Kvantová hrozba

a

kvantově odolná kryptografie

RNDr. Bohuslav Rudolf, NÚKIB,

18. října 2023, Policejní akademie, Praha,

Bezpečnostní seminář: Kvantová a postkvantová kryptografie, AFCEA

Dvojí význam názvu příspěvku

A) Kryptografický

1. Podstata a aktuálnost kvantové hrozby, její důsledky pro bezpečnost schválených kryptografických algoritmů,

2. Typy kvantově odolné kryptografie, výhledově doporučená kvantově odolná kryptografie

B) Název dokumentu NÚKIB

Příloha: „Kvantová hrozba a kvantově odolná kryptografi“ k aktualizovanému dokumentu: „Minimální požadavky na kryptografické algoritmy“.

Objev **Shorova algoritmu**

a jeho důsledky

O nejrozšířenějších typech kryptografie s veřejnými klíči

Kryptografie s veřejnými klíči umožňuje nebo podstatně usnadňuje zejména:

- Digitální podpisy
- Ustanovení šifrovacích klíčů.

Bezpečnost daného typu kryptografie s veřejnými klíči je založena na obtížnosti řešení, tj. na praktické neřešitelnosti příslušného matematického problému pro určitou oblast hodnot jeho vstupních parametrů.

Mezi kryptosystémy s veřejnými klíči nimi hrají zásadní roli typy kryptografie založené na obtížnosti řešení problémů

- *Faktorizace velmi velkých čísel*
- *Hledání diskrétního logaritmu na číselném tělese nebo na eliptické křivce.*

Tedy například: RSA, Diffie-Hellman, El Gamal, DSA, ECDH, ECDSA, ACE a další.

Tato kryptografie má velmi výhodné praktické vlastnosti, a proto je nasazena „téměř všude“.

Patří do ní veškerá kryptografie s veřejnými klíči schválená v dokumentu NÚKIB:

„Minimální požadavky na kryptografické algoritmy“.

Podstata kvantové hrozby – Shorův algoritmus a jeho varianty

Teorie o možnostech kvantových výpočtů dlouho nebrali praktičtí lidé
(včetně „praktických teoretických fyziků“) vážně.

Až do objevu Shorova algoritmu v r. 1994. **A jeho variant.**

Pokud by se podařilo implementovat Shorův algoritmus (a/nebo jeho varianty)
na rozumném počtu qubitů a běžící v rozumném čase,

znamenalo by to:

zlomení většiny v současnosti (i v minulosti) prakticky používaných kryptografických algoritmů s veřejnými klíči.

Tj. zlomení kryptosystémů na bázi:

RSA, Diffie-Hellman, El Gamal, DSA, ECDH, ECDSA a dalších.

Tedy zlomení již zmíněných:

- Nejrozšířeji používaných kryptosystémů s veřejnými klíči
- Všech schválených kryptografických algoritmů s veřejnými klíči

Podmínka realizace kvantové hrozby

realizace kryptoanalyticky relevantních kvantových počítačů (CRQC)

CRQC – Cryptanalytically Relevant Quantum Computer

Shorův algoritmus je kvantový algoritmus, a proto může běžet pouze na vhodném kvantovém počítači, tj. na CRQC.

Důsledky objevu Shorova algoritmu pro vývoj kvantových počítačů

V důsledku objevu Shorova algoritmu začal hon na

- Vhodný kvantový hardware,
- Implementace kvantových hradel
- kódy na opravu kvantových výpočtů,
- další efektivní kvantové algoritmy

Do výzkumu a vývoje kvantového počítání začaly proudit peníze …

Důsledky objevu Shorova algoritmu pro vývoj kvantově odolné kryptografie

Vznik (názvu) a rozvoj post-kvantové kryptografie

- Dan Bernstein tak v r. 2003 nazval ty kryptografické algoritmy s veřejnými klíči, které nebudou zlomeny ani kvantovými algoritmy.
- Od r. 2006 pravidelné konference „*Post-Quantum Cryptography*“.

Vývoj a komercionalizace kvantové distribuce klíčů

- Objevena již v r. 1984,
- Detekce odposlechu na bázi kvantové mechaniky
- Nepodmíněná bezpečnost

Rozvoj kvantového počítání a kvantově odolné kryptografie zhruba do r. 2015

Zhruba 15 let po objevu Shorova algoritmu byl pokrok v oblasti kvantového počítání velmi pomalý… „Užitečné kvantové počítání“ bylo chápáno jako vzdálená hypotetická možnost…

Mezi lety 2012 až 2014 došlo ke zlomu.

Zlom ve vývoji kvantového počítání a jeho důsledky

Podstata zlomu (mezi lety 2012 a 2014)

- Realizace supravodivých qubitů a jim odpovídajících kvantových hradel
- Přiblížení chybovostí kvantových hradel k prahu jejich opravitelnosti pomocí kvantových kódů

Důsledky pro rozvoj post-kvantové kryptografie

V r. 2014 publikovala EU výzvu Horizon 2020, jejíž součástí byl i projekt **PQCRYPTO EU**.

V r. 2015 vydala americká NSA **doporučení přípravy přechodu ke kvantově odolné kryptografii**.

Koncem **r. 2016** vyhlásil **NIST soutěž**, jejíž vítězové budou **standardy post-kvantových algoritmů.**

(Dnes jsou známi první vítězové soutěže. Jejich standardy budou k dispozici v r. 2024).

Důsledky předchozího pro rozvoj nových kvantových technologií

Michelle Mosca – výzva vládě USA, aby pro vývoj kvantových počítačů vytvořila analogii projektu Manhattan.

ČLR (Čína) – vývoj, implementace a nasazení QKD (kvantové distribuce klíčů), v r. 2016 vypustila satelit Micius, realizace QKD mezi satelitem a zemí, v nedávné minulosti významné úspěchy v oblasti vývoje kvantových počítačů

EU – Quantum Technologies Flagship, Horizon 2020 -, Open QKD, 2019 – vznik Euro QCI, budování evropské páteřní QKD sítě.

Druhá kvantová revoluce – kvantové počítání, kvantová distribuce klíčů, kvantové sensory, kvantové simulace.

Hektický, téměř nepřehledný, téměř nepředvídatelný vývoj…

Přirozené otázky

ke kvantové hrozbě:

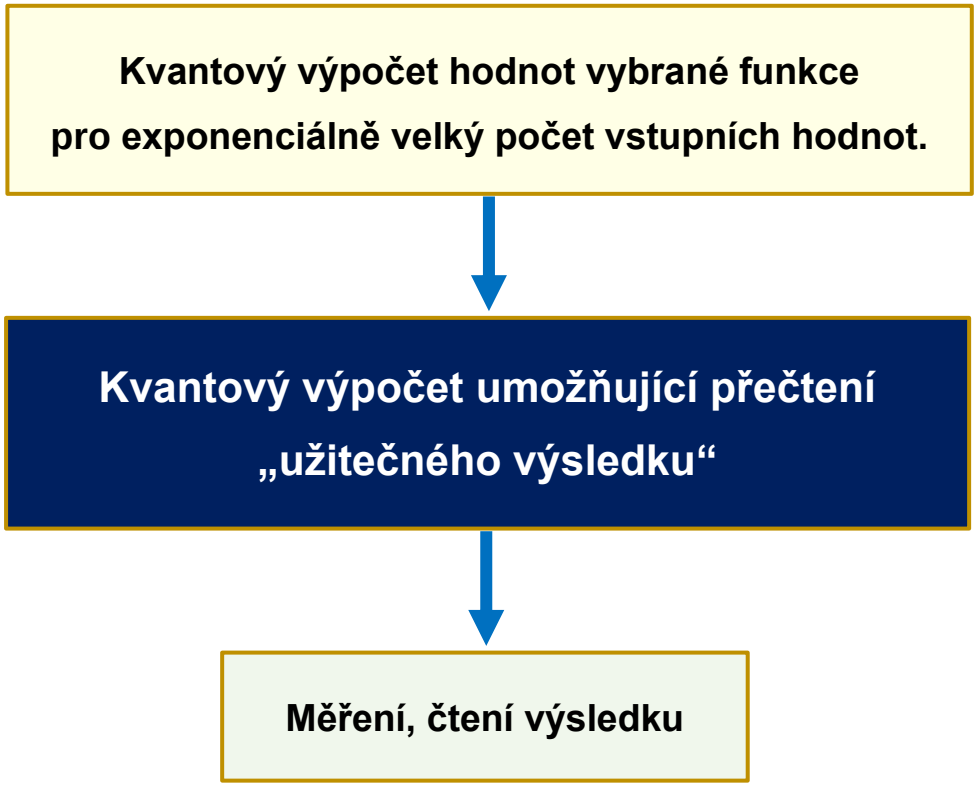
Přirozené otázky ke kvantové hrozbě:

- Je Shorův algoritmus jediným kvantovým algoritmem relevantním pro kryptoanalýzu?
- Jaké máme záruky, že post-kvantová kryptografie nebude zlomena novými dosud neznámými kvantovými algoritmy?

Zdroje síly a zdroje omezení „standardních“ kvantových algoritmů, kontra-intuitivnost kvantového počítání

- To, co je v klasickém světě (výpočetně) extrémně obtížné, může být v kvantovém světě (výpočetně) poměrně snadné.
- To, co je v klasickém světě poměrně snadné, může být v kvantovém světě extrémně obtížné nebo nemožné.

„Standardní“ kvantový algoritmus má tyto hlavní části:



To je v klasickém světě extrémně obtížné,
ale v kvantovém světě poměrně snadné.

Odtud se bere potenciální síla kvantového výpočtu.

Kvantový svět umožňuje jediné čtení výsledku kvantového výpočtu.

To znamená, že výstup z předchozí části je nutno dalším kvantovým výpočtem transformovat tak, aby jediné čtení výsledku dalo dostatečně užitečnou informaci.

To je nejtěžší část návrhu kvantových algoritmů a obvykle také jejich výpočetně nejnáročnější část.

Odpovědi na otázky ke kvantové hrozbě

Je Shorův algoritmus jediným kvantovým algoritmem relevantním pro kryptoanalýzu?

V Shorově algoritmu je jeho druhá část řešena nesmírně efektivní kvantovou Fourierovou transformací.
Proto snadno láme příslušnou kryptografii s veřejnými klíči.

Pro **útok hrubou silou** na libovolný kryptografický algoritmus (libovolnou funkci) byl navržen

Groverův algoritmus.

- Jeho druhá část má jen kvadratické navýšení efektivity vůči klasickému útoku.
- V případě jeho použití proti symetrické kryptografii jako ochrana proti němu stačí **256-bitové klíče**.

Groverův algoritmus byl využit pro návrh kvantového tzv. **BHT-algoritmu pro hledání kolizí hašovacích funkcí**.
Jako ochrana proti němu stačí použití hašovacích funkcí s délkou výstupu alespoň **384-bitů.**

Je známo **několik dalších kvantových algoritmů relevantních pro kryptoanalýzu**.

- Například Kuperbergův algoritmus nebo Simonův algoritmus.
- V současnosti mají převážně jen teoretický význam pro vývoj post-kvantové kryptografie.

Odpovědi na otázky ke kvantové hrozbě

Jaké máme záruky, že post-kvantová kryptografie nebude zlomena novými dosud neznámými kvantovými algoritmy?

Je to velmi podobné jako v případě klasické kryptoanalýzy.

Nikdy nevíme, zda někdo nebude mít nový nápad, jak pro nějaký problém navrhnout efektivní kvantový algoritmus (druhou část) umožňující získat relevantní užitečnou informaci z výstupu z první části kvantového výpočtu.

Důvěra v to, že to nejde, vzniká obdobně jako v klasické kryptoanalýze.

Tím, že se na pokusy o návrhy těchto algoritmů (pro zlomení daného kryptosystému) vrhne velmi mnoho velmi chytrých lidí, kteří se o to snaží poměrně dlouhou dobu, ale bez úspěchu, je stále považováno za dostatečnou záruku neprolomitelnosti tohoto kryptosystému.

Post-kvantová kryptografie

a standardizační soutěž NIST

O post-kvantové kryptografii, PQC – *Post-Quantum Cryptography*

- Oblast kryptografie s veřejnými klíči.
- Podle našich současných znalostí je odolná proti útokům kvantovými počítači.

Hlavní předpokládaná a dnes doporučovaná metoda ochrany proti kvantové hrozbě.

Oproti dnes nejvíce používané kryptografii s veřejnými klíči je „těžkopádnější“.

Obvykle:

- Pomalejší kryptografické operace.
- Velmi dlouhé:
  - Veřejné klíče
  - Šifrové texty
  - Digitální podpisy

Od roku 2016 se pohledy těch, kdo se zabývají ochranou proti kvantové hrozbě, upínají k **NIST**.

Veřejná soutěž NIST o standardy post-kvantové kryptografie

- Vyhlášená v r. 2016.
- Veřejná transparentní soutěž.
- Velké množství publikovaných návrhů post-kvantových algoritmů, a ještě mnohem větší množství na ně publikovaných útoků.

Soutěží se ve dvou kategoriích:

- *Encryption, KEM* – obojí je v podstatě asymetrické šifrování klíčů.
- *Digital signatures*

Bezpečnostní garance soutěžících algoritmů jsou rozděleny do **pěti bezpečnostních úrovní**.

Jsou známy první vítězné PQC-algoritmy:

- Vítězem v kategorii *Encryption, KEM* je CRYSTALS Kyber.
- Vítězné algoritmy v kategorii *Digital signatures* jsou
  - CRYSTALS Dilithium
  - SPHINCS+
  - Falcon

Během r. 2024 mají být publikovány jejich standardy.

Dilemata

Primární dilemata spjatá s přechodem k post-kvantové kryptografii

A) Post-kvantová kryptografie v hybridní kombinaci s „klasickou“ kryptografií s veřejnými klíči nebo samostatná PQC?

Hybridní kombinace PQC s klasickou asymetrickou kryptografií a smysl jejího doporučení

- Obava z toho, že post-kvantová kryptografie je „příliš mladá“ a že zatím nemáme dostatečné záruky její odolnosti proti kryptoanalýze.
- Doporučení kombinovat ji s „prověřenou“ klasickou asymetrickou kryptografií tak, aby v případě zlomení PQC klasickou kryptoanalýzou zůstal celek bezpečný.

Tento postoj zastává většina odborné veřejnosti a většina evropských bezpečnostních autorit.

Překvapení od NSA , doporučení sady kvantově odolných algoritmů pro NSS

NSS (*National Security Systems*) jsou národní bezpečnostní systémy USA,
vyskytují se v nich i utajované informace.

NSA pro NSS doporučují samostatné použití algoritmů CRYSTALS

- Pro *KEM/Encryption* samostatný CRYSTALS-Kyber bezpečnostní úrovně 5 implementovaný dle budoucího (r. 2024) standardu NIST.
- Pro *Digital Signature* s obecným použitím samostatný CRYSTALS-Dilithium bezpečnostní úrovně 5.

Podstata zdůvodnění tohoto doporučení NSA

- NSA provedla vlastní analýzy bezpečnosti algoritmů CRYSTALS.
- S růstem složitosti kryptografického systému obvykle roste množství příležitostí ke vnášení chyb při jeho implementaci.
- Ušetří se tak pozdější přechod od hybridní kryptografie k samostatné PQC.

Přístup NÚKIB k řešení dilematu

Samostatné nebo hybridní použití post-kvantové kryptografie?

Na jedné straně

doporučení odborné veřejnosti a evropských bezpečnostních autorit.

hybridní použití PQC + klasické asymetrické kryptografie

Na straně druhé

doporučení jedné z nejsofistikovanějších bezpečnostních autorit světa (americké NSA)

samostatné použití algoritmů rodiny CRYSTALS s bezpečnostní úrovní 5.

NÚKIB bude akceptovat oba uvažované přístupy!

B) Časové rozvržení přechodu ke kvantově odolné kryptografii

Příčiny dilematu

Neurčitost doby realizace kvantové hrozby:

Nevíme, kdy budou zkonstruovány kryptograficky relevantní kvantové počítače.

- Dle některých odhadů to může být začátkem třicátých let.
- Ale podle jiných odborných názorů to může být i mnohem, mnohem později.

Možnost útoku z budoucnosti na důvěrnost dnešní komunikace

Při útocích na důvěrnost šifrované komunikace lze odposlouchanou komunikaci nahrát, uložit a vyluštit, až budou k dispozici kryptograficky relevantní kvantové počítače.

To jsou silné důvody pro:

Realizaci a dokončení přechodu ke kvantově odolné kryptografii co nejdříve.

Na straně druhé:

Přechod ke kvantově odolné kryptografii bude:

- komplexní,
- odborně náročný,
- ekonomicky náročný
- a bolestný proces.

Pravděpodobně bude v řadě případů nutné vyměnit celé části nebo dokonce celé komunikační nebo informační systémy.

Post-kvantové algoritmy mají výrazně vyšší některé provozní nároky.

Standardy vítězů PQC-soutěže NIST budou publikovány až během r. 2024.

Přístup NÚKIB k řešení dilematu

časového rozvržení přechodu ke kvantově odolné kryptografii

1) Pro **ochranu informací s kritickou úrovní důvěrnosti nebo integrity** bude NÚKIB vycházet z odhadu realizace kryptograficky relevantních kvantových počítačů **počátkem 30-tých let**.

Zdůvodnění:

- Pro kritickou úroveň citlivosti informací bychom měli počítat s nejhorší reálnou variantou.
- Například BSI počítá s tímto odhadem pro případy „aplikací s vysokými požadavky na bezpečnost“.

Jak stanovit deadline pro kryptografické systémy chránící důvěrnost informací?

Deadline zde:

Termín přechodu ke kvantově odolné kryptografii v oblasti ochrany důvěrnosti.

Komplikace:

Nutnost uvažovat útok (na bázi uložené odposlouchané šifrované komunikace) z budoucnosti do minulosti.

Což takhle podle doby trvání kritičnosti důvěrnosti informací?

Problém:

Komunikační a informační systémy obvykle nejsou specializovány nebo rozlišovány podle délky doby citlivosti nebo délky doby utajení jimi chráněných informací.

Co s tím?

1. V úvahách NIST se objevuje odhad 5 let trvání citlivosti informací (ale jen jako příklad).

2. Ono vlastně není moc času – a tedy ani není moc na výběr:

- Standardy post-kvantové kryptografie budou k dispozici v r. 2024.
- Pro informace kritické úrovně bereme vážně odhad: „počátek třicátých let“.
- Odhad 5 let trvání doby kritické úrovně citlivosti informací je často minimem.
- 30 – 5 = 25, ale to se nedá stihnout!

NÚKIB stanovil odhad doporučení ukončení přechodu ke kvantově odolné kryptografii pro ochranu informací kritické úrovně důvěrnosti

na rok 2027.

Ale zatím je to formulováno pouze jako odhad, a nikoliv jako závazné doporučení.

Přechod ke kvantově odolným digitálním podpisům

V případě ochrany informací s kritickou úrovní integrity vychází NÚKIB v současnosti z odhadu realizace CRQC **počátkem 30-tých let**.

Ale s postupujícím časem se tento odhad bude měnit. Takže jde o **odhad orientační.**

V dalším uvidíme, že existuje specifická oblast digitálních podpisů, které je vhodné vyměnit za kvantově odolné co nejrychleji.

Ostatní důležité případy

Výjimečný případ digitálních podpisů pro ochranu integrity FW a SW

Málo známé skutečnosti:

A) Přechod ke kvantově odolné kryptografii spěchá i v této oblasti!

Zdůvodnění:

Některé paměti nejsou později přepisovatelné, a proto bude problém do nich v budoucnosti nahrát veřejný klíč kvantově odolného podpisu.

B) Kvantově odolné algoritmy pro tuto oblast jsou známy, jsou konsensuálně uznány a jsou již standardizovány.

Jde o algoritmy: **LMS** a **XMSS**.

V r. 2020 vydal NIST jejich standardy a doporučuje je NSA pro NSS a rovněž BSI.

C) Tyto algoritmy mají tak vysoké bezpečnostní garance, že konsensuálně je doporučováno jejich samostatné (nehybridní) použití

Jejich bezpečnost je založena na bezpečnosti v nich použitých hašovacích funkcí.

Stanovisko NÚKIB

NÚKIB doporučuje:

V rámci možností co nejrychlejší přechod v oblasti digitálních podpisů pro ochranu integrity FW a SW k používání algoritmů LMS nebo XMSS.

Přechod ke kvantově odolné symetrické kryptografii a ke kvantově odolným hašovacím funkcím

Relativní snadnost přechodu

Postačí přejít:

- ke schváleným šifrám s délkou klíče 256 bitů
- a ke schváleným hašovacím funkcím s délkou výstupu 384 bitů nebo větší.

Nižší naléhavost rychlosti přechodu

- V dané oblasti bude mít největší naléhavost přechod od symetrických šifer s klíčem 128 bitů k šifrám s klíčem 256 bitů.
- Avšak podle odhadů BSI by útok kvantovým počítačem na AES se 128 bitovým klíčem trval zhruba 30 let.
- Pokud jde o kvantový útok na symetrickou šifru s klíčem 196 bitů nebo na hašovací funkci s délkou výstupu 256 bitů, bude dlouho po realizaci kvantových počítačů zůstávat čistě teoretický.

Závěrečná doporučení a dokumenty NÚKIB

Přímo související dokumenty NÚKIB:

Minimální požadavky na kryptografické algoritmy

Kvantová hrozba a kvantově odolná kryptografie

Dokument: „Kvantová hrozba a kvantově odolná kryptografie“ je přílohou dokumentu: „Minimální požadavky na kryptografické algoritmy“.

Příloha popisuje cestu (zdůvodnění) vedoucí k doporučením uvedeným v hlavním dokumentu a tato doporučení podrobně vysvětluje.

Aktuální doporučení – pro ustanovení klíčů

Doporučení (orientační odhad) přechodu ke kvantově odolné kryptografii pro ochranu citlivých informací **kritické úrovně důvěrnosti** do konce roku **2027**.

Podstatné poznámky:

1) Jde o výměnu všech současných schválených algoritmů pro dohody na klíčích nebo pro asymetrické šifrování za buď **samostatný CRYSTALS Kyber** úrovně 5 implementovaný dle budoucího standardu NIST, nebo za jednu z **doporučených hybridních kombinací** PQC typu KEM/Encryption a schválené asymetrické kryptografie (bude specifikováno později).

2) Odhad termínu se týká pouze ochrany informací kritické úrovně důvěrnosti.

3) NÚKIB zatím chápe a prezentuje toto doporučení (zejména rok 2027) pouze jako orientační odhad, a tudíž zatím není tento odhad závazný.
   V návaznosti na vývoj situace v oblasti realizace CRQC a další podstatné faktory se tento odhad může změnit.

Doporučená hybridní kvantově odolná kryptografie pro ustanovení klíčů

Bezpečná hybridní kombinace

- Důvěryhodného post-kvantového algoritmu typu KEM/Encryption
- Schváleného algoritmu s veřejnými klíči pro dohody na klíči nebo pro asymetrické šifrování

Mezi důvěryhodné post-kvantové algoritmy typu KEM/Encryption NÚKIB (v souladu s BSI) řadí:

- CRYSTALS-Kyber
- Classic McElliece
- FrodoKEM

V obou přímo souvisejících dokumentech NÚKIB jsou uvedeny doporučené:

- parametry PQC-algoritmů (převzaty od BSI)
- bezpečná schémata hybridních kombinací

Aktuální doporučení – pro DS pro ochranu integrity FW a SW

U nově zaváděných systémů NÚKIB doporučuje, aby:

pro ochranu integrity SW a FW používaly buď LMS nebo XMSS.

Je to ve vlastním zájmu jejich vlastníků/uživatelů.

Doporučení přechodu ke kvantově odolným digitálním podpisům „s obecným použitím“

Konkrétní termín ukončení přechodu zatím není stanoven, a to ani pro informace kritické úrovně integrity.

Očekáváme, že nejbližší termín bude počátkem 30-tých let.

Pod kvantově odolnými podpisy s obecným použitím zde rozumíme:

- buď samostaný CRYSTALS-Dilithium úrovně 5 implementovaný dle standardu NIST
- nebo některou z doporučených hybridních kombinací PQC a schválených digitálních podpisů

Doporučené hybridní kvantově odolná digitální podpisy s obecným využitím

Bezpečná hybridní kombinace

- Důvěryhodného post-kvantového digitálního podpisu
- Schváleného digitálního podpisu

Mezi důvěryhodné post-kvantové digitální podpisy NÚKIB (v souladu s BSI) řadí vítěze soutěže NIST:

- CRYSTALS-Dilithium
- SPHINCS+
- Falcon

V obou přímo souvisejících dokumentech NÚKIB jsou doporučená schémata hybridních kombinací.
V souladu s BSI budou parametry PQC-algoritmů uvedeny až po jejich standardizaci.

Stanovisko NÚKIB k případnému nasazení kvantové distribuce klíčů

Pro nejbližší budoucnost považuje NÚKIB za hlavní ochranu proti kvantové hrozbě tzv. „post-kvantovou kryptografii“.

Možnost využití kvantové distribuce klíčů NÚKIB nevylučuje, ale doporučuje:

- Velmi pečlivé zvážení důvodů jejího použití
- Její použití pouze v bezpečné hybridní kombinaci s doporučenou kvantově odolnou kryptografií.

Připomeňme, že pod doporučenou kvantově odolnou kryptografií zde rozumíme

- Buď CRYSTALS-Kyber úrovně 5 implementovaný dle (budoucího) standardu NIST
- Nebo některé doporučené hybridní kombinace PQC a schválené asymetrické kryptografie

Závěrečné „povzbuzení“

Přechod ke kvantově odolné kryptografii bude vysoce náročný a bolestný proces.

Povinné subjekty budou při jeho přípravě a realizaci postaveny před řadu obtížných dilemat.

Zde prezentované přímo související dokumenty mají téměř čistě kryptografický charakter.

Autor této prezentace je přesvědčen, že v blízké budoucnosti by měly rovněž vzniknout podpůrné dokumenty systémového charakteru a že by měly probíhat konzultace mezi pracovníky NÚKIB a zástupci povinných subjektů.