

Kwantumcomputers & Cryptografie

**Kwantumcomputers, hun impact op moderne
cryptografie en de zoektocht naar kwantumresistentie**

Kristof Verslype
Cryptographer, PhD
Smals Research



**Innovation with
new technologies**



**Consultancy
& expertise**



**Internal & external
knowledge transfer**



**Support for
going live**

**NewSQL
Databases**

**Anomalies &
Transaction
Management**

**Conversational
Interfaces**

**Near-real-time
Translation**

**Web Scraping
for Analytics**

**GIS for
Analytics**

**Augmented
Reality**

**Graph Analytics
Visualisation**

2020

**AI Cases &
Deployment**

**Robotic Process
Automation**

Crypto Cases

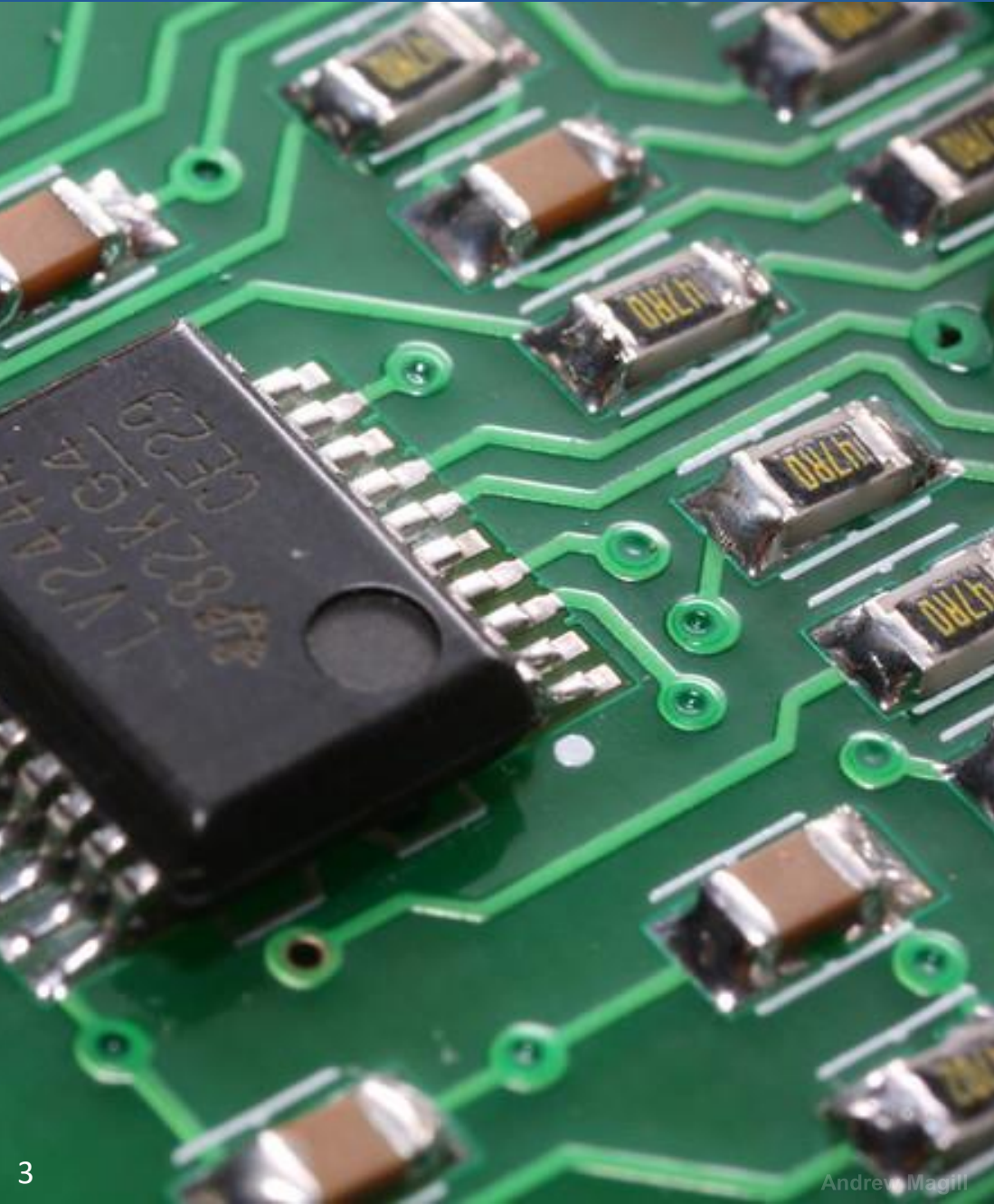
**European
Blockchain
Infrastructure**

**Knowledge
Graphs**

**Advanced
Cryptography**

**Quantum
Computing &
Cryptography**

**FIDO2 / Web
Authentication**



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

CRYPTO WERKPAARDEN

Encryptie

DES, AES, ElGamal, RSA, ...

Digitale handtekeningen

RSA, DSA, Schnorr, ...

Authenticatie

SSH, CHAP, ...

Hashing

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

Key exchange

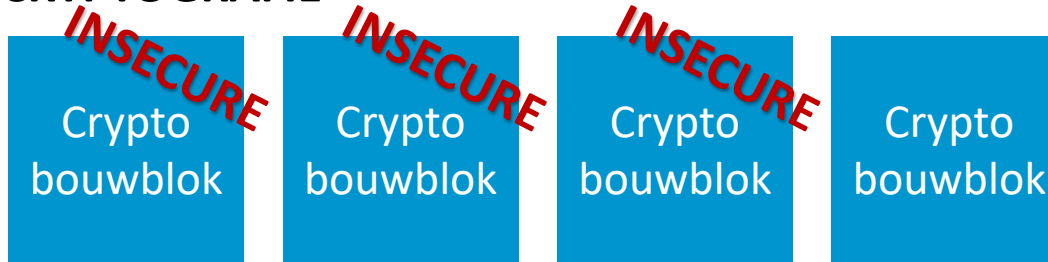
Diffie-Hellman, ...

Message authentication code

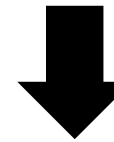
HMAC, ...

HEDENDAAGSE CRYPTOGRAFIE

Mogelijkheden:

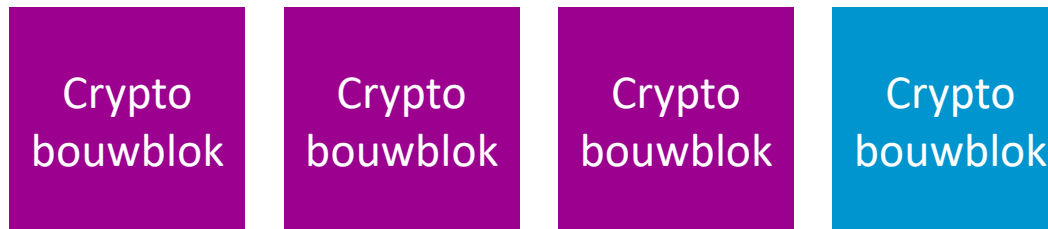


Fundamenten:



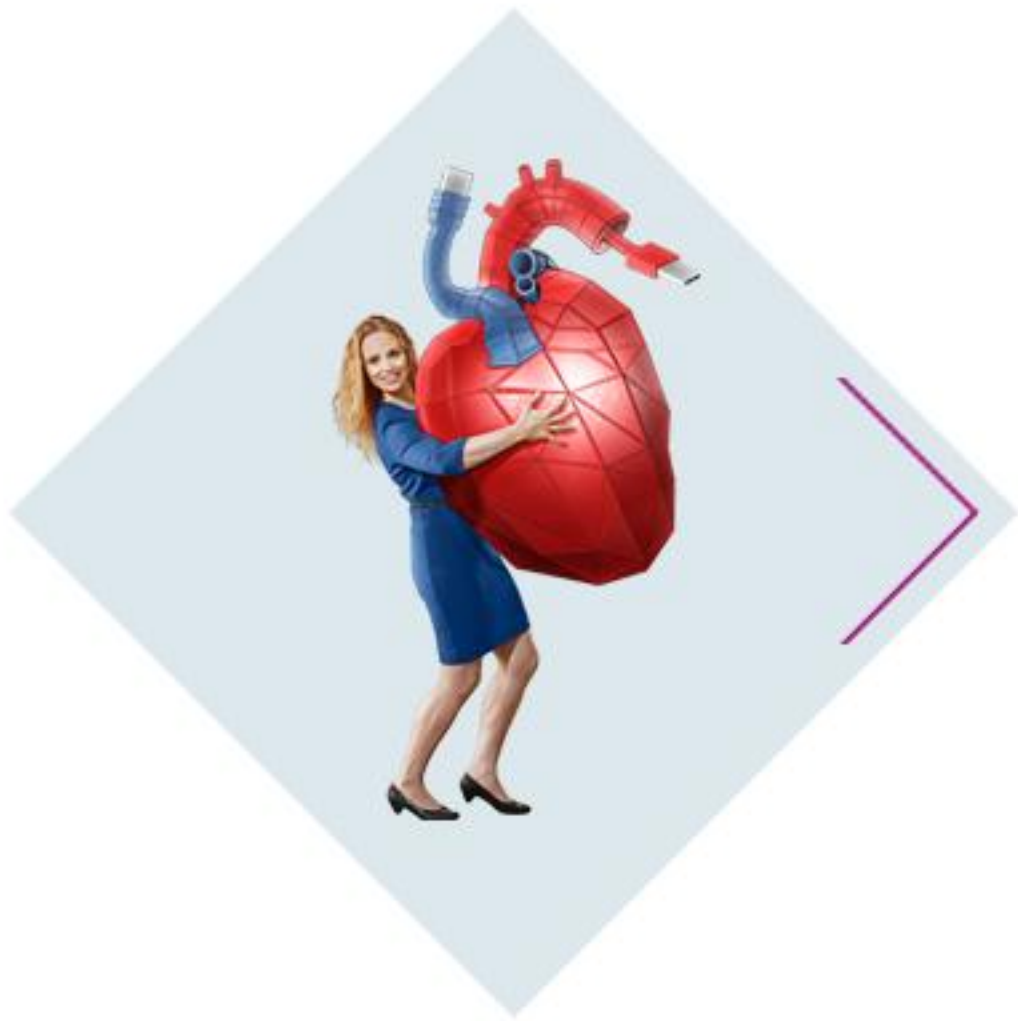
KWANTUMRESISTENTE CRYPTOGRAFIE

Mogelijkheden:



Fundamenten:





Agenda

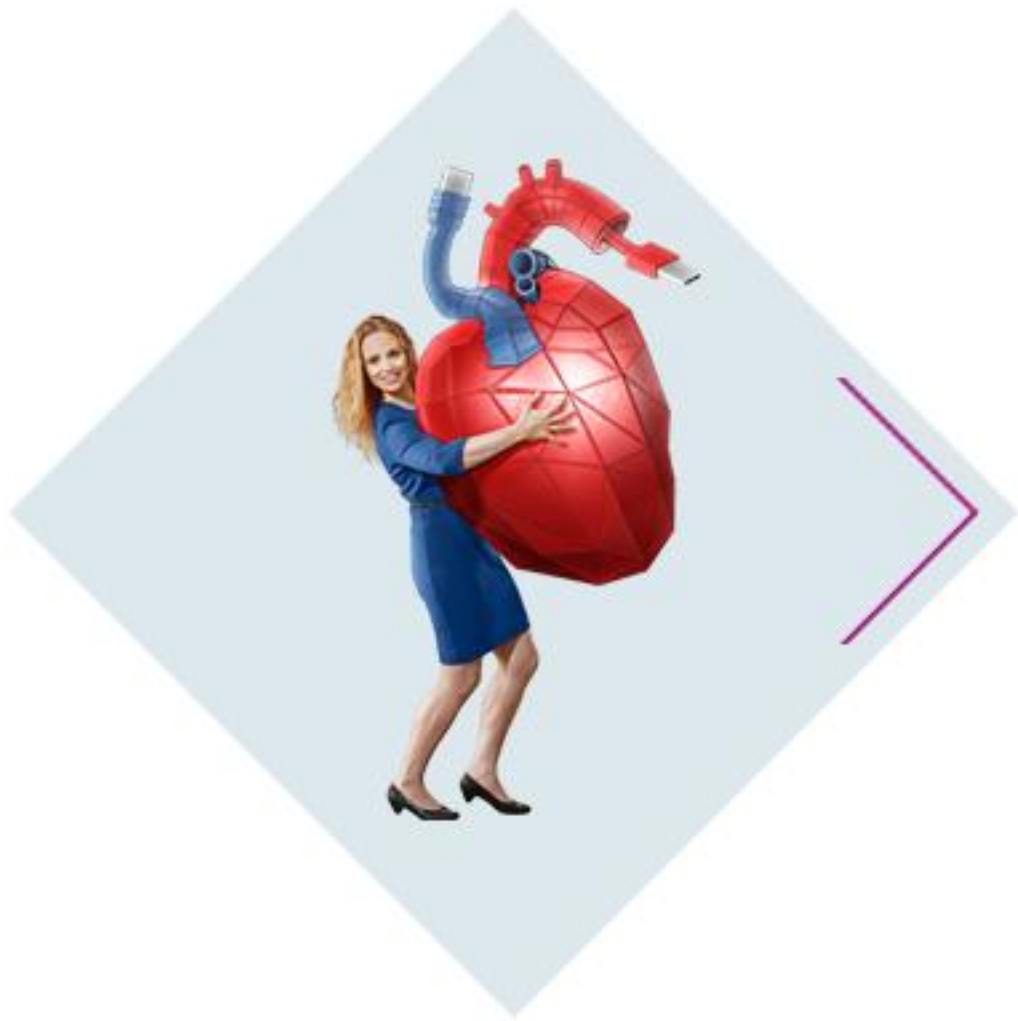
◆ Kwantum- Vs. klassieke computer

◆ Kwantumcomputers (niet) in de praktijk

◆ De crypto-apocalypse?

◆ Kwantumresistente cryptografie

◆ Conclusies



Agenda

◆ Kwantum- Vs. klassieke computer

◆ Kwantumcomputers (niet) in de praktijk

◆ De crypto-apocalypse?

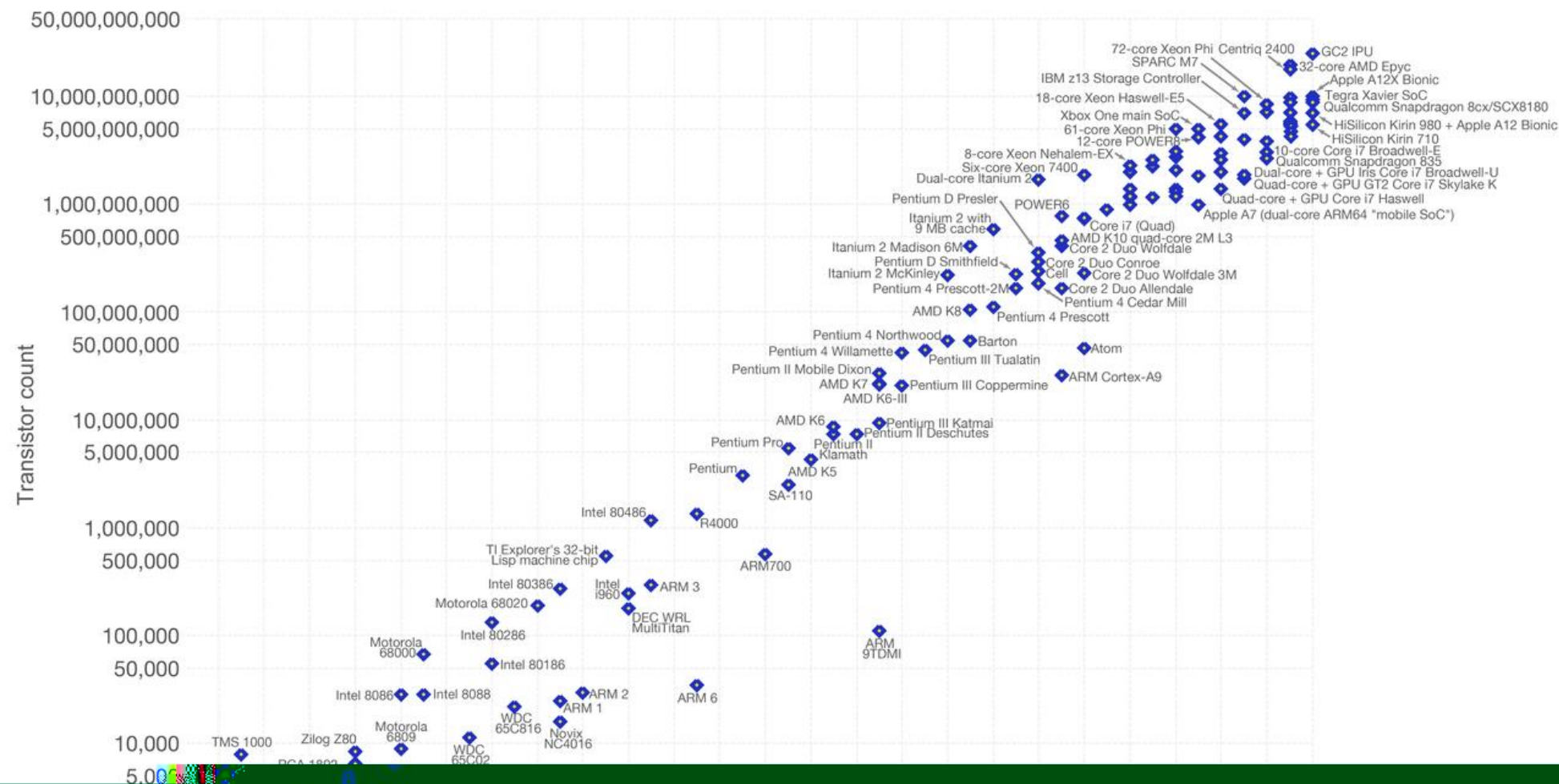
◆ Kwantumresistente cryptografie

◆ Conclusies

Wet van Moore

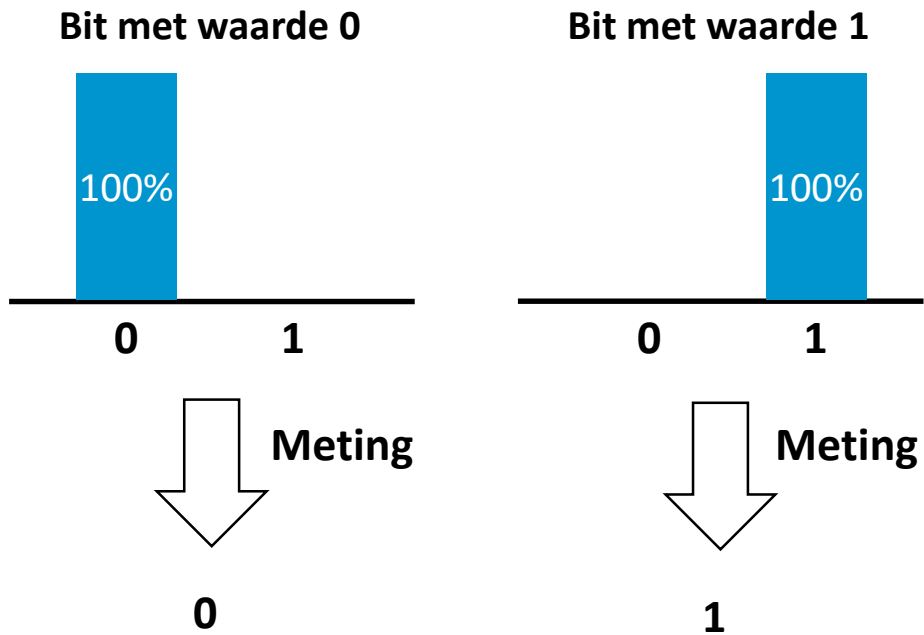
Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.



- ❖ 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?

Klassieke computer

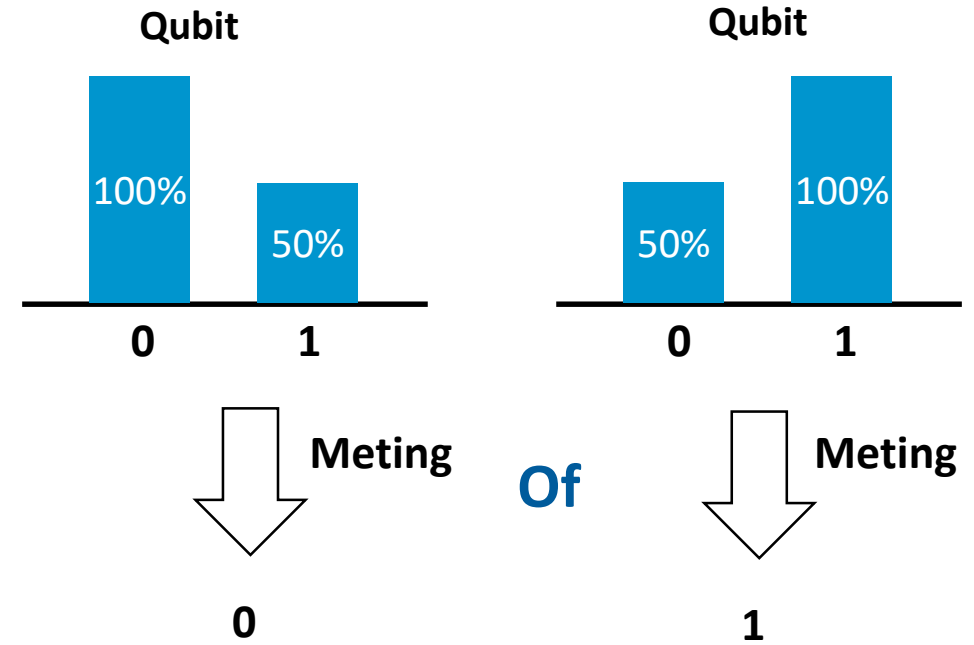


Elektrische lading

Waarde ligt al vast van voor de meting

Meting geen impact op toestand bit

Kwantumcomputer

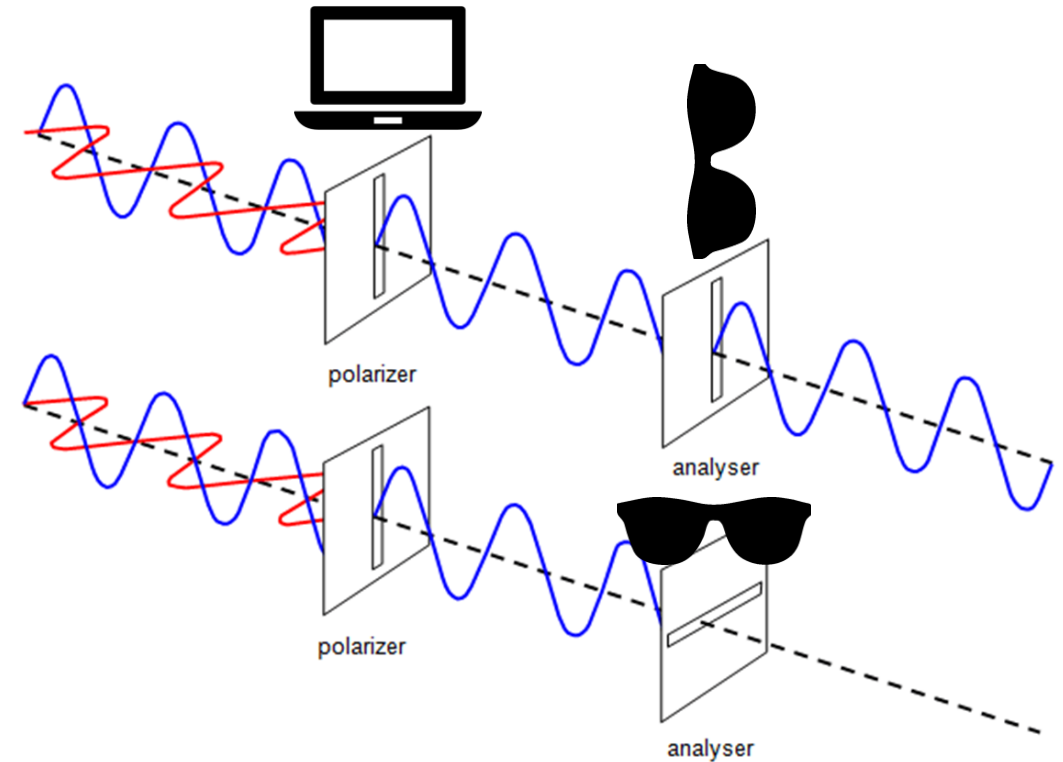
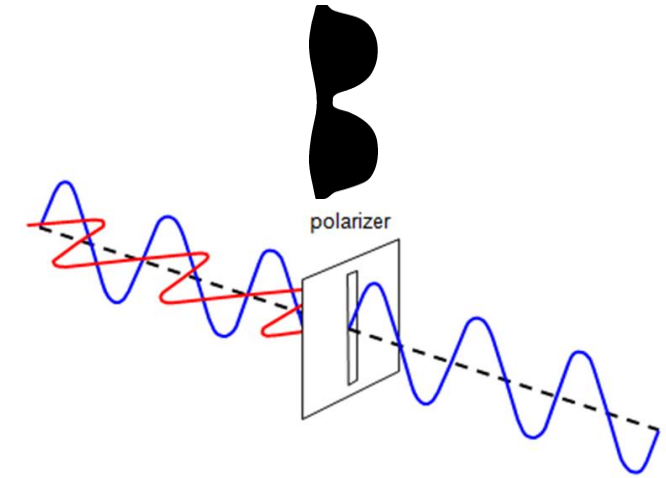
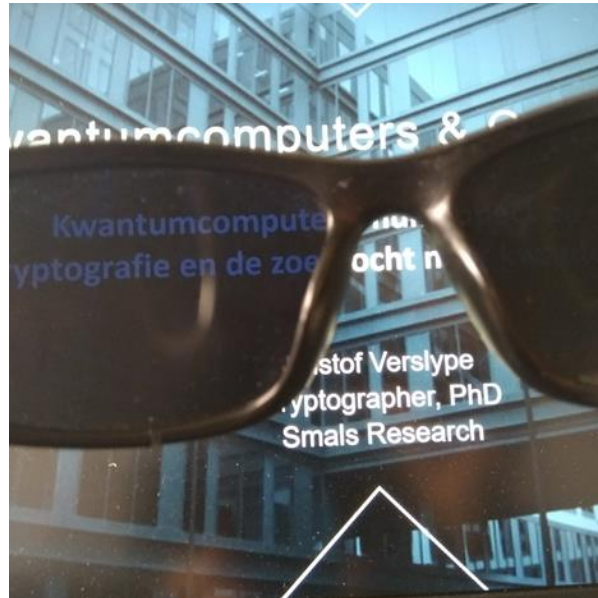
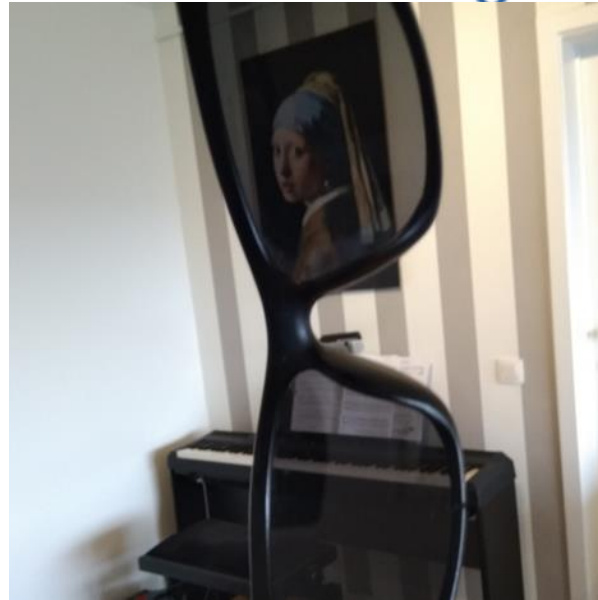


(Sub)atomair 'deeltje' (vb. Foton, elektron)

Waarde onbepaald (uitgesmeerd) tot op moment van meting

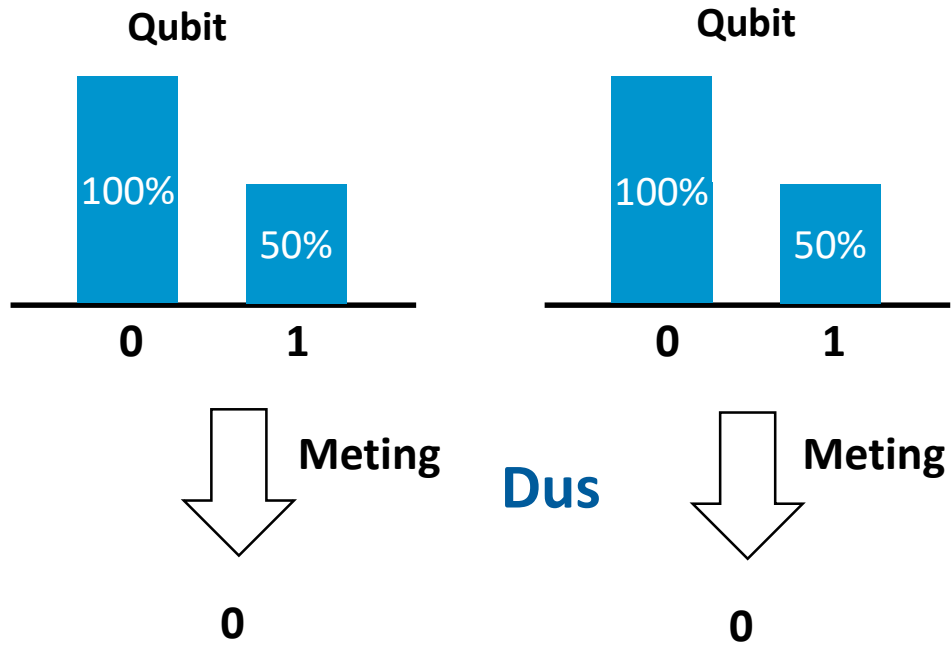
Meting vernietigt kwantumtoestand: Het mogelijke wordt een concrete waarde

Polarisatie van fotonen – Zonnebrillexperiment

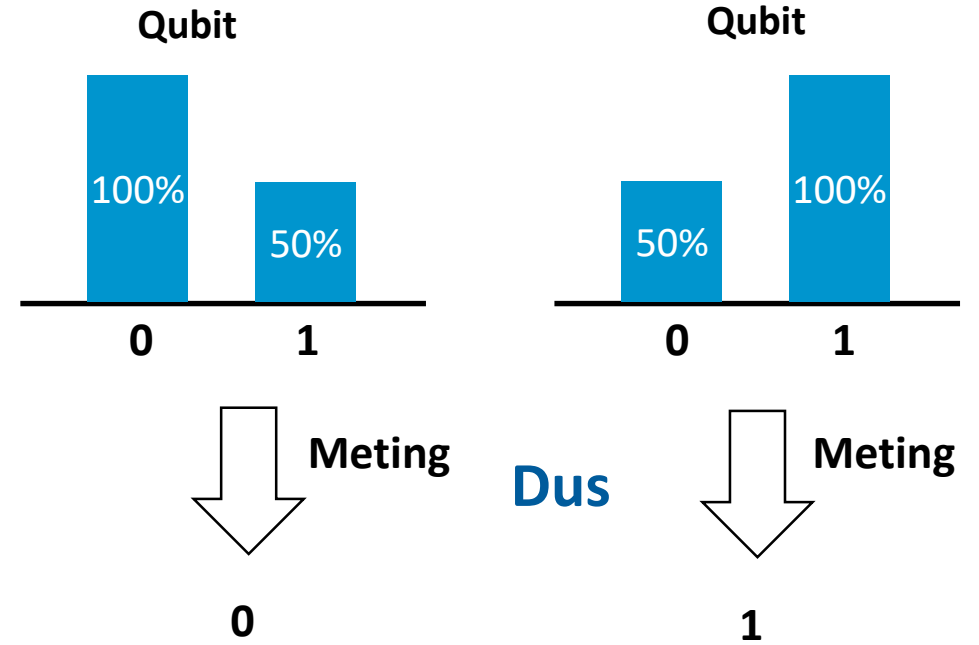


Verstrengeling (entanglement)

Gelijke superpositie



Tegengestelde superpositie



Correlatie tussen metingen van verwante deeltjes

Meting ene qubit volstaat om resultaat andere te kennen

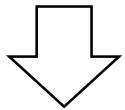
Onafhankelijk van onderlinge afstand qubits ($\leftrightarrow$ Newtoniaanse fysica)

Verstrengeling van meer dan 2 qubits kan ook

Verstrengeling (entanglement)

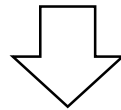
Superpositie

Waarde is onbepaald tot op het moment van meting



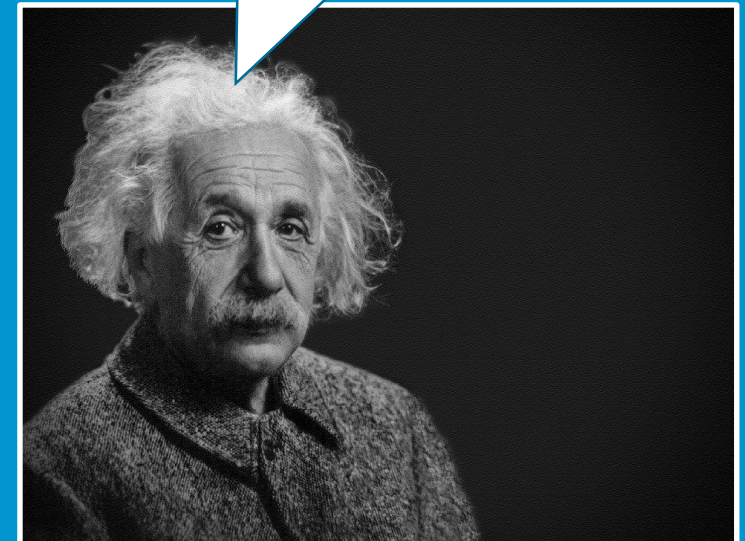
Verstrengeling

Meting ene qubit heeft impact op uitkomst meting andere qubit



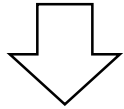
**Op moment meting van ene qubit wordt waarde andere qubit bepaald
→ Soort connectie, onafhankelijk van afstand**

Spukhafte Fernwirkung!
(Spookachtige werking
op afstand!)



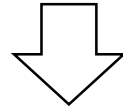
Met hoge waarschijnlijkheid
bevestigd door experimenten
(vb. Bell test experiments)

Bouwstenen voor berekeningen: Logische poorten



Klassieke computer

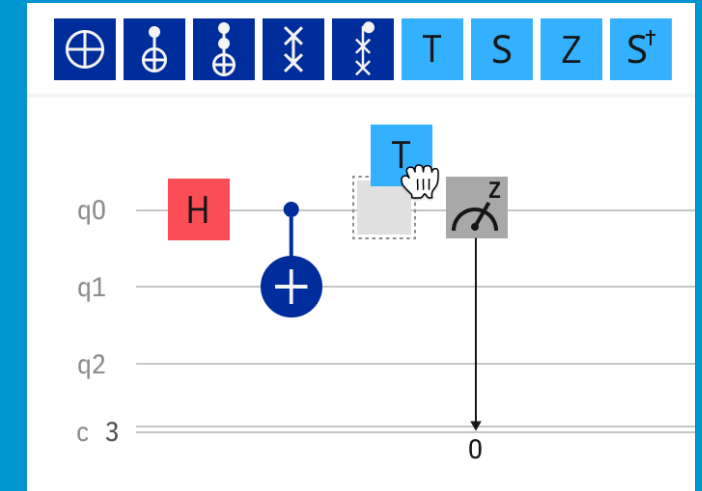
Logische poorten:
AND, NOT, OR, XOR, ...



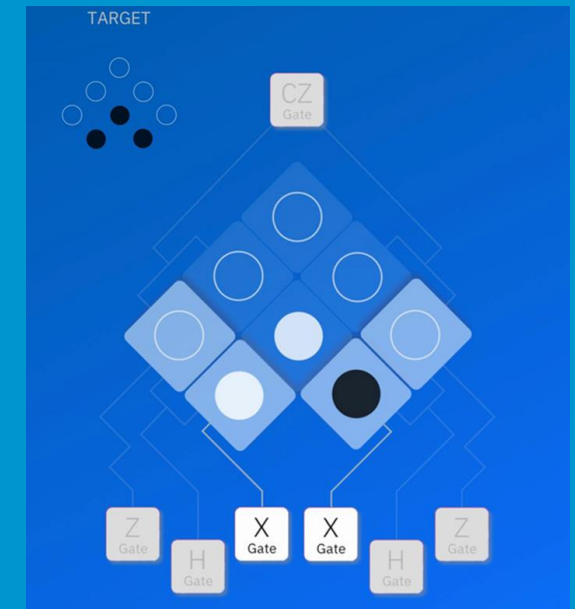
Kwantumcomputer

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

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



IBM Quantum Experience



IBM Hello quantum app

Misvatting

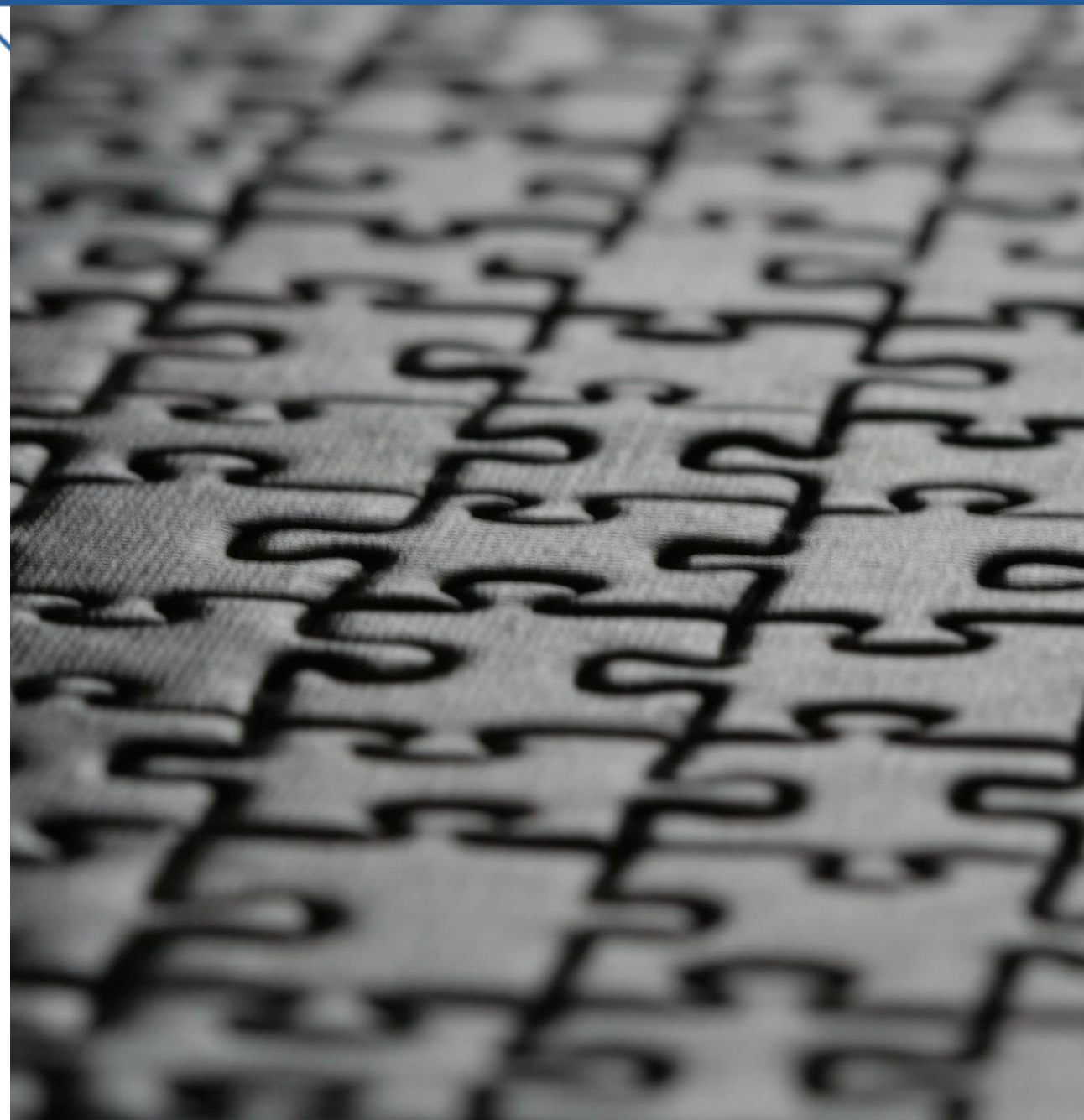
“Kwantumcomputers zullen alle problemen kunnen oplossen die moeilijk (of zelfs onmogelijk) zijn voor klassieke computers.”

Correcter

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

Wapenwedloop

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



Kwantumcomputers

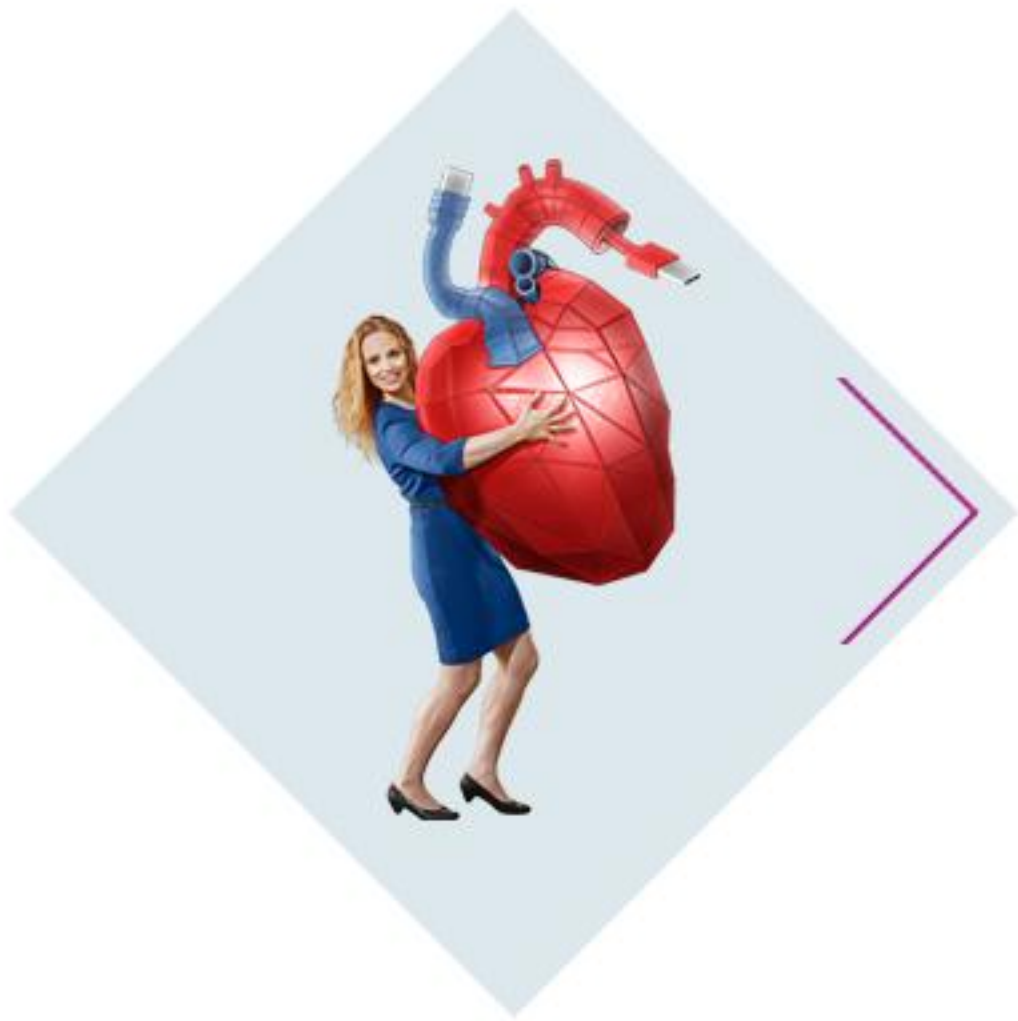
- ❖ Steunen op weinig intuïtieve principes zoals verstrengeling en superpositie
- ❖ Hebben Qubits – (sub)atomaire deeltjes / golven – als kleinste opslag- en rekeneenheid
- ❖ Berekening gebeuren op fundamenteel andere wijze dan bij klassieke computers
- ❖ Zijn – op papier – krachtig voor een beperkte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

Koen Bertels

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



Agenda

◆ Kwantum- Vs. klassieke computer

◆ **Kwantumcomputers (niet) in de praktijk**

◆ De crypto-apocalypse?

◆ Kwantumresistente cryptografie

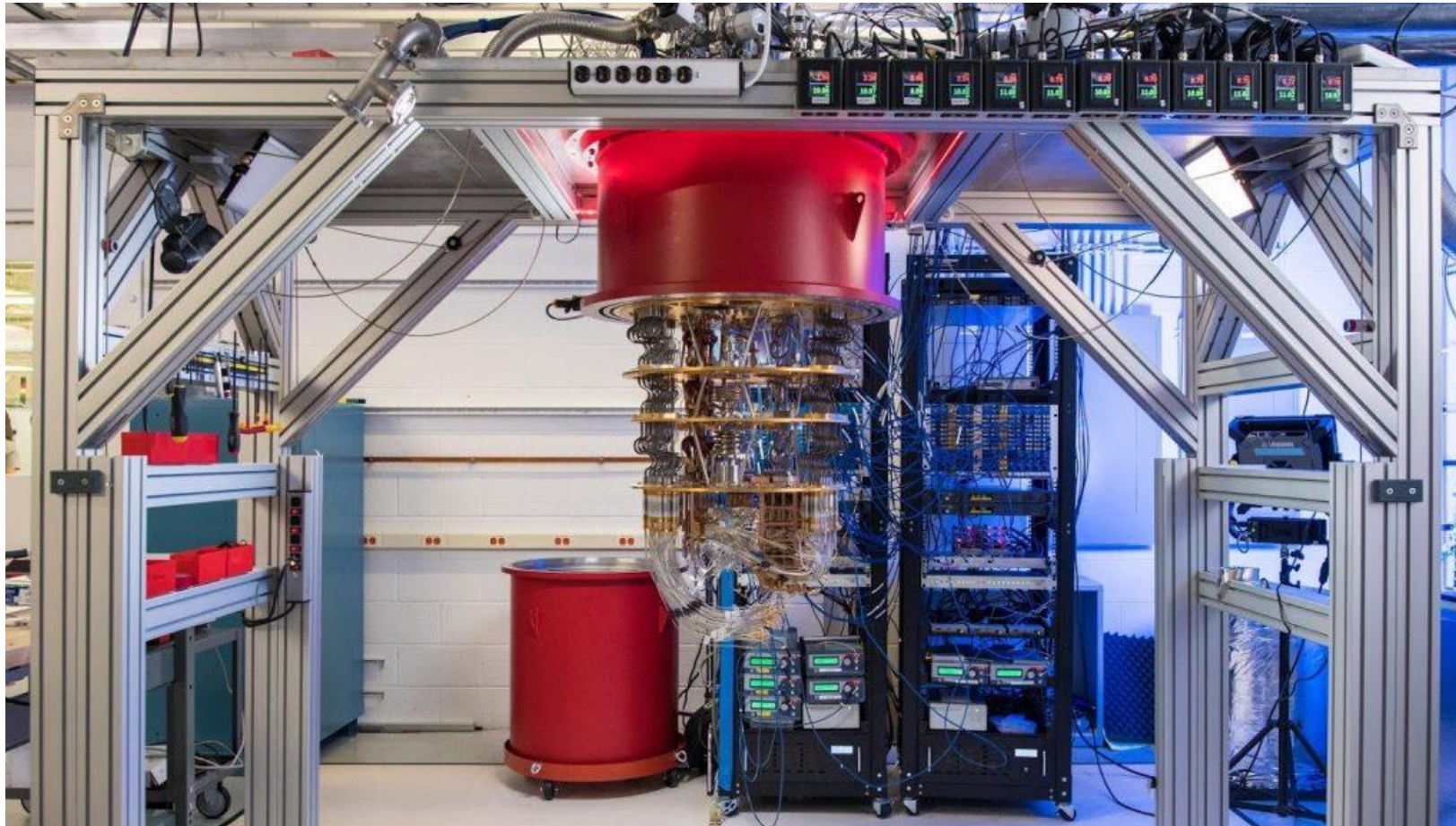
◆ Conclusies

23 October 2019



Article

Quantum supremacy using a programmable superconducting processor



23 October 2019



Article

Quantum supremacy using a programmable superconducting processor



Quantum supremacy

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

Eén, in de praktijk nutteloos probleem, volstaat!

John Preskill, 2012

Het probleem

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

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”

23 October 2019



Article

Quantum supremacy using a programmable superconducting processor



Quantum supremacy

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

Eén, in de praktijk nutteloos probleem, volstaat!

John Preskill, 2012

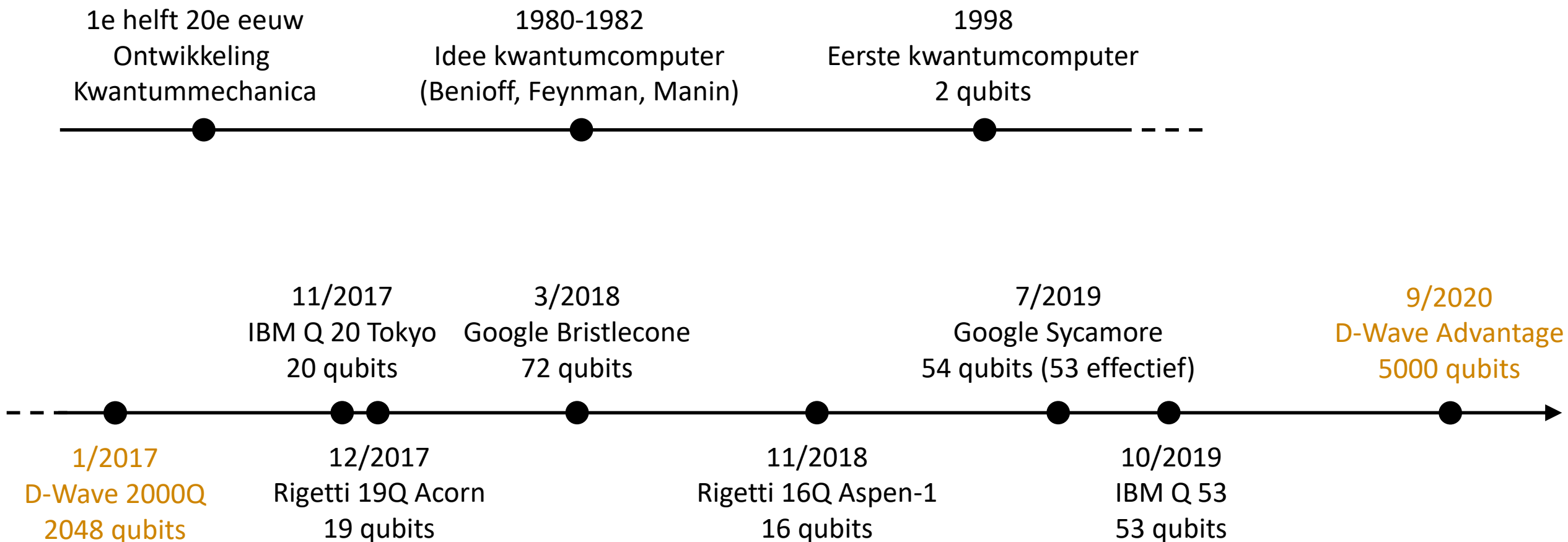
Quantum advantage

Kwantumcomputer kan probleem sneller oplossen dan een klassieke computer

Conclusie

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

Historiek & State of the art





Kenmerken

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

**Nu voor slechts
\$ 15 000 000**



Meer qubits ≠ meer rekenkracht

Type kwantumcomputer (principe)

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

Ruis / nauwkeurigheid

...

→ IBM prefereert de term ***Quantum Volume***

→ Vergelijken niet evident. Bedrijven niet steeds transparent over inner workings & specs



Waarom is het bouwen van een kwantumcomputer zo complex?

Isolatie

Foutencorrectie

Schaalbaarheid

Topologie



Interferentie

- ❖ Qubits enorm gevoelig voor interferentie buitenaf
- ❖ Temperaturen dicht tegen absolute nulpunt ($-273,15^{\circ}\text{C}$)
- ❖ Afgeschermd van trillingen, licht & magnetische straling

Decoherence time

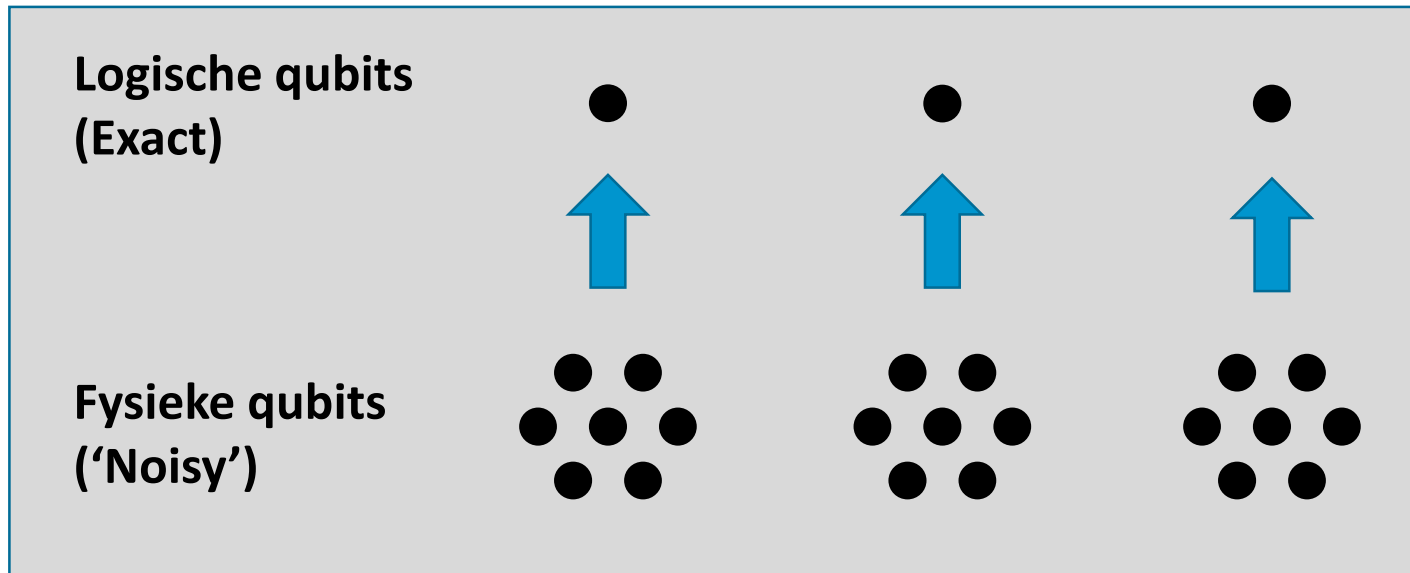
- ❖ Nooit volledig vrij van interferentie
- ❖ Uitdaging: voldoende lang coherent houden kwantumtoestand
- ❖ Googles Sycamore: tienden of honderdsten van een microseconde

Evolutie

- ❖ Veel vooruitgang geboekt voorbij jaren
- ❖ Toch fouten wellicht onvermijdelijk

Fouten wellicht onvermijdelijk → foutencorrectie noodzakelijk

Meerdere fysieke qubits vormen samen 1 logische qubit



Evolutie

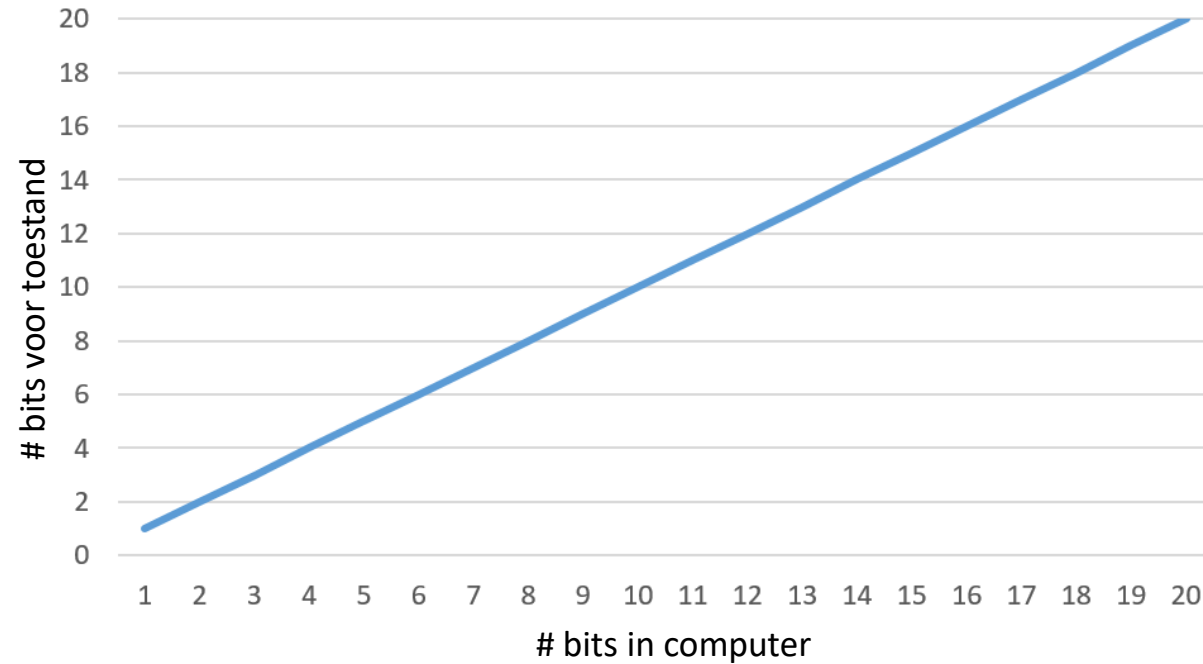
- ❖ Jaren '80 en '90: “*onmogelijk!*”
- ❖ Theoretisch mogelijk
- ❖ Nog geen experimenten (in de praktijk mogelijk?)

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

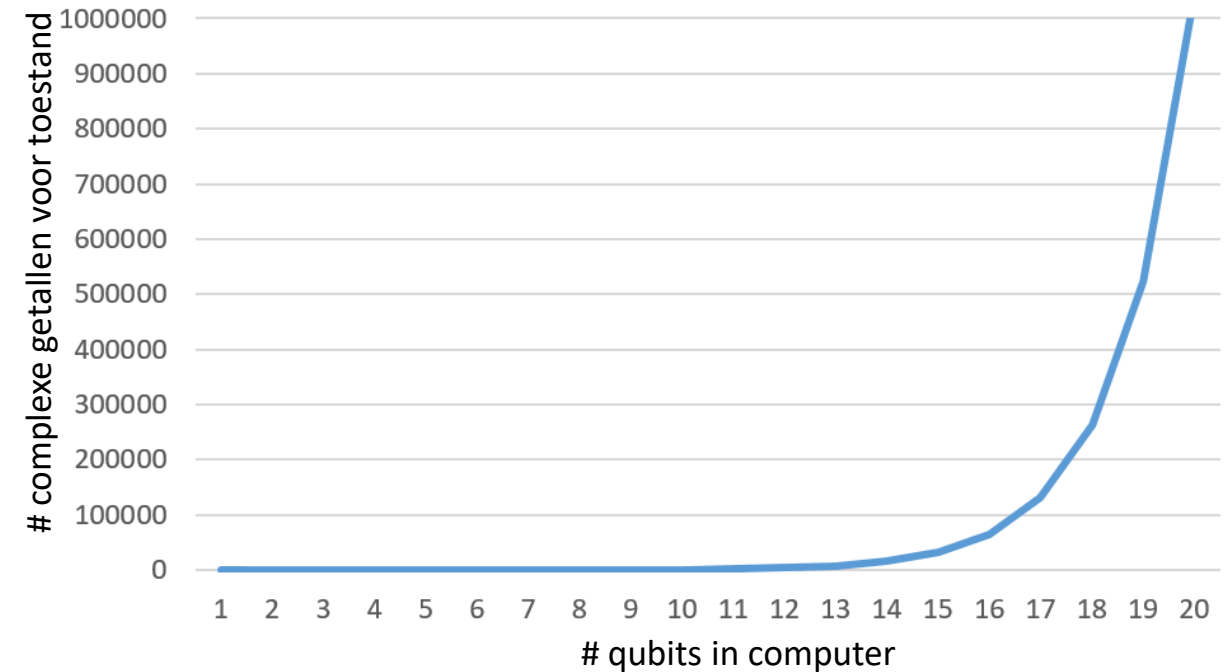
Aantal bits voor beschrijving
toestand klassieke computer



Complexiteit groeit lineair

Verdubbeling complexiteit bij verdubbeling aantal bits

Aantal complexe getallen voor beschrijving
toestand kwantum computer



Verdubbeling groeit exponentieel

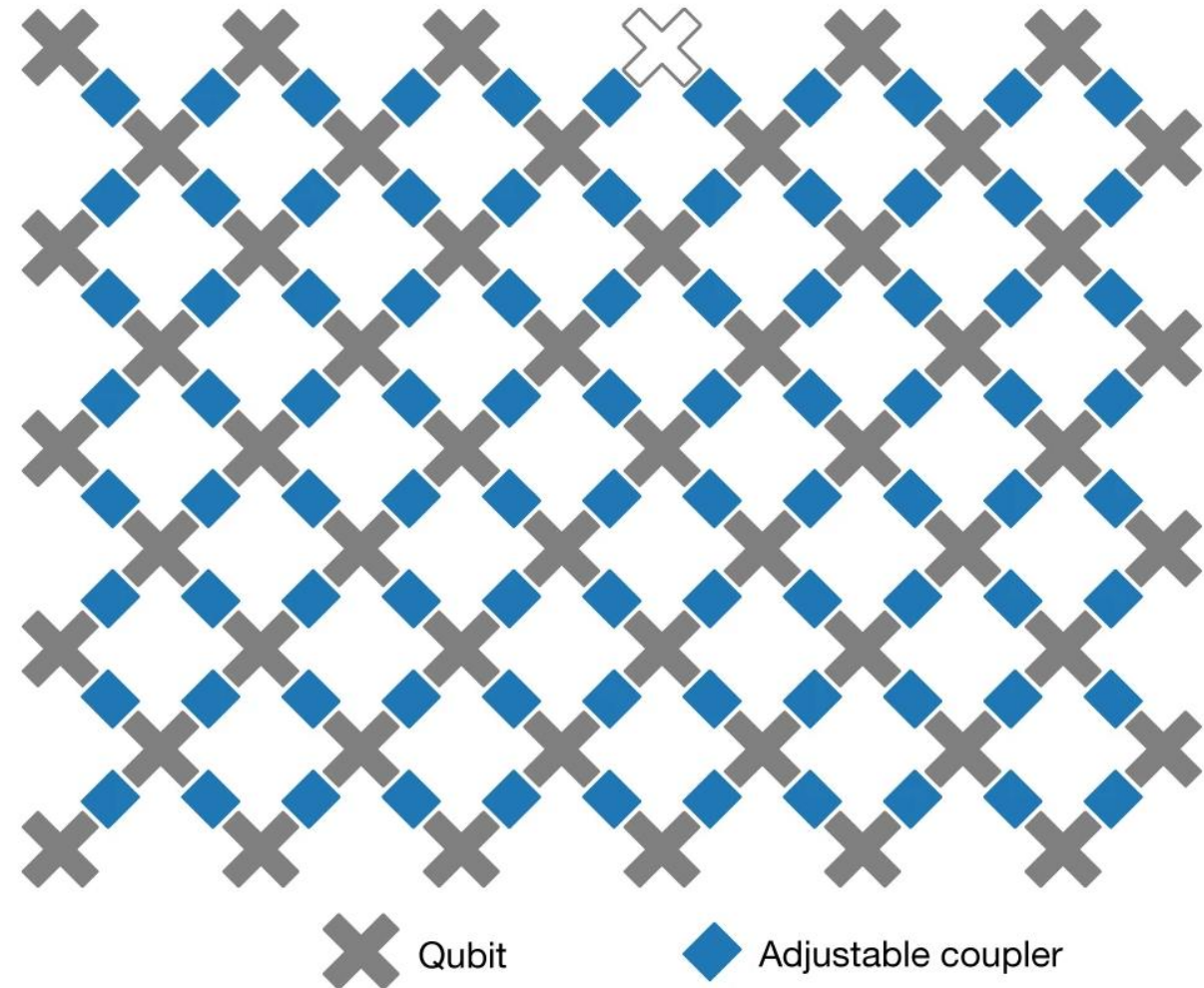
Complexiteit verdubbeld per extra qubit

Vb. 1000 qubits

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

Klassieke computer

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



Operaties enkel mogelijk op één enkele of twee aan elkaar grenzende qubits



Waarom is het bouwen van een kwantumcomputer zo complex?

Isolatie

Foutencorrectie

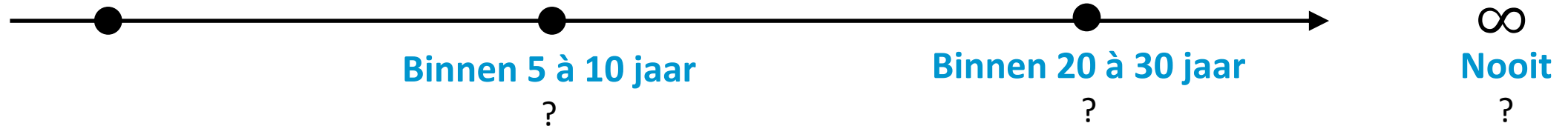
Schaalbaarheid

Topologie

De uitdagingen zijn astronomisch!

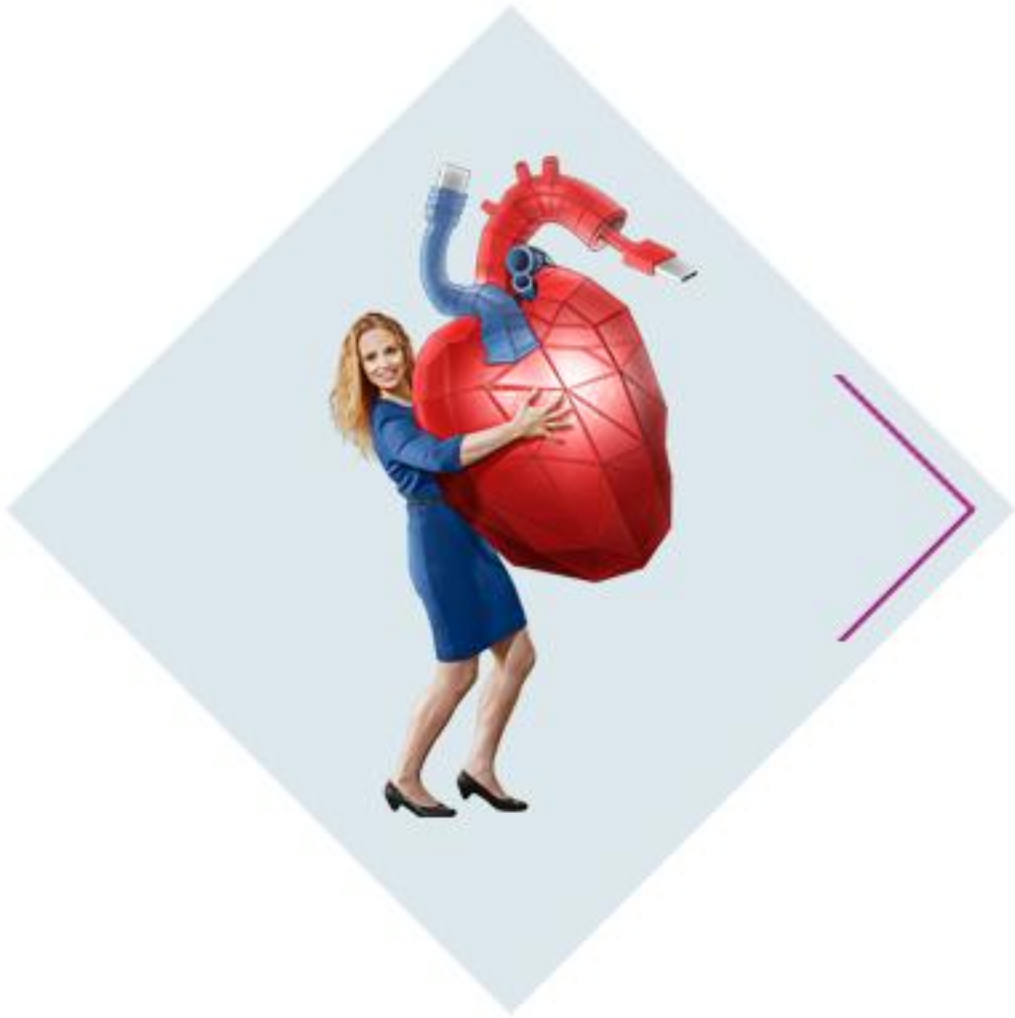
Vandaag

- ❖ 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

◆ Kwantum- Vs. klassieke computer

◆ Kwantumcomputers (niet) in de praktijk

◆ **De crypto-apocalypse?**

◆ Kwantumresistente cryptografie

◆ Conclusies

Impact kwantumcomputers op moderne cryptografie?

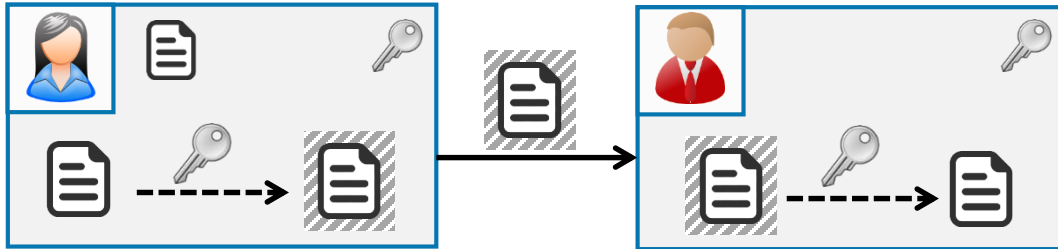
Symmetrische
cryptografie

Cryptografische
hashfuncties

Publieke
sleutelcryptografie

Symmetrische vercijfering

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



Kraken = vinden sleutel

Toy klassieke computer

- ▶ 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

Toy kwantumcomputer

- ▶ 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

256 → 512 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

Algoritme van Grover op kwantumcomputer

Aantal vereiste LOGISCHE qubits

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

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

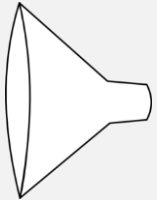


Krachtige kwantumcomputers vormen geen bedreiging voor symmetrische cryptografie

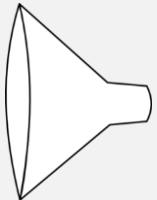
(Zorg wel voor voldoende lange sleutels)

Cryptografische hashfunctie

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

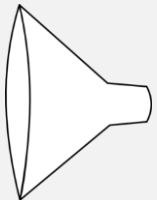


5e 50 6e 82 7f d5 50 ec 4e 08 8e e7 75 8f 34 b3
a6 8e 34 93 d5 89 98 52 97 48 f0 c6 c1 70 f3 3c



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

“Hello world!”

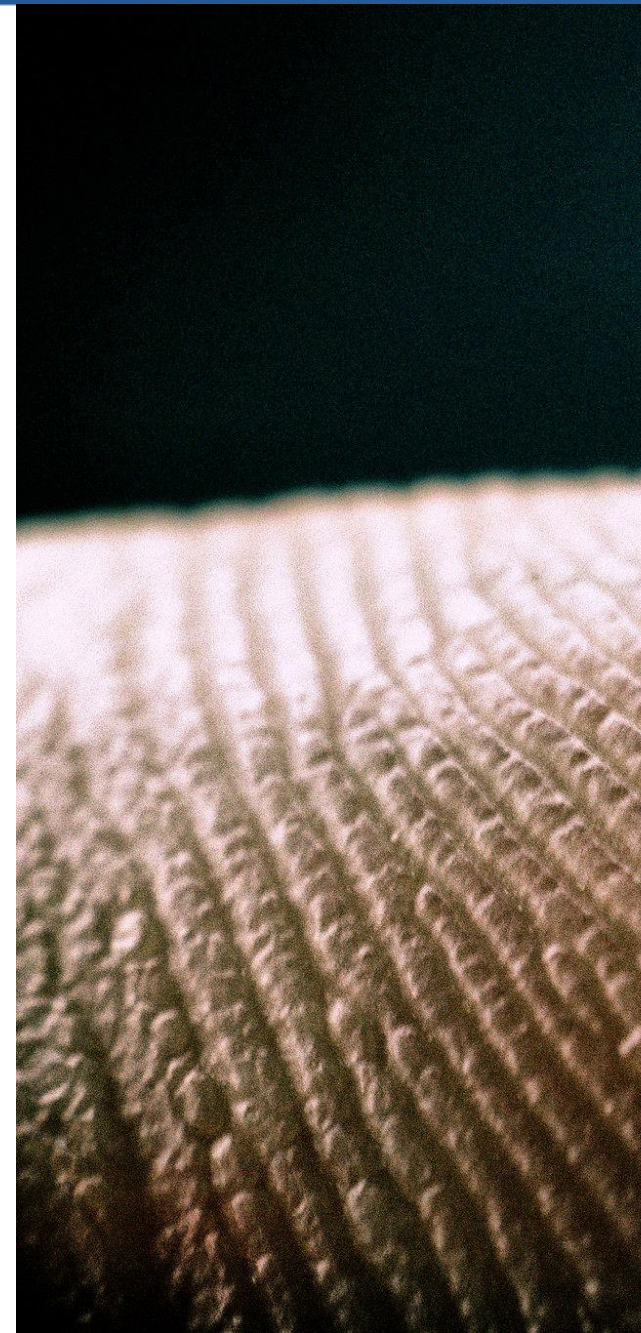


c0 50 50 4b e2 52 94 f4 9a 20 19 00 04 00 38 89
d3 4e 4b 20 a2 d0 5b f6 f3 8b 2d f9 17 49 85 10

Fixed-length output

One-way

Collision resistant



Collision attack

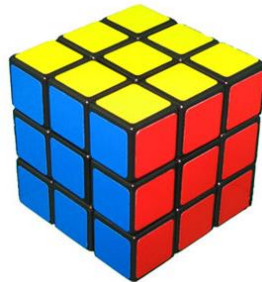
- ▶ Vinden van twee inputs die resulteren in dezelfde output
- ▶ Voor SHA1 slaagde zo'n aanval in 2017

Klassieke computer

- ▶ 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

Kwantumcomputer

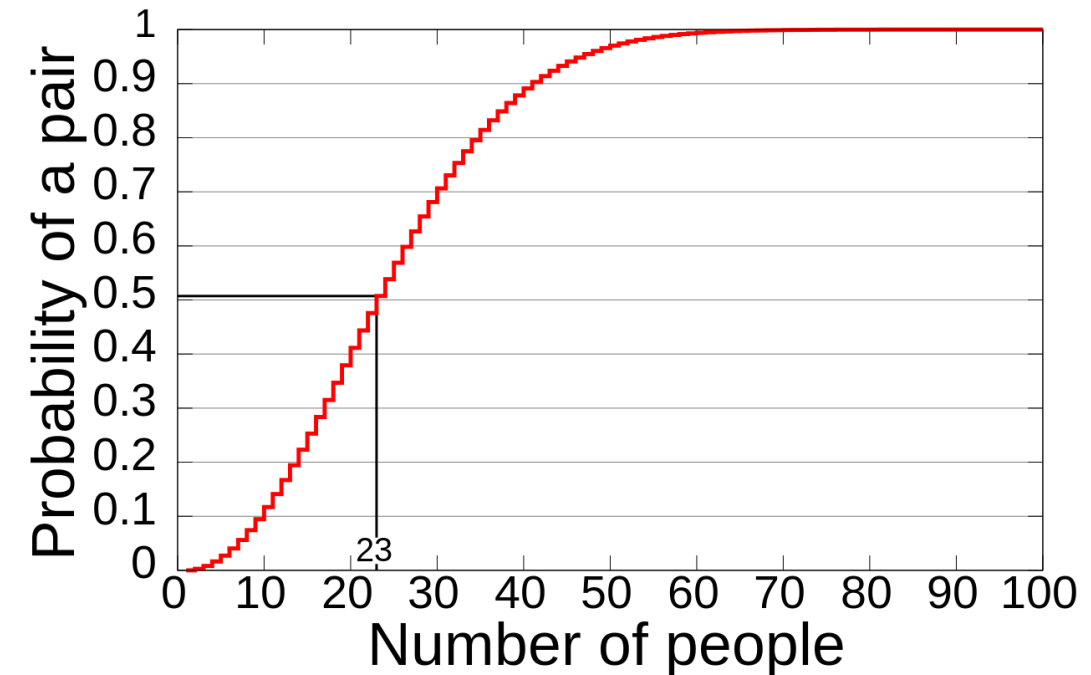
- ▶ Algoritme van Grover
- ▶ Veiligheid daalt
van $\sqrt{2^{256}} = 2^{128}$
tot $\sqrt[3]{2^{256}} = 2^{85} \approx 10^{26}$ (Onveilig)



Maatregel

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

Verjaardagenparadox



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

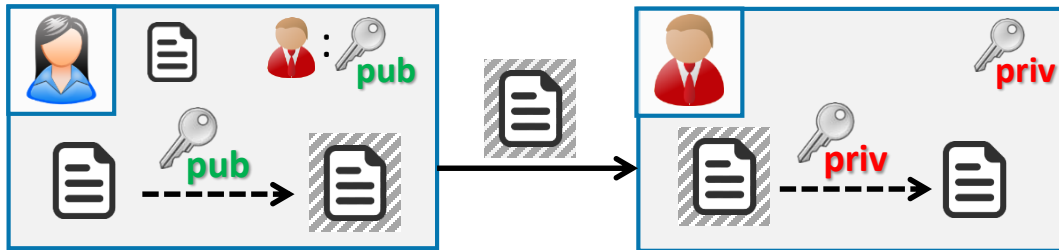


Krachtige kwantumcomputers vormen geen bedreiging voor cryptografische hashfuncties

(Zorg wel voor voldoende lange uitvoer)

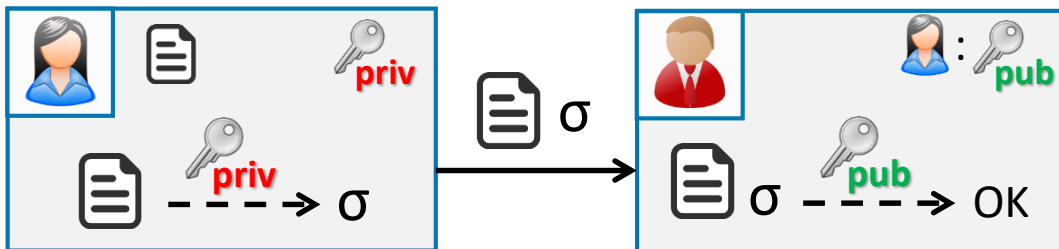
Publieke sleutel encryptie

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



Digitale handtekeningen

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



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 kwantumcomputers
zouden dit wel efficiënt kunnen!**

Voorbeeld

RSA-250 (829 bits) gepubliceerd in 1991

214032465024074496126442307283933356300861
471514475501779775492088141802344714013664
334551909580467961099285187247091458768739
626192155736304745477052080511905649310668
769159001975940569345745223058932597669747
1681738069364894699871578494975937497937

=

641352894770715802787901901705773890848250
147429434472081168596320245323446302386235
98752668347708737661925585694639798853367

×

333720275949781565562260106053551142279407
603447675546667845209870238417292100370802
57448673296881877565718986258036932062711

**Werd in februari 2020 door klassieke
computers gefactoriseerd**

Algoritme van Shor (1994)

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

	Logische qubits	Fysieke qubits
<i>RSA-2048</i> (112 bit security)	4096	20 miljoen (8 uur, studie uit 2019)
<i>ECC-224</i> (112 bit security)	1300 tot 1600 (!)	?

RSA-2048 (2048 bits)

251959084756578934940271832400483985
 714292821262040320277771378360436620
 207075955562640185258807844069182906
 412495150821892985591491761845028084
 891200728449926873928072877767359714
 183472702618963750149718246911650776
 133798590957000973304597488084284017
 974291006424586918171951187461215151
 726546322822168699875491824224336372
 590851418654620435767984233871847744
 479207399342365848238242811981638150
 106748104516603773060562016196762561
 338441436038339044149526344321901146
 575444541784240209246165157233507787
 077498171257724679629263863563732899
 121548314381678998850404453640235273
 819513786365643912120103971228221207
 20357

**Grootste RSA getal gefactoriseerd door
klassieke computer**

RSA-250 (829 bits)

214032465024074496126442307283933356
300861471514475501779775492088141802
344714013664334551909580467961099285
187247091458768739626192155736304745
477052080511905649310668769159001975
940569345745223058932597669747168173
8069364894699871578494975937497937

(in 2020, 2700 core-years)

**Grootste RSA getal gefactoriseerd
met algoritme Shor door kwantumcomputer...**

21

(in 2012)

RSA-2048 (2048 bits)

251959084756578934940271832400483985
714292821262040320277771378360436620
207075955562640185258807844069182906
412495150821892985591491761845028084
891200728449926873928072877767359714
183472702618963750149718246911650776
133798590957000973304597488084284017
974291006424586918171951187461215151
726546322822168699875491824224336372
590851418654620435767984233871847744
479207399342365848238242811981638150
106748104516603773060562016196762561
338441436038339044149526344321901146
575444541784240209246165157233507787
077498171257724679629263863563732899
121548314381678998850404453640235273
819513786365643912120103971228221207
20357

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



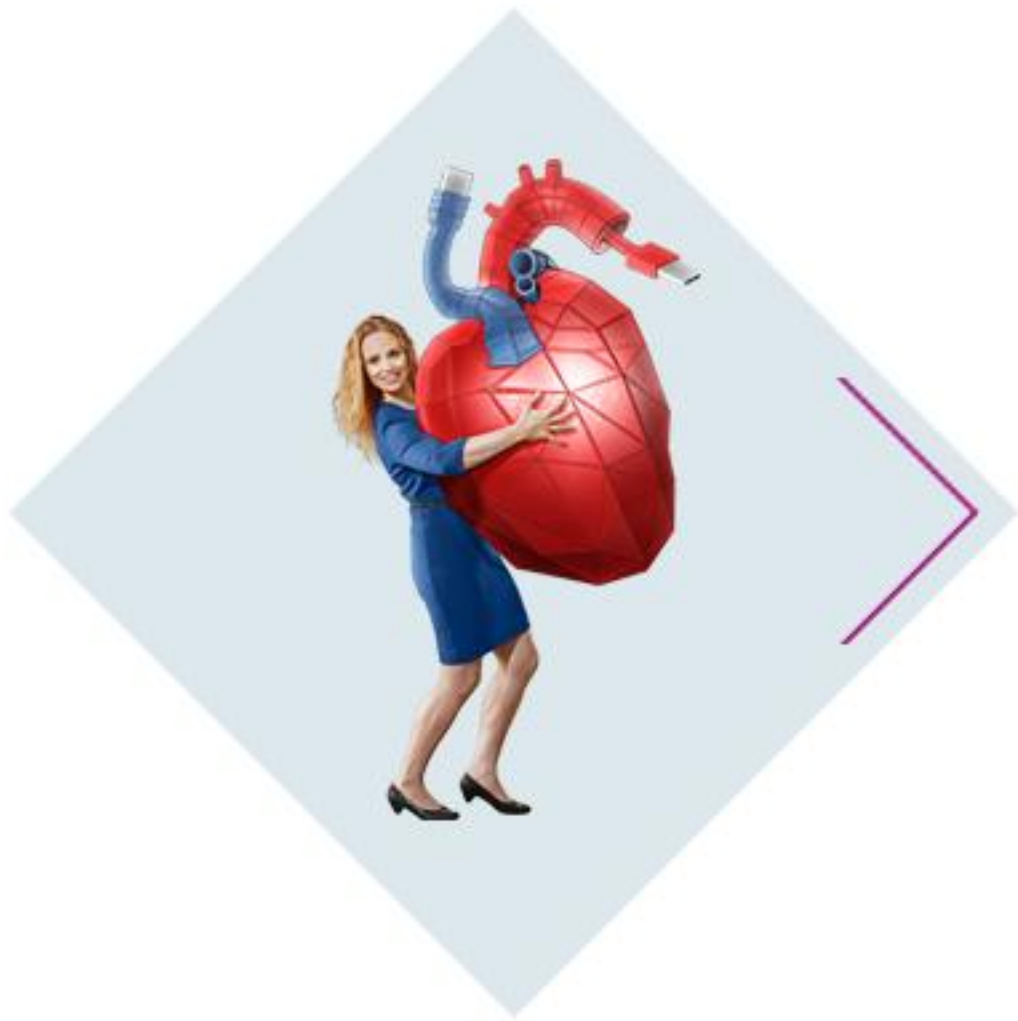
Krachtige kwantumcomputers met miljoenen fysieke qubits vormen een bedreiging voor publieke sleutelcryptografie

(Maar daar zijn we nog lang niet)

Impact kwantumcomputers op moderne cryptografie

	Symmetrische cryptografie	Cryptografische hashfuncties	Publieke sleutelcryptografie
Kwantumdreiging	Algoritme van Grover	Algoritme van Grover	Algoritme van Shor
Aantal Qubits	Enkele duizenden logische = enkele miljoenen fysieke qubits		
What if?	Sleutellengte x 2	Uitvoerlengte x 1,5	Kwantumresistente alternatieven
Impact efficiëntie	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

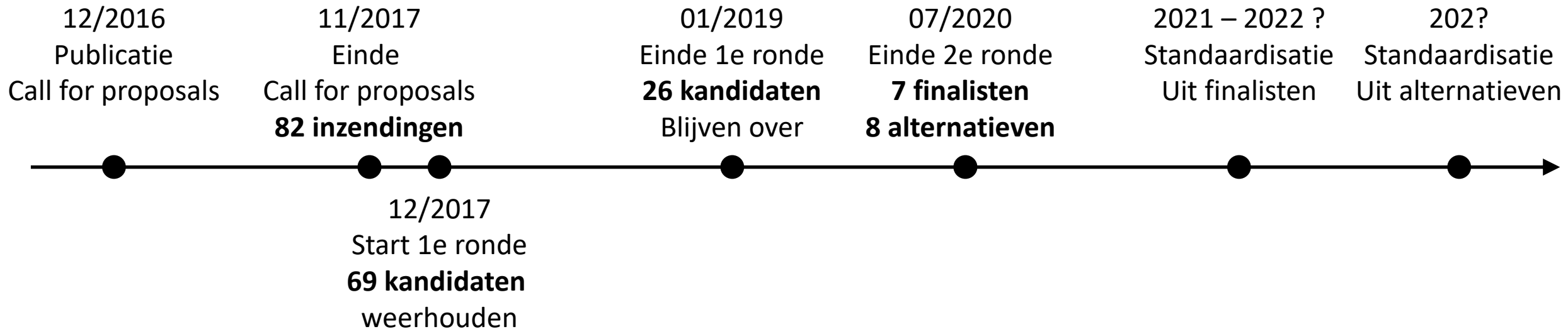
◆ De crypto-apocalypse?

◆ **Kwantumresistente cryptografie**

◆ Conclusies

Twée luiken

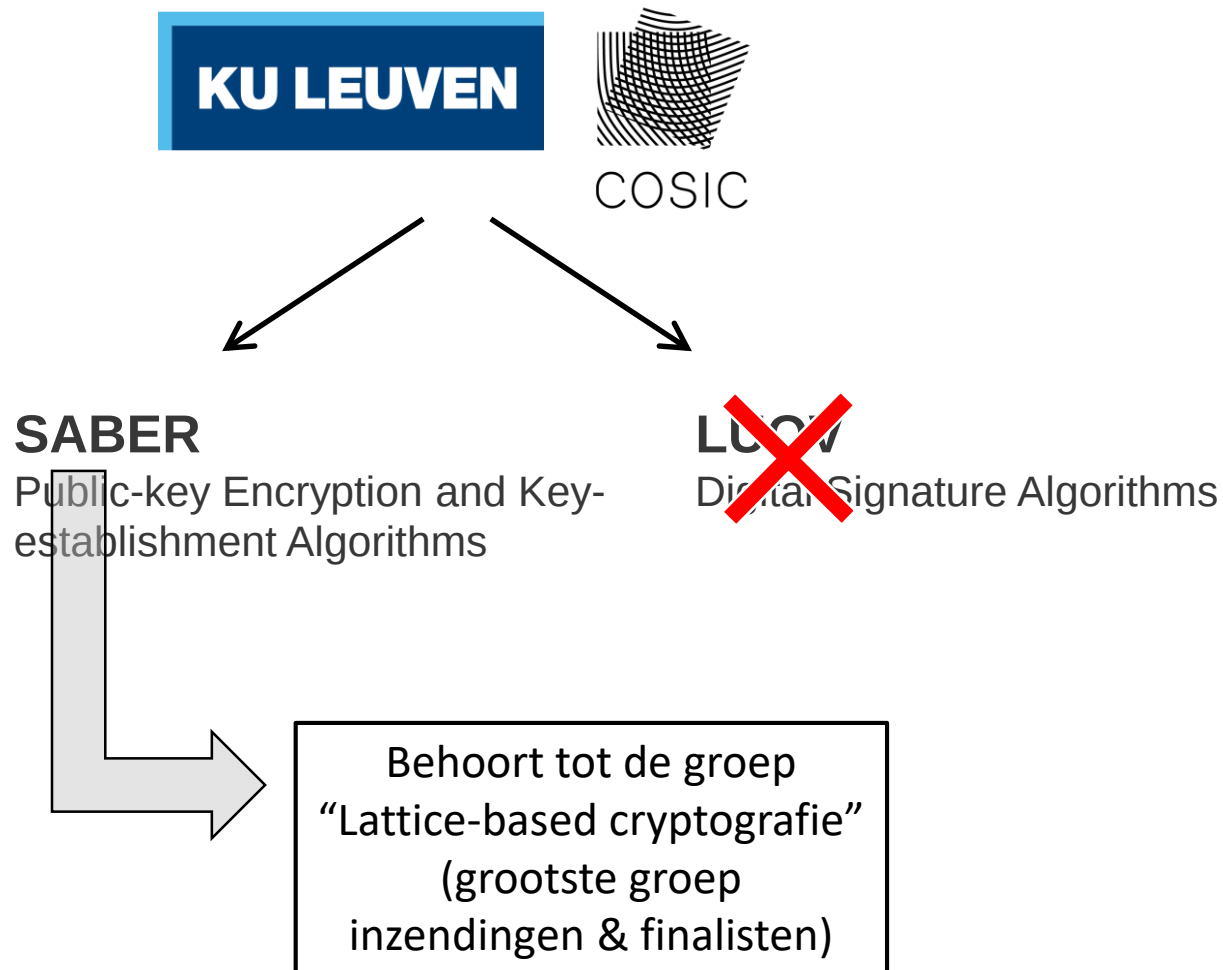
- Public-key Encryption and Key-establishment Algorithms
- Digital Signature Algorithms



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



TESTIMONIALS

All you need is LUOV.

- J. Lennon

LUOV is the only force capable of transforming an enemy into a friend.

- Martin Luther King Jr.

There is nothing better or more necessary than LUOV.

- Saint John of The Cross

I would do anything for LUOV.

- Meat Loaf

Do not pity the dead, Harry. Pity those who live without LUOV.

- Albus Dumbeldore.

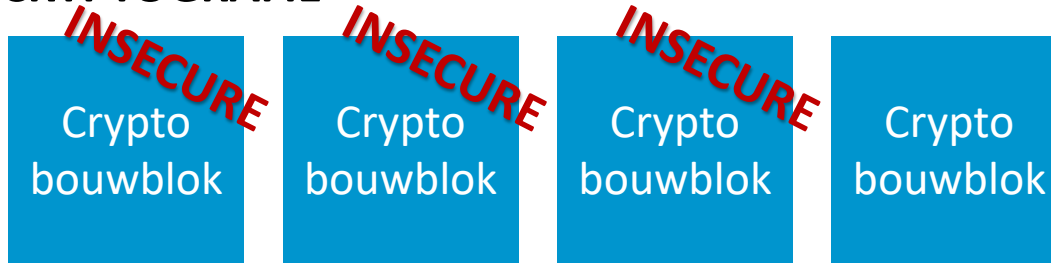
NIST

“Parameter sets of LUOV were significantly affected [by this type of attack]”

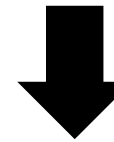
“Too new to be incorporated into a standard”

HEDENDAAGSE CRYPTOGRAFIE

Mogelijkheden:

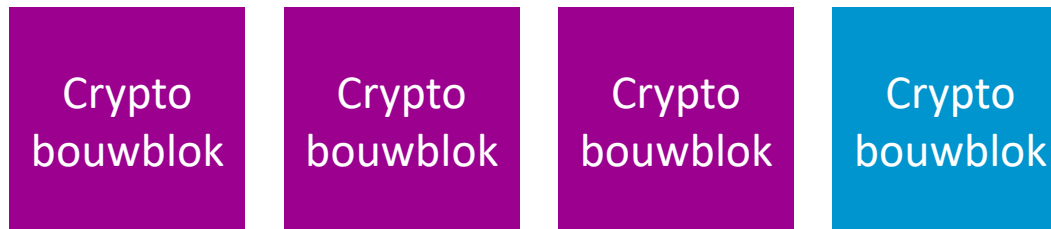


Fundamenten:



KWANTUMRESISTENTE CRYPTOGRAFIE

Mogelijkheden:



Fundamenten:



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
- ❖ Kans dat vreemde mogendheid op termijn over kwantumcomputer beschikt, wordt ernstig genomen

2020

- ❖ 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.”

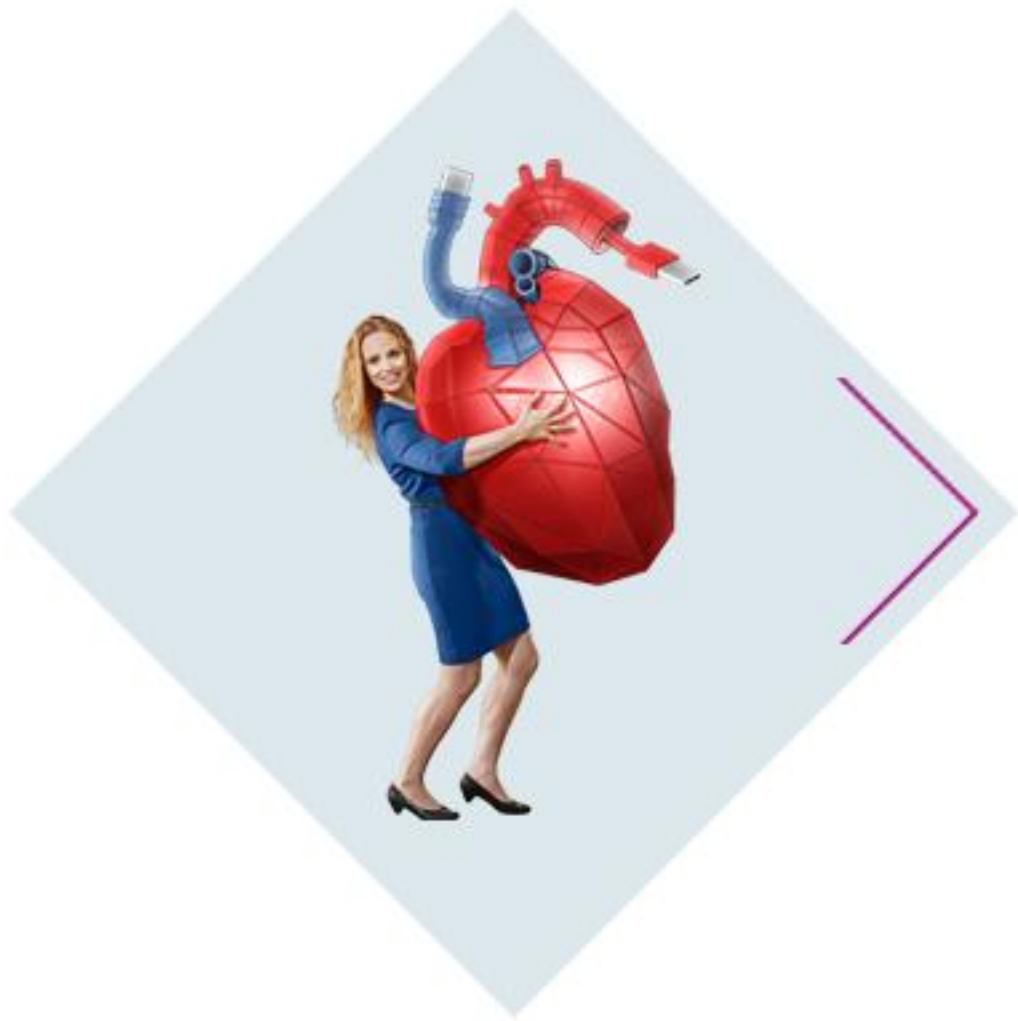
IAD, defensieve tak NSA, 2015

Migratie

- ❖ NIST standaardisatieprocedure loopt
- ❖ Wacht standaardisatieprocedure af
- ❖ Daarna ev. geleidelijk migreren
- ❖ Urgentie hangt af van risicoinschatting

Crypto agility

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



Agenda

◆ Kwantum- Vs. klassieke computer

◆ Kwantumcomputers (niet) in de praktijk

◆ De crypto-apocalypse?

◆ Kwantumresistente cryptografie

◆ **Conclusies**

Conclusie

Kwantumcomputers steunen op principes uit kwantumfysica (verstrengeling & superpositie)

Bouw kwantumcomputers gigantisch complex (Isolatie, foutencorrectie, schaalbaarheid, topologie)
Nog in kinderschoenen

Langere symmetrische sleutels en hash uitvoer
Een paar miljoen fysieke qubits vereist om publieke sleutelcryptoografie te kraken → Alternatieven nodig

De NIST standaardisatieprocedure loopt

Agenda

◆ Kwantum- Vs. klassieke computer

◆ Kwantumcomputers (niet) in de praktijk

◆ De crypto-apocalypse?

◆ Kwantumresistente cryptografie

Kristof Verslype

Cryptographer, PhD

Smals Research



✉ kristof.verslype@smals.be

☎ +32(0)2 7875376

🌐 www.smals.be
www.smalsresearch.be
www.cryptov.net (personal)



PRIMEUR

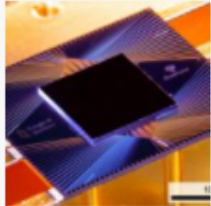
Rapport “Kwantumcomputers & Cryptografie”



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

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 de bouw van kwantumcomputers?", "Hoe moeilijk is ... [Continue reading](#) →

Posted in [Security](#) | Tagged [cryptography](#), [physics](#), [quantum computing](#) | [1 Reply](#)

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](#)

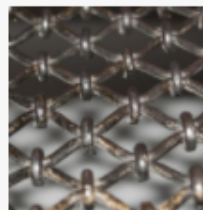


Welke impact zullen kwantumcomputers hebben op onze moderne cryptografie, die levensnoodzakelijk is in onze samenleving? Deze blogpost bespreekt de impact op symmetrische encryptie, op cryptografische hashfuncties en op publieke sleutelcryptografie. Impact op symmetrische encryptie Bij symmetrische encryptie gebeurt encryptie en ... [Continue reading](#) →

Posted in [Security](#) | Tagged [cryptography](#), [quantum computing](#), [Security](#) | [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](#)

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*. IEEE 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/>

- 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>