
POST
QUANTUM OF SOLACE
007
12A

HYPER HYPER

HYPER HYPER

Quantum Computing Hype Cycle Just Getting Started

Quantum computing could be to the 2020s what cloud computing was to the 2010s

By Dana Blankenhorn, InvestorPlace Contributor Jul 25, 2018, 1:24 pm EST

Quantum computing is not a cure-all for business computing challenges

Quantum Computing Under Hype Cycle and Market Clock Scrutiny

With new technology come the pleuaits and the critics. Quantum computing is no different from any other sector

By James Dargan - August 1, 2019

The hype around quantum computing: it's not too early to get in

by Jurgita Lapienytė © 15 February 2021

UNIVERSITY OF TWENTE.

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*


QUANTUMSUPREMACY
10.23.19

HYPE ➡️ DRUK ➡️ VERGISSINGEN

HYPE ➡️ DRUK ➡️ VERGISSINGEN

NOS Nieuws • Maandag 8 maart 2021, 17:00 •
Aangepast maandag 8 maart 2021, 22:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden

HYPE ➡️ DRUK ➡️ VERGISSINGEN

NOS Nieuws • Maandag 8 maart 2021, 17:00 •
Aangepast maandag 8 maart 2021, 22:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden

SCIENCE

17 maart 2022 - 11:05 door Jos Vlassink

Kouwenhoven departs, Microsoft presents Majoranas

In a strange combination of events, Microsoft announced both the departure of Leo Kouwenhoven this week and the discovery of scalable Majoranas – developed in Denmark.

UNIVERSITY OF TWENTE.

HYPE ➡️ DRUK ➡️ VERGISSINGEN

NOS Nieuws • Maandag 8 maart 2021, 17:00 •
Aangepast maandag 8 maart 2021, 22:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden

SCIENCE

17 maart 2022 - 11:05 door Jos Vlassink

Kouwenhoven departs, Microsoft presents Majoranas

In a strange combination of events, Microsoft announced both the departure of Leo Kouwenhoven this week and the discovery of scalable Majoranas – developed in Denmark.

Delftse onderzoekers kwantumcomputers 'verwijtbaar onzorgvuldig'

Geen schending wetenschappelijke integriteit.

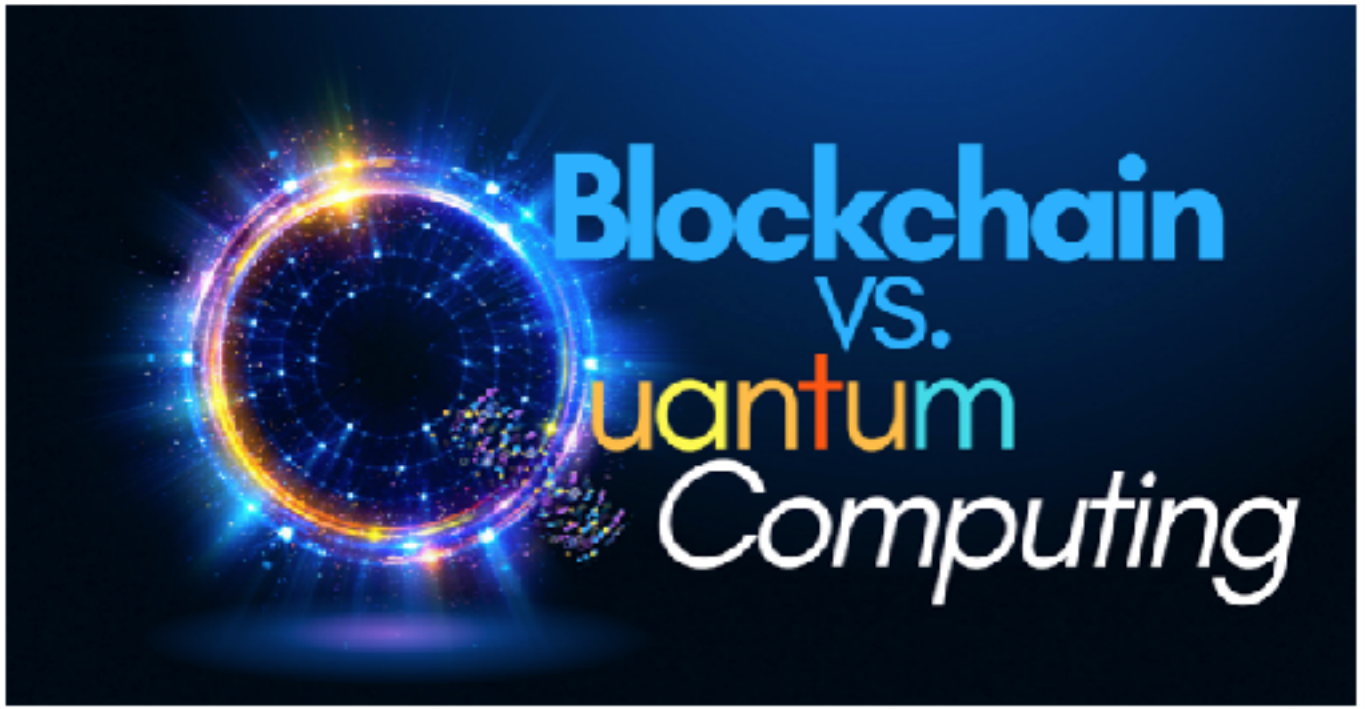
Het College van Bestuur van de TU Delft oordeelt dat Leo Kouwenhoven en Hao Zhang 'onzorgvuldig' hebben gehandeld en dat er deels ook sprake is van 'verwijtbare onzorgvuldigheid' bij de publicatie van hun werk over Majoranadeeltjes. Deze deeltjes zijn veelbelovend als basis voor een stabiele kwantumcomputer.

NOU, NOG EENTJE DAN...

Quantum Computing: Is it the end of blockchain?

June 3rd 2018

TWEET THIS



Is this the end of blockchain?

UNIVERSITY OF TWENTE.

NOU, NOG EENTJE DAN...

Quantum Computing: Is it t
blockchain?

June 3rd 2018

Is this the end of blockchain?

SPOILER: JA!

DE HYPE HELPT NIET

- **Tech sites** staan **vol** artikelen **over quantumdoorbraken**
- Wekt de indruk dat een **quantum computer “om de hoek staat”**
- En dat dit de wereld **voor goed gaat veranderen** (dat klopt!)
- Een paar **snelle feiten**:
  - Voor **praktische quantum computers** zijn **duizenden** *logische qubits* nodig, die weer uit **tienduizenden** *fysieke qubits* bestaan
  - Google’s **quantum supremacy machine had 53 fysiek qubits** — hoe “supreme” is dat nou helemaal?

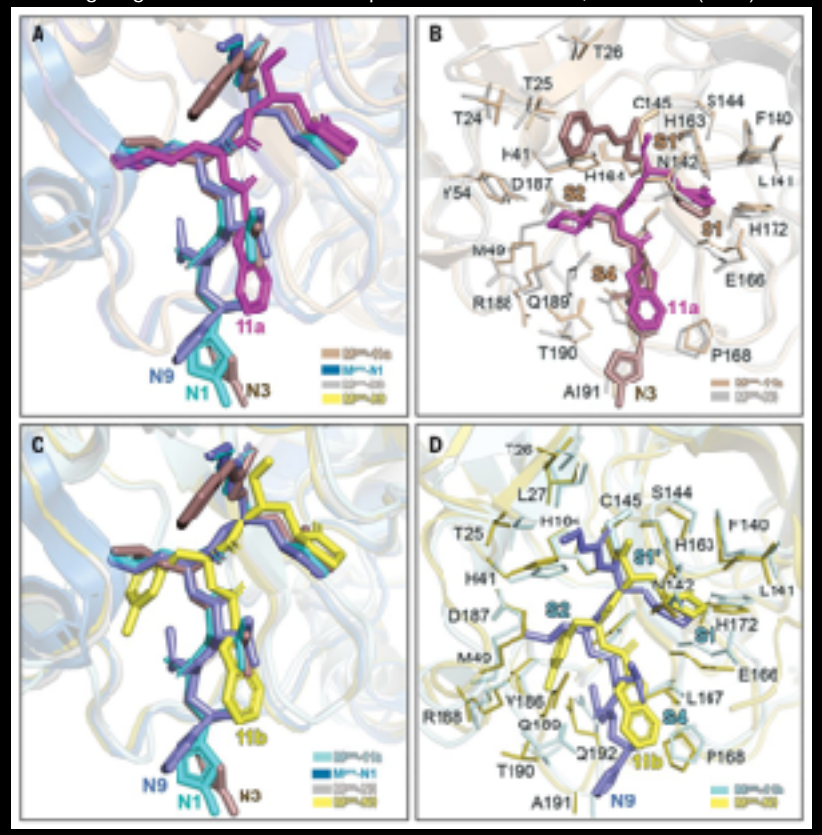
DE HYPE HELPT NIET

- **Tech** **n**
- Wekt **ek staat”**
- En da opt!)
- Een p
  - Vo *logische qu bits* bestaan
  - G **ek qubits** — hoe “supreme” is dat nou helemaal?

Doel van deze lezing:
Door de hype ballon heenprikken en uitleggen *waarom we ons* **nu** *zorgen moeten maken* en wat we *nu, of in de nabije toekomst* moeten doen

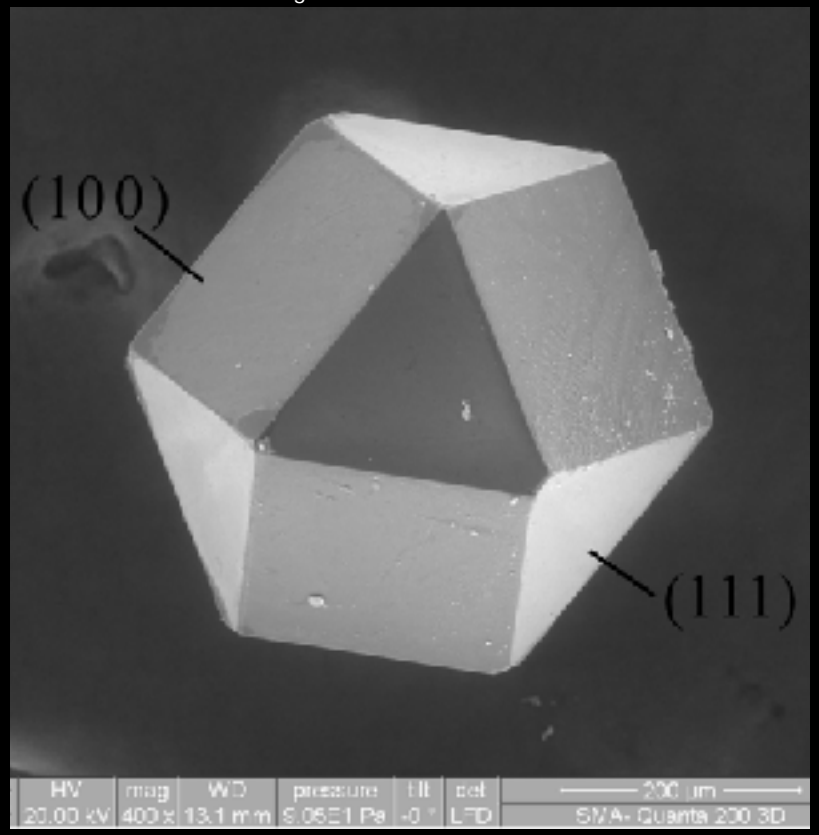
Eerst even de belofte van quantumcomputers

Wenhao Dai et al. ‚Structure-based design of antiviral drug candidates targeting the SARS-CoV-2 main protease. Science 368, 1331-1335(2020).



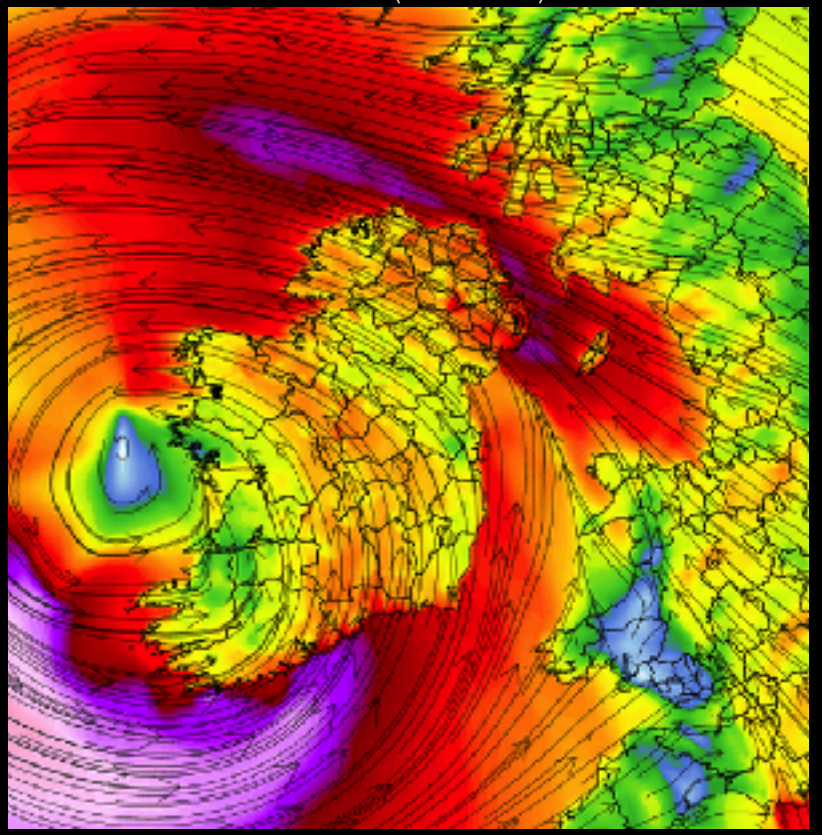
Medicijnontwikkeling

© Ludvig14 / Wikimedia / CC BY-SA 3.0



Materiaalkunde

Storm Barra (source: Twitter)

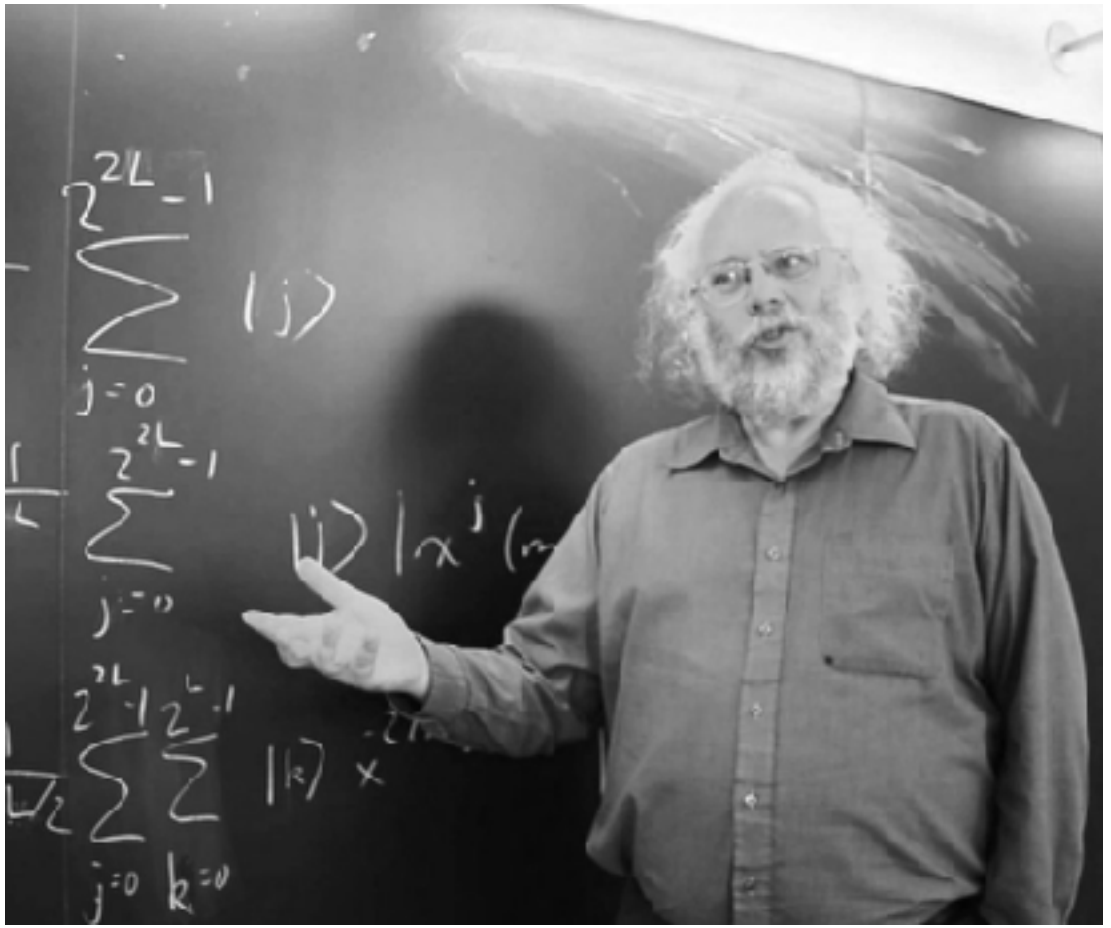


Weermodellen

WAAROM WE WÉL BEZORGD ZIJN

Lov Grover

(image: dotquantum.io)



Peter Shor

(image: dotquantum.io)

UNIVERSITY OF TWENTE.

GROVER'S ALGORITME

Lov Grover

(image: dotquantum.io)

- **Verbetert ongeordend zoeken** op onvoorspelbare functies
- **Reduceert** het aantal pogingen **van N naar √N**
- Heeft **consequenties voor** zogenaamde **symmetrische cryptografie**
- **Reduceert de kracht van bijvoorbeeld AES**-128 tot 64 bits security (problematisch!)

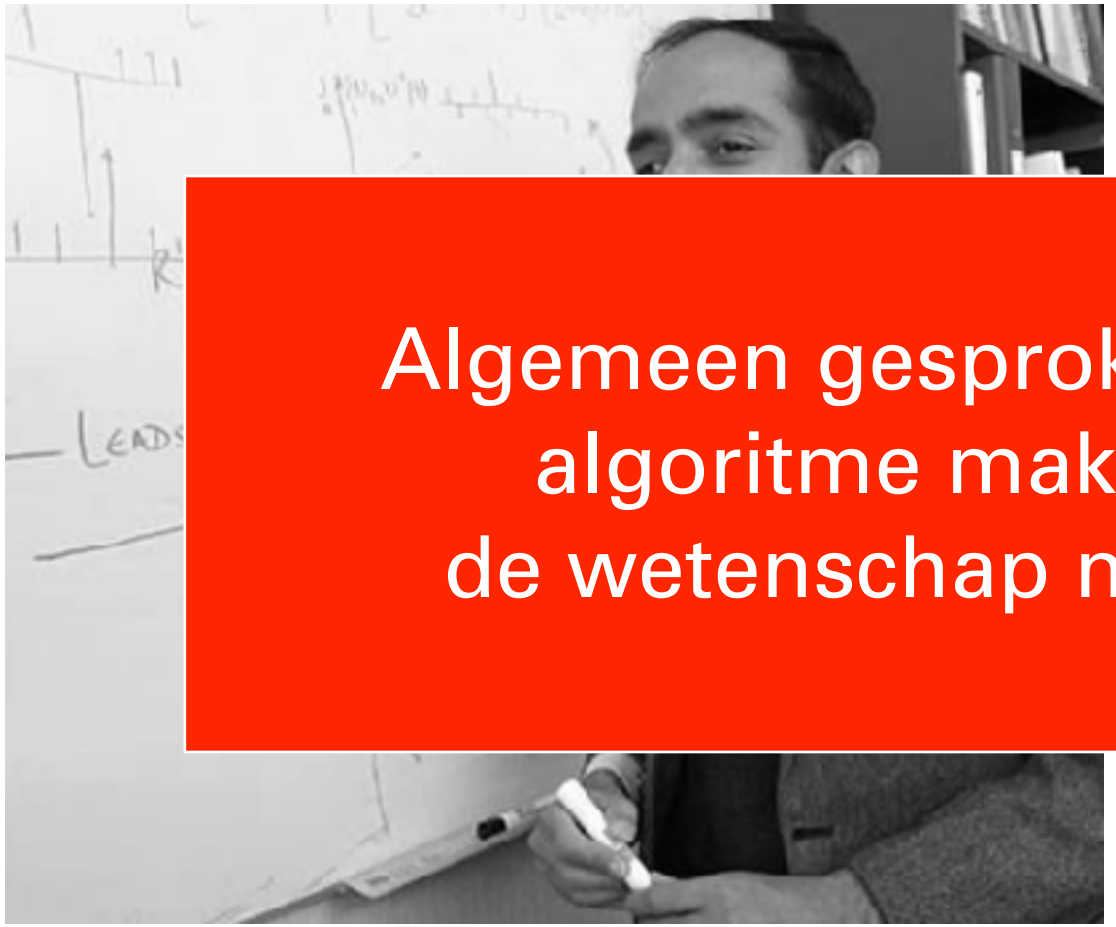
GROVER'S ALGORITME: IMPACT

Lov Grover

(image: dotquantum.io)

- **Symmetrische cryptografie gebruiken we op veel plekken:** versleutelde communicatie, tweede factor authenticatie, diskversleuteling, …
- **Wat** moeten we **doen?**
- **Geen paniek**, gewoon de **sleutels twee keer zo groot maken**
- **AES-256** in plaats van AES-128

GROVER'S ALGORITME: IMPACT



Lov Grover

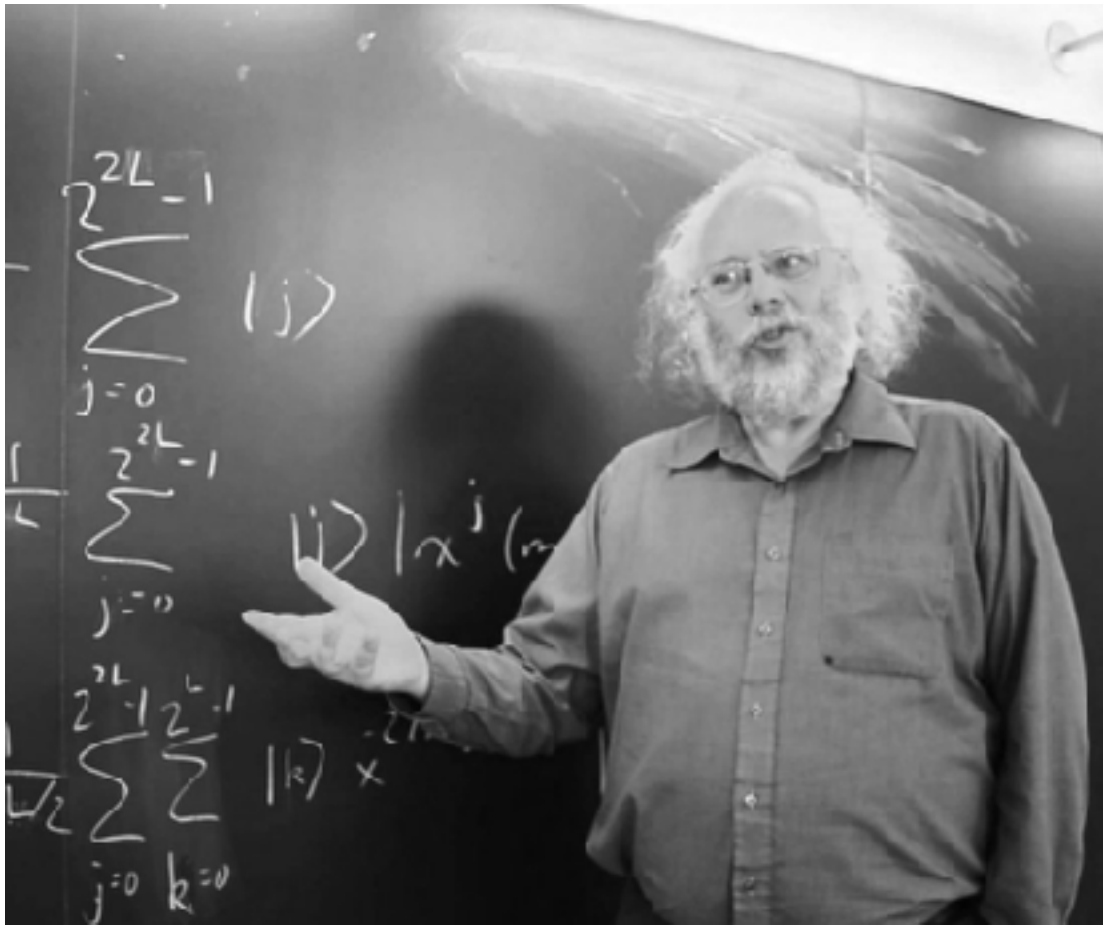
(image: dotquantum.io)

- **Symmetrische cryptografie gebruiken we op veel plekken:**
  - tie,
  - tie,
  - e
  - **oot**
  - **maken**
- **AES-256** in plaats van AES-128

Algemeen gesproken: om Grover's algoritme maken we ons in de wetenschap niet echt zorgen

SHOR'S ALGORITME

- **Verkleint de inspanning voor het ontbinden in factoren van priemgetallen** (en het zgn. discrete logaritmeprobleem) **zeer significant**
- **Dit is een groot probleem!** Het **bedreigt** alle bekende public key cryptografie (**de basis van een veilig internet**)

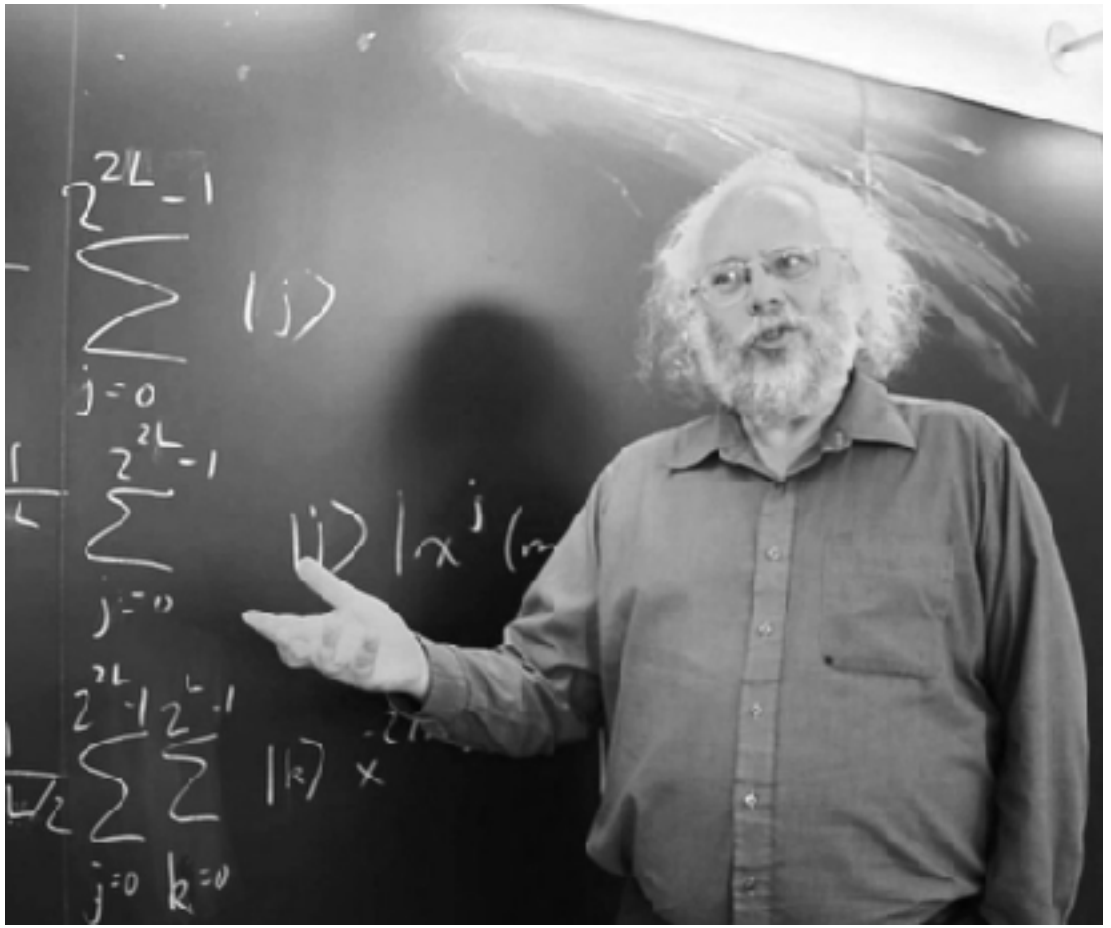


Peter Shor

(image: dotquantum.io)

SHOR'S ALGORITME: IMPACT

- **Public key cryptografie** wordt **breed gebruikt**: voor alle veilige websites, voor wettig geldige digitale handtekeningen (**UZI pas!**), …
- Een **krachtige quantum computer** zou **enorme problemen voor het internet** opleveren!



Peter Shor

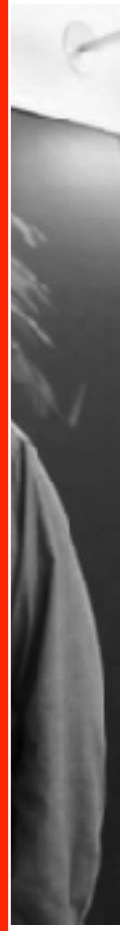
(image: dotquantum.io)

SHOR'S ALGORITME: IMPACT

- Vanuit gebruikersperspectief gaan we **van dit:**

- **naar dit:**

Voor het **hele internet!**



(image: dotquantum.io)

SHOR'S ALGORITME: IMPACT

- **Public key cryptografie** wordt
- opleveren!

Vanwege Shor's algoritme moeten we in de toekomst - en in sommige gevallen **nu** - actie ondernemen

Peter Shor

(image: dotquantum.io)

WANNEER WORDT SHOR EEN PROBLEEM?

Public Key System	Key Size	Security	Logical qubits	Physical qubits	Running time
RSA	1024 bits	80 bits	2,050	8.05×10^6	4 hours
	2048 bits	**112 bits**	**4,098**	**8.56×10^6**	**29 hours**
	4096 bits	128 bits	8,194	1.12×10^7	~10 days
ECC	**256 bits**	**128 bits**	**2,330**	**8.56×10^6**	**11 hours**
	384 bits	192 bits	3,484	9.05×10^6	38 hours
	512 bits	256 bits	4,719	1.13×10^7	~2 days

Source: Grumbling, E. and Horowitz, M. (eds.), "Quantum Computing: Progress and Prospects", National Academy of Sciences, 2019

IBM unveils its 433 qubit Osprey quantum computer

Frederic Lardinois @frederic 3:00 PM GMT+1 • November 9, 2022

Comment

Image Credits: Amardeep Singh / 500px / Getty Images

IBM unveils its 433 qubit Osprey quantum computer

Frederic Lardinois @frederic | 3:00 PM GMT+1 • November 9, 2022 | Comment

Image Credits: Amardeep Singh / 500px / Getty Images

WANNEER WORDT SHOR EEN PROBLEEM?

Public Key System	Key Size	Security	Logical qubits	Physical qubits	Running time
RSA	1024 bits	80 bits	2,050	8.05×10^6	4 hours
	2048 bits	**112 bits**	**4,098**	**8.56×10^6**	**29 hours**
	4096 bits	128 bits	8,194	1.12×10^7	~10 days
ECC	**256 bits**	**128 bits**	**2,330**	**8.56×10^6**	**11 hours**
	384 bits	192 bits	3,484	9.05×10^6	38 hours
	512 bits	256 bits	4,719	1.13×10^7	~2 days

Source: Grumbling, E. and Horowitz, M. (eds.), "Quantum Computing: Progress and Prospects", National Academy of Sciences, 2019

WANNEER WORDT SHOR EEN PROBLEEM?

De meestgebruikte algoritmes kunnen in een **kwestie van uren** gekraakt worden…

Maar het aantal qubits wat daarvoor nodig is ligt **bij lange na niet binnen het bereik van de huidige prototype quantumcomputers**

Betekent dat dat we veilig zijn?

Source: Grumbling, E. and Horowitz, M. (eds.), "Quantum Computing: Progress and Prospects", National Academy of Sciences, 2019

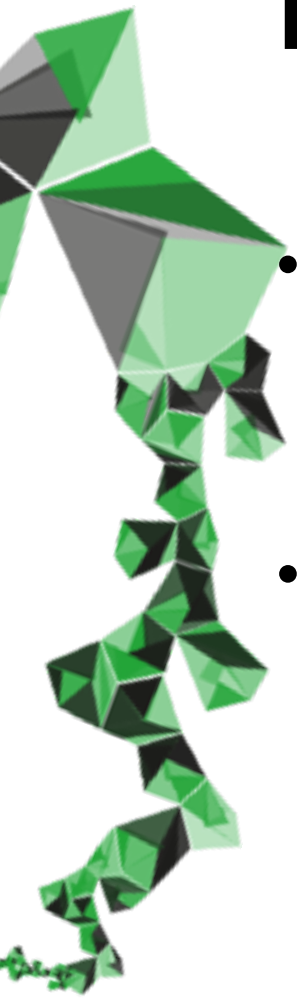
LEVENSDUUR VAN DATA

- Of we **veilig** zijn **hangt af van hoe lang** data wordt bewaard en gebruikt

- Vuistregel:
  - **Kortdurend gebruik: geen zorgen** en **geen** reden om nu in **actie** te komen
  - **Lange bewaartermijn:** er is **nu** al **actie nodig!**

Photo by Abdul A on Unsplash

LEVENSDUUR VAN DATA



- (
- (
- V

Vraag voor jullie: wat is volgens jullie kortdurend gebruik en wat een langdurige bewaartermijn?

Waar zit de pijn in het zorgdomein?

- **Lange bewaartermijn:** er is **nu** al **actie nodig!**

Photo by Abdul A on Unsplash

VOORBEELDEN

- **Kortdurend gebruik:**
  (Two-factor) authenticatie, kort gebruikte digitale handtekeningen (bv. websitecertificaten), online authenticatie protocollen zoals OpenID connect, SAML, … (denk: **DigiD**); **in essentie alles waarbij het resultaat van een cryptografisch algoritme snel niet meer relevant is**

- **Langdurig gebruik:**
  Versleutelde archieven (**EPD?**), wettig geldige digitale handtekeningen, tijdelijke sleutels bij het opzetten van een veilige verbinding, …; in essentie **alles waarbij het resultaat van een cryptografisch algoritme tientallen jaren veilig moet blijven**

VOORBEELDEN

- **Kortdurend gebruik:**
  (Two-factor) auth handtekeningen (bv. websitecertificat ollen zoals OpenID connect, SAML, **les waarbij het resultaat van een cryptogr r relevant is**

Weet iemand waarom deze in de lijst staat?

- **Langdurig gebru k:**
  Versleutelde arch ieven (**EPD?**), wettig geldige digitale handtekeningen, tijdelijke sleutels bij het opzetten van een veilige verbinding, …; in essentie **alles waarbij het resultaat van een cryptografisch algoritme tientallen jaren veilig moet blijven**

HERINNEREN JULLIE JE DEZE NOG?

+

HERINNEREN JULLIE JE DEZE NOG?

Langdurige opslag van gegevens kan ook *zonder toestemming* gebeuren!

UNIVERSITY OF TWENTE.

POST QUANTUM CRYPTOGRAFIE

- Cryptografen werken aan **nieuwe public key algoritmen die "quantumveilig" zijn**
- Dat betekent dat ze **veilig** blijven, **zelfs als er een krachtige quantumcomputer komt**
- Deze algoritmen zijn er van **rijp tot groen**

post- /pɔst/ *voorvoegsel*, betekent "achter", "nadat", "later", "volgend op", van origine uit leenwoorden uit het Latijn *(postscript),* nu echter vrij gebruikt bij de vorming van nieuwe samenstellingen *(postcovid; postacademisch)*.

RADICAAL ANDERS

- Bij sommige algoritmen kan **elke sleutel maar één keer gebruikt worden**
- Sommigen vereisen **significant meer rekenkracht** of **geheugenruimte**
- Algoritmen hebben vaak **veel grotere sleutels** en **veel grotere digitale handtekeningen**
- Dit heeft **gevolgen voor heel veel toepassingen!**

Photo by Varvara Grabova on Unsplash

RADICAAL ANDERS

- Bij sommige algoritmen kan **elke sleutel maar één keer gebruikt worden**
- Sommigen vereisen **significant meer rekenkracht** of **geheugenruimte**
- Algoritmen hebben vaak **veel grotere sleutels** en **veel grotere digitale handtekeningen**
- Dit heeft **gevolgen voor heel veel toepassingen!**

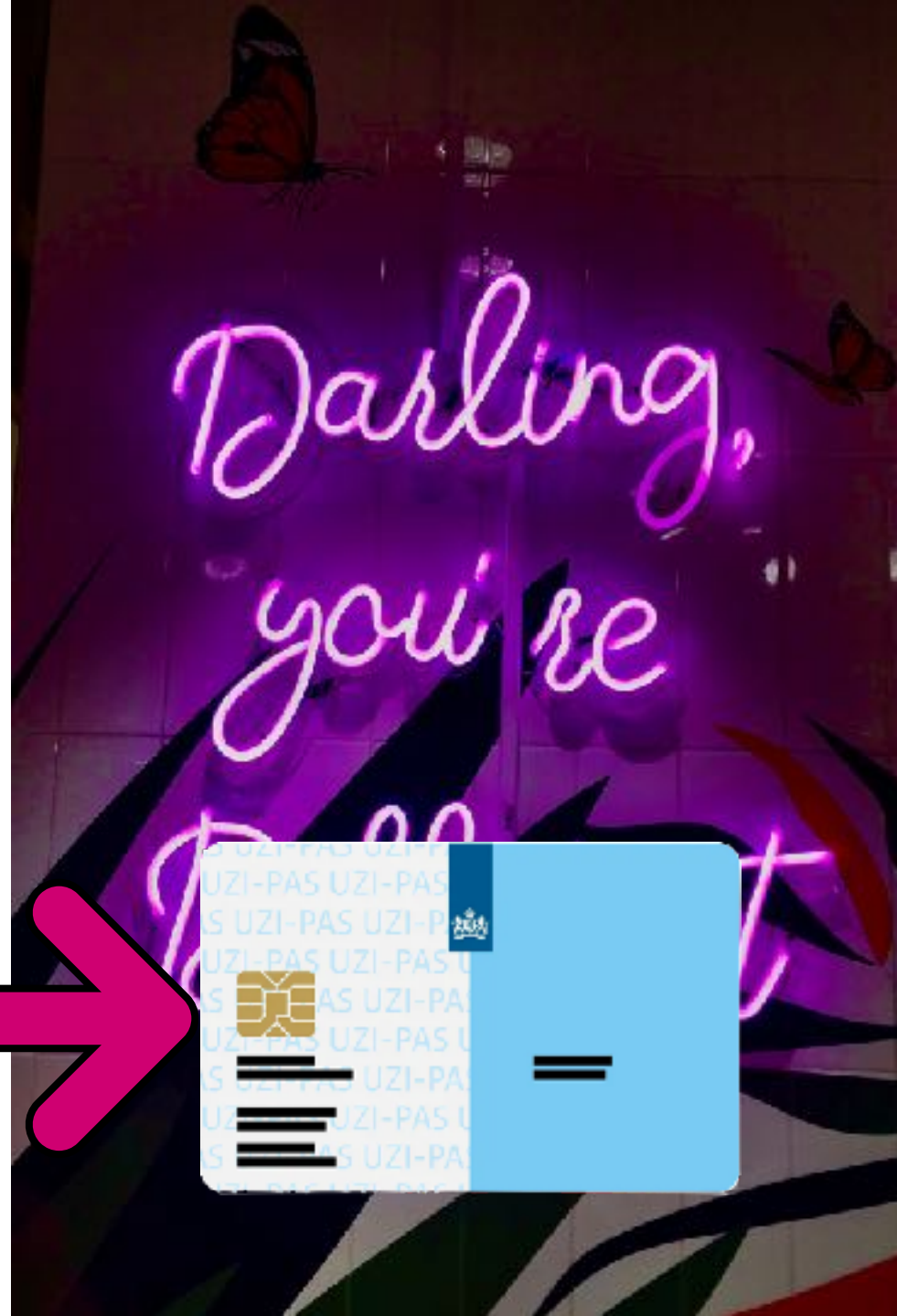


Photo by Varvara Grabova on Unsplash

NIST COMPETITIE

- “Wedstrijd” om de veilige **post quantum algoritmen** te kiezen **voor diverse toepassingen**
- Einddoel: **algoritmes** kiezen die **gestandaardiseerd** kunnen worden **voor algemeen gebruik**
- Huidige status: **eerste set algoritmes** zijn vorig jaar **geselecteerd voor standaardisatie**

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

NIST COMPETITIE

Belangrijk om te weten:

De focus van deze competitie lag tot nu toe op de meest urgente toepassingen (langetermijn opslag), de focus verschuift nu naar bredere toepassing, met name op het gebied van digitale handtekeningen

WANNEER, NIET OF

- Het is nu een **kwestie van wánneer**, en **niet óf** post quantum algoritmen uitgerold zullen worden
- De **standaarden komen eraan**, als die er zijn gaan **overheden** het **gebruik verplicht stellen in aanbestedingen**
- Dit **gaat** nog **jaren duren**, maar **raakt** in essentie **alle automatisering**

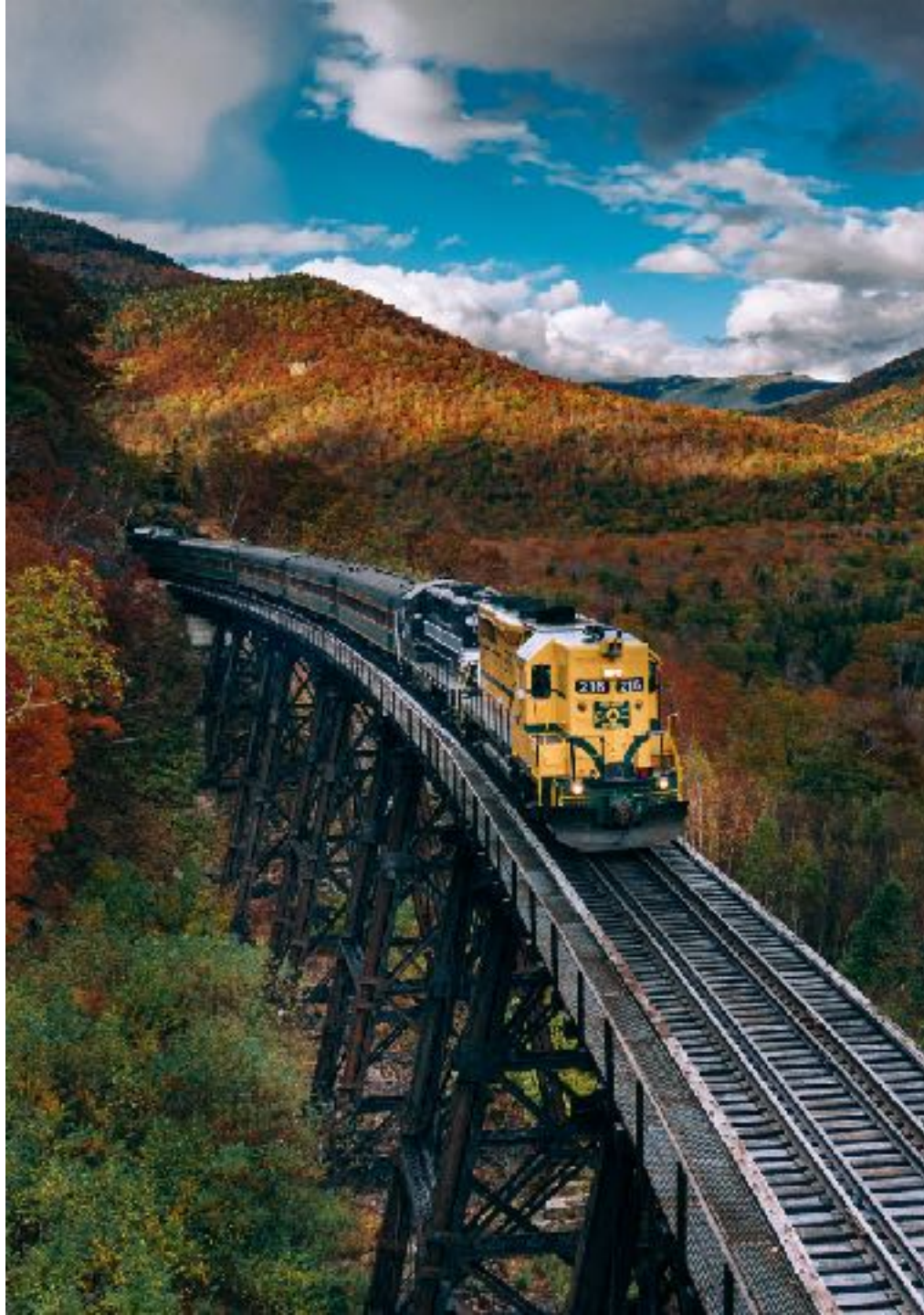


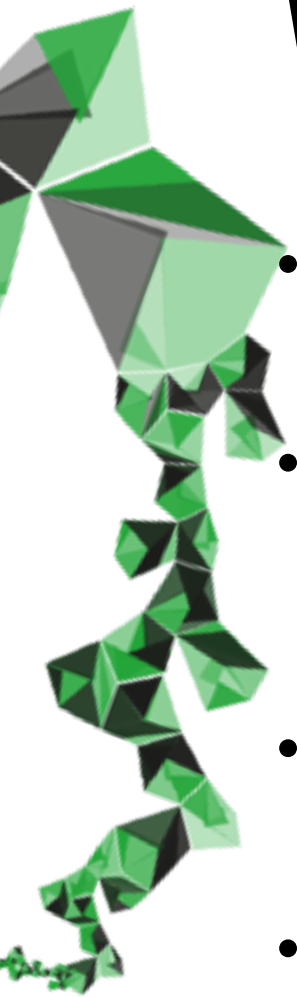
Photo by Martin Sanchez on Unsplash

HINDERNISSEN

- De **weg** naar de uitrol van post quantum is **vol hindernissen**
- **Algoritmen** zijn tot nu toe **vooral in webtoepassingen getest**
- Het **internet is** echter veel **meer dan** alleen **het wereldwijde web**
- De vraag voor 1 miljard euro: **hoe zetten we het hele internet over?**

Photo by John Salzarulo on Unsplash

WAT KOMT ER OP JULLIE AF?



- Kwestie van tijd voordat dit **informatiebeveiliging in de zorg** gaat raken (NEN 7510)
- Sterker nog: misschien moet de **zorg** wel **koploper** zijn; **elektronische patiëntendossiers** liggen maatschappelijk gevoelig (en worden lang opgeslagen!)
- Leun niet achterover, maar **ga bij leveranciers vragen wat hun plannen zijn** (**zodat ze in actie komen!**)
- **Let op de de overheid**; er is een overheidsbrede werkgroep rondom dit onderwerp aan de slag

DANK VOOR UW AANDACHT!

VRAGEN?

UNIVERSITY OF TWENTE.
DIGITAL SOCIETY INSTITUTE
FACULTY OF ELECTRICAL ENGINEERING, MATHEMATICS AND COMPUTER SCIENCE
DESIGN AND ANALYSIS OF COMMUNICATION SYSTEMS