Pohled a přístup NÚKIB

ke kvantové distribuci klíčů

CyberCon 2022

RNDr. Bohuslav Rudolf,

zástupce ČR v Euro QCI Security Group

a zástupce NÚKIB v Euro QCI

Předběžné informace,

kterým se těžko vyhnout:

Reakce na kvantovou hrozbu

Připomenutí podstaty kvantové hrozby

Kvantová hrozba: V případě konstrukce kryptologicky relevantních kvantových počítačů dojde ke zlomení **nejrozšířenějších kryptografických systémů s veřejnými klíči.**

Aktuální rizika kvantové hrozby: zpětné luštění v budoucnosti

1) Odposlechni šifrovanou komunikaci
2) Ulož ji
3) Jakmile budeš mít vhodný kvantový počítač, vylušti ji.

V ohrožení jsou zejména informace vyžadující dlouhodobou ochranu své důvěrnosti.

Možnosti reakce na kvantovou hrozbu

a) Větší využití **symetrické kryptografie** – nepříliš praktické řešení, nelze využít výhod kryptografie s veřejnými klíči.

b) Využití **PQC (*Post Quantum Cryptography*) post-kvantové kryptografie** – kryptografie s veřejnými klíči odolná (avšak podmíněně) proti kvantové hrozbě

c) Využití **QKD (*Quantum Key Distribution*) kvantové distribuce klíčů** – ustanovení kryptografických klíčů, jehož bezpečnost je důsledkem zákonů kvantové mechaniky (nepodmíněná odolnost).

Současný přístup k reakci na kvantovou hrozbu

Kvantově odolná kryptografie PQC

- **Hlavní nástroj ochrany proti kvantové hrozbě**
- Plnohodnotně nahradí dosavadní kryptografii s veřejnými klíči
- Kryptografické algoritmy mající tzv. výpočetní bezpečnost,
- Jejich bezpečnost tedy nelze dokázat a je dána především neúspěšností a rozsáhlostí dosavadních snah o její prolomení

Kvantová kryptografie – kvantová distribuce klíčů QKD

- **Doplňkový (možná konkurenční) nástroj ochrany proti kvantové hrozbě**
- Zatím je reálná pouze tzv. „kvantová distribuce klíčů“ QKD (nikoliv „kvantové podpisy“)
- Má nepodmíněnou bezpečnost

Typy QKD z hlediska svého nasazení

Typy QKD z hledisek:

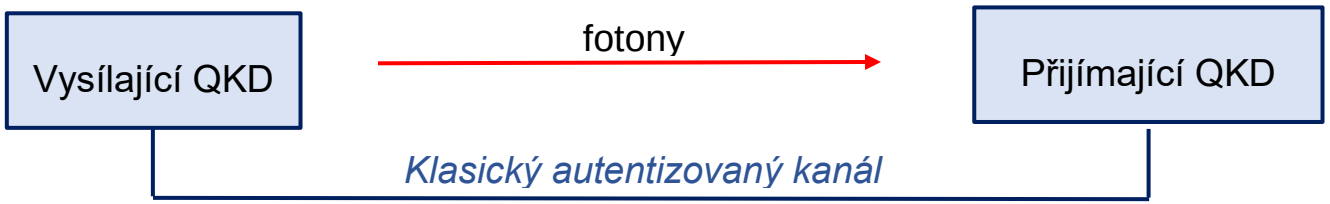
- **Principu svého fungování**
- **Fyzikálního komunikačního kanálu**

Dva hlavní typy QKD z hlediska principu svého fungování:

QKD typu: „Připrav a změř“

Jedno QKD-zařízení vysílá fotony, druhé QKD-zařízení je detekuje.

- Hlavní výhoda: poměrně rychlé ustanovování QKD klíčů.
- Hlavní nevýhoda: problém s dokazatelností implementační bezpečnosti.



QKD na bázi *entanglementu*:

Zdrojové QKD-zařízení vysílá provázané (entaglované) dvojice fotonů, každé z obou přijímacích QKD-zařízení detekuje „jemu příslušející fotony“ a obě přijímací QKD-zařízeníspolečně ustanoví QKD-klíč.

- Hlavní výhoda: „náběh“ na dokazatelnou implementační bezpečnost.
- Hlavní nevýhoda: velmi pomalé ustanovování QKD klíčů.

Dva hlavní typy QKD z hlediska fyzikálního komunikačního kanálu

Pozemní QKD

QKD-zařízení jsou propojena pomocí **optických vláken**.

Hlavní omezení: Efektivní bezpečné ustanovení QKD klíčů typu End-to-End typicky do 100 km, maximálně do 300 km.

QKD využívající satelity

QKD-zařízení jsou v tomto případě dvojího typu:

- Satelitní
- Pozemské stanice

Fyzikálním komunikačním kanálem je volný prostor.

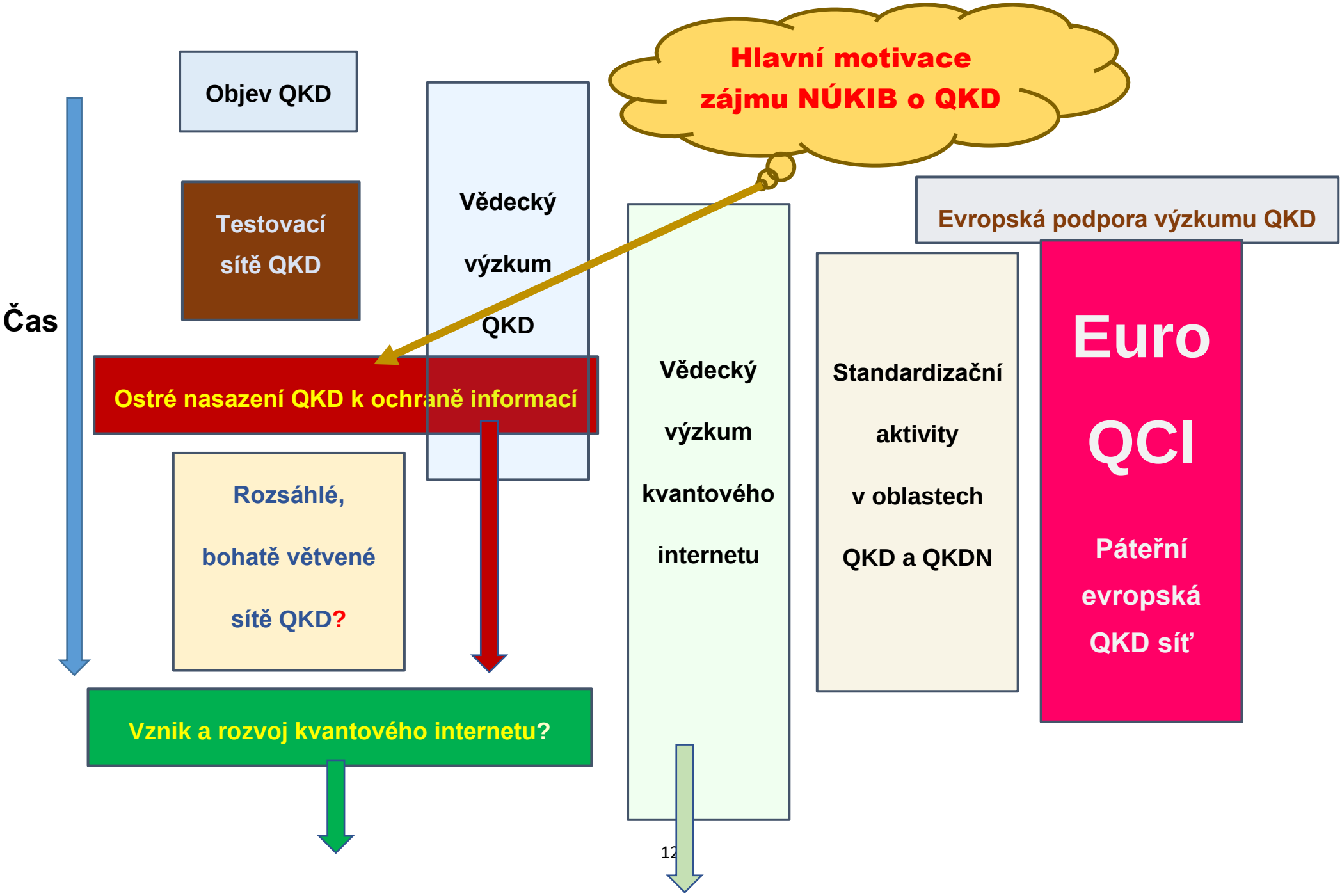
Hlavní výhoda proti pozemnímu QKD: Lze dosáhnout ustanovení QKD-klíčů i na velké pozemské vzdálenosti.

Dilema: V případě QKD typu „připrav a změř“ je problém s bezpečností satelitního QKD-zařízení.
V případě QKD na bázi entanglementu bezpečnost satelitního QKD sice není problémem, ale ustanovování QKD-klíčů je velmi (mimořádně) pomalé, a navíc musí být v době služby na obě pozemská zařízení „vidět“.

Další problém: Dostupnost služby závisí v tomto případě na počasí!

Dosavadní a předpokládaný vývoj problematiky QKD (QCI)

a hlavní zájmová oblast NÚKIB


Hlavní motivace zájmu NÚKIB o QKD
Objev QKD
Testovací sítě QKD
Vědecký výzkum QKD
Evropská podpora výzkumu QKD
Čas
Ostré nasazení QKD k ochraně informací
Vědecký výzkum kvantového internetu
Standardizační aktivity v oblastech QKD a QKDN
Euro QCI
Páteřní evropská QKD síť
Rozsáhlé, bohatě větvené sítě QKD?
Vznik a rozvoj kvantového internetu?

Nejdůležitější skutečnosti ovlivňující přístup NÚKIB

k podpoře rozvoje

kvantové distribuce klíčů

A) Hlavní motivace a úskalí

podpory ostrého nasazení

kvantové distribuce klíčů

v blízké budoucnosti

Hlavní motivace

Hlavním nástrojem obrany proti kvantové hrozbě je sice PQC – kvantově odolná kryptografie, ale….

Prosazovatelé nasazení QKD argumentují

A) **Podmíněností bezpečnosti PQC.** Nelze vyloučit, že v budoucnosti budou objeveny luštící algoritmy, které zlomí buď některé nebo dokonce všechny algoritmy PQC.

B) **Nepodmíněností bezpečnosti QKD.** Bezpečnost QKD je dána zákony kvantové fyziky, a tudíž ji nelze zlomit bez jejich porušení.

Úskalí ostrého nasazení pozemního QKD v blízké budoucnosti:

QKD nemůže v mnoha svých aspektech konkurovat PQC (kvantově odolné algoritmické kryptografii s veřejnými klíči).

Cena

- PQC je/bude v podstatě zadarmo a nepotřebuje žádné specifické přenosové prostředí.
- QKD je stále ještě poměrně drahé zařízení a jako přenosové prostředí potřebuje optická vlákna, typicky „temná optická vlákna“,

Bezpečnost typu: End-to-End

- PQC bez problémů zajišťuje bezpečnost typu End-to-End.
- Pozemní QKD v současnosti zajišťuje bezpečnost typu End-to-End typicky pouze do 100 km. Na delší vzdálenosti typicky End-to-End-bezpečnost nezajišťuje!

Zranitelnost útoky na dostupnost služby

- U malých (málo větvených) QKD sítí – snadná zranitelnost útoky na dostupnost služby.

Úskalí ostrého nasazení QKD využívající satelity v blízké budoucnosti:

Připomenutí:

Hlavní motivací pro QKD využívajícího satelity je možnost ustanovení QKD-klíčů na velké vzdálenosti.

Již zmíněné dilema

A) **QKD na bázi „Připrav a změř“** – pak ale musí být satelit důvěryhodným uzlem (bezpečnostní problém).

B) **QKD na bázi *entanglementu*** – pak ale dosáhneme „velmi bídné“ rychlosti ustanovování QKD-klíčů.

Výměna QKD zařízení

- V případě potřeby vyměnit (porouchané nebo zastaralé nebo nedostatečně bezpečné) QKD-zařízení za nové to zřejmě bude znamenat vypuštění nového satelitu.
- Zatímco bezpečná vzdálená výměna PQC nebude problém.

Závislost dostupnosti služby QKD využívajícího satelity na počasí

O implementační (ne)bezpečnosti QKD

Aby uvažovaná **implementace QKD** byla nepodmíněně dlouhodobě bezpečná, musí splňovat všechny **předpoklady** důkazu bezpečnosti použitého QKD-protokolu.

A to je problém!

Není snadné vyvinout QKD-zařízení, které by prokazatelně naplnilo

předpoklady důkazu bezpečnosti QKD-protokolu.

Implementační útoky na QKD – ještě větším problémem je fakt, že:

Na řadu realizací QKD-protokolů byly skutečně navrženy a uskutečněny **úspěšné útoky na implementaci**.

Ochraně proti implementačním útokům

byla v tzv. kvantové kryptografii věnována v posledních 10 letech mimořádná pozornost.

Implementační útok na *COW-QKD*-protokol – za závažný a do značné míry i za signifikantní příklad považuji fakt, že:

Na jedno z finančně dostupnějších komerčních QKD-zařízení na bázi ***Coherent One Way QKD*** byl **v roce 2021** objeven **závažný útok**.

B) Argumenty pro podporu

prací na rozvoji QKD

a na přípravě možnosti nasazení QKD

Technologické argumenty pro podporu přípravy nasazení QKD

1) Již zmíněná „nepodmíněná dlouhodobá bezpečnost QKD“.

2) Ve světě probíhá tzv. „**druhá kvantová revoluce**“ – bouřlivý rozvoj nových kvantových technologií, často relevantních pro informační a kybernetickou bezpečnost. **Rozvoj QKD je její součástí**.

3) QKD sítě se ve střednědobé, ale spíše až ve dlouhodobé budoucnosti pravděpodobně stanou základem **kvantového internetu**, tedy internetu, který bude propojovat rovněž kvantové počítače a který umožní komunikaci pomocí provázaných qubitů (přenosy kvantové informace).

Strategické a společenské argumenty pro podporu přípravy nasazení QKD

4) **Relevantní bezpečnostní autority** jako NSA, NCSC a ANSSI se sice stavějí proti ostrému nasazení QKD v nejbližší budoucnosti, ale **podporují výzkum a vývoj v oblasti QKD**.

5) **Evropská Unie uvolnila masivní finanční prostředky** na přípravu ostrého nasazení QKD k ochraně důvěrnosti vybraných informací.

6) Financování programů typu **Open QKD**, dále přípravy páteřní Evropské kvantové QKD infrastruktury, tzv. **Euro-QCI**, (***QCI – Quantum Communication Infrastructure***)

Pravděpodobná příčina toho všeho

7) **Náskok Číny** v oblasti testování a rozsáhlého nasazení QKD.

C) Stanoviska relevantních

bezpečnostních autorit NATO

k případnému ostrému nasazení QKD

v blízké budoucnosti

Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

National Security Agency/Central Security Service > Cybersecurity > Quantum Key Distribution (QKD) and Quantum Cryptography QC (nsa.gov)

Synopsis

NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

NSA nedoporučuje použití kvantové distribuce klíčů a kvantové kryptografie pro zabezpečení přenosu dat v národních bezpečnostních systémech (NSS), pokud nebudou překonána níže uvedená omezení.

O jaká (výše zmíněná) omezení se jedná?

1. Quantum key distribution is only a partial solution.

Současná QKD vyžaduje zajištění autentičnosti klasické komunikace mezi QKD-zařízeními.

2. Quantum key distribution requires special purpose equipment.

QKD vyžaduje optická vlákna nebo satelitní přenos, má problémy s výměnou (v porovnání s PQC).

3. Quantum key distribution increases infrastructure costs and insider threat risks.

Mimo jiné narážka na „důvěryhodné uzly“.

4. Securing and validating quantum key distribution is a significant challenge.

Zejména problém nedostatečných garancí implementační bezpečnosti.

5. Quantum key distribution increases the risk of denial of service.

Zvýšené riziko úspěšnosti útoku na dostupnost služby.

Závěr stanoviska NSA/CSS

Conclusion
In summary, NSA views quantum-resistant (or post-quantum) cryptography as a more cost effective and easily maintained solution than quantum key distribution. For all of these reasons, NSA does not support the usage of QKD or QC to protect communications in National Security Systems, and does not anticipate certifying or approving any QKD or QC security products for usage by NSS customers unless these limitations are overcome.

NSA nepodporuje použití QKD nebo QC k ochraně komunikace v národních bezpečnostních systémech a nepředpokládá certifikaci nebo schválení jakýchkoli bezpečnostních produktů QKD nebo QC pro použití zákazníky NSS, pokud tato omezení nebudou překonána.

National Cyber Security Centre

Quantum security technologies

Quantum Key Distribution

Quantum security technologies - NCSC.GOV.UK

NCSC Position

Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the **NCSC does not endorse the use of QKD for any government or military applications**, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.

In addition, we advise that any other organisations considering the use of QKD as a key agreement mechanism ensure that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them.

NCSC advice is that the best mitigation against the threat of quantum computers is quantum-safe cryptography. Our white paper on quantum-safe cryptography is available on the NCSC website.

Nejdůležitější části v češtině

NCSC nepodporuje použití QKD pro jakékoli vládní nebo vojenské aplikace,

a varuje před výhradním spoléháním se na QKD pro kritické obchodní sítě, zejména v sektorech kritické národní infrastruktury.

Rada NCSC zní, že nejlepším zmírněním hrozby kvantových počítačů je kvantově bezpečná kryptografie.

ANSSI | Agence nationale de la sécurité des systèmes d'information

SHOULD QUANTUM KEY DISTRIBUTION BE USED FOR SECURE COMMUNICATIONS?

Should Quantum Key Distribution be Used for Secure Communications? | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Summary

Quantum Key Distribution (QKD) presents itself as a technology functionally equivalent to asymmetric key agreement schemes that are used in nearly all secure communication protocols over the Internet or in private networks. The defining characteristic of QKD is its alleged superior secrecy guarantee that would justify its use for high security applications. However, deployment constraints specific to QKD hinder large-scale deployments with high practical security. Furthermore, new threats on existing cryptography, and in particular the emergence of universal quantum computers, are taken into account by upcoming standardized "post-quantum" algorithms.

QKD may find some use in a few niche applications, for instance as a defense-in-depth measure on point-to-point links. However, the use of state-of-the art classical cryptography including post-quantum algorithms is by far the preferred way to ensure long-term protection of data, as it is the only technology choice that offers the functional properties needed in modern communication systems.

In any case, the cost incurred by the use of QKD should not jeopardize the fight against current threats to information systems which overwhelmingly do not exploit cryptographic weaknesses.

For another point of view on this topic with similar arguments and conclusions, the reader may consult the white paper of the National Cyber Security Centre (UK) [1], or the position of the NSA (USA) [2].

Nejdůležitější části v češtině

QKD může najít určité **využití v několika málo velmi specifických aplikacích**, jako například **opatření pro hloubkovou ochranu u spojení typu bod-bod**.

Použití nejmodernější klasické kryptografie včetně **postkvantových algoritmů je zdaleka nejvíce preferovaným způsobem zajištění dlouhodobé ochrany dat**, protože je jedinou volbou technologie, která nabízí funkční vlastnosti potřebné v moderních komunikačních systémech.

V žádném případě **by náklady vzniklé používáním QKD neměly ohrozit boj proti současným hrozbám na informační systémy**, které v drtivé většině nevyužívají kryptografické slabiny.

BSI - Quantenkryptografie - Quantenkryptografie (bund.de)

BSI upozorňuje na řadu **otevřených bezpečnostních otázek** v souvislosti s případným nasazením QKD.

Obdobně jako NSA, NCSC a ANSSI upozorňuje na **problémy QKD** spojené

- s implementační bezpečností QKD,
- s krátkostí bezpečného spojení QKD,
- s nutností bezpečně autentizované klasické komunikace

a upozorňuje na provozní problémy vznikající při narůstání QKD sítě.

Ve spolupráci s ETSI pracuje BSI na profilu ochran (***Protection Profile***) pro hodnocení bezpečnosti vybraných QKD zařízení.

Upozorňuje

- na **příliš velkou variabilitu QKD**-protokolů a technických přístupů ke QKD.
- na **chybějící standardy** omezující tyto možnosti, což by usnadnilo interoperabilitu a hodnocení QKD.

V případě potřeby definuje BSI tato omezení v technických směrnicích a poskytne aplikační informace o použití klíčů.

BSI nepovažuje QKD za konkurenta PQC, ale spíše za jeho doplněk

Problém standardizace (včetně bezpečnostní) QKD a QKDN

QKDN – QKD Network

Pokusy o **standardizaci QKD** již probíhají poměrně dlouhou dobu.

- Hlavní iniciativy v této oblasti: ETSI, ISO/IEC.
- Dokončení podstaty této (zejména bezpečnostní) standardizace bylo plánováno během r. 2021, s výjimkou *QKD-Protection Profiles* zhruba uprostřed r. 2022,
- **Otázka bezpečnostních garancí plynoucích ze splnění těchto standardů**.

Pokusy o **standardizaci QKDN**

- Jakmile rozšíříme „zájem“ na standardizaci QKD-sítí, prudce se **rozšíří počet oblastí**, ke kterým bude potřeba vytvořit standardy
- Hlavní iniciativy v této oblasti: ETSI, ISO/IEC, ITU-T, IEEE
- Předpokládané ukončení těchto prací do r. 2030.

EURO QCI

Cíle EURO QCI

Střednědobý cíl:

Vybudovat vysoce zabezpečenou komunikační infrastrukturu založenou na QKD, která bude propojovat evropskou kritickou infrastrukturu

Krátkodobé cíle:

- Vytvoření evropského ekosystému výrobců QKD a jejich subdodavatelů.
- Vytvoření páteřní evropské sítě QKD a integrovat ji do současné komunikační infrastruktury.

Dlouhodobý cíl:

Vybudovat vysoce zabezpečený kvantový internet.

Národní plán ČR v EURO QCI

eQCI Czech National Plan - work progress

Jan Bouda [1] Bohuslav Rudolf [2]

[1]Masaryk University

[2]Czech National Cyber and Information Security Agency

November 22, 2020

Úvodní práce na národním plánu ČR

- Jan Bouda – šerpa ČR v Euro QCI
- Bohuslav Rudolf – NÚKIB

Později na NP z této dvojice pracoval pouze šerpa ČR Jan Bouda.

B. Rudolf se stal členem *Security Group Euro QCI.*

Podstata národního plánu

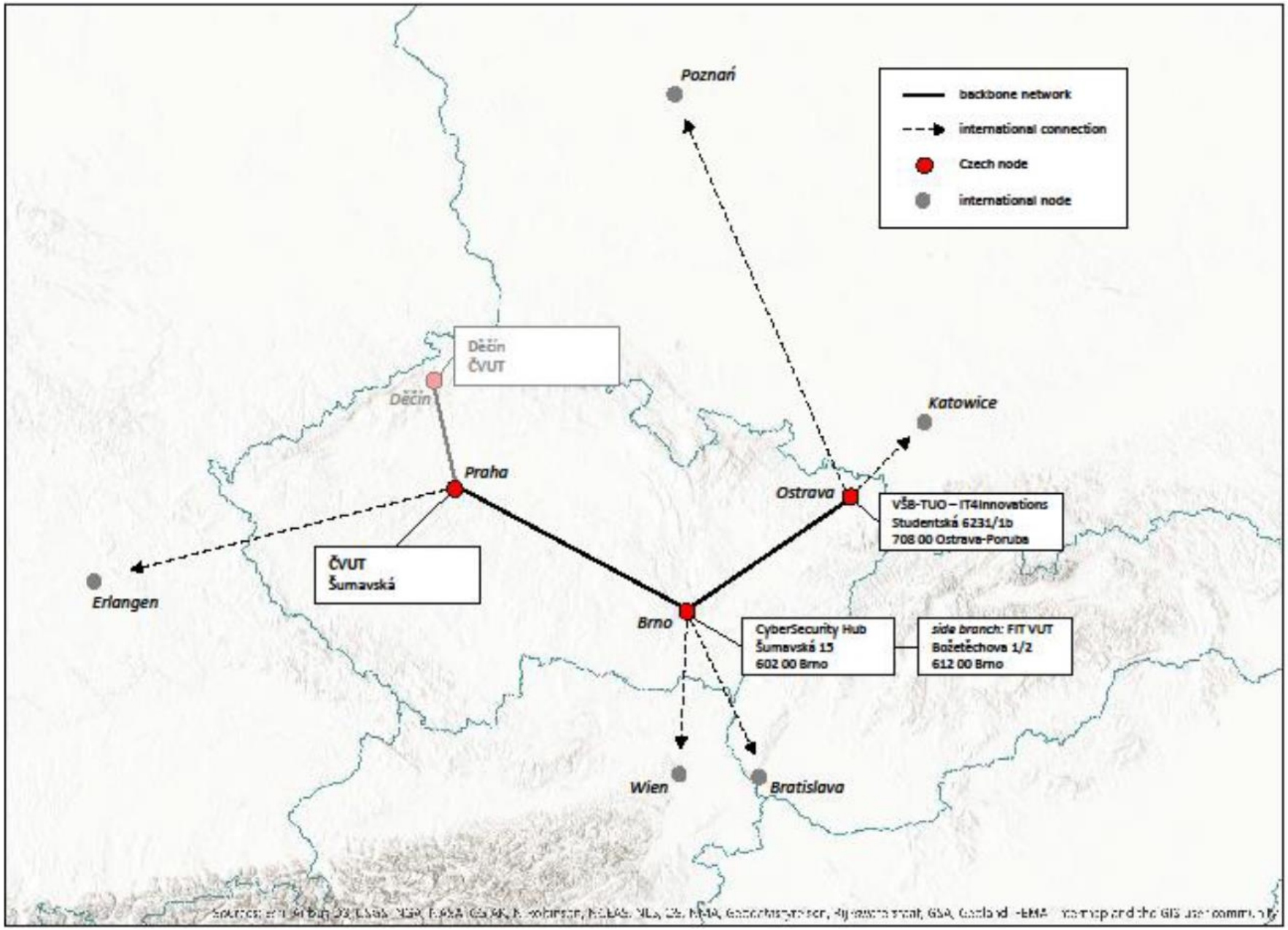
Vytvoření národní QKD sítě, která bude propojená do evropské páteřní sítě,

A zajištění souvisejících činností, jako jsou:

- Tréning a zaškolování expertů na kvantovou komunikaci
- Vývoj a testování integrace QKD do stávající zabezpečené komunikace
- Vývoj a testování QKD zařízení

Projekt (NP ČR EURO QCI) bude řešen prostřednictvím konsorcia **Cybersecurity hub.z.ú.** s bohatým zastoupením akademických institucí ČR.

Na dalším obrázku je mapa připravované české QKD sítě a její propojení do evropské infrastruktury. (J. Bouda)


Poznań
backbone network
international connection
Czech node
international node
Děčín
ČVUT
Děčín
Katowice
Praha
Ostrava
VŠB-TUO – IT4Innovations
Studentská 6231/1b
708 00 Ostrava-Poruba
ČVUT
Šumavská
Erlangen
Brno
CyberSecurity Hub
Šumavská 15
602 00 Brno
side branch: FIT VUT
Božetěchova 1/2
612 00 Brno
Wien
Bratislava


NESPOQ
KYBERNETICKÁ BEZPEČNOST SÍTÍ V POSTKVANTOVÉ ÉŘE
PROJEKT VÝZVY MVČR IMPAKT VJ01010008

NESPOQ: Kybernetická bezpečnost sítí v postkvantové éře

Základní informace o projektu

Téma projektu

Využití kvantové distribuce klíčů (***QKD*** – *Quantum Key Distribution*) a postkvantové kryptografie (***PQC*** - *Post Quantum Cryptography*) při ochraně sítí proti kvantové hrozbě v oblasti kybernetické bezpečnosti.

Další předpokládané přínosy projektu

Rozvoj témat, ve kterých je ČR svým způsobem jedinečná:

- Optické sensory
- Hardwarově akcelerované šifrování při rychlostech nad 100 GBps,
- Přenosy ultrastabilních veličin
- Atd.

Součástí projektu budou aktivity zaměřené na vzdělávání a praktické školení odborníků.

Hlavní části projektu

Z neformálního pohledu má projekt zatím tři hlavní části, z nichž každá pokrývá jednu z oblastí řešené problematiky.

a) Jeho významnou praktickou částí je **vývoj zařízení kombinujícího PQC a QKD k ustanovení symetrických klíčů**. Tyto klíče jsou pak využity k zajištění komunikace chráněné symetrickým autentizovaným šifrováním.

b) Samostatnou podporou pro vývoj výše zmíněného zařízení pro postkvantově chráněnou komunikaci je **část zajišťující QKD**. Jde o dvojici QKD zařízení propojených optickým vláknem.

c) A konečně třetí částí dosavadního průběhu projektu je **simulace možností konstrukce a omezení rozsáhlých QKD sítí** vycházející z vlastností jejich základních komponent.

Závěry – osobní názor autora prezentace

1)Doporučení míry podpory QKD v nejbližší budoucnosti

a) **Masivně se věnovat podpoře výzkumu a vývoje** v této oblasti, a to zejména v rámci Evropské spolupráce
   - To se již do jisté míry děje.
   - Zvážit potřebnost a možnost utajeného výzkumu a vývoje v těchto oblastech.

b) **Střízlivě a s rozvahou se zapojit do budování Evropské páteřní QKD sítě (Euro-QCI).**
   - To se již do značné míry děje.
   - Utajení některých informací v této oblasti se zvažuje.

2)Otázka podpory QKD a budování kvantového internetu z dlouhodobého hlediska

Předpovídání je velmi obtížné. Zejména, pokud jde o předpovídání budoucnosti.

Bonmot přisuzovaný Nielsu Bohrovi

Bude záležet na úspěších dalšího vývoje v oblastech:

A) Kryptologicky relevantních kvantových počítačů

B) Kryptoanalytických útoků na bázi kvantových algoritmů (a umělé inteligence) na PQC

C) Kvantových opakovačů

D) …

Na cestě je ještě mnoho překážek a nejasností,

ale může jít o technologie strategické z dlouhodobého hlediska.