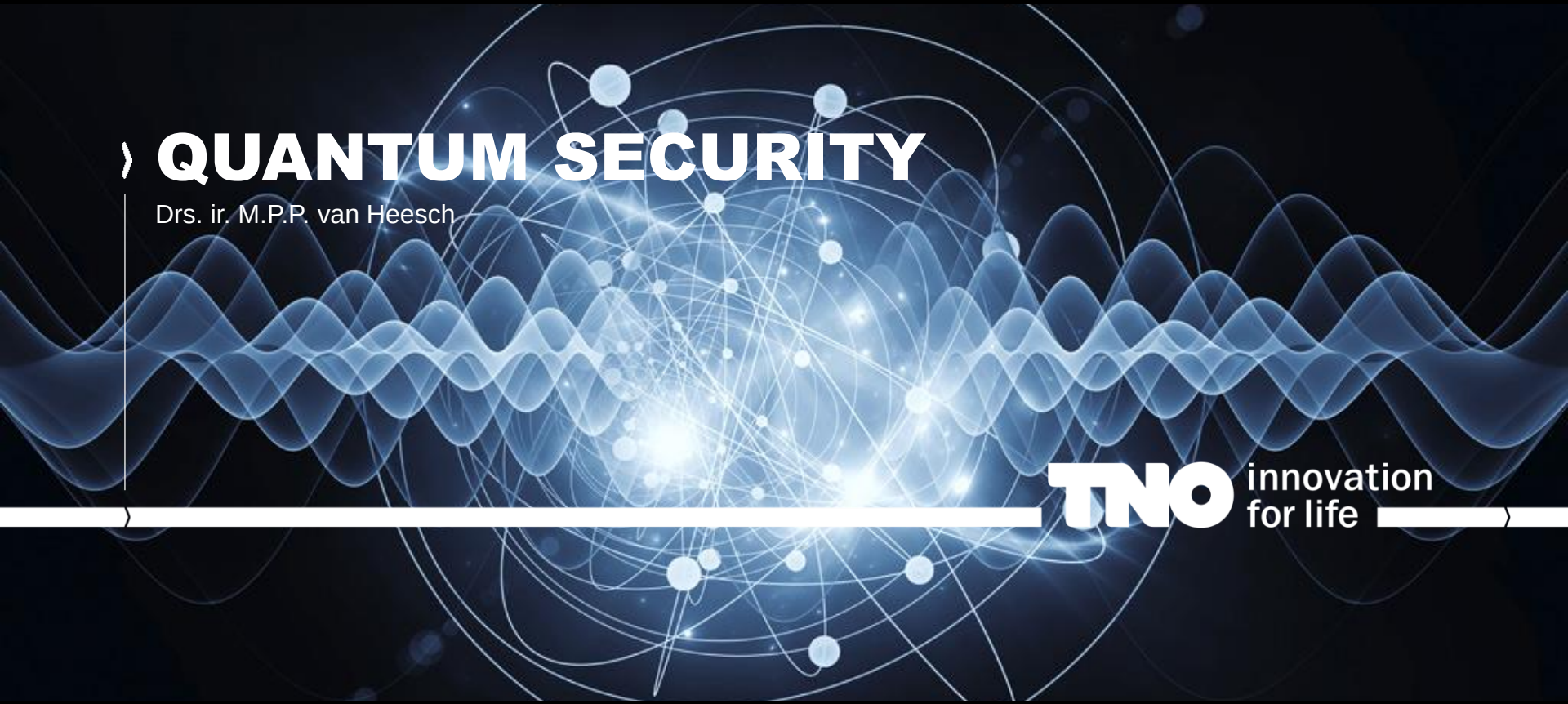
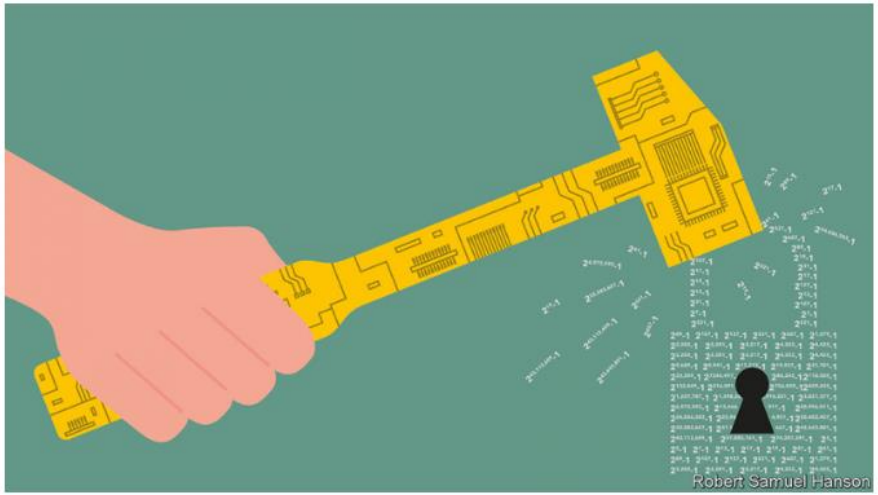

QUANTUM SECURITY
Drs. ir. M.P.P. van Heesch
TNO innovation for life

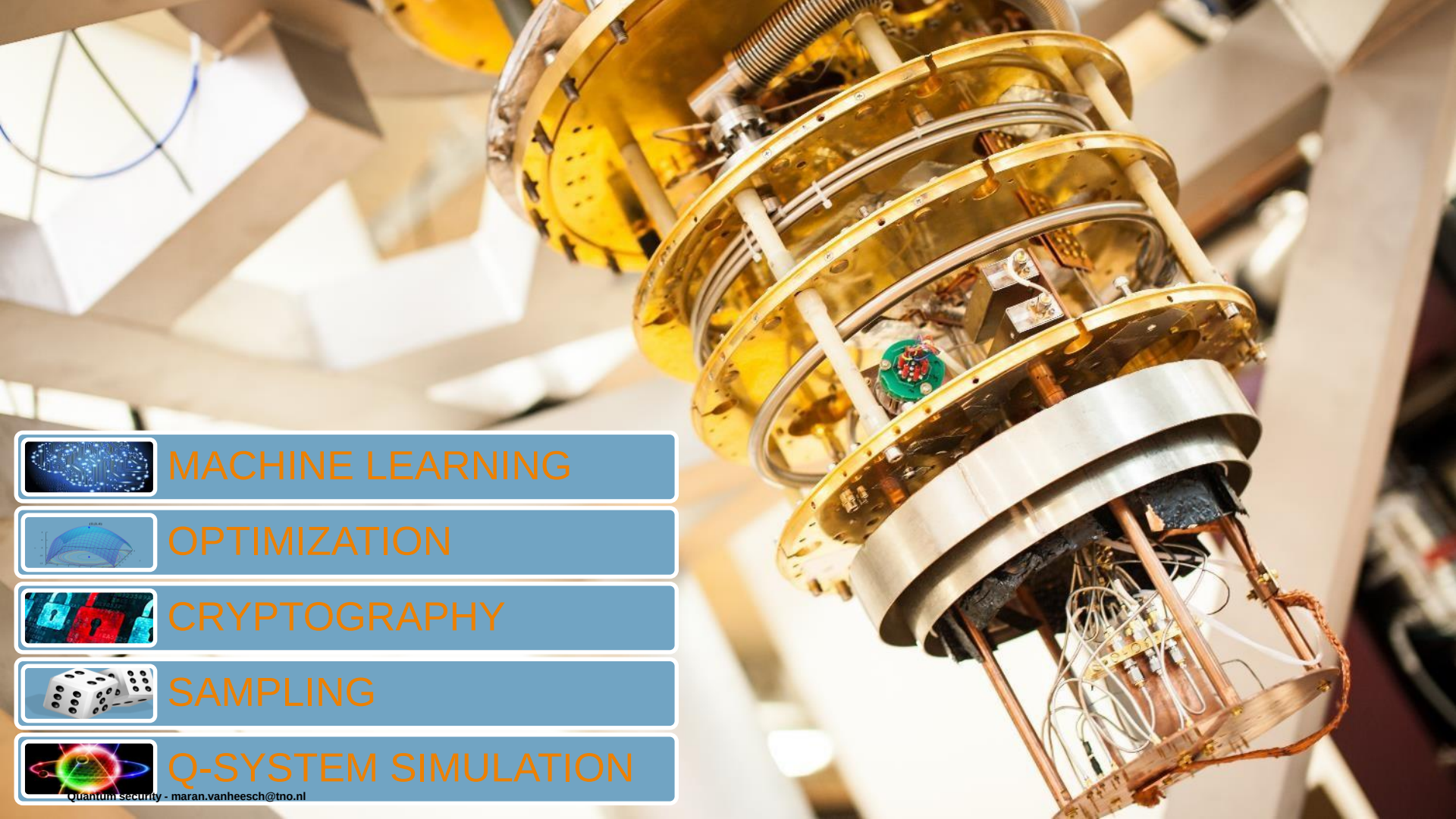
Future-proofing the internet

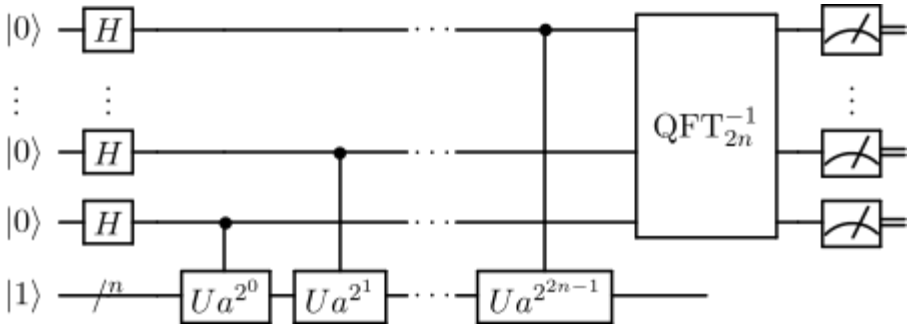
Quantum computers will break the encryption that protects the internet

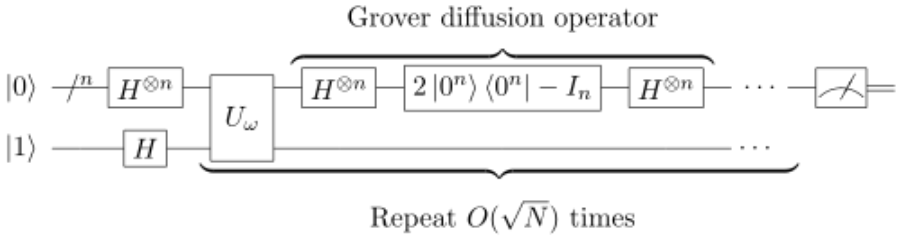
Fixing things will be tricky



Print edition | Science and technology ›
Oct 20th 2018


MACHINE LEARNING
OPTIMIZATION
CRYPTOGRAPHY
SAMPLING
Q-SYSTEM SIMULATION

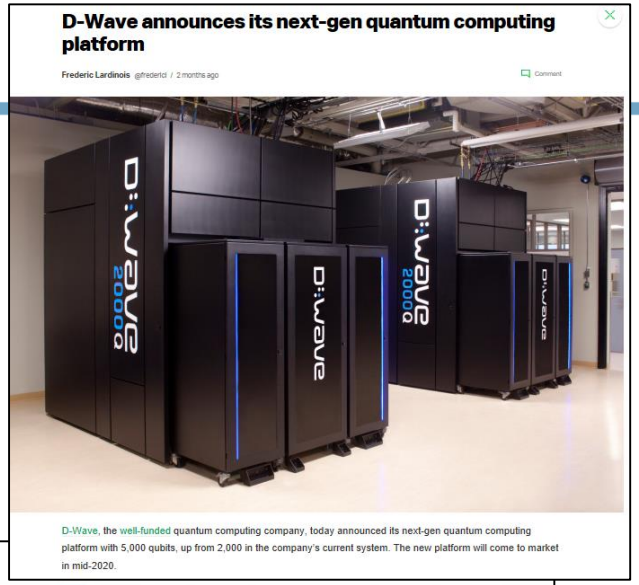




Broken:
RSA
ECC
DH

Weakend:
AES

2000 qubits

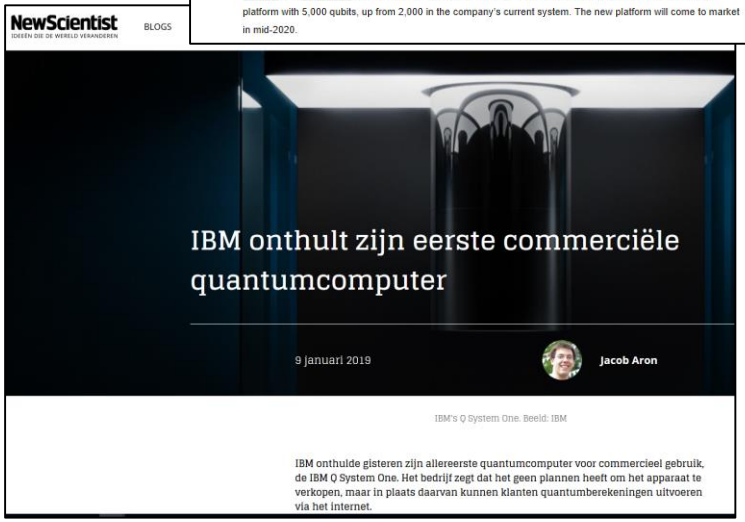


D-Wave announces its next-gen quantum computing platform

Frederic Lardinois @frederld / 2 months ago

Comment

D-Wave, the well-funded quantum computing company, today announced its next-gen quantum computing platform with 5,000 qubits, up from 2,000 in the company's current system. The new platform will come to market in mid-2020.



NewScientist IDEEËN DIE DE WERELD VERANDEREN BLOGS

IBM onthult zijn eerste commerciële quantumcomputer

9 januari 2019 Jacob Aron

IBM's Q System One. Beeld: IBM

IBM onthulde gisteren zijn allereerste quantumcomputer voor commercieel gebruik, de IBM Q System One. Het bedrijf zegt dat het geen plannen heeft om het apparaat te verkopen, maar in plaats daarvan kunnen klanten quantumberekeningen uitvoeren via het internet.

53 qubits

Breaking RSA

Classically
RSA-768
2010

IBM Q
35 (6 bits)
2019
7 qubits

D-Wave 2000Q
1005973 (20 bits)
2019
89 qubits

https://commons.wikimedia.org/wiki/File:EFF_photograph_of_NSA%27s_Utah_Data_Center.jpg

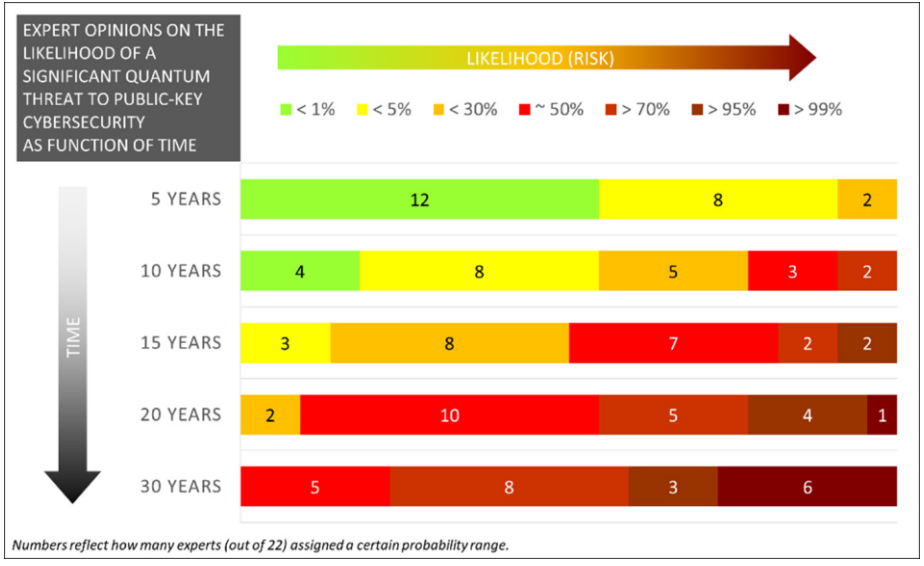
WHY START NOW?

Time you want information protected

Time to update IT infrastructure

Time to develop quantum computer

Time

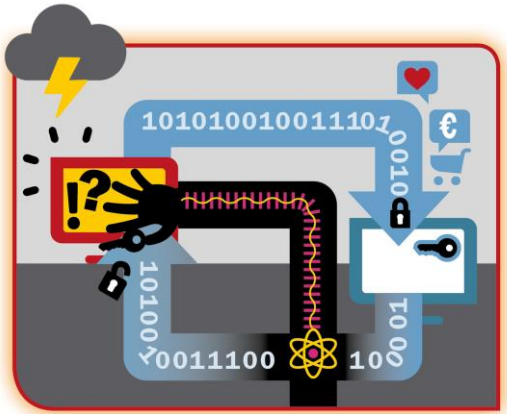


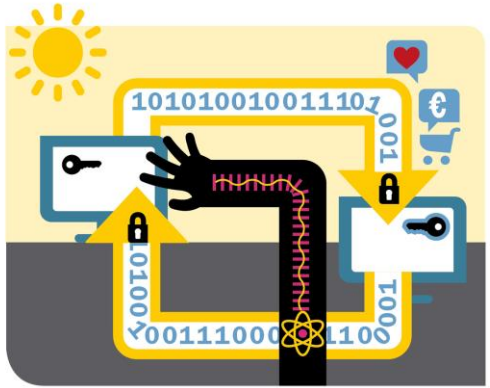
https://globalriskinstitute.org/publications/quantum-threat-timeline/

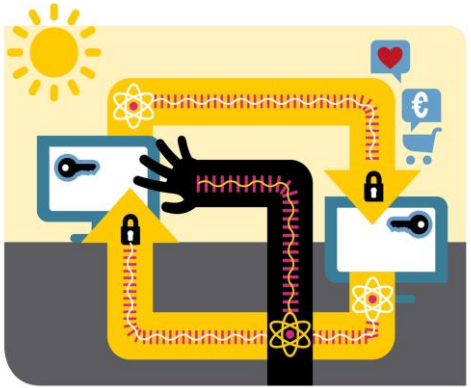
GETTING QUANTUM-READY

Broken:
RSA
ECC
DH

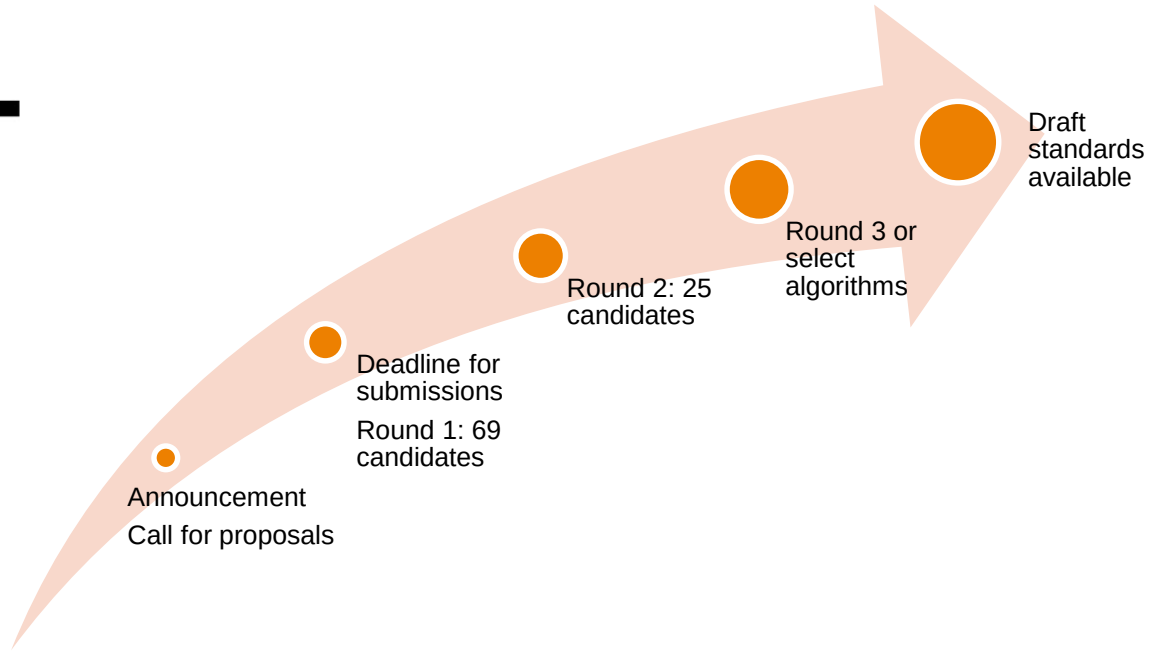
Weakend:
AES





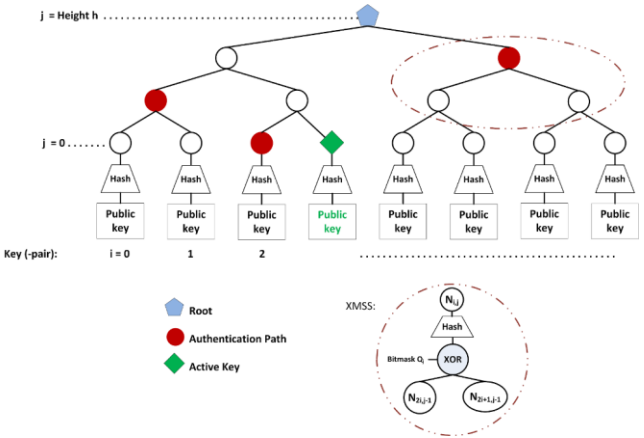


STANDARDISATION: NIST

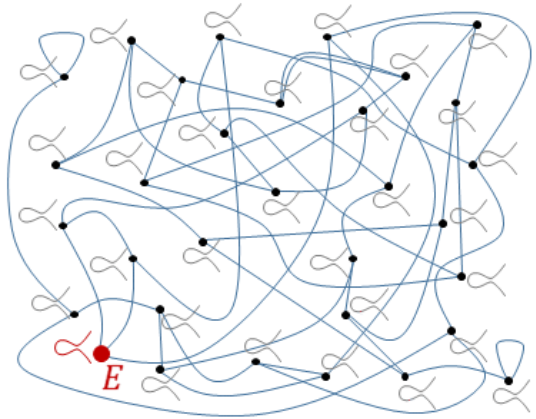


POST-QUANTUM CRYPTOGRAPHY

- Need to ***diversify*** the cryptographic protocols and associated mathematical problems.



Hash-based



Supersingular Isogenies

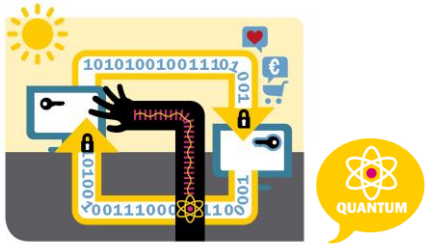
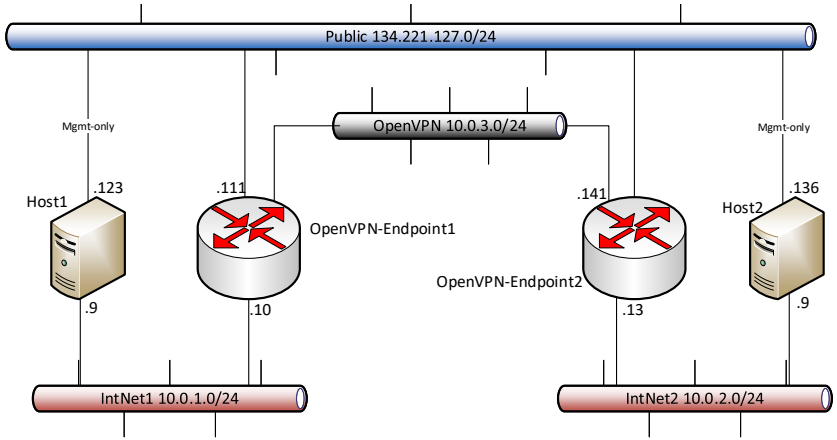


Figure: https://www.esat.kuleuven.be/cosic/elliptic-curves-are-quantum-dead-long-live-elliptic-curves/

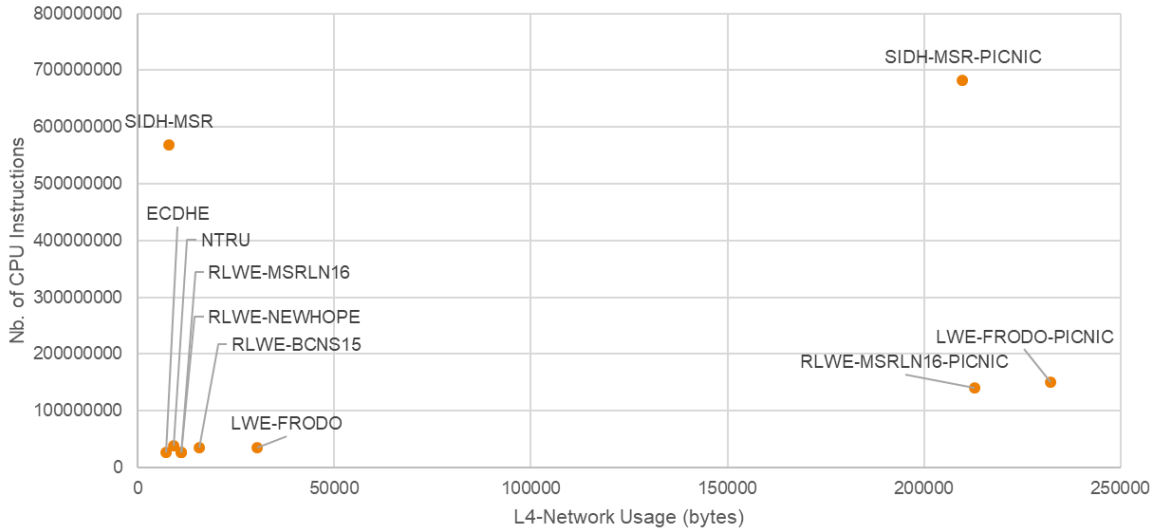
THE IMPACT OF POST-QUANTUM CRYPTOGRAPHY

Quantum-safe VPN

- Compiled OpenVPN with PQC support using shared objects from *OpenSSL-OQS*, *liboqs* and *lib_sigpicnic*
- Evaluated
  - Quantum-Safe Key Exchange
  - Quantum-Safe Hybrid Key Exchange (ECDHE+OQSKEX)
  - Quantum-Safe Authentication
- Experiments using TLS 1.2 and TLS 1.3



QUANTUM-SAFE VPN (TLS 1.2)
INCLUDING A SELF-SIGNING CA



Towards Quantum-Safe VPNs and Internet https://eprint.iacr.org/2019/1277

WHAT ABOUT LEGACY SYSTEMS?

Quantum-safe proxy

- Instead of just performing traditional proxy functions, we will enhance the proxy through network programmability to confirm whether encrypted TLS channels are quantum-safe.

- Investigate whether and Network Programmability / Hardware Acceleration in particular, can aid in transitioning from traditional encryption to quantum-safe encryption in networks.

https://www.technologyreview.com/s/612342/us-unhackable-quantum-networks/

Connectivity

The US is finally getting a hacker-proof quantum network that people can use

The fiber-optic cables carrying data across the internet are vulnerable. Two US initiatives aim to fix that by creating super-secure quantum transmissions.

by Martin Giles October 25, 2018

A few years ago, Edward Snowden, a contractor working for the US National Security Agency, leaked documents that showed the ways in which intelligence agencies were spying on our data. One of the most striking revelations was that spies had tapped into fiber-optic cables to monitor the vast amounts of information flowing through them.

secure communication

distributed computation

high resolution sensors

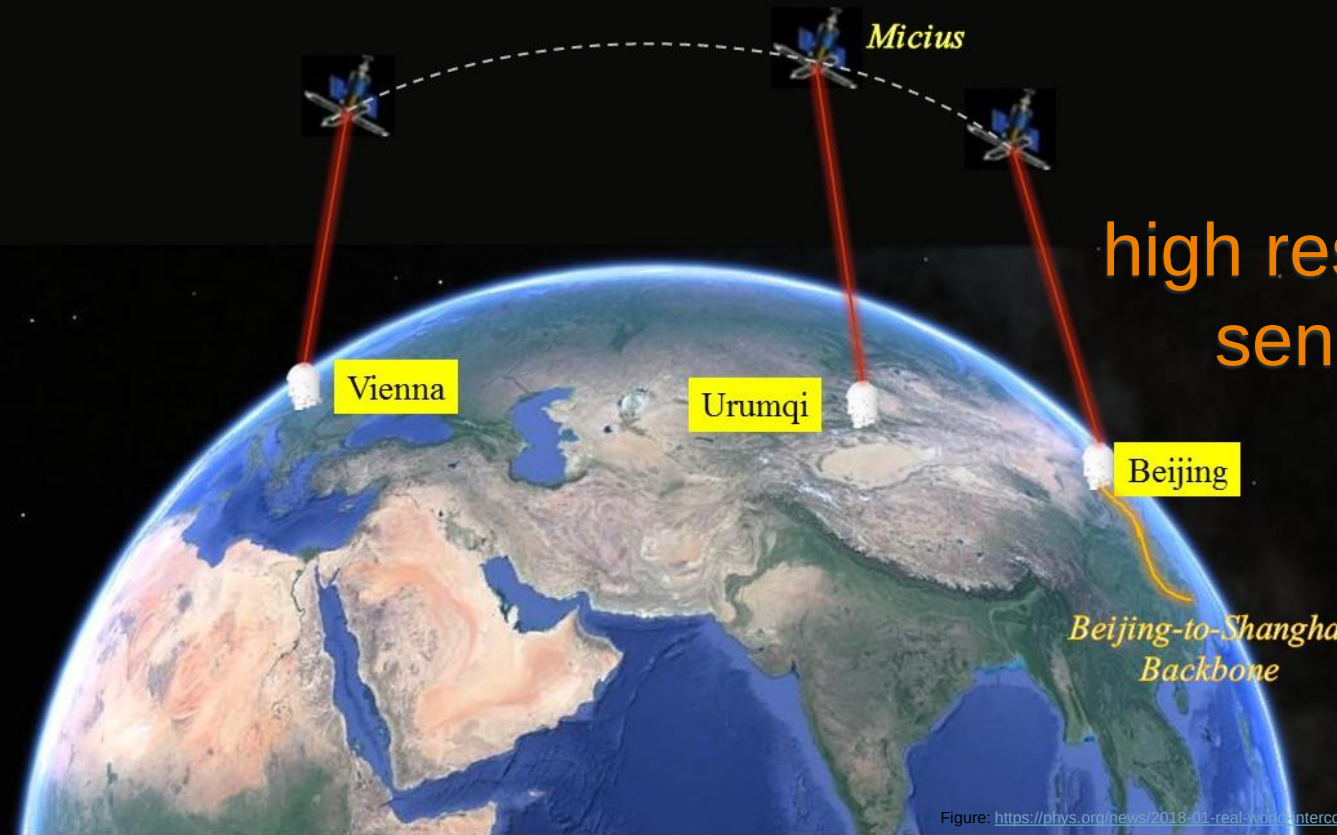
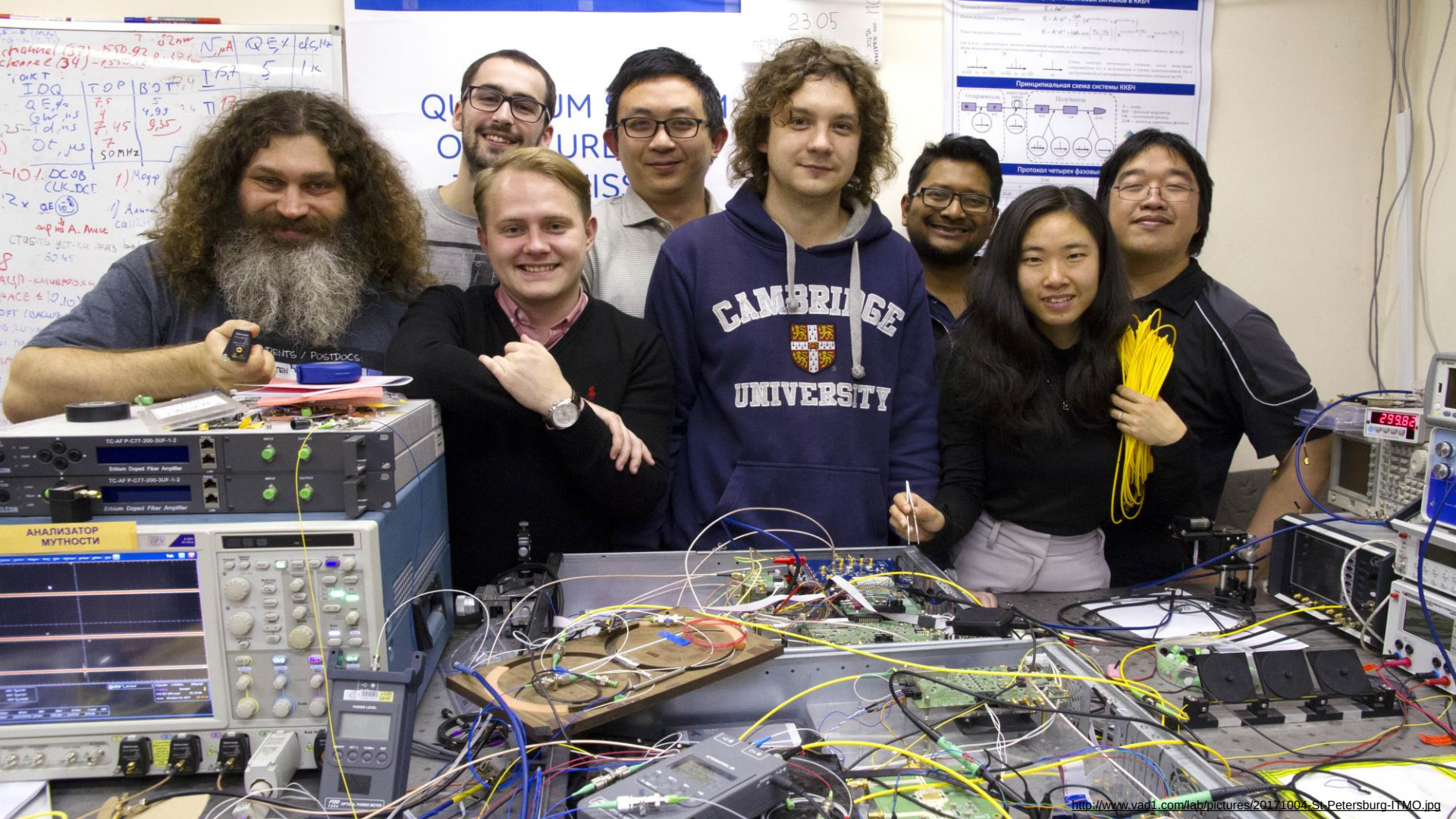


Figure: https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html



http://www.vad1.com/lab/pictures/20171004-St-Petersburg-ITMO.jpg

https://commons.wikimedia.org/wiki/File:EFF_photograph_of_NSA%27s_Utah_Data_Center.jpg

The Economist Topics Current edition More

Schrödinger's cheetah

Proof emerges that a quantum computer can outperform a classical one

A leaked paper has given the game away

Print edition | Science and technology ›
Sep 26th 2019

IN AN ARTICLE published in 2012 Joh
posed a question: "Is controlling lar
really, really hard, or is it ridiculously h
is in: it is merely really, really hard.

The Economist Topics Current edition More

Future-proofing the internet

Quantum computers will break the encryption that protects the internet

Fixing things will be tricky

n | Science and technology ›

QUANTUM FLAGSHIP

Discover Understand Engage Participate

The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

LEARN MORE

Maran van Heesch – maran.vanheesch@tno.nl