ADVANCED TECHNOLOGY OF LASER

Zavartatásvédelem és kvantum titkosítás az optikai hálózatoknál

2024. április 24.

Optikai hálózatok

Az optikai hálózatok jellemzői:

- **Nagy sávszélesség, nagy kapacitás**
- **Kis energiafogyasztás**
- **Kis interferencia**
- **Nagy távolság**
- **Biztonság**
- **Mérési-, adatgyűjtési lehetőségek**

Biztonságos-e az optikai hálózat?

Kísérlet:

1. **Csatoljunk be egy optikai kábelbe látható fényt.**
2. **Hajlítsuk meg az optikai kábelt.**

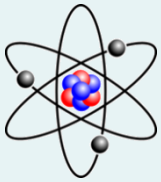
Tapasztalat:

A fény kilép a köpenyen keresztül.

Veszélyben a biztonság!

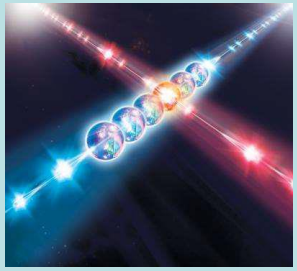
A kvantumszámítógép számítási kapacitása komoly fenyegetést jelent mindazon távközlési/adatátviteli infrastruktúrák számára, amelyeknek a biztonsága azon alapul, hogy „áh, ezt számítógéppel évekig vagy évezredekig tart feltörni”!

A kvantumtechnológia lehetőség vagy fenyegetettség?

Klasszikus fizika	Kvantum fizika
	
1900-as évek előtt	1900-as évek után
A makroszkópikus világ törvényszerűségeinek leírása	A mikroszkópikus világ törvényszerűségeinek a leírása
Determinisztikus jelenségek	Valószínűségi jelenségek
Intuitív	Nem annyira intuitív

Kvantum fizika → Újszerű információ feldolgozási lehetőségek → Kvantum Információs Elmélet (QIT)

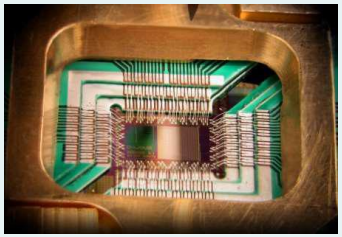
Kvantumtechnológiai áttekintés



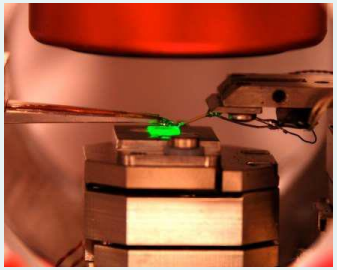
kvantum szimuláció

kvantum titkosítás

kvantum kommunikáció



kvantum számítás



kvantum mérés/érzékelés

atomóra

Kvantum számítógép a számok tükrében

30 Qbites számítógép műveleti sebessége/S	30 bites számítógép műveleti sebessége/s
10 teraFLOPS	~0,5 megaFLOPS

A kvantum számítógép 2 milliószor gyorsabb!

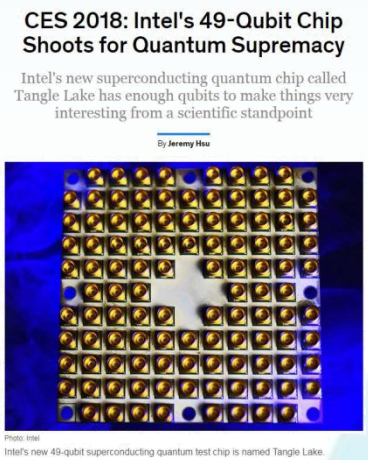

Intelligent Machines

IBM Raises the Bar with a 50-Qubit Quantum Computer

Researchers have built the most sophisticated quantum computer yet, signaling progress toward a powerful new way of processing information.

by Will Knight November 10, 2017

IBM's 50-qubit machine.


CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy

Intel's new superconducting quantum chip called Tangle Lake has enough qubits to make things very interesting from a scientific standpoint

By Jeremy Hsu

Photo: Intel

Intel's new 49-qubit superconducting quantum test chip is named Tangle Lake.


NEWS IN BRIEF QUANTUM PHYSICS

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018

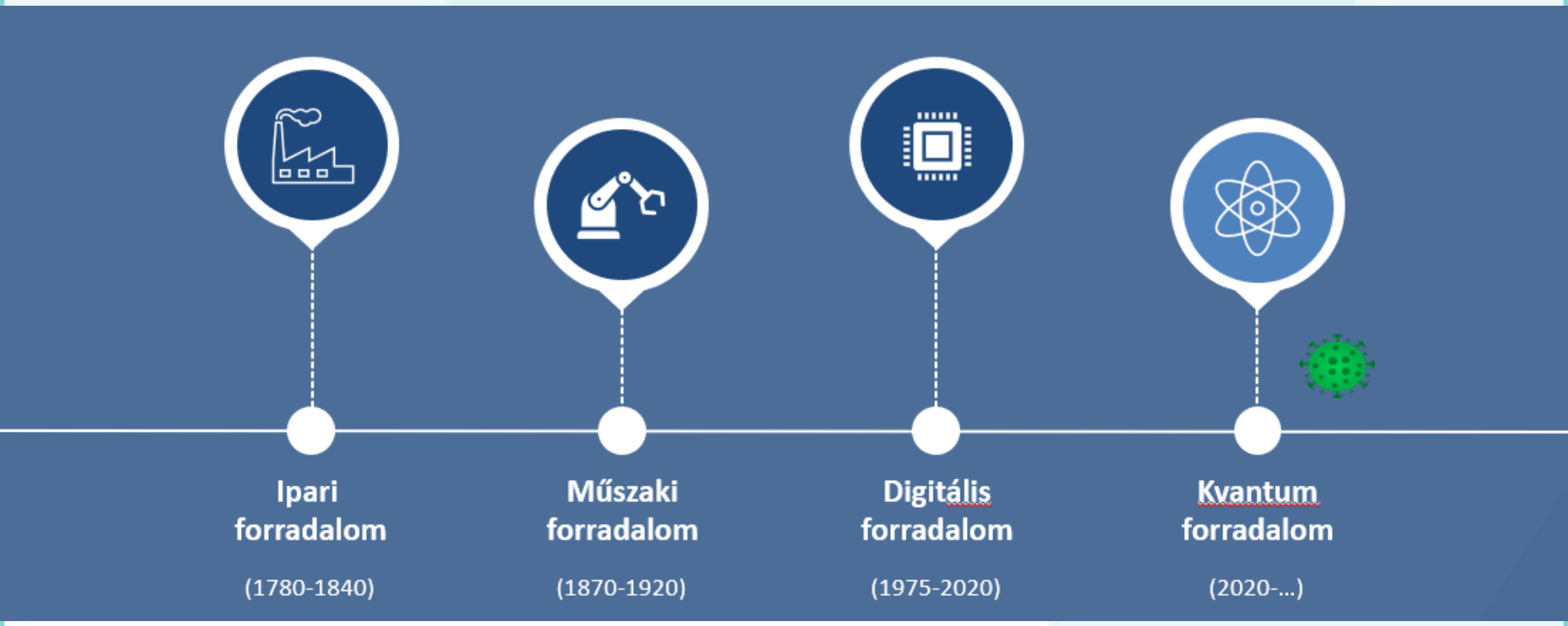
SHARE ARTICLE

Bristlecone

Google

QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.

Paradigmaváltás

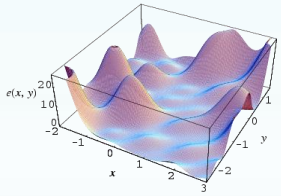


A kvantumszámítógép előnyei

- Úgy működik, mintha számos hagyományos számítógépet párhuzamosan kötnénk
- Sokkal kisebb a műveleti sor hossza
- Néhány megoldhatatlan számítás megoldhatóvá válik
- 1994 Shore algoritmus (prímszorzatok keresése)
- 1996 Grover algoritmus (keresés lerövidítése)

Kémia

- Molekuláris szimulációk
- Gyógyszerkutatás
- Új anyagok



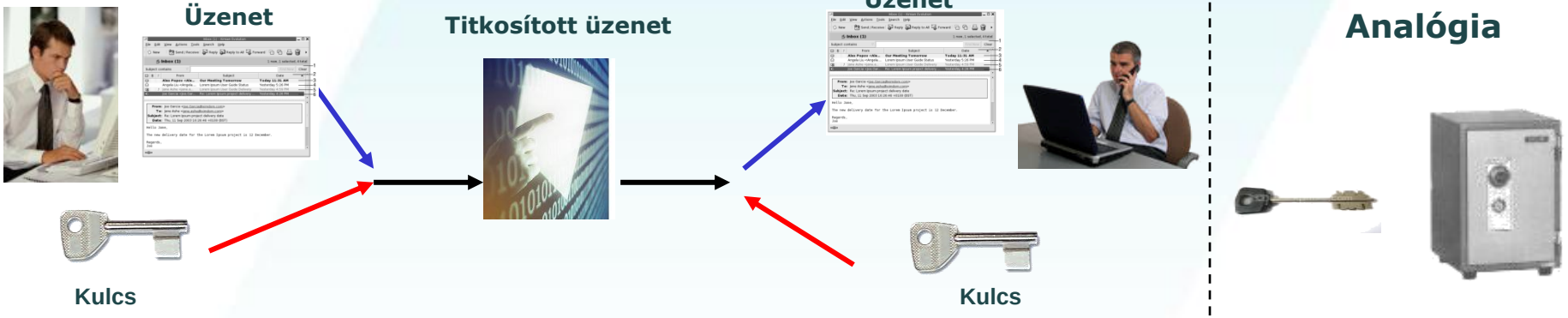
Optimalizáció

- Logisztika
- Pénzügy
- Gyártás
- Energetika

AI & Gépi tanulás

- Új kvantum alapú algoritmusok

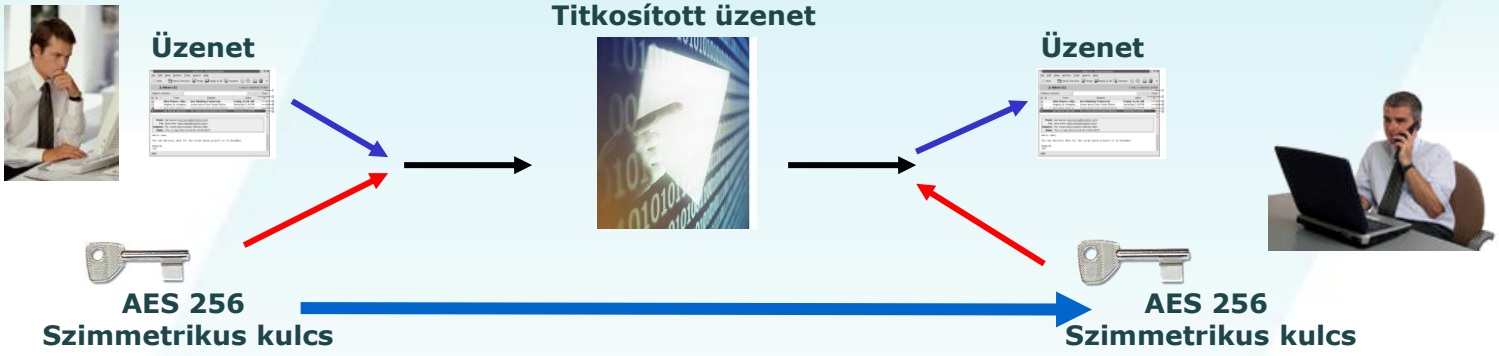
Hagyományos titkosítás



Kódoló kulcs titkosítása – AES 256 bit

- **Szimmetrikus kulcsú titkosítás**
- **Abszolút biztonságos, ha bizonyos előírásokat betartunk**
- **Kérdés, hogy a kulcsot miként juttassuk el a túloldalra?**

Klasszikus titkosító kulcs technika



Publikus kulcs továbbítás

Egy utas matematikai függvények

2357 x 4201 = ? **A x B = 9901757**

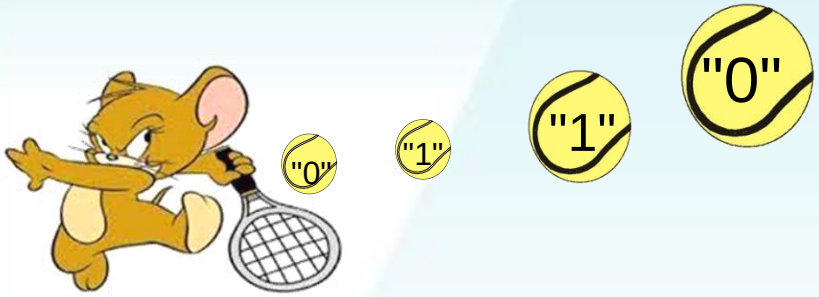
Sebezhető

- **A publikus kulcs matematikai algoritmusokon alapszik**
- **Az algoritmuson alapuló kulcs feltörhető, csak számítástechnikai kapacitás kérdése**

Kvantum számítógéppel a nagy számítási kapacitás adott!

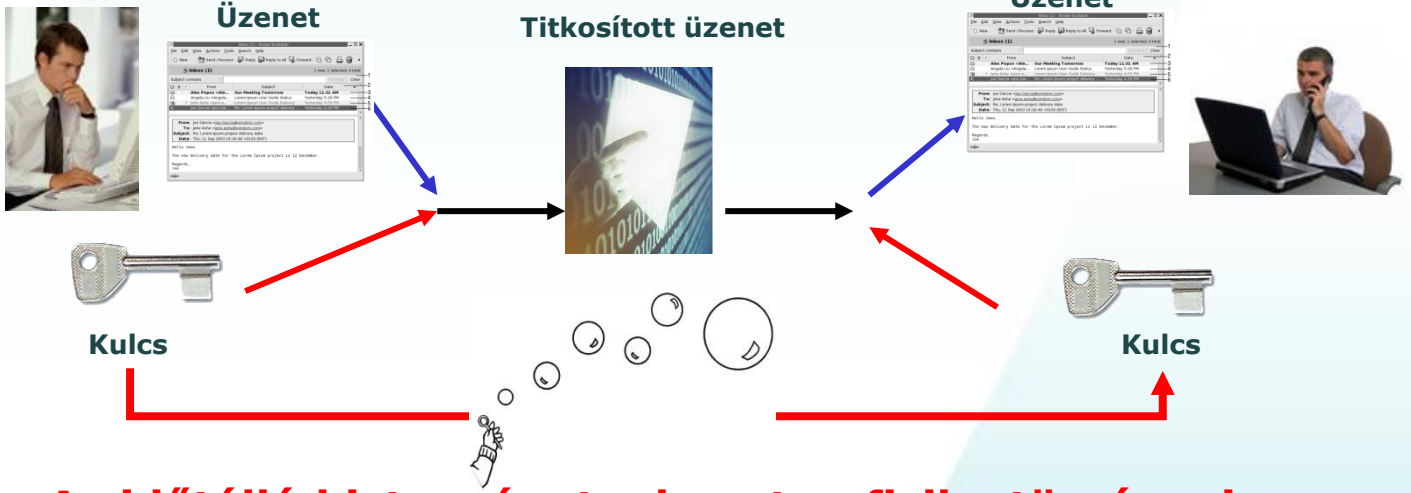
Kvantum kulcs továbbítás

Klasszikus kommunikáció



Kvantum kommunikáció

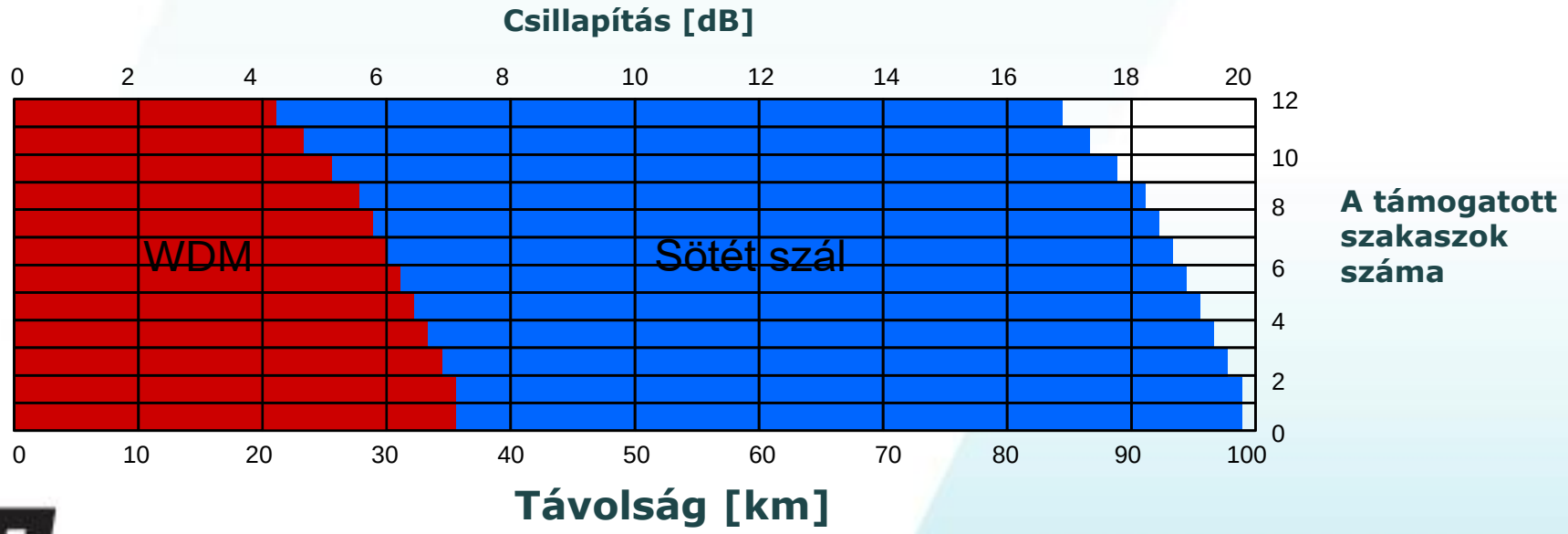
Törékeny !



Az időtálló biztonságot a kvantumfizika törvényei garantálják!

Átviteli közeg 1: vezetékes összeköttetés

- **Vezetékes szál (távközlési üvegszál)**
- **Csak pont-pont közötti összeköttetés lehetséges, és az optikai szálon a távolság max. 80-100-200km**
- **Dedikált optikai szál (sötét szál) szükséges a kvantum kulcs átviteléhez, ellenkező esetben az áthidalható távolság csökken**



Átviteli közeg 2: szabadtéri link

- **Szabadtéri link (műholdas kapcsolat)**
- **Nagy távolságokat tud lefedni (több ezer km)**
- **Ez idáig csak egyetlen ország épített kvantumkommunikációs műholdat (Kína, 2016)**

Space.com › Tech

China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite

By Mike Wall, Space.com Senior Writer | August 16, 2016 06:13pm ET

385 54 19 37 1388 MORE

China launched the first-ever quantum-communication satellite, known as QUESS, atop a Long March-2D rocket from the Jiuquan Satellite Launch Center on Aug. 15, 2016 (Aug. 15 local time).

Credit: Xinhua/Jin Liwang

'Much better than expected': Chinese 'hack-proof' quantum communication satellite put into service

Published time: 19 Jan, 2017 04:43 Get short URL

Beijing Aerospace Control Center. © Ju Zhenhua / Xinhua / Global Look Press via ZUMA Press

The world's first quantum communication satellite is now officially operational following months of in-orbit testing, the Chinese Academy of Sciences (CAS) announced, saying that performance of the device is "much better" than was initially expected.

Miért kell műholdas szegmens?

- **Csak földi (optikai szálas) összeköttetéssel nem lehet nagy távolságokat lefedni, ugyanis kvantumkommunikációban nem tudunk jeleket erősíteni**
- **100-200 kilométernél nagyobb távolság optikai szálon nem működik, csak ha kvantum biztos állomásokat iktatunk be.**
- **Műhold segítségével viszont összeköthetünk két nagy távolságú földi állomást**

Európai kezdeményezés EuroQCI

Cél: 2027-re kiépíteni egy olyan európai kvantumkommunikációs infrastruktúrát (QCI), amelynek földi- és űr szegmense egyaránt van (27 EU tagállam, Európai Bizottság és Európai Űrügynökség (ESA) együttműködése)

A hálózat segítségével biztonságosan lehet üzeneteket továbbítani akkor is, ha a kvantumszámítógép támadásai miatt a hagyományos kriptográfiai eljárások már elestek

Hungary, Portugal and Poland Enter EU Quantum Communication Infrastructure Initiative

July 22, 2019

July 22, 2019 — Hungary, Portugal and Poland signed a declaration to work together with the other EU Member States to develop and deploy a quantum communication infrastructure (QCI) across the EU within the next ten years. The aim of the QCI is to boost European capabilities in quantum technologies, cybersecurity and industrial competitiveness.

Belgium, Germany, Italy, Luxembourg, Malta, the Netherlands, and Spain have already signed the declaration on the quantum communication infrastructure at the Digital Assembly in Bucharest on 13 June: The future is quantum: EU countries plan ultra-secure communication network.

10.08.2021 10:55

Teilen:

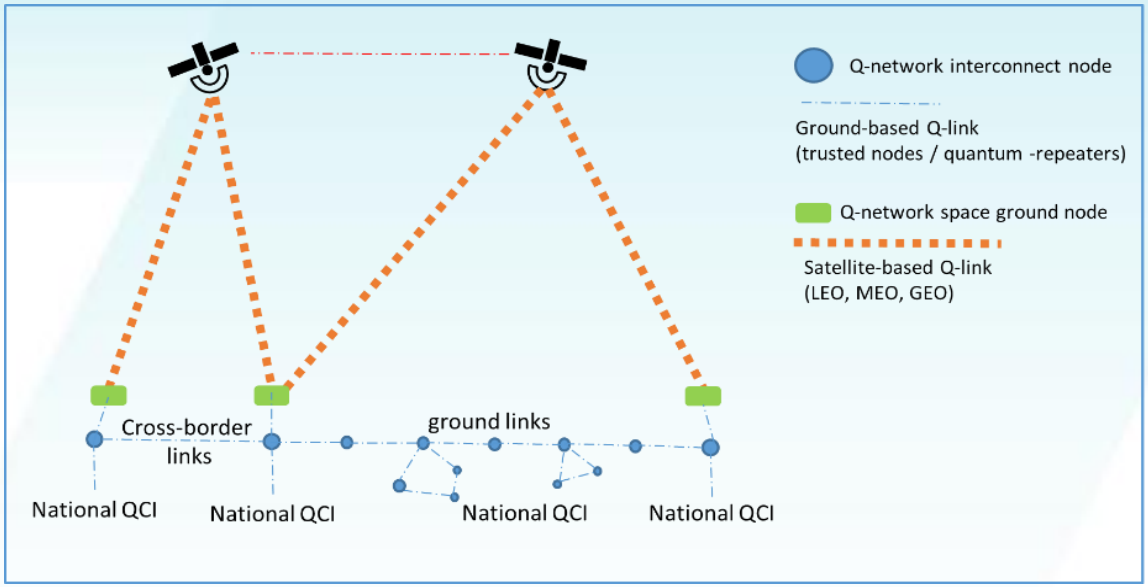
First quantum-secured video conference between German Federal agencies: QuNET demonstrates quantum communication

Desiree Haak *Strategie / Marketing / Koordination*
Fraunhofer-Institut für Angewandte Optik und Feinmechanik IOF

Today, two German federal authorities communicated via video for the first time in a quantum-secure manner. The QuNET project, an initiative funded by the German Federal Ministry of Education and Research (BMBF) to develop highly secure communication systems, is thus demonstrating how data sovereignty can be guaranteed in the future. This technology will not only be important for governments and public authorities but also to protect everyday data.

It was a foretaste of the communication of the future - or rather, the "data security" of the future. Because when Federal Research Minister Anja Karliczek invited members of the Federal Office for Information Security (BSI) to a video conference today, everything looked the same, at least for outsiders. Together with Andreas Könen, Head of Department CI "Cyber and IT Security" at the Federal Ministry of the Interior, Building and Community (BMI) and BSI Vice President Dr. Gerhard Schabhüser, the minister talked via video stream.

EuroQCI



Földi szakasz: nemzeti QCI összekapcsolása

- **Nemzeti QCI hálózatok (biztonságos kapcsolatok és megbízható köztes állomások)**
- **EU összekapcsolt állomásai a nemzeti QCI-re támaszkodva**
- **Határokon átívelő kapcsolatok**
- **Kvantum képes földi állomások**

Űr szegmens: LEO/MEO/GEO műholdakon alapuló műholdas kapcsolatok

- **Az első működő rendszer tervezése kipróbálása**
- **Üzembe állás előtti rendszer tesztelés**
- **LEO/MEO/GEO bevetése (időzítés függ a biztonsági követelményektől)**
- **A kvantumképes földi állomások és a földi hálózatok összekapcsolása**

Optikai vevőállomások

- **A közeljövő európai kvantumkommunikációs műholdakkal való kommunikációhoz európai optikai vevőállomásokra van szükség a nemzeti földi QCI mellett**

- **A vevőállomásoknak képeseknek kell lennie egy-egy fotont detektálni a világűrben alacsony Föld körüli pályán (LEO), közepes Föld körüli pályán (MEO), illetve geostracionáris pályán (GEO) pályán keringő műholdakról**

Kinek lehet fontos egy ilyen infrastruktúra által nyújtott szolgáltatások köre?

Kormányzati & Védelmi intézmények

Pénzügyi szolgáltatók és banki szektor

Telekom & MSP

Egyetemek, kutatóintézetek

Adatközpontok & Felhő szolgáltatók

Kritikus infrastruktúrák

Hogyan védekezzünk a kvantumszámítógép által kelthető fenyegetés ellen?

Védekezési lehetőségek

Fizikai biztonság: A jel útjának teljes védelme mind az optikai, mind az elektromos szakaszon. Az optikai kábelek fizikai védelme, speciális kábel szerkezet, elektromos rész EMC védelme.

Titkosítás: Az adatok titkosítása és QKD alkalmazása.

Megfigyelés és észlelés: Rendszerek telepítése és használata, amelyek észlelik az optikai hálózatban bekövetkező változásokat és próbálkozásokat, segíthet a fiber tapping támadások azonosításában és megakadályozásában. (QKD, RFTS)

Folyamatos monitoring és karbantartás: A jel útjának folyamatos monitorozása és karbantartása segíthet az esetleges biztonsági rések és problémák azonosításában és kezelésében. Biztonsági protokollok szigorú betartása az adat hozzáférés és adatkezelés területén. (védett helyiségek és adatkezelési protokoll)

Kvantum biztonság

Quantum Cyber Security eszközök a feltörhetetlen kommunikáció érdekében

QRNG

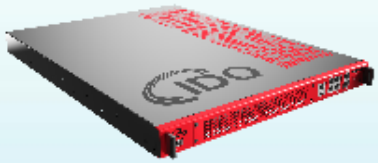
Quantum Random Number

- **USB**
- **PCIe kártya**
- **Készülék**
- **Chip**

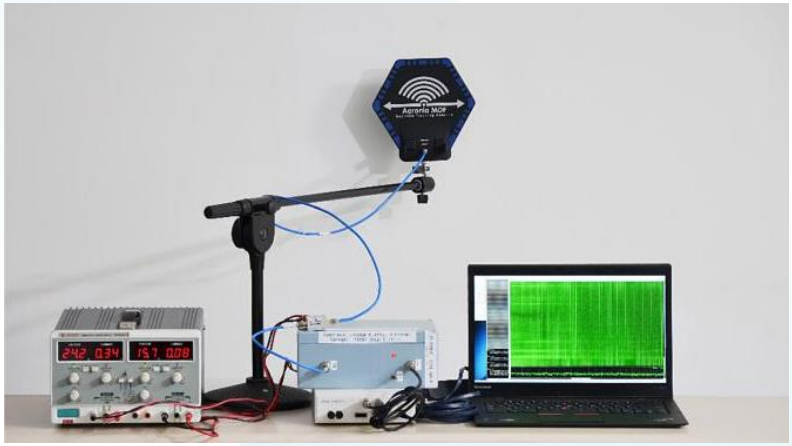
QKD

Quantum Key Distribution

- **Kereskedelmi környezethez**
- **Tudományos célokra, kutatóintézetek és innovációs laboratóriumok számára**



A jel útvonalának végponttól végpontig terjedő védelme

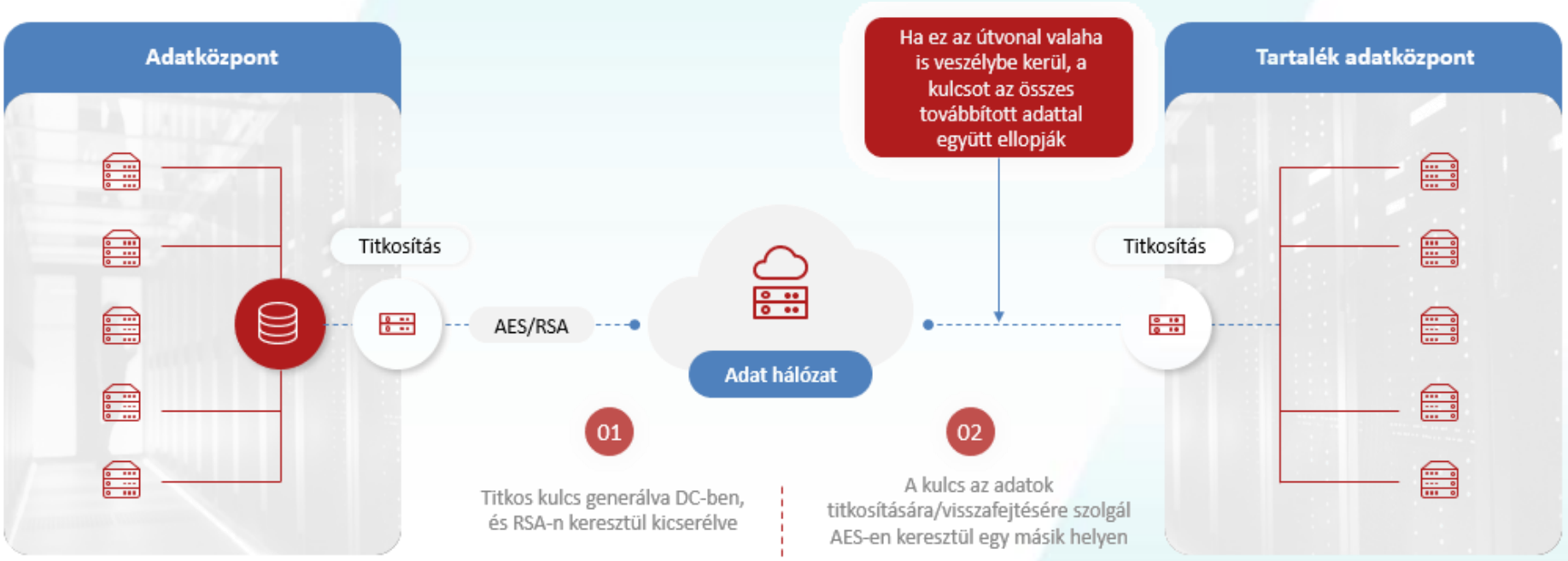


Official distributor

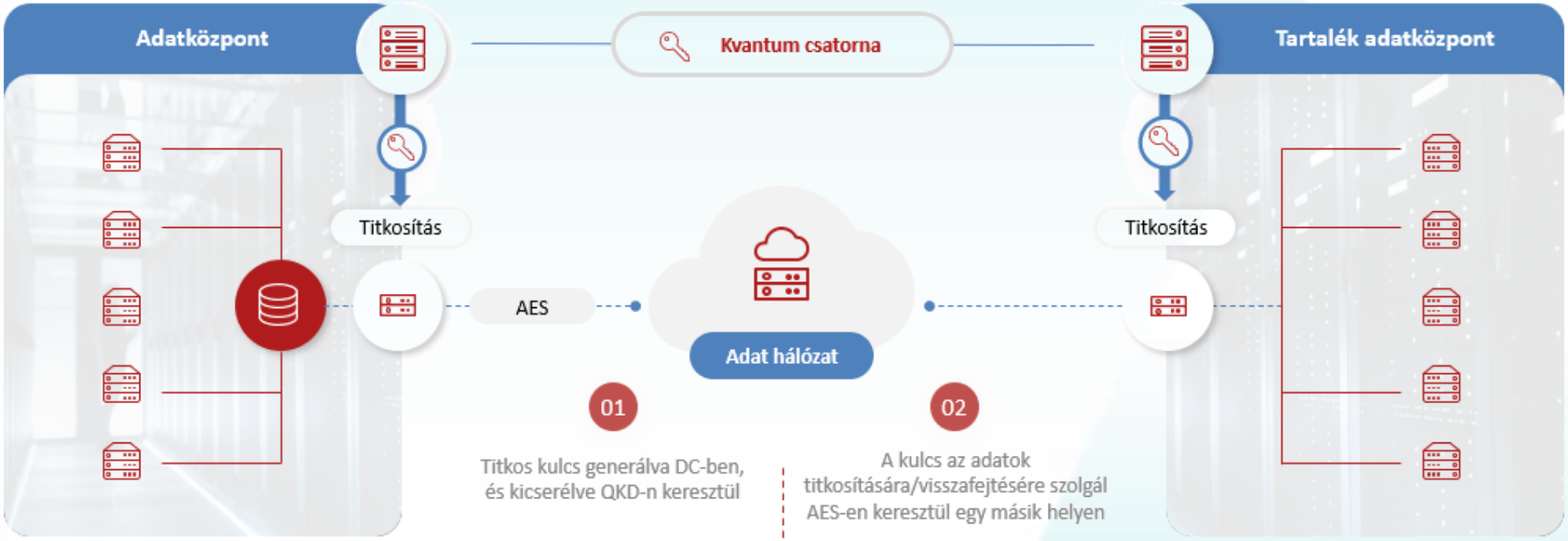
A végponti védekezés EMC védelmének fontos szempontjai

Kvantum kulcs szétosztás(QKD)

Jelenlegi kulcs csere PKI-n keresztül

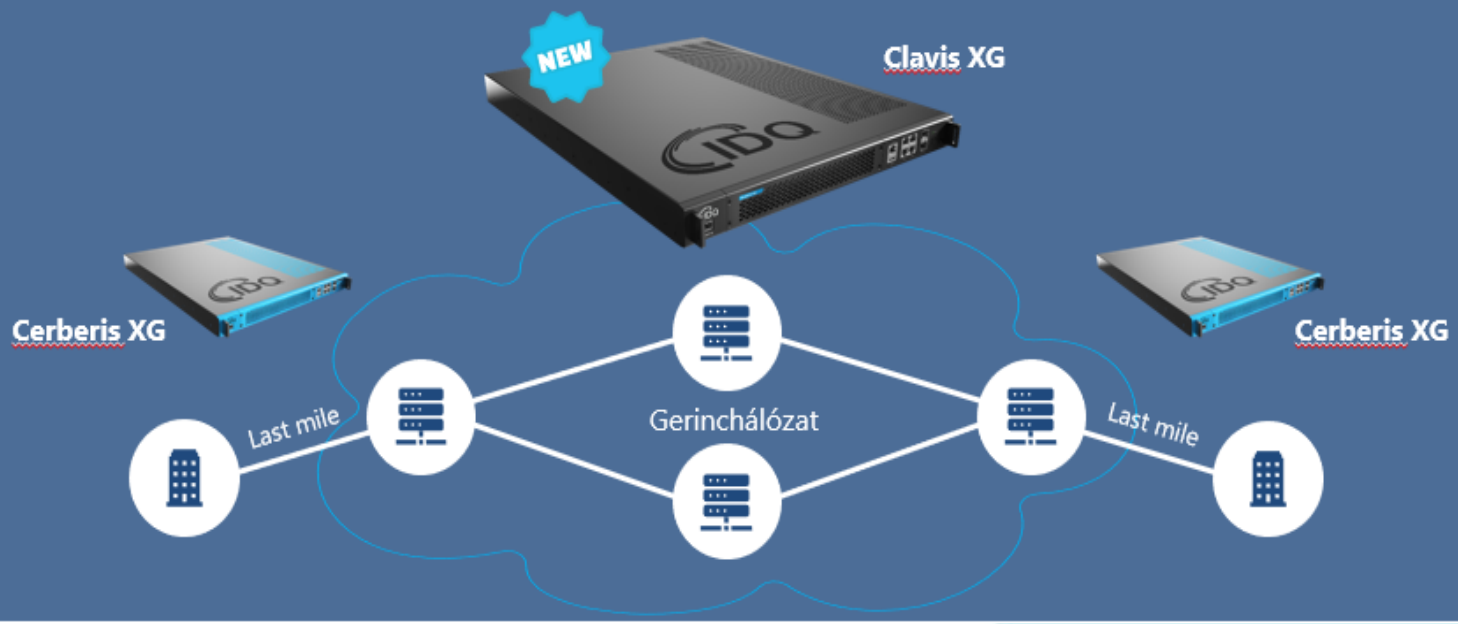


A QKD hozzáadása az infrastruktúrához



A Quantum Key Distribution megoldások első átfogó választéka

- **Bevált és megbízható technológia**
- **Komplex topológiákhoz és kiterjedt telepítésekhez tervezték**

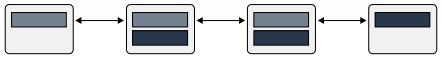


Kulcs menedzselő rendszer – QNET & KMS szoftver

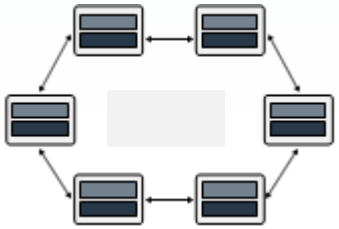
Az XG sorozatú rendszerek bármilyen hálózati konfigurációban telepíthetők:

- **Pont - pont kulcs cserével**
- **Gyűrű**
- **Csillag**
- **Háló**

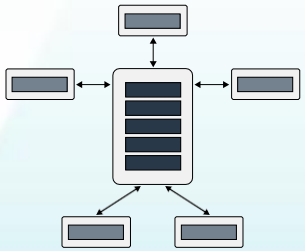
Pont - pont



Gyűrű

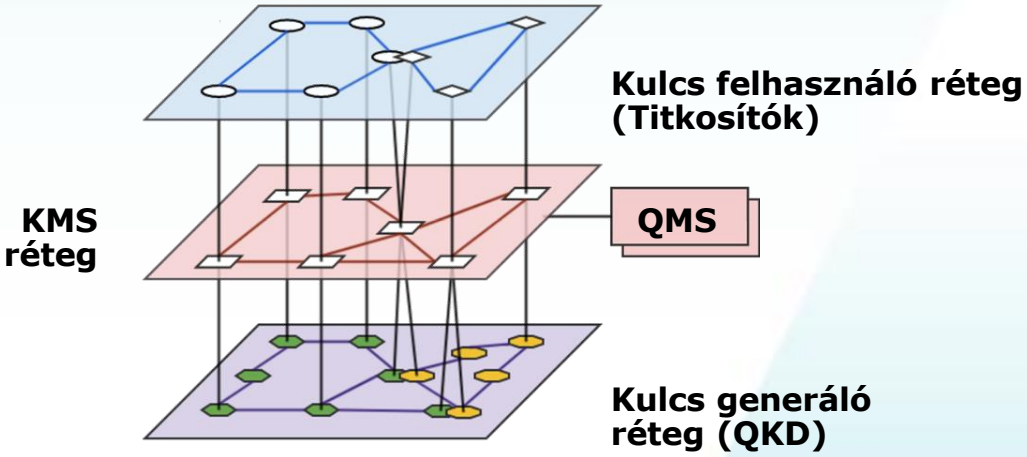


Csillag



Kulcs menedzselő rendszer – QNET & KMS szoftver

Mindegyik QKD csomóponton egy beágyazott kulcskezelő rendszer (KMS) szoftver dönt a QKD közötti kulcselosztásról, és kezeli a kulcskéréseket és a QKD optikai rendszerek és külső titkosítók közötti kulcsátvitelt.



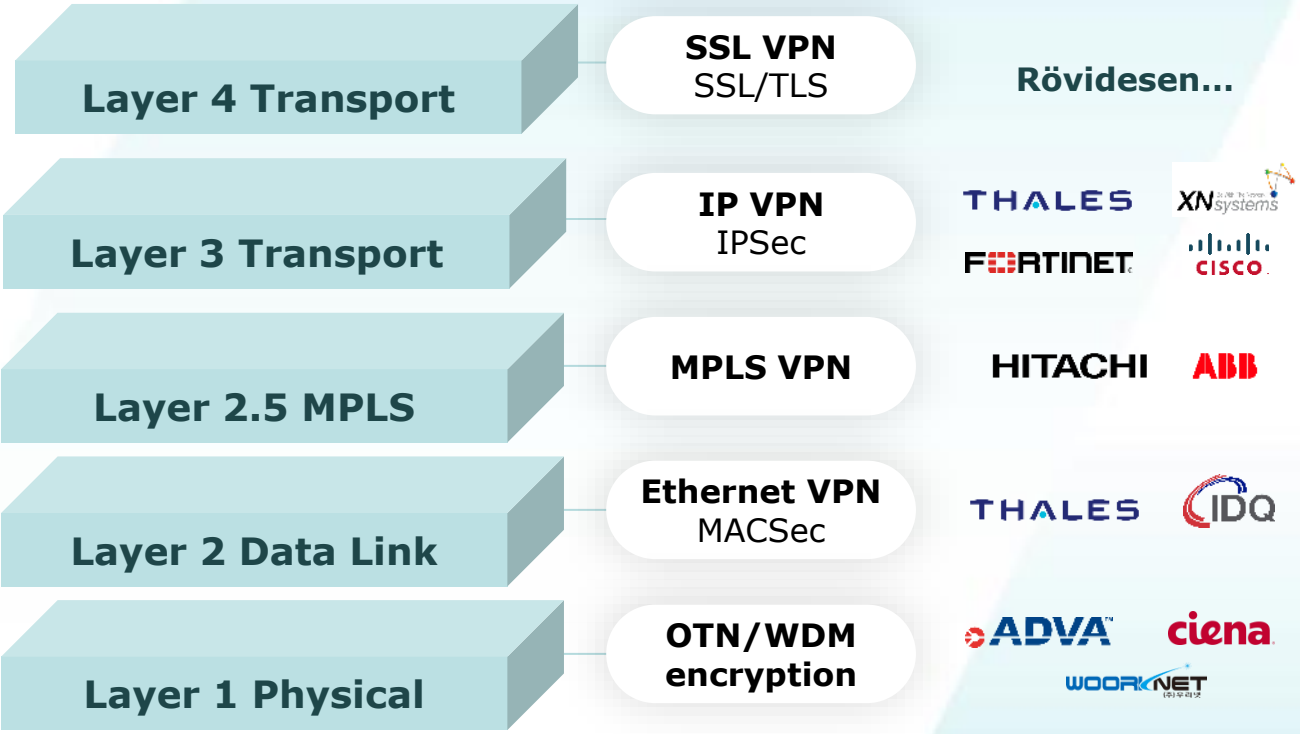
A QKD integrálása meglévő titkosítási megoldásokkal

Az IDQ különböző hálózati titkosítási megoldásokkal működik, amelyek QKD-vel bővíthetőek ki, hogy kvantumbiztosak legyenek

A QKD kiegészítés előnyei:

1. **Szervezetének biztonsága a kvantum utáni korszakban**
2. **A hosszú távú titoktartás elérése és az adatok integritásának elősegítése**
3. **Az inkumbens titkosítási megoldás TCO-jának és ROI-jának javítása**
4. **„hozzáadott értékként” demonstrálható kiberbiztonsági kötelezettségvállalás az érdekelt felek felé**

A QKD integrálása meglévő titkosítási megoldásokkal



Köszönöm a figyelmet!

andras.nagy@atl-fo.eu