quantum encryptie en quantum-resistente cryptografie

Eddie Michiels

NOREA Quantum-seminar
UvA/Quantum Startup Village, Science Park Amsterdam

18 november 2022

onderwerpen

- korte inleiding
- quantum computing dreiging voor bestaande cryptografie
- quantum security technologie
  - Quantum Random Number Generator (QRNG)
  - Quantum Key Distribution (QKD)
- quantum-resistente cryptografie
  - algemeen
  - National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standaardisatie
- post-quantum migratie

INLEIDING

quantum computing / quantum security

superposition

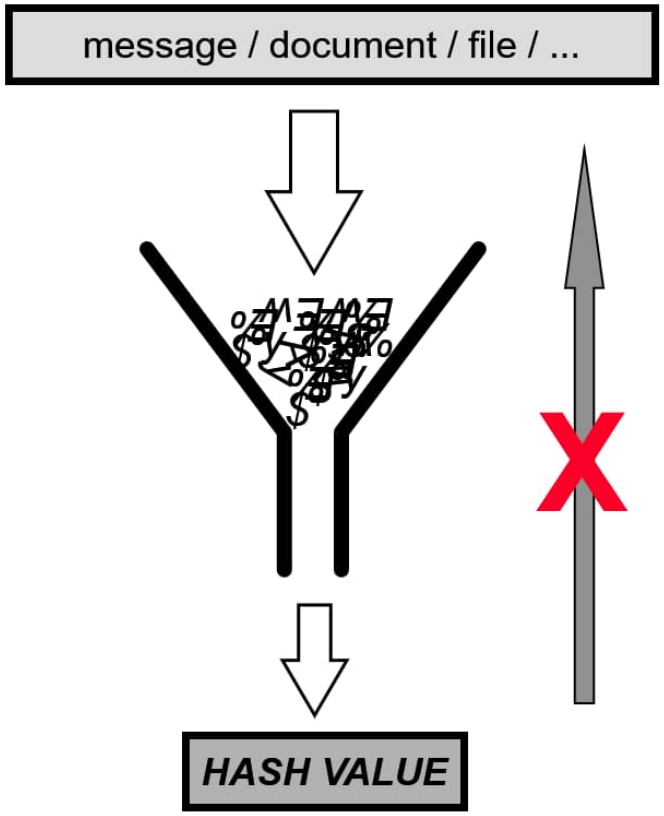
entanglement

measurement – quantum state collapse

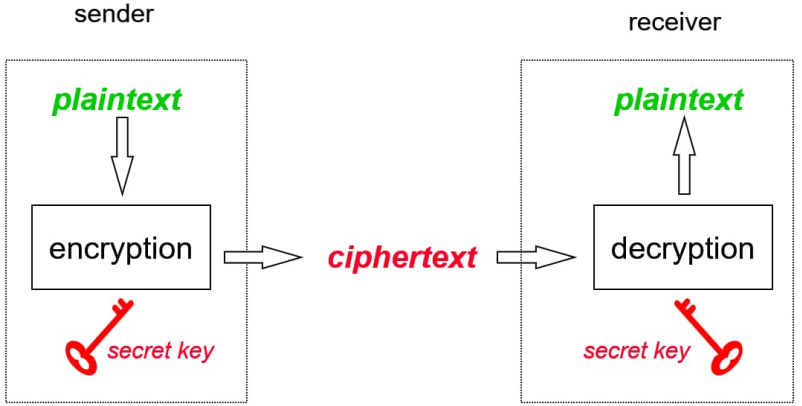
no cloning principle

cryptografische algoritmen

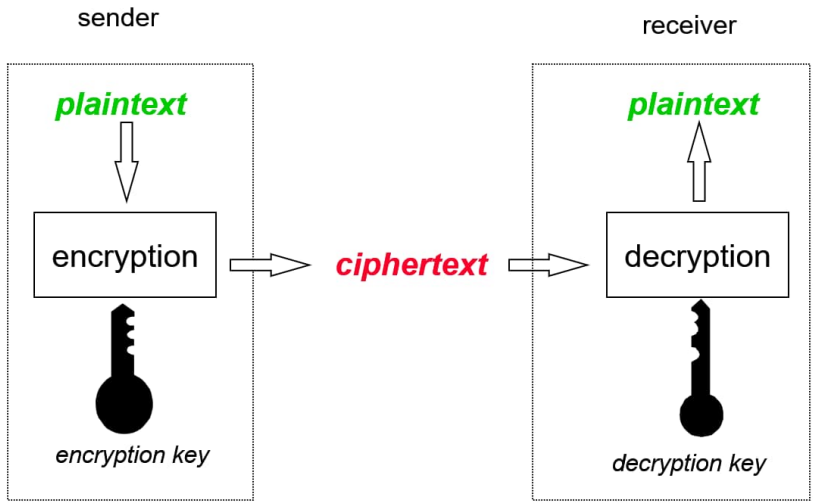
cryptographic hash function



symmetric (secret-key) cryptography



asymmetric (public-key) cryptography



QUANTUM COMPUTING
DREIGING

quantum algoritmes t.b.v. cryptanalyse m.b.v. kwantumcomputers

- cryptanalyse van cryptografische hash functies en symmetrische cryptografie
  - Grover's quantum algoritme (FTQC kwantumcomputer): kwadratische versnelling
  - HHL quantum algoritme (FTQC kwantumcomputer): exponentiële versnelling ???
  - variational quantum algoritmes (quantum annealer of NISQ kwantumcomputer): exponentiële versnelling ???
  - ???

FTQC Fault-Tolerant Quantum Computer
HHL Harrow-Hassidim-Lloyd
NISQ Noisy Intermediate-Scale Quantum
RSA Rivest-Shamir-Adleman
VQF Variational Quantum Factoring

- cryptanalyse van asymmetrische cryptografie
  - Shor's quantum algoritmes (FTQC kwantumcomputer): exponentiële versnelling
  - variational quantum algoritmes (quantum annealer of NISQ kwantumcomputer): exponentiële versnelling ???
  - Zapata Computing's VQF quantum algoritme (gepatenteerd): exponentiële versnelling ??? (claim: één uur voor kraken van 2048-bit RSA m.b.v. 6.000-qubit NISQ kwantumcomputer)
  - ???

quantum computing dreiging voor huidige crypto algo's
huidige consensus

- hash algoritmes (zoals bijvoorbeeld SHA) en symmetrische crypto algoritmes (zoals bijvoorbeeld AES) zijn quantum-resistent mits de hashcode / cryptosleutel voldoende lang is
  - aanname: Grover's kwantumalgoritme op een Fault-Tolerant Quantum Computer (FTQC) vormt de grootste dreiging
  - best practices voor cryptografie blijven uiteraard van toepassing

"ontwerp en implementatie van cryptografie is duivels moeilijk want bij cryptografie is niets vanzelfsprekend"
(Bruce Schneier)

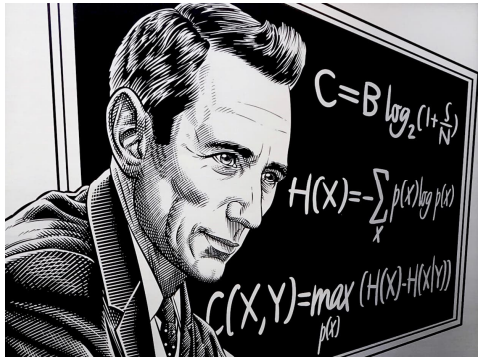
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve DSA
DH	Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm

- asymmetrische crypto algoritmes die zijn gebaseerd op wiskundige "trapdoors" (zoals bijvoorbeeld RSA, DH, ECDH, DSA en ECDSA) kunnen worden gekraakt met Shor's kwantumalgoritmes op een FTQC

wat is “voldoende lang” in gewoon Nederlands?

er zijn 2^{128} mogelijke waarden voor een 128-bit cryptosleutel, dat zijn er welgeteld 340 sextiljoen 282 quintiljard 366 quintiljoen 920 quadriljard 938 quadriljoen 463 triljard 463 triljoen 374 biljard 607 biljoen 431 miljard 768 miljoen 311 duizend 456

cryptanalyse op basis van geproduceerde ciphertext



Claude Shannon

Unicity length: least amount of plaintext that can be deciphered uniquely by an attacker armed with unlimited resources

L: maximum length of ciphertext that can be ***assumed*** to be safe

U **<<<** **L** (guesstimate)

safety margin

total length of generated ciphertext

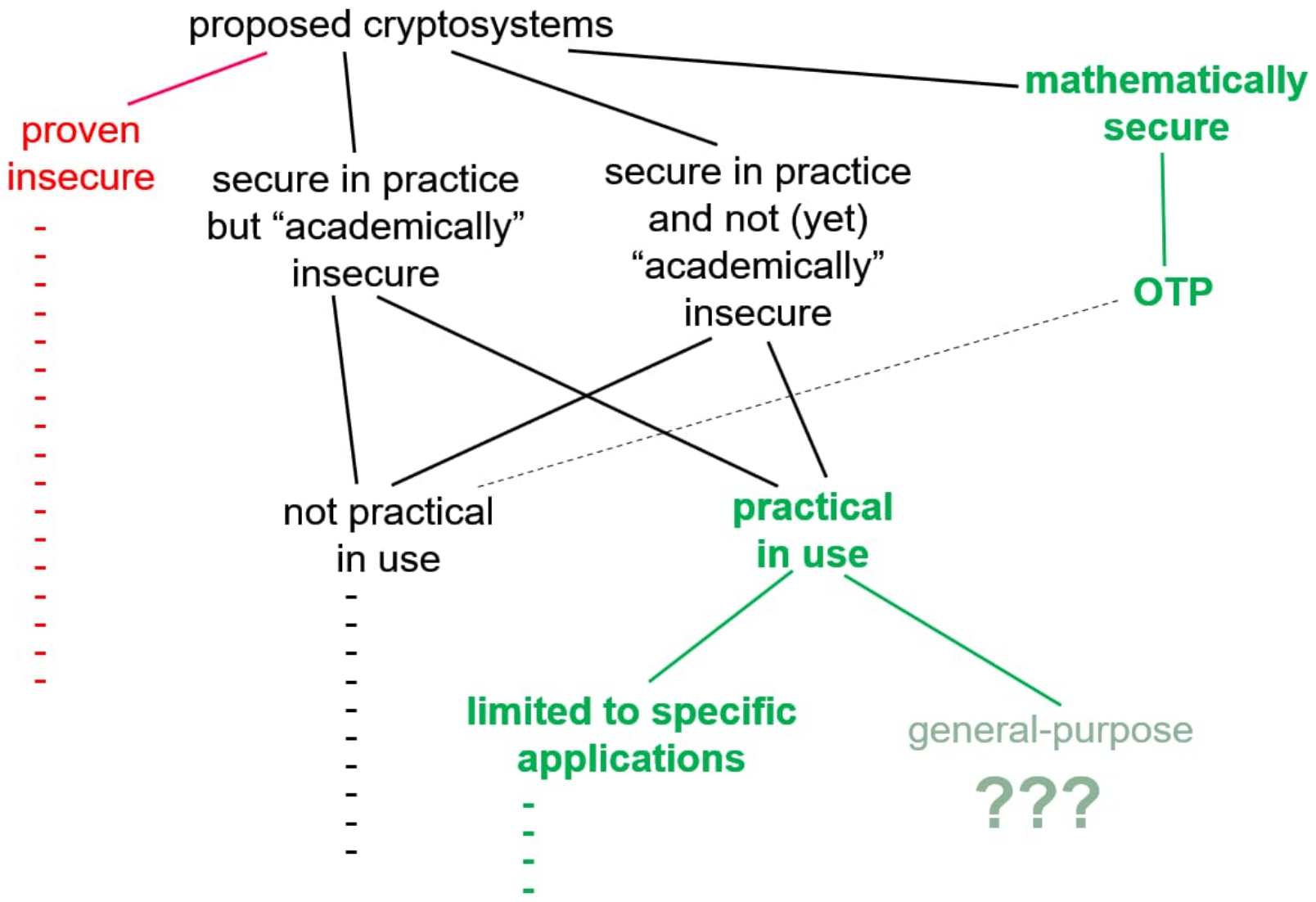
cipher unsolvable by principle

cipher solvable in principle, but unsolvable in practice

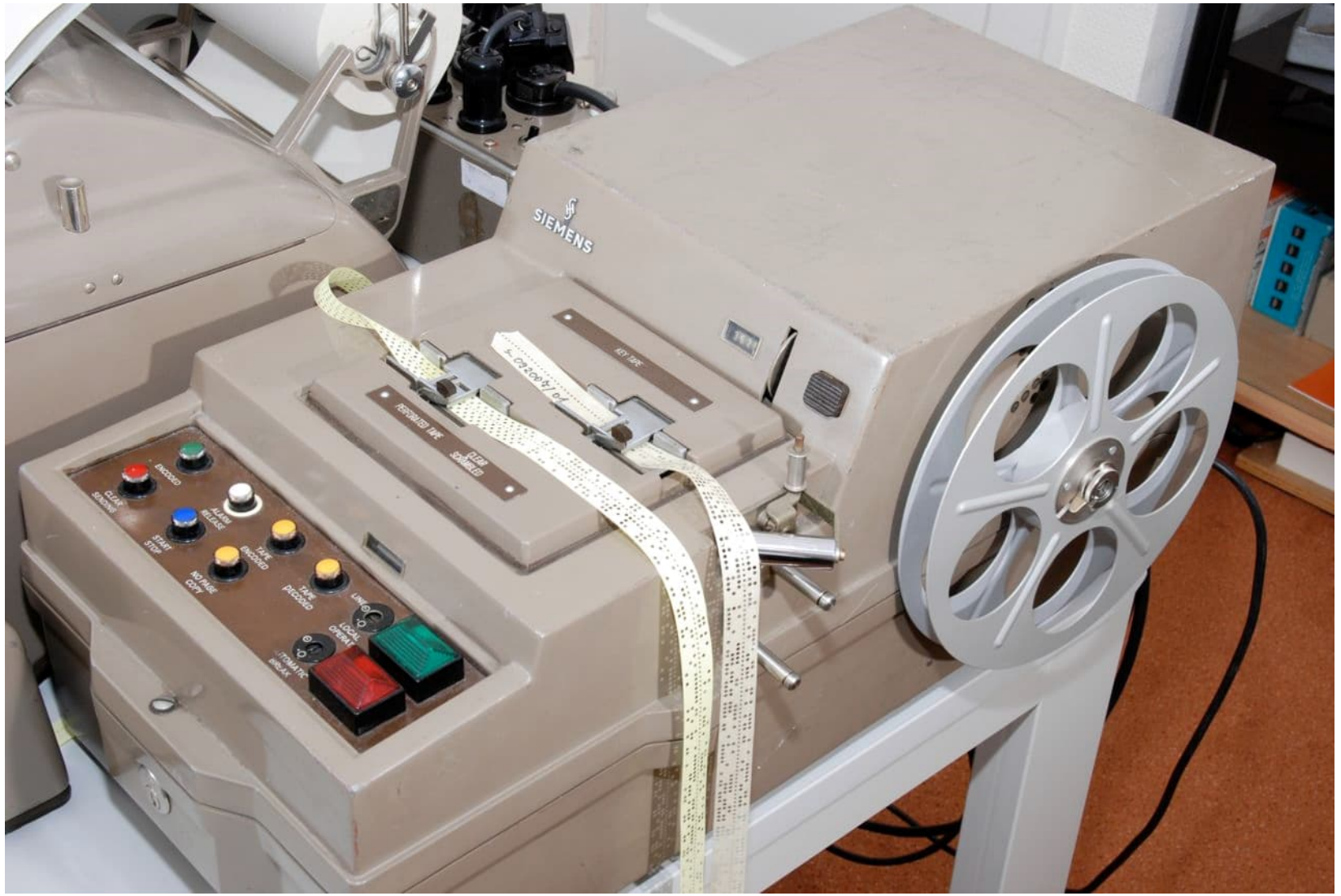
cipher solvable in practice

key change required

non-quantum cryptography taxonomy



OTP voor deWashington-Moskou hotline (1963)



wanneer zal de quantum dreiging zich manifesteren?

- het duurt nog ••• jaar voordat krachtige Fault-Tolerant Quantum Computers (FTQC's) met vele duizenden "foutvrije logische qubits" beschikbaar zullen zijn

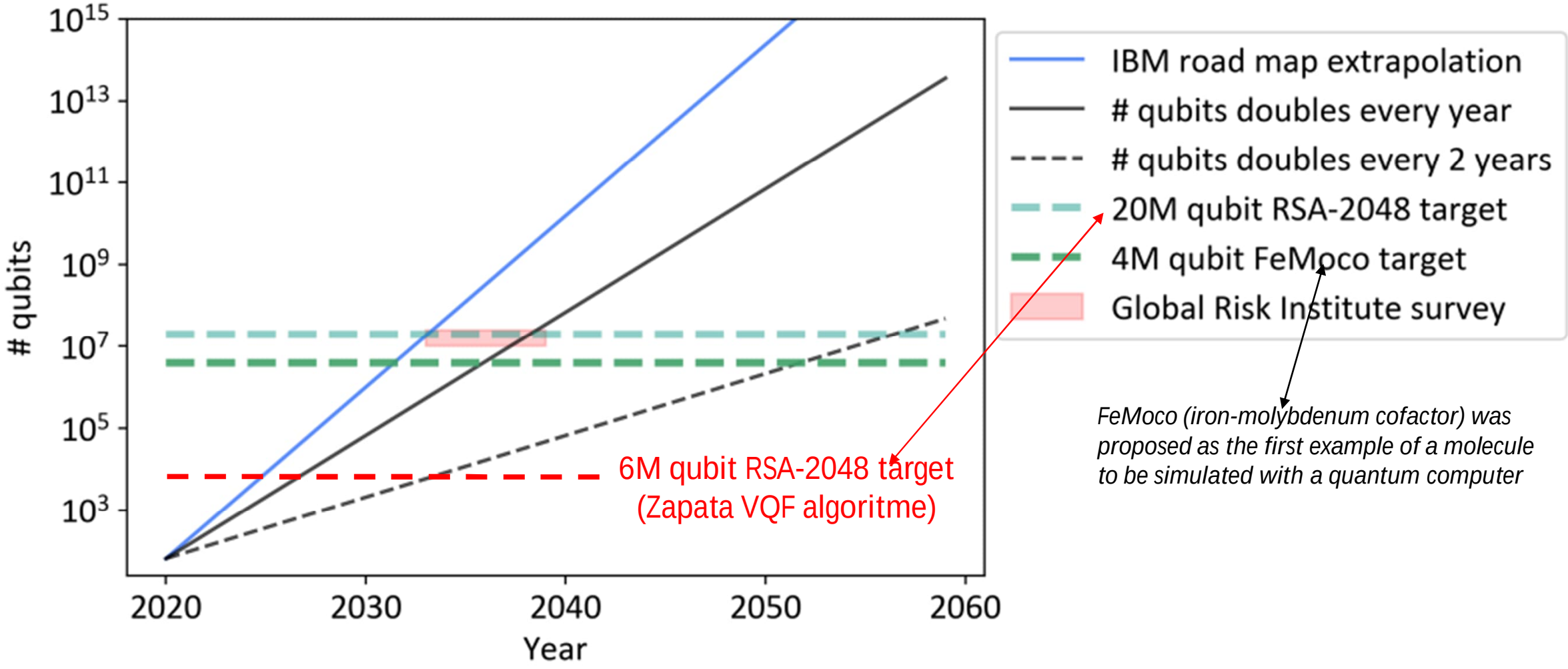
  (voor één "foutvrij logisch qubit" zullen ••• "noisy fysieke qubits" nodig zijn)

  maar voor gegevens die zeer lang vertrouwelijk moeten blijven bestaat nú al het gevaar van zgn. "store now, decrypt later" aanvallen ("harvest attacks")

- het is overigens niet aangetoond dat bestaande crypto algo's niet gekraakt kunnen worden m.b.v. conventionele (non-quantum) cryptanalyse

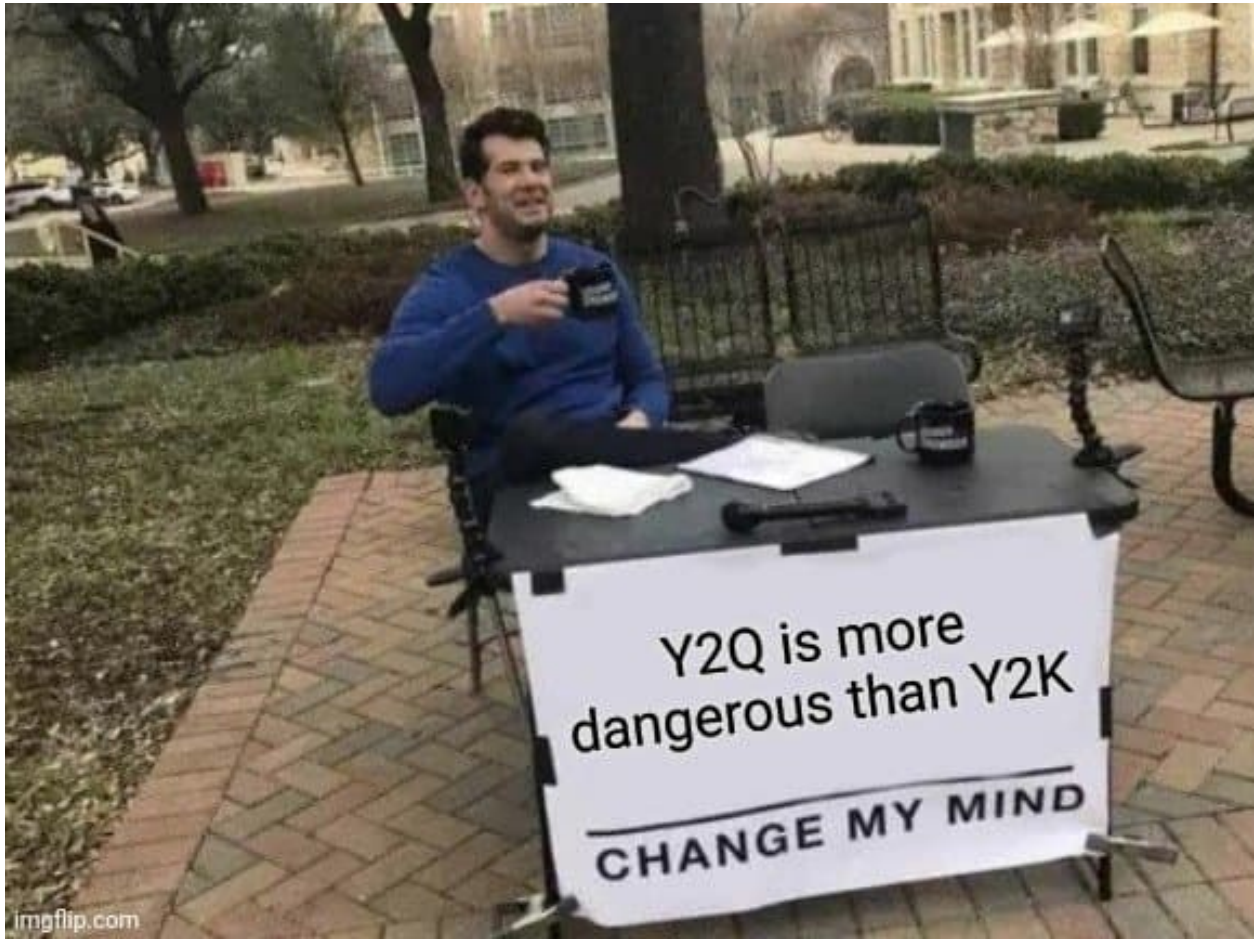
  alleen het One-Time Pad (OTP) crypto algo kan – althans in theorie – niet worden gekraakt

voorspellingen voor de groei van het aantal qubits



FeMoco (iron-molybdenum cofactor) was proposed as the first example of a molecule to be simulated with a quantum computer

Y2Q versus Y2K



kwantumcomputer dreiging heel kort samengevat

- ten eerste, er is op dit gebied nog veel dat we niet weten of waarvan we niet eens weten dat we het niet weten

- ten tweede, we moeten nu al beginnen met het treffen van voorbereidingen voor hetgeen ons mogelijk in de toekomst allemaal te wachten staat

QRNG

randomness: een filosofische discussie

- klassieke randomness is van epistomologische aard: het is geen inherente eigenschap van de natuur, maar komt voort uit onwetendheid of –in het geval van randomness- beperkingen in de beschikbare rekenkracht

  epistomologie (kennisleer of kennistheorie) is een tak binnen de filosofie die zich bezig houdt met de vraag hoe men aan kennis komt en wat de precieze aard is van deze kennis, met als centrale vragen:
  - wat is kennis?
  - hoe kan ik iets weten?
  - op welke manier kom ik aan kennis?

- kwantummechanische randomness is van ontologische aard: het is een inherente eigenschap van de natuur

  ontologie (zijnsleer) is een tak binnen de filosofie waarin het ‘zijn’ van het geheel van dingen wordt behandeld

random number generation

- Pseudo-Random Number Generator (PRNG)
  m.b.v. conventionele computer (inclusief CSPRNG)
- True Random Number Generator (TRNG)

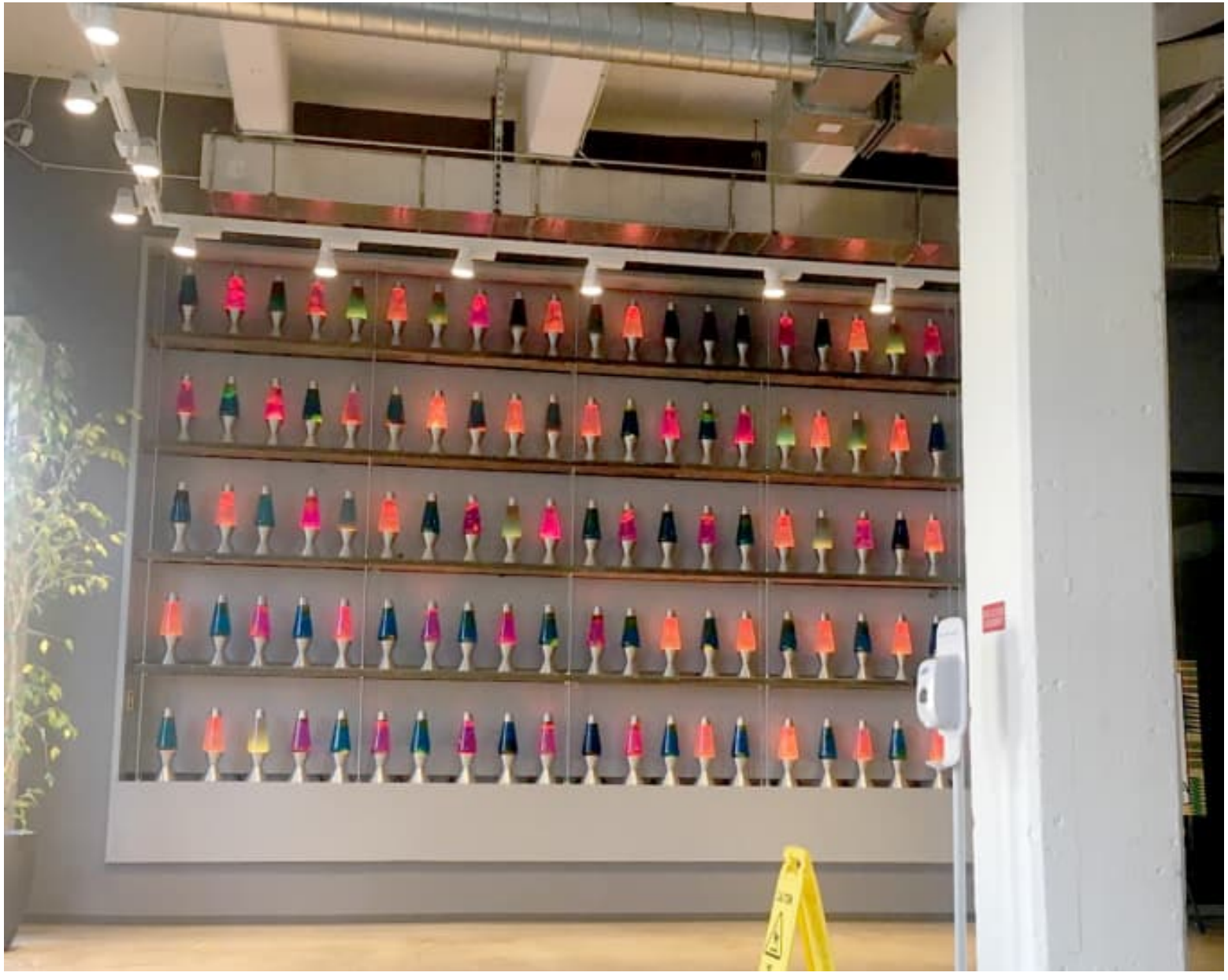
  - physical TRNG
    - conventionele Hardware Random Number Generator (HRNG)
    - Quantum Random Number Generator (QRNG)
      - niet gebaseerd op quantum computing
      - gebaseerd op quantum computing

      al dan niet Device-Independent QRNG (DI-QRNG)

  - non-physical TRNG (niet betrouwbaar)
    - onvoorspelbaarheid van de duur van computer processen
    - onvoorspelbaarheid van mens-computer interacties
- combinaties

CSPRNG Cryptographically Secure PRNG
NISQ Noisy Intermediate-Scale Quantum

random number generation bij Cloudflare in San Francisco



QRNG technieken anders dan quantum computing

- gebaseerd op “quantum randomness” van optische technieken
  - branching-path generator (measurement of entangled photons)
  - time-of-arrival generator (arrival time of successive single photons)
  - photon-counting generator (number of photons detected during fixed time interval)
  - quantum-vacuum-fluctuation generator (balanced homodyne measurements of vacuum fluctuations in magnetic field of the radiofrequency sidebands of a single-mode laser diode)
  - phase-noise/diffusion generator (output field of a laser caused by spontaneous emission)
  - amplified-spontaneous-emission generator (spontaneous emitted photons from a light source)
  - en nog meer …

- <u>niet</u> gebaseerd op optische technieken
  - tunnelling QRNG (unpredictable tunnelling noise)
  - radioactive-decay QRNG (random timing of radioactive atom decay)
  - skyrmion-based QRNG
  - en nog meer …

QRNG issues

- gebruik in Virtual Machine (VM) en containerized omgevingen is problematisch
- QRNG producten bevatten ook conventionele elektronica

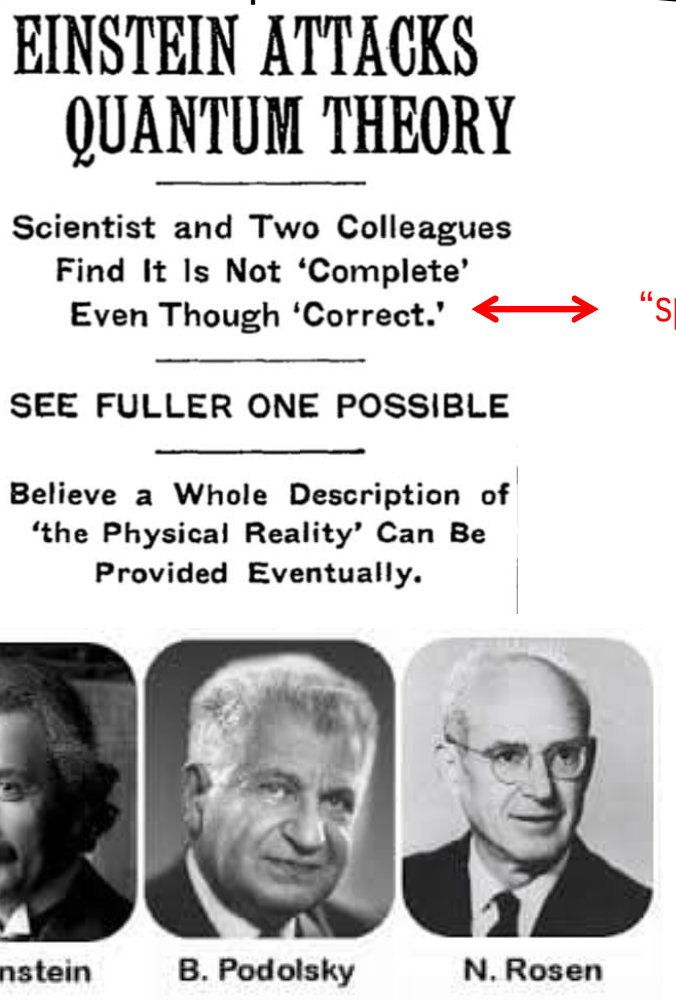
  claims van leveranciers (“gegarandeerd random want gebaseerd op kwantummechanica principes”) kunnen niet worden geverifieerd m.b.v. de standaard randomness tests van bijvoorbeeld NIST

  daarom Device-Independent QRNG (DI-QRNG) research
- QRNG standaardisatie
  daarom het EITCI Quantum Standards Group (QSG) initiatief
- certificatie van QRNG producten/diensten
- UK NCSC, NSA en anderen: gebruik QRNG niet voor toepassingen van de overheid en ook niet voor militaire toepassingen

EITCI	European IT Certification Institute
NIST	National Institute of Standards and Technology
NSA	National Security Agency
UK NCSC	United Kingdom National Cyber Security Center

DI-QRNG op basis van Bell inequality test

1935: EPR paradox



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

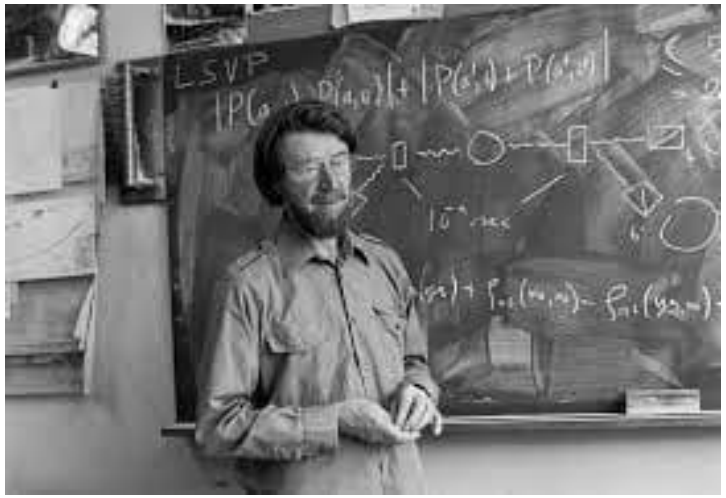
SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

A. Einstein B. Podolsky N. Rosen

↔ "spukhafte Fernwirkung"

1964: Bell test invented by John Stewart Bell



Bell Test by Alain Aspect, 1981

- Done in Paris
- First experiment to measure the Bell inequality directly
- Prior only single-channel-analyzer experiments

2022: Alain Aspect, John Clauser en Anton Zeilinger delen een Nobelprijs

DI-QRNG Device-Independent QRNG
EPR Einstein, Podolsky and Rosen

voorbeelden van QRNG producten/diensten (1)

- Alibaba: QRNG Cloud Platform
- Australian National University (ANU):
  - ANU Quantum Numbers on AWS Marketplace
  - ANU API3
- ComScire:
  - CryptoStrong
  - PureQuantum
- Crypta Labs:
  - QOM
  - QaaS
- CRYPTO4A: QAOS

API Application Programming Interface
AWS Amazon Web Services
QaaS Quantum-as-a-Service

ANU's QRNG service - AWS Marketplace

API Application Programming Interface
AWS Amazon Web Services

QUANTUM RANDOM NUMBERS
POWERED BY ANU

About Quantum numbers by ANU

The ANU quantum random numbers provides secure and trusted random numbers on demand. By harnessing the quantum nature of lasers, high speed and truly random numbers are generated in real time.

Quantum numbers by ANU

Visit the Quantum numbers by ANU website

All products (1 result) showing 1 - 1

1

Sort By: Relevance

Quantum Random Numbers API

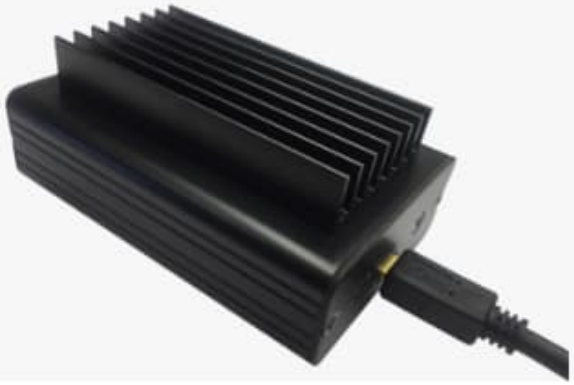
By **Australian National University**

True randomness generated in a physics laboratory at the Australian National University. We use lasers and high speed detectors to continuously measure quantum vacuum fluctuations which provide an endless source of reliable and trusted entropy. This high quality entropy source can be accessed...

ComScire's QRNG products

The ComScire® MicroStrong™ True Random Number Generator

4 to 16 million bits per second in a truly tiny package. 7x7mm QFN or 2.2×2.6mm CSP (shown in image). Flexible interface options, low power: 12 or 15mW. Contact us for details.



The ComScire® CryptoStrong™ Cryptographic TRNG

128 million bits per second, USB interface. Certified for both NIST SP 800-90C and BSI AIS 20/31 Class PTG.3 standards. Guaranteed Quantum Computer Secure™

The ComScire® PureQuantum® Quantum Random Number Generator

4 to 128 million bits per second, USB interface. Guaranteed to pass any properly designed test for randomness.

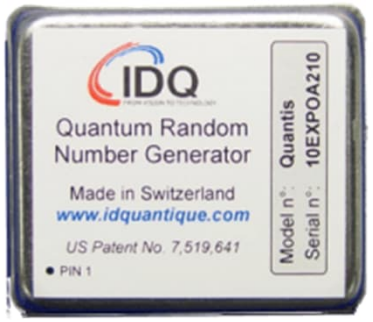
Gaming Labs Certified®

voorbeelden van QRNG producten/diensten (2)

- EYL: QRNG chip
- Go Quantum: Quantum-RNG
- Hub Security: Quantum Secured Cloud Workspace QRNG
- ID Quantique:
  - Quantis QRNG chip (met BSI certificatie)
  - Quantis USB QRNG
  - Quantis PCIe card
- KETS Quantum Security: QRNG chip
- Micro Photon Devices: MPD QRN
- PicoQuant: QRNG chip
- QRANGE: QRNG chips
- Quantinuum: Quantum Origin (verifiable quantum randomness)
- Quantropi: QiSpace SaaS platform

BSI Bundesamt für Sicherheit in der Informationstechnik
PCIe Peripheral Component Interconnect Express
SaaS Software-as-a-Service
USB Universal Serial Bus

ID Quantique's Quantis QRNG producten



protected chip module

PCIe insteekkaart

USB module

PCIe Peripheral Component Interconnect Express
USB Universal Serial Bus

Quantinuum's Quantum Origin

The NCSC is Right to Criticise Existing Quantum Security Technology
CAMBRIDGE QUANTUM TAKES FUNDAMENTALLY DIFFERENT APPROACH

PUBLISHED ON
28.03.2021

Articles

Written by
Duncan Jones

Published on
Medium

Share

It's been a year since the United Kingdom's National Cyber Security Centre (NCSC) posted a damning statement about quantum random number generators (QRNGs), which discouraged their use for government and military applications. Other agencies, including the NSA, made similar comments about related technology.

At Cambridge Quantum, we develop quantum entropy products, so at first it may come as a surprise that we thoroughly agree with the NCSC's position and amplify it loudly to our customers. The NCSC got it spot on – there's no place in a high security environment for noisy QRNGs.

To mark the (almost) anniversary of the NCSC statement, this article carefully examines the criticisms levelled at existing QRNGs and explains the flawed approach taken so far. We then explain the approach taken by Cambridge Quantum, which tackles the issues head-on; not by slippery debate, but with deliverable and measurable actions. Cambridge Quantum's approach provides truly perfect quantum random numbers that we then use in our cybersecurity products.

dit is een op quantum computing gebaseerde QRNG implementatie die wordt geverifieerd m.b.v. een eveneens op quantum computing gebaseerde implementatie van een variant van de Bell inequality test

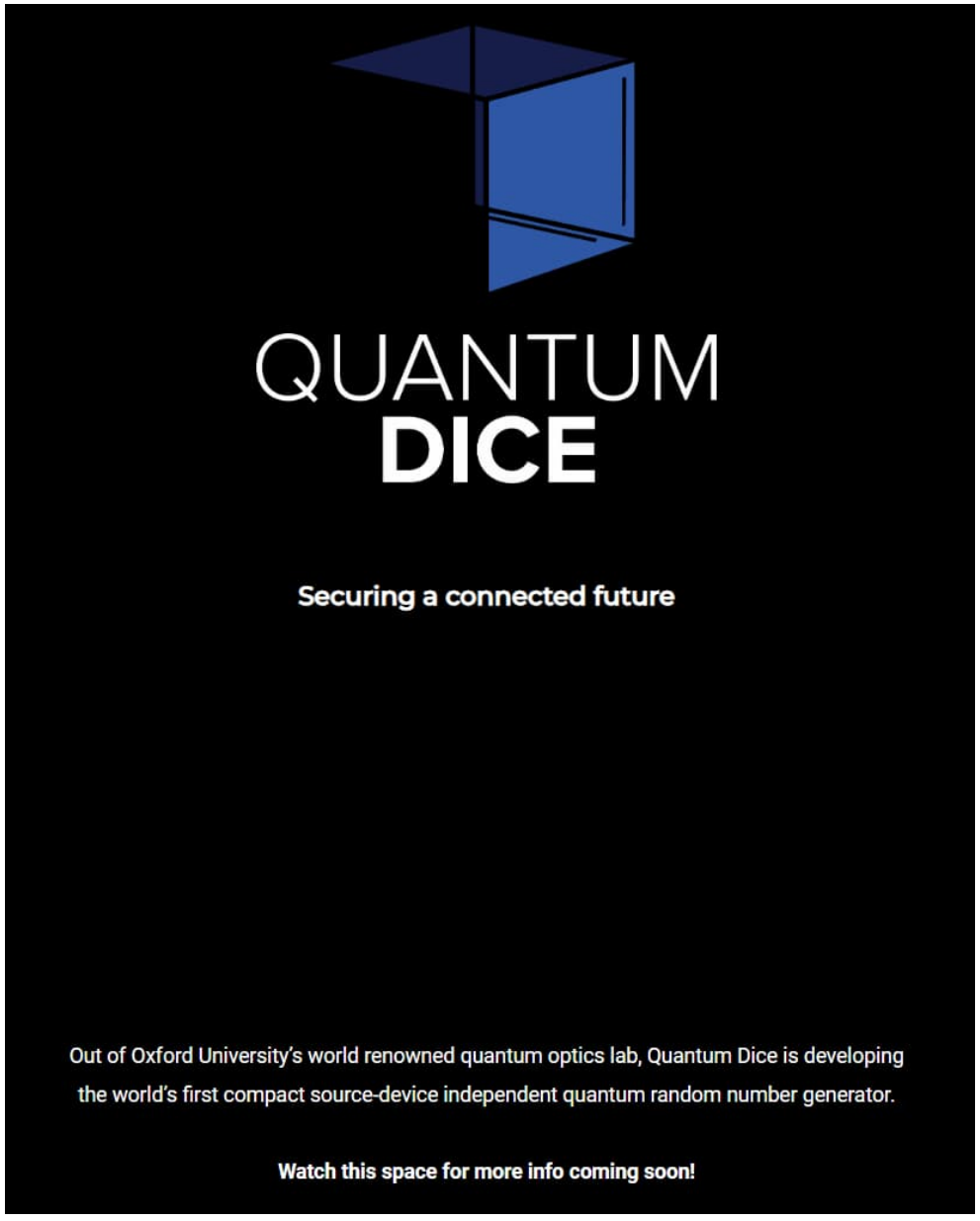
maar, de uitslag van de test is ook positief als voor de QRNG en voor de inequality test een kwantumcomputer *simulator* wordt gebruikt i.p.v. een echte kwantumcomputer!

voorbeelden van QRNG producten/diensten (3)

- Quantum Blockchain: QRNG voor blockhain
- Quantum CTek: QRNG 100E
- Quantum Dice: self-certified QRNG device
- Quantum eMotion: QRNG2 hardware wallet voor cryptocurrencies
- Quantum Trilogy: Integrated Quantum Communication Platform
- Quintessence Labs:
  - qStream 100 PCIe card
  - qRand 100 Quantum Entropy Enhancer
- Quside: FMC 400
- Samsung: Galaxy A Quantum smartphone (ID Quantique chip)
- SPAD lab: QRNG USB
- ThinkQuantum: THIKE
- XT Quantech: QRNG-200

PCIe Peripheral Component Interconnect Express
USB Universal Serial Bus

Quantum Dice website



embedded QRNG (Samsung smartphone)

QRNG heel kort samengevat

- ten eerste, randomness is van primair belang voor cryptografie
- ten tweede, QRNG kan daar in specifieke situaties mogelijk een bijdrage aan leveren
- ten derde, QRNG levert op zichzelf in de praktijk geen bijdrage aan quantum-resistentie
- ten vierde, kijk goed uit bij de aanschaf van QRNG producten of bij het gebruik van QRNG diensten:

  zorg er voor dat je een “kat in de zak” koopt, dan weet je zeker dat het écht kwantum is ☺

QKD(N)

QKD (Quantum Key Distribution)

- QKD is technologie voor de bilaterale uitwisseling van symmetrische cryptosleutels en is gebaseerd op het “no-cloning” principe van kwantummechanica

- QKD maakt hiervoor gebruik van twee aparte communicatiekanalen
  1. een point-to-point quantum channel
  2. een conventioneel datacommunicatiekanaal

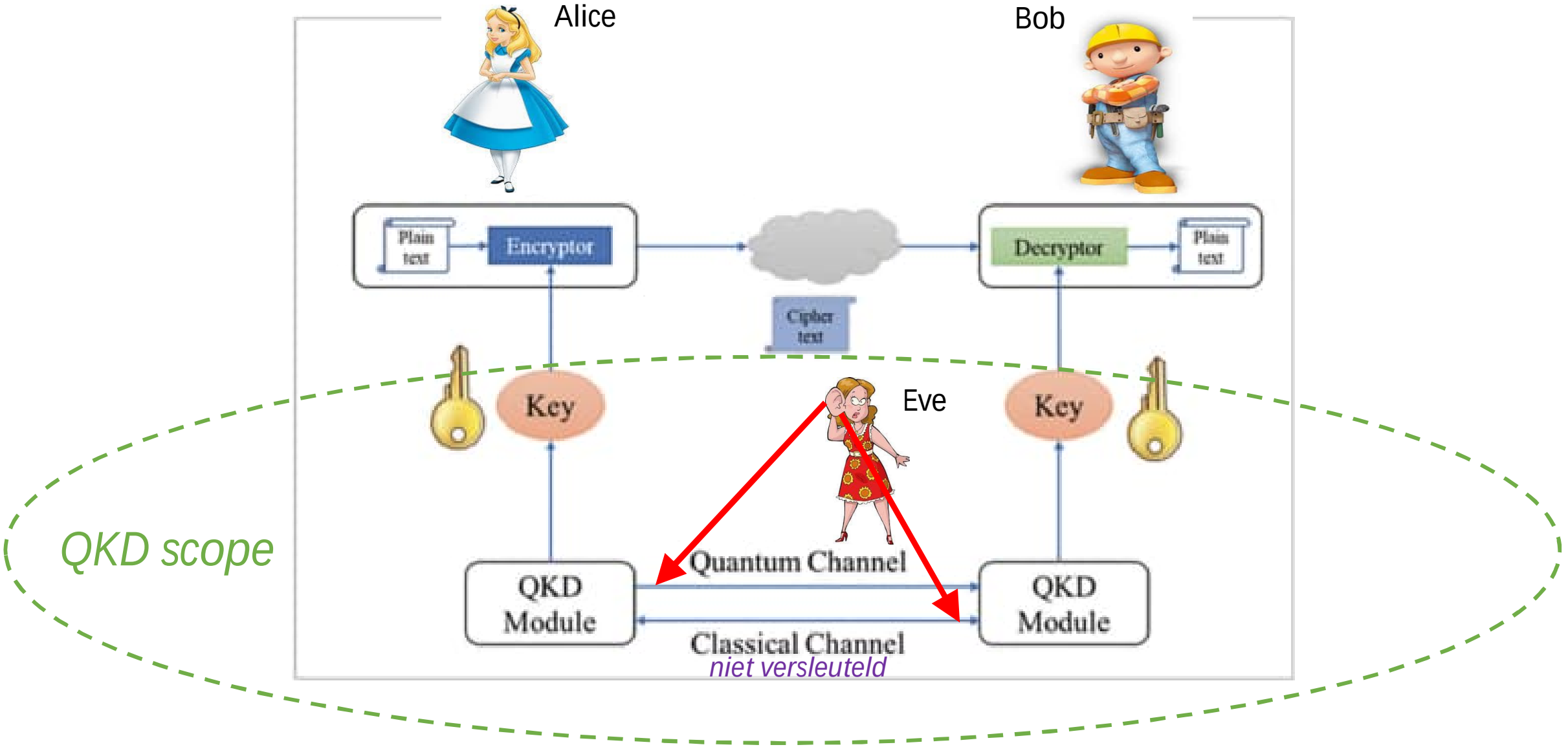
- er zijn verschillende QKD technologieën en er bestaan meerdere soorten QKD protocollen (plus een heleboel varianten van beide)

- er is een significant verschil tussen QKD glasvezeltechnologie en QKD “free space” technologie

- er bestaan al sinds geruime tijd (prototype) implementaties van QKD
  - 1996: eerste demo in de Verenigde Staten (free space QKD technologie)
  - 2007: gegevensuitwisseling voor de Zwitserse verkiezingen (glasvezel QKD technologie)

- er zijn uiteenlopende scenario’s (use cases) voor het gebruik van QKD technologie (vaak is dat gebruik nog beperkt tot experimenten)

de basisprincipes van QKD



generiek QKD protocol

- quantum exchange protocol (quantum channel)
  - aanmaak, uitwisseling en measurement van fotonen
  - produceren van ruwe cryptografische sleutels door beide partijen op basis van deze uitwisseling

- conventionele post-processing van de ruwe cryptografische sleutel
  inclusief uitwisseling van –uiteraard- niet versleutelde, maar wél geauthenticeerde berichten van post-processing protocollen (conventionel datacommunicatiekanaal)
  - schatting van de *quantum exchange error rate* op basis van de vergelijking van een klein percentage van de bits van de ruwe cryptografische sleutels
  - *error reconciliation* en tevens bepalen van de *Quantum Bit Error Rate* (QBER) voor de gehele ruwe cryptografische sleutel
  - schatting van de hoeveelheid sleutelinformatie die mogelijk kan zijn gelekt en minimaliseren van partiële sleutelinformatie verkregen door eventueel afluisteren van het quantum channel en/of het conventioneel datacommunicatiekanaal *(privacy amplification)*
  - vergelijking van de hashcodes berekend over de sleutelwaarden van beide partijen; als deze hashcodes gelijk zijn dan is m.b.v. QKD een bilaterale symmetrische cryptosleutel bepaald

  (sommige post-processing stappen zijn optioneel en er zijn vele varianties)

soorten QKD protocollen

- methode toegepast voor coding
  - Discrete Variable coding QKD (DV-QKD)
    - Prepare-and-Measure (P&M): superpositie van polarisaties van enkelvoudige fotonen
    - entanglement van fotonparen
  - Continuous Variable coding QKD (CV-QKD)
  - …
- voorbeelden
  - BB84 (Bennett and Brassard 1984): P&M DV-QKD
  - E91 (Ekert 1991): entanglement DV-QKD
  - B92 (Bennett 1992): simpeler variant van BB84 (ook als CV-QKD)
  - BBM92 (Bennett, Brassard and Mermin 1992): simpeler variant van E91
  - GG02 (Grosshans and Grangier 2002): CV-QKD
  - SARG04 (Scarani, Acín, Ribordy and Gison 2004): robuuster versie van BB84

BB84 QKD protocol
Discrete Variable (DV) coding
Prepare & Measure (P&M)

gegenereerd door een (Q)RNG

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

ruwe cryptosleutel

BB84 QKD opstelling bij Quantum.Amsterdam

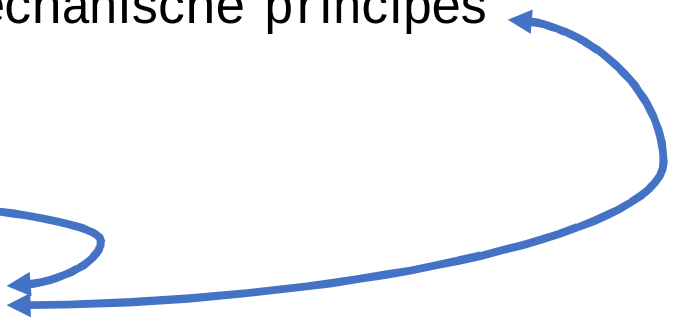
Eve

Alice

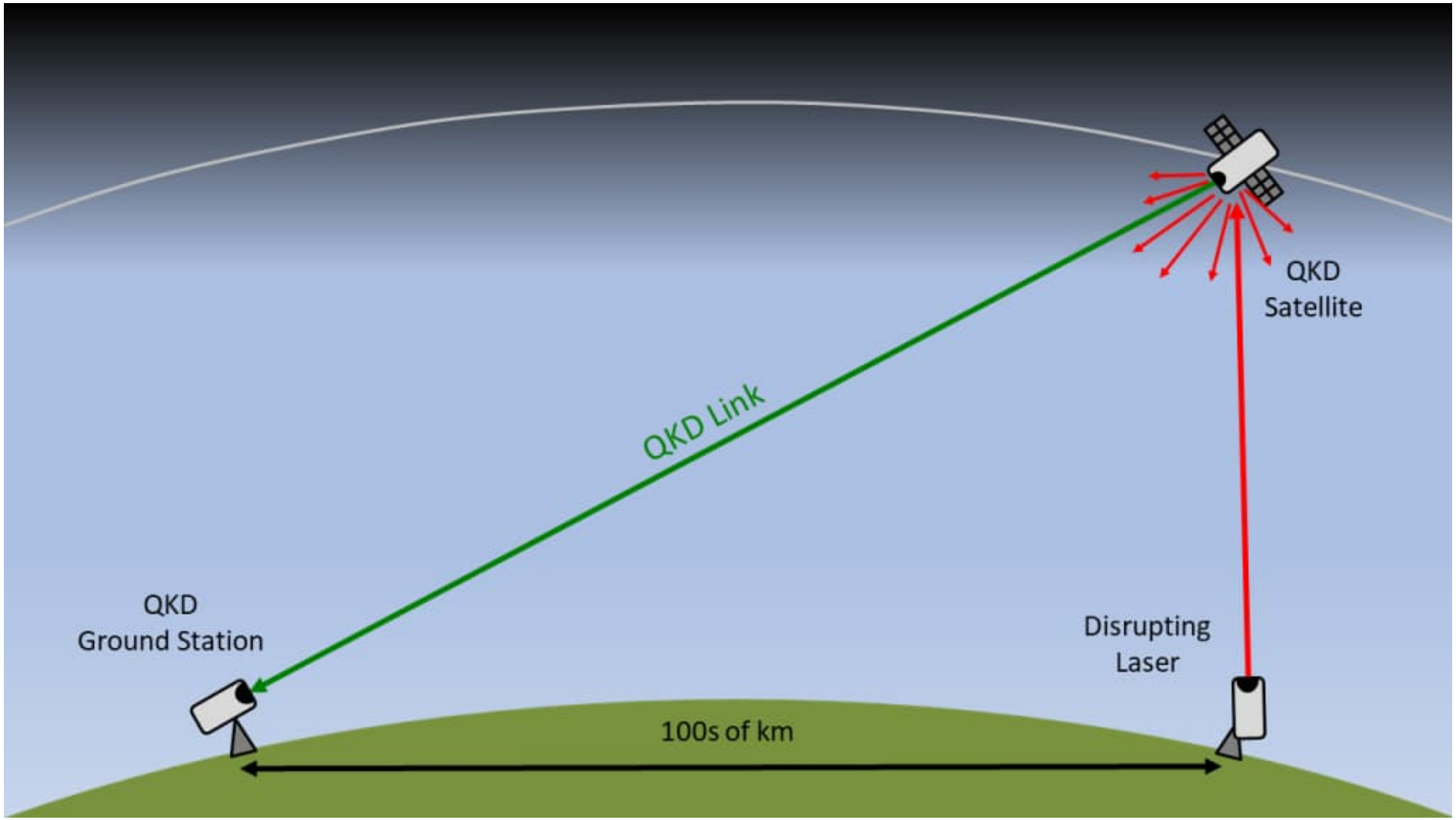
Bob

QKD issues

- alleen point-to-point verbindingen (fysieke netwerklaag)
- beperkte afstanden (met name bij glasvezel)
- beperkte key rate (t.o.v. de maximale transmissiesnelheid van het medium)
- vereist (in principe) dedicated optische componenten en dedicated glasvezels
- géén garantie voor de door leveranciers geclaimde “absolute veiligheid op basis van kwantummechanische principes”
- Denial-of-Service (DoS) aanvallen
- fragmentarische standaardisatie
- certificatie van QKD producten en diensten



DoS aanval op QKD implementatie

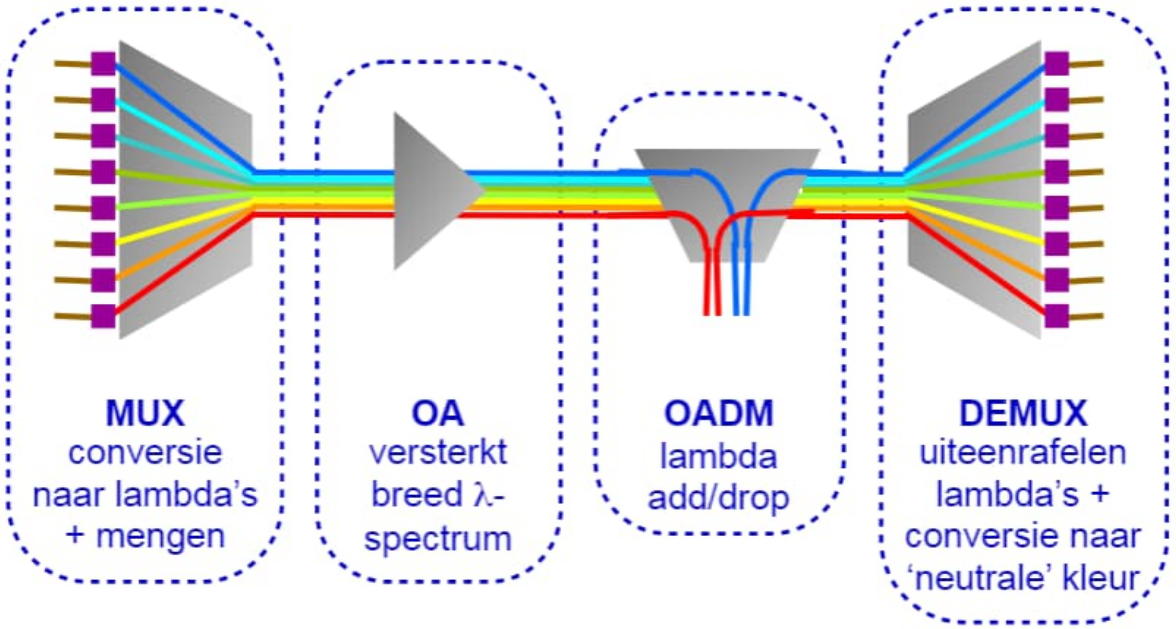


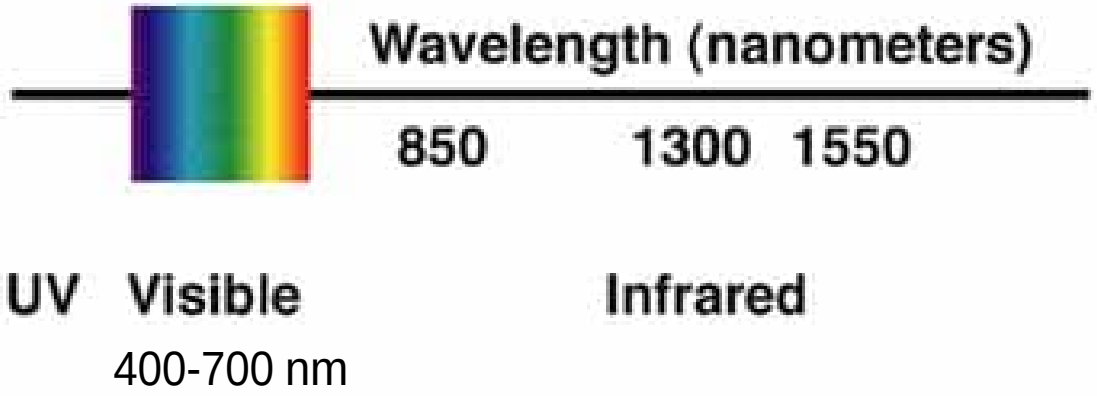
QKD ontwikkelingen

- off-the-shelf optische componenten en WDM/DWDM technologie
- Measurement Device-Independent QKD (MDI-QKD) op basis van Bell tests
- Twin-Field QKD (TF-QKD) research/experimenten (op basis van Bell tests)
- Device-Independent QKD (DI-QKD) research (op basis van Bell tests)
- QKD netwerken *≠ quantum netwerk/quantum internet (untrusted quantum repeaters)*
  - QKD glasvezelnetwerken
    - stervormige netwerken op basis van photonic switch technologie
    - stervormige netwerken op basis van untrusted midstation (device-independent) technologie op basis van Bell tests (MDI-QKD of TF-QKD)
    - QKD Network (QKDN) netwerken m.b.v. trusted relay technologie
  - satelliet QKD netwerken en UAV QKD netwerken
  - combinaties

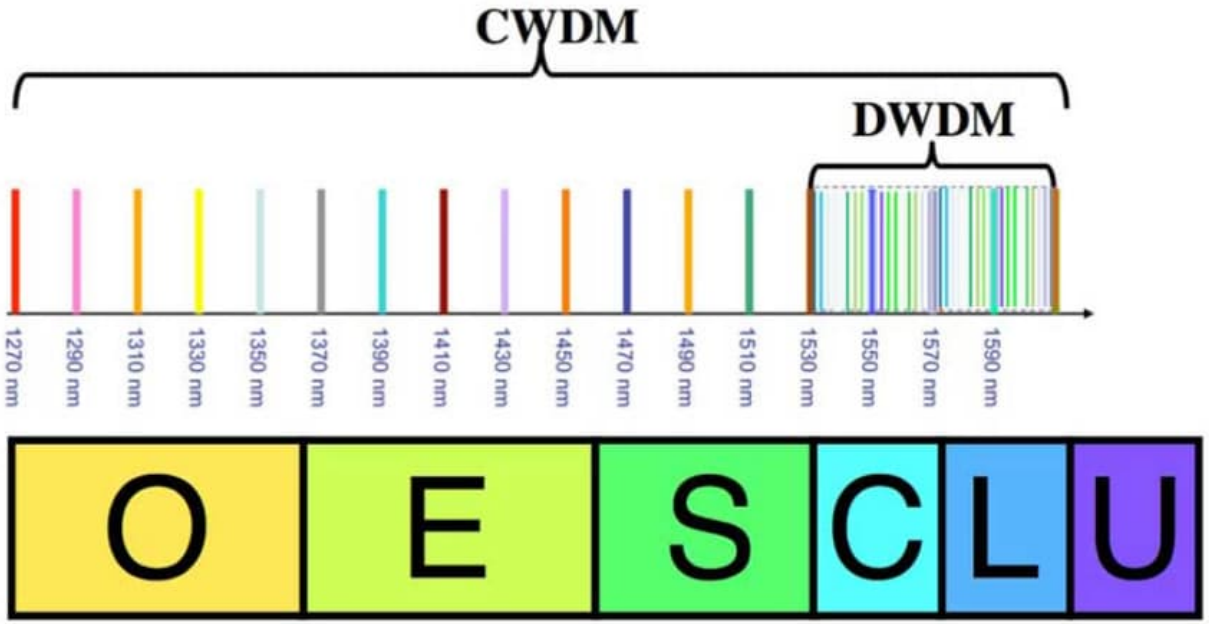
DWDM Dense Wavelength-Division Multiplexing
UAV Unmanned Aerial Vehicle
WDM Wavelength-Division Multiplexing

telecom (D)WDM multimode glasvezeltechnologie



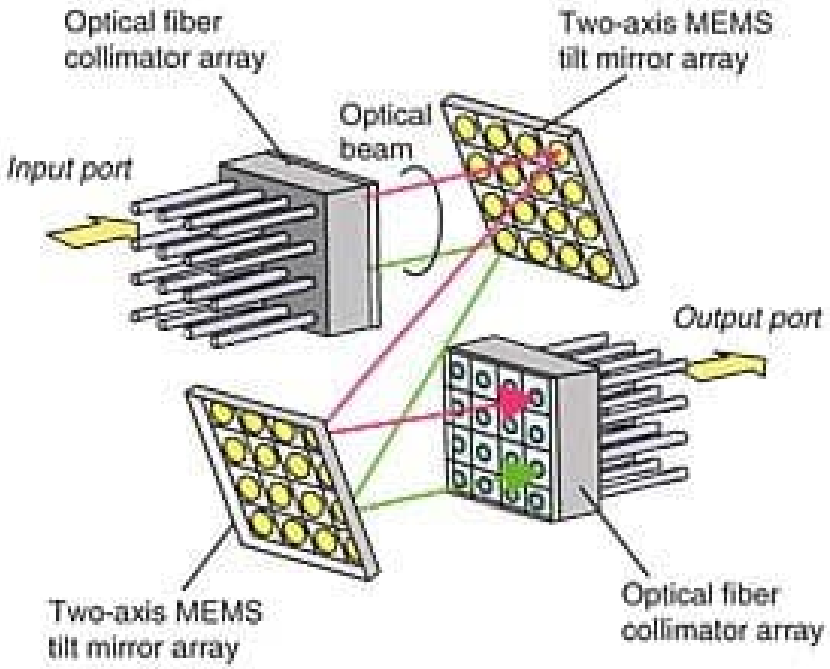


- **Meerdere (~ 16 – 160) kanalen in 1 glasvezel mogelijk**
- **Versterking met OA's: elke 70 – 120 km**



CWDM	Course Wavelength Division Multiplexing
DEMUX	Demultiplexer
DWDM	Dense Wavelength Division Multiplexing
IR	Infrared
MUX	Multiplexer
nm	nanometre
OA	Optical Amplifier
OADM	Optical Add/Drop Multiplexer
UV	Ultraviolet
WDM	Wavelength Division Multiplexing

photonic switch technologie



How Google uses mirrors to dynamically reconfigure its networks

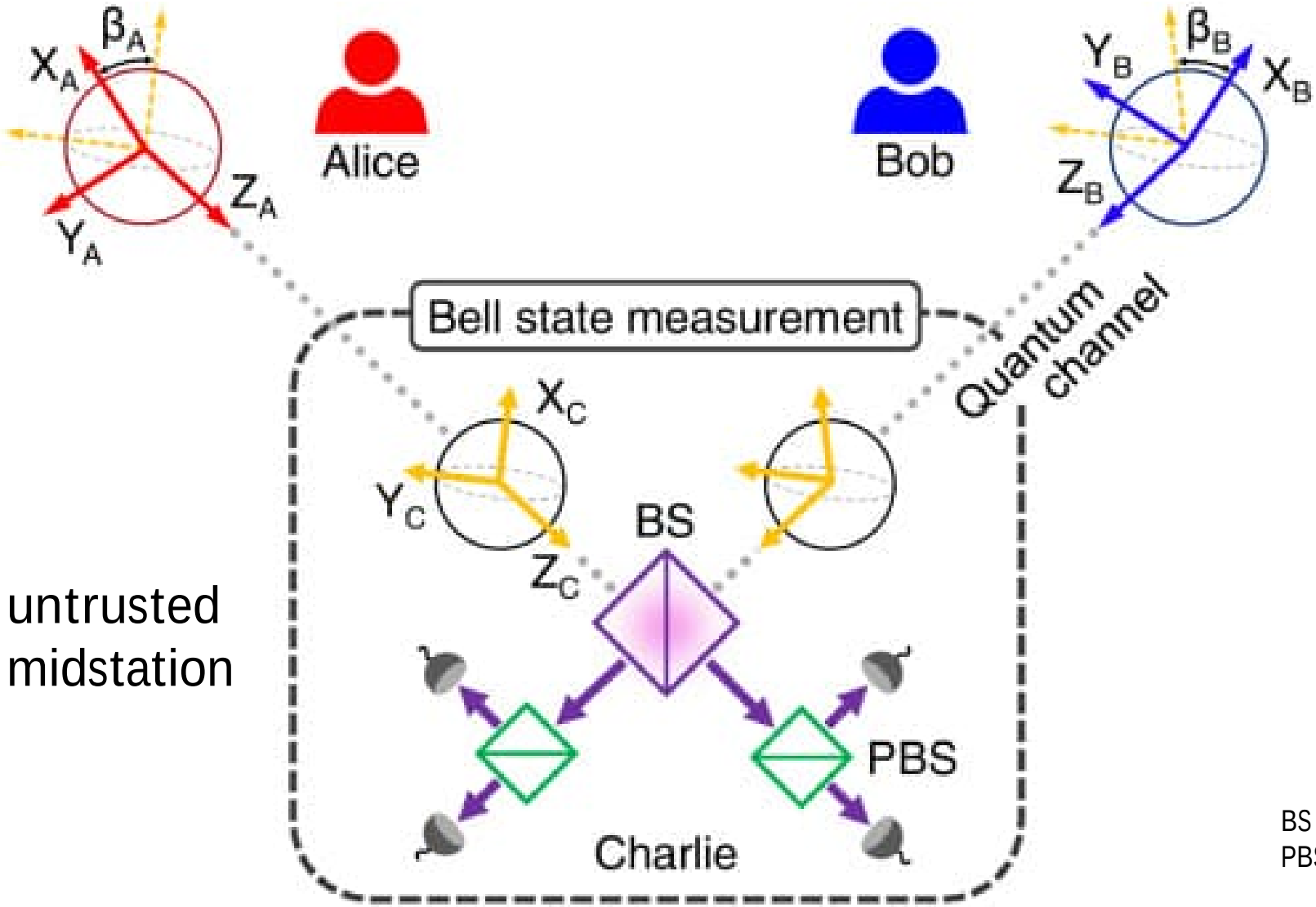
Tiny electromechanical units bounce traffic down different fibers

Simon Sharwood — Wed 24 Aug 2022 // 11:33 UTC

Google has scaled its network capacity from over one petabit per second to beyond six petabits per second since 2015, and some of that growth has come from switches that bounce optical signals off an array of mirrors to redirect traffic.

MEMS Micro-Electro-Mechanical Systems

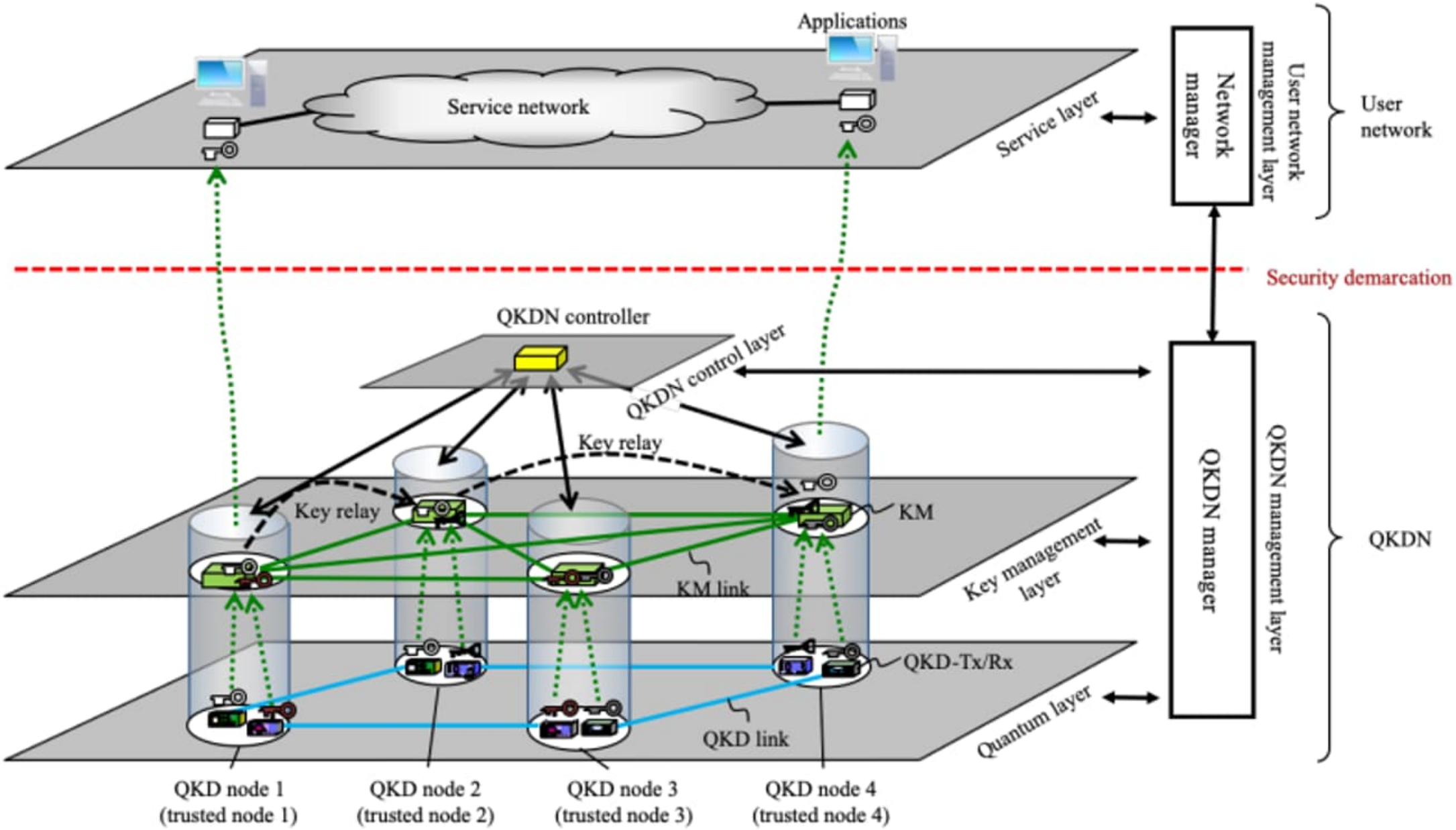
Measurement Device-Independent QKD (MDI-QKD)



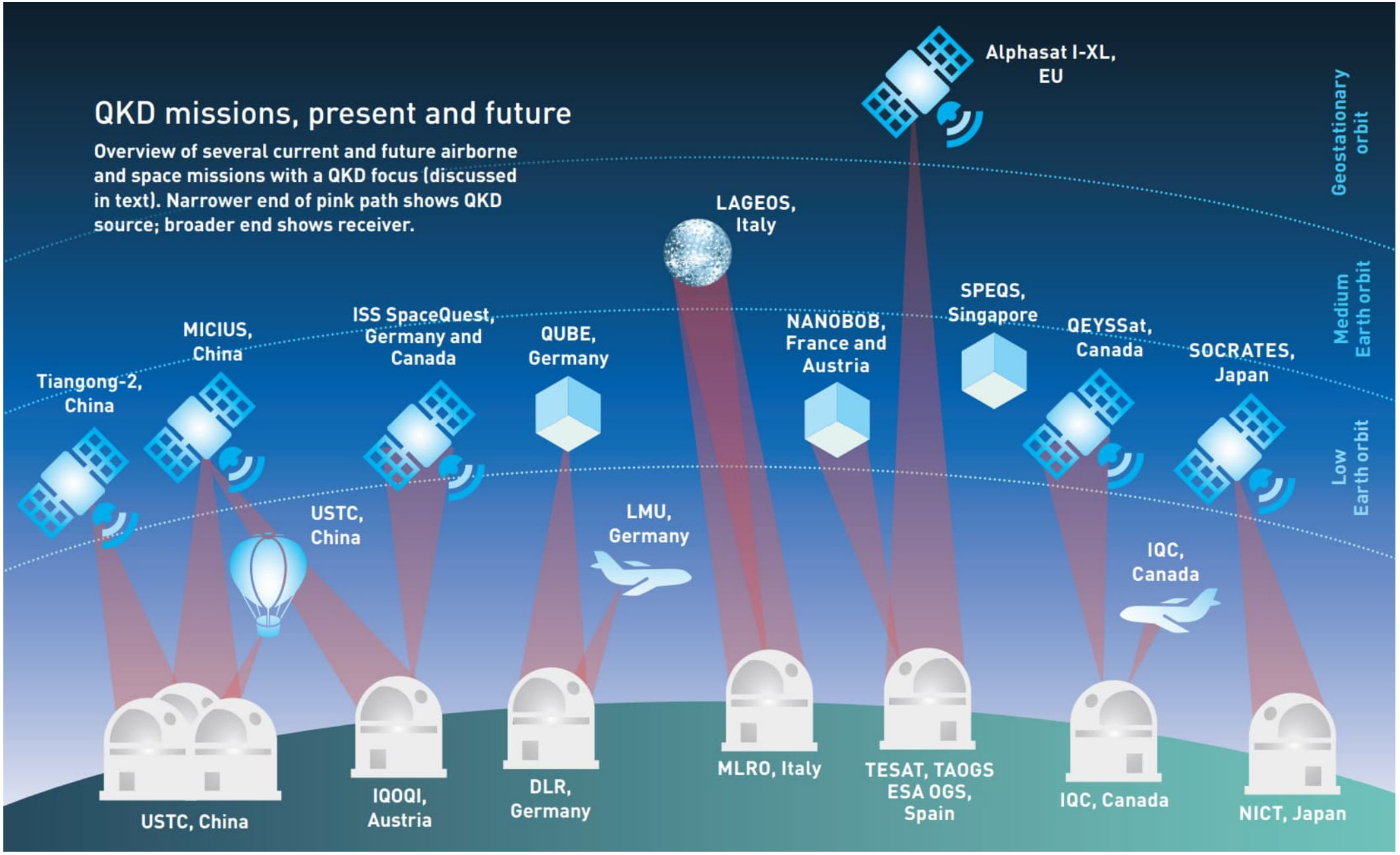
untrusted midstation

BS Beam Splitter
PBS Polarizing Beam Splitter

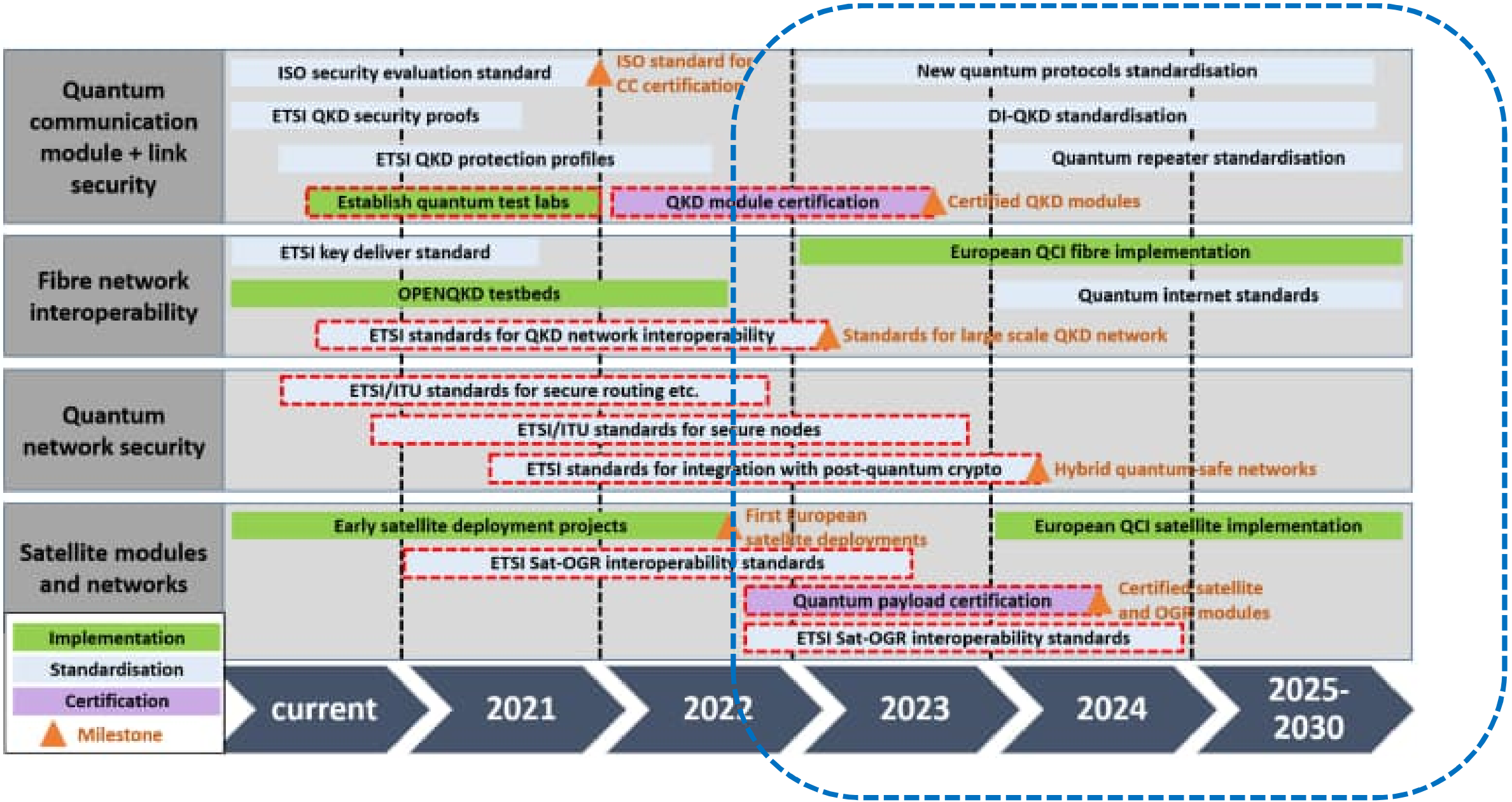
QKDN netwerkarchitectuur



satelliet QKD

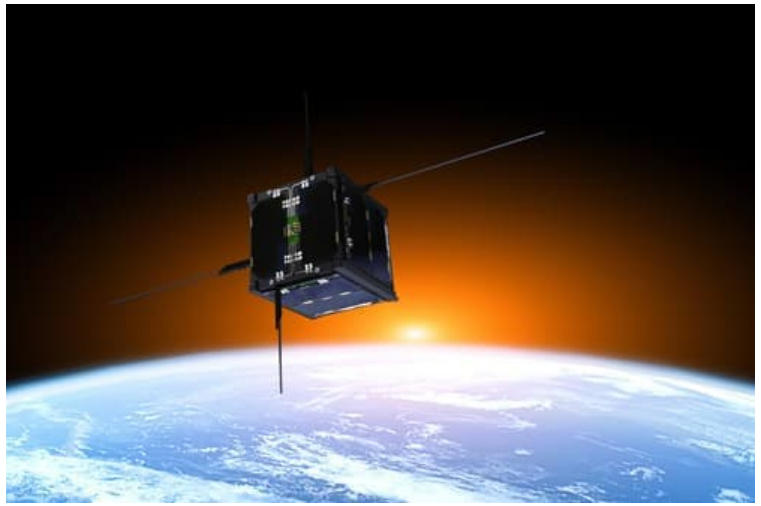


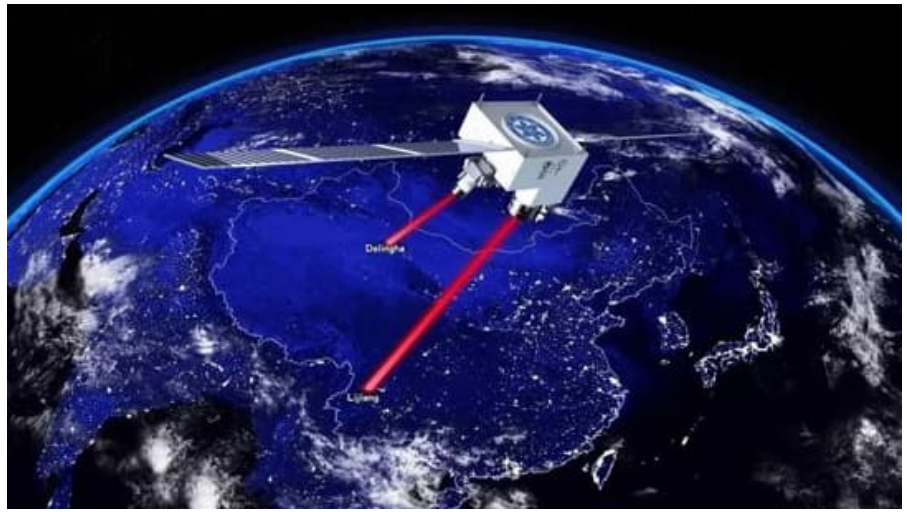
QKD(N) standards roadmap

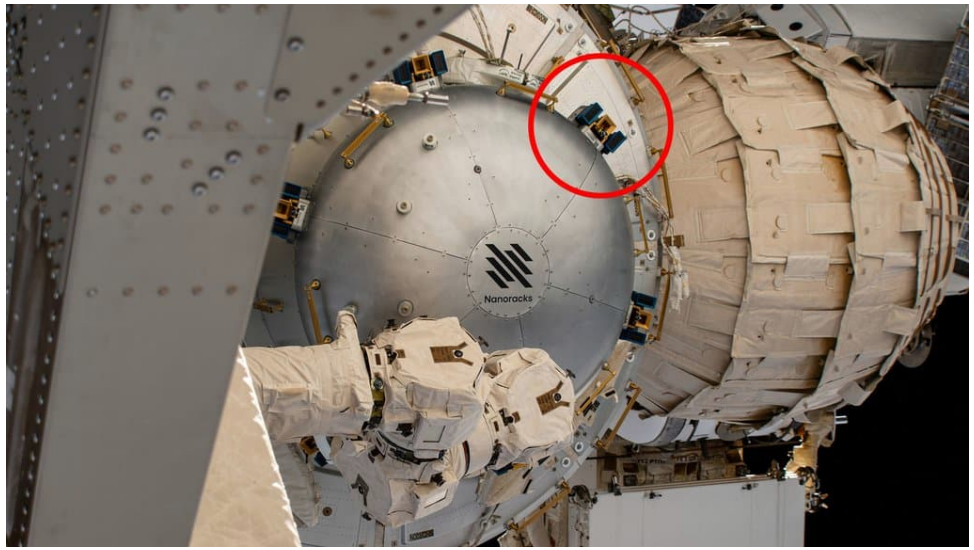


voorbeelden van QKD modules

satelliet QKD modules







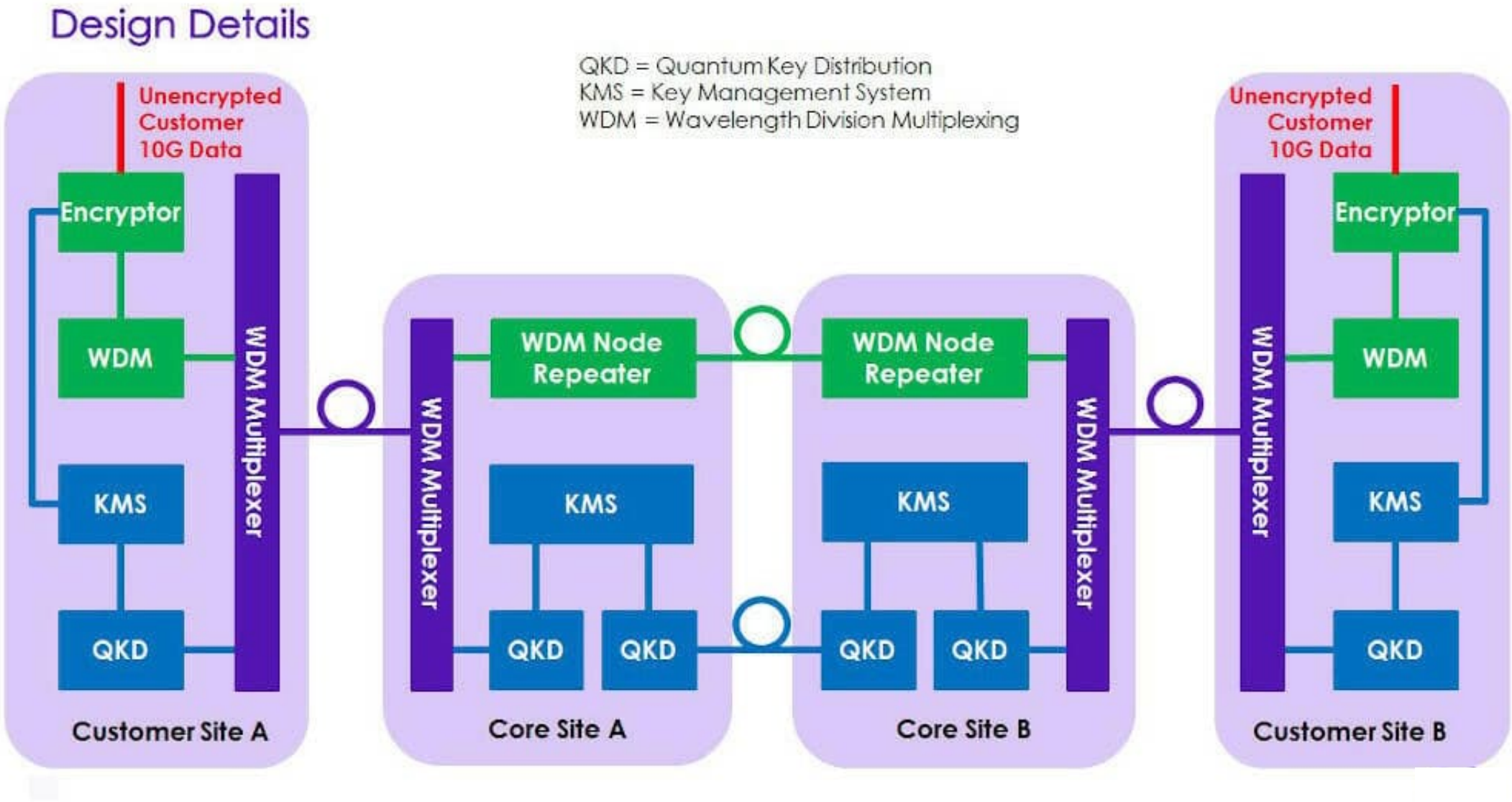
voorbeelden van QKD(N) producten en diensten (1)

- ADVA: FSP 3000 platform
- AegiQ: QKD componenten
- Aliro Quantum: Alironet
- Altice Portugal: QKDaaS (i.s.m. met ID Quantique)
- Arqit: QuantumCloud (“QKD with a twist”)
- BasejumpQDN: software voor QKDN netwerken
- British Telecom (BT): London metro QKDN netwerk (i.s.m. Toshiba)
- Chicago area QKDN netwerk
- DARPA Quantum Network
- Eagle-1 LEO QKD system
- Haven van Rotterdam QKD netwerk: MDI-QKD technologie van Q*Bird (QuTech spin-off)
- ID Quantique: Clavis XG, Clavis^{300}, Cerberis XG, Cerberis^{3} en XGR Series

  (150/200/250 k€ voor 2 apparaten, 40/80/120 km maximaal)

DARPA Defense Advanced Research Projects Agency
LEO Low Earth Orbit
QKDaaS QKD-as-a-Service

BT's London Metropolitan QKDN



QKD netwerk Haven Rotterdam

Haven Rotterdam is aangesloten op quantumnetwerk

Een aantal bedrijven in de Rotterdamse haven is aangesloten op het quantumnetwerk van Q*Bird. Dat bedrijf komt voort uit QuTech, een samenwerkingsverband van de TU Delft en de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek.

In een verklaring van de TU Delft claimt Q*Bird de eerste te zijn die een beveiligd quantumnetwerk van een nieuw type inzet om via een centrale hub meerdere gebruikers te verbinden. Dit zorgt voor een onaftapbare internetverbinding tussen meerdere gebruikers, verspreid over het hele havengebied, meldt de universiteit.

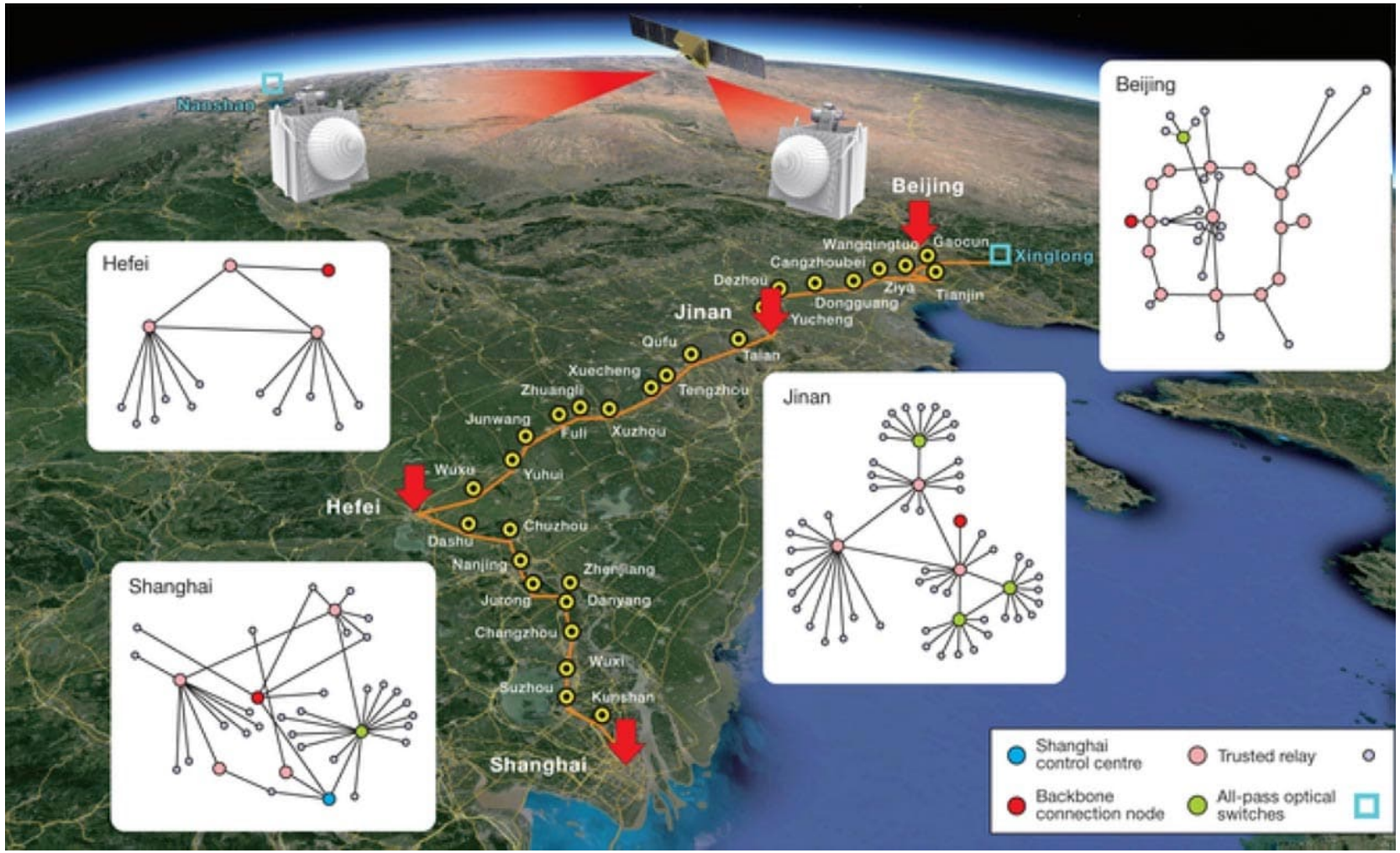
Een klein aantal bedrijven, waaronder Havenbedrijf Rotterdam en Portbase, test en gebruikt het quantumnetwerk. De centrale computer voor de distributie van quantumsleutels staat bij het Havenbedrijf Rotterdam. Met de sleutels kan Q*Bird meerdere gebruikers aansluiten op het netwerk. Wanneer een derde partij de sleutels probeert te stelen, informeert het systeem de gebruikers dat de sleutels gecompromitteerd kunnen zijn. Het systeem maakt dan een andere set sleutels aan om verdere berichten veilig te versleutelen. Uiteindelijk is het de bedoeling dat meer bedrijven en partijen gebruik gaan maken van het quantumnetwerk. Wanneer Q*Bird het aantal gebruikers uitbreidt, is nog niet duidelijk.

voorbeelden van QKD(N) producten en diensten (2)

- JPMorgan, Ciena en Toshiba: QKDN metro netwerk
- Keequant: Andariel QKD
- Ki3 Photonics: QKD componenten
- KETS Quantum Security: DLK DX
- Lijan 1 raketlancering: satellieten met micro-QKD
- LUQCIA QKDN netwerk
- LuxQuanta: CV-QKD systems
- MagiQ: MagiQ QPN (BB84 QKD)
- Mt Pelerin: Quantum Vault (i.s.m. ID Quantique)
- NASA: SEAQUE QKD (ISS)
- Nationaal QKDN netwerk van China
- NATO: NCSC VPN
- NLPQT: QKDN netwerk (i.s.m. ID Quantique)

ISS International Space Station
NCSC NATO Cyber Security Centre
VPN Virtual Private Network

het grootste QKD netwerk ter wereld



de stand van zaken begin 2021:

- een glasvezel QKDN netwerk met 32 trusted relays (2.000 km totale lengte)
- QKD satellietverbindingen (Micius) met 2 grondstations, in Oost-Beijing en bij de grens met Kazakstan (2.600 km apart)
- 4 QMAN's (Beijing, Jinan, Hefei en Shanghai) met trusted relays en optical switches (het Jinan QMAN heeft 95 user nodes)
- in totaal 700 QKD glasvezelverbindingen
- een netwerkbeheercenter in Shanghai
- in totaal 150 QKD user nodes
  - datacenters
  - financiële instellingen en toezichthouders
  - nieuwsagentschappen
  - etc.
- diverse "use cases"
  - IPsec VPN
  - met AES versleutelde spraak en video
  - etc.

AES Advanced Encryption Standard
IP Internet Protocol
Ipsec IP security
QMAN Quantum Metropolitan Area Network
VPN Virtual Private Network

voorbeelden van QKD(N) producten en diensten (3)

- NQSN: QKDN netwerk
- nodeQ: software voor QKDN netwerken
- ORNL (DoE): QLAN testbed
- QEYnet: micro-satelliet QKDN netwerk
- QNF: metro QKDN netwerk (New York)
- QNU Labs: QKDN netwerk
- QuantLR: QKD software (voor bestaande typen QKD modules)
- Quantum CTek: QKD platform
- Quantum Trilogy: Quantum Trilogy Platform
- Quantum Xchange: QKDN netwerk
- Qubitekk: Quantum Network Essentials Platform
- Quintessence Labs: qOptica QKD

DoE Department of Energy
ORNL Oak Ridge National Laboratory
QLAN Quantum Local Area Network

voorbeelden van QKD(N) producten en diensten (4)

- Qunnect: QKDN componenten
- QuTech/Juniper Networks/Eurofiber: QKDN testbed
- SECOQC: QKDN netwerk
- SKT: QKDN netwerk (i.s.m. ID Quantique)
- South Korea Gangwon-do provincie: drone QKDN netwerk
- Space Hellas: QKDN netwerk
- Spectral/RAL Space: Spectral-1 satelliet
- Swissquantum: QKDN network (i.s.m. ID Quantique)
- Surrey Satellite Technology: satelliet QKD
- Terra Quantum: QKDN netwerk
- ThinkQUANTUM: QUKY
- Tiangong-2 Space Lab: compact QKD

Terra Quantum: QKD "quantelaers" ?

Long-distance quantum key distribution based on the physical loss control

N. S. Kirsanov, N. R. Kenbaev, A. B. Sagingalieva, D. A. Kronberg, V. M. Vinokur, G. B. Lesovik

Terra Quantum AG, St. Gallerstrasse 16A, CH-9400 Rorschach, Switzerland

May 4, 2021

Abstract

Existing quantum cryptography is resistant against secrecy-breaking quantum computers but suffers fast decay of the signal at long distances. The various types of repeaters of propagating quantum states have been developed to meet the challenge, but the problem is far from being solved. We step in the breach and put forth long-distance high secrecy optical cryptography, creating the fast quantum key distribution over distances up to 40,000 kilometers. The key element of the proposed protocol is the physical control over the transmission line.

voorbeelden van QKD(N) producten en diensten (5)

- Toshiba:
  - Long Distance QKD System (tot 120 km)
  - Multiplexed QKD System (tot 70 km)
- UKQN: QKDN network (i.s.m. ID Quantique en Toshiba)
- US DoD: drone-based QKDN netwerk
- US Navy: Washington area QKDN netwerk
- VeriQloud: Qline quantum Ethernet
- XT Quantech: CVQ KD-101

QKD(N) heel kort samengevat

- ten eerste, in specifieke situaties kan QKD(N) mogelijk een bijdrage leveren aan de informatiebeveiliging (inclusief quantum-resistentie)

- ten tweede, de gebruiksmogelijkheden voor QKD(N) zijn beperkt

- ten derde, kijk heel goed uit bij de aanschaf van QKD(N) producten of bij het gebruik van QKD(N) diensten:

  eis dat bewijs wordt geleverd ter ondersteuning van de “volkomen veilig op basis van kwantummechanische principes” claims van de leveranciers

quantum-resistente cryptografie

quantum-resistente cryptografie

- eerste helft 1980'er jaren: eerste ideeën voor kwantumcomputers
- 1994: Peter Schor's kwantumalgoritmes → belangstelling voor quantum-resistente crypto algo's
  - hash-based: vanaf 1979 (Ralph Merkle/Leslie Lamport)

    pre-PQC: LMS (Leighton-Micali Signatures) en XMSS (eXtended Merkle Signature Scheme)
  - code-based: vanaf 1979 (Robert McEliece)
  - lattice-based: vanaf 1996 (Miklós Ajtai)
  - multivariate-based: vanaf 1988 (Jacques Patarin)
  - ~~isogeny-based: vanaf 2011 (David Jao en Luca De Feo)~~
  - overige: bv. Picnic digital signature algoritme (Microsoft et al)
- 2006: PQCrypto – eerste internationale workshop
- 2015: NSA komt met een grote verrassing:
  ~~"Suite B" algoritmes~~ → quantum-resistente crypto algoritmes

NSA National Security Agency

Post-Quantum Cryptography (PQC)

2016: NIST start Post-Quantum Cryptography (PQC) “competitie”

- in scope zijn Key Encapsulation Mechanisms (KEMs) en digital signature schemes
- 82 PQC voorstellen worden ingediend, waarvan er 69 worden geaccepteerd
- na de 3de ronde annonceert NIST in juli 2022 de standaardisatie van
  - lattice-based CRYSTALS-Kyber KEM
  - lattice-based CRYSTALS-Dilithium digsig
  - lattice-based FALCON digsig
  - hash-based SPHINCS+ digsig
- code-based BIKE KEM, code-based Classic McEliece KEM, code-based HQC KEM ~~en isogeny-based SIKE KEM~~ gaan door naar de 4de ronde
- in december 2022 zal NIST een minder omvangrijke “competitie” starten voor digsig PQC voorstellen anders dan lattice-based
- NIST’s PQC inspanningen zullen nog vele jaren doorgaan

BIKE Bit Flipping Key Encapsulation
CRYSTALS Cryptographic Suite for Algebraic Lattices
FALCON Fast Fourier Lattice-based Compact Signatures over NTRU
HQC Hamming Quasi-Cyclic
NTRU N-th Degree Truncated Polynomial Ring Units
SIKE Supersingular Isogeny Key Encapsulation

CRYSTALS-Kyber en CRYSTALS-Dilithium

In Star Wars worden kyberkristallen gebruikt voor het vervaardigen van lichtgevende sabels.

In Star Trek worden dilithiumkristallen in massa/anti-massa reactoren gebruikt. In ons universum is dilithium (Li_2) een molecule die uit twee lithiumatomen bestaat.

CRYSTALS PQC (sub)project

Institutions involved in the design of Kyber and Dilithium:

NSA achterdeurtje in 2007 NIST Dual_EC_DRBG standaard (in 2013 aan het licht gebracht door Edward Snowden)

Dual_EC_DRBG Dual Elliptic Curve Deterministic Random Bit Generator

PQC issues

- performance en/of lengte van cryptosleutels en/of digitale handtekeningen van PQC algoritmes is anders dan voor bestaande asymmetrische algoritmes (vaak nadelig)

  ⇩

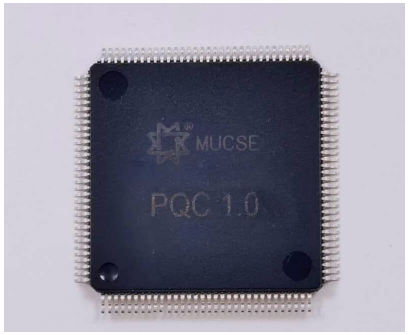
  (significante) impact op security protocollen zoals bijvoorbeeld TLS en IKE
  en op “resource-constrained” IT-platformen zoals bijvoorbeeld IoT

- PQC algoritmes zijn veel minder op de proef gesteld door de crypto community dan bestaande asymmetrische algoritmes

- nog geen overeenstemming inzake (geclaimde) patentrechten

IKE Internet Key Exchange
IoT Internet of Things
TLS Transport Layer Security

PQC implementaties



voorbeelden van PQC producten en diensten (1)

- 01 Communique Laboratory: quantum-safe blockchain
- ADVA: FSP 3000 platform ConnectGuard
- Algurand Foundation: blockchain (FALCON)
- Alternatio: PQC IP core for chipsets
- Amazon Web Services (AWS):
  - AWS Key Management Server (KMS)
  - AWS Certificate Manager (ACM)
  - AWS Secrets Manager (voor TLS endpoints)

  hybride oplossing met CRYSTALS-Kyber, BIKE en ~~SIKE~~
- Cloudflare:
  - CRYSTALS-Kyber hybride oplossing
  - PQC algo's in CIRCL crypto library

BIKE	Bit Flipping Key Encapsulation
CICRL	Cloudflare Interoperable, Reusable Cryptographic Library
CRYSTALS	Cryptographic Suite for Algebraic Lattices
FALCON	Fast Fourier Lattice-based Compact Signatures over NTRU
IP	Intellectual Property
NTRU	N-th Degree Truncated Polynomial Ring Units
SIKE	Supersingular Isogeny Key Encapsulation
TLS	Transport Layer Security

Algorand's FALCON digsig implementation

Algorand leads quantum-proof technology with development of Falcon

John Woods, CTO at the Algorand Foundation, said Falcon signatures will roll out across several applications starting with "State Proofs."

Samuel Wan

Aug. 18, 2022 at 2:00 pm UTC

2 min read

Updated: August 18, 2022 at 3:56 pm

COVER ART/ILLUSTRATION VIA CRYPTOSLATE

FALCON Fast Fourier Lattice-based Compact Signatures over NTRU
NTRU N-th Degree Truncated Polynomial Ring Units

Cloudflare's CIRCL crypto library PQC algo's

Post Quantum Key Exchange with CIRCL

- **SIDH using Cloudflare**. SIDH. Post-quantum key exchange.
- **SIKE Secret Shares with Go**. SIKE. Post-quantum key exchange with key encapulation.
- **CSIDH Go**. CSIDH. Post-quantum key exchange.
- **Kyber Key Exchange**. Kyber. In this case we will implement Kyber512, Kyber738 and Kyber1024, in order to create a quantum-robust key exchange.
- **SIKE Key Exchange**. SIKE. Supersingular Isogeny Key Encapsulation (SIKE) is a post-quantum cryptography key encapsulation method for key exchange, and is based on Supersingular Isogeny Diffie-Hellman (SIDH). In this case we will implement Kyber512, Kyber738 and Kyber1024, in order to create a quantum-robust key exchange. In this case we will implement SIKEp434, SIKEp503 and SIKEp751.
- **Kyber, SIKE and Hybrid Key Exchange**. Hybrid. Two popular PQC key exchange methods are SIKE and Kyber. In order to improve the performance of PQC key exchange, we can create a hybrid model and use X25519 and X488. In this case we will use Kyber512-X25519, Kyber768-X448 and Kyber1024-X448, and which uses X25519 and X448 key exchange methods. The key size for this change a little, and where Kyber512 produces an 800 byte public key, and with 832 bytes for Kyber512-X25519.
- **Frodo**. Frodo. Frodo KEM is based on the learning with errors (LWE) problem, and has a number of levels: FrodoKEM-640 (Level 1, equivalent in security to AES-128), FrodoKEM-976 (Level 3, equivalent in security to AES-192), and FrodoKEM-1344 (Level 5, equivalent in security to AES-256). There are two main variants of these for FrodoKEM-X-AES and FrodoKEM-X-SHAKE. The -AES version has hardware acceleration for AES, and can run faster on processors that support hardware acceleration for AES, while the -SHAKE version is faster on systems that do not support this. For FrodoKEM-640-SHAKE, we can see that the size of Alice's public key is 9,616 bytes long, and her private key is 19,888 bytes long. The ciphertext passed is 9,270 bytes long.

Post Quantum Digital Signatures with CIRCL

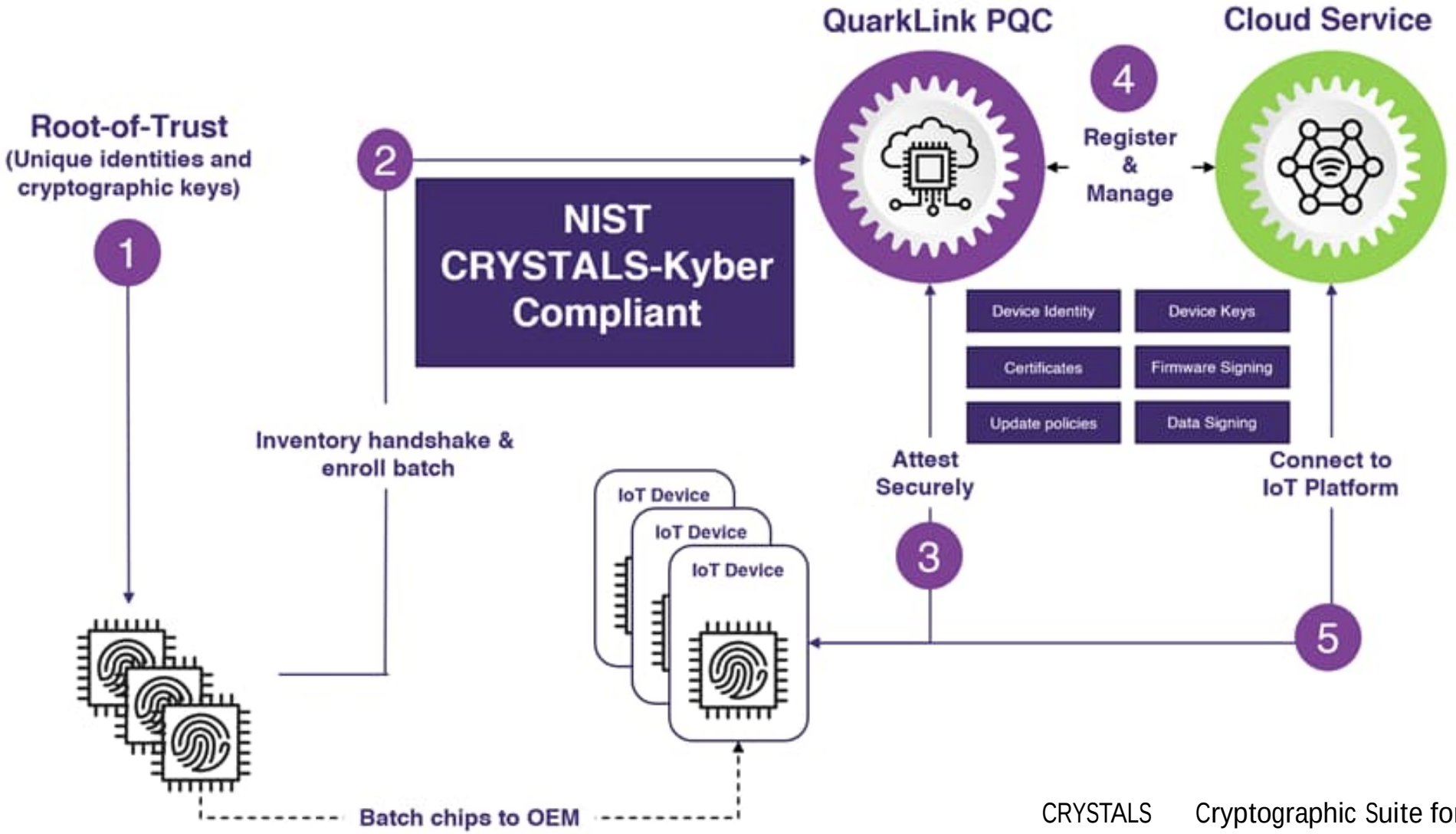
- **CRYSTALS Dilithium**. Dilithium. CRYSTALS Dilithium uses lattice-based Fiat-Shamir schemes, and produces one of the smallest signatures of all the post-quantum methods, and with relatively small public and private key sizes. The three main implementations for the parameters used are: Dilithium 2, Dilithium 3 and Dilithium 5. Overall, Dilithium 3 is equivalent to a 128-bit signature, and is perhaps the starting point for an implementation This page implements Dilithium 2, Dilithium 3 and Dilithium 5 using the Cloudflare CIRCL library.

voorbeelden van PQC producten en diensten (2)

- CryptoExperts:
  - crypto libraries
  - cryptographic product review
- Crypto Quantique: QuarkLink PQC IoT platform (CRYSTALS-Kyber)
- CryptoNext Security SAS: messaging voor mobiele communicatie (Frodo-KEM, CRYSTALS-Kyber en –Dilithium)
- CRYPTO4A: Hybrid Security Platform
- CryptoMathic: Crypto Service Gateway
- Cyph: Quantum-Resistant Cryptographic Platform
- Dencrypt: Dencrypt Communication Solution
- Entrust: SDK voor nShield HSM
- evolutionQ: Quantum-safe Product Verification Service

CRYSTALS	Cryptographic Suite for Algebraic Lattices
HSM	Hardware Security Module
IoT	Internet of Things
KEM	Key Exchange Mechanism
SDK	Software Development Kit

Crypto Quantique's QuarkLink IoT PQC platform



CRYSTALS	Cryptographic Suite for Algebraic Lattices
OEM	Original Equipment Manufacturer
IoT	Internet of Things

voorbeelden van PQC producten en diensten (3)

- GoQuantum:
  - VPN gateway
  - USB token
- Hub Security: Quantum Secured Cloud Workspace (PQC algoritmes)
- International Business machines (IBM):
  - z16 mainframe met ingebouwde HSM (CRYSTALS-Kyber en –Dilithium)
  - quantum-safe tape drive (CRYSTALS-Kyber en –Dilithium)
- infotecs: ViPNet
- Life's Good (LG) Uplus: PQC service
- MUCSE: PQC 1.0 chip (CRYSTALS-Kyber en –Dilithium)
- NXP Semiconductors: S32G vehicle network processor (CRYSTALS-Dilithium secure boot)

CRYSTALS	Cryptographic Suite for Algebraic Lattices
HSM	Hardware Security Module
USB	Universal Serial Bus
VPN	Virtual Private Network

IBM's z16 mainframe met ingebouwd CEX8S HSM

IBM

Prepare for the next era of computing with quantum-safe cryptography on IBM z16

CEX8S CryptoExpress8S
HSM Hardware Security Module

Redbooks
ibm.com/redbooks

Transitioning to Quantum-Safe Cryptography on IBM Z

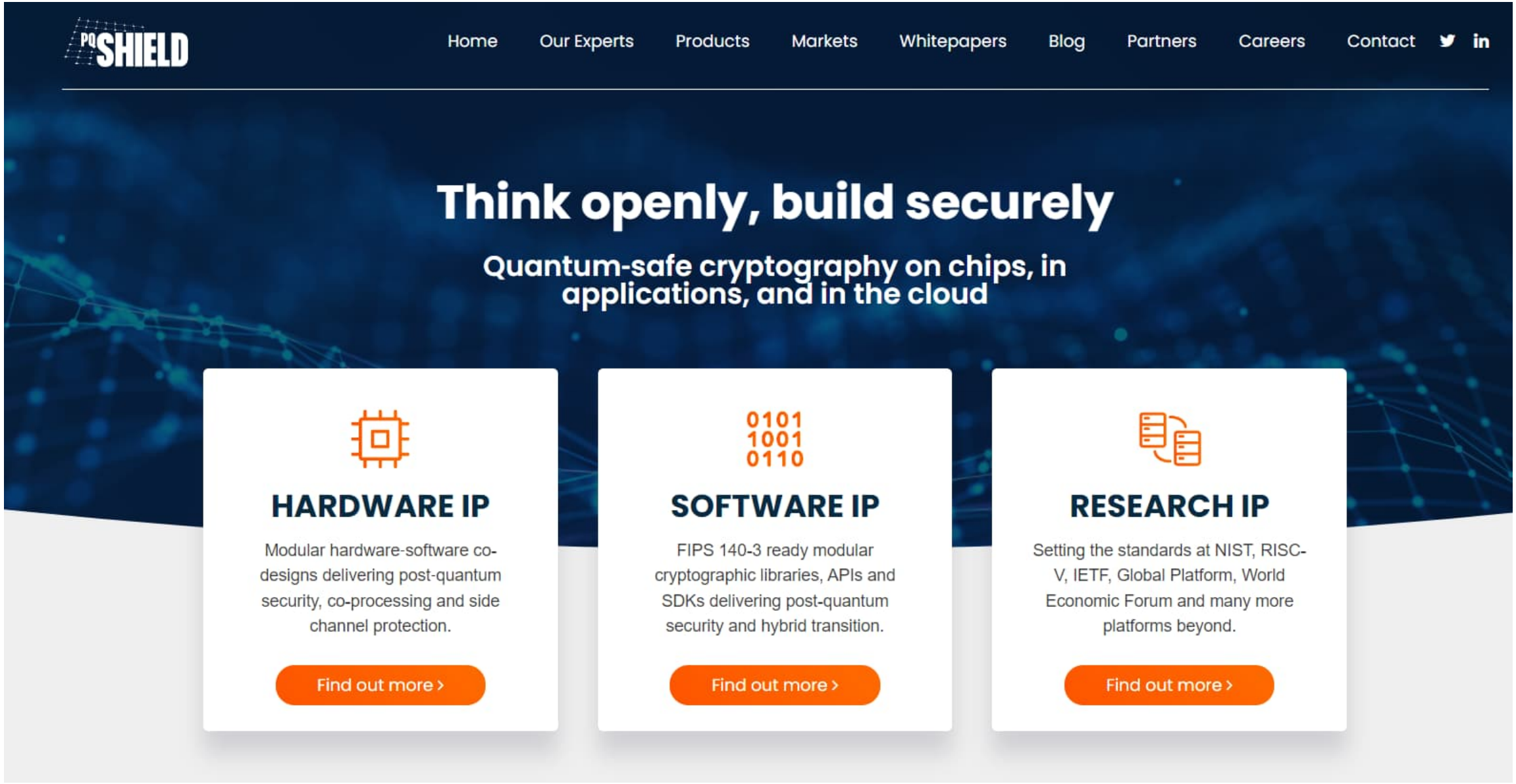
voorbeelden van PQC producten en diensten (4)

- OpenSSH library versie 9.0: NTRU-Prime default algoritme
- Patero: CryptoQOR (hybride oplossing)
- Post-Quantum: Quantum-Safe Platform
- PQSecure Technologies:
  - Suite-Q HW (ASIC en FPGA)
  - Suite-Q SW (assembler en C)
- PQShield: PQC Crypto Lib, inclusief CRYSTALS-Kyber en –Dilithium

  (FIPS 140-3 certificatie in gang gezet)
- PureVPN: VPN service
- QANplatform: quantum-proof blockchain

ASIC	Application-Specific Integrated Circuit
CRYSTALS	Cryptographic Suite for Algebraic Lattices
FIPS	Federal Information Processing Standards
FPGA	Field-Programmable Gate Array
HW	Hardware
NTRU	N-th Degree Truncated Polynomial Ring Units
SSH	Secure SHell
SW	Software
VPN	Virtual Private Network

PQShield's PQC Crypto Lib



voorbeelden van PQC producten en diensten (5)

- Quanticor Security:
  - Quantum Idencrypt (IoT)
  - Quantum Secure Endpoint Security
  - Quantum Cloud Security
  - Q-PKI
  - Quantum-Multisign
  - Quantum blockchain for IoT
  - (Q)-TLS Proxy Load-balancer
  - Q-VPN
- Quantropi: True QiSpace SaaS platform
- Quantum Collective: PQC Safety Solutions and Services
- Quantum Xchange: Phio TX/QuantumXC

IoT Internet of Things
PKI Public Key Infrastructure
SaaS Software-as-a-Service
TLS Transport Layer Security
VPN Virtual Private Network

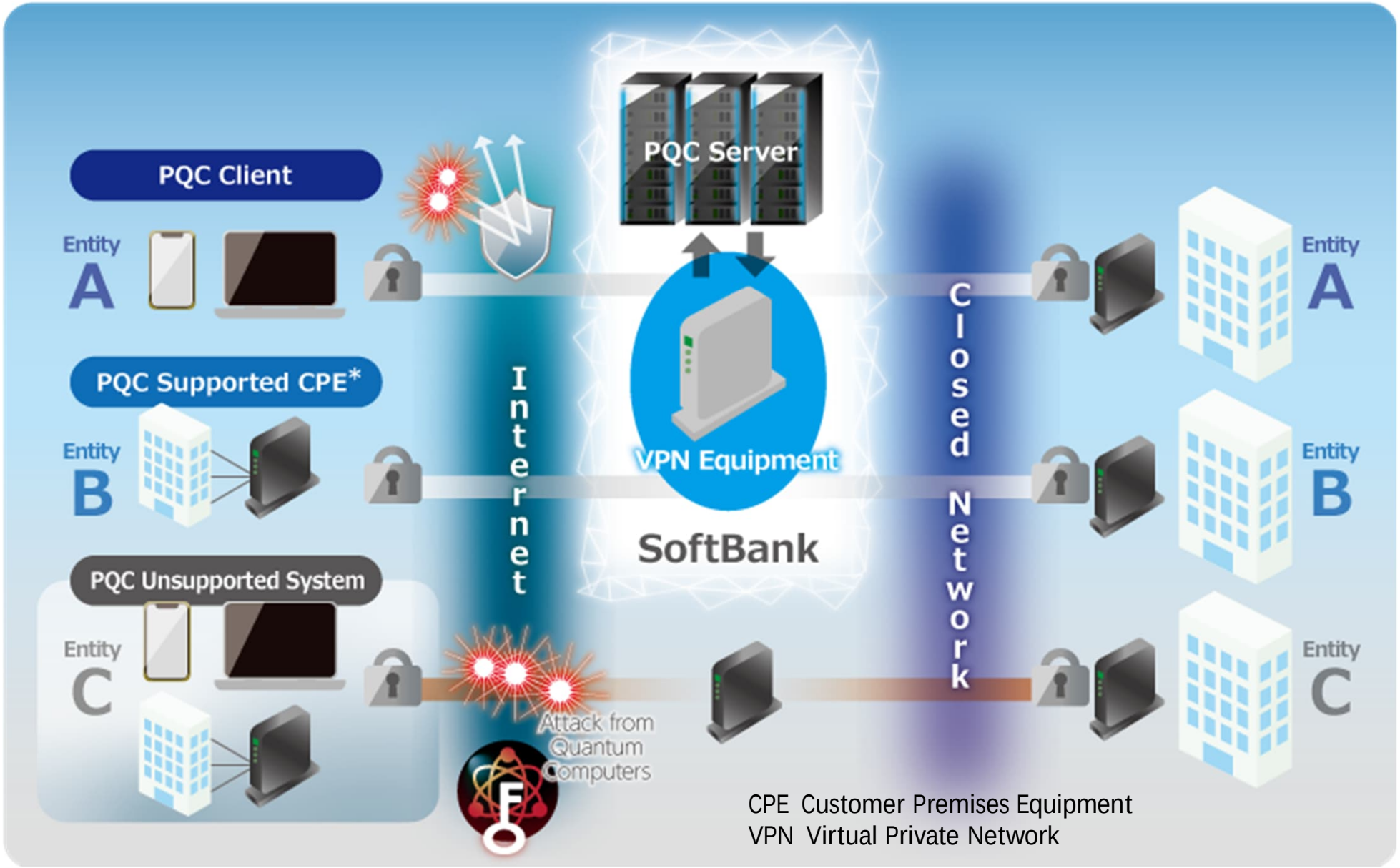
Quantum Collective

voorbeelden van PQC producten en diensten (6)

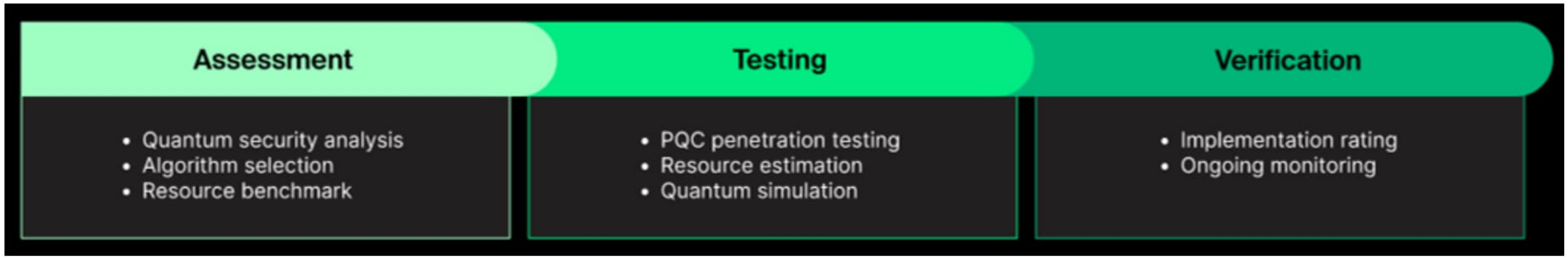
- QuSecure: QuProtect (QaaS)
- SandboxAQ: SecuritySuite
- SKT: VPN infrastructuur (CRYSTALS-Kyber en –Dilithium)
- SoftBank: PQC netwerkinfrastructuur (i.s.m. SandboxAQ)
- SSH Communications Security: NQX, Tectra Quantum Safe Edition (SSH)
- Synergy Quantum: SQ27 Post-Quantum Encryption chip
- Utimaco: Q-safe (t.b.v. quantum-resistente crypto infrastructuur)
- WiseKey International: Secure Semiconductors MS600X (CRYSTALS-Kyber en –Dilithium)
- Xiphera: PQC IP cores voor ASIC en FPGA
- Zapata Computing: Quantum Resilience solution

ASIC	Application-Specific Integrated Circuit
CRYSTALS	Cryptographic Suite for Algebraic Lattices
FPGA	Field-Programmable Gate Array
IP	Intellectual Property
QaaS	Quantum-as-a-Service
SKT	South Korea Telecom
SSH	Secure SHell
VPN	Virtual Private Network

SoftBank's PQC netwerkinfrastructuur



Zapata Computing's 3-part Quantum Resilience Solution



quantum-resistente cryptografie heel kort samengevat

- ten eerste, ontwikkeling van quantum-resistente crypto algo's is nog volop gaande; de eerste standaarden zijn er op z'n vroegst in 2024

  (voor 4 PQC algo's, waarvan 3 digsig algo's en slechts 1 key exchange algo)

- ten tweede, het risico dat een crypto algo binnen enkele jaren wordt gekraakt is (aanzienlijk) groter voor de PQC algo's dan voor de conventionele crypto algo's

- ten derde, overgang naar PQC algo's kan (significante) impact hebben op de performance van diverse security protocollen

- ten vierde, implementeren van PQC algo's op ernstig "resource-constrained" IT-platformen kan (zeer) problematisch zijn

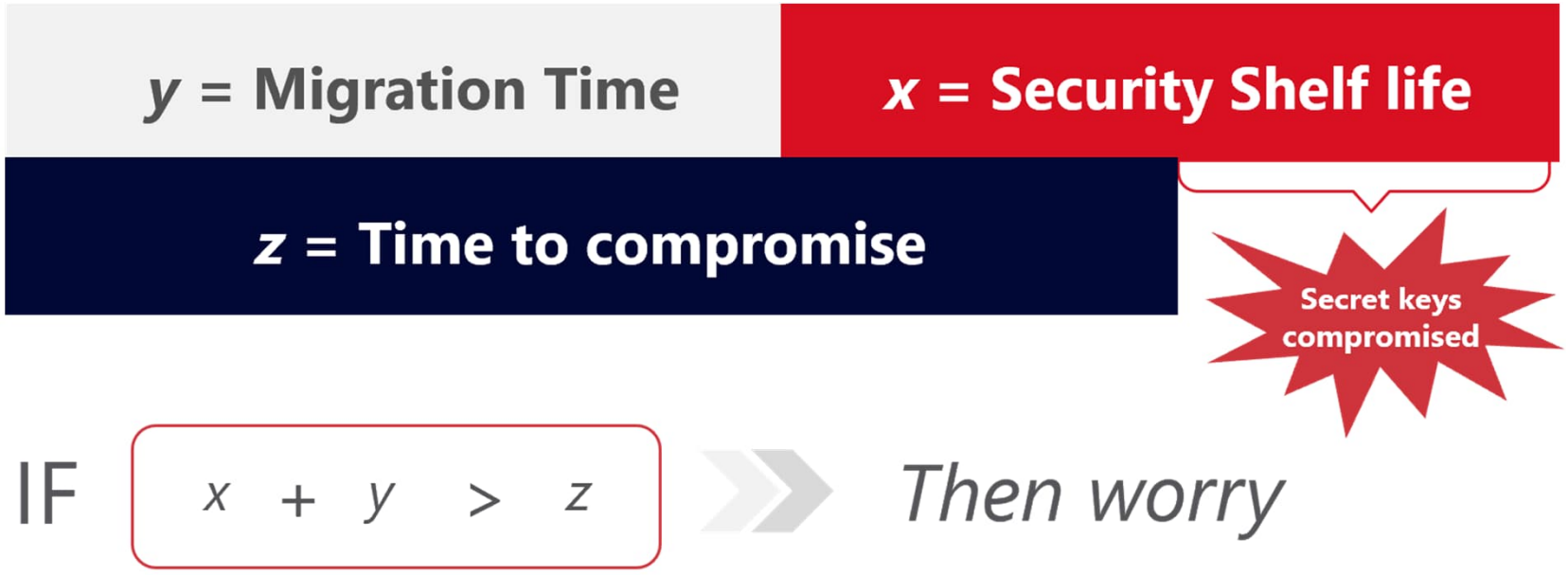
post-quantum migratie

tijdlijn post-quantum migratie

post-quantum migratie zal vele jaren in beslag nemen; dat geldt in het bijzonder als er meerdere partijen betrokken zijn, bijvoorbeeld

- PKI-infrastructuren
- het TLS ecosysteem
- betaalsystemen
- IoT platformen
- etc.

IoT Internet of Things
PKI Public Key Infrastructure
TLS Transport Layer Security



aandachtspunten voor de post-quantum migratie

- begin niet overhaast met het implementeren van PQC crypto
  - er zijn nog geen definitieve NIST standaarden (de eerste vier worden pas in 2024 verwacht)
  - IT-leveranciers, open-source communities en IT-service providers zijn nog niet gereed
  - security protocollen moeten nog worden aangepast voor PQC ondersteuning (TLS, IKE, etc.)
  - compliance eisen zullen nog worden aangepast (PCI, etc.)
  - krachtige fault-tolerant kwantumcomputers zijn er pas over … jaar

  maar risico van “store now, decrypt later” is er nú al !

IKE Internet Key Exchange
PCI Payment Card Industry
TLS Transport Layer Security

- begin nú met verzamelen van relevante informatie (inventarisatie)
  - wat zijn de gegevens waarvan de vertrouwelijkheid moet worden geborgd?
  - hoe lang moet de vertrouwelijkheid van deze gegevens worden geborgd?
  - welke cryptomechanismen worden hiervoor toegepast (inclusief relevante parameters)?
  - waar worden die cryptomechanismen gebruikt (IT-infrastructuur en applicaties)?
  - welke leveranciers, open-source communities en service-providers zijn hier bij betrokken?
  - welke van deze cryptomechanismen zijn kwetsbaar voor quantum computing aanvallen?
  - op welke wijze kunnen de geïnventariseerde kwetsbaarheden worden gemitigeerd?

voorbereiding van de toekomstige post-quantum migratie

- zorg voor voldoende bewustwording t.a.v. het belang van cryptografie voor informatiebeveiliging bij het management, bij de IT-afdeling en bij IT-auditors
- zorg voor voldoende bewustwording t.a.v. de quantum computing dreigingen
- volg de ontwikkelingen op het gebied van quantum computing, quantum security en Post-Quantum Cryptography (PQC)
- stel een team/kennisgroep samen die over de benodigde kennis beschikt of deze anders verwerft (eventueel i.s.m. met ter zake deskundige partners)
- verzamel informatie m.b.t. de plannen van relevante open-source communities
- overleg met IT-leveranciers en IT-dienstverleners (post-quantum roadmap)
- ontwikkel een strategie voor het adopteren en integreren van nieuwe cryptografische algoritmes in de eigen IT-infrastructuur en applicaties

  met aandacht voor crypto agility en crypto diversificatie

Australisch initiatief (qroegentocht)

post-quantum migratie scenario's (voor PKE crypto)

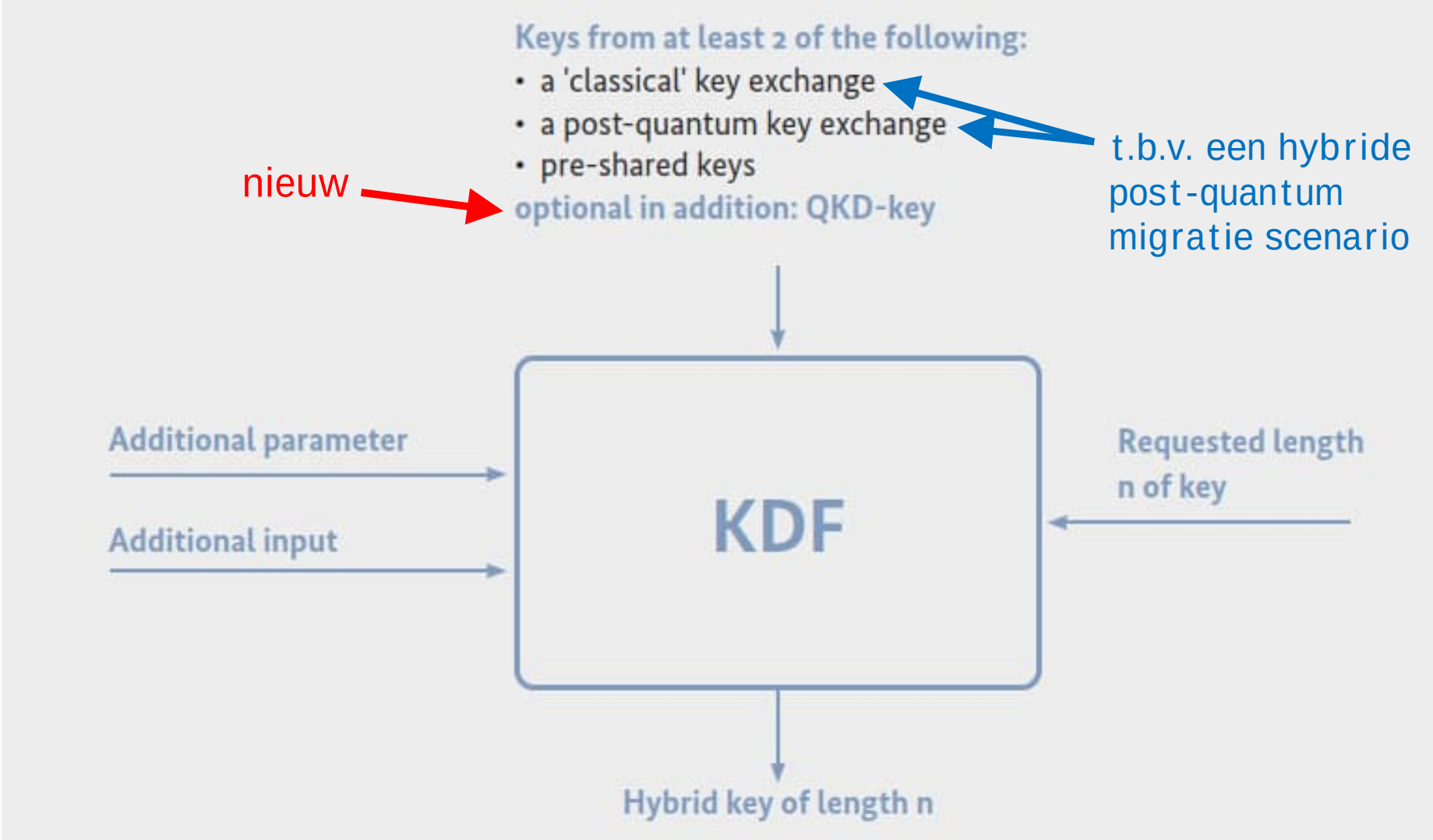
- isoleer gegevens waarvan de vertrouwelijkheid gedurende zeer lange tijd geborgd dient te zijn
- fysiek transport voor uitwisseling van cryptosleutels
- aanmaak cryptosleutels m.b.v. QKD technologie
- aanmaak cryptosleutels m.b.v. KDF en sleutelmateriaal van verschillende bronnen (PSK, QKD, conventioneel KEM, PQC KEM)
- PSK optie van security protocollen (bijvoorbeeld TLS)
- pre-PQC quantum-secure stateful hash-based digital signature schemes
- PQC crypto algo's (KEM's en digital signature schemes)
- hybride public-key cryptografie (conventioneel én PQC)
- quantum-secure oplossingen anders dan de bovenstaande

KDF Key Derivation Function
KEM Key Encapsulation Mechanism
PKE Public-Key Encryption
PSK Pre-Shared Key
QKD Quantum Key Distribution
TLS Transport Layer Security

in vrijwel alle gevallen zal een combinatie van meerdere scenario's van toepassing zijn

BSI's KDF post-quantum migratie scenario

BSI Bundesamt für Sicherheit in der Informationstechnik
KDF Key Derivation Function
QKD Quantum Key Distribution



ten slotte …

ANSSI (Frankrijk), BSI (Duitsland), NCSC (Verenigd Koninkrijk), NCSC/AIVD/NBV (Nederland) en NSA (Verenigde Staten) adviseren om t.b.v. de post-quantum migratie voor systemen van de overheid, voor kritieke systemen die van nationaal belang zijn (en voor militaire systemen) in principe op PQC gebaseerde oplossingen te gebruiken en QKD(N) oplossingen alleen in te zetten

- als uit zorgvuldig onderzoek is gebleken dat deze significante voordelen bieden
- als m.b.v. testen of d.m.v. certificatie blijkt dat de door de leveranciers geclaimde werking volgens kwantummechanica principes in voldoende mate is gegarandeerd

AIVD Algemene Inlichtingen- en Veiligheidsdienst
ANSSI Agence Nationale de Sécurité des Systèmes d'Information
BSI Bundesamt für Sicherheit in der Informationstechnik
NBV Nationaal Bureau voor Verbindingsbeveiliging
NCSC Nationaal Cyber Security Centrum / National Cyber Security Centre
NSA National Security Agency

post-quantum migratie heel kort samengevat

streef zoveel mogelijk naar

crypto agility en

crypto diversificatie

VRAGEN → paneldiscussie