Kvantové počítače sú schopné riešiť matematické problémy, ktoré sú pre klasické počítače náročné na výpočet. Niektoré aktuálne používané kryptografické algoritmy sa spoliehajú práve na výpočtovú zložitosť matematických problémov, ktoré by kvantové počítače dokázali efektívne riešiť (napr. faktorizácia prvočísel). Preto ak za niekoľko rokov budú existovať funkčné kvantové počítače schopné veľkých a relatívne presných výpočtov, bezpečnosť týchto kryptografických algoritmov bude značne znížená. Kvantové počítače pravdepodobne budú schopné prelomiť kryptosystémy založené na verejných kľúčoch, vrátane RSA, DSA a eliptických kriviek. Tieto algoritmy sú používané na elektronické podpisy, výmenu kľúčov a zabezpečujú dôvernosť a autentifikáciu pri komunikácii na internete a iných sieťach.

Kvôli týmto zisteniam sa mnoho výskumníkov začalo zaoberať oblasťou postkvantovej kryptografie, ktorá zahŕňa algoritmy odolné voči útokom kvantových počítačov. Aj keď v čase písania tohto textu existujú odhady, že plne funkčný a využiteľný kvantový počítač pravdepodobne bude vyrobený až za niekoľko rokov (odhadovaný čas je približne 10 rokov), je potrebné zaoberať sa postkvantovou kryptografiou už teraz. Proces výberu a štandardizácie vhodných algoritmov totiž môže zabrať niekoľko rokov. Na to, aby bol algoritmus považovaný za spoľahlivý, musí prejsť procesom kryptoanalýzy, byť preskúmaný mnohými odborníkmi a úspešne odolať rôznym navrhovaným útokom. Dôvera v kryptografický algoritmus sa zvyčajne buduje dlhé roky.

NIST (National Institute of Standards and Technology - Národný inštitút pre štandardy a technológie) má zaužívané, že pri výbere a štandardizácii kryptografických algoritmov vyhlasuje výzvy pre verejnosť, aby sa rôzni odborníci z celého sveta mohli do tohto procesu zapojiť. Podstatou je, aby celý proces výberu algoritmu ostal transparentný. Kryptografická verejnosť má počas trvania výzvy možnosť posielať návrhy algoritmov alebo testovať bezpečnosť a výkonnosť algoritmov prihlásených do výzvy. Celý proces uzavrú odborníci na kryptografiu z NIST-u, ktorí na základe zaslaných komentárov a článkov verejnosti a vlastného výskumu zvolia vyhovujúce algoritmy, prípadne ich upravia tak, aby lepšie spĺňali požiadavky na bezpečnosť a efektívnosť.

Medzi rokmi 1997 a 2000 bol takýmto spôsobom zvolený algoritmus AES (Advanced Encryption Standard) ako nástupca DES (Data Encryption Standard). Do súťaže bolo zapojených 15 rôznych návrhov blokových šifier a zvíťazil algoritmus nazvaný Rijndael. Podobným spôsobom bol zvolený aj algoritmus SHA-3: medzi rokmi 2007 a 2012 prebiehala súťaž, ktorej víťazom sa stal Keccak algoritmus.

Keďže prístup v podobe výziev pre verejnosť sa osvedčil, NIST sa rozhodol rovnakým spôsobom vybrať a štandardizovať aj postkvantové algoritmy. V roku 2012 preto NIST začal

PQC (Post-quantum Cryptography) projekt, vytvoril výskumný tím a spojil sa s inými organizáciami pre štandardizáciu. V januári 2017 NIST začal s procesom štandardizácie postkvantovej kryptografie a vydal výzvu pre verejnosť na zasielanie návrhov algoritmov. Do výzvy bolo prihlásených 82 algoritmov a z toho bolo 69 algoritmov akceptovaných ako úplné a vhodné riešenia. Prebehlo prvé kolo, v čase písania textu prebieha druhé a aj keď pôvodne nebolo plánované, chystá sa aj tretie kolo výzvy.

Rozdiel oproti predchádzajúcim výzvam je ten, že pravdepodobne nebude vybratý iba jeden najlepší algoritmus – postkvantové algoritmy sa totiž veľmi líšia, každý má určité výhody aj nevýhody a existuje veľa kritérií, ktoré je potrebné pri výbere zvážiť. Ak sa počas procesu štandardizácie zúži výber algoritmov, neznamená to, že algoritmy mimo tohto výberu budú zabudnuté. V dôsledku nových poznatkov v danom poli sa môže stať, že víťazné algoritmy výzvy budú nepoužiteľné a bude potrebné preskúmať algoritmy mimo užšieho výberu. Existujú rôzne rodiny postkvantových kryptografických algoritmov a algoritmy v každej rodine sú založené na iných matematických problémoch. Algoritmy zapojené do výzvy sa dajú rozdeliť do štyroch hlavných rodín: mrežové, kódové, multivariačné a hašové.

V procese výberu sa najviac bude prihliadať na bezpečnosť, ďalej na výkon, kompatibilitu s aktuálne používanými protokolmi, odolnosť voči útokom cez bočné kanály, ale aj na jednoduchosť a názornosť. Niektoré návrhy boli vybraté aj kvôli ich jedinečnosti, ilustratívnosti a inovatívnosti prístupu, ktorý ukazovali. Množstvo rozličných a inovatívnych návrhov totiž poskytne kryptografom a kryptoanalytikom možnosť rozšíriť poznatky o rôznych prístupoch a pomôže informatickej verejnosti lepšie pochopiť nové princípy a problémy, na ktorých sú podobné algoritmy založené. Preto do procesu štandardizácie boli zahrnuté algoritmy, ktoré dobre ozrejmujú princípy danej rodiny algoritmov. Navyše ak budú algoritmy založené na rôznych princípoch, je málo pravdepodobné, že nejaký typ útoku by bol úspešný pri všetkých týchto algoritmoch.

Práve z dôvodu vysvetlenia princípov fungovania postkvantových algoritmov a ich priblíženia informatickej verejnosti je naším ***prvým cieľom*** **popísať a názorne prezentovať základné algoritmy postkvantovej kryptografie na grupách mrežových bodov**. Pre naplnenie tohto cieľa vytvoríme webstránku, na ktorej bude vizualizácia výpočtu postkvantového algoritmu spolu s jeho vysvetlením. Používateľ si bude môcť zvoliť parametre a nechať si zašifrovať jednoduchý text, pričom bude môcť sledovať, ako proces prebieha.

Najväčšia nádej je vkladaná do kódových a mrežových algoritmov. Kódové algoritmy boli známe už dávnejšie (algoritmus McEliece vznikol v roku 1978) a preto sú ich silné aj slabé stránky viac preskúmané a pôsobia o niečo dôveryhodnejšie než mrežové algoritmy (prvý mrežový algoritmus vznikol v roku 1996). Avšak čo sa týka veľkosti kľúčov, kódové algoritmy

potrebujú väčšinou kľúče veľkosti okolo 1MB, pričom mrežovým algoritmom stačí niekoľko KB. V súčasnosti sa začínajú viac skúmať práve mrežové algoritmy. Google sa medzi prvými rozhodol začať zavádzať postkvantové algoritmy a začal práve implementáciou varianty mrežového algoritmu NTRU do protokolu TLS. Keďže mrežové algoritmy sú efektívne, odborníci sa o nich zaujímajú, ale je potrebné ich ešte preskúmať, rozhodli sme sa v našej práci venovať práve im.

Naším ***druhých cieľom*** je **implementovať odľahčené verzie týchto algoritmov a porovnať ich priemernú výpočtovú a pamäťovú zložitosť**. Takáto odľahčená implementácia bude totiž jasnejšie ukazovať, akým spôsobom prebieha výpočet daného algoritmu. Navyše odľahčené implementácie je vhodné použiť, ak potrebujeme rýchlo a efektívne vykonať proces šifrovania a nepotrebujeme, aby dáta ostali utajené dlhú dobu, t.j. aby šifra odolala aj dlho trvajúcim pokusom o útok hrubou silou, ale stačí nám aby algoritmus garantoval dôvernosť zašifrovaných údajov počas určeného kratšie trvajúceho časového obdobia.

Naším ***tretím cieľom*** je zapojiť sa do NIST výzvy na štandardizáciu postkvantových algoritmov a teda **porovnať modifikácie týchto základných algoritmov na grupách mrežových bodov použitých v štandardizačnom procese NIST (Post-Quantum Cryptography Standard)**. Porovnávať budeme algoritmy, ktoré prešli do druhého kola štandardizačného procesu. Týchto algoritmov je dokopy 9 a konkrétne sa jedná o CRYSTALS-KYBER, FrodoKEM, LAC, NewHope, NTRU, NTRU Prime, Round5, SABER a Three Bears.

Literatúra:

1. Micciancio, D., Regev, O. : Lattice-based Cryptography, In: Post-Quantum Cryptography, Springer Berlin Heidelberg, 2009, ISBN 978-3-540-88702-7

2. Doulgerakis E., Laarhoven T., de Weger B.: Finding Closest Lattice Vectors Using Approximate Voronoi Cells. In PQCrypto 2019, LNCS vol. 11505, Springer, (Cryptology ePrint Archive, Report 2016/888)

3. NISTIR 8240 Status Report on the First Round of the NIST Post-Quantum Cryptography, NIST 2019, (https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf)