Bezpečnostní a praktické aspekty QKD

RNDr. Bohuslav Rudolf

Skupina matematicko-analytická OBIT NÚKIB

Možné 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 („kupředu do minulosti“).

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

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

Různost pohledů

na vhodnost využití QKD k ochraně

před kvantovou hrozbou

Varovné hlasy

Řešení doporučované relevantními bezpečnostními autoritami – **NSA, NCSC, ANSSI** – pro ochranu proti kvantové hrozbě – **Využití post-kvantové kryptografie**

Před použitím kvantové distribuce klíčů NSA, NCSC, ANSSI spíše varují

NCSC – nedoporučuje ani vládní ani vojenské použití QKD a varuje před výhradním spoléháním na QKD v kritické infrastruktuře.

NSA - nedoporučuje použití QKD v národních bezpečnostních systémech (NSS) a nepředpokládá schválení (nebo certifikaci) QKD v NSS, dokud nebudou vyřešeny současné nedostatky QKD.

ANSSI – investice do nasazení QKD by neměly být na úkor investic do standardních oblastí kybernetické bezpečnosti

Všichni se shodují v tom, že, když už by v blízké budoucnosti měla být QKD nasazena k „ostré ochraně“ utajovaných a vysoce citlivých dat, musí být kombinována s PQC.

Bezpečnostní argument pro podporu přípravy nasazení QKD

1) **Kvantová distribuce klíčů umožňuje dlouhodobou bezpečnost** v následujícím smyslu:

Pokud není útočník schopen získat QKD-klíč z odposlechu kvantového protokolu v jeho průběhu nebo krátce po jeho běhu, pak ho nebude schopen zlomit na základě výsledků tohoto odposlechu ani nikdy v budoucnosti.

Rozdíl proti PQC. Pokud si útočník uloží výsledky odposlechu PQC protokolu, nelze vyloučit, že někdy v budoucnosti budou známy algoritmy, které ho umožní zlomit (viz scénář: odposlechni, poté ulož, poté čekej, až budeš mít kryptoanalytické prostředky – vylušti).

Jinými slovy: V případě QKD nehrozí zpětné luštění klíče a následně dat, jaké hrozí v případě pokroku kryptoanalytických metod v budoucnu v případě PQC.

To znamená, že: Pokud nezlomím běh QKD protokolu v jeho průběhu, zůstane bezpečný navždy.

Ke garancím nezlomitelnosti QKD protokolu v jeho průběhu se vrátíme později.

Technologické argumenty pro podporu přípravy nasazení 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) Všechny výše zmíněné **relevantní bezpečnostní autority** NSA, NCSC, ANSSI a další **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.

Pokus o shrnutí na rámcové úrovni bez hlubší a detailnější argumentace

A) **Proti „ostrému nasazení“ QKD v blízké budoucnosti** pro ochranu utajovaných informací a vládní komunikace **se staví relevantní bezpečnostní autority**.
Jejich argumentaci jsme dosud neuvedli, ale vrátíme se k ní.
Považujeme ji za věcnou, za správnou a za vysoce relevantní.

B) Uvedli jsme rovněž **několik argumentů ve prospěch** přípravy (případného) **nasazení QKD**.
Všechny tyto argumenty se v podstatě vztahují ke dlouhodobé budoucnosti.

Z toho lze usoudit, že:

- **V krátkodobém a střednědobém** horizontu **je ostré nasazení QKD** přinejmenším **sporné**.
- Ale příprava praktického nasazení a testování QKD může mít **strategický význam především z dlouhodobého hlediska.**

Základní

bezpečnostní a provozní

vlastnosti QKD

Základní bezpečnostní vlastnosti QKD

„Nepodmíněná“ dlouhodobá bezpečnost – obecně řečeno, plyne bezpečnost QKD ze zákonů kvantové mechaniky.

Konkrétněji, **pokud**:

1. **QKD-zařízení splňují (implementační) předpoklady** důkazu bezpečnosti použitého QKD-protokolu

2. **Platí zákony kvantové mechaniky** použité v důkazu bezpečnosti použitého QKD-protokolu

Pak dané instance QKD-zařízení nejsou zlomitelné a jimi ustanovené klíče jsou bezpečné. Potom nehrozí, že by útočník mohl QKD klíče získat díky nějaké slabině QKD.

Proto mluvíme v této souvislosti o **nepodmíněné bezpečnosti**.

Poznamenejme, že **bezpečnost PQC je podmíněná výpočetní bezpečnost**. Je podmíněná předpokladem, že po celou dobu citlivosti chráněných informací nebude nikomu znám žádný reálný způsob, jak daný PQC protokol (zpětně) zlomit.

Základní bezpečnostní vlastnosti QKD

Problematická implementační bezpečnost QKD – problémem je fakt, že:

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

Základní bezpečnostní vlastnosti QKD

Nutnost doplnění QKD kanálu autentizovaným klasickým kanálem

QKD – součástí komunikace sloužící k zajištění bezpečnosti QKD je autentizovaná komunikace obou uzlových QKD-zařízení.

Oba uzly se v rámci této klasické komunikace informují:

- o nastavení svých měřicích zařízení pro jednotlivé fotony
- a pro vybranou náhodnou skupinu fotonů pak o výsledcích měření na těchto fotonech. Statistika výsledků těchto měření musí být v souladu s předpokladem o tom, že kvantové ustanovení klíčů nebylo odposloucháváno.

K tomu, abychom mohli QKD pokládat za nepodmíněně bezpečné, by muselo být doplněno i nepodmíněně bezpečně autentizovanou klasickou komunikací.

Hlavní omezení QKD

Realizace QKD probíhá pomocí **přenosu fotonů**. Kanálem pro tento přenos fotonů může být:

a) **Optické vlákno** – pozemní QKD

b) **Volný prostor** – QKD probíhající přes **satelity**.

Pravděpodobně nejzávažnějším praktickým problémem QKD na optických vláknech je omezení vzdálenosti, na kterou lze provést bezpečné QKD ustanovení klíčů – zhruba 200 km (pro různé QKD protokoly a pro různé experimenty je to různé a navíc se to mění s časem).

Předpokládané **řešení** tohoto problému – je použití tzv. „**důvěryhodných uzlů**“ (*Trusted Nodes*), jejichž důvěryhodnosti se musí dosáhnout pomocí **fyzické, režimové a personální bezpečnosti**. **Jedna z nejvážnějších věcných námitek proti širokému ostrému nasazení QKD**.

QKD v kosmickém prostoru

Satelitní spojení se dvěma pozemskými stanicemi. Díky němu se mezi pozemskými stanicemi ustanoví QKD klíče.

Výhoda ustanovení QKD klíče přes satelit – QKD klíče lze tímto způsobem ustanovit i na velmi velké vzdálenosti.

Dva základní typy QKD:

a) Typ **„Připrav a změř**“ – QKD zařízení A připravuje a vysílá fotony a QKD-zařízení B tyto fotony přijímá a měří.

b) Typ „**s provázanými fotony**“ – centrální zařízení generuje dvojice provázaných (entaglovaných) fotonů, které jsou vysílány ke dvěma přijímacím QKD-zařízením.

QKD v kosmickém prostoru

Ad a) **QKD přes satelit** na bázi **„Připrav a změř“**: V tom případě je nutné, aby **satelit** byl **důvěryhodným uzlem**. Jak to zajistit?

Ad b) Pokud je **QKD** ustanovení klíčů **přes satelit** založeno na využití **provázaných fotonů**, pak **satelit** musí obsahovat zdroj těchto fotonů, ale **nemusí být důvěryhodným uzlem**. To je **pozoruhodný důsledek vlastností kvantového provázání**.

Ale v případě Ad b) jsou rychlosti ustanovování QKD klíčů extrémně nízké.

Další problémy QKD v kosmickém prostoru:

A) **Závislost dostupnosti služby na počasí**. Nad jednou z pozemních stanic je zataženo ⇒ služba není dostupná.

B) **Problematičnost obměny QKD zařízení na satelitu nebo opravy** v případě, že došlo k poruše.

Důsledky vlastností QKD kanálu

Snadnost útoku na dostupnost služby u malých QKD sítí

QKD-kanál je z podstaty věci typu **end-to-end**. Kdyby šlo fotony klonovat, bylo by po bezpečnosti.

Důsledkem u malých sítí QKD je **snadný útok na dostupnost služby**.

Obrana proti tomuto útoku: Ustanovování QKD klíčů může být prováděno „do zásoby“.
To znamená, že v uzlech QKD mohou vznikat zásoby směrových QKD klíčů ustanovených „do zásoby“.

Možnost přesměrování QKD kanálu

Existují „kvantové routery“, které mohou bez újmy na bezpečnosti přesměrovat dráhy QKD fotonů z jednoho optického vlákna na jiné optické vlákno.

To může být podstatné, pokud časem přejdeme k budování rozsáhlých a značně větvených QKD sítí.

Finanční a provozní náročnost QKD

A) Každý **komunikační uzel** znamená jedno **fyzické QKD zařízení**.

B) Každý „**důvěryhodný uzel**“ znamená nutnost **uplatnění režimových, fyzických a personálních ochran** v místě, kde je realizován.

C) Pro **pozemní QKD** je nutný **pronájem** příslušných **optických vláken**. V současnosti se typicky jedná o tzv. „**temná vlákna**“ – nesmí na nich být jiný provoz.

D) Pro „**kosmické QKD**“ je nutné použití QKD-zdroje na satelitu a pozemních stanic. **Evropa** zatím svůj **„QKD-satelit“ nemá(!)** a hodlá ho na oběžnou dráhu teprve vypustit. Pokud jde o pozemní stanice, jsou značně finančně náročné.

E) **Problémy s oběma typy kosmického QKD**. V případě typu: „**Připrav a změř**“ je nutné, aby **satelit** byl **důvěryhodným uzlem**. V případě využití **provázaných fotonů** je rychlost ustanovování klíčů (***key rate***) **extrémně nízká**.

F) Nutnost připojení QKD-zařízení ke „standardním komunikačním zařízením“.

Snahy o řešení zásadních technologických problémů QKD

A) Snahy o náhradu *Trusted Nodes* pomocí *Quantum Repeators*

Vývoj Kvantových opakovačů – ***Quantum Repeators*** – kvantově bezpečná zařízení, která by měla v budoucnosti nahradit „důvěryhodné uzly“.

Umožní **QKD na velké vzdálenosti bez** nutnosti využití **důvěryhodných uzlů**.

Bezpečnost v místě kvantového opakovače již nebude zajištěna fyzicky (režimově a personálně), ale **bude zajištěna** fyzikálně **pomocí kvantové mechaniky**.

V současnosti probíhá v této oblasti **intenzivní výzkum a vývoj**. Jde ale o náročný vědecký problém.

B)Snahy o zajištění vysokých garancí implementační bezpečnosti QKD

Zahrnují dva hlavní přístupy:

1) **Vývoj QKD-zařízení, která splňují všechny předpoklady důkazu bezpečnosti**.
   Obtížné a obtížně ověřitelné.
   Reálné je postupné snižování odchylek od ideálního stavu.

2) **Vývoj nových protokolů a nových důkazů jejich bezpečnosti**, které tolerují (zahrnují) nepřesné (neideální) chování reálných QKD-zařízení.
   V této souvislosti se používají pojmy:
   - ***DI QKD – Device Independent QKD***, tj. QKD, jehož bezpečnost nezávisí na vlastnostech implementace.
   - ***MDI QKD – Measurement Device Independent QKD***, tj. QKD, jehož bezpečnost nezávisí (do značné míry) na nedokonalostech detektorů fotonů.

Vývoj QKD sítí

(částečně dle článku: *D. Stebila, M. Mosca, D. Lütkenhaus: The Case for Quantum Key Distribution*)

1. **Spojení typu: bod-bod**. Dvě QKD zařízení jsou spojena na poměrně krátkou vzdálenost.

2. **Sítě s optickými přepínači:** Několik QKD-zařízení propojených optickými vlákny a optickými přepínači je propojeno do sítě. Přepínače nemusí být důvěryhodnými uzly, ale nejsou schopny prodloužit vzdálenosti, na které lze ustanovovat QKD-klíče.

3. **Bohatě větvené sítě s přepínáním a s ukládáním QKD-klíčů:** Zde se poněkud odchýlíme od článku (z r. 2009). Bohatě větvené QKD-sítě s důvěryhodnými uzly, které zajišťují ustanovování QKD-klíčů mezi libovolnými svými komunikačními uzly do zásoby. Ustanovení klíčů mezi dvojicí komunikačních uzlů může probíhat po dráze, která vznikla vhodnou kombinací dostupných spojení.
    - Mohou být poměrně odolné proti útokům na dostupnost služby.
    - Ale jsou náročné na množství QKD-zařízení, pronajatých optických vláken a na počet důvěryhodných uzlů.

Pravděpodobný další vývoj *QCI – Quantum Communication Infrastructure*

4. **Bohatě větvené sítě s kvantovými opakovači, s *přepínači* a s ukládáním QKD-klíčů:** Realizace těchto typů sítí připadá v úvahu ve vzdálenější budoucnosti, kdy lze očekávat, že budou dostupné prakticky použitelné a bezpečné kvantové opakovače a kdy budou dostatečně levná a bezpečná komerční QKD-zařízení a kdy bude levný pronájem optických vláken pro QKD.

5. **Kvantový internet:** Jakmile budou běžně dostupné relevantní kvantové počítače, lze očekávat, že dojde k transformaci QKD-sítí typu 4 na kvantový internet, tedy na internet, který bude schopen „víceméně běžně“ přenášet kvantovou informaci a umožnit tak distribuované kvantové výpočty.

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 QKD sítí - 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.

Srovnání s post-kvantovou kryptografií

Základní charakteristiky post-kvantové kryptografie

Bezpečnostní vlastnosti PQC:

- Podmíněná **výpočetní dokazatelná bezpečnost**. Je to dlouhodobý standard bezpečné kryptografie.
- **Ve spekulativním smyslu ji lze prolomit**, ale je to vysoce nepravděpodobné.
- V rámci **standardizační iniciativy NIST** **otevřené odborné veřejnosti** vznikají standardy PQC. Dlouhodobé **zkušenosti s předchozími** obdobným způsobem vzniklými **standardy NIST**, konkrétně **s AES a s SHA3** jsou více než **skvělé**.
- **Implementační bezpečnost PQC** je náročná, ale **její zajištění** s vysokými bezpečnostními garancemi je **mnohem snazší než u QKD**. Kromě toho se její principy neliší od principů **implementační bezpečnosti předchozích krypto-algoritmů** a ta je na světě **čtvrt století**.

Provozní vlastnosti PQC:

- Ve většině případů je **PQC** v některém smyslu **provozně náročnější než „klasická kryptografie s veřejnými klíči**.
  - Buď **časové** – doby generování klíčů nebo šifrování nebo dešifrování,
  - nebo hlavně značnými nároky na **délky klíčů** nebo **šifrového textu.**

- Ale tyto nároky jsou **zanedbatelné ve srovnání s** provozními nároky, které by kladlo využívání **QKD**.

- Kromě toho, současné návrhy (RFC) začlenění PQC do používaných kryptografických protokolů, jakým je například IPsec, předpokládají **ustanovení klíčů na bázi sériového použití několika PQC algoritmů**.

  Aby se útočník k PQC klíči dostal, **musel by zlomit všechny PQC algoritmy pro ustanovení klíčů**, na jejichž základě byl odvozen.

Tím padá téměř celé zdůvodnění potřebnosti ostrého nasazení QKD v blízké budoucnosti

ANSSI Should Quantum Key Distribution be Used for Secure Communications?

Poměrně nový text – několik důležitých bodů

Ke schopnosti QKD zajistit „nové služby“.

1) Veškeré služby, které by mohlo zajistit QKD, mohou být zajištěny již existujícími technologiemi.

2) **Vlastnosti QKD zabraňují** tomu, aby společně se symetrickým šifrováním mohlo být použito k zajištění end-to-end **bezpečnosti mezi virtualizovanými prostředími** nebo **mezi softwarovými službami**.

3) Za **nejrozumnější způsob využití QKD** dokument (a s ním i autor této prezentace) považuje zajištění komunikační bezpečnosti v kombinaci **se symetrickou kryptografií mezi pevnými lokalitami,** které jsou vzájemně **dostatečně blízko** a jsou **propojeny optickým vláknem**. (**Autor** této **prezentace** dodává: Ale **pouze tam, kde není podstatná dostupnost služby**).

K bezpečnostnímu „zdůvodnění“ potřebnosti QKD

1) Dokument (ani autor této prezentace) **neočekává, že by existence kvantových počítačů mohla významně ohrozila bezpečnost symetrické kryptografie**.

2) **Obtížnost implementace QKD** tak, aby splňovala požadavky nepodmíněné QKD **bezpečnosti**.

- Zdůraznění role **aktivních útoků na QKD**.
- Připomenutí **nedávných implementačních útoků na QKD** (z r. 2019). My připomeňme útok na COW-QKD z r. 2021.
- Doposud byla věnována **zanedbatelná pozornost tempest-bezpečnosti QKD** (úniku elektromagnetického záření) nebo **SW slabinám QKD**.

K možnostem rozsáhlého využití QKD a k ochraně utajovaných informací

1) **Rozsáhlé QKD sítě** by vyžadovaly použití **značného množství tzv. „důvěryhodných uzlů“**, což by **garance bezpečnosti významně degradovalo**.

2) **Spojení přes satelity** buď potřebuje, aby satelit byl „**důvěryhodným bodem**“ (a je po garancích bezpečnosti),
(Nebo je „opravdu děsivě neefektivní“ – poznámka autora prezentace).

3) **U klasifikovaných sítí** na bázi **QKD** nastanou **prakticky neřešitelné problémy**, **pokud** budeme požadovat, aby **pro různé stupně utajení** byla použita **různá QKD-zařízení**.

Velmi hrubé srovnání různých typů bezpečných sítí - typy sítí a kritéria

1) Velmi hrubé srovnání 4 typů sítí podle použité kryptografie:

I. Na bázi PKI

II. Čistě symetrická kryptografie

III. QKD s PKI (pro autentizaci) a se symetrickou kryptografií

IV. „nepodmíněně bezpečné“ QKD

2) Použitá kritéria hodnocení:

a) Lze nasadit v internetu nebo v soukromých sítích?

b) Je odolná vůči (kvantové) kryptoanalýze?

c) Lze síť snadno škálovat a snadno spravovat uživatele?

d) Může zajistit end-to-end bezpečnost?

e) Může dosáhnout vysoké efektivity (cca 100 Gb/s rychlosti šifrování)?

Velmi hrubé srovnání různých typů bezpečných sítí - výsledky

Ad I.) **Na bázi PKI** – splňuje všechna kritéria

(odolnost proti kvantové kryptoanalýze „pouze“ v praktickém smyslu).

Ad IV.) **„Nepodmíněně bezpečné“ QKD** – splňuje jediné kritérium – a tím je odolnost proti (kvantové) kryptoanalýze.

Nezajišťuje:

- Možnost nasadit v internetu nebo v soukromých sítích
- Snadnou škálovatelnost sítě a snadnou správu uživatelů
- End-to-end bezpečnost
- Dosažitelnost vysoké efektivity (cca 100 Gb/s rychlosti šifrování)

Ad III.) QKD s PKI (pro autentizaci) a se symetrickou kryptografií

Splňuje pouze dvě kritéria

- odolnost proti (kvantové) kryptoanalýze a
- možnost dosažení vysoké šifrovací rychlosti díky symetrické kryptografii.

Nezajišťuje:

- Možnost nasadit v internetu nebo v soukromých sítích
- Snadnou škálovatelnost sítě a snadnou správu uživatelů
- End-to-end bezpečnost

Ad I.) Čistě symetrická kryptografie

Splňuje

- odolnost proti (kvantové) kryptoanalýze
- možnost dosažení vysoké šifrovací rychlosti.
- End-to-end bezpečnost
- Možnost nasadit v internetu nebo v soukromých sítích

Nezajišťuje:

- Snadnou škálovatelnost sítě a snadnou správu uživatelů

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.
  - Možná o trochu velkoryseji, než bych očekával.
  - Ale EU má mnohem, ale opravdu mnohem velkorysejší přístup než já.
  - A navíc personální zajištění ČR v této oblasti mě spíše uklidňuje.
- 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 (mně) neznámého autora

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.