

Kybernetická bezpečnost v éře kvantových počítačů

Miroslav Vozňák

voznak@ieee.org



Konvenční kryptografie vs. budoucnost

Dnešní moderní kryptografie

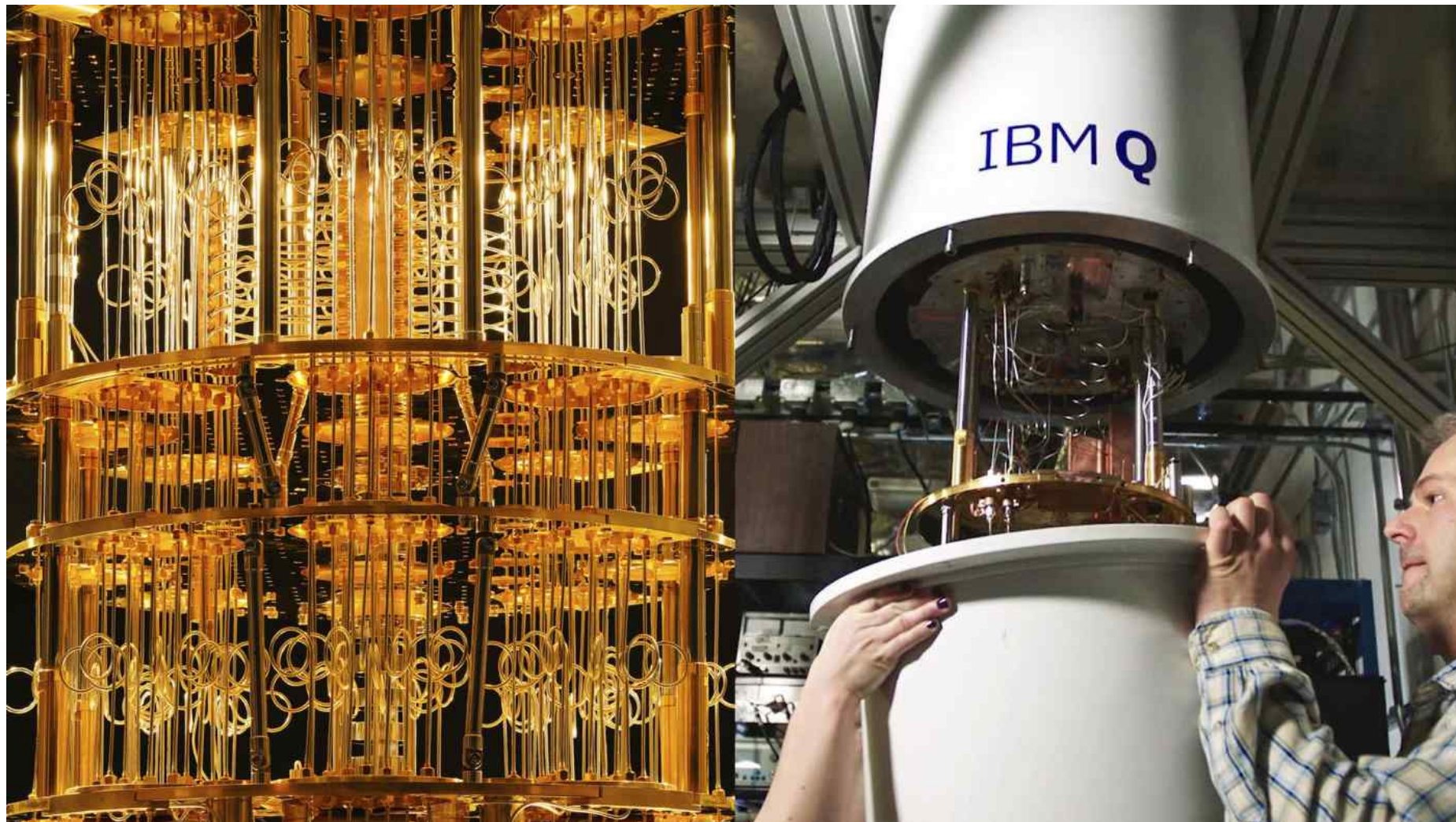
- Symetrická vs. asymetrická kryptografie
- Asymetrická využívá různé problémy výpočetní složitosti

Současná asymetrická kryptografie není odolná vůči útokům kvantových počítačů



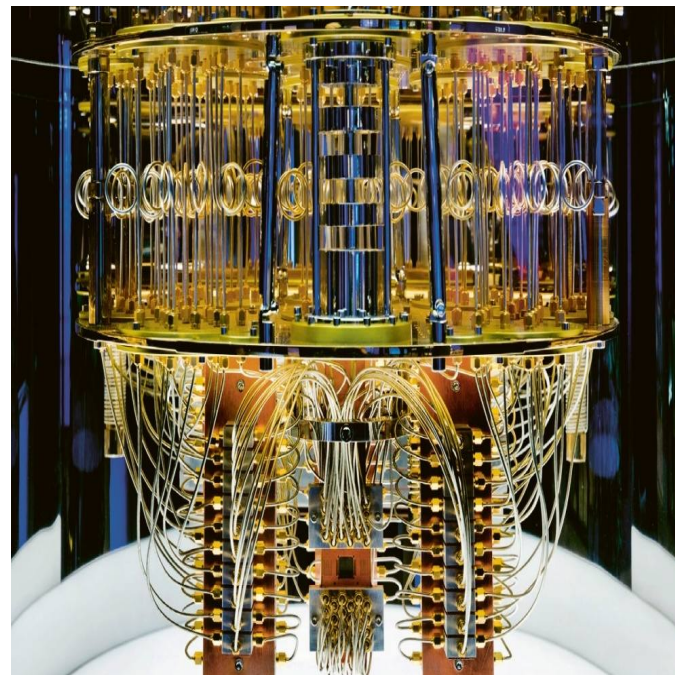
Shor's quantum computer algorithm *

P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*. **Proceedings 35th Annual Symposium on Foundations of Computer Science**. IEEE Comput. Soc. Press: 124–134, (1994).



Kvantový počítač

- Superpozice stavů, kvantový bit (qubit) může představovat jakoukoliv superpozici „1“ a „0“, navíc lze vytvářet qubitovou provázanost
- Komerční modely jako - Q System One anebo D-Wave



SRC: https://www.technickytydenik.cz/rubriky/ict/evropa-ma-prvni-komerčni-kvantovy-pocitac_53470.html



- Národní superpočítačové centrum IT4Innovations

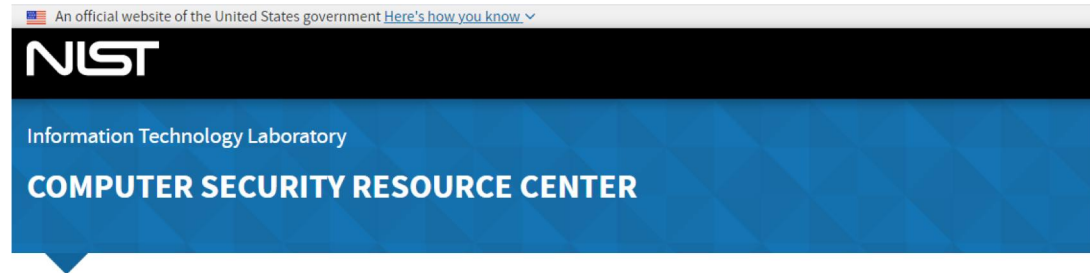
<https://www.it4i.cz/>

ANSELM, SALOMON,
BARBORA, KAROLÍNA

Kryptografie v éře kvantových počítačů

PQC - Postkvantová kryptografie
(NTRU či Classic McEliece)

<https://github.com/open-quantum-safe>



PROJECTS

POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography PQC



Post-Quantum Cryptography Standardization

The [Round 3 candidates](#) were announced July 22, 2020. [NISTIR 8309](#), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process is now available. NIST has developed [Guidelines for Submitting Tweaks for Third Round Finalists and Candidates](#).

QKD – Kvantová distribuce klíče

BB84 – diskretní, na principu polarizace

COW – Coherent One Way, na principu koherence dvou po sobě následujících pulzů

QKD (Quantum Key Distribution)

- Koncept QKD byl publikován v roce 1983* a první protokol BB84 záhy v roce 1984**
- Klíč je vygenerován náhodně a zakódován do polarizace fotonů a přenesen kvantovým kanálem (optické vlákno anebo FSO)



SRC <https://www.cesnet.cz/2021/07/prvni-mezimestsky-kvantovy-prenos-klicu-v-cr/?lang=en>

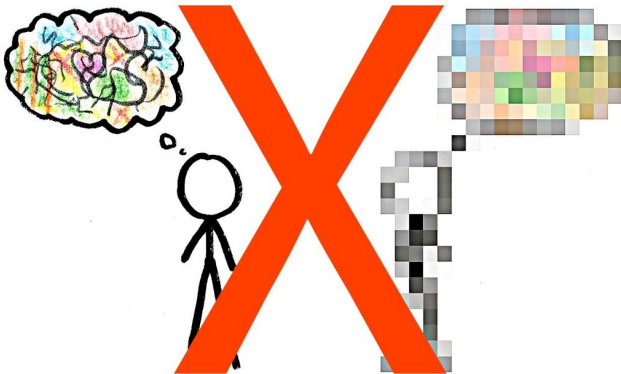
* S. Wiesner, *Conjugate coding*, **ACM Sigact News**, vol. 15, no. 1, pp. 78-88, (1983).

** C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in Proc. of **IEEE International Conference on Computers, Systems and Signal Processing**, vol. 175, no. 150. New York, (1984).

Proč je QKD bezpečná technologie ?

Problém odposlechu klíče

Heisenbergův princip neurčitosti odposlech významně znesnadňuje = > nárůst chybovosti v kvantovém kanále

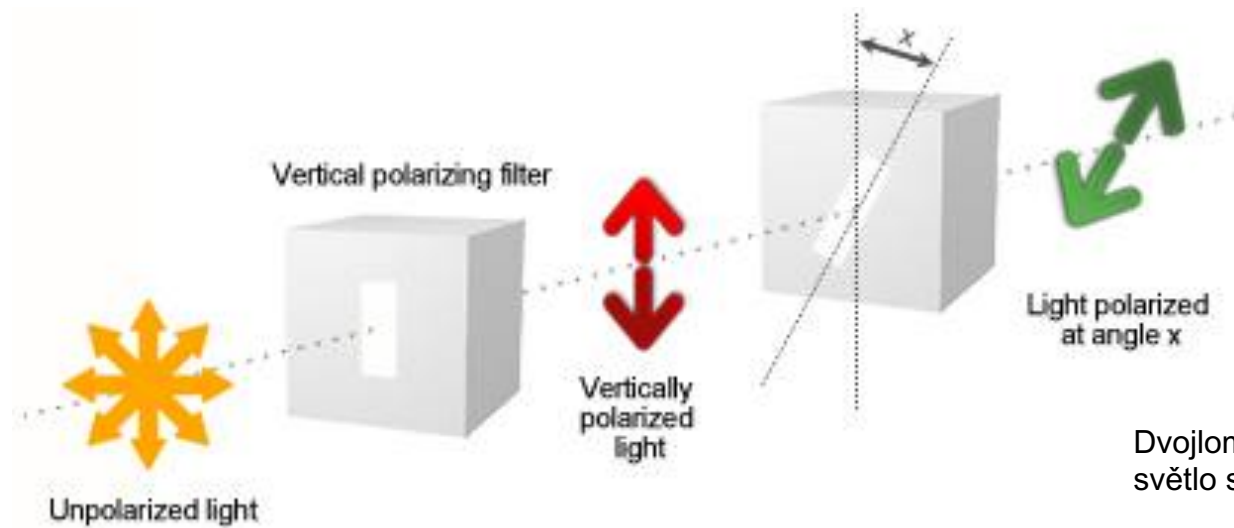


SRC: wikipedia.org/wiki/Werner_Heisenberg (1926)

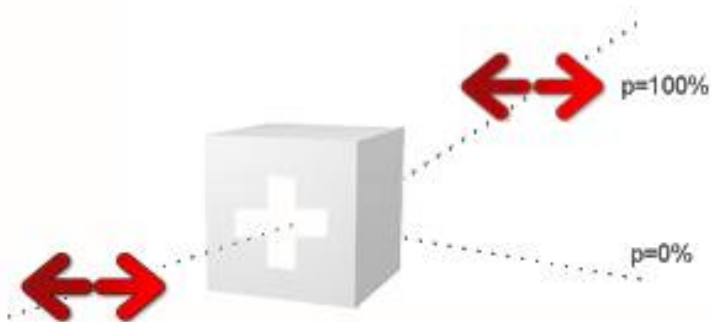
Ne-klonovací teorém

Neznámý kvantový stav nelze bezchybně kopírovat

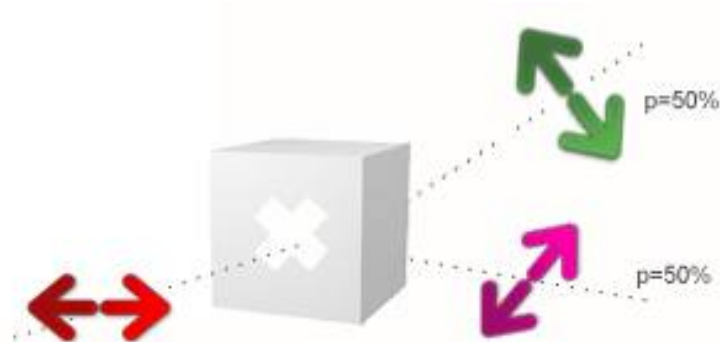
Proč je QKD bezpečná technologie ?



Dvojlomné krystaly kalcitu (CaCO_3) lámou světlo s rozdílnou polarizací do různých směrů

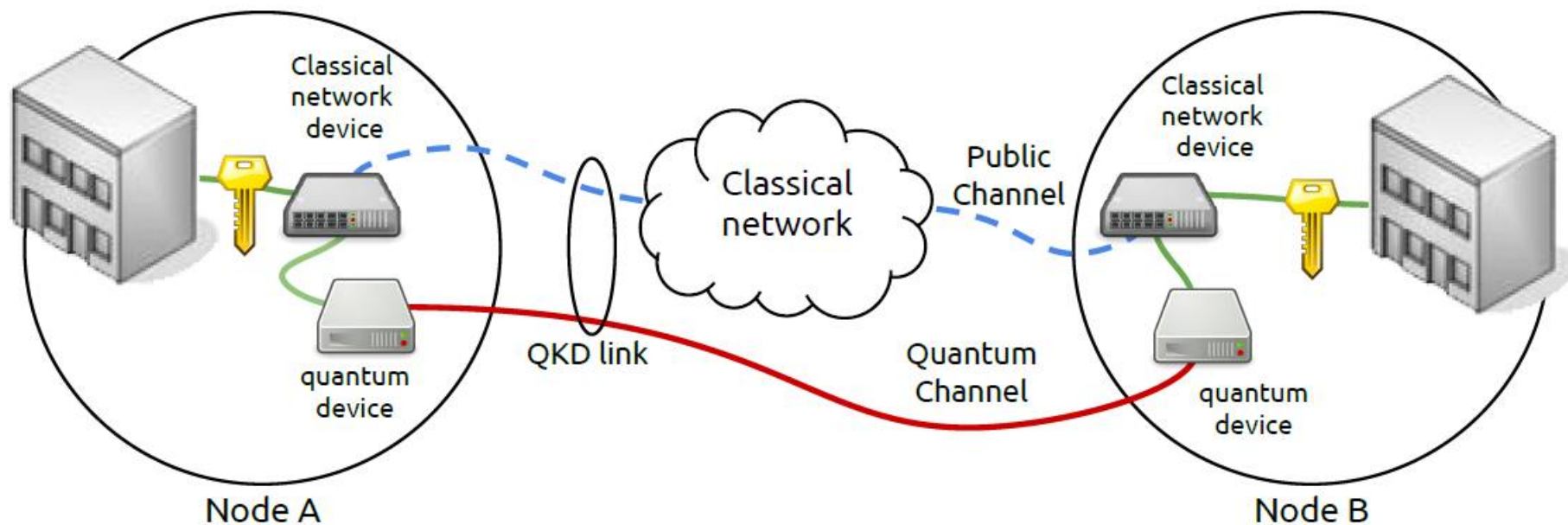


(a)

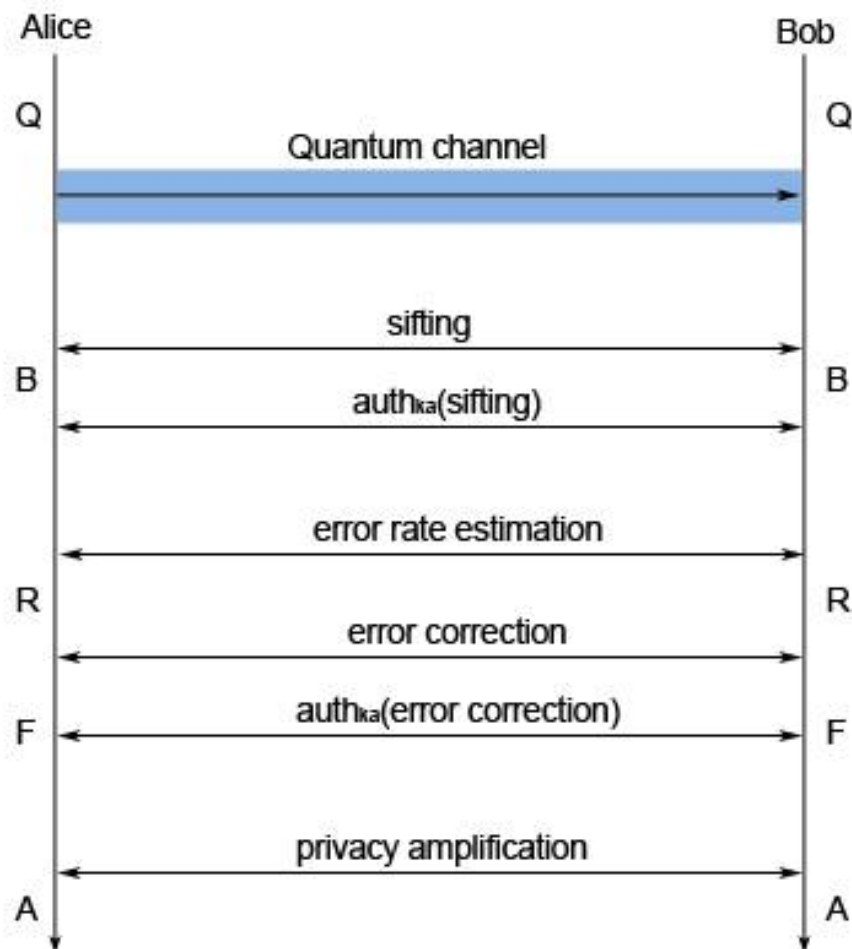


(b)

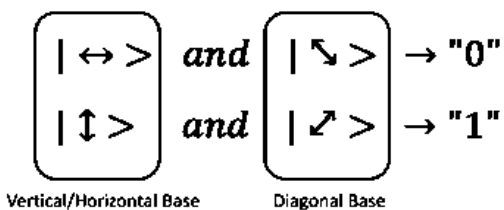
QKD link



BB84 QKD protocol



BB84 QKD protocol

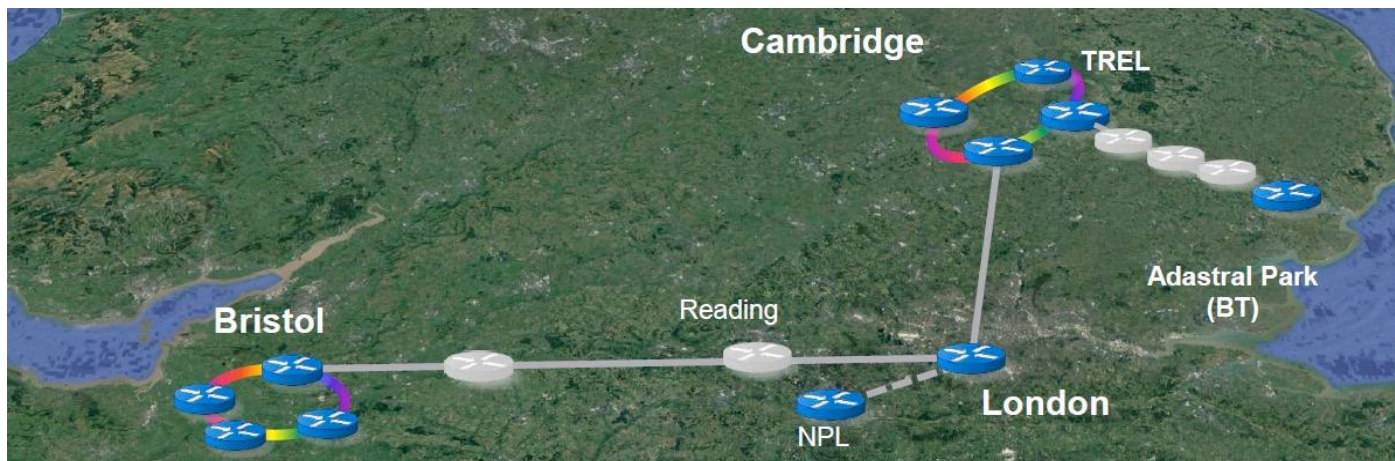
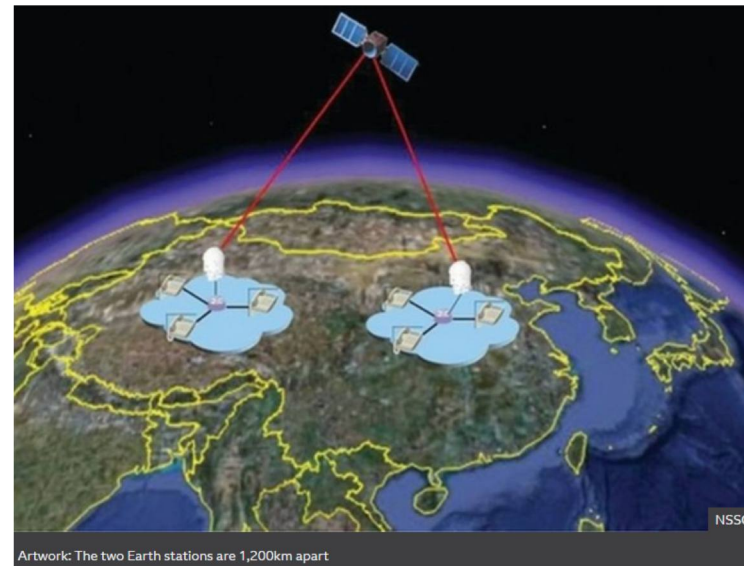


AN EXAMPLE OF KEY DISTRIBUTION IN BB84 PROTOCOL

Alice						
	0	0	1	1	0	1
Bob						
						
	0	0	1	1	1	0
Result	OK	OK	OK	Luck	Error	Error

QKD – praktické implementace

- 1989, poprvé na vzdálenost cca 30 cm
- 2005, DARPA QKD network (10 uzlů, 1kbps)
- 2008, SECOQC v Evropě (5 uzlů, 3.1 kbps, 33 km)
- 2010, Tokyo QKD network (6 uzlů, 304 kbps na 45 km)
- 2013, Munich, link mezi letadlem a pozemním vysílačem, přenos v rychlosti 290 kmph
- 2017, satelit Micius (LO, 500 km, komunikace 7 600 km Xinglong – Graz)
- 2017, Beijing-Shanghai, 2000 km (32 uzlů, 250 kbps na 43 km)
- 2018, QKD network v UK
- 2019 - 2022, OpenQKD v Evropě (38 partnerů z 13 členů EU)
- 2022 - 2027 experimentální síť v rámci EuroQCI



EU OPENQKD

Project description



Europe-wide quantum communication testing

Quantum communication has the potential to protect the EU's sensitive data and digital infrastructure for years to come. A test quantum communication infrastructure will be set up in several European countries. Launched by the EU-funded OPENQKD project, its activities will take place in Austria, Czech Republic, France, Germany, Greece Italy, Netherlands, Poland, Spain, Switzerland and the UK. It will boost the security of critical applications in various fields – from telecommunications to electricity supply and healthcare. Bringing together a multidisciplinary team (leading European telecommunication equipment manufacturers, end-users and critical infrastructure providers, network operators, quantum key distribution equipment providers, digital security professionals and scientists) from 13 EU countries, the aim is to bolster Europe's leadership in quantum technologies.



Project Information

OPENQKD

Grant agreement ID: 857156

Start date

2 September 2019

End date

1 September 2022

Funded under

H2020-EU.2.1.1.

Overall budget

€ 17 974 246,25

EU contribution

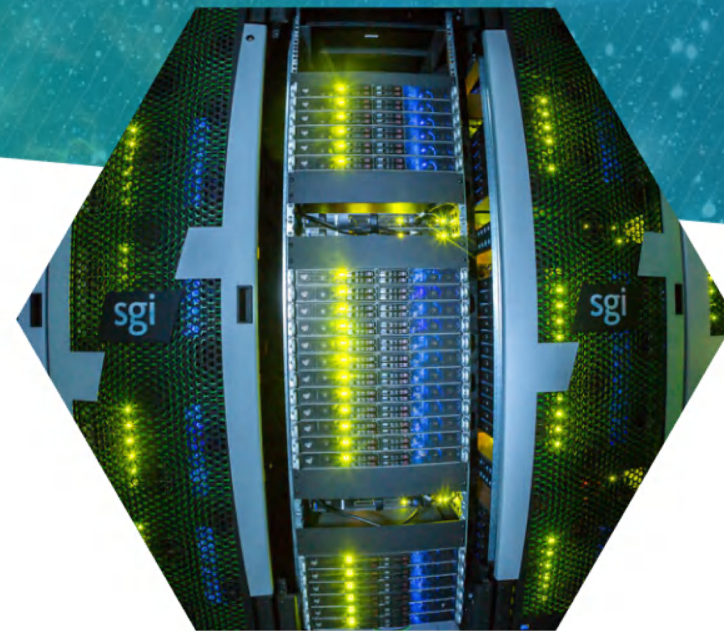
€ 14 999 989,89



[→](#) [O IT4I](#) [→](#) [INFOSERVIS](#) [→](#) [TISKOVÉ ZPRÁVY](#) [→](#) [STARTUJE PROJEKT OPENQKD PRO BEZPEČNOU CELOEVROPSKOU KVANTOVOU KOMUNIKAČNÍ INFRASTRUKTURU](#)

STARTUJE PROJEKT OPENQKD PRO BEZPEČNOU CELOEVROPSKOU KVANTOVOU KOMUNIKAČNÍ INFRASTRUKTURU

V IT4Innovations národním superpočítačovém centru startuje další z projektů Horizont 2020. Pilotní projekt s názvem OPENQKD implementuje a otestuje pilotní kvantovou komunikační infrastrukturu v několika evropských zemích. Jeho hlavním cílem je posílit bezpečnost kritických aplikací v oblasti telekomunikací, zdravotnictví, energetiky a řady dalších strategických oblastí.



Evropská komise se rozhodla financovat projekt OPENQKD v rámci programu Horizont 2020. Jeho posláním je vyvinout experimentální komunikační síť založenou na QKD (Quantum Key Distribution je distribuce klíčů s využitím principů kvantové mechaniky) a vyzkoušet

PRVNÍ MEZIMĚSTSKÝ KVANTOVÝ PŘENOS KLÍČŮ V ČR – NEJBEZPEČNĚJŠÍ ŠIFROVANÁ KOMUNIKACE

Konsorcium e-INFRA CZ realizovalo kvantový přenos klíčů, který má několik prvenství. Komunikace zabezpečená šifrováním prostřednictvím výměny kvantových klíčů (QKD) představuje nový posun v oblasti zabezpečení komunikace a řeší rizika spojená s nástupem kvantových počítačů, který s sebou přináší i reálné nebezpečí snadnějšího prolomení stávajících způsobů šifrování. Jedná se o první národní, ale i mezinárodní meziměstský přenos kvantových klíčů v ČR, a to konkrétně do Polského Cieszynu. Realizace přenosu je výsledkem spolupráce sdružení CESNET a IT4Innovations národního superpočítačového centra při VŠB – Technické univerzitě v Ostravě a polskou akademickou sítí PSNC.



INFORMACE O PROVOZU KVANTOVÉ KRYPTOGRAFIE NA TRASE OSTRAVA–TĚŠÍN

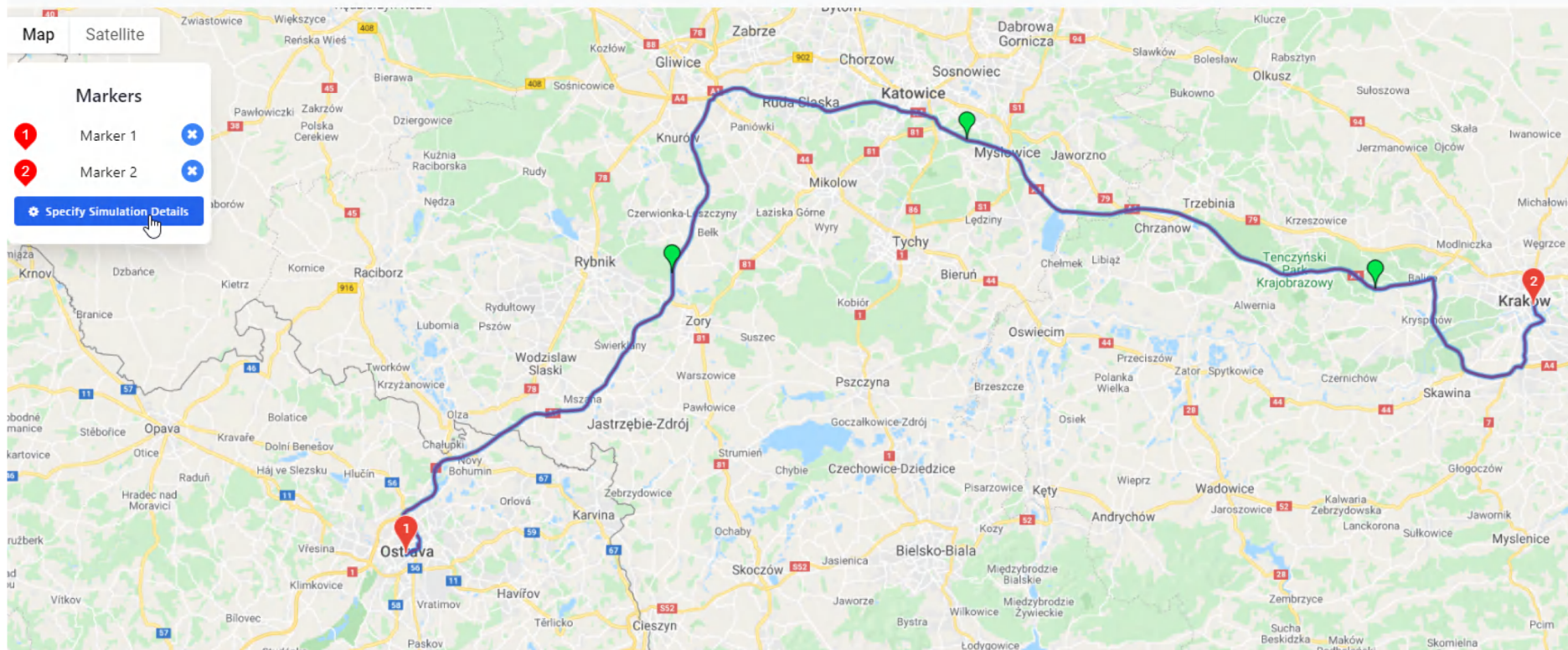
Nedávno jsme v [tiskové zprávě](#) informovali o prvním uskutečněném meziměstském přenosu kvantových klíčů v České republice, který byl spuštěn 1. 7. 2021 v rámci [projektu OPENQKD](#) na trase Ostrava–Těšín (Polsko) v optické infrastruktuře české sítě CESNET a polské PSNC.



Na QKD trase je instalován systém Systém Cerberis 3 od IDQuantique doplněný o šifrovače Centauris 6140. Šifrovače mají schopnost šifrovat a dešifrovat maximální provoz 40 Gb/s. Celý systém je konfigurován tak, že klíče QKD jsou přenášeny mezi systémem QKD a šifrováním přes vyhrazené rozhraní s využitím standardu ETSI GS QKD 014 založeném na REST API. Klíče QKD se používají k šifrování a dešifrování provozu v šifrovacích Centuaris pomocí 256 bitových klíčů AES. Šifrovače si vyměňují šifrovaný provoz pomocí nezávislé trasy zapojené do jednotek systému QKD – jednotky jsou propojeny pomocí rozhraní 10 Gb/s a schopné plného šifrování linky 10 Gb/s. Šifrovaný provoz je směrován pomocí páteřních přenosových systémů CESNET a PSNC DWDM.

<https://open-qkd.eu>

Quantum Key Distribution Network Simulator



Quantum Key Distribution Network Simulator

Set Parameters

● Docker ON

QKD Systems

Settings of QKD systems used to generate secret keys

DISTANCE (M) ⓘ

182074

KEY RATE (BPS) ⓘ

10811.955

KEY SIZE (BYTES) ⓘ

800

PP PACKET SIZE (BYTES) ⓘ

100

PP RATE (BPS) ⓘ

10000

OKD START TIME (SEC) ⓘ

0

OKD STOP TIME (SEC) ⓘ

30

End-user applications

Settings of end-user applications that consume secret keys

AUTHENTICATION TYPE ⓘ

SHA1

ENCRYPTION TYPE ⓘ

AES-128

AES LIFETIME (PACKETS) ⓘ

1

APP PACKET SIZE (BYTES) ⓘ

300

NUM OF KEYS TO FETCH FROM KMS ⓘ

10

APP TRAFFIC RATE (BPS) ⓘ

10000

APP START TIME (SEC) ⓘ

10

APP STOP TIME (SEC) ⓘ

30

CLOSE

APPLY

T A
Č R **STARFOS**

Zadejte klíčová slova v angličtině...



Vyhledávejte v angličtině

Vyhledávejte v češtině



English

Kybernetická bezpečnost sítí v postkvantové éře

VJ01010008 [Sdílet projekt](#)

Projekt výzkumu a vývoje řešený v programu **IMPAKT 1** je realizovaný v letech 2021 - 2025 se státní podporou **46 735 tis. Kč** a zaměřením na oblast **Information science (social aspects)**.

Základní informace

Finance

Účastníci (3)

Výsledky (2)

Podobné projekty (10)



Uznané náklady: 46 735 tis. Kč
Podpora: 46 735 tis. Kč



Poskytovatel: Ministerstvo vnitra



OECD FORD: Information science (social aspects)



Doba řešení:
1. 1. 2021 — 31. 12. 2025

Klíčová slova

Kybernetická bezpečnost sítí v postkvantové éře

Cíle projektu

Projekt je zaměřen na strategický dlouhodobý výzkum a vývoj systémů pro zabezpečení moderních komunikačních sítí. Projekt poskytne reálná data o efektivitě a připravenosti systémů pro zajištění bezpečnosti zejména kritických komunikačních sítí, umožní ověření praktické uplatnitelnosti QKD (kvantového ustanovení klíčů) a PQC (postkvantové kryptografie) v reálných aplikacích specifických pro ČR a bude dále rozvíjet témata, ve kterých je ČR svým výzkumem jedinečná (např. optické senzory, hardwarově akcelerované šifrování na rychlostech nad 100 Gbps, přenosy ultrastabilních veličin atp.). Mimo klíčových výzkumných témat identifikovaných výše obsahuje projekt také aktivity zaměřené na vzdělávání a praktické školení odborníků z praxe, zejména ve státní sféře.

Děkuji za pozornost

Varování ministra zdravotnictví

*Přemýšlení nad kvantovou kryptografií
způsobuje nespavost*

