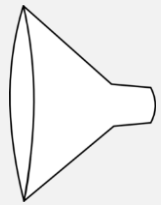


```
5e 50 6e 82 7f d5 50 ec 4e 08 8e e7 75 8f 34 b3
a6 8e 34 93 d5 89 98 52 97 48 f0 c6 c1 70 f3 3c
```



```
5f 3b fa 41 9c 63 be 2a 3a 09 ad bd 06 30 c5 1f
64 5e b0 3a ba fc d5 f2 ad 39 63 7a 30 6b 41 77
```

“Hell0 world!”



```
c0 5a 70 4b ef b7 9f fd 9a f0 19 05 04 70 f8 87
d1 de 4b 20 ae d0 5b f6 f3 bb 2d f9 92 49 85 10
```

Fixed-length output

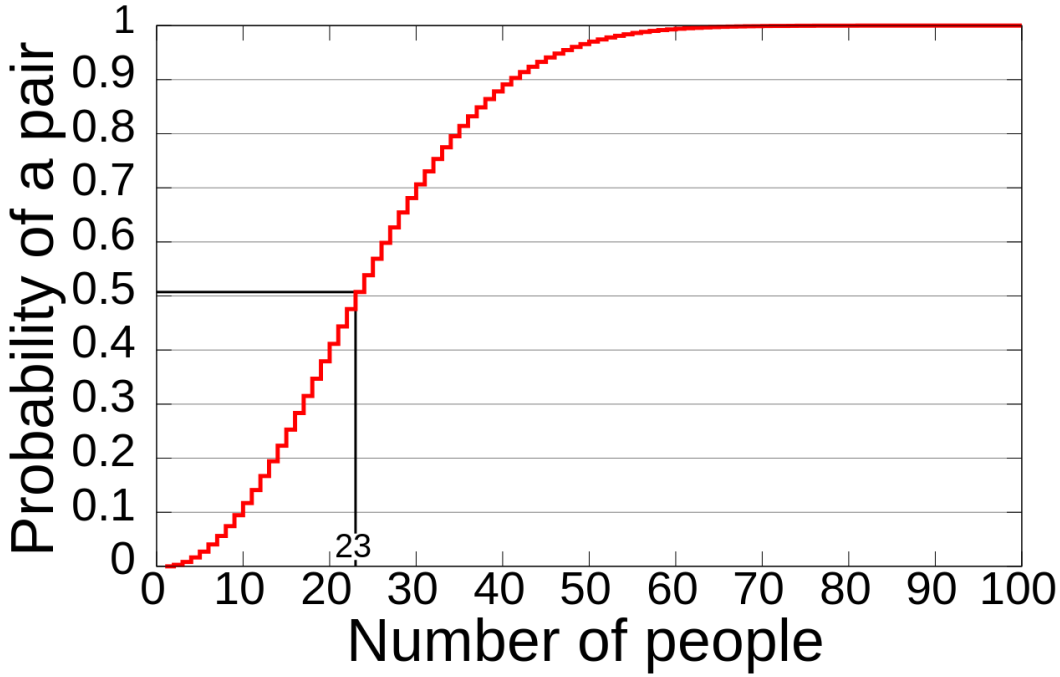
One-way

Collision resistant

Cryptografische hashfunctie

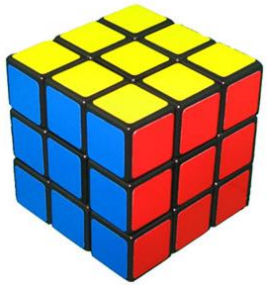
- Vinden van twee inputs die resulteren in dezelfde output
- Voor SHA1 slaagde zo'n aanval in 2017

- Output van 256 bit levert een veiligheid op van 128 bit
  Grote kans op botsing (collision) na $\sqrt{2^{256}} = 2^{128}$ pogingen
- Cfr. Verjaardagenparadox



By Rajkiran, CC BY-SA 3.0,
https://commons.wikimedia.org/w/index.php?curid=10784025

- Algoritme van Grover
- Veiligheid daalt
  van $\sqrt{2^{256}} = 2^{128}$
  tot $\sqrt[3]{2^{256}} = 2^{85} \approx 10^{26}$ (Onveilig)



- Uitvoerlengte x 1,5: 256 → 384 bits ($\sqrt[3]{2^{384}} = 2^{128}$)
- Valt mee!

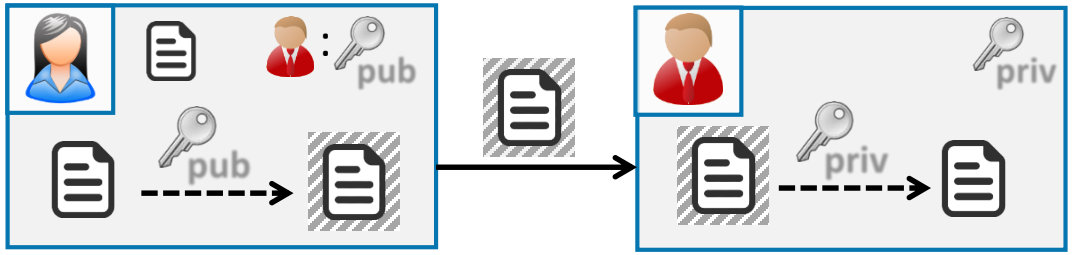
Smals ICT for society

Cryptografische hashfuncties - Conclusie

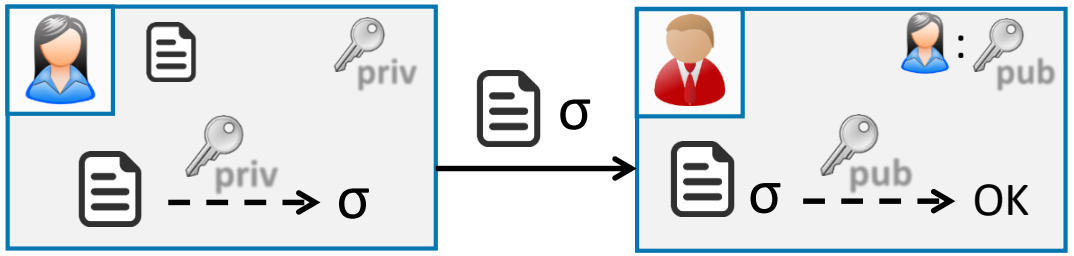
(Zorg wel voor voldoende lange uitvoer)

Publieke sleutelcryptografie

Confidentialiteit
Encryptie en decryptie met verschillende sleutel
Vb. RSA, ElGamal



Integriteit, authenticiteit
Vb. RSA, DSA, ECDSA
Vb. BE eID



Publieke sleutelcryptografie – Getallen factoriseren in priemgetallen

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

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

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.

21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979374 = 64135289477071580278790190170577389084825014742943447208116859632024532344630238623598752668347708737661925585694639798853367 × 33372027594978156556226010605355114227940760344767554666784520987023841729210037080257448673296881877565718986258036932062711

Algoritme van Shor (1994)

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

RSA-2048 (112 bit security)	4096	(8 uur, studie uit 2019)
ECC-224 (112 bit security)	1300 tot 1600 (!)	?

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

Publieke sleutelcryptografie – Algoritme van Shor

21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979372519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658482382428119816381501067481045166037730605620161967625613384414360383390441495263443219011465754445417842402092461651572335077870774981712577246796292638635637328991215483143816789988504044536402352738195137863656439121201039712282212072035 7

21
(in 2012)

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

Publieke sleutelcryptografie - Conclusie

(Maar daar zijn we nog lang niet)

Impact kwantumcomputers op moderne cryptografie

	Algoritme van Grover	Algoritme van Grover	Algoritme van Shor
	Enkele duizenden logische = enkele miljoenen fysieke qubits		
	25% meer tijd vereist (*)	Nihil (*)	Mogelijks beter dan EC-crypto

(*) Resultaat testen uitgevoerd op Thinkpad laptop with core i5 processor

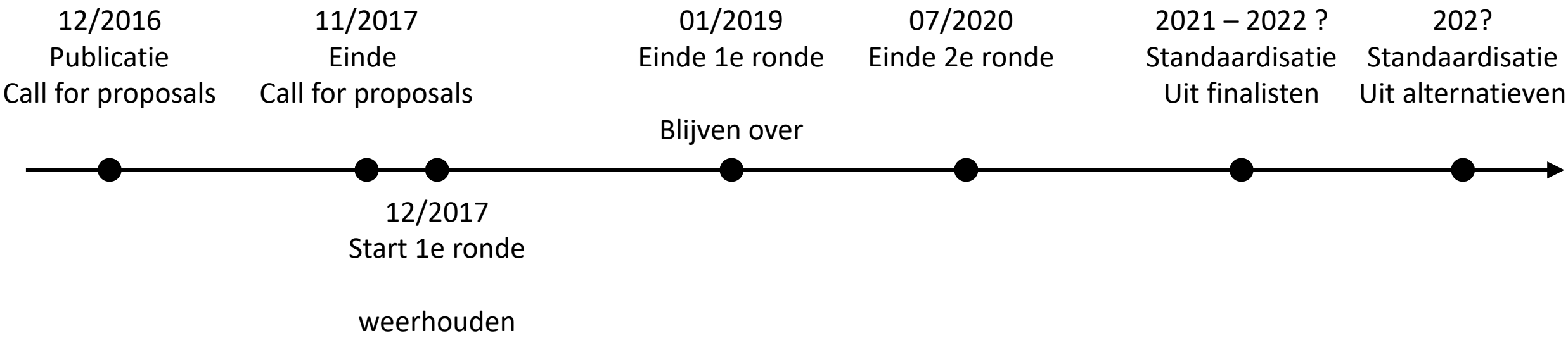
Agenda

- Kwantum- Vs. klassieke computer
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- Conclusies

Twee luiken

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

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



Doorheen procedure , waardoor kandidaten afvielen

Algoritmes . Vb. Met QOS (Quantum Open Safe) library

Meer gevanceerde cryptografische bouwblokken

Smals ICT for society

Kwantumresistente cryptografie – NIST standaardisatieprocedure

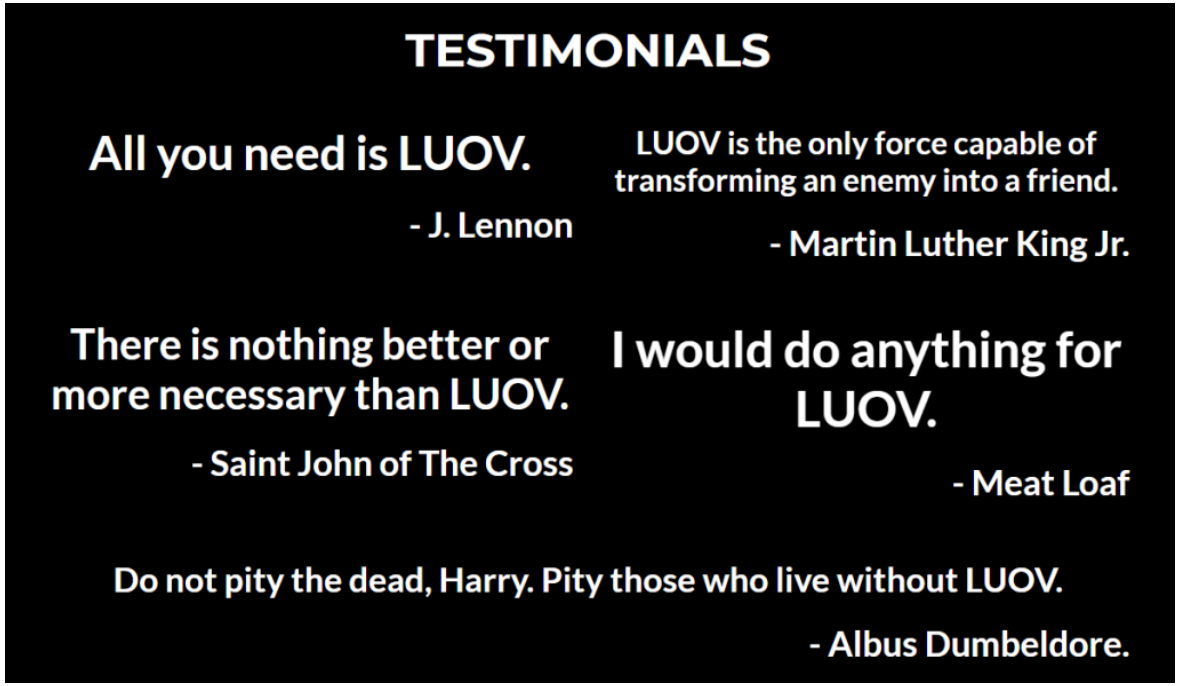
KU LEUVEN

COSIC

SABER
Public-key Encryption and Key-establishment Algorithms

~~**LUOV**~~
~~Digital Signature Algorithms~~

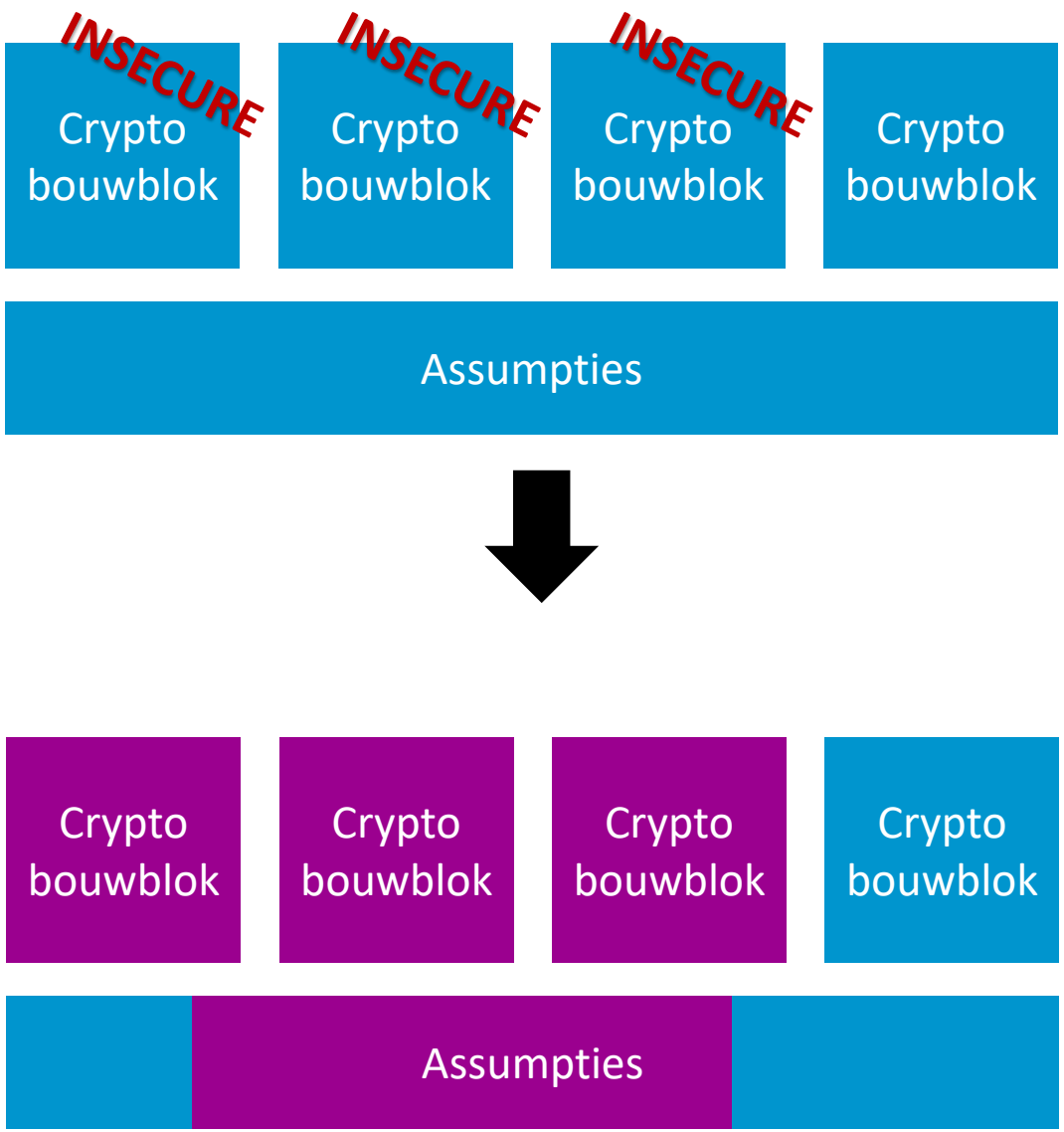
Behoort tot de groep
“Lattice-based cryptografie”
(grootste groep
inzendingen & finalisten)



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

Smals ICT for society

Crypto assumpties & kwantumcomputers



Kwantumresistente cryptografie – NSA

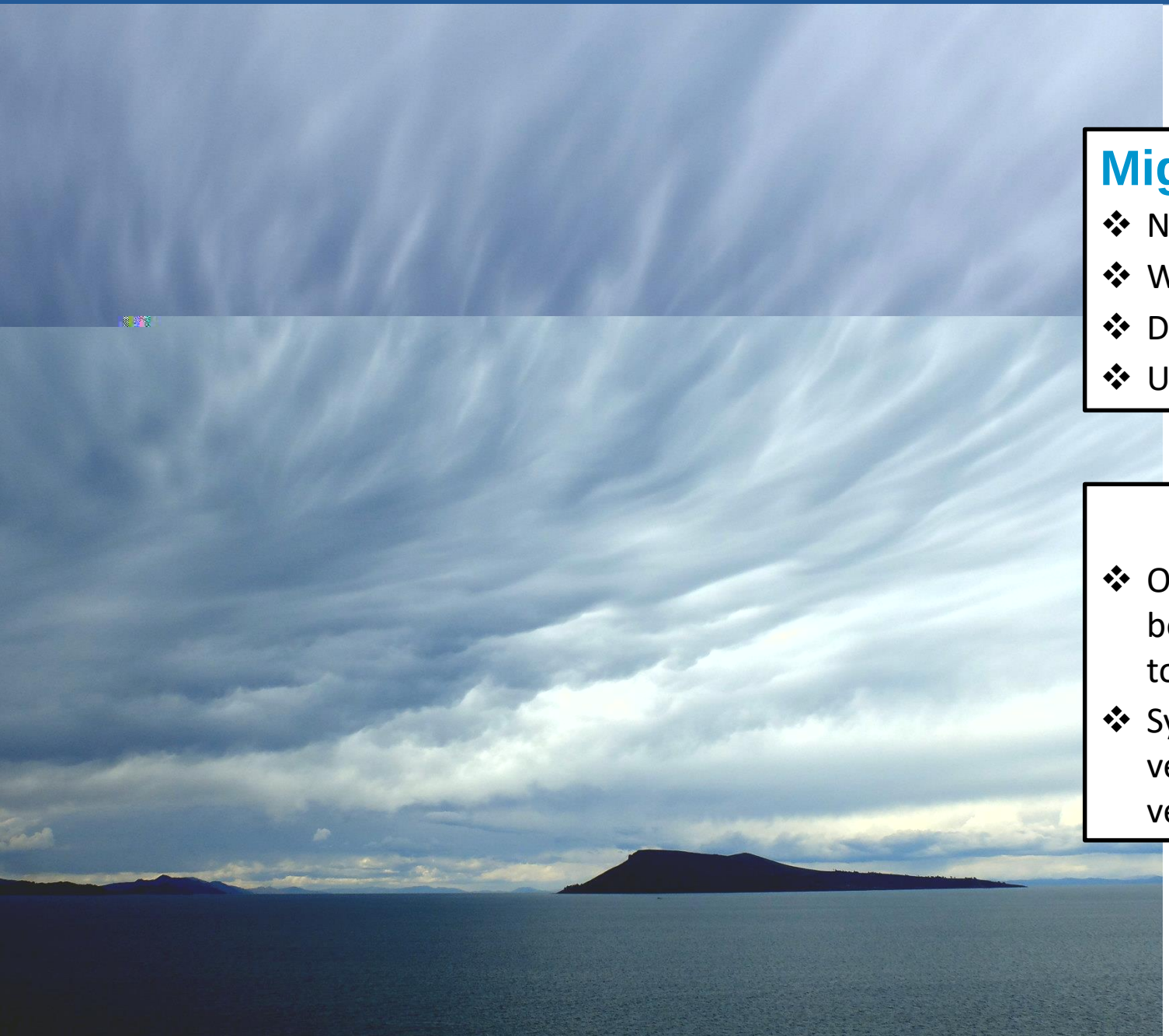
- RSA en EC voor informatie tot niveau top-secret
- Indien je nog niet overgeschakeld bent van RSA naar EC, wacht je beter op kwantumresistente standaard
- Kans dat vreemde mogendheid op termijn over kwantumcomputer beschikt, wordt ernstig genomen

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

"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
- Wacht standaardisatieprocedure af
- Daarna ev. geleidelijk migreren
- Urgentie hangt af van risicoinschatting

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

Smals
ICT for society

Agenda

- Kwantum- Vs. klassieke computer
- Kwantumcomputers (niet) in de praktijk
- De crypto-apocalypse?
- Kwantumresistente cryptografie

Conclusie

Agenda

Vragen?

Kristof Verslype
Cryptographer, PhD
Smals Research

Smals
ICT for society

kristof.verslype@smals.be
+32(0)2 7875376
www.smals.be
www.smalsresearch.be
www.cryptov.net (personal)

PRIMEUR

http://www.smalsresearch.be/download/research_reports/Report-kwantum-en-crypto.pdf

Smals
ICT for society

Blogposts

Kwantumcomputers & cryptografie deel 2: Kwantum (niet) in de praktijk

Posted on 08/04/2020 by Kristof Verslype

Welkom in het 2e deel van de reeks kwantumcomputers & cryptografie. We gaan in op de huidige stand van zaken in kwantumcomputerland en schijnen licht op vragen zoals: "Hoe ver staan we met

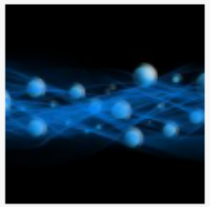
Continue reading →

y | Tagged cryptography, physics, quantum computing | 1 Reply

Posted in Securit

Kwantumcomputers & cryptografie deel 1: Kwantum- Vs. klassieke computer

Posted on 25/02/2020 by Kristof Verslype



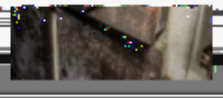
Het tijdperk van de kwantumcomputers lijkt snel dichterbij te komen. Dergelijke computers zouden een mokerslag geven aan de hedendaagse cryptografie. Bedrijven claimen revolutionaire doorbraken. Grootmachten investeren miljarden waardoor het zelfs wat doet denken aan een wapenwedloop. De dominantie van de … Continue reading →

Posted in Security | Tagged cryptography, physics, quantum computing | Leave a reply

Kwantumcomputers & cryptografie deel 3: De Crypto-apocalypse?

Posted on 19/05/2020 by Kristof Verslype

Welke impact zullen kwantumcomputers hebben op onze moderne cryptografie, die levensnoodzakelijk is in onze samenleving? Deze blogpost bespreekt de



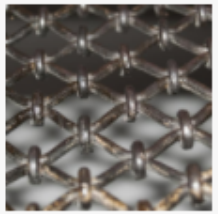
quantum computing, Security |

Posted in Security | Tagged cryptography,

Leave a reply

Kwantumcomputers & cryptografie deel 4: Kwantumresistentie

Posted on 01/09/2020 by Kristof Verslype



Het vorige deel van de reeks kwantumcomputers & cryptografie ging in op de bedreiging die krachtige kwantumcomputers op termijn kunnen vormen voor de moderne publieke sleutelcryptografie. Dit vierde en laatste deel bespreekt hoe we ons daartegen kunnen wapenen met behulp … Continue reading →

Posted in Security | Tagged cryptography, quantum computing, Security | Leave a reply

Smals ICT for society

Referenties

- D. ROTMAN. *We're not prepared for the end of Moore's Law.* MIT technology review, 24 February 2020
  https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/
- 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/
- 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
- S. SRIVASTAVA. Top 10 countries leading in quantum computing technology. 14 December 2019, Analytics Insight
  https://www.analyticsinsight.net/top-10-countries-leading-quantum-computing-technology/

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