Kvantumtitkosítás a jelenben és a jövő hálózataiban

Farkas Lóránt

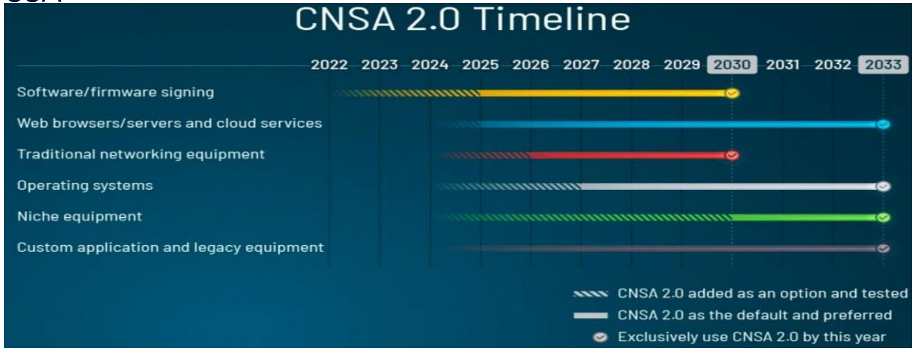
Barta Péter

NOKIA BELL LABS

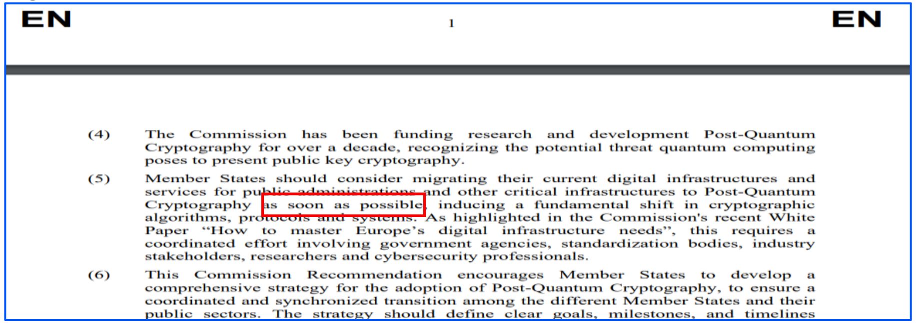
Poszt-kvantum ütemtervek – forró téma

A 24. órában vagyunk

USA



EU



EN 1 EN

(4) The Commission has been funding research and development Post-Quantum Cryptography for over a decade, recognizing the potential threat quantum computing poses to present public key cryptography.

(5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White Paper "How to master Europe's digital infrastructure needs", this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

(6) This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography, to ensure a coordinated and synchronized transition among the different Member States and their public sectors. The strategy should define clear goals, milestones, and timelines

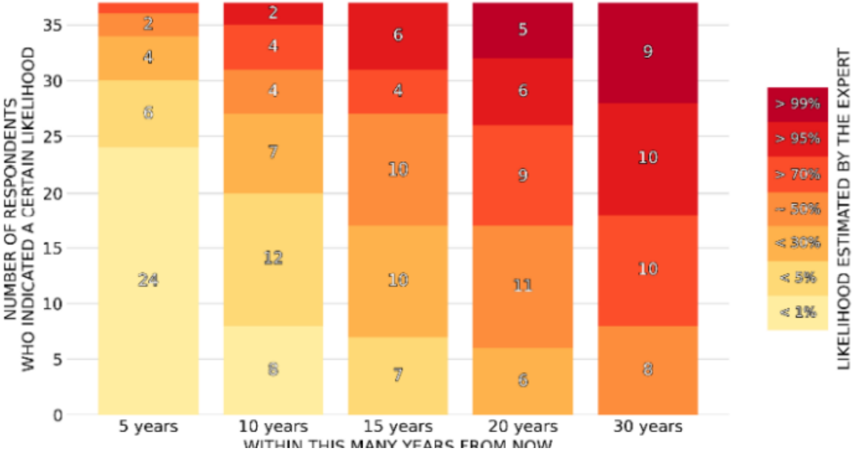
Forrás: NIST, Európai Bizottság

Államok/régiók által kiválasztott PQC technológiák:

NIST (80%),
FrodoKEM (10%)
KpqC (5%)
nem döntött (5%)

Forrás: GSMA

Mikor lesz a Q nap:



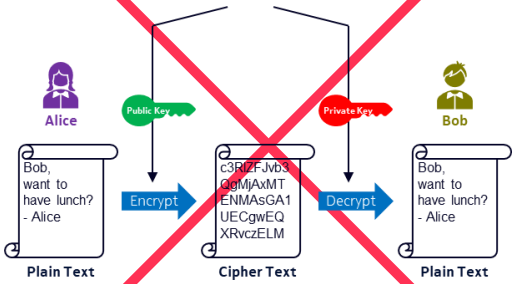
Forrás: Global Risk Institute

NOKIA BELL LABS

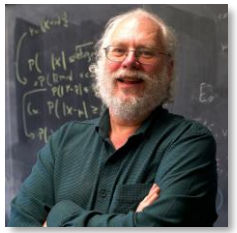
Mi szóltunk, hogy gond lesz

Nem mostanában, hanem 30 évvel ezelőtt

Aszimmetrikus kripto



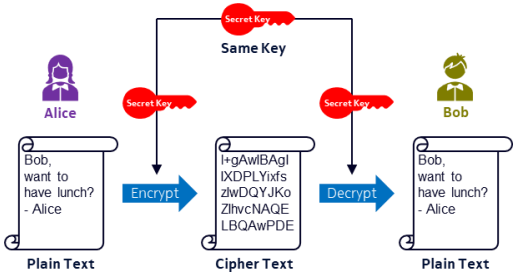
Feltörve



Peter **Shor** – Bell Labs

Nagy számok prím tényezőkre bontási algoritmusa - 1994

Szimmetrikus kripto



Biztonságos

Lov **Grover** – Bell Labs

$\sqrt{N}$ idejű keresés rendezetlen halmazokban

NOKIA BELL LABS

Poszt-kvantum biztonság fajtái

Matematika vs. fizika

PQC
Poszt-kvantum kriptográfia

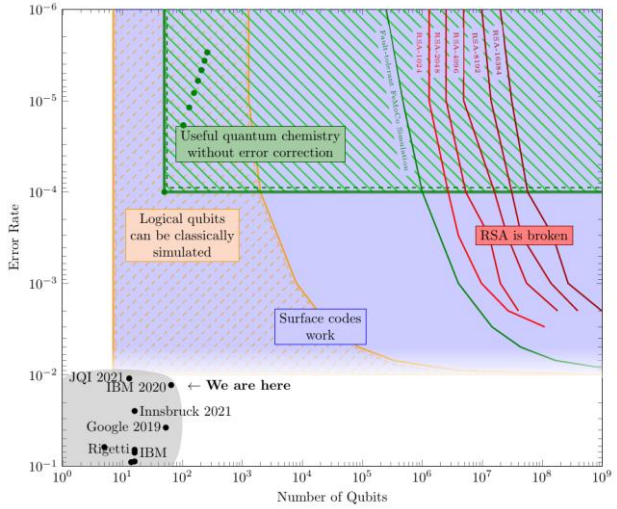
- Matematikán alapul
- Titkosító kulcsok biztonságos létrehozására és a kommunikáció biztonságossá tételére alkalmas, megbízhatatlan hálózatokban
- Alkalmazási rétegben működik
- Szoftveres megoldás, frissítés lehetősége adott
- Feltörhetetlen a jelenlegi tudásunk szerint, de ez változhat

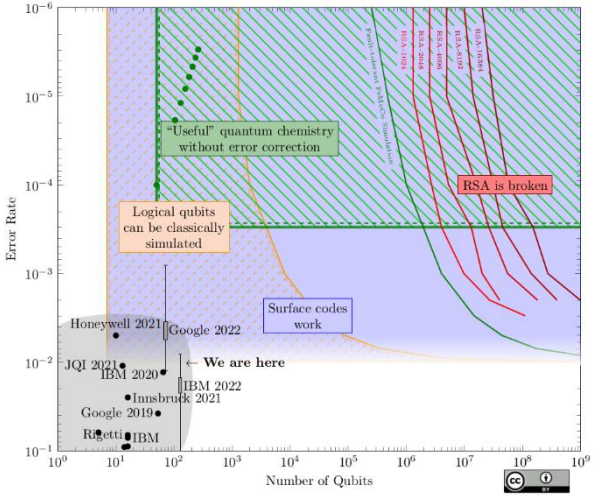
QKD
Kvantumos kulcselosztás

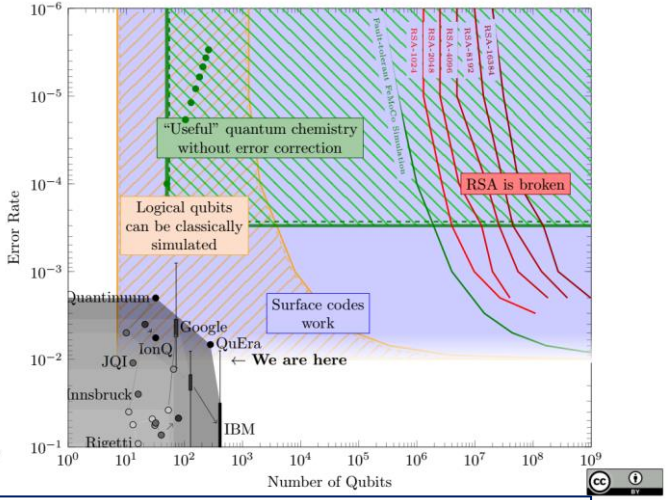
- A fizikai anyag kvantumos tulajdonságain alapul
- Titkosító kulcsok biztonságos szétosztására alkalmazható
- Fizikai rétegben működik (optikai szál, Ethernet, mikrohullám)
- Speciális hardvert igényel
- Pont-pont protokoll alapvetően, megbízható köztes csomópontokat feltételez
- Amennyiben a kvantumfizika érvényes, törvényeiből adódóan feltörhetetlen

NOKIA BELL LABS

PQC







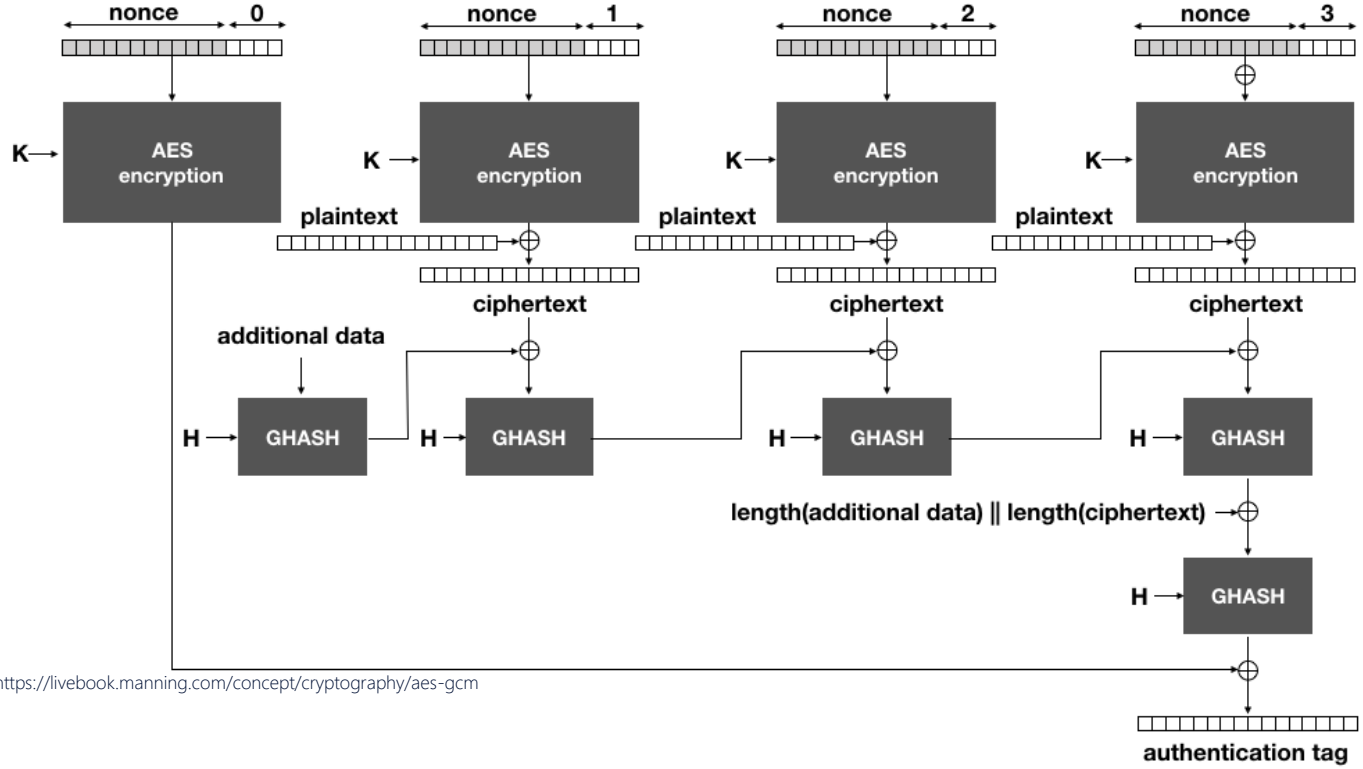
Frissítendő folyamatok:

- Kvantumbiztos biztonsági kulcsok használata
- Biztonsági kulcskezelés folyamatának kvantumbiztossá tétele
- Aláírások, tanúsítványok kvantumbiztossá tétele

NOKIA BELL LABS

PQC – kvantumbiztos kulcsok

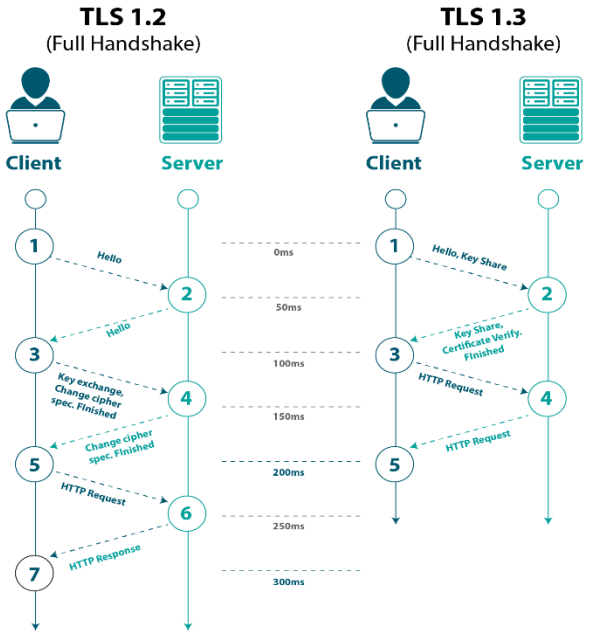
Készen állunk – AES-GCM kvantum-biztos és széles körben elterjedt



Forrás: https://livebook.manning.com/concept/cryptography/aes-gcm

PQC –kulcskezelés és osszifikáció

Nem állunk készen, de viszonylag jók a kilátások

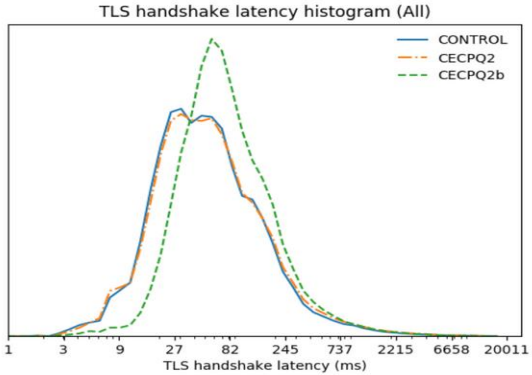


Forrás: https://www.appviewx.com/blogs/why-is-tls-1-3-better-and-safer-than-tls-1-2/

Osszifikáció

- TLS 1.3 – 2014 óta
- 2018-ban még csak 0.06% (rev 11)
- Rev 22: a TLS1.3 TLS1.2-nek tűnik régebbi szerverek, routerek számára. 2 hónap alatt 0.6% -> 66% (ma: 93%)

Erőforrásigény és méretbeli különbségek:



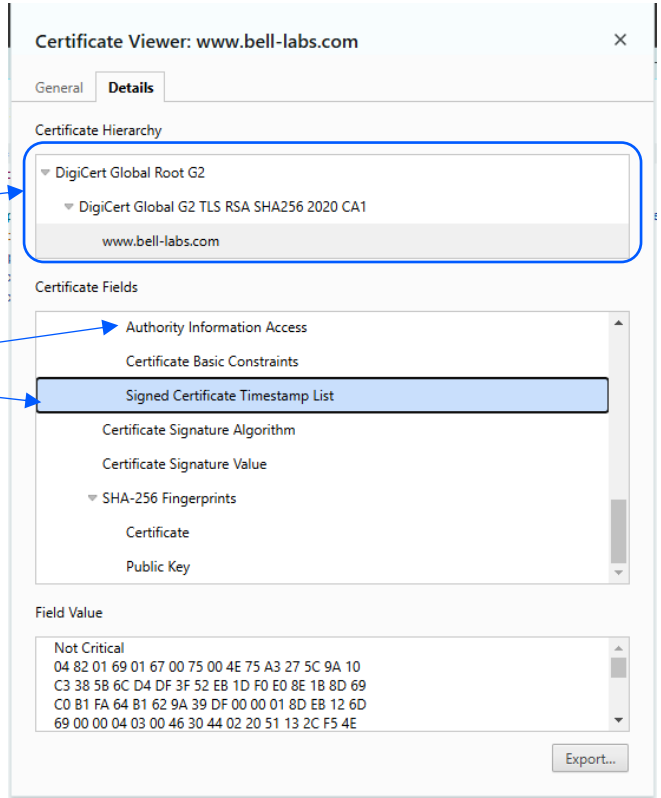
Forrás:https://blog.cloudflare.com/pq-2024/

		Kulcsméret (bájtban)		Művelet / sec	
Algoritmus	PQ	Kliens	Szerver	Kliens	Szerver
ML-KEM512	Igen	800	768	45e	70e
ML-KEM768	Igen	1184	1088	29e	45e
ML-KEM1024	Igen	1568	1568	20e	20e
X25519	Nem	32	32	19e	19e

PQC –tanúsítványkezelés

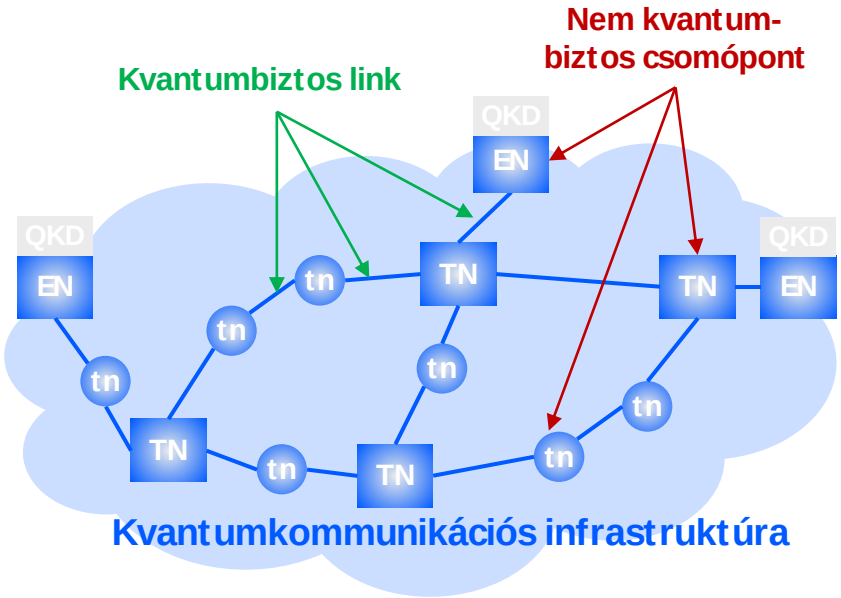
Még sok meló van vele

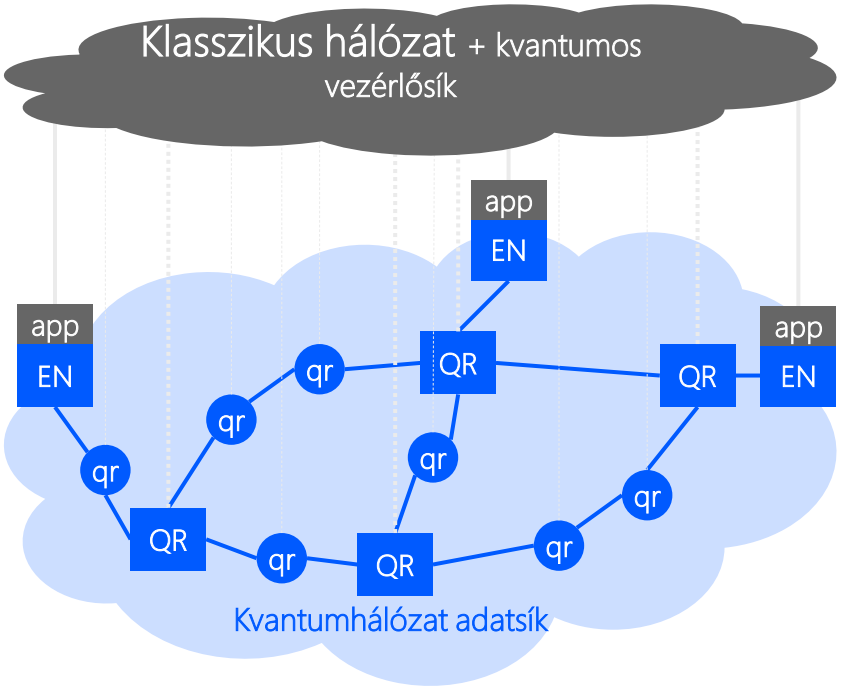
- Aláírás dzsungel
- Típusok
  - Tanúsítványlánc
  - Tanúsítvány időbélyeg
  - Online tanúsítvány státusz protokoll (OCSP)
- Kulcs része a bitfolyamnak/nem része a bitfolyamnak
  - Más, ha felfújt Javascript kódot/képeket véd
  - Más, ha pár bájtot forgalmazó IoT eszközt véd
- Aláírás komplexitása/ellenőrzés komplexitása lehet fontos/nem fontos szempont
- PQC szempontok:
  - NIST vs. stateful vs onramp
  - Törekedés kevesebb szignatúrára
  - TLS-en kívül van más is, pl DNSSec



QKD -> QCI

Ehhez még évek kellenek





NOKIA BELL LABS

Bell Labs kutatások a PQC és a QKD vonatkozásában

A fényes múlt

-Kvantumos faktorizáció (Peter Shor)

-Gyors kvantumos keresés rendezetlen adatbázisokban (Grover)

A pragmatikus jelen

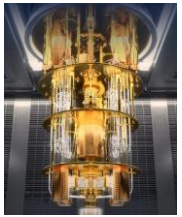
- Kvantumos hibajavító kódok, kvantum konvolúciós kódok, kvantum repeaterek (Ashikhmin)
- Kvantum internet, QKD kódok (Noirie)
- Poszt-kvantum kriptográfia (Shoiniakis)
- (Topologikus kvantumszámítógép – Willett)

NOKIA BELL LABS

Nokia titkosítás megoldások

Connectivity and cybersecurity in the “Quantum era”

A combination that we simply cannot ignore



Quantum computing

=

Current asymmetric cryptography (PKI)

Harvest Now Decrypt Later

Duration of **your** data sensitivity

+

Your time to evolve to Q-S cryptography

+

=

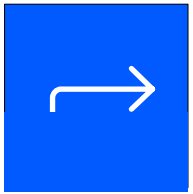
Your ZERO DAY VULNERABILTY

Threats to Information - Info Life-Span considerations

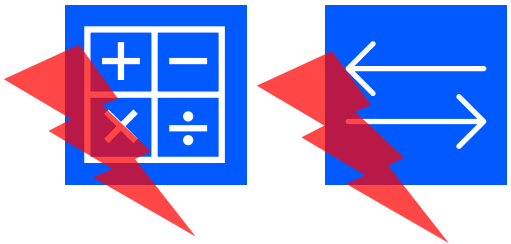
Zero-Day vulnerability

CRQC (Q Day)

- Information may be transactional in nature, or may have short-, medium-, or long-term life span
- The longer the information life-span, the greater the risk from quantum cryptographic threats



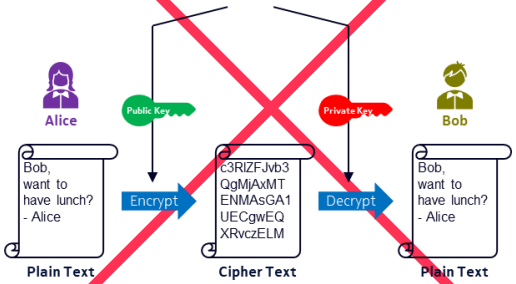
Harvest Now Decrypt Later



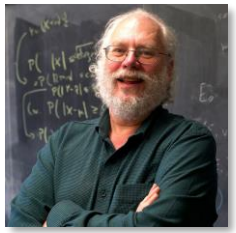
Seconds / Minutes / Hours	1 – 3 Years	5 – 10 years	10 – 50 years	50 – 100+ years
•Business Electronic Transactional info •**Cryptographic session keys**	•Organizational business information •**Cryptographic keys**	•Organizational “Crown Jewels” •**Cryptographic keys**	• Nation state secrets • Organizational “Crown Jewels	• Nation state secrets • Personally Identifiable Information (PII) • Citizen info

Impact of Quantum computational power on cryptography

Asymmetric Crypto



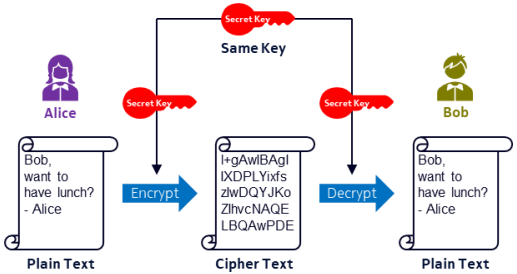
Broken



Peter **Shor**

Algorithm for prime factorization of large integers

Symmetric Crypto



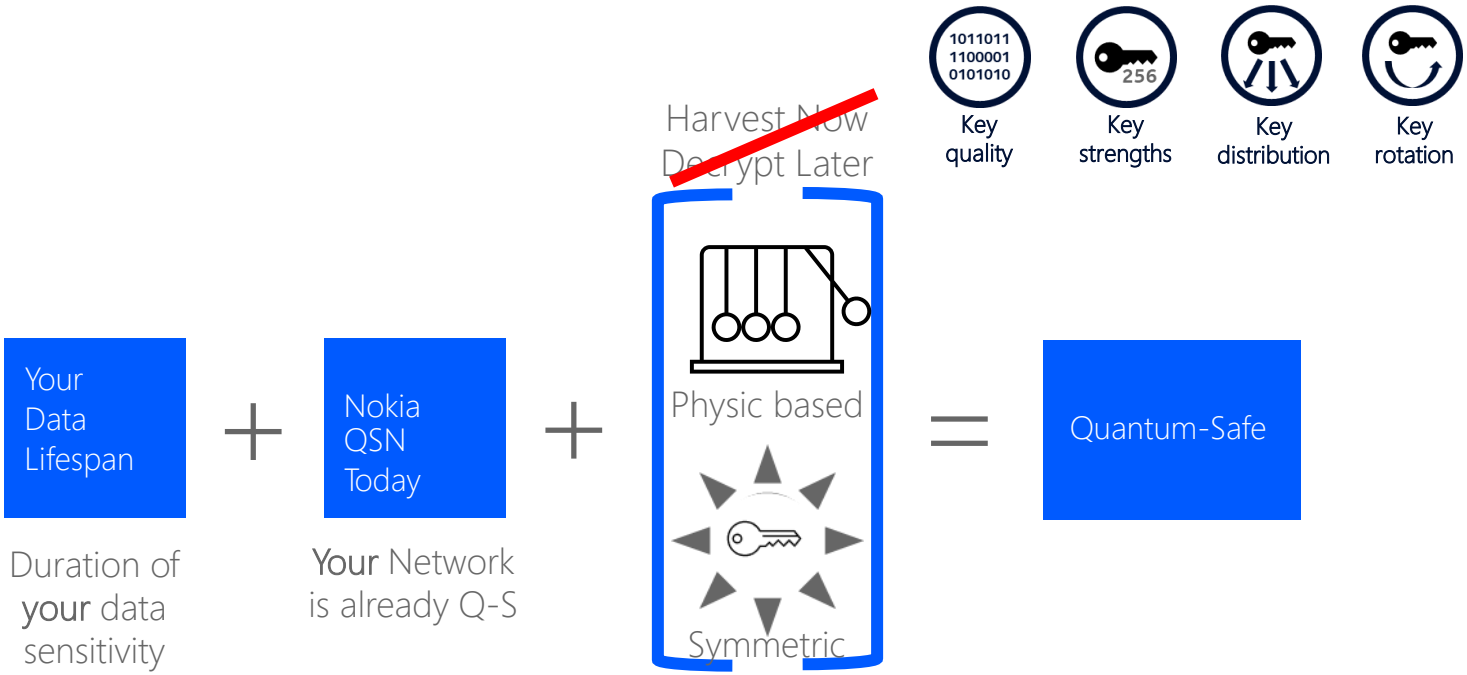
Safe

Lov Kumar **Grover**

shows how to search in $\sqrt{N}$

Connectivity and cybersecurity in the “Quantum era”

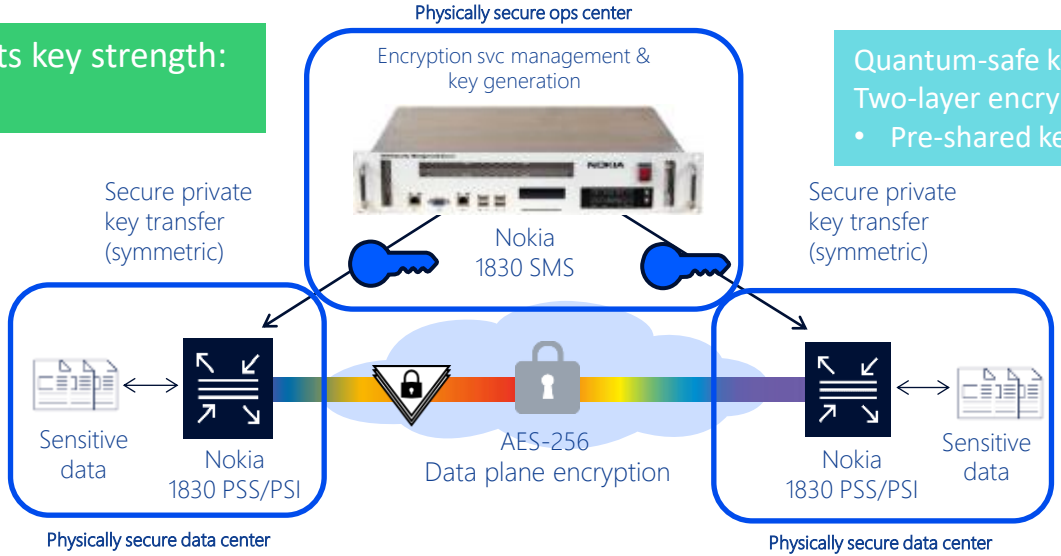
Nokia has the solution using multiple blueprint reference architectures



The solution with Nokia for Optical Networks

OTNSec pre-shared-key management

All links ensure 256 bits key strength: Quantum-safe



Quantum-safe key transport: Two-layer encryption

- Pre-shared key w/SNMPv3

Quantum-safe data transport:

- Data plane fiber taps contain only ciphertext
- Optical overhead does not contain key agreement

Quantum-safe data transport:

- Symmetric, AES-256
- No key exchange on fiber link

Why secure at Layer 1?

Low latency	Ultra low **latency** and bandwidth efficiency
Transparency	Better scale and support for **any** traffic type
Better performance	**High bandwidth** wire speed encryption
High availability	Robust network protection with **high availability**
Management	Simpler security and network **management**

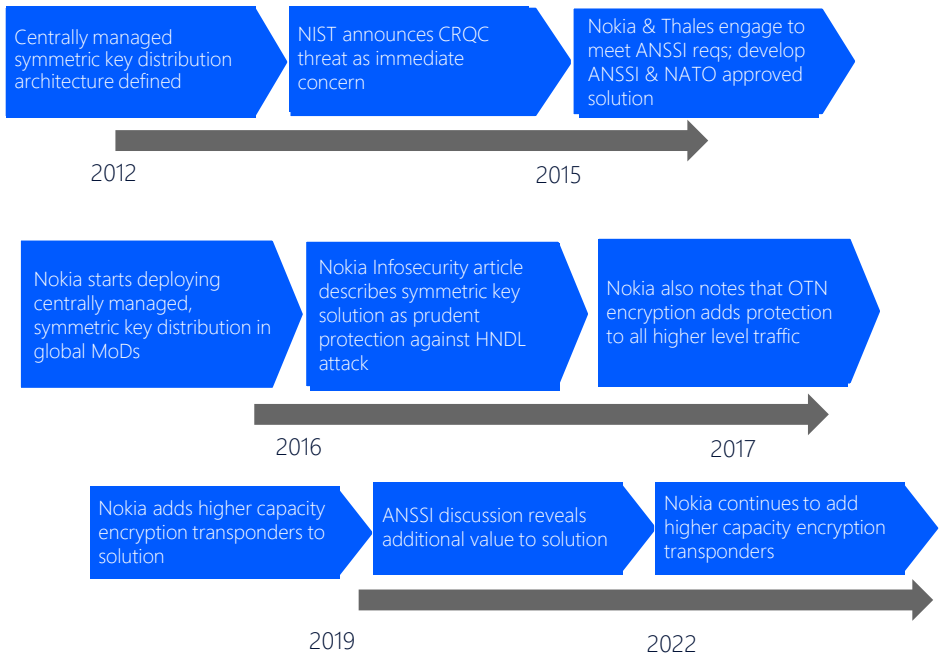
Nokia 1830 Security Management Server (SMS)

Quantum-key generation & distribution hybrid

Nokia 1830 SMS

- Centralized, symmetric key distribution
- Embedded cryptographic System-On-Chip
- Ensures key quality and strength
- Offloads intensive cryptographic processing
- SW integrity validation (Digital signature PP CWA 14167-2 compliant)
- CC EAL4+, ANSSI QR including EU and NATO restricted certs
- FIPS 140-2 Level 1 Software for Hardened Server

Over 10 years of quantum-safe development



Nokia L1 encryptors throughout various product lines

PSS-8/16/32 Core/Metro WDM

11QPEN4 – Quad Port 10G Encryption

Provides per port, 10G Encryption (AES-256)
4 x 10G XFP (OTU2) network ports
4 x XFP client ports
Client services: 8G / 10G FC, 10 GE, OTU2, 10G Infiniband
AES-256 Encryption
FIPS and CC certified

S13X100E 100G Muxponder

Provides per 100G port Encryption (AES-256)
100G Multi-service Muxponder supporting 10G, 40G, 100G clients in single card
100 GE/OTU4, 40GE / OTU3, 10GE, OTU2, OC192/STM64
CFP4, QSFP28/QSFP+, SFP+ client ports
AES-256 Encryption
FIPS certified, CC (in-progress)

PSI-M (DCi)

DFC12E / DFC12 Module – High Capacity nx100G

2x WDM line interfaces
100G - 400G capacity per line
10x100GE/OTU4
10xQSFP28 ports (active)
100GE-LR4/SR4/CWDM4
AES-256 Encryption
FIPS (submitted)

S6AD600E 600G Module

1x WDM line interface
100G - 600G capacity per line
6x100GE/OTU4
5xQSFP28 ports
1xQSFP-DD (400GE) port
100GE-LR4/SR4/CWDM4
AES-256 Encryption
FIPS (planned)

SFM6E 600G Module

1x WDM line interface
100G - 600G capacity per line
6x100GE/OTU4
5xQSFP28 ports
1xQSFP-DD (400GE) port
100GE-LR4/SR4/CWDM4
AES-256 Encryption
FIPS (planned)

PSD-2 (CPE)

1830 Photonic Service Demarcation (CPE)

Redundant AC/DC power
New High-Performance FPGA
2x Client, 2x Line Ports
Remote Power Off
New System Mode
GbE/10GbE via ODUflex (OTU2) – Dual Client, Dual Line Mode for spur / ring application (ADM)
AES256 encryption (planned)
FIPS (future)

PSS-24x (OTN fabric)

2UC400E – 2 Carrier (400G) Uplink

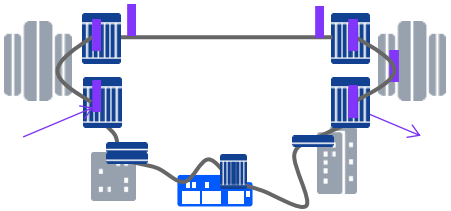
Provides per line port Encryption (AES-256)
2 x Flexible 100G / 200G Super Coherent line ports
AES-256 Encryption
FIPS (submitted)

2UC1TE – 2 Carrier (1T) Uplink

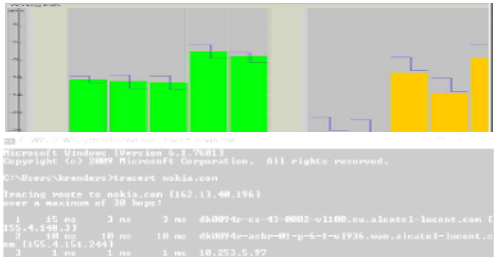
Provides per line port Encryption (AES-256)
2 x programmable 200-500G 90 Gbaud Super Coherent line ports

Optical security is more than just encryption

Wavelength tracker – monitor optical link health

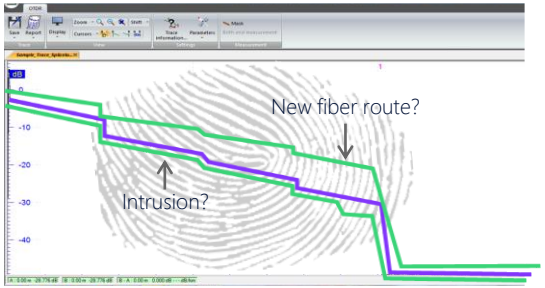


Allows wavelength tracking, power and fiber monitoring and reporting

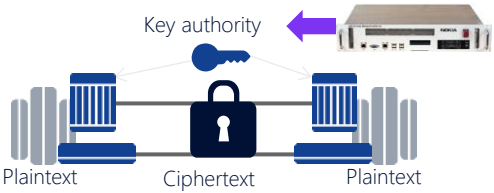


OTDR – localize faults or taps immediately

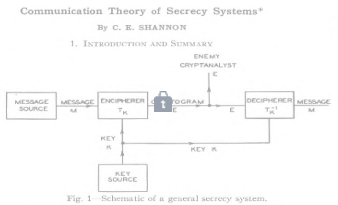
Detect and localize precisely any anomalies on fiber network



Key management – the key quality is vital to any encryption



Protect data with a strong quality key and symmetric distribution



Quantum-Safe symmetric key distribution and generation

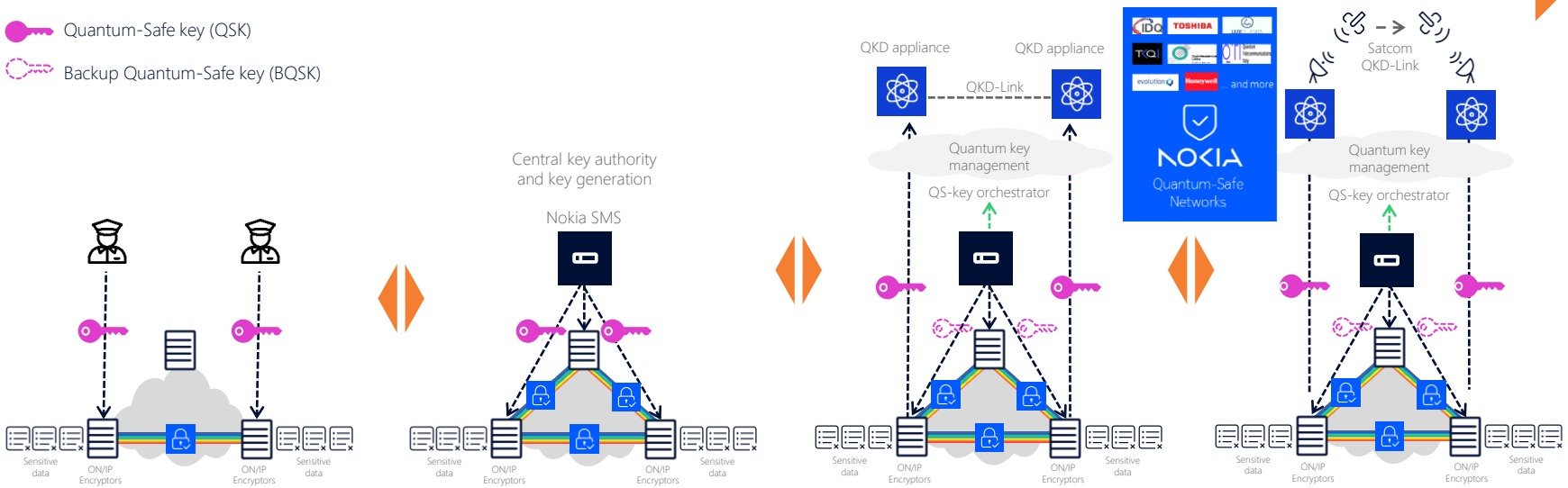
Nokia Optical quantum-safe networks

An architecture that evolves with the quantum landscape

Your Quantum-Safe roadmap: Begin today and adapt to tomorrow's innovations

Quantum-Safe key (QSK)

Backup Quantum-Safe key (BQSK)



Pre-Shared Keys with Manual distribution

PSK with Automated symmetric distribution

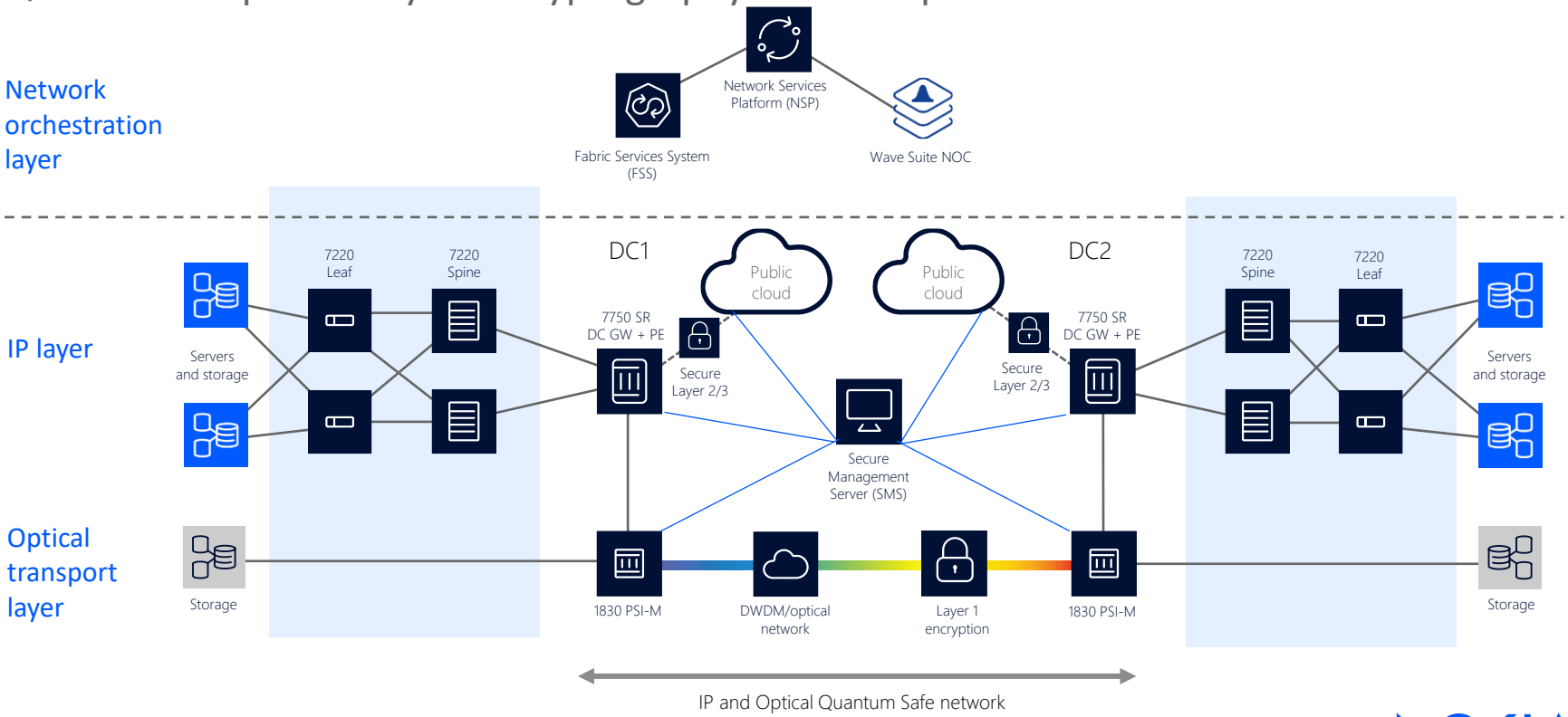
Pre-Shared Keys with Quantum physics hybrid QKD distribution

Deploy quantum-safe solution today

Engage PoC/Pilot today

Key distribution

QSN with adapted & layered cryptography for IP + Optical



Nokia Optical Secure Solutions Certified and Widely Deployed

proven

EU area Countries 27	Encryption customers >80
1830 SMS customers 38	Encryption cards shipped >4,000

CERTIFIED

COMMON CRITERIA CERTIFIED EAL4+

Nokia Quantum-Safe Networks

*'Helping the world to **securely** act together'*


NOKIA