NÚKIB

KVANTOVÁ HROZBA A KVANTOVĚ ODOLNÁ KRYPTOGRAFIE

Příloha k dokumentu:
Minimální požadavky na kryptografické algoritmy

Verze 2.0, platná ke dni 5. 2. 2025

Obsah

Úvod

Hlavní motivací této přílohy dokumentu „Minimální požadavky na kryptografické algoritmy“ je podpora přípravy přechodu k používání kvantově odolné kryptografie v oblasti kybernetické bezpečnosti. Vzhledem k předpokládané vysoké náročnosti tohoto procesu je primárním cílem této přílohy vysvětlení kryptografických aspektů a souvislostí a bližší zdůvodnění uvedených kryptografických doporučení.

V případě dotazů právního charakteru se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 777

E-mail: nckb@nukib.gov.cz

Dotazy, připomínky a podněty kryptologického charakteru můžete zasílat na e-mailovou adresu: **kryptoalgoritmy@nukib.gov.cz**

1 Kvantová hrozba

(1) Podstata kvantové hrozby

V roce 1994 publikoval Peter Shor kvantový algoritmus, který je téměř exponenciálně efektivnější než nejlepší dosud známé klasické algoritmy pro faktorizaci dlouhých čísel nebo pro hledání diskrétního logaritmu[1],[2]. To znamená, že s pomocí Shorova algoritmu lze v principu efektivně zlomit všechny asymetrické kryptografické algoritmy, jejichž bezpečnost je založena na obtížnosti některého z následujících problémů:

- faktorizace velkých čísel,
- hledání diskrétního logaritmu nad klasickým tělesem,
- hledání diskrétního logaritmu nad eliptickou křivkou[3].

Na předpokladu praktické neřešitelnosti uvedených problémů je založena bezpečnost většiny dnes nejvíce používaných asymetrických kryptografických algoritmů. Všechny klasické asymetrické kryptografické algoritmy schválené podle dokumentu „Minimální požadavky na kryptografické algoritmy“ jsou zlomitelné pomocí Shorova algoritmu.

V roce 1996 objevil Lov Grover kvantový algoritmus, který lze použít na hledání klíčů libovolného kryptografického systému hrubou silou[4], který je ale také podstatně méně efektivní než Shorův algoritmus. Důsledkem je to, že za bezpečné vůči Groverovu algoritmu považujeme pouze ty blokové a proudové šifry, které mají klíče dlouhé 256 bitů nebo větší[1].

V roce 1997 publikovali Brassard, Høyer a Tapp kvantový algoritmus (BHT-algoritmus) vycházející z Groverova algoritmu, který snižuje náročnost hledání kolizí hašovacích funkcí v porovnání s klasickými algoritmy hledajícími kolize na bázi narozeninového paradoxu[5]. Za bezpečné vůči útoku zmíněným kvantovým algoritmem dnes považujeme pouze ty hašovací funkce, jejichž výstupy jsou dlouhé alespoň 384 bitů[2].

[1] Rizika spojená s kvantovými útoky hrubou silou na bázi Groverova algoritmu na schválené blokové šifry s délkou klíče 128 bitů budou i po konstrukci kryptoanalyticky relevantních kvantových počítačů pravděpodobně velmi nízká a obdobná rizika pro délku klíče 192 bitů budou pravděpodobně téměř zanedbatelná.

[2] Rizika spojená s kvantovými útoky hrubou silou na bázi BHT-algoritmu a jeho vylepšení na schválené hašovací funkce s délkou výstupu 256 bitů budou i po konstrukci kryptoanalyticky relevantních kvantových počítačů pravděpodobně téměř zanedbatelná.

(2) Kryptoanalyticky relevantní kvantový počítač, nutná podmínka realizace kvantové hrozby

Pro praktické využití výše zmíněných kvantových algoritmů ke kryptoanalýze je nutné, aby běžely na tzv. „kryptoanalyticky relevantním kvantovém počítači“. Takový počítač by měl být univerzální, škálovatelný a spolehlivý[3].

Za nejperspektivnější oblasti výzkumu a vývoje směřující k tomuto cíli jsou dlouhodobě považovány kvantové počítání na bázi iontových pastí a kvantové počítání se supravodivými qubity. V současnosti jsou výrazné pokroky rovněž dosahovány v oblasti fotonického kvantového počítání. Žádný z dosud realizovaných kvantových počítačů se k vlastnostem kryptoanalyticky relevantních kvantových počítačů ani zdaleka nepřiblížil[4]. V této souvislosti jsou navrhovány i alternativní metody faktorizace na kvantovém počítači, který nemusí být obecně ani univerzální a ani plně odolný vůči chybám[5] [25].

V současnosti pravděpodobně nikdo neví, kdy k realizaci kryptoanalyticky relevantních kvantových počítačů dojde. Vycházejí práce s nejrůznějšími odhady a jako jeden z nejlepších je běžně prezentován výsledek ankety mezi odborníky na tuto problematiku[6], sl. 11 a 13. Velmi známé jsou i odhady uváděné M. Moscou[6], sl. 12, podle kterých s pravděpodobností ⅟ dojde k jejich realizaci v roce 2026 a s pravděpodobností ½ k ní dojde do roku 2031[6].

Německá BSI[7], str. 28 a 35 odhaduje, že první kryptoanalyticky relevantní kvantové počítače budou realizovány na počátku třicátých let tohoto století. V souladu s BSI považujeme tento odhad termínu realizace prvních kvantových počítačů za značně nejistý.

---

[3] Pojem univerzální kvantový počítač je kvantová analogie pojmu klasický univerzální počítač. Velmi zhruba řečeno: Na univerzálním kvantovém počítači může běžet libovolný kvantový algoritmus. Škálovatelnost kvantového počítače znamená, že nevelké zvětšení rozsahu jeho výpočtů (například prodloužení vstupů) nebude enormně náročné a že délky vstupů do škálovatelného kvantového počítače budou postupně více a více prodlužovány. Spolehlivý (*Fault Tolerant*) kvantový počítač by měl s dostatečnou přesností odstraňovat chyby libovolně dlouhého kvantového výpočtu.

[4] Současné univerzální kvantové počítače jsou označovány jako *NISQ – Noisy Intermediate Scale Quantum (Computer)*, tedy jako zašuměné kvantové počítače střední škály. Pravděpodobně největším problémem na cestě ke konstrukci kryptoanalyticky relevantních kvantových počítačů je obtížnost zajištění dostatečně spolehlivého odstraňování šumu. Podle některých odhadů je k realizaci jednoho spolehlivě pracujícího logického qubitu potřeba řádově tisíc fyzických qubitů[23], [24]. Logický qubit je kvantová analogie bitu. Kvantové algoritmy pracují s logickými qubity. Fyzický qubit je kvantový systém s kontrolovatelnými obecnými superpozicemi dvou bázových stavů. Logické qubity jsou systémy fyzických qubitů, které jsou schopné reprezentovat qubity v kvantových algoritmech při spolehlivých kvantových výpočtech.

[5] Například v práci [25] je navržen alternativní způsob faktorizace velkých čísel založený na digitalizovaném adiabatickém kvantovém počítání, které nevyžaduje velkou hloubku výpočtu, a proto nemusí být zcela odolné vůči chybám. A vzhledem k tomu, že je založené na Isingově modelu typickém pro optimalizační (kvantové) výpočty[65], nemusí být ani univerzální.

[6] Existuje velmi malá skupina renomovaných odborníků, kteří tvrdí, že k realizaci univerzálních, škálovatelných a spolehlivých kvantových počítačů pravděpodobně nedojde ani za deset, ba ani za dvacet let, ale za mnohem delší dobu, možná nikdy[8], [9], [10], [11].

Zároveň jej v souladu s BSI[7] považujeme za směrodatný pro přípravu přechodu ke kvantově odolné kryptografii v oblasti ochrany citlivých informací kritické úrovně důvěrnosti nebo integrity[8].

(3) Kvantově zranitelné algoritmy s vyššími nároky na rychlost své náhrady

Z výše uvedeného je zřejmé, že zhruba do začátku třicátých let bychom v oblasti ochrany vysoce citlivých informací měli přejít ke kvantově odolné kryptografii.

Problém je, že existují typy a způsoby použití kryptografických algoritmů, které i v případě správnosti zmíněného odhadu BSI vyžadují podstatně rychlejší výměnu za své kvantově odolné náhrady. Jde jednak o kryptografické algoritmy určené k ochraně důvěrnosti dat a dále jde o algoritmy digitálního podpisu určené k ochraně integrity firmwaru při jejich aktualizaci.

V prvním případě je nutné reagovat na možnost, že útočník si bude šifrovanou komunikaci nahrávat a ukládat s cílem ji rozluštit, až bude mít k dispozici kryptoanalyticky relevantní kvantový počítač (jde o scénář nazývaný „harvest now, decrypt later“).

Ve druhém případě je potřeba vzít v úvahu možnost, že některé paměti obsahující veřejné klíče nemusí být v budoucnosti přepisovatelné.

V těchto dvou případech jsou nároky na rychlost přechodu ke kvantově odolné kryptografii podstatně vyšší než v případech ostatních.

---

[7] BSI v případech „*high security applications*“ pracuje s hypotézou, že kryptograficky relevantní kvantové počítače budou dostupné začátkem třicátých let[7, str. 35].

[8] Kritická úroveň důvěrnosti/integrity/dostupnosti je nejvyšší úroveň důvěrnosti/integrity/dostupnosti, dle přílohy č. 1 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

2 Kvantově odolná kryptografie

(1) Hlavní možné reakce na kvantovou hrozbu

Možnost používání symetrické kryptografie ve větší míře a novými způsoby

Vzhledem k tomu, že symetrická kryptografie s délkou klíče 256 bitů není kvantově zranitelná, jednou z možností reakce by byl návrat k používání pouze symetrické kryptografie. To by ale vedlo ke ztrátě výhod asymetrické kryptografie.

Ve specifických případech kryptografických protokolů je možné použít předdistribuované symetrické klíče jako součást vstupu do funkce pro odvozování relačních klíčů (*session keys*). To ovšem zvýší nároky na ochranu těchto předdistribuovaných klíčů.

Možnost přechodu k postkvantové kryptografii

Další možností je použití jiných asymetrických kryptografických algoritmů, které jsou proti útokům na bázi kvantového počítání odolné. Tyto algoritmy bývají nazývány kvantově bezpečná kryptografie nebo kvantově odolná kryptografie, nejčastěji se ale pro ně používá název postkvantová kryptografie (se zkratkou PQC – *post quantum cryptography*). Přechod k jejímu použití je podporován relevantními bezpečnostními autoritami, které jej považují za nejvhodnější způsob reakce na kvantovou hrozbu[7], [36], [37], [55], [56].

Možnost využití kvantové distribuce klíčů

Z dlouhodobého hlediska může být perspektivní použití kvantové distribuce klíčů (QKD – *quantum key distribution*). Má podstatné bezpečnostní výhody, ale zatím i podstatné bezpečnostní a praktické nevýhody, a proto přechod k jejímu širokému použití v blízké budoucnosti není (na rozdíl od jejího výzkumu) v současnosti podporován významnými bezpečnostními autoritami[7], [52], [53], [54], [69].

Přechod ke kvantově odolné kryptografii doporučujeme uskutečnit na bázi postkvantové kryptografie.

(2) Postkvantová kryptografie

Název postkvantová kryptografie zavedl americký kryptolog Dan Bernstein[59], sl. 21 a označil jím ty asymetrické kryptografické algoritmy, které zůstanou bezpečné i v době kryptoanalyticky relevantních kvantových počítačů. K tomu je nutné, aby jejich bezpečnost byla založena na obtížnosti řešení jiných matematických problémů než těch, které jsou zlomitelné Shorovým algoritmem. K zajištění jejich bezpečnosti je ale také potřebné, aby tyto kryptografické systémy nebyly zlomitelné ani žádným jiným kvantovým a samozřejmě ani klasickým algoritmem.

a) Hlavní typy současné postkvantové kryptografie

1) **Kryptografie na bázi kódů** *(Code-based cryptography):* Její bezpečnost je založena na obtížnosti efektivně dekódovat obecný lineární kód pro opravu chyb. Vybrané algoritmy z této kategorie, například Classic McEliece, jsou považovány za jedny s nejvyššími bezpečnostními zárukami. Jejich velkou praktickou nevýhodou jsou extrémně dlouhé veřejné klíče.

2) **Kryptografie na mřížkách** (*Lattice-based cryptography*): Její bezpečnost je založena na obtížnosti řešení některých problémů na mřížkách, jako například problém nejkratšího vektoru, problém nejbližšího vektoru, učení s chybami. V současnosti je díky kombinaci svých bezpečnostních a praktických vlastností považována za jednu z nejperspektivnějších oblastí postkvantové kryptografie. Zlepšení praktických vlastností těchto postkvantových algoritmů lze dosáhnout tím, že jsou definovány na strukturovaných mřížkách. Nutno dodat, že příliš vysoká strukturovanost mřížky může vést k úspěšné kryptoanalýze.

3) **Digitální podpisy na bázi hašovacích funkcí** (*Hash-based cryptography*): Jejich bezpečnost je založena na bezpečnostních vlastnostech použitých hašovacích funkcí. Vzhledem k tomu, že kvantová odolnost hašovacích funkcí je dobře podložena, jsou tyto podpisové algoritmy považovány za postkvantovou kryptografii s vysokými zárukami bezpečnosti. To je ale vykoupeno určitými praktickými problémy. V některých případech je podstatně omezen maximální počet podpisů jedním klíčem, v jiných je mimořádně dlouhý veřejný klíč, a jsou tedy vhodné pouze pro specifické způsoby použití.

4) **Kryptografie na bázi isogenií nad supersingulárními eliptickými křivkami** (*Isogeny-based cryptography*): Její bezpečnost je založena na obtížnosti hledání isogenie mezi dvěma supersingulárními eliptickými křivkami (pokud tato isogenie existuje). Tento přístup byl poměrně dlouho považován za vysoce perspektivní, ale v roce 2022 byl na jeden z kryptosystémů na bázi isogenií nalezen efektivní útok, kterým je jejich bezpečnost vážně zpochybněna[13].

5) **Multivariační kryptografie**[9] (*Multivariate cryptography*): Její bezpečnost je založena na obtížnosti řešení soustav polynomiálních rovnic s mnoha proměnnými nad číselnými tělesy. Tato oblast kryptografie byla v minulosti terčem mnoha úspěšných útoků, takže záruky její bezpečnosti nejsou v současnosti považovány za příliš důvěryhodné[14], [15].

[9] *Multivariate* znamená vícerozměrný a ve spojení se slovem *cryptography* odkazuje na to, že tento typ kryptografie pracuje s velkým počtem proměnných. Překlad „multivariační kryptografie“ se pokouší vystihnout specifičnost tohoto typu postkvantové kryptografie.

3 Standardizace postkvantové kryptografie řízená institucí NIST

Od roku 2016[17], [18] probíhá proces standardizace postkvantové kryptografie organizovaný institucí NIST formou veřejné soutěže. V závěru jejího třetího kola byla vybrána první čtveřice postkvantových algoritmů ke standardizaci (viz kap. 3, odst. (4)) a jiná čtveřice kryptografických algoritmů postoupila do čtvrtého kola, ve kterém by se mělo rozhodnout o případné standardizaci některých z nich (viz kap. 3, odst. (5)).

V roce 2020 NIST standardizoval (mimo soutěž, ale v konsensu s odbornou veřejností) dvojici postkvantových digitálních podpisů LMS a XMSS založených na hašovacích funkcích[16].

(1) Kategorie soutěžních kandidátů z hlediska jejich funkcionalit

Postkvantová kryptografie má nahradit v současnosti používanou asymetrickou kryptografii ve dvou oblastech:

- kryptografii pro ustanovení klíčů a pro asymetrické šifrování,
- digitální podpisy.

Tomu do značné míry odpovídají i dvě hlavní kategorie soutěže NIST:

A) *KEM/Encryption*[10] – metody ustanovení symetrických klíčů na bázi asymetrického šifrování[11]
B) *Signatures* – digitální podpisy

(2) Požadavky NIST na bezpečnost postkvantových kandidátů

V případě kvantově odolné kryptografie musí být zvažována nejen její bezpečnost vůči klasickým útokům, ale také její odolnost vůči případným budoucím útokům využívajícím kvantové počítače[17], [18].

---

[10] KEM a Encryption jsou v tomto kontextu dvě blízké metody, jejichž podstatou je asymetrické šifrování symetrických klíčů:

- *Encryption* zde znamená standardní asymetrické šifrování symetrických klíčů.
- *KEM – Key Encapsulation Mechanism* je mechanismus zapouzdření klíče[33]. Od asymetrického šifrování se odlišuje tím, že při procesu zapouzdření nejdříve vygeneruje náhodné tajemství, to zašifruje pomocí veřejného klíče na šifrový text a ze zmíněného náhodného tajemství odvodí hašováním symetrický klíč.

[11] Důsledky výběru funkcionalit KEM/Encryption:

Algoritmy vybrané v kategorii KEM/Encryption mají doplnit nebo nahradit buď klasické asymetrické šifrování klíčů, nebo Diffieovu-Hellmanovu výměnu (ať již klasickou nebo nad eliptickou křivkou). V případě klasického asymetrického šifrování půjde o náhradu za algoritmus stejného typu, ale v případě Diffieovy-Hellmanovy výměny půjde o její náhradu za KEM nebo za asymetrické šifrování, tedy za jiný typ kryptografického algoritmu. To může být jedním z mnoha zdrojů problémů při přechodu ke kvantově odolné kryptografii v této oblasti.

Požadavky na bezpečnost postkvantových kandidátů přihlášených do soutěže jsou specifikovány jednak pomocí předpokládaných omezení výpočetních možností útočníka, jednak pomocí standardních předpokladů o jeho přístupových možnostech k napadenému zařízení a dále pomocí kritérií úspěšnosti útoku. V tomto případě je do výpočetních možností útočníka zahrnuta též možnost použít i značně rozsáhlý kvantový výpočet.

a) Bezpečnostní úrovně

NIST definoval pět různých předpokladů o omezení výpočetních možností útočníka a každé z těchto pěti možností přiřadil jednu bezpečnostní úroveň[18] str. 15 až 18. Bezpečnostní úrovně postkvantových algoritmů definované NIST jsou určeny počty kroků, ať již klasického nebo kvantového kryptoanalytického algoritmu, potřebnými ke zlomení daného schématu[12].

Bezpečnostní úrovně dle NIST:

- Úroveň 1, odpovídá náročnosti útoku hrubou silou na AES-128[13]
- Úroveň 2, odpovídá náročnosti generického hledání kolizí SHA-256
- Úroveň 3, odpovídá náročnosti útoku hrubou silou na AES-192
- Úroveň 4, odpovídá náročnosti generického hledání kolizí SHA-384
- Úroveň 5, odpovídá náročnosti útoku hrubou silou na AES-256

Hlubší studium omezení možností útočníka definujících bezpečnostní úroveň 5 ukazuje, že požadavky na tuto úroveň jsou z hlediska odhadů jeho reálných možností ve střednědobé budoucnosti značně předimenzované. Zřejmě proto NIST při vyhlášení soutěže vyzval

---

[12] Tři z těchto bezpečnostních úrovní (1, 3 a 5) NIST definoval pomocí výpočetní náročnosti hledání klíče blokové šifry AES hrubou silou. Úrovně jsou odlišeny délkami klíčů (128, 192 a 256 bitů). V klasickém případě odpovídají uvažované úrovně výpočetním náročnostem 2^{127}, 2^{191} a 2^{255} šifrování AES. V kvantovém případě bez použití paralelizace by odpovídaly 2^{64}, 2^{96} a 2^{128} krokům Groverova algoritmu. Uvažujeme-li možnost paralelizace a omezení hloubky bezchybného výpočtu, stává se konkrétní obsah definice podstatně složitější[19], [20].

Dvě zbývající bezpečnostní úrovně (2 a 4) NIST definoval pomocí výpočetní náročnosti hledání kolizí hašovací funkce SHA-2 hrubou silou. Úrovně jsou odlišeny vybranými délkami výstupů SHA-2, a to 256 a 384 bitů. V klasickém případě odpovídají uvažované úrovně výpočetním náročnostem 2^{128} a 2^{192} výpočtů kompresní funkce SHA-2. V kvantovém případě by měly odpovídat 2^{85} a 2^{128} krokům BHT-algoritmu[5]. Ten ale vyžaduje nereálně rozsáhlou kvantovou paměť. Pravděpodobně proto v definicích úrovní 2 a 4 nespecifikoval NIST kvantovou náročnost. V letech 2017 a 2019 byly navrženy efektivnější alternativy[21], [22] k BHT-algoritmu s podstatně nižšími (i když stále velmi vysokými) nároky na rozsah kvantové paměti, takže práce [20] se zabývá i kvantovými náročnostmi úrovní 2 a 4.

[13] Odtud dostáváme jiný pohled na kvantovou zranitelnost/odolnost symetrické kryptografie s délkami klíčů 128 bitů a 192 bitů. Odpovídá bezpečnostním úrovním 1 a 3 postkvantové kryptografie. Obdobně kvantová zranitelnost/odolnost SHA-2 s délkou výstupu 256 bitů odpovídá bezpečnostní úrovni 2 postkvantové kryptografie.

vývojáře, aby se soustředili hlavně na bezpečnostní úrovně 1 až 3, protože lze očekávat, že ty v dohledné budoucnosti poskytnou dostatečnou bezpečnost[14].

b) Bezpečnostní požadavky NIST z hlediska uvažovaných scénářů útoků

Z hlediska uvažovaných scénářů útoků má NIST standardní požadavky[18] str. 14 a 15:

A) V případě schémat KEM/Encryption je požadována sémantická bezpečnost při útocích s adaptivní volbou šifrového textu, je tedy požadována IND-CCA2 bezpečnost[15].

B) V případě algoritmů pro digitální podpisy je požadováno, aby útočník při tzv. útoku s volbou zprávy nebyl schopen zkonstruovat žádnou platnou podvrženou dvojici zpráva a její podpis. Je tedy požadována EUF-CMA bezpečnost.

c) Další požadavky na bezpečnost kandidátů[18] str. 19

Dokonalá dopředná bezpečnost[16]: Některé vlastnosti postkvantových kandidátů by mohly komplikovat zajištění dopředné bezpečnosti. Mohlo by jít například o přílišnou pomalost generování nového páru veřejného a soukromého klíče, která by mohla komplikovat jejich dostatečně častou výměnu, nebo o příliš velkou délku veřejného klíče, která by mohla komplikovat jeho přenosy. NIST preferuje kandidáty, u nichž tyto problémy nenastávají.

Odolnost vůči útokům na bázi fyzikálních postranních kanálů: NIST avizoval, že bude preferovat taková schémata postkvantové kryptografie, u kterých bude zajištění jejich odolnosti vůči útokům využívajícím postranní kanály méně náročné.

Odolnost vůči útokům na mnoho klíčů: V ideálním případě by útočník neměl získat relevantní výhodu tím, že bude současně útočit na mnoho klíčů použitých daným schématem.

Odolnost vůči chybným implementacím a chybným použitím schématu: Další žádoucí vlastnost postkvantových schémat můžeme zformulovat zhruba takto: Bezpečnost schématu by neměla být dramaticky devastována za situací, jako je například omezená (nepříliš velká)

---

[14] Avšak pro případ možného budoucího průlomu v kryptoanalýze nebo v technologiích požádal i o specifikaci parametrů odpovídající podstatně vyšší úrovni bezpečnosti než 3[18] str. 18.

[15] NIST rovněž uvažoval KEM/Encryption s efemérními veřejnými klíči, tedy s klíči na jedno použití. Podstatné je zde to, že jakmile v protokolu pro ustanovení symetrických klíčů dojde k první chybě, vygeneruje se nový pár veřejného a soukromého klíče a starý pár se poté, co není potřebný, vymaže. V takovém případě samozřejmě postačí pouze sémantická bezpečnost při útoku s volbou otevřeného textu, tedy IND-CPA.

[16] V případech KEM/Encryption chrání dopředná bezpečnost důvěrnost dříve zašifrovaných dat za situace, že útočník v minulosti odposlouchával a ukládal šifrovanou komunikaci a poté se zmocnil některého z aktuálně používaných soukromých klíčů. K tomu, aby dříve zašifrovaná data byla i za těchto okolností chráněna, je nutné, aby příslušné soukromé klíče byly po svém použití mazány a nahrazovány nově generovanými soukromými klíči.

chyba v kódu schématu, nebo selhání náhodného generátoru, nebo opakované použití páru soukromého a veřejného klíče u KEM/Encryption schématu s efemérními klíči a podobně.

(3) Ostatní kritéria hodnocení kandidátů

a) Výkonnost, délky přeposílaných kryptografických proměnných a jiné[18] str. 20

Velikosti veřejných klíčů, šifrových textů a digitálních podpisů: V případech, v nichž způsoby použití schématu nevyžadují časté posílání veřejných klíčů, nemá jejich velikost vážnější praktické dopady. Opačná situace nastává například všude tam, kde je vyžadována dokonalá dopředná bezpečnost.

Výpočetní efektivnost operací s veřejnými a se soukromými klíči: Tyto vlastnosti schématu jsou důležité téměř vždy, nicméně existují způsoby použití postkvantové kryptografie, pro které mohou mít důležitost kritickou.

Výpočetní efektivnost generování klíčů: Tato vlastnost schématu je důležitá zejména v případech, kdy je vyžadována dokonalá dopředná bezpečnost.

Selhání dešifrování: V případech schémat s možností selhání dešifrování[17] NIST požaduje záruky, že k němu bude docházet se zanedbatelnou (s prakticky nulovou) pravděpodobností.

b) Další požadované vlastnosti souhrnně označované jako flexibilita[18] str. 21

Pod flexibilitou schématu NIST chápe vlastnosti jako například:

- možnost nepříliš obtížné modifikace schématu tak, aby získalo další požadované vlastnosti,
- možnost dostatečně snadno pozměnit parametry schématu za účelem dosažení jeho jiných bezpečnostních nebo provozních vlastností,
- možnost paralelizace implementace,
- možnost začlenění schématu do existujících protokolů a aplikací vyžadující pouze jeho minimální změny[18].

[17] V případech některých schémat postkvantové kryptografie je teoreticky možné, aby došlo k selhání dešifrování (zde k odmítnutí šifrového textu) i za okolností, kdy schéma bylo korektně implementováno a šifrový text byl korektně vygenerován a cestou do dešifrovacího zařízení nebyl zmodifikován.

[18] Přílišné délky veřejných klíčů nebo šifrových textů, případně pomalost kryptografických operací mohou začlenění postkvantových schémat do existujících protokolů a aplikací komplikovat.

(4) Postkvantové algoritmy dosud vybrané NIST ke standardizaci

V červenci 2022[26], [27] vybral NIST v rámci soutěže první čtveřici kvantově odolných algoritmů určených pro standardizaci. V srpnu 2024 NIST vydal standardy tří z nich (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+) a na standardu čtvrtého pracuje (Falcon).

a) Algoritmy CRYSTALS, skuteční vítězové soutěže

Ačkoliv NIST dosud vybral ke standardizaci čtyři algoritmy, algoritmy CRYSTALS mají mezi nimi mimořádné postavení. V kategorii KEM/Encryption byl zatím pro standardizaci vybrán jediný algoritmus, a to CRYSTALS-Kyber. V kategorii postkvantových digitálních podpisů byly sice vybrány tři algoritmy, z nich ale NIST doporučuje CRYSTALS-Dilithium jako primární volbu algoritmu pro digitální podpis[26], sl. 13.

NIST oba tyto algoritmy hodnotí tak, že jejich návrhy jsou kvalitně vědecky podloženy[19], jsou relativně jednoduché, lze je snadno implementovat a umožňují dosáhnout dobrou výkonnost kryptografických operací. Část implementace obou algoritmů může být společná.

V srpnu 2024 NIST vydal standardy obou těchto algoritmů, a to:

- FIPS 203[66], v němž je CRYSTALS-Kyber standardizován jako ML-KEM (Module Lattice Based Key Encapsulation Mechanism)[20]
- FIPS 204[67], v němž je CRYSTALS-Dilithium standardizován jako ML-DSA (Module Lattice Based Digital Signature Algorithm)

b) Kategorie KEM/Encryption

V této kategorii NIST dosud vybral pro standardizaci jediný algoritmus:

CRYSTALS-Kyber (standardizovaný jako **ML-KEM**)
Je IND-CCA2-bezpečné postkvantové schéma na bázi strukturovaných mřížek[21].
Ke standardizaci byl vybrán pro svou bezpečnost a výkonnost. Jeho výkonnost na různých platformách je institucí NIST hodnocena jako excelentní.

[19] Bezpečnost obou zmíněných algoritmů typu CRYSTALS je založena na obtížnosti řešení Module-LWE (tj. Module Learning with Errors) problému, který odpovídá problému hledání malého vektoru na strukturované (modulární) mřížce.

[20] Standardizovaný algoritmus ML-KEM se od původního algoritmu Kyber z třetího kola soutěže NIST mírně odlišuje. Základní matematické a kryptografické principy obou algoritmů jsou ale stejné a z hlediska tohoto dokumentu je lze v mnoha místech ztotožnit. Totéž platí o algoritmech ML-DSA a Dilithium.

[21] Jeho bezpečnost je založena na obtížnosti řešení Module-LWE problému.

Standard FIPS 203[66] definuje tři varianty ML-KEM, které odpovídají variantám původního algoritmu CRYSTALS-Kyber:

- ML-KEM-512 – Kyber-512 (úroveň 1)
- ML-KEM-768 – Kyber-768 (úroveň 3)
- ML-KEM-1024 – Kyber-1024 (úroveň 5)

Pro jednotlivé bezpečnostní úrovně 1, 3 a 5 mají jeho veřejné klíče po řadě délky 800, 1184 a 1568 bajtů a jeho šifrové texty mají po řadě délky 768, 1088 a 1568 bajtů.

Vývojový tým algoritmů CRYSTALS doporučuje[60] používat Kyber v hybridním módu s klasickou asymetrickou kryptografií. Jako preferovanou variantu v této kombinaci doporučuje úroveň 3 s odůvodněním, že „podle velmi konzervativních analýz zajišťuje více než 128bitovou bezpečnost vůči všem známým klasickým a kvantovým útokům“.

c) Kategorie digitální podpis

V této kategorii NIST dosud vybral pro standardizaci tři algoritmy:

CRYSTALS-Dilithium (standardizovaný jako **ML-DSA**)

Je EUF-CMA-bezpečné postkvantové podpisové schéma na bázi strukturovaných mřížek[22]. Ke standardizaci bylo vybráno pro svou bezpečnost, vysokou výkonnost a poměrně jednoduché schéma návrhu. Institucí NIST je hodnoceno jako vysoce efektivní schéma se snadnou implementací a silnými bezpečnostními zárukami.

Standard FIPS 204[67] definuje tři varianty ML-DSA, které odpovídají variantám původního algoritmu CRYSTALS-Dilithium:

- ML-DSA-44 – Dilithium 2 (úroveň 2)
- ML-DSA-65 – Dilithium 3 (úroveň 3)
- ML-DSA-87 – Dilithium 5 (úroveň 5)

Pro jednotlivé bezpečnostní úrovně 2, 3 a 5 mají jeho veřejné klíče po řadě délky 1312, 1952 a 2592 bajtů a jeho podpisy mají po řadě délky 2420, 3293 a 4595 bajtů.

Vývojový tým algoritmů CRYSTALS doporučuje[61] používat Dilithium v hybridním módu s klasickým podpisovým algoritmem. Jako preferovanou variantu v této kombinaci doporučuje úroveň 3 s odůvodněním, že „podle velmi konzervativních analýz zajišťuje více než 128bitovou bezpečnost vůči všem známým klasickým a kvantovým útokům“.

Falcon (bude standardizován jako **FN-DSA**)

Je EUF-CMA-bezpečné postkvantové podpisové schéma na bázi strukturovaných mřížek[23]. Jeho výhodou jsou malé délky klíčů a digitálních podpisů. Nevýhodou je jeho velmi složitý návrh, který znesnadňuje dobré porozumění detailům schématu a korektní implementaci.

[22] Bezpečnost algoritmu CRYSTALS-Dilithium je založena na obtížnosti řešení Module-LWE a Module-SIS problému.

[23] Bezpečnost algoritmu Falcon je založena na obtížnosti řešení SIS problému na NTRU mřížce.

Právě krátkost klíčů a podpisů při dobrých zárukách bezpečnosti byla důvodem jeho výběru pro standardizaci.

NIST předpokládá, že bude standardizovat varianty[26], sl. 14:

- Falcon-512 (úroveň 1, bude standardizován jako FN-DSA-512)
- Falcon-1024 (úroveň 5, bude standardizován jako FN-DSA-1024)

Pro bezpečnostní úrovně 1 a 5 mají jeho veřejné klíče po řadě délky 897 a 1793 bajtů a jeho podpisy mají po řadě délky 666 a 1280 bajtů.

Jeho standard zatím nebyl vydán[24].

SPHINCS+ (standardizován jako **SLH-DSA**)

Je EUF-CMA-bezpečné postkvantové podpisové schéma na bázi hašovacích funkcí. Jeho bezpečnost je založena na bezpečnosti použité hašovací funkce, v tomto případě buď SHAKE256, nebo SHA-256, nebo Haraka.

Na rozdíl od schémat XMSS a LMS není v případě SPHINCS+ nutné, aby podepisující zařízení udržovalo informaci o podpisech vytvořených daným klíčem, a proto v jeho případě nevzniká omezení počtu podpisů týmž klíčem. To je ale do značné míry vyváženo enormně dlouhými digitálními podpisy. Tento podpisový algoritmus byl vybrán ke standardizaci, protože má velmi silné bezpečnostní garance a protože je zkonstruován na jiné bázi než na mřížkách.

Standardizovány byly varianty SPHINCS+ na bázi hašovacích funkcí SHA2 a SHA3 (SHAKE):

A) Na bázi SHA2

- SLH-DSA-SHA2-128s (úroveň 1), SLH-DSA-SHA2-128f (úroveň 1)
- SLH-DSA-SHA2-192s (úroveň 3), SLH-DSA-SHA2-192f (úroveň 3)
- SLH-DSA-SHA2-256s (úroveň 5), SLH-DSA-SHA2-256f (úroveň 5)

B) Na bázi SHAKE

- SLH-DSA-SHAKE-128s (úroveň 1), SLH-DSA-SHAKE-128f (úroveň 1)
- SLH-DSA-SHAKE-192s (úroveň 3), SLH-DSA-SHAKE-192f (úroveň 3)
- SLH-DSA-SHAKE-256s (úroveň 5), SLH-DSA-SHAKE-256f (úroveň 5)

(5) Další kandidáti podstatní z hlediska doporučené kvantově odolné kryptografie

Do třetího kola standardizační soutěže NIST vstoupili 4 finalisté a 5 alternativních kandidátů v kategorii KEM/Encryption a 3 finalisté a 3 alternativní kandidáti v kategorii digitální podpis.

[24] V době vydání této verze Přílohy.

a) Další kandidáti třetího kola s vysokými bezpečnostními garancemi[28]

Pro praktická doporučení kvantově odolné kryptografie v blízké budoucnosti považujeme za podstatné v kategorii KEM/Encryption i kandidáta třetího a čtvrtého kola Classic McEliece a alternativního kandidáta třetího kola FrodoKEM. Důvod, proč tomu tak je, úzce souvisí s jejich bezpečností. Mají totiž principiálně vyšší teoretické záruky bezpečnosti než vítěz v této kategorii CRYSTALS-Kyber. A důvody, proč (zatím) nebyly vybrány ke standardizaci, souvisí s některými jejich praktickými vlastnostmi[7], str. 34.

Classic McEliece je IND-CCA2-bezpečný postkvantový algoritmus na bázi kódů. Za čtyřicet let od jeho publikace nebyly na tento algoritmus nalezeny závažnější útoky[30], sl. 3, přestože je z bezpečnostního hlediska jedním z nejlépe prozkoumaných kandidátů soutěže[25]. Proto má odborná veřejnost v jeho dlouhodobou bezpečnost mimořádnou důvěru[42], sl. 88. BSI[20] str. 39 ho doporučuje k okamžitému hybridnímu použití jakožto postkvantový KEM algoritmus s nejvyššími bezpečnostními garancemi. Jeho výkonnost ve smyslu rychlosti kryptografických operací je velmi dobrá. Jeho hlavní nevýhodou jsou extrémně dlouhé veřejné klíče (od 250 kB pro úroveň 1 až do 1,3 MB pro úroveň 5). To znamená, že je vhodný především pro taková použití, ve kterých je jeho veřejný klíč statický a nemusí se posílat. Zatím nebyl institucí NIST vybrán ke standardizaci, ale jakožto kandidát postoupil do čtvrtého kola soutěže.

FrodoKEM je IND-CCA2-bezpečný postkvantový algoritmus založený na nestrukturovaných mřížkách. Využití nestrukturované mřížky podstatným způsobem zvyšuje jeho teoretickou bezpečnost, a to i v porovnání s vítězem CRYSTALS-Kyber v kategorii KEM/Encryption. To je důvodem, proč ho BSI[7], str. 34, [29], str. 35 a ANSSI[57], sl. 20 doporučují k okamžitému hybridnímu použití jakožto postkvantový KEM. Nicméně do čtvrtého kola soutěže NIST jako alternativní kandidát nepostoupil. Je to dáno jeho poměrně nízkou výkonností, dlouhými soukromými a veřejnými klíči a také snahou NIST standardizovat i jiné kandidáty než ty, které jsou založeny na mřížkách.

Bezpečnostní úrovně algoritmu FrodoKEM:

- FrodoKEM-640, úroveň 1,
- FrodoKEM-976, úroveň 3,
- FrodoKEM-1344, úroveň 5.

b) Další kandidáti ze čtvrtého kola soutěže NIST

Dalšími kandidáty čtvrtého kola standardizační soutěže NIST, a tedy i potenciálními budoucími standardy, jsou algoritmy BIKE a HQC. Jejich společnou výhodou jsou výrazně menší velikosti veřejných a soukromých klíčů než u algoritmu Classic McEliece (ze stejné rodiny postkvantových algoritmů – založených na bázi kódů). Za nevýhodu v porovnání

[25] Za celou tu dobu se bezpečnostní parametry algoritmu Classic McEliece měnily pouze v souvislosti s růstem výpočetních možností případného útočníka a v návaznosti na možnost realizace kvantových počítačů.

s algoritmem Classic McEliece ale může být považováno, že jsou poměrně nové, a tedy byly kratší dobu vystaveny analýzám odborné veřejnosti.

HQC je IND-CCA2-bezpečný postkvantový algoritmus založený na kvazicyklických kódech. Návrh z posledního kola využívá složení Reed-Mullerova a Reed-Solomonova samoopravného kódu. Pro bezpečnostní úrovně 1, 3 a 5 jsou velikosti jeho veřejných klíčů 2249 až 7245 bajtů a jeho šifrových textů 4497 až 14485 bajtů. Velikost jeho soukromého klíče pro všechny úrovně bezpečnosti je pouhých 40 bajtů.

BIKE je postkvantový algoritmus založený na QC-MDPC kódech (*quasi-cyclic moderate density parity-check codes*). Oproti ostatním alternativním kandidátům jsou jeho výhodou velmi krátké veřejné klíče a šifrové texty, ale zatím chybí důkaz jeho IND-CCA2 bezpečnosti. Pro bezpečnostní úrovně 1, 3 a 5 jsou velikosti jeho veřejných klíčů necelých 1541 až 5122 bajtů, jeho šifrových textů necelých 1573 až 5154 bajtů a jeho soukromých klíčů necelých 281 až 580 bajtů.

c) Varovná překvapení ve finále soutěže NIST

Rainbow byl finalistou soutěže NIST v kategorii digitální podpis. Rovněž byl jediným finalistou na bázi polynomů s mnoha proměnnými (multivariační kryptografie). Poměrně krátce poté byla jeho varianta bezpečnostní úrovně 1 zlomena útokem realizovaným na laptopu během jednoho víkendu[15].

SIKE byl alternativním kandidátem třetího kola soutěže NIST v kategorii KEM/Encryption a byl jediným alternativním kandidátem na bázi isogenií supersingulárních eliptických křivek. Na rozdíl od algoritmu Rainbow ale prošel až do čtvrtého kola soutěže. A krátce poté byl zlomen devastujícím útokem na klasickém počítači pro všechny své bezpečnostní úrovně[13].

Zvláště případ SIKE je velmi varující. Kryptografie založená na isogeniích supersingulárních eliptických křivek byla dlouho považována za vysoce perspektivní a o jejím zdravém bezpečnostním základu nebyly vážnější pochyby. Přesto byla nedávno zlomena praktickým útokem na klasickém počítači.

d) Výzva NIST k návrhům dalších postkvantových digitálních podpisů[27]

NIST v září 2022 vyzval odbornou veřejnost k tvorbě návrhů dalších postkvantových podpisů. Má zájem zejména o algoritmy[27], str. 2 založené na jiných principech než na strukturovaných mřížkách. Z hlediska některých aplikací, zejména ověřování certifikátů, se NIST zřejmě bude zajímat o algoritmy digitálního podpisu s krátkým výstupem a s rychlým ověřením platnosti podpisu.

(6) Důvěryhodné postkvantové kryptografické algoritmy soutěže NIST

a) Předpokládaný způsob jejich použití

Hlavním cílem této části je výběr postkvantových algoritmů soutěže NIST, jejichž použití lze doporučit k zajištění ochrany citlivých informací kritické úrovně důvěrnosti nebo integrity proti kvantové hrozbě[26]. Na základě konsensu odborné veřejnosti a evropských bezpečnostních autorit předpokládáme, že nejprve budou používány v hybridních kombinacích s příslušnými schválenými klasickými asymetrickými algoritmy.

b) Digitální podpis pro obecné použití

V případě postkvantových algoritmů digitálního podpisu s předpokládaným obecným použitím považujeme za důvěryhodné ty dosavadní vítěze soutěže, kteří již byli standardizováni:

- ML-DSA úrovně 3 a 5
- SLH-DSA úrovně 3 a 5

K nim po své standardizaci pravděpodobně přibude FN-DSA úrovně 5.

c) KEM/Encryption

Tato kategorie má zatím jediného vítěze CRYSTALS-Kyber, standardizovaného jako ML-KEM.

Odborná veřejnost a zejména BSI upozorňují na kandidáty, kteří sice v soutěži nezvítězili, ale v porovnání s jejím vítězem mají vysoké bezpečnostní záruky. Jde jednak o algoritmus Classic McEliece, na který nebyly během 40 let jeho existence zkonstruovány relevantní útoky, a dále o algoritmus FrodoKEM, který je definován na nestrukturovaných mřížkách, a proto má vyšší teoretickou bezpečnost než vítěz soutěže[7], str. 34.

Za důvěryhodné považujeme algoritmy, které odpovídají bezpečnostním úrovním 3 a 5.

Tabulka 1: Důvěryhodné postkvantové algoritmy typu KEM/Encryption[27]

ML-KEM-1024	FrodoKEM-1344	mceliece8192128	mceliece8192128f
ML-KEM-768	FrodoKEM-976	mceliece6688128	mceliece6688128f
		mceliece460896	mceliece460896f

[26] Nebudeme tedy v této části uvádět již standardizované digitální podpisy LMS a XMSS, které sice neprošly soutěží NIST, ale mají natolik vysoké bezpečnostní garance, že jsou všemi relevantními autoritami doporučovány k samostatnému nasazení, zejména pro ochranu integrity softwaru a firmwaru.

[27] Pokud jde o bezpečnostní úrovně, pak v případě ML-KEM (CRYSTALS-Kyber) vycházíme ze závěrečného doporučení jeho vývojového týmu a v případech ostatních dvou algoritmů zejména z doporučení BSI[29] str. 35 a 36.

4 Hybridní nebo samostatné použití postkvantové kryptografie?

(1) Důvody pro hybridní použití postkvantové kryptografie v blízké budoucnosti

Ve vědecké komunitě panuje dlouhodobý konsensus v názoru, že po nějakou dobu bychom měli postkvantovou kryptografii používat k ochraně informací pouze v hybridní kombinaci s klasickou asymetrickou kryptografií[28]. Na tomto přístupu stále trvá i většina evropských bezpečnostních autorit jako například německá BSI[29], str. 25 a francouzská ANSSI[56].

Některé novější postkvantové algoritmy byly totiž zlomeny pomocí útoků využívajících pouze klasické počítače[29]. V těchto případech by použití samostatných postkvantových algoritmů místo schválené asymetrické kryptografie vedlo k degradaci bezpečnosti. Avšak hybridní kombinace postkvantové kryptografie s klasicky bezpečnou asymetrickou kryptografií bude bezpečná alespoň proti klasickým útokům[30].

Jedním z důvodů zlomitelnosti některých postkvantových algoritmů je to, že některé typy postkvantové kryptografie jsou poměrně nové. To znamená, že zatím nemáme dostatečné záruky toho, že odpovídající matematické problémy, na jejichž praktické neřešitelnosti je založena bezpečnost příslušných postkvantových algoritmů, jsou opravdu prakticky neřešitelné, a to ani na současných počítačích[31].

Ale ani to, že bezpečnost poměrně nového kryptografického algoritmu je založena na opravdu prakticky neřešitelném matematickém problému, nemusí znamenat, že je tento algoritmus bezpečný.[32]

---

[28] BSI[7], str. 38 (a nejen BSI) navrhuje obecnější přístup, a to, aby pro ustanovení symetrických klíčů mohla být použita hybridní kombinace libovolných dvou z následujících tří mechanismů: klasická asymetrická kryptografie, postkvantová kryptografie a ochrana na bázi (případných) předdistribuovaných klíčů.

[29] Případně byly zlomeny útoky vyžadujícími pouze klasické počítače a využívajícími i fyzikální postranní kanály.

[30] Pokud by útoky na nové postkvantové algoritmy byly založeny pouze na kvantových algoritmech, nebyly by důvodem k používání hybridních kombinací postkvantové a klasické asymetrické kryptografie.

[31] Příkladem je postkvantový KEM algoritmus SIKE dlouho považovaný za vysoce perspektivní, na který byl zkonstruován devastující útok vyžadující pouze laptop[13].

[32] Příkladem je klasický útok na algoritmus Rainbow[15], který se dokonce dostal mezi finalisty třetího kola soutěže[28]. Jiným příkladem mohou být chybná klonování náhodného orákula v konstrukcích některých novějších postkvantových algoritmů typu KEM, která vedla v některých případech k jejich zlomení[35].

(2) Sada kvantově odolných algoritmů CNSA 2.0 schválených americkou NSA

V září 2022 americká agentura NSA publikovala sadu komerčních algoritmů pro národní bezpečnost CNSA 2.0. V ní obsažené algoritmy jsou schváleny NSA pro použití v národních bezpečnostních systémech (NSS – *National Security Systems*). Tato sada CNSA 2.0 nahrazuje předchozí sadu CNSA 1.0 kvantově odolnými kryptografickými algoritmy.

a) Algoritmy sady CNSA 2.0[36]

Sada CNSA 2.0 obsahuje algoritmy rozdělené do tří oblastí svého použití:

- Algoritmy pro digitální podpisy softwaru a firmwaru
- Algoritmy se symetrickými klíči
- Kvantově odolné asymetrické algoritmy s obecným použitím

Algoritmy pro digitální podpisy softwaru a firmwaru

NSA doporučuje přejít v této oblasti co nejrychleji k používání algoritmů digitálního podpisu založených na hašovacích funkcích, které již byly standardizovány NIST. Jsou specifikovány standardem NIST SP 800-208[64]. Jde o algoritmy:

- LMS (*Leighton Micali Signature*) s doporučenými hašovacími funkcemi SHA-256/192
- XMSS (e*Xtended Merkle Signature Scheme*)

Jsou schváleny všechny jejich parametry pro všechny klasifikované úrovně.
V případě algoritmů LMS a XMSS NSA doporučuje jejich samostatné použití.

Algoritmy se symetrickými klíči

Pro tuto oblast jsou pro NSS schváleny algoritmy:

- AES-256 dle FIPS PUB 197
- SHA-384 nebo SHA-512 dle FIPS PUB 180-4

Jsou schváleny pro všechny klasifikované úrovně.

Kvantově odolné asymetrické algoritmy s obecným použitím

Pro tuto oblast jsou pro NSS schváleny algoritmy:

- ML-KEM – asymetrický algoritmus pro ustanovení klíčů
- ML-DSA – asymetrický algoritmus pro digitální podpis

Jsou schváleny (pouze) jejich varianty úrovně 5 pro všechny klasifikované úrovně.
V případě algoritmů ML-KEM a ML-DSA NSA schvaluje jejich samostatné použití.

b) Zdůvodnění NSA[37] schválení samostatného použití algoritmů rodiny CRYSTALS (ML-KEM a ML-DSA)

Rozhodnutí NSA o možnosti samostatného použití algoritmů rodiny CRYSTALS v amerických národních bezpečnostních systémech bylo pro většinu odborné veřejnosti překvapivé, protože je v rozporu s široce konsensuálním názorem o nutnosti používat postkvantovou kryptografii v nejbližší době pouze v hybridní kombinaci. Proto níže uvádíme příslušnou argumentaci NSA.

NSA na dotaz: „Za jak silné považuje NSA algoritmy sady CNSA 2.0?“ odpovídá, že provedla své vlastní analýzy těchto algoritmů a považuje je za vhodné pro dlouhodobé použití při ochraně různých misí US NSS[37], str. 3.

Na dotaz: „Jaký má NSA názor na použití hybridních řešení?“ NSA odpovídá, že má v algoritmy sady CNSA 2.0 důvěru a po vývojářích NSS nebude požadovat používání hybridních certifikovaných produktů z bezpečnostních důvodů[37], str. 13.

V reakci na dotaz: „Měla by se během čekání na postkvantové standardy NIST používat hybridní nebo jiná nestandardizovaná kvantově odolná řešení?“ NSA doporučuje nepoužívat hybridní nebo jiné nestandardizované řešení v NSS misí. Vyzývá k omezeným nákupům pro účely výzkumu a plánování, ale pouze za účelem přechodu k CNSA 2.0. Protože je NSA přesvědčena, že CNSA 2.0 bude NSS dostatečně chránit, nepožaduje hybridní řešení pro bezpečnostní účely[37], str. 14.

Na dotaz: „Jaké komplikace mohou být spojeny s použitím hybridního řešení?“ uvádí NSA mimo jiné tyto argumenty[37], str. 13 a 14:

- Hybridní řešení zvyšuje komplikovanost příslušných protokolů, zejména o nutnost další negociace a zpracování chyb.
- Hybridní řešení přináší problémy s interoperabilitou, protože oba algoritmy hybridního řešení musí být pro všechny strany společné.
- Po nějaké době se přejde na použití pouze kvantově odolných algoritmů. V případě hybridního řešení bude vyžadován další přechod.
- Více bezpečnostních produktů selže díky implementačním nebo konfiguračním chybám než kvůli použitým kryptografickým algoritmům. Máme-li ke zvýšení kryptografické složitosti jen omezené zdroje, můžeme tím potenciálně oslabit bezpečnost.

Postoj Kanadského centra pro kybernetickou bezpečnost k použití hybridních řešení

Kanadské centrum pro kybernetickou bezpečnost v prezentaci z března 2023 uvádí řadu konkrétních argumentů převážně proti použití hybridních řešení, z nichž je zřejmé, že ke vhodnosti jeho použití má rezervovaný postoj[39], sl. 10. Poznamenává, že vláda Kanady dosud nerozhodla, kde by mělo být hybridní řešení použito, a dále to, že o případném použití hybridních řešení by měli rozhodnout vlastníci příslušných kybernetických systémů[39], sl. 10.

c) Omezení schválení ML-KEM a ML-DSA na bezpečnostní úroveň 5

Zkušenost s historií útoků na kryptografii na mřížkách říká, že jejich hlavním důsledkem je potřeba postupného zvyšování bezpečnostních parametrů kryptografie na mřížkách[42], sl. 88. A volba bezpečnostní úrovně 5 představuje obrovskou praktickou bezpečnostní rezervu[33].

[33] Připomeňme, že návrhový tým algoritmů CRYSTALS je přesvědčen, že bezpečnostní úroveň 3 je pro jejich použití dostatečná.

(3) Postoj NÚKIB k samostatnému použití ML-KEM a ML-DSA úrovně 5

Konsensus odborné veřejnosti a evropských bezpečnostních autorit na potřebě použití hybridní kombinace postkvantové kryptografie s dalším ochranným mechanismem stále trvá.

Na druhou stranu, americká NSA je jednou z nejsofistikovanějších bezpečnostních autorit na světě s vysokým smyslem pro svou odpovědnost v oblasti národní bezpečnosti. Možnost, že by na základě vlastních analýz doporučila pro použití v amerických národních bezpečnostních systémech (NSS) kryptografii, která by se ve střednědobé budoucnosti ukázala být bezpečnostně slabou, má zanedbatelnou pravděpodobnost.

Proto NÚKIB v současnosti akceptuje oba uvažované přístupy pro zavádění kvantově odolné kryptografie pro ochranu citlivých informací kritické úrovně důvěrnosti nebo integrity v blízké budoucnosti. Tedy jak hybridních kombinací, tak i samostatných použití ML-KEM a ML-DSA úrovně 5, implementovaných dle příslušných standardů NIST[66],[67].

(4) Výjimečný status kvantově odolných digitálních podpisů LMS a XMSS

Kvantově odolné digitální podpisy LMS a XMSS byly standardizovány institucí NIST již v roce 2020, takže nic nebrání jejich implementaci. Při správném použití mají vysoké garance bezpečnosti a nevyžadují hybridní kombinaci s klasickým algoritmem digitálního podpisu. Jsou vhodné pro ochranu integrity firmwaru při jeho aktualizaci a lze s nimi nakládat jako se schválenými algoritmy s dlouhodobou bezpečností.

NSA doporučuje jejich urychlené nasazení pro ochranu integrity firmwaru a softwaru[36], str. 2 a 3. Rovněž BSI doporučuje tento způsob jejich použití[7], str. 62.

Postoj NÚKIB k samostatnému nasazení LMS a/nebo XMSS pro ochranu integrity firmwaru a softwaru

NÚKIB doporučuje uskutečnit v oblasti ochrany integrity firmwaru a softwaru při jejich aktualizacích přechod k využití samostatných kvantově odolných algoritmů LMS a XMSS, co nejdříve to bude možné.

5 Kvantově zranitelné algoritmy schválené v dokumentu „Minimální požadavky na kryptografické algoritmy“

(1) Význam níže používaného pojmu „kvantově zranitelný algoritmus“

a) Základní typy scénářů útoků na bázi kvantových technologií na kryptografii

Současná odborná literatura rozlišuje dva základní typy útoků s pomocí kvantových technologií na kryptografické algoritmy.

1) Útoky na kryptografii chránící klasickou informaci reprezentovanou řetězci bitů. To znamená, že v těchto scénářích se předpokládá, že útočník má k dispozici informace v bitech (například šifrové texty nebo digitální podpisy) a k jejich luštění nebo falšování využije mimo jiné i kvantové algoritmy v budoucnu implementované na kvantových počítačích.

2) Útoky na kryptografii chránící kvantovou informaci reprezentovanou řetězci provázaných qubitů. Tyto scénáře vycházejí z předpokladu, že v budoucnosti bude realizován a používán kvantový internet umožňující komunikaci pomocí kvantové informace. To kvalitativně podstatně rozšíří útočníkovy možnosti, protože jeho vstupy už nebudou klasické informace, ale informace kvantové.

Z výše uvedeného vyplývá, že mnohé dnes známé kryptografické algoritmy, které jsou kvantově odolné při ochraně klasické informace, by bezpečnostně selhaly při ochraně kvantové informace přenášené v budoucím kvantovém internetu.

b) Specifikace pojmu „kvantově zranitelný algoritmus“ používaného v této příloze

Na základě dostupných odhadů nepředpokládáme, že kvantový internet bude realizován dříve než za 15 až 20 let.

Proto jak v hlavním dokumentu „Minimální požadavky na kryptografické algoritmy“, tak i v této příloze budeme pod kvantově zranitelným (kryptografickým) algoritmem striktně chápat pouze takový algoritmus, který je při ochraně klasické informace zranitelný útoky využívajícími kryptograficky relevantní kvantový počítač.

V obou uvažovaných dokumentech tedy uvažujeme výlučně výše zmíněný scénář 1) a existenci scénáře 2) ignorujeme.

(2) Kvantová odolnost/zranitelnost symetrické kryptografie

Kvantová odolnost schválených módů symetrické kryptografie
Schválené módy v oblasti symetrické kryptografie považujeme za kvantově odolné, pokud jsou použity s kvantově odolnou schválenou blokovou šifrou nebo s kvantově odolnou schválenou hašovací funkcí.

Kvantová odolnost/zranitelnost schválených blokových a proudových šifer
Kvantově odolné jsou všechny schválené blokové a proudové šifry s délkou klíče 256 bitů. Všechny schválené blokové a proudové šifry s délkami klíčů 128 bitů a 192 bitů jsou kvantově zranitelné.

Míra naléhavosti přechodu ke schváleným kvantově odolným blokovým a proudovým šifrám
Přechod ke schváleným blokovým šifrám není ani příliš naléhavý, ale ani příliš náročný. Poněkud vyšší míru naléhavosti mají případy, kdy je šifra se 128bitovým klíčem používána k ochraně důvěrnosti dat[34]. Doporučujeme přejít do poloviny třicátých let v maximální míře k používání schválených symetrických šifer pouze s klíčem délky 256 bitů[35].

(3) Kvantová odolnost/zranitelnost hašovacích funkcí

Kvantová odolnost/zranitelnost schválených hašovacích funkcí
Kvantově odolné jsou všechny schválené hašovací funkce s délkou výstupu 384 nebo více bitů. Všechny schválené hašovací funkce s délkou výstupu 256 bitů jsou kvantově zranitelné.

Míra naléhavosti přechodu ke kvantově odolným schváleným hašovacím funkcím
Přechod ke schváleným kvantově odolným hašovacím funkcím není ani naléhavý, ale ani příliš náročný[36]. Přesto doporučujeme přejít do poloviny třicátých let v maximální míře k používání schválených hašovacích funkcí pouze s délkou výstupu 384 a více bitů[37].

(4) Kvantová zranitelnost schválených klasických algoritmů pro digitální podpis

a) Obecné použití klasických algoritmů digitálního podpisu

Kvantová zranitelnost schválených klasických algoritmů digitálního podpisu
Žádný ze schválených klasických algoritmů digitálního podpisu není kvantově odolný.

---

[34] Kvantová odolnost/zranitelnost symetrické kryptografie s délkami klíčů po řadě 128 bitů a 192 bitů odpovídá z definice bezpečnostním úrovním 1 a 3 postkvantové kryptografie. BSI uvádí[29], str.37, že Groverův algoritmus sice teoreticky umožňuje kvadratické zrychlení při prolomení klíče hrubou silou, ale že v současnosti stále není jasné, do jaké míry lze této výhody dosáhnout i prakticky. Na druhé straně, přechod ke kvantově odolné symetrické kryptografii je poměrně snadný. Postačí nahradit šifry s příliš krátkými klíči za schválené šifry s délkou klíčů 256 bitů.

[35] Připomeňme, že NSA sada CNSA 2.0 připouští pouze AES-256.

[36] Kvantová zranitelnost hašovacích funkcí s délkou výstupu 256 bitů úzce souvisí[20] s bezpečnostní úrovní 2 postkvantové kryptografie. Podle obr. 1 v [20] je pro realističtější nároky na paměť dokonce blízká úrovni 3. Na druhé straně, přechod k plně kvantově odolným hašovacím funkcím je poměrně snadný. Postačí nahradit hašovací funkce s délkou výstupu 256 bitů za hašovací funkce s délkou výstupu 384 bitů.

[37] Připomeňme, že NSA sada CNSA 2.0 připouští pouze SHA-384 a SHA-512.

Míra naléhavosti přechodu ke kvantově odolným digitálním podpisům ve většině případů
Na rozdíl od schválené symetrické kryptografie a od schválených hašovacích funkcí bude schválená asymetrická kryptografie po realizaci kryptoanalyticky relevantních kvantových počítačů zlomitelná. Proto musí k její výměně za kvantově odolnou kryptografii dojít dříve, než budou uvažované počítače zkonstruovány. To bude podle většiny odhadů zhruba na začátku třicátých let. Ve většině případů použití digitálního podpisu bude stačit, když krátce předtím budou kvantově falšovatelné podpisy znovu podepsány kvantově odolnými algoritmy.

b) Digitální podpisy sloužící k ochraně integrity firmwaru při jeho aktualizaci

Zvýšenou naléhavost své výměny za kvantově odolné algoritmy mají schválené digitální podpisy používané pro ochranu integrity při aktualizaci firmwaru. Důvodem je skutečnost, že některé paměti, ve kterých jsou uloženy veřejné klíče pro ochranu integrity při aktualizaci firmwaru, nemusí být později přepisovatelné.

K dispozici jsou standardy kvantově odolných digitálních podpisů LMS a XMSS, jejichž bezpečnost je konsensuálně akceptována jak odbornou veřejností, tak i bezpečnostními autoritami. Přechod k používání algoritmů LMS a XMSS k ochraně integrity firmwaru při jeho aktualizaci proto doporučujeme zahájit, co nejdříve to bude možné[38].

(5) Naléhavost přechodu ke kvantově odolné kryptografii v oblasti klasických algoritmů pro ustanovení klíčů

Kvantová zranitelnost schválených klasických algoritmů pro ustanovení klíčů
Žádný ze schválených klasických algoritmů pro ustanovení klíčů není kvantově odolný.

Naléhavost přechodu ke kvantově odolným algoritmům pro ustanovení klíčů
Jakmile budou kryptoanalyticky relevantní kvantové počítače realizovány, bude možné s nimi luštit veškerou dosud schválenou asymetrickou kryptografii. Pokud si útočník zachycenou kryptograficky chráněnou komunikaci ukládá, pak v době, kdy bude mít k dispozici vhodný kvantový počítač, ji bude moci vyluštit. Proto má přechod ke kvantové odolné kryptografii v oblasti ustanovení klíčů vysokou naléhavost zejména v případě ochrany dlouhodobě citlivých informací[39] kritické úrovně důvěrnosti[8] a měl by být realizován v nejbližších několika letech.

---

[38] Rychlý přechod k použití LMS nebo XMSS k ochraně integrity firmwaru a softwaru je především v ekonomickém zájmu provozovatele kryptografického systému. Jakmile se přiblíží realizace kryptoanalyticky relevantních kvantových počítačů, bude nutné uskutečnit tento přechod velmi rychle.

[39] Po věcné stránce můžeme rozdělit citlivé informace podle doby, po kterou je jejich citlivost zachována. Krátkodobá citlivost dat znamená, že je jisté, že doba jejich citlivosti nepřesáhne několik málo měsíců. Takové situace, kdy předem víme, že daná aplikace nebo zařízení bude pracovat pouze s krátkodobě citlivými informacemi, jsou však výjimečné, a navíc i těžko detekovatelné. Protože v praxi je často velmi obtížné

6 Výběr kvantově odolné kryptografie

(1) Kvantově odolná kryptografie pro ustanovení symetrických klíčů

Schválená klasická kryptografie pro ustanovení klíčů má vysokou naléhavost své náhrady za kvantově odolnou kryptografii. Pro případy kryptografické ochrany citlivých informací kritické úrovně důvěrnosti odhadujeme jako vhodný termín ukončení přechodu ke kvantově odolným ustanovením klíčů konec roku 2030[40].

a) Typy přechodu ke kvantově odolným ustanovením symetrických klíčů

Náhrada klasické asymetrické kryptografie symetrickou kryptografií

Symetrickou kryptografii s délkou klíčů 256 bitů považujeme za kvantově odolnou. Nicméně asymetrická kryptografie má oproti symetrické podstatné bezpečnostní a praktické výhody. Soukromé klíče není potřeba distribuovat a při distribuci veřejných klíčů stačí ochrana jejich integrity. Proto přechod ke kvantově odolné kryptografii na bázi symetrické kryptografie až na zdůvodněné výjimky nedoporučujeme.

Přechod k samostatnému použití algoritmu ML-KEM úrovně 5

V tomto případě bude nutné, aby algoritmus ML-KEM úrovně 5 byl implementován podle standardu NIST FIPS 203[66]. Tento algoritmus doporučujeme jako jeden z hlavních způsobů přechodu ke kvantově odolnému ustanovení klíčů.

Přechody k hybridním kombinacím

V hybridní kombinaci musí být k odvození[41] ustanovených symetrických klíčů použity alespoň dvě z následujících možností[7], str. 38:

- klasické asymetrické ustanovení klíčů (dohoda na klíči nebo asymetrické šifrování),
- postkvantové schéma KEM/Encryption,
- předdistribuované klíče[42].

Ve specifických případech lze navíc přidat i kvantovou distribuci klíčů.

---

hromadně rozlišovat mezi krátkodobě citlivými a střednědobě až dlouhodobě citlivými informacemi, doporučujeme, aby bylo se všemi kriticky citlivými informacemi zacházeno tak, jako by vyžadovaly nejméně střednědobou ochranu.

[40] Tento termín je stanoven v souladu se společným prohlášením většiny členských států EU ohledně přechodu k postkvantové kryptografii[12].

[41] Hlavním účelem hybridních řešení je zajištění (alespoň částečné) bezpečnosti i v situacích, kdy některá jeho složka bude zlomena. Na mechanismus odvození klíče tedy klademe požadavek, aby k zajištění bezpečnosti odvozeného klíče postačovala bezpečnost alespoň jednoho z ustanovených tajemství, z nichž je odvozen.

[42] Typickým reprezentantem předdistribuovaných klíčů jsou tzv. předsdílené klíče PSK, tj. *Pre-Shared Keys*.

(2) Kvantově odolné hybridní kombinace pro ustanovení symetrických klíčů

a) Využití předdistribuovaných klíčů

Typicky se bude jednat o situace, kdy výchozí kryptografický systém k ustanovení klíčů již používá schválenou klasickou asymetrickou kryptografii a předdistribuované klíče[43]. Ustanovený symetrický klíč hybridního řešení se pomocí KDF[44] odvodí jak z tajemství ustanoveného klasickou asymetrickou kryptografií, tak i z příslušného předsdíleného klíče. Využití klasické asymetrické kryptografie chrání proti klasickým útokům při kompromitaci některého předsdíleného klíče. Nikoliv ale proti útokům na bázi kvantových počítačů. Tudíž, aby tento způsob využití předsdílených klíčů vůbec měl smysl, je nutné, aby k jejich kompromitaci nedošlo nikdy během jejich životního cyklu[45]. Proto tato hybridní řešení kromě výjimečných dobře zdůvodněných případů nedoporučujeme, a pokud budou využita, budou schválena jen krátkodobě.

V případech hybridních kombinací zahrnujících využití postkvantové kryptografie a ochrany na bázi předsdílených klíčů (a případně i klasické asymetrické kryptografie) budeme považovat ochranu poskytovanou předsdílenými klíči pouze za doplňkovou. Hlavní garance kvantové odolnosti bude v těchto případech poskytovat využití postkvantové kryptografie.

b) Hybridní kombinace klasické asymetrické a postkvantové kryptografie pro ustanovení klíčů

Klasická asymetrická kryptografie pro hybridní ustanovení klíčů
Pro hybridní kombinaci s postkvantovou kryptografií lze použít libovolné schválené klasické algoritmy pro ustanovení klíčů.

Postkvantová kryptografie pro hybridní ustanovení klíčů
Pro hybridní kombinaci se schváleným algoritmem pro ustanovení klíčů lze použít libovolný z algoritmů uvedených v Tabulce 1: „Důvěryhodné postkvantové algoritmy typu KEM/Encryption“ v kapitole 3 odst. (6) písm. c) tohoto dokumentu.

Výše uvedené hybridní kombinace doporučujeme jako jeden z hlavních způsobů přechodu ke kvantově odolnému ustanovení klíčů.

---

[43] Typickým reprezentantem předdistribuovaných klíčů jsou například PSK (*Pre-Shared Keys*) k zajištění autentičnosti Diffieovy-Hellmanovy výměny.

[44] KDF (*Key Derivation Function*) je funkce pro odvozování klíčů.

[45] Ochrana proti kvantové hrozbě se v tomto případě přenáší na fyzickou ochranu důvěrnosti předdistribuovaných klíčů během jejich distribuce a na ochranu jejich důvěrnosti až do jejich smazání. Přiměřená ochrana jejich důvěrnosti může být poměrně nákladná.

c) Využití kvantové distribuce klíčů

Hlavní výhodou kvantové distribuce klíčů je její absolutní teoretická bezpečnost plynoucí ze zákonů kvantové mechaniky. Teoretická bezpečnost ale ani v tomto případě neznamená bezpečnost praktickou. Kvantová distribuce klíčů je stejně jako ostatní typy kryptografie zlomitelná útoky na bezpečnostní nedostatky v její implementaci.

K hlavním problémům kvantové distribuce klíčů patří její cena a zejména praktická omezení její využitelnosti. V některých případech, ve kterých nehrají její praktická omezení roli, ji lze využít, ale pouze jako doplňující ochranný mechanismus, typicky k postkvantové kryptografii, tedy pouze ve specifických hybridních řešeních.

(3) Praktické a bezpečnostní aspekty hlavních doporučených typů kvantově odolných ustanovení klíčů

Hlavní doporučené typy kvantově odolných ustanovení klíčů

- samostatné použití ML-KEM úrovně 5 implementovaného dle standardu NIST
- hybridní kombinace schválené klasické asymetrické kryptografie a postkvantové kryptografie dle 6 (2) b)

Samostatné použití ML-KEM úrovně 5 implementovaného dle standardu NIST FIPS 203[66]

Garance bezpečnosti tohoto řešení vychází ze skutečnosti, že ho americká NSA schválila pro NSS (*National Security Systems* – národní bezpečnostní systémy) s odůvodněním, že má vysokou důvěru v jeho dlouhodobou bezpečnost. To znamená, že toto řešení bude mít s vysokou pravděpodobností dlouhodobý charakter a nebude nutné ho v blízké budoucnosti měnit. Předpokládáme, že implementace ML-KEM úrovně 5 podle standardu NIST[66] budou dlouhodobě patřit mezi schválené kvantově odolné algoritmy.

Výhody a nevýhody uvažovaných hybridních řešení v porovnání s použitím samostatného algoritmu ML-KEM

Hybridní řešení budou pravděpodobně považována za přechodná v tom smyslu, že dříve nebo později budou nahrazena samostatnou postkvantovou kryptografií. Na druhou stranu nabízí obecně vyšší bezpečnostní garance vzhledem k menší zralosti postkvantových kryptosystémů, a tedy možnému dosud neznámému útoku na ně.

Hybridní řešení s McEliece nebo s FrodoKEM mohou mít vyšší teoretickou bezpečnost než samostatné použití ML-KEM stejné bezpečnostní úrovně. To platí pouze za podmínky, že tyto algoritmy budou implementovány podle akceptovaných standardů, což je v rozporu s ambicí je implementovat co nejdříve.

Classic McEliece má poměrně krátký šifrový text, velmi pomalé generování klíčů a mimořádně dlouhé veřejné klíče[41], sl. 14. Typicky se tedy bude používat k velkému počtu šifrování s týmž veřejným klíčem. V tom případě bude problematická jeho dopředná bezpečnost.

FrodoKEM má poměrně rychlé kryptografické operace, poměrně velké veřejné klíče a zhruba stejně velké šifrové texty[41], sl. 14. Bude možné jej použít v souladu s požadavkem dopředné bezpečnosti, ale v tom případě bude nutné ošetřit časté posílání dlouhých veřejných klíčů.

Hybridní kombinace ML-KEM úrovně 3 a ECDH může mít lepší praktické vlastnosti než samostatné použití ML-KEM úrovně 5. Bude mít ale nižší bezpečnostní garance ve vztahu ke kvantovým útokům.

(4) Kvantově odolná kryptografie pro digitální podpisy sloužící k ochraně autentičnosti firmwaru při jeho aktualizaci

LMS a XMSS, standardizované algoritmy digitálního podpisu na bázi hašovacích funkcí

Algoritmy LMS a XMSS doporučujeme implementovat pro ochranu integrity při aktualizaci softwaru a firmwaru dle standardů NIST, co nejdříve to bude možné.

(5) Kvantově odolná kryptografie pro digitální podpisy s obecným použitím

a) Kvantově odolné mechanismy digitálního podpisu s obecným použitím

Samostatný postkvantový algoritmus

- ML-DSA úrovně 5 v souladu se standardem NIST[67]
- SLH-DSA úrovně 3 a 5 v souladu se standardem NIST[68]

Hybridní kombinace – dvojitý digitální podpis

- hybridní kombinace klasického digitálního podpisu a postkvantového digitálního podpisu metodou dvojitého digitálního podpisu[46]

b) Doporučené složky hybridního (dvojitého) digitálního podpisu

Klasická asymetrická kryptografie

Pro hybridní kombinaci s postkvantovou kryptografií lze použít libovolné schválené klasické algoritmy pro mechanismus digitálního podpisu.

Postkvantová kryptografie

Pro hybridní kombinaci se schváleným klasickým algoritmem pro mechanismus digitálního podpisu lze použít jeden z následujících postkvantových algoritmů:

- ML-DSA úrovně 3 a 5
- SLH-DSA úrovně 3 a 5

K nim po své standardizaci pravděpodobně přibude FN-DSA úrovně 5.

---

[46] Dvojitý digitální podpis zprávy se provádí tak, že nejdříve se zpráva podepíše jednou metodou a poté se zřetězení zprávy a jejího prvního digitálního podpisu podepíše druhou metodou[43], str. 19.

c) Poznámky k praktickým a bezpečnostním aspektům

Hlavní doporučené typy kvantově odolných digitálních podpisů pro obecné použití

- Samostatné použití ML-DSA úrovně 5 implementovaného dle standardu NIST FIPS 204
- Hybridní kombinace schválené klasické asymetrické kryptografie a postkvantové kryptografie

Samostatné použití ML-DSA úrovně 5 implementovaného dle standardu NIST FIPS 204

Výhody tohoto řešení jsou obdobné jako v případě samostatného použití ML-KEM. S vysokou pravděpodobností bude mít dlouhodobý charakter, tudíž ho nebude nutné v blízké budoucnosti měnit. Lze očekávat, že bude patřit mezi dlouhodobě schválené kvantově odolné algoritmy.

Hybridní kombinace EC-DSA a Falcon-1024 (budoucí FN-DSA 1024)

Toto řešení může mít význam v případě, kdy způsob použití kvantově odolné kryptografie vyžaduje co nejkratší podpis.

Hybridní kombinace obsahující SLH-DSA úrovně 5

V případě, kdy vyžadujeme ještě vyšší bezpečnostní garance, než poskytuje ML-DSA úrovně 5, je možné místo něj jako postkvantovou složku hybridní kombinace použít SLH-DSA úrovně 5.

7 Začlenění postkvantové kryptografie do kryptografických protokolů

(1) Potřebnost vývoje nových variant kryptografických protokolů v návaznosti na implementace postkvantové kryptografie

Přechod k používání kvantově odolné kryptografie si vyžádá nejen implementaci postkvantových algoritmů, ale i přizpůsobení kryptografických protokolů jejich vlastnostem.[47]

Délky postkvantových veřejných klíčů

V některých případech kryptografických protokolů jsou omezeny délky veřejných klíčů a přechod k používání postkvantové kryptografie s typicky delšími veřejnými klíči zde může vést k problémům. Bude nutné implementovat mechanismy, které tento problém ošetří.

Náhrada Diffieovy-Hellmanovy výměny za KEM/Encryption

Diffieova-Hellmanova výměna je proces, u kterého nezáleží na tom, který z jeho účastníků je jeho iniciátorem a který mu odpovídá (respondent). KEM nebo asymetrické šifrování je proces, kdy jeho iniciátor generuje svůj veřejný klíč a posílá ho respondentovi. Ten vygeneruje symetrický klíč, zašifruje ho veřejným klíčem iniciátora a pošle mu ho. To znamená, že jejich role nejsou symetrické a v případě přechodu od Diffieovy-Hellmanovy výměny ke KEM je toto nutno zohlednit.

Hybridní kombinace postkvantové kryptografie s klasickým mechanismem

Pod klasickým mechanismem zde rozumíme buď klasickou asymetrickou kryptografii nebo specifické využití předsdílených klíčů k ochraně proti kvantové hrozbě. Uvažovaná hybridní kombinace nesmí mít nižší bezpečnost jak než samotné použití postkvantové kryptografie, tak než samotné použití příslušného klasického mechanismu.

Využití KEM v protokolech pro ustanovení klíčů místo digitálních podpisů

Délky postkvantových digitálních podpisů jsou značně velké, což může být v případě některých protokolů pro ustanovení klíčů zdrojem problémů. Proto probíhají práce na zajištění implicitní autentičnosti ustanovení klíčů pomocí statického KEM. Typickým příkladem je vývoj protokolu KEMTLS[45].

[47] Modifikace, vývoj a testování nových variant kryptografických protokolů patří do kompetence kryptologů a standardizačních subjektů ve spolupráci s komerčními firmami podnikajícími v dané oblasti.

(2) Přístupy k mechanismům kombinace složek hybridních řešení

a) Přístup na bázi KDF doporučený NIST[26], sl. 16 a BSI[7] pro ustanovení klíčů

Tento přístup předpokládá, že v původním protokolu pro ustanovení klíčů je implementovaná kryptograficky kvalitní KDF[48] s volitelnou délkou vstupu, do níž vstupovalo tajemství ustanovené na bázi klasické asymetrické kryptografie a jejímž výstupem byl odvozený ustanovený symetrický klíč.

Přechod k hybridnímu rozšíření o postkvantovou kryptografii v tomto případě znamená, že do KDF vstupuje zřetězení obou ustanovených tajemství, tedy jak tajemství ustanovené pomocí klasické kryptografie, tak i tajemství ustanovené pomocí postkvantové kryptografie[49].

BSI doporučuje následující zobecnění předchozího postupu. Jednak možnost obecnějšího použití KDF[7], str. 37 dle standardu NIST SP 800-56C[63], a dále možnost, aby vstupy do KDF zahrnovaly alespoň dvě z následujících tří tajemství:

a) tajemství ustanovené pomocí klasické asymetrické kryptografie,
b) tajemství ustanovené pomocí postkvantové kryptografie,
c) příslušný předsdílený klíč.

Ke zmíněné dvojici tajemství BSI přidává jako dobrovolnou možnost připojit rovněž tajemství ustanovené na bázi kvantové distribuce klíčů. Její využití ale nesnižuje požadavky na použití dvou ze tří výše uvedených tajemství[7], str. 38.

Poznamenejme, že NIST[26], sl. 16 specifikuje i způsob ustanovení obou uvažovaných tajemství, a to formou sériové kombinace klasického a postkvantového ustanovení tajemství.

b) Podstata dvojího KEM a dvojího podpisu doporučeného iniciativou ENISA

Tento přístup v případě dvojího KEM[43], str. 17, 18 předpokládá, že byly ustanoveny dva dílčí klíče: jeden na bázi klasické KEM a druhý na bázi postkvantové KEM. Výsledný kombinovaný (hybridní) klíč vznikne aplikací hašovací funkce na zřetězení obou použitých veřejných klíčů a obou ustanovených dílčích klíčů.

V případě dvojího podpisu[43], str. 19 daný vstup buď nejdříve podepíšeme klasickým podpisovým algoritmem a poté podepíšeme zřetězení vstupu a výsledku postkvantovým algoritmem, nebo můžeme postupovat analogicky, ale v opačném pořadí. Oba způsoby mají své výhody a nevýhody.

---

[48] KDF (*Key Derivation Function*) je funkce pro odvozování klíčů.

[49] BSI uvažuje i možnost obecnějšího použití KDF, nicméně v případech konkrétních protokolů se zabývá především možností zřetězení tajemství různého původu vstupujících do KDF.

(3) Kryptografická agilita

Během přechodu ke kvantově odolné kryptografii může docházet k potřebě opakovaných výměn kryptografických algoritmů. V případě použití hybridních kombinací je to zřejmé, ale nelze ani vyloučit potřebnost výměny kryptografie na základě nových nečekaných poznatků.

Proto je vhodné při nasazování nových kryptografických systémů dbát na to, aby byly kryptograficky agilní, tj. aby umožňovaly, aby případné výměny kryptografických algoritmů probíhaly pokud možno co nejsnadněji a nejhladčeji. K tomu je nutné zajistit jednak zpětnou kompatibilitu, tedy možnost, aby podporovaly více sad kryptografických algoritmů najednou, ale také jejich snadnou výměnu.

8 Shrnující doporučení

(1) Míry naléhavosti přechodu ke kvantově odolné kryptografii v jednotlivých oblastech

a) Vysoce prioritní oblasti

Algoritmy pro ustanovení klíčů pro ochranu citlivých informací kritické úrovně důvěrnosti

Přechod ke kvantově odolným hybridním kombinacím nebo k samostatným postkvantovým KEM/Encryption v této oblasti ochrany informací je vysoce naléhavý. Jako vhodný termín jeho ukončení odhadujeme konec roku 2030.

Digitální podpisy pro ochranu integrity firmwaru a softwaru při jejich aktualizacích

Přechod k postkvantovým algoritmům LMS nebo XMSS v této oblasti by měl začít, co nejdříve to bude možné. Algoritmy LMS a XMSS jsou již nyní mezi schválenými algoritmy.

b) Prioritní oblasti

Přechod ke kvantově odolné kryptografii v těchto oblastech ochrany informací bude potřebné dokončit před realizací kryptoanalyticky relevantních kvantových počítačů. Podle současných odhadů k ní dojde začátkem třicátých let.

Ostatní[50] digitální podpisy pro ochranu citlivých informací kritické úrovně integrity[8]

Přechod k samostatným postkvantovým podpisům nebo ke kvantově odolným hybridním digitálním podpisům. Všechny digitální podpisy právně relevantní v době realizace uvažovaných kvantových počítačů bude nutné podepsat kvantově odolným digitálním podpisem.

Algoritmy pro ustanovení klíčů pro ochranu důvěrnosti ostatních citlivých informací

Přechod k samostatné postkvantové kryptografii, případně k hybridní kvantově odolné kryptografii.

Symetrické šifrování s délkou klíče 128 nebo 192 bitů pro ochranu citlivých informací kritické úrovně důvěrnosti[51]

Symetrické šifrování s délkou klíče 128 nebo 192 bitů, ať již samostatné nebo jako součást autentizovaného šifrování, bude nutné nahradit šifrováním s délkou klíče 256 bitů.

---

[50] Pod pojmem „ostatní digitální podpisy“ zde rozumíme digitální podpisy, které nejsou určeny k ochraně integrity firmwaru a softwaru při jejich aktualizacích (viz kapitola 8 odst. (1) písm a)).

[51] Prodloužení délek klíčů schválené symetrické kryptografie na 256 bitů bude v porovnání s ostatními potřebnými kroky poměrně snadné. Proto je vhodné k němu přistoupit co nejdříve.

c) Ostatní oblasti přechodu ke kvantově odolné kryptografii

Vhodný termín dokončení přechodu ke kvantově odolné kryptografii v těchto oblastech odhadneme později.

Digitální podpisy s obecným použitím pro ochranu ostatních citlivých informací
Předpokládáme přechod k samostatné kvantově odolné kryptografii.

Symetrické šifry s délkou klíče 128 nebo 192 bitů pro ochranu ostatních citlivých informací
Symetrické šifry s délkou klíče 128 nebo 192 bitů bude vhodné nahradit šiframi s délkou klíče 256 bitů. Týká se jejich veškerého použití v symetrické kryptografii[52].

Hašování s délkou výstupu 256 bitů
Přechod k hašování s délkou výstupu 384 a více bitů[53].

(2) Doporučená kvantově odolná kryptografie

a) Doporučená samostatná postkvantová kryptografie

- LMS a XMSS pro digitální podpisy pro ochranu integrity firmwaru a softwaru
- ML-KEM-1024 pro ustanovení klíčů
- ML-DSA-87 pro digitální podpis s obecným použitím

b) Doporučená hybridní kvantově odolná kryptografie

Ustanovení klíčů
Doporučená hybridní kvantově odolná kryptografie pro ustanovení klíčů je popsána v kapitole 6 odst. (2) písm. b) „Hybridní kombinace klasické a postkvantové kryptografie pro ustanovení klíčů“. Podstata doporučených způsobů hybridní kombinace je popsána v kapitole 7 odst. (2) „Přístupy k mechanismům kombinace složek hybridních řešení“. K těmto řešením lze přistupovat jako ke schváleným kryptografickým algoritmům s předpokládanou zkrácenou dobou platnosti[54].

---

[52] Použití kvantových počítačů k luštění uvažovaných symetrických šifer bude podle současných znalostí mimořádně výpočetně nákladné. Proto očekáváme, že v případě ochrany „ostatních citlivých informací“ bude v této oblasti řada zdůvodněných výjimek.

[53] Zdůvodněné výjimky se mohou týkat i hašování citlivých informací. Důvodem jsou vysoké paměťové a výpočetní nároky doposud známých zdokonalení BHT-algoritmu.

[54] Předpoklad zkrácení doby platnosti souvisí s pozdějším přechodem k samostatné postkvantové kryptografii.

Digitální podpisy

Doporučená hybridní kryptografie pro digitální podpisy s obecným použitím je popsána v kapitole 6 odst. (5) „Kvantově odolná kryptografie pro digitální podpisy s obecným použitím“.

(3) Začlenění kvantově odolné kryptografie do vyšších celků

a) Kryptografická agilita

Při nasazování nových kryptografických systémů je vhodné dbát na to, aby byly kryptograficky agilní, tj. aby umožňovaly, aby případné výměny kryptografických algoritmů probíhaly pokud možno co nejsnadněji a nejhladčeji[55].

b) Začlenění do kryptografických protokolů

Začlenění kvantově odolné kryptografie do informačních a komunikačních systémů si vzhledem k některým jejím vlastnostem vyžádá řadu modifikací a přizpůsobení kryptografických protokolů[56].

[55] Více v kapitole 7 odst. (3) tohoto dokumentu.

[56] Více v kapitole 7 odst. (1) tohoto dokumentu.

9 Odkazy

[1] P. W. Shor: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, IEEE, 1994, Algorithms for quantum computation: discrete logarithms and factoring – Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on

[2] P. W. Shor: Polynomial Time Algorithms for Prime Factorizations and Discrete Logarithms on a Quantum Computer, arXiv:quant-ph/9508027v2 25 Jan 1996

[3] J. Proos, Chr. Zalka: Shor's discrete logarithm quantum algorithm for elliptic curves, arXiv preprint quant-ph/0301141 (2003). [quant-ph/0301141] Shor's discrete logarithm quantum algorithm for elliptic curves (arxiv.org)

[4] L. K. Grover: A Fast Quantum mechanical Algorithm for Database Search, [quant-ph/9605043] A fast quantum mechanical algorithm for database search (arxiv.org)

[5] Brassard, Høyer, Tapp: Quantum Algorithm for the Collision Problem, [quant-ph/9705002] Quantum Algorithm for the Collision Problem (arxiv.org)

[6] M. Mosca: The Latest View on Quantum Computing and its Impact on Critical Digital Infrastructures, PowerPoint Presentation (securetechalliance.org)

[7] BSI: Quantum-safe cryptography – fundamentals, current developments and recommendations, Quantum-safe cryptography – fundamentals, current developments and recommendations (bund.de)

[8] N. Koblitz: QUANTUM COMPUTING: REALITY OR HYPE? TiaSangQC.pdf (washington.edu)

[9] G. Kalai: The Argument against Quantum Computers, the Quantum Laws of Nature, and Google's Supremacy Claims, Laws, Rigidity and Dynamics, Proceedings of the ICA workshops 2018 & 2019 Singapore and Birmingham, [2008.05188] The Argument against Quantum Computers, the Quantum Laws of Nature, and Google's Supremacy Claims (arxiv.org)

[10] M.I. Dyakonov: When will we have a quantum computer? 1903.10760.pdf (arxiv.org)

[11] M.I. Dyakonov: Will we ever have a quantum computer? Will We Ever Have a Quantum Computer? | SpringerLink

[12] Securing Tomorrow, Today: Transitioning to Post-Quantum Cryprography, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3

[13] W. Castryck, T. Decru: An efficient key recovery attack on SIDH, An efficient key recovery attack on SIDH (iacr.org)

[14] Multivariate Public Key Cryptography and its Cryptanalysis, Quantum Cryptanalysis, Simons Institute, 02.2020, mpkc-hhl-1.pdf (berkeley.edu)

[15] W. Beullens: Breaking Rainbow Takes a Weekend on a Laptop: 214.pdf (iacr.org)

[16] D. A. Cooper, D. C. Apon Q. H. Dang, M. S. Davidson, M. J. Dworkin, C. A. Miller: NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes, Recommendation for Stateful Hash-Based Signature Schemes (nist.gov)

[17] L. Chen: NIST Post-Quantum Cryptography Standardization, AWACS 2016, Microsoft PowerPoint – AWACS-PQC-2016-05082016 (cryptoexperts.com)

[18] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, call-for-proposals-final-dec-2016.pdf (nist.gov)

[19] S. Jaques, M. Naehrig, M. Roetteler, F. Virdia: Implementing Grover Oracles for Quantum Key Search on AES and LowMC, 1910.01700.pdf (arxiv.org)

[20] P. Kim, D. Han, K. Chul Jeong: Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2, [1805.05534] Time-Space Complexity of Quantum Search Algorithms in Symmetric Cryptanalysis (arxiv.org)

[21] A. Chailloux, M. Naya-Plasencia, A., Schrottenloher: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: ASIACRYPT 2017. pp. 211–240 (2017], and in: 847.pdf (iacr.org)

[22] M. N.Plasencia, A. Schrottenloher, A. Chailloux, L. Grassi: New Algorithms for Quantum (Symmetric) Cryptanalysis, New Algorithms for Quantum (Symmetric) Cryptanalysis (malb.io)

[23] Physical and Logical Qubits, WikipediA, The Free Encyclopedia, Physical and logical qubits - Wikipedia

[24] A. G. Fowler, M. Mariantoni, J. M. Martinis, A. N. Cleland: "Surface codes: Towards practical large-scale quantum computation". Physical Review A. 86 (3) 032324, [1208.0928] Surface codes: Towards practical large-scale quantum computation (arxiv.org)

[25] N. N. Hegade, P. Koushik , F. Albarrán-Arriagada, Xi Chen, E. Solano: Digitized Adiabatic Quantum Factorization, 2105.09480.pdf (arxiv.org)

[26] D. Moody: NIST PQC: LOOKING IN THE FUTURE, Selected presentations of the Fourth PQC Standardization Conference, NIST PQC: LOOKING INTO THE FUTURE

[27] NIST: Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process, Call for Additional Digital Signature Schemes for the PQC Standardization Process (nist.gov)

[28] Overview of NIST Round 3 Post-Quantum cryptography Candidates, Round-3.pdf (pqsecurity.com)

[29] BSI TR-02102-1, BSI-Technical Guideline, Designation: Cryptographic Mechanisms and Key Length, Version: 2024-01, Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2024-01 (bund.de)

[30] M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, Ed. Persichetti, Chr. Peters, P. Schwabe, N. Sendrier, J. Szefer, M. Tomlinson, W. Wang: Classic McEliece: conservative code-based cryptography: Classic McEliece Round 3 Update (nist.gov)

[31] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, Chr. Peikert, An. Raghunathan, D. Stebila: FrodoKEM, A simple and conservative KEM from generic lattices, FrodoKEM Practical post-quantum key exchange from the Learning with Errors Problem (nist.gov)

[32] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, Chr. Peikert, An. Raghunathan, D. Stebila: FrodoKEM practical quantum-secure key encapsulation from generic lattices. =1=FrodoKEM practical quantum-secure key encapsulation from generic lattices (nist.gov)

[33] T. Lange: KEM-DEM Framework 2WF80, Introduction to Cryptology, KEM-DEM framework (hyperelliptic.org)

[34] P. Campbell, M. Groves, D. Shepherd: SOLILOQUY: A Cautionary Tale, S07_Groves_Annex.pdf (etsi.org)

[35] M. Bellare, H. Davis, F. Güther: Separate Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability, Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability (iacr.org)

[36] National Security Agency | Cybersecurity Information Sheet, Announcing the Commercial National Security Algorithm Suite 2.0, CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov)

[37] National Security Agency | Cybersecurity Information Sheet, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, CSI_CNSA_2.0_FAQ_.PDF (defense.gov)

[38] National Security Agency | Frequently Asked Questions, Quantum Computing and Post-Quantum Cryptography, Quantum_FAQs_20210804.PDF (defense.gov)

[39] CANADIAN CENTRE FOR CYBERSECURITY: How the Canadian goverment is Preparing for PQC, PKI Comsortium, Post-Quantum Cryptography Conference, March 2023, PowerPoint Presentation (pkic.org)

[40] GSMA: Post Quantum Telco Network Impact Assessment Whitepaper, Version 1.0, 17 February 2023, PQTN_1_Doc_006 PQTN White Paper CLEAN (gsma.com)

[41] D. Bong: A bouquet of crypto flowers, The Impacts of Post Quantum Cryptography (post-quantum.nl)

[42] D. Bernstein, T. Lange: Post-Quantum Cryptography: Detours, delays, and disasters, slides-dan+tanja-20220820-pqcrypto-16x9.pdf

[43] ENISA: POST-QUANTUM CRYPTOGRAPHY, Integration study. Post-Quantum Cryptography - Integration study — ENISA (europa.eu)

[44] T. Lange: Post-quantum cryptography, 2022, Post-quantum cryptography (hyperelliptic.org)

[45] D. Stebila: Recent Results in KEMTLS, 20220512-TII.pdf

[47] D. Moody: Let's Get Ready to Rumble-The NIST PQC "Competition": Let's Get Ready to Rumble- The NIST PQC "Competition"

[48] D. Moody: What was NIST thinking? Round 2 of the NIST PQC "Competition", Round 2 of the NIST PQC "Competition" - What was NIST Thinking?

[49] L. Chen: An Overview of NIST PQC Standardization, Microsoft PowerPoint - CHEN_NIST.pptx (etsi.org)

[50] NIST IR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8413, PQC Project Third Round Report | CSRC

[51] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, Gr. Seiler, D. Stehle: CRYSTALS (Cryptographic Suite for Algebraic Lattices) CCA KEM: Kyber Digital Signature: Dilithium, CRYSTALS-Dilithium (nist.gov)

[52] National Security Agency | Central Security Service, Quantum Key Distributions and Quantum Cryptography, Quantum Key Distribution (QKD) and Quantum Cryptography QC (nsa.gov)

[53] ANSII: 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)

[54] National Cyber Security Centre: Whitepaper, Quantum security technologies, Quantum security technologies - NCSC.GOV.UK

[55] National Cyber Security Centre: Whitepaper, Quantum-safe cryptography, Quantum-safe cryptography - NCSC.GOV.UK

[56] ANSSI views on the Post-Quantum Cryptography transition March 25, 2022, anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

[57] B. A. Macchia: The Long Road Ahead to Transiton to Post-Quantum Cryptography, MS Ressearch of Security & cryptography, 19-October 2022, IEEE SecDev 2022, PowerPoint Presentation (ieee.org)

[58] D. J. Bernstein, Ch. Dobraunig, M. Eichlseder, S. Fluhrer, S. L. Gazdag, A. Hülsing, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, Ch. Rechberger, J. Rijneveld, P. Schwabe: SPHINCS+, SPHINCS+ (nist.gov)

[59] T. Lange: Introduction to post-quantum cryptography, 22 June 2017, Executive School on Post-Quantum Cryptography, Introduction to post-quantum cryptography (pqcrypto.org)

[60] Kyber Home, CRYSTALS, Cryptographic Suite for Algebraic Lattices, Kyber (pq-crystals.org)

[61] Dilithium Home, CRYSTALS, Cryptographic Suite for Algebraic Lattices, Dilithium (pq-crystals.org)

[62] GSM Association Non-Confidential Official Document PQ.01, Post Quantum Telco Network Impact Assessment Whitepaper, Post Quantum Telco Network Impact Assessment Whitepaper, Version 1.0, 17 February 2023, PQTN_1_Doc_006 PQTN White Paper CLEAN (uk5g.org)

[63] E. Barker, L. Chen, R. Davis: NIST Special Publication 800-56C, Revision 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, August 2020, Recommendation for Key-Derivation Methods in Key-Establishment Schemes (nist.gov)

[64] D. A. Cooper, D. C. Apon, Q. H. Dang, M. S. Davidson, M. J. Dworkin, C. A. Mille: NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes, October 2020, Recommendation for Stateful Hash-Based Signature Schemes (nist.gov)

[65] E. R. Anschuetz, J. P. Olson, A. Aspuru-Guzik, Y. Cao: Variational Quantum Factoring, [1808.08927] Variational Quantum Factoring (arxiv.org)

[66] National Institute of Standards and Technology (2024) Module-Lattice-based Key Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[67] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[68] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf https://doi.org/10.6028/NIST.FIPS.205.ipd

[69] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces; Position Paper on Quantum Key Distribution https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
1. 6. 2023	1.0	Odbor bezpečnosti informačních a komunikačních technologií, NÚKIB	Vytvoření dokumentu
5. 2. 2025	2.0	Národní úřad pro kybernetickou a informační bezpečnost	Aktualizace dokumentu, postkvantové standardy NIST, algoritmy BIKE a HQC, úprava časových odhadů dle společného prohlášení států EU[12]