# Kvantová komunikace a kryptografie
## Co nás čeká a nemine

**Dr Michal KŘELINA**, michal.krelina@cvut.cz

FJFI ČVUT v Praze

*BS72 – Bezpečnostní seminář: Kvantová a postkvantová kryptografie*
18. 10. 2023

# Obsah

- Hrozba od kvantových počítačů
- Protiopatření – QKD & PQC
- Kvantové sítě/komunikace
- Kvantová distribuce klíče
- EuroQCI
- Standardizace
- Bezpečnost QKD

# Hrozba od kvantových počítačů

- Kvantové počítače budou **velmi efektivní (až exponenciálně)** pro jisté typy výpočtů
  - Ale nikdo neví, kdy tu budou – odhady jsou na úrovni 5 – 30 let
  - Zatím to jsou spíše laboratorní hračky
- **Hrozba pro asymetrická šifrování** (RSA, eliptické křivky, atd.)
  - Shorův algoritmus – exponenciální zrychlení: se stovek tisíc let na minuty a méně
    - RSA2048: budeme potřebovat zhruba 8k perfektních (logických) qubitů nebo 20M nedokonalých (fyzických) qubitů
- Hrozba pro symetrická šifrování (AES, hash, atd.)
  - Např. Grooverův algoritmus – kvadratické zrychlení pro útok formou brutální síly
  - Nároky jsou masivní
- Budoucí hrozby – kvantová informatika je mladá a plná překvapení
  - Slušná šance, že se objeví nový algoritmus, třeba vůči novým kvantově-odolným šifrám
- Hrozba nyní: **Harvest now, decrypt later (HNDL)**
  - Problém pro data, která by měla být utajena po dlouhou dobu
  - Je známo, že Čína již tento útok realizuje

# Protiopatření: QKD a PQC

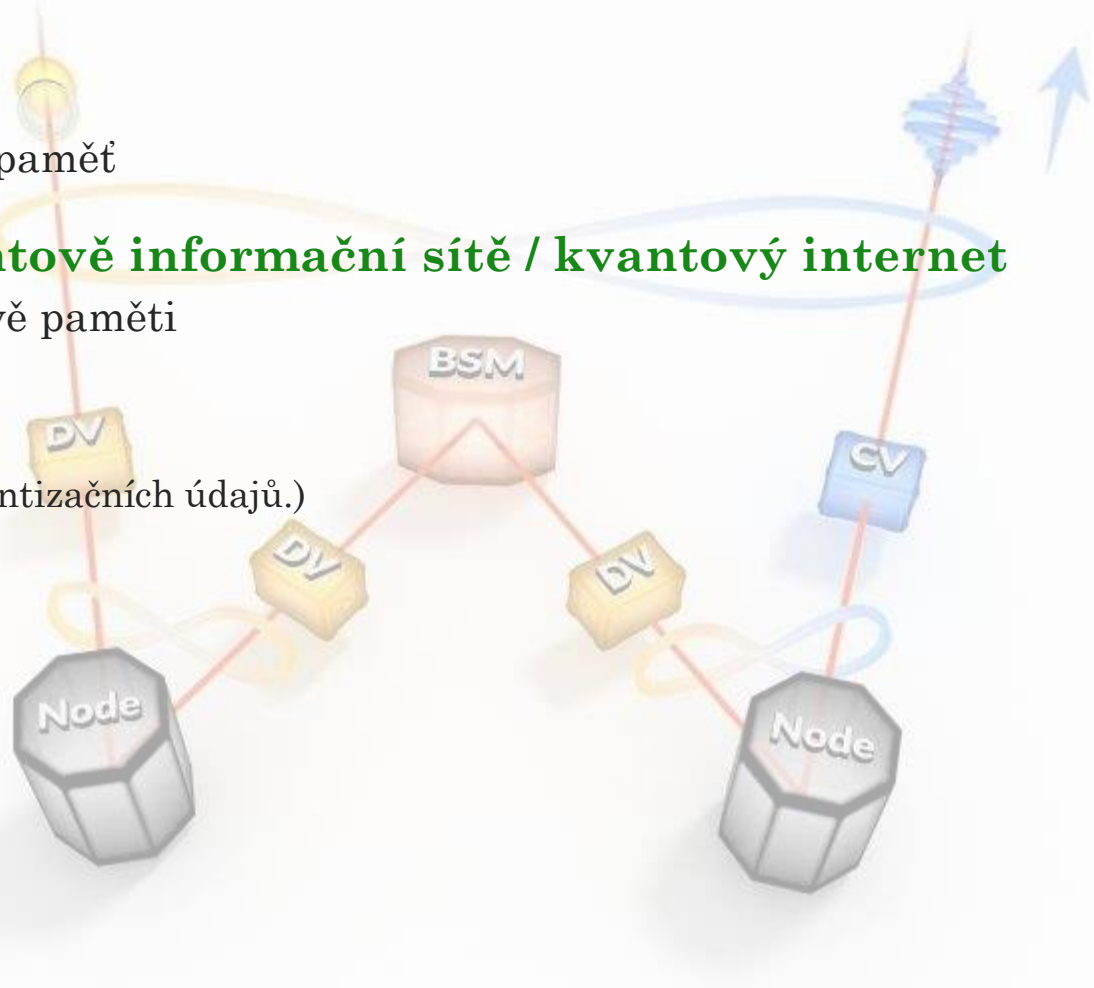
- **QKD (quantum key distribution)** – kvantová distribuce klíče
  - Na bázi kvantové informatiky a fyziky – služba na kvantových sítí
  - Složité na implementaci, potřeba nové infrastruktury
  - Když je to dobře implementované, tak je to neprolomitelné
- **PQC (post-quantum cryptography)** – kvantově odolné šifrování
  - Není to nic kvantového, jenom těžší matematika
  - Jednodušší na implementaci
  - Nikdy nedokážete, že je to neprolomitelné
  - Problém důvěry a standardizace
- **Reálně, nejsou to konkurenti, ale spíše se budou doplňovat**
  - **Včetně hybridních forem kombinující obě metody**

# Kvantové sítě/komunikace I

- Cílem je přenesení kvantové informace – kvantových bitů (qubitů)
- Qubity mají speciální vlastnosti:
  - Jako klasické bity, mohou mít hodnotu 0 nebo 1, ale i jejich superkombinaci – **superpozice**
  - Nelze je zkopírovat – **no-cloning theorem**
  - Dva a více qubitů mohou být silně korelované – **kvantové provázání**
- Na nejnižší úrovni v případě kvantových sítí používá **jednotlivé fotony** (anebo skupinky fotonů)
  - Velmi citlivý systém, musíme je vyrábět i detekovat
  - Exponenciální ztráty v optických vláknech
  - Kvadratické ztráty ve volném prostoru
- **Klíčový problém:** fotony nemůžeme zesílit, jako to děláme u optické komunikace
  - Dosah bod-bod: 80-100 km, se speciálními protokoly a technologií až 500 km (ale velmi pomalé)
  - Pro delší vzdálenosti potřebujeme opakovače: věrohodný vs kvantový
  - Můžeme použít satelity – efektivně jen 10 km atmosféry, pak prázdno
- **Pozor, kvantová síť vždy bude potřebovat ke svému provozu i tu klasickou!**

# Kvantové sítě/komunikace II

- **1. generace kvantových sítí**
  - To je to, co máme dnes.
  - Komerčně dostupné
  - Jediná služba: QKD
  - Nepotřebuje provázání a ani kvantovou paměť
- **2. generace kvantových sítí – kvantově informační sítě / kvantový internet**
  - Na bázi kvantového provázání a kvantově paměti
  - Mnoho služeb (kromě QKD):
    - Přímá kvantová komunikace
    - Bezpečná identifikace (bez prozrazení autentizačních údajů.)
    - Autorizace na základě vaší polohy
    - Slepé a distribuované kvantové počítání
    - Bezpečné sdílení mezi více účastníky
    - Bezpečné a anonymní volby
    - Přesnější synchronizace času
    - Kvantově síťované kvantové senzory
    - A další se vyvíjí



# Kvantová distribuce klíče I

- Účel: poslat šifrovací klíč z místa A do místa B, podobně jako u asymetrického šifrování
- Tři rodiny QKD protokolů:
  - Připrav a změř (Prepare & measure), např. BB84
  - Na bázi provázání (Entanglement based), např. E91
  - Nezávislé na měřícím stroji (Measurement Device Independent)
- **QKD protokoly:**
  - Přenos fotonů/qubitů (různé kódování)
  - Prosívání
  - Korekce kvantových chyb
  - Zesílení zabezpečení
- Komerčně dostupné
  - ID Quantique, Toshiba, startupy

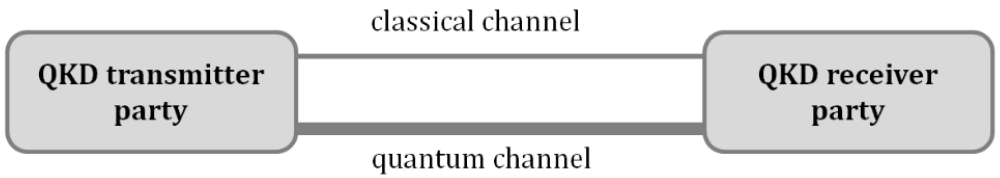



Figure 1 — Prepare-and-measure QKD protocol

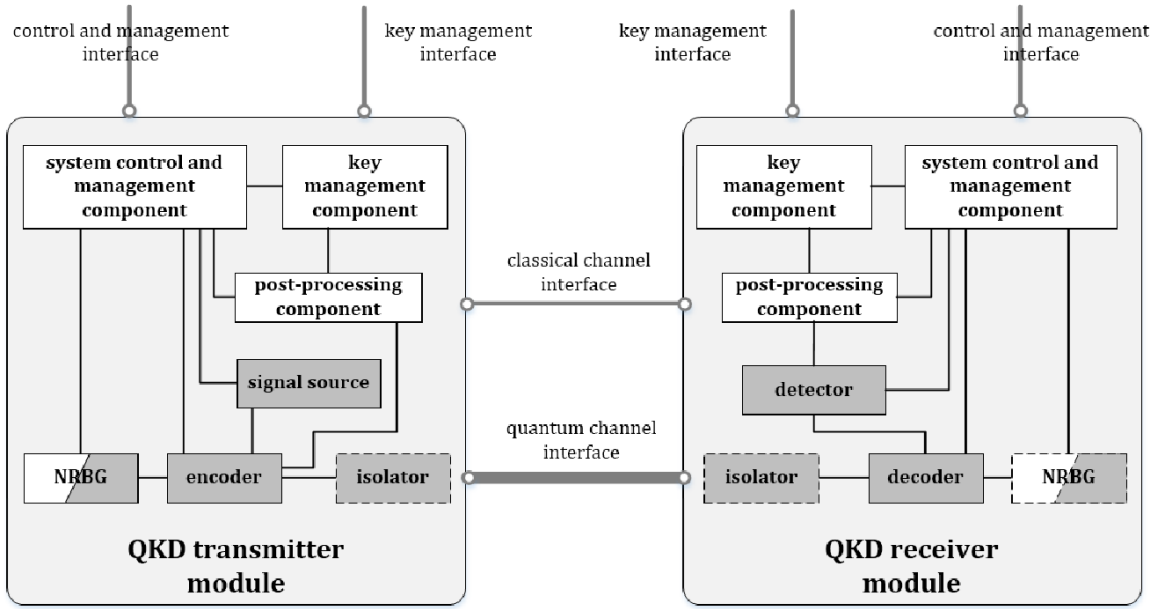



Figure 5 — Generic internal structure of a P&M-QKD protocol implementation

# Kvantová distribuce klíče II

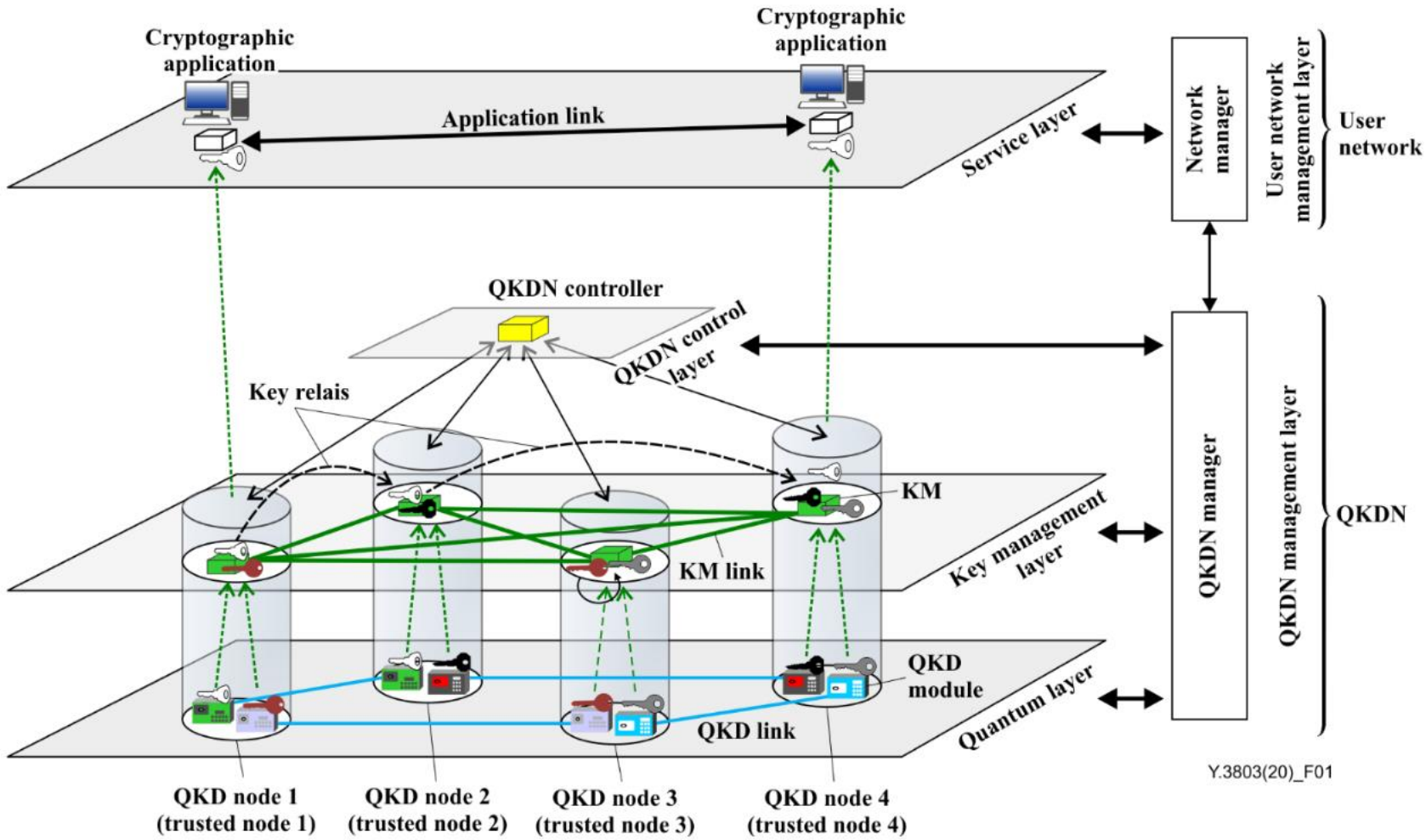



**Figure 1 – Basic key management operations in a QKDN**

# Kvantová distribuce klíče III

- **Využití:**
  - Zabezpečení konkrétních spojů (centrála-backup/datové centrum)
  - Podnikové MAN sítě
  - SCADA kritické infrastruktury
  - Zabezpečení backbone linek a long-haul spojů
  - Velmi vysoký stupeň zabezpečeného přístupu
  - Obnova před-nahraných klíčů

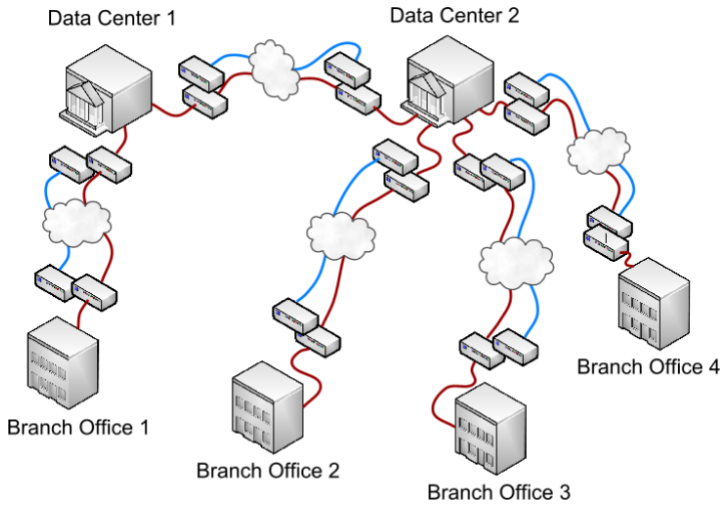
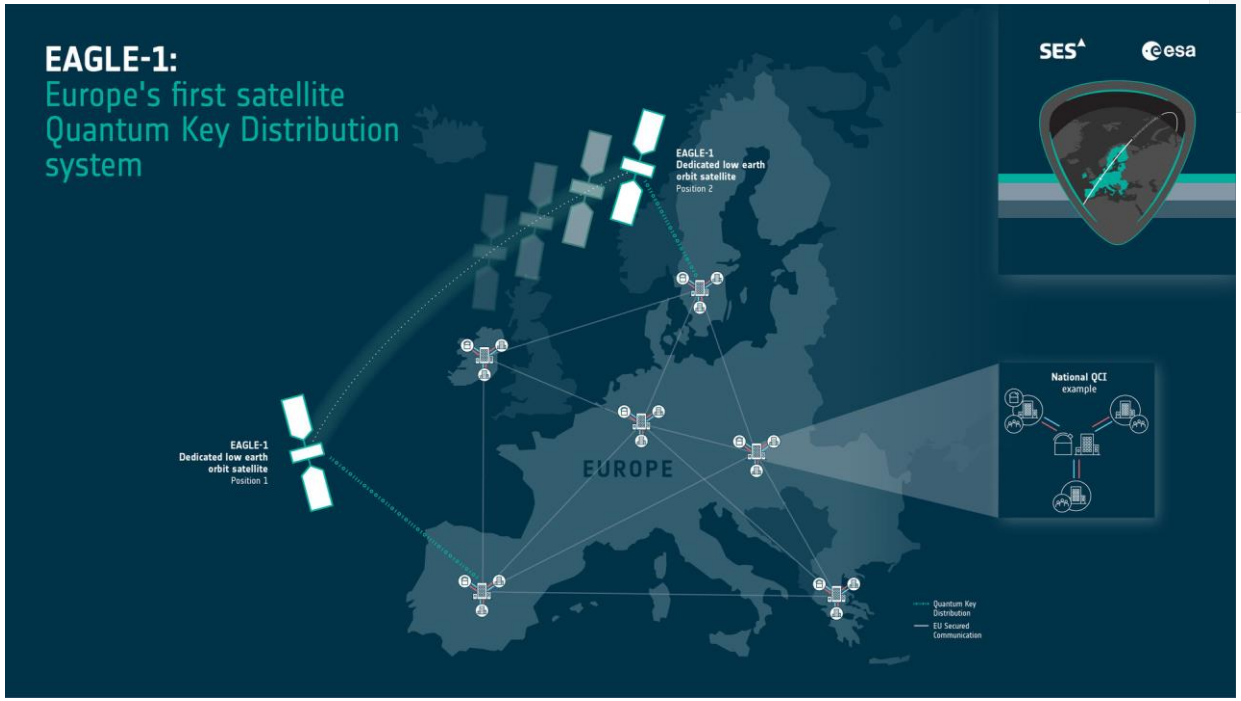


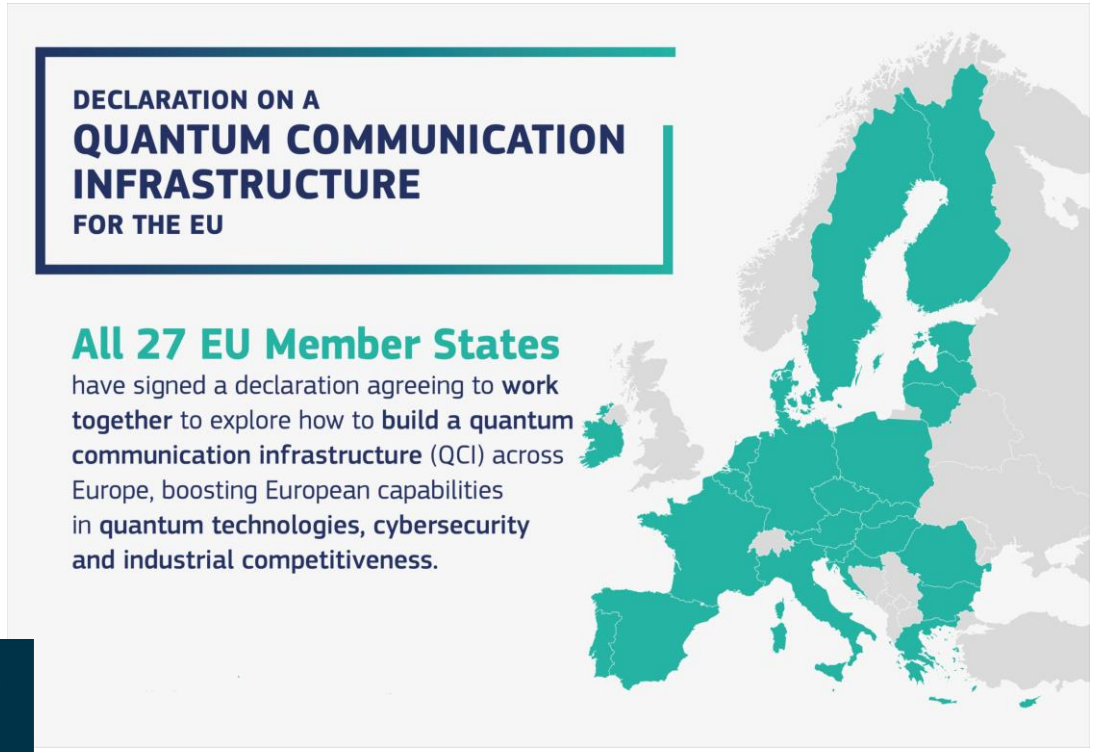

**Figure 5: Enterprise MAN using QKD link encryptors**

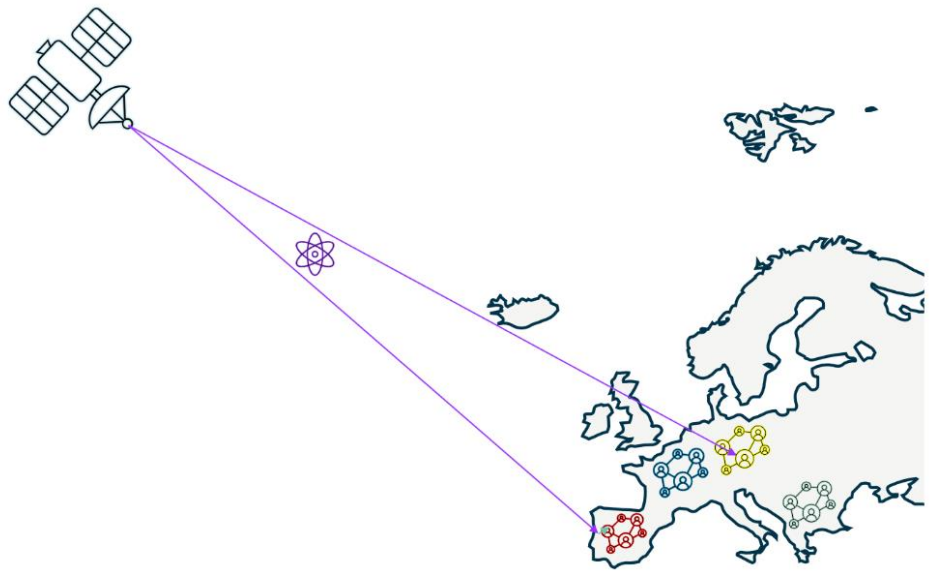
- **Příklady:**
  - Ženeva: zabezpečení ústředního volebního štábu s datacentrem
  - Londýn: HSBC propojení centrály s datacentrem za městem
  - Integrovaná kvantová síť v Číně
  - EuroQCI
  - A spousta dalších testbedů a testovacích spojů

# EuroQCI

- Panevropská kvantová síť
- Skládá se z národních kvantových sítí
  - Ty budou propojené
- Až do úrovně EU SECRET



# QKD - Standardizace

- ETSI GS QKD 016 V1.1.1 (2023-04) *Published*
  Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules
  *An update is in preparation.* DETAILS ALERT
- ETSI GS QKD 018 V1.1.1 (2022-04) *Published*
  Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks
- ETSI GS QKD 015 V2.1.1 (2022-04) *Published*
  Quantum Key Distribution (QKD); Control Interface for Software Defined Networks
  *An update is in preparation.* DETAILS ALERT
- ETSI GS QKD 015 V1.1.1 (2021-03) *Published*
  Quantum Key Distribution (QKD); Control Interface for Software Defined Networks
  *An update is in preparation.* DETAILS ALERT
- ETSI GS QKD 004 V2.1.1 (2020-08) *Published*
  Quantum Key Distribution (QKD); Application Interface
  *An update is in preparation.* DETAILS ALERT
- ETSI GS QKD 012 V1.1.1 (2019-02) *Published*
  Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment
- ETSI GS QKD 014 V1.1.1 (2019-02) *Published*
  Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API
- ETSI GR QKD 007 V1.1.1 (2018-12) *Published*
  Quantum Key Distribution (QKD); Vocabulary

Y.3800-Y.3999: Quantum key distribution networks

- Y.3800: Overview on networks supporting quantum key distribution
- Y.3801: Functional requirements for quantum key distribution networks
- Y.3802: Quantum key distribution networks – Functional architecture
- Y.3803: Quantum key distribution networks – Key management
- Y.3804: Quantum key distribution networks – Control and management
- Y.3805: Quantum key distribution networks – Software-defined networking control
- Y.3806: Quantum key distribution networks – Requirements for quality of service assurance
- Y.3807: Quantum key distribution networks – Quality of service parameters
- Y.3808: Framework for integration of quantum key distribution network and secure storage network
- Y.3809: A role-based model in quantum key distribution networks deployment
- Y.3810: Quantum key distribution network interworking – Framework
- Y.3811: Quantum key distribution networks – Functional architecture for quality of service assurance
- Y.3812: Quantum key distribution networks - Requirements for machine learning based quality of service assurance
- Y.3813: Quantum key distribution network interworking – Functional requirements
- Y.3814: Quantum key distribution networks – functional requirements and architecture for machine learning enablement
- Y.3815: Quantum key distribution networks - overview of resilience
- Y.3816: Quantum key distribution networks - Functional architecture enhancement of machine learning based quality of service assurance
- Y.3817: Quantum key distribution networks interworking - Requirements of quality of service assurance
- Y.3818: Quantum key distribution networks interworking - architecture

## ISO/IEC 23837-1:2023

### Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements

### Abstract

Preview

This document specifies a general framework for the security evaluation of quantum key distribution (QKD) according to the ISO/IEC 15408 series. Specifically, it specifies a baseline set of common security functional requirements (SFRs) for QKD modules, including SFRs on the conventional network components and the quantum optical components, and the entire implementation of QKD protocols. To facilitate the analysis of SFRs, security problems that QKD modules can face in their operational environment are analysed based on a structural analysis of the security functionality of QKD modules and the classification of QKD protocols.

The SFRs on conventional network components of QKD modules are mainly characterized under the framework of the ISO/IEC 15408 series and also refer to the methodology of ISO/IEC 19790 and relevant standards on testing of cryptographic modules and network devices.

### General information

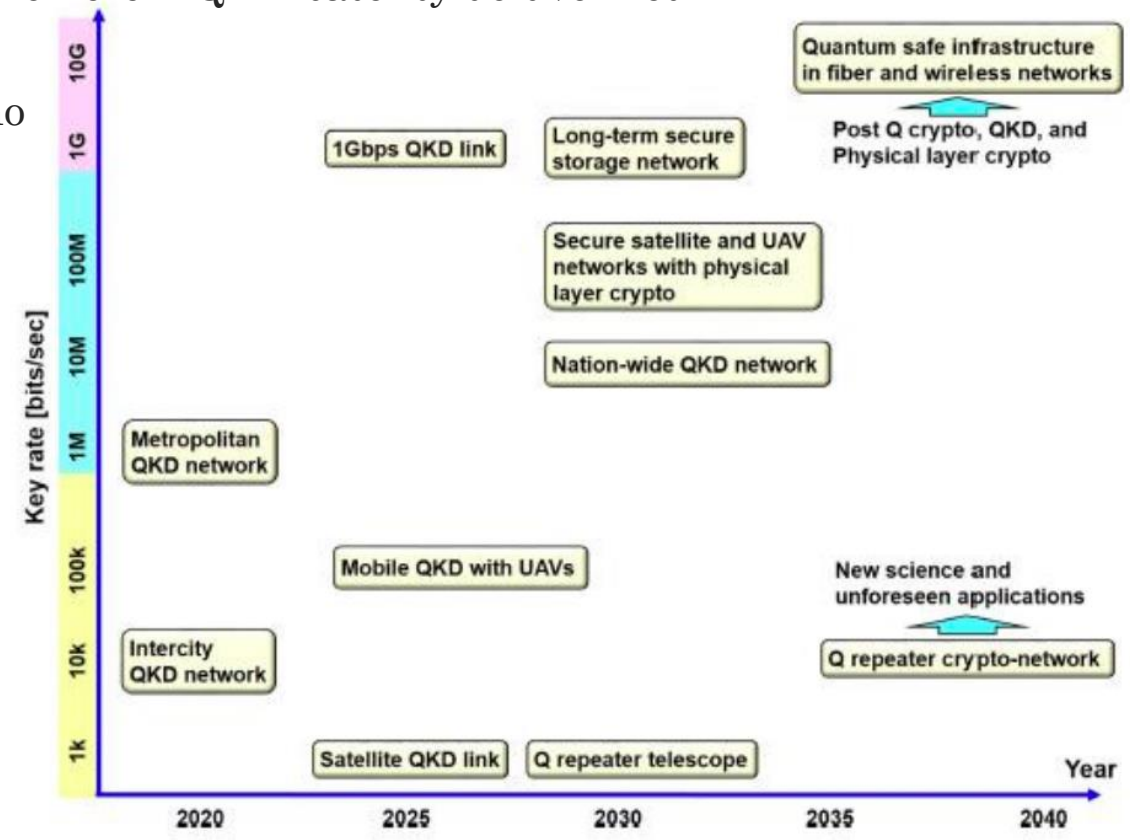
| | |
|---|---|
| **Status** : Published | **Publication date** : 2023-08 |
| **Edition** : 1 | **Number of pages** : 52 |

# QKD - bezpečnost

- **Vědecko-výzkumný pohled:**
  - Quantum hacking – teoretické i experimentální pokusy o prolomení QKD
  - Spousta teoretických důkazů o bezpečnosti platí jen za určitých předpokladů
- **Kyber bezpečnostní pohled:**
  - Potřebuji vše zabezpečit horizontálně i vertikálně
  - Koncové body = nejslabší článek
  - Poměrně slabá odolnost vůči DoS
- **Aktivity:**
  - Infrastruktura pro testování a hodnocení evropské kvantové komunikační infrastruktury (EuroQCI)
  - Bezpečnostní rámce:
    - ETSI GS QKD 008 V1.1.1 - QKD Module Security Specification
    - ETSI GS QKD 005 V1.1.1 - Security Proofs
    - Recommendation ITU-T X.1710 - Security framework for quantum key distribution networks
    - ISO/IEC DIS 23837-1:2022 - Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements
    - ISO/IEC DIS 23837-2:2022 - Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Test and evaluation methods

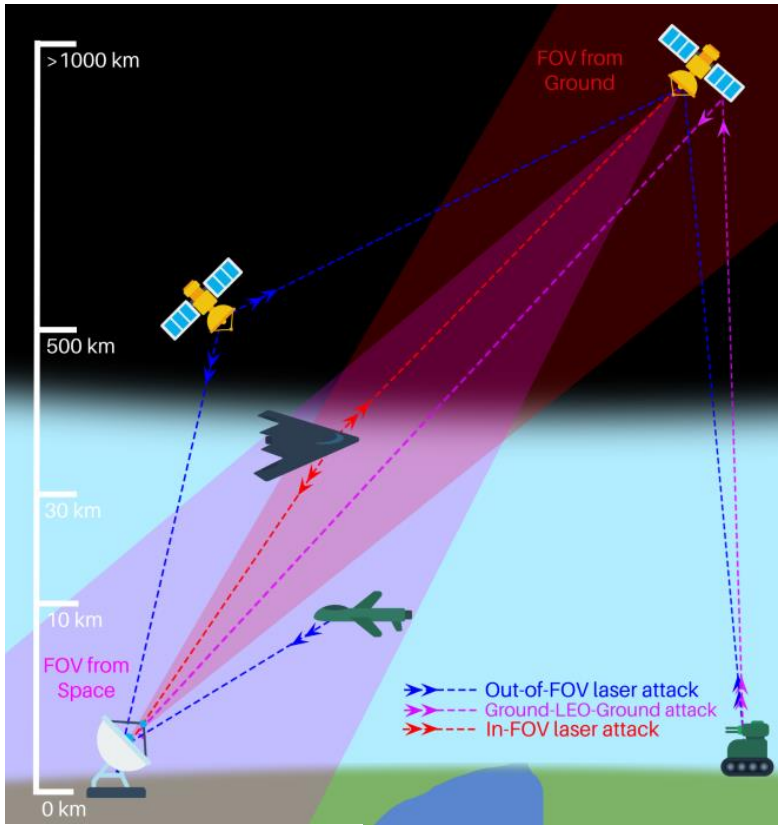
# Kvantové komunikace - výhled

- QKD zatím nedoporučované příslušnými autoritami
- Na vědecko-výzkumné úrovni je podpora docela slušná – vzniká spousta testbedů
- Rozvoj platforem:
  - Satelity: Čína má nahoře již druhou generaci, komerční QKD satelity do dvou let
  - Drony – na úrovni laboratorního testování
  - Podvodní QKD – spíše výzkum, nic praktického
  - Kombinace QKD s laserovou komunikací?
- **EuroQCI**
  - Vývoj a testování již v běhu
  - 2023 – první QKD satelit (Eagle I)
  - 2030 – vypuštění CLA satelitů
  - 2024 – Počáteční (testovací) provoz
  - 2027 – UNCLA provoz
  - 2030 – CLA provoz



# Kvantové sítě - rušení

- https://arxiv.org/abs/2310.08728
- Stačí i velmi malý výkon laseru pro dostatečný šum
- Výzva je zaměřit daný kvantový přijímač (např. satelit)




| | In-FOV attack | | | Out-of-FOV attack | | |
|---|---|---|---|---|---|---|
| **Scenario** | **Likelihood** | **Impact** | **Risk** | **Likelihood** | **Impact** | **Risk** |
| Ground-LEO-Ground | No | No | None | Frequent | Marginal | Serious |
| Ground-LEO | Improbable | Catastrophic | Medium | Probable | Marginal | Serious |
| Ground-GEO | Improbable | Critical | Medium | Frequent | Marginal | Serious |
| Air-Ground | Improbable | Critical | Medium | Remote | Marginal | Medium |
| Air-LEO | Improbable | Critical | Medium | Frequent | Marginal | Serious |
| LEO-Ground | Improbable | Marginal | Low | Probable | Marginal | Serious |
| LEO-LEO | Improbable | Critical | Medium | Remote | Marginal | Medium |
| LEO-GEO | Improbable | Marginal | Low | Remote | Marginal | Medium |
| GEO-Ground | Improbable | Marginal | Low | Frequent | Marginal | Serious |

# Reklama

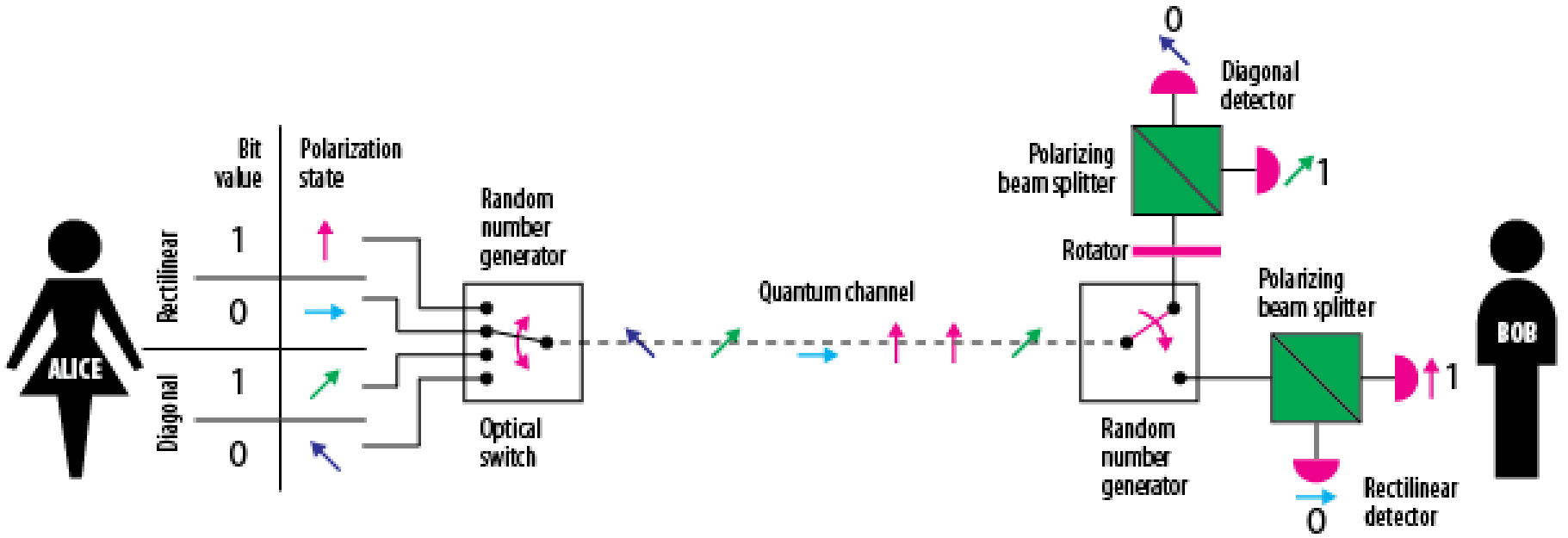
- Pravidelné novinky ze světa kvantových technologií na https://qubits.cz/
  - Týdenní přehled přebírá i https://www.lupa.cz/serialy/qubity/
- Novinky z oblasti kvantové bezpečnosti dávám na LinkedIn
  - https://www.linkedin.com/in/krelina/

**Děkuji za pozornost.**

V případě pozdějších dotazů, napište email ;-)

Michal KŘELINA, michal.krelina@cvut.cz

# BB84




| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Quantum transmission & detection | ALICE sends photons | ↖ | ↗ | → | ↑ | ↑ | ↗ | ↖ | ↑ |
| | ALICE's random bits | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| | BOB's detection events | ↑ | ↗ | ↖ | ↑ | ↗ | ↗ | ↖ | ↖ |
| | BOB's detected bit values | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| Public discussion (i.e., sifting) | BOB tells ALICE the basis choices he made | Rect | Diag | Diag | Rect | Diag | Diag | Diag | Diag |
| | ALICE tells BOB which bits to keep | | ✔ | | ✔ | | ✔ | ✔ | |
| | ALICE and BOB's shared sifted key | – | 1 | – | 1 | – | 1 | 0 | – |