**Úvod do postkvantové kryptografie**

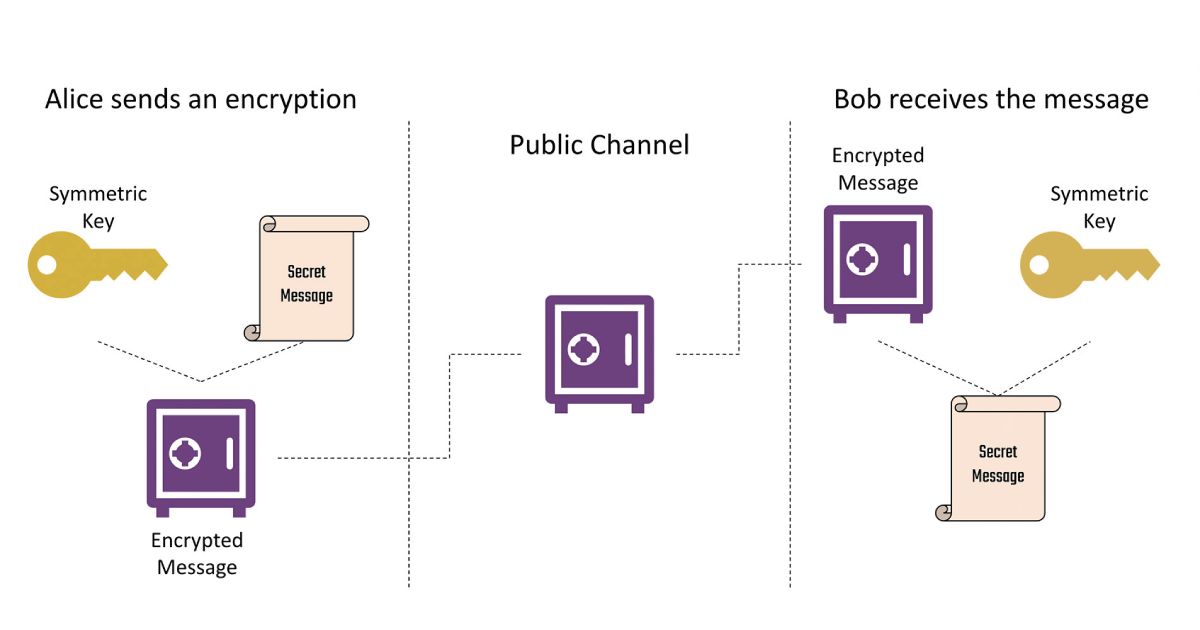
Pohled na kryptografii v budoucím postkvantovém bezpečnostním prostředí IoT

Je to vzrušující čas pracovat na kvantových technologiích; konečně, kvantové počítače jsou téměř tady. Jeho zastánci již nějakou dobu s jistotou tvrdili, že první komerčně dostupné kvantové počítače budou vyrobeny během příštích dvaceti let, ale úspěchy, jako jsou úspěchy týmů IBM, DWave a naposledy Google, naznačují, že tentokrát tato víra může být připisován více než jen optimismu a prodejním názorům. Ačkoli je příliš brzy na pochopení důsledků zařízení skutečně schopného využívat kvantové efekty, je nepochybné, že uvidíme pokroky v oblastech, kde lze správně využít sílu kvantového počítače k ​​pochopení vzorců ve velkých svazcích dat, jako je např. jako datová věda.

Bohužel ne každý může sledovat příchod kvantových počítačů jen s nadšením. Kryptografové, praktici zodpovědní za ochranu dat a soukromí lidí na internetu i mimo něj, se připravují na to, že desítky let dobře vyladěných technik skrývání dat budou zrušeny první vlnou sofistikovaných kvantových strojů. Naštěstí je zde rozhodující slovo příprava. Algoritmus vyvinutý Peterem Shorem v polovině 90. let ukázal, že kvantové počítače budou schopny vyřešit slavný problém „faktorizace celého čísla“, bezpečnostní páteř slavného kryptosystému RSA, dramaticky rychleji, než to dokážou naše moderní počítače. Ještě horší je, že hlavní stavební blok Shorova algoritmu, kvantová Fourierova transformace, lze upravit tak, aby prolomila většinu ostatních běžně implementovaných kryptografií, jako je výměna klíčů Diffie-Helman a digitální podpisy elliptické křivky. Otázka tedy zní: co dělali kryptografové za posledních dvacet let, aby se na tuto eventualitu připravili? Stručně řečeno, vyvinuli předmět Post-Quantum Cryptography (PQC), studium kryptografie, kterou lze provozovat na klasických počítačích a přitom si zachovat odolnost vůči kvantovým útokům.​

**Kryptografie 101**

Než se dostaneme k postkvantové kryptografii, měli bychom nejprve porozumět některým základům kryptografie a tomu, co pro kvantový počítač znamená, že ji rozbije. Tradičně se kryptografové snažili vyřešit varianty následujícího problému: Alice chce poslat zprávu – „Schoval jsem poklad v knihovně“ – svému příteli Bobovi, ale nemá žádný soukromý kanál, přes který by tuto zprávu poslala. Navíc se obává, že by se Eva mohla pokusit zachytit její tajnou zprávu a ukrást poklad. Co tedy Alice umí? Tady přichází na scénu šifrování. Řekněme, že když byli Alice a Bob spolu naposledy, věděli, že by si mohli chtít posílat zprávy poté, co Alice ukryla poklad. Dohodli se tedy na klíči, jak to udělat tajně. Nyní, když chce Alice poslat zprávu Bobovi, použije tento klíč k zašifrování své zprávy (představte si, že zprávu vloží do zamčené schránky), a jakmile dorazí s Bobem, on pouze dešifruje pomocí stejného klíče (odemknutí krabice). Pokud se Evě podaří zachytit jejich komunikaci, nebude schopna odemknout schránku, protože nemá klíč. Protože Alice a Bob sdílejí stejný klíč, ten, na kterém se shodli dříve, nazýváme to symetrická kryptografie.

*Symetrická kryptografie v akci*

Matematicky šifrování zprávy představuje použití klíče ke zkomolení Aliciny zprávy do řetězce nesmyslů – „vrbayebcjaelaiyurbjeaby!“ – to lze rozbalit do Aliciny zprávy pouze pomocí jejího a Bobova klíče. Evě, která zprávu úspěšně zachytila, ale postrádala klíč, zjistí, že nedokáže pochopit, co Alice poslala .

S tímto nastavením je samozřejmě zřejmý problém. Co když Alice a Bob potřebují vést tajný rozhovor, aniž by se mohli sejít a předem se dohodnout na klíči? Zde se setkáváme s více zapojenými technikami kryptografie s veřejným klíčem. Pro nastavení výměny si Bob vytvoří pár klíčů: veřejný klíč a soukromý klíč. Veřejný klíč, který posílá do světa, a lze si ho představit jako šifrovací klíč pro posílání zpráv Bobovi. Když chce Alice poslat zprávu Bobovi, vyhledá jeho veřejný klíč a použije jej k zašifrování své zprávy. Vzhledem k tomu, že Eve má přístup pouze k veřejnému šifrovacímu klíči, pokud se jí podaří zachytit Alicinu zprávu, stejně uvidí jen nesmysly. Jakmile Bob zprávu přijme, nyní použije svůj soukromý klíč, v podstatě dešifrovací klíč, k rozbalení a přečtení Aliciny komunikace .

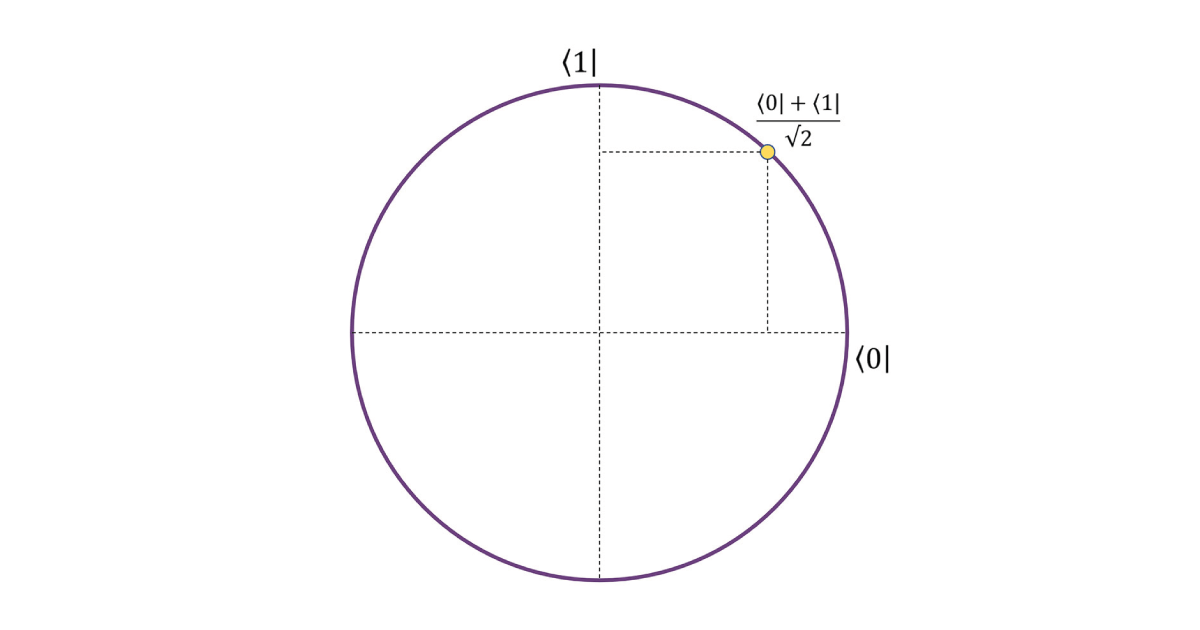
V praxi je nepravděpodobné, že by se strany dokázaly dohodnout na klíči předem – zamyslete se nad tím, jak často musíte zadávat své bankovní údaje, abyste mohli nakupovat na webové stránce, kterou jste nikdy předtím nenavštívili. V důsledku toho jsou bezpečné techniky pro kryptografii veřejného klíče pro bezpečnost internetu nanejvýš důležité. Bohužel se ukazuje, že vytváření schémat s veřejnými klíči je docela obtížné a obvykle to skončí velmi pomalu, když chcete poslat spoustu informací. Naštěstí to jde snadno opravit. Alice a Bob začínají pomocí schématu veřejného klíče nebo podobné techniky známé jako protokol výměny klíčů, aby tajně sdělili jednu malou zprávu, která je pouze sdíleným klíčem. Poté použijí tento sdílený klíč s dobře zavedeným symetrickým schématem, typicky schématem nazývaným  [AES](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) , aby pokračovali ve své tajné komunikaci bez režie, kterou vyžadují techniky veřejného klíče. Takto běžné internetové standardy, jako je  [TLS,](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://en.wikipedia.org/wiki/Transport_Layer_Security)  navrhují, aby byla v praxi zabezpečena komunikace.

Robustní symetrická kryptografie ve formě AES existuje již od 90. let a při správné implementaci je považována za extrémně bezpečnou. Potenciální slabé místo v tomto nastavení tedy spočívá ve fázi veřejného klíče. Jak bezpečné je schéma veřejného klíče? Je známé, že bezpečnost kryptografie s veřejným klíčem, obtížnost prolomení schématu, je možné založit na výpočetních matematických problémech. Nejznámějším příkladem je samozřejmě schéma RSA. V RSA je Bobův veřejný klíč nějaké velké celé číslo n a jeho tajný klíč je nějaká další informace o n, konkrétně to, že jej lze faktorizovat jako součin dvou prvočísel p a q, takže pq = n. Aby poslala zprávu Bobovi, může ji Alice zašifrovat pomocí n takovým způsobem, že k dešifrování zprávy potřebujeme p a q. Pro Boba je to snadné, protože tato prvočísla zná, ale zachycující Eva je musí být schopna získat zpět faktorizací veřejného klíče n. Úkolem Evy je tedy právě problém „rozkladu celého čísla“ řešený Shorovým algoritmem, který nelze na dnešních počítačích efektivně vyřešit za předpokladu, že p a q jsou dostatečně velké. Jiné běžné techniky výměny veřejných klíčů a klíčů odvozují svou bezpečnost z různých těžkých matematických problémů, například problém diskrétního logaritmu, ve stejném smyslu – schéma se ukázalo být stejně těžké prolomit, jako je těžké problém vyřešit .

Jedna věc, které jsme se ještě nedotkli, je problém autentizace: když Bob obdrží zprávu od Alice, jak si může být jistý, že ji skutečně poslala Alice a že to bylo skutečně to, co Alice chtěla říct? Koneckonců, když je Eva schopná zachytit zprávy, mohla by být také schopná s nimi manipulovat, než se dostanou k Bobovi? Zejména v době internetové komunikace může být těžké věřit, že každá zpráva přišla od toho, od koho se vydává. Abychom to vyřešili, spoléháme na příhodně pojmenované téma digitálních podpisů, které fungují podobně jako jejich skutečný světový jmenovec. Alice používá soukromý klíč, svou moc podepisovat zprávy, k připojení podpisu ke zprávě Bobovi, který říká Bobovi, že to byla Alice, kdo poslal tuto zprávu. Podpis navíc shrnuje zamýšlený obsah takovým způsobem, že pokud je s obsahem manipulováno, podpis by se jevil jako nesprávný. Po obdržení této zprávy se Bob může podívat na Alicin odpovídající veřejný klíč, který mu říká, jak vypadá podpis Alice, aby si ověřil, že Eva nezasáhla do zamýšlené zprávy a že pochází od Alice. Podobně jako u šifrování i zde kryptografické techniky spoléhají na komplikovanou matematiku, kde obtížnost padělání Alicina podpisu odpovídá náročnosti řešení výpočetního problému. Například k padělání podpisu v běžně používaném podpisovém schématu známém jako ECDSA musí být Eva schopna vyřešit problém diskrétního logaritmu na něčem známém jako eliptická křivka .

**Kvantové počítání a těžké problémy**

Přestože úplné vysvětlení mechanismů kvantového počítače by samo o sobě zaplnilo blogový příspěvek, stručné shrnutí nám pomůže pochopit myšlenky, které stojí za vytvořením kvantově odolné kryptografie. Pamatujte, že pro vytvoření postkvantových schémat veřejného klíče hledáme matematické problémy, které ani kvantový počítač nedokáže rozluštit. Kvantové počítače jsou hodně podobné klasickým počítačům, až na to, že nahrazují hradla na klasických bitech, objektu, který je buď ve stavu 0 nebo 1, operacemi na kvantové variantě zvané qubit. Qubit představuje bod na jednotkové kružnici, kružnici o poloměru 1 a kvantová brána představuje mapování z bodu na jednotkové kružnici do jiného. Záludné je, že když se pokusíte přečíst qubit, neřekne vám, kde leží na jednotkovém kruhu. Místo toho se náhodně zhroutí do stavu 0 nebo 1, s pravděpodobností 0 nebo 1 v závislosti na jeho poloze na kruhu.

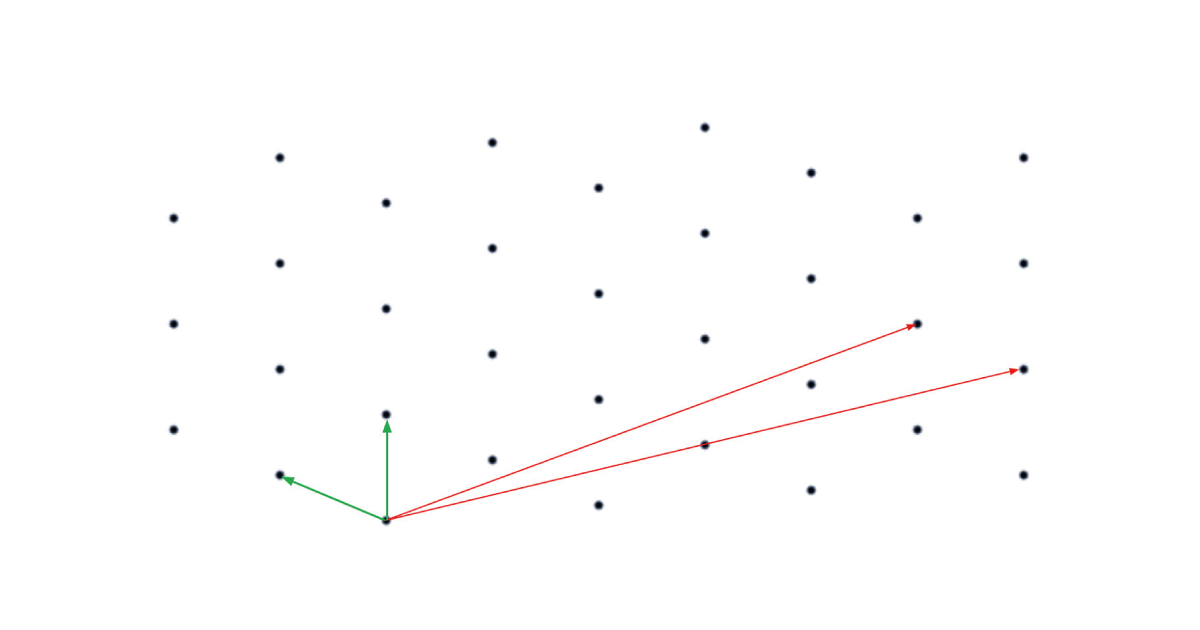
*Qubit na jednotkovém kruhu*

Díky své komplikovanější povaze jsou qubity schopny reprezentovat a uchovávat mnohem více informací než běžný bit. To neznamená, že jsou lepší ve všech úkolech a výzkumníci začínají chápat, pro jaké úkoly jsou vhodnější. Jako užitečný kus intuice si lze představit kvantový počítač, který dokáže velmi levně „paralelizovat“ úkoly. To znamená, že pokud lze úkol rozdělit na několik menších dílčích úkolů, které lze provést současně, pak je kvantové zařízení zběhlé v provádění každého z těchto menších úkolů najednou. Oproti klasickému zařízení, které musí provádět každý úkol sekvenčně, si kvantový počítač ušetří spoustu času. Vezměme si například prvočíselný faktoring: kvantový počítač by mohl pouze rozdělit možné faktory do skupin a pak paralelně kontrolovat, zda se některá čísla v každé skupině dělí , spíše než muset začínat od 1 a kontrolovat každé číslo postupně. Porovnejte to s úkoly, které vyžadují neustálou aktualizaci stejného objektu – to jsou úkoly, kde kvantové počítače nemusí fungovat o mnoho lépe než klasické počítače. Ve skutečnosti se bezpečnost běžných symetrických schémat, jako je AES, spoléhá na „smíšení“ objektů dohromady, takže k prolomení šifrování zprávy musíte ručně provést řadu kroků rozpojení. Tato myšlenka vysvětluje, proč se PQC zaměřuje především na aktualizaci kryptografie s veřejným klíčem – kvantové počítače nejsou dramaticky lepší v odstraňování symetrického šifrování než klasické počítače, takže většině symetrických konstrukcí stačí jen mírně změnit jejich parametry, aby byly stále považovány za bezpečné.

**Kvantově těžké problémy**

Vyzbrojeni těmito znalostmi o tom, co ztěžuje problém kvantovému počítači, se můžeme rychle podívat na hlavní kandidáty na výpočetní problémy v PQC. Existuje nějaký výzkum v modré obloze, ale většina navrhovaných schémat PQC leží v jedné ze čtyř hlavních kategorií: mřížková, kódově založená, multivariační a izogenní kryptografie.

Na prvním místě je nejoblíbenější kategorie, mřížková kryptografie. Mřížku lze chápat jako pravidelnou mřížku bodů v prostoru, kde body na mřížce jsou vybírány systematicky z objektu zvaného její základna, který popisuje mřížku tím, že vysvětluje, jak se pohybujete mezi mřížkovými body.

*Mříž se dvěma různými základnami*

Mříže jsou klasické matematické objekty a výpočetně náročné problémy na nich byly studovány již dávno předtím, než existoval kryptosystém RSA, což dává jistou důvěru představě, že tyto problémy by měly zůstat těžké i tváří v tvář kvantovým útokům. Archetypální problém tvrdé mřížky je nejkratší vektorový problém: po obdržení základu pro mřížku je řešitel požádán, aby našel bod mřížky nejblíže k počátku. Ačkoli je to snadné pro malé mřížky, jako je ta znázorněná výše, když je mříž objektem ve stovkách rozměrů, tento problém se stává velmi náročným. Páteř budování kryptografie z problémů s mřížkou pochází ze zajímavého pozorování o definování mřížky ze základu. Základ použitý ke konstrukci mřížky není jedinečný a je možné mít „dobrý“ a „špatný“ základ stejné mřížky. Například ve výše uvedeném diagramu lze všech bodů mřížky dosáhnout tak, že začneme na 0 a pak půjdeme po kombinacích buď červených nebo zelených čar, nazývaných vektory. Pokud máte zelený základ, je snadné rychle porozumět tvaru mřížky, protože vaše vektory jsou krátké a navzájem téměř 90 stupňů. Jakmile dobře porozumíte mřížce, můžete jen odečíst nejkratší vektor. A naopak, pomocí červených čar musíte hodně kroutit, abyste našli body blízké 0, a i když už nějaký najdete, jak byste ověřili, že tam není nic kratšího? Kryptosystémy založené na mřížkách využívají tuto myšlenku k budování kryptografie – na vysoké úrovni je myšlenkou použít špatný základ pro mřížku jako veřejný klíč a dobrý základ pro stejnou mřížku jako soukromý klíč. Špatný základ popisuje mřížku dostatečně dobře, aby skryl zprávu jako těžký problém na mřížce. Pak může tento problém snadno vyřešit pouze zamýšlený příjemce, protože to vyžaduje přístup k dobrému základu. Mřížková kryptografie má tendenci být nejflexibilnější kategorií PQC, protože existuje mnoho prostoru pro návrh, se kterým lze pracovat, pokud jde o to, jak si vybrat mřížky a skrýt body. Tato flexibilita vedla k úspěšné aplikaci mřížek na problémy šifrování i digitálních podpisů .

Kryptografie založená na kódu je nejstarší ze čtyř hlavních rodin, datuje se od vývoje kryptosystému  [McEliece](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://en.wikipedia.org/wiki/McEliece_cryptosystem)  v roce 1978. Je založena na oblasti teorie kódování, která je studiem toho, jak úspěšně přenášet informace přes nespolehlivý kanál. K odesílání informací tímto způsobem používáte něco, čemu se říká kód pro opravu chyb, kde je zpráva zakódována způsobem, který toleruje určité množství chybných dat pocházejících z nespolehlivého kanálu, přičemž příjemce je stále schopen obnovit zamýšlenou zprávu. . Soukromý klíč pro kryptosystém založený na tomto je jen dobře zvolený kód pro opravu chyb a odpovídající veřejný klíč je recept na zakódování zprávy, která má být dekódována. Šifrování je jednoduché – odesílatel provede obvyklý proces kódování zprávy a poté simuluje nespolehlivý kanál ručním zadáním některých chyb. Dokud existuje dostatek chyb, protivník bez přístupu k popisu kódu pro opravu chyb nemůže zprávu obnovit, zatímco zamýšlený příjemce je schopen ji dekódovat pomocí svého kódu pro opravu chyb. Pěkné na těchto schématech je, že McEliece existuje již dlouhou dobu, a proto existuje velká míra důvěry v jejich bezpečnost a schémata jemu podobná. Na druhou stranu, McEliece existuje už dlouho a nikdo ho nepoužívá – má velmi velké veřejné klíče, což může trochu zpomalit, a obecně se špatně srovnává s RSA v předkvantové éře .

Vícerozměrná kryptografie je založena na problému řešení systémů mnohorozměrných polynomiálních rovnic, typicky vícerozměrných kvadratických. Tedy soustava rovnic, která vypadá takto:

Ačkoli mnoho existujících forem kryptografie eliptických křivek, jako je ECDSA, je citlivých na kvantové počítače, je to důsledek specifické povahy algoritmů a nikoli slabina samotných eliptických křivek. Abychom kryptografii založili na izogeniích, použijeme následující pozorování: vzhledem ke dvěma eliptickým křivkám E1 a E2 je těžké najít izogenii φ, která posílá E1 na E2. Veřejný klíč by tedy mohl být pár eliptických křivek, se soukromým klíčem odpovídající izogeneze φ: E1 -> E2. Nyní může vlastník soukromého klíče použít izogenii φ k výpočtu operací zahrnujících E1 a E2, které jsou neovladatelné pro někoho, kdo nemá přístup k φ, a jako obvykle lze k nastavení těchto problémů použít veřejný pár E1 a E2. Přestože je oblast kryptografie na bázi izogeny stále v relativních plenkách, v kryptografické komunitě je o ní značné vzrušení, zejména po  [úspěšných experimentech](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://www.imperialviolet.org/2019/10/30/pqsivssl.html)  s využitím schémat založených na izogenii v internetových protokolech. Navíc působivě efektivní schéma podpisů nazvané SQISign, založené na novém problému v kryptografii založené na izogenii, získalo na letošní konferenci Asiacrypt cenu za nejlepší knihu .

**Směrem ke standardizaci: Proces NIST**

Vzhledem ke všem těmto konkurenčním nápadům může být těžké pochopit, kde leží budoucnost kryptografie. Jedním z míst, kde se můžete obrátit s žádostí o radu, je proces postkvantové standardizace, který provozuje Národní institut pro standardy a technologie (NIST) ve Spojených státech. NIST již dříve spouštěl procesy pro standardizaci symetrické kryptografie a hašovacích funkcí, což vedlo k široce používaným primitivům AES a SHA3. Ačkoli se nejedná o oficiální globální standard, je pravděpodobné, že jakýkoli algoritmus podporovaný NIST bude mít úrovně absorpce podobné těm u AES a SHA3, takže zkoumání tohoto procesu by mělo poskytnout nejmodernější pochopení pravděpodobné budoucnosti PQC. . NIST se snaží objasnit, že by to mělo být považováno za proces a ne za soutěž s „vítězem“, takže se mohou rozhodnout standardizovat nebo navrhnout více algoritmů pro různé případy použití, pokud neexistuje jasná nejlepší technika. Dvě hlavní vlastnosti, které NIST hledá, jsou bezpečnost a efektivita: pokud protokol není bezpečný, nemá smysl jej používat k ochraně dat, a pokud není efektivní, zpomaluje internetovou komunikaci. Obecně má PQC tendenci pracovat pomaleji než jeho předkvantový protějšek, takže algoritmus lze považovat za účinný, pokud nedojde k žádnému nebo malému poklesu výkonu při jeho použití namísto stávajícího předkvantového schématu .

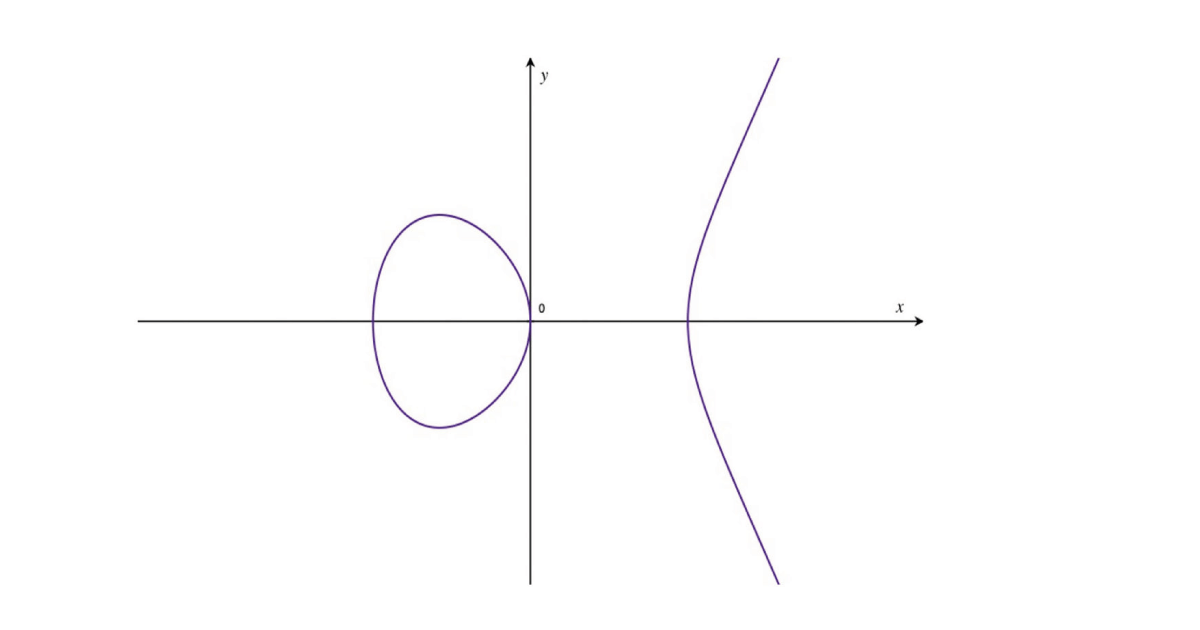
Proces byl zahájen NIST v roce 2016 ve formě otevřené výzvy kryptografické komunitě, která žádala o návrhy mechanismů postkvantového zapouzdření klíčů (v podstatě asymetrická šifrovací schémata určená k odeslání symetrického klíče) a podpisová schémata s nastavením parametrů. vhodné pro různé praktické případy použití. Tato otevřenost je hlavním rysem procesu NIST; existuje  [veřejná google skupina](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://groups.google.com/a/list.nist.gov/forum/%23!forum/pqc-forum)  obsahující podrobné diskuse o konkrétních kandidátských schématech a také o obecnějších rysech procesu. Původně bylo předloženo 69 kandidátů, i když hrstka se rychle stáhla poté, co byly objeveny chyby, a v lednu 2019 NIST ukončil první kolo procesu a oznámil 26 programů, které se dostaly do druhého kola. V červenci 2020, po téměř 18 měsících soustředění komunity na tato schémata, NIST oznámil své kandidáty do posledního kola: 4 mechanismy zapouzdření klíčů a 3 schémata podpisů, se záměrem vybrat na konci procesu alespoň jeden z každého typu. Přestože byla všechna tato schémata důkladně prověřena, každý z nich má jiné silné a slabé stránky, kterým je užitečné porozumět.

Ačkoli mnoho existujících forem kryptografie eliptických křivek, jako je ECDSA, je citlivých na kvantové počítače, je to důsledek specifické povahy algoritmů a nikoli slabina samotných eliptických křivek. Abychom kryptografii založili na izogeniích, použijeme následující pozorování: vzhledem ke dvěma eliptickým křivkám E1 a E2 je těžké najít izogenii φ, která posílá E1 na E2. Veřejný klíč by tedy mohl být pár eliptických křivek, se soukromým klíčem odpovídající izogeneze φ: E1 -> E2. Nyní může vlastník soukromého klíče použít izogenii φ k výpočtu operací zahrnujících E1 a E2, které jsou neovladatelné pro někoho, kdo nemá přístup k φ, a jako obvykle lze k nastavení těchto problémů použít veřejný pár E1 a E2. Přestože je oblast kryptografie na bázi izogeny stále v relativních plenkách, v kryptografické komunitě je o ní značné vzrušení, zejména po  [úspěšných experimentech](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://www.imperialviolet.org/2019/10/30/pqsivssl.html)  s využitím schémat založených na izogenii v internetových protokolech. Navíc působivě efektivní schéma podpisů nazvané SQISign, založené na novém problému v kryptografii založené na izogenii, získalo na letošní konferenci Asiacrypt cenu za nejlepší knihu .

**Směrem ke standardizaci: Proces NIST**

Vzhledem ke všem těmto konkurenčním nápadům může být těžké pochopit, kde leží budoucnost kryptografie. Jedním z míst, kde se můžete obrátit s žádostí o radu, je proces postkvantové standardizace, který provozuje Národní institut pro standardy a technologie (NIST) ve Spojených státech. NIST již dříve spouštěl procesy pro standardizaci symetrické kryptografie a hašovacích funkcí, což vedlo k široce používaným primitivům AES a SHA3. Ačkoli se nejedná o oficiální globální standard, je pravděpodobné, že jakýkoli algoritmus podporovaný NIST bude mít úrovně absorpce podobné těm u AES a SHA3, takže zkoumání tohoto procesu by mělo poskytnout nejmodernější pochopení pravděpodobné budoucnosti PQC. . NIST se snaží objasnit, že by to mělo být považováno za proces a ne za soutěž s „vítězem“, takže se mohou rozhodnout standardizovat nebo navrhnout více algoritmů pro různé případy použití, pokud neexistuje jasná nejlepší technika. Dvě hlavní vlastnosti, které NIST hledá, jsou bezpečnost a efektivita: pokud protokol není bezpečný, nemá smysl jej používat k ochraně dat, a pokud není efektivní, zpomaluje internetovou komunikaci. Obecně má PQC tendenci pracovat pomaleji než jeho předkvantový protějšek, takže algoritmus lze považovat za účinný, pokud nedojde k žádnému nebo malému poklesu výkonu při jeho použití namísto stávajícího předkvantového schématu .

Proces byl zahájen NIST v roce 2016 ve formě otevřené výzvy kryptografické komunitě, která žádala o návrhy mechanismů postkvantového zapouzdření klíčů (v podstatě asymetrická šifrovací schémata určená k odeslání symetrického klíče) a podpisová schémata s nastavením parametrů. vhodné pro různé praktické případy použití. Tato otevřenost je hlavním rysem procesu NIST; existuje  [veřejná google skupina](https://translate.google.com/website?sl=auto&tl=cs&hl=cs&client=webapp&u=https://groups.google.com/a/list.nist.gov/forum/%23!forum/pqc-forum)  obsahující podrobné diskuse o konkrétních kandidátských schématech a také o obecnějších rysech procesu. Původně bylo předloženo 69 kandidátů, i když hrstka se rychle stáhla poté, co byly objeveny chyby, a v lednu 2019 NIST ukončil první kolo procesu a oznámil 26 programů, které se dostaly do druhého kola. V červenci 2020, po téměř 18 měsících soustředění komunity na tato schémata, NIST oznámil své kandidáty do posledního kola: 4 mechanismy zapouzdření klíčů a 3 schémata podpisů, se záměrem vybrat na konci procesu alespoň jeden z každého typu. Přestože byla všechna tato schémata důkladně prověřena, každý z nich má jiné silné a slabé stránky, kterým je užitečné porozumět.

*Eliptická křivka ve dvou částech*

Zbývající 4 schémata zapouzdření klíče jsou NTRU, klasické schéma založené na mřížce využívající techniky pocházející z 90. let, CRYSTALS-Kyber, modernější schéma mřížky založené na problému zvaném Module LWE, SABRE, ještě modernější schéma založené na mřížce. na „zakulaceném“ problému zvaném Module LWR a Classic McEliece, modernizaci schématu založeného na kódu z konce 70. let. Tato tři mřížková schémata lze považovat za výběr různých kompromisů mezi bezpečností a efektivitou: na jedné straně SABRE funguje lépe než CRYSTALS-Kyber, který zase funguje lépe než NTRU. Naopak NTRU má nejlépe zavedené bezpečnostní vlastnosti, zatímco SABRE se spoléhá na problém modulu LWR, který stále není příliš dobře pochopen, přičemž spoléhání CRYSTALS-Kyber na modul LWE jej opět umisťuje doprostřed. Classic McEliece má horší výkon než jeho konkurenti na bázi mřížky, ale mohl by být standardizován jako bezpečný pro případ selhání v případě, že by se ukázalo, že síla kvantových útoků na mřížková schémata byla značně podceněna; rozmanitost v kryptografických předpokladech může být mocným nástrojem tváří v tvář neznámému. NIST naznačil, že pravděpodobně zpočátku zvolí jeden z NTRU nebo CRYSTALS-Kyber ke standardizaci, ale důkladnější bezpečnostní analýza SABER nebo kvantové útoky na mřížky by mohly změnit jejich směr.

Když obrátíme svou pozornost na podpisová schémata, znovu vidíme, že mřížky jsou pravděpodobnou budoucností PQC. Dva ze tří zbývajících kandidátů používají mřížky: CRYSTALS-Dilithium, podpisové schéma vyvinuté stejným týmem jako CRYSTALS-Kyber s použitím podobných technik, a Falcon, podpisové schéma podobné NTRU s několika novými technickými příspěvky. Další zbývající schéma, Rainbow, je vícerozměrné schéma s horším celkovým výkonem než jeho mřížkové protějšky. Podobně jako v případě Classic McEliece se NIST domnívá, že je přínosné zahrnout kandidáty bez mřížky, a relativní mládí Rainbow jako schématu znamená, že je možné, že by mohl být v blízké budoucnosti vylepšen, nebo by mohl vynikat v konkrétních případech použití. . NIST opět navrhl, že pravděpodobně standardizují jedno ze dvou mřížkových schémat: Falcon je pravděpodobně o něco efektivnější, ale přichází s podstatnými technickými komplikacemi při implementaci, které mohou vést k tomu, že je považován za zbytečně komplikovaný ve srovnání s elegantnějším designem. CRYSTALS-Dilithium, který si stále vede velmi dobře.

NIST také vybírá 8 schémat jako „alternativní“, schémata, která by podle jejich názoru měla být dále studována, protože NIST jsou otevřeny možnosti jejich standardizace v budoucnu. Vybrané alternativy mají kombinaci žádoucích vlastností a pozoruhodných nedostatků: mohou být například vysoce bezpečné, ale dosti neefektivní, vyžadují větší racionalizaci nebo postrádají potřebnou úroveň vystavení odhodlaným útočníkům, což je typické při vytváření důvěry v kryptografické zabezpečení. Z pěti klíčových alternativ zapouzdření lze čtyři nejlépe pochopit ve srovnání s finalisty: FrodoKEM lze považovat za konzervativnější verzi CRYSTALS-Kyber, která běží pomaleji, ale je bezpečnější, a NTRU Prime je schéma podobné NTRU, které funguje předpokládaná slabost v jiných technikách mřížky a malé náklady na efektivitu. Bike a HQC jsou dvě moderní šifrovací schémata založená na kódu, která fungují efektivněji než Classic McEliece, ale zavádějí nové bezpečnostní předpoklady, a proto potřebují podstatně větší kontrolu. Páté schéma, SIKE, je jediným zbývajícím kryptosystémem založeným na izogenii v procesu. NIST se domníval, že SIKE není dostatečně vyspělý, aby mohl být standardizován, ale jeho jedinečnost znamená, že je to kandidát, který pravděpodobně podstoupí seriózní výzkumné úsilí v budoucnu. Co se týče alternativních podpisů, pouze jeden má nějakou podobnost s finalisty: schéma známé jako GeMSS, které úzce konkuruje Rainbow, ale očekává se, že bude ve většině aplikací méně žádoucí. Další dvě alternativy, SPHINCS+ a Picnic, jsou založeny na hashovacích funkcích. Oba běží dost pomalu, ale mají extrémně silné bezpečnostní záruky, takže mohou být standardizovány pro použití s ​​vysoce citlivými daty nebo v případě kvantového „Armageddonu“, kde se ukazuje, že kvantové počítače mohou prolomit kryptografii, která používá cokoli složitějšího než jednoduchá primitiva, jako je hash. funkce .

**Výhled**

Kvantové počítače přicházejí a každý, kdo má zájem o adekvátní zabezpečení svých dat, se musí začít dívat do budoucnosti již nyní. Pro zvědavého pozorovatele bude sledování procesu NIST stále aktuální. Od nynějška až do doby, kdy si NIST vybere své standardy, což očekávají, že to bude trvat přibližně 12–18 měsíců, bude 7 finalistů podrobeno enormní úrovni zkoušek a časem bude pravděpodobně jasné, od kterých kandidátů se očekává, že projdou. Pro aktivnější lidi tam nikdy nebyl lepší čas zvážit, jaké algoritmy nejlépe podporují vaše případy použití. Všechna schémata zbývající v procesu NIST mají jedinečné prodejní body, ale počáteční standardy se pravděpodobně zaměří na schémata, která jsou nejlépe vyvážená. Pokud například pracujete s daty, která jsou obzvláště citlivá, může být vhodné zapojit se do diskusí o konzervativnějších schématech. Naopak, pokud potřebujete zabezpečit zařízení, která nemusí mít přístup k velkému výpočetnímu výkonu, jako jsou zařízení IoT, možná budete muset zvážit, která schémata lze provozovat ve zvláště nenáročných nastaveních; možná dobrý námět na další blogový příspěvek!