Kryptoanalytické algoritmy pro kvantové počítače

Patrik Kováč

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Patrik Kováč**
Osobní číslo:	**A19687**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Kryptoanalytické algoritmy pro kvantové počítače**
Téma práce anglicky:	**Cryptanalytic Algorithms for Quantum Computers**

Zásady pro vypracování

1. Vypracujte literární rešerši na dané téma.
2. Popište vybrané kryptoanalytické kvantové algoritmy včetně charakterizace různých typů kvantových počítačů.
3. Vypracujte podrobný přehled, kategorizaci a popište využitelnost algoritmů.
4. Proveďte průzkum aplikovatelnosti algoritmů pro symetrickou i asymetrickou kryptografii.
5. Vyhodnoťte dosažené poznatky a proveďte závěr.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. BERNSTEIN, Daniel J., Johannes A. BUCHMANN a Erik DAHMEN, ed. *Post-quantum cryptography*. Berlin: Springer, [2009], viii, 245 s. ISBN 978-3-540-88701-0.
2. LANGE, Tanja a Rainer STEINWANDT, ed. *Post-Quantum cryptography: 9th International conference, PQCrypto 2018 Fort Lauderdale, FL, USA, April 9-11, 2018 Proceedings*. Cham: Springer, [2018], xiii, 527 s. ISBN 978-3-319-79062-6.
3. KUMAR, Neeraj, et al. (ed.). *Limitations and Future Applications of Quantum Cryptography*. Information Science Reference, 2020.
4. NIELSEN, Michael A. a Isaac L. CHUANG. *Quantum computation and quantum information*. 10th Anniversary ed. Cambridge: Cambridge University Press, 2010, xxxi, 676 s. ISBN 9781107002173.
5. MEGLICKI, Zdzislaw. *Quantum computing without magic: devices*. Cambridge, MA: MIT Press, c2008, 1 online zdroj (xx, 422 p.). Scientific and engineering computation series. ISBN 9780262288187. Dostupné také z: https://proxy.k.utb.cz/login?url=http://ieeexplore.ieee.org/xpl/bkabstractplus.jsp?bkn=6267464
6. SWENSON, Christopher. *Modern cryptanalysis: techniques for advanced code breaking*. Indianapolis: Wiley, c2008, xxviii, 236 s. ISBN 9780470135938.

Vedoucí bakalářské práce: **doc. Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **3. prosince 2021**
Termín odevzdání bakalářské práce: **23. května 2022**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 24. ledna 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 18.5.2020

Kováč
…….
podpis studenta

ABSTRAKT

Táto bakalárska práca sa zaoberá mapovaním kryptoanalytických algoritmov pre kvantové počítače. V teoretickej časti je popísaný úvod do kryptológie, základy a charakterizácia kvantových počítačov spolu s súčasným vývojom v tejto oblasti. Ako ďalšie sú predstavené kvantové algoritmy. Praktická časť sa zaoberá kategorizáciou kvantových algoritmov, ktoré sú nebezpečné pre modernú kryptografiu. Sú tu uvedené dopady využitia týchto algoritmov na symetrickú a asymetrickú kryptografiu a ponúknutá alternatíva k prelomeným kryptografickým systémom, v podobe post-kvantovej kryptografie.

Klíčová slova: kvantové počítanie, kvantová distribúcia kľúčov, Shorov algoritmus, Groverov algoritmus, post-kvantová kryptografia

ABSTRACT

This bachelor thesis aims to map cryptanalytic algorithms for quantum computers. The theoretical part of the thesis begins with an introduction to cryptology, the basics of quantum computing, and the progress made in this field nowadays. The last part of the theoretical part introduces quantum algorithms. The practical part of the thesis deals with the categorization of quantum algorithms which are a threat to modern cryptography. Furthermore, this part describes the impact of these algorithms on symmetric and asymmetric cryptography and offers an alternative to bro-ken ciphers in the form of post-quantum cryptography.

Keywords: quantum computing, quantum key distribution, Shor’s algorithm, Grover’s algorithm, post-quantum cryptography

Chcel by som sa poďakovať vedúcemu tejto bakalárskej práce, doc. Ing. Romanovi Šenkeříkovi, Ph.D. za ochotu a odbornú spätnú väzbu, ktorú mi počas písania tejto bakalárskej práce ponúkal.

Ďalej by som chcel poďakovať celej svojej rodine a blízkym za podporu a motiváciu pri písaní tejto práce.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

„Je kryptografia mŕtva?“ [1] na túto otázku sa pýta Daniel J. Bernstein vo svojej knihe Post-Quantum cryptography. Vzhľadom na pokrok súčasných technológií ide o celkom opodstatnenú otázku, na ktorú hľadám čiastočne odpoveď aj ja, vo svojej bakalárskej práci. Kryptografia sa v súčasnosti široko používa na zabezpečenie digitálnej komunikácie a bezpečného prehliadania internetu, digitálnych podpisov a hrá veľmi dôležitú úlohu pri ochrane citlivých údajov, ktoré je potrebné udržiavať v tajnosti. Hrozbu pre tieto kryptografické systémy predstavujú kvantové počítače.

V súčasnosti sú najvýkonnejšie kvantové počítače zatiaľ ťažko použiteľné v praxi tak, aby boli hrozbou pre moderné kryptografické systémy, ktoré používame. O túto oblasť je veľký záujem, a tak v nej môžeme očakávať obrovský pokrok. S týmto vývojom v oblasti kvantových počítačov prichádza ohrozenie pre kryptografické systémy, ktoré využívame každý deň. Kvantové algoritmy, ktoré sú v tejto bakalárskej práci popísané dokážu mnoho z týchto systémov prelomiť.

Cieľom tejto bakalárskej práce je podrobné zmapovanie rôznych algoritmov pre kvantové počítače, ich možnosti pre útoky na kryptografické protokoly a šifry, a ich dopady na symetrickú a asymetrickú kryptografiu.

V teoretickej časti sa táto bakalárska práca zaoberá základmi kryptológie a rozdelením kryptografie na symetrickú a asymetrickú kryptografiu spolu s využitím týchto dvoch disciplín. V ďalšej kapitole sú popísané kvantové počítače, ich možné využitie v budúcnosti a ich rozdelenie. Na konci teoretickej časti sú predstavené a popísané a charakterizované kvantové algoritmy.

V praktickej časti sú tieto algoritmy kategorizované a je popísané ich podrobné fungovanie a ako ohrozujú modernú kryptografiu. Práca pokračuje rozborom dopadov týchto algoritmov na symetrickú a asymetrickú kryptografiu, pričom v záverečnej kapitole ponúka riešenie v podobe post-kvantovej kryptografie, ktorej súčasťou je aj kvantová distribúcia kľúčov.

I. TEORETICKÁ ČÁST

1 ZÁKLADY KRYPTOLÓGIE

Výmena dôverných informácií je v spoločnosti veľmi dôležitá. Od vojenských rozkazov, až po čísla kreditných kariet, po tisícky rokov ľudia potrebovali ochranu pre svoje dáta. Veda, ktorá sa zaoberá bezpečným prenosom informácií, sa nazýva kryptológia. Zaoberá sa utajením správ vo všetkých formách. Zvyčajne sa rozdeľuje do dvoch jednotlivých príbuzných vied, ktorými sú kryptoanalýza a kryptografia. [2]

1.1 Kryptoanalýza a kryptografia

1.1.1 Kryptoanalýza

Kryptoanalýza je veda, ktorá sa zaoberá dešifrovaním a analýzou kódov, šifier a zašifrovaného textu. Používa matematické formuly, aby našla slabiny a prelomila kryptografické systémy. Vývoj v oblasti kryptoanalýzy tlačí dopredu vývoj v oblasti kryptografie. [3]

1.1.2 Kryptografia

Kryptografia je presným opakom kryptoanalýzy. Zaoberá sa bezpečnými komunikačnými technikami, ktoré umožňujú iba odosielateľovi a príjemcovi správy, aby poznali jej obsah. Používa sa už tisícky rokov aby zabezpečila utajenú komunikáciu. V minulosti bola používaná hlavne v odvetviach armády. V súčasnosti sa využíva takmer všade v podobe modernej kryptografie. [4]

Moderná kryptografia sa využíva na zabezpečenie komunikácie cez internet, autentifikáciu užívateľov, platby cez internet, zabezpečenie VPN, zabezpečenie kryptomien a podobne. [5]

Kryptografia má podľa [6] štyri aspekty:

1. Utajenosť: správa je skrytá pred nežiaducimi stranami
2. Integritu: so správou nie je nijako manipulované
3. Autentifikáciu: možnosť účastníkov identifikovať identitu toho druhého
4. Nepopierateľnosť: komunikácia neskôr nemôže byť popretá žiadnym z účastníkov

1.2 Šifrovanie

Šifrovanie je prevod otvoreného textu na šifrovaný text, za pomoci kryptografického systému, pri čom sa využíva kľúč.

1.2.1 Otvorený text

Pri šifrovaní je často spomínaný pojem otvorený text. Tento pojem označuje pôvodnú správu, pred aplikáciou kryptografických postupov, ktorá je voľne čitateľná. [2]

1.2.2 Šifrovaný text

Naopak, šifrovaný text je zašifrovaná správa, ktorú si prečíta iba príjemca s príslušným návodom, k dešifrovaniu tejto správy. Systém, ktorý slúži k prevádzaniu otvoreného textu, na šifrovaný text a naopak, sa nazýva šifrový alebo taktiež kryptografický systém (skrátene šifra). [2]

1.2.3 Kľúč

V kryptografii je kľúč reťazec znakov, ktorý sa používa v rámci šifrovacieho algoritmu na premenu otvoreného textu na šifrovaný text. [7]

Na základe toho, či sa pre šifrovanie používa súkromný alebo verejný kľúč, sa kryptografia rozdeľuje na symetrickú a asymetrickú.

1.3 Symetrická a asymetrická kryptografia

1.3.1 Symetrická kryptografia

Pri symetrickej kryptografii sa využíva ten istý kľúč na šifrovanie, aj dešifrovanie. Jedným z najväčších problémov symetrickej kryptografie, je nájsť efektívnu metódu bezpečnej výmeny kľúčov na šifrovanie. Tento problém sa nazýva problém distribúcie kľúčov. [8]

Symetrická kryptografia sa rozdeľuje na prúdové a blokové šifry. Prúdové šifry text šifrujú po jednotlivých bitoch. Príkladom prúdovej šifry je Vernamova šifra.

Blokové šifry rozdelia otvorený text do menších celkov, ktoré sa nazývajú bloky a zašifrujú tento text blok po bloku. Najznámejšími blokovými šiframi sú DES a AES. [8] [9]

1.3.1.1 DES

DES (Data Encryption Standard) bol kedysi najpoužívanejšou šifrou. Pri takomto šifrovaní sú dáta šifrované v 64-bitových blokoch, s využitím 56-bitového kľúča, aby vznikol 64-bitový zašifrovaný výstup. DES sa stal dominantným symetrickým šifrovacím algoritmom, využívaným hlavne v oblasti financií. [10]

Funguje tak, že po prvej permutácii, kedy sa bity preskupia podľa matice, sa blok textu rozdelí na dve polovice o dĺžke 32 bitov. Nasleduje 16 permutácií daného textu každej polovice pomocou zvoleného kľúča. Napokon sa tieto dve polovice spoja a nasleduje posledná permutácia, kedy sa spraví presný opak prvej permutácie, a vznikne tak zašifrovaný text. [10] [11]

Medzi najväčšie slabiny DES patrí, že 56-bitový kľúč neposkytuje adekvátnu ochranu a jeho pomalosť.

Neskôr bol tento algoritmus používaný ako 3DES, kedy sa DES použil trikrát za sebou pre zašifrovanie jedného bloku informácií. Ani toto s rýchlym vývojom technológií nestačilo a DES musel byť neskôr nahradený algoritmom AES. [11]

1.3.1.2 AES

AES (Advanced Encryption Standard) nahradil DES, v roku 2000, a od toho momentu sa stal novým šifrovacím štandardom. AES je v súčasnosti jedným z najpoužívanejších šifrovacích algoritmov a NSA (National Security Agency) ho uznala vhodným na ochranu prísne tajných informácií. [11]

AES spracováva dáta po blokoch o veľkosti 128 bitov, za použitia kľúčov s veľkosťou 128, 192 alebo 256 bitov. AES nepracuje s bitmi ale s bajtami, ktoré sú postupnosťou 8 bitov. AES pracuje s informáciami pomocou dvojdimenzionálneho poľa bajtov. Toto pole má vždy 4 riadky, takže na jeden riadok pripadá 32 bitov. Počet stĺpcov závisí od dĺžky kľúča. Ak je kľúč 128-bitový, 128/32 = 4, čiže stĺpce budú 4. Ak je 192-bitový, bude ich 6, a ak má 256 bitov, tak ich bude 8. Počet opakovaní pri AES závisí takisto od dĺžky kľúča. Ak má 128 bitov, opakovaní bude 10, ak 192, tak ich bude 14 a pri 256-bitovom kľúči bude opakovaní 14. Pred samotným šifrovaním, AES algoritmus vygeneruje pre každé opakovanie jeden príslušný kľúč. [11] [12] [13]

Každé opakovanie pozostáva zo 4 krokov:

1. SubBytes – v tomto kroku sa každý bajt nahradí iným bajtom.
2. ShiftRows – každý riadok sa posunie o určitý počet miest.
    - prvý riadok sa neposunie
    - druhý riadok sa posunie o jedno miesto doľava
    - tretí riadok sa posunie o dve miesta doľava
    - štvrtý riadok sa posunie o tri miesta doľava

3. MixColumns – tento krok je v podstate násobenie matice. Každý stĺpec sa vynásobí určitou maticou a tým sa zmení pozícia každého bajtu v matici. Tento krok sa pri poslednom opakovaní vynecháva.
4. Add RoundKeys – výsledný výstup sa XOR-uje s príslušným kľúčom pre dané opakovanie.

1.3.2 Využitie symetrickej kryptografie

AES je jedna z najbezpečnejších šifier na svete, o ktorej panuje predpoklad, že najmä vo verzii s 256-bitovým kľúčom je takmer nemožné ju prelomiť. Pôvodne bola navrhnutá na zabezpečenie prísne tajných informácií v USA. V súčasnosti sa používa vo veľkej miere aj v iných oblastiach.

AES sa podľa [14] [15] využíva na:

- Zabezpečenie Wi-Fi kde sa využíva na overenie klientov a routerov. Wi-Fi siete majú na tomto algoritme založené celé bezpečnostné systémy, ktoré sa využívajú každý deň.
- AES hrá veľkú úlohu pri overovaní serverov webových stránok a to ako na strane klienta, tak aj na strane serveru. V kombinácii s asymetrickou kryptografiou sa používa pri SSL/TLS šifrovacích protokoloch aby bola zabezpečená najvyššia bezpečnosť pri prehliadaní webových stránok.
- Tento algoritmus sa využíva aj na šifrovanie súborov. Od textových správ až po fotografie a legálne dokumenty.
- Takisto slúži aj na zabezpečenie ochrany procesora. Výrobcovia umožňujú hardvérovú implementáciu AES šifrovania aby zamedzili napríklad zraniteľnosť meltdown, čo je zraniteľnosť hardvéru, ktorá dovoľuje používateľským procesom čítať dáta z ľubovoľnej časti fyzickej pamäti. To zahŕňa dáta aj z iných procesov alebo dokonca jadra systému.

1.3.3 Asymetrická kryptografia

Alternatívou k symetrickej kryptografii je kryptografia s verejným kľúčom (asymetrická kryptografia). Pri asymetrickej kryptografii sa používa verejný kľúč, ktorý slúži na šifrovanie a súkromný kľúč, ktorý slúži na dešifrovanie tejto správy. Súkromný kľúč musí byť udržiavaný v tajnosti. Tento systém kryptografie vyriešil problém distribúcie kľúčov. Medzi najznámejšie a naviac používané kryptografické systémy patria práve asymetrické

šifry. Tieto systémy sú prevažne založené na matematických problémoch, ako napríklad problém faktorizácie alebo problém diskrétneho logaritmu. [16] [17]

S ohľadom na zameranie tejto bakalárskej práce a hrozbu, ktorú kvantové počítače pre asymetrickú kryptografiu predstavujú, sú detailne popísané princípy a matematické základy vybraných najpoužívanejších algoritmov, ktorými sú RSA, Diffie-Hellman, ElGamal a DSA spolu s ECDSA.

1.3.3.1 RSA

RSA, pomenovaný podľa svojich autorov: Rivest, Shamir a Adleman, funguje na princípe voľne dostupného verejného kľúča, ktorý môže použiť hocikto na zašifrovanie informácií. Akonáhle sú informácie zašifrované, môžu byť dešifrované iba pomocou súkromného kľúča. Ide o momentálne jeden z najpopulárnejších a najpoužívanejších šifrovacích algoritmov. Tento kryptosystém je založený na probléme faktorizácie, ktorá je časovo veľmi náročná. Kľúč vzniká násobením obrovských prvočísiel. Pri dostatočne veľkých prvočíslach je RSA nedobytná. Najznámejším rizikom pre RSA však je, že by mohol niekto objaviť spôsob rýchlej faktorizácie. Od toho momentu by bola RSA nepoužiteľná. [2] [16] [18]

RSA funguje tak, že sú zvolené dve obrovské prvočísla p a q. Ak je pomocou nich vygenerované $n = p*q$, tak je pri znalosti n, veľmi ťažké získať p alebo q, pri čom platí, že čím sú väčšie hodnoty, tým je ťažšie faktorizovať n. Nasledujú 4 kroky fungovania tohto algoritmu:

1. S využitím obrovských prvočísiel p a q, sa vypočíta n.
2. Vypočíta sa $t = \phi(n) = (p-1)(q-1)$.
3. Zvolí sa e, pre ktoré platí, že je väčšie než 1 a menšie než t, a zároveň je relatívnym prvočíslom pre t. To znamená, že najväčší spoločný deliteľ týchto čísiel je 1.
4. Vypočíta sa $d = e^{-1}$, pre ktoré platí, že $ed = 1(mod\ t)$.

Pár (e, n) sa potom používa ako verejný kľúč a pár (d, n) sa využíva ako súkromný kľúč. [2]

1.3.3.2 Diffie-Hellman

Ďalším z veľmi obľúbených a používaných algoritmov je Diffie-Hellman. Tento algoritmus je jedným z najjednoduchších a najpoužívanejších kryptografických systémov, ktorý

je založený na probléme diskrétneho logaritmu. Diffie a Hellman prišli na spôsob, ako môžu dve entity získať ten istý kľúč cez nezabezpečený kanál.

Povedzme, že komunikujú dvaja ľudia, Alica a Bob.

1. Alica a Bob sa dohodnú na konečnom poli F a na generátore g, ktoré sú verejne známe.
2. Alica si vyberie tajné číslo a, a Bob si vyberie tajné číslo b.
3. Alica pošle Bobovi verejne číslo g^a vypočítané v F.
4. Bob pošle Alici číslo g^b vypočítané v F.

Na konci tejto výmeny, môže Alica vypočítať $(g)^b = g^{ab}$ v F, a Bob môže vypočítať $(g^b)^a = g^{ab}$ v F, takže obidvaja zdieľajú to isté g^{ab} ktoré vedia iba oni dvaja. Ktokoľvek v danom kanáli pozná g, F, g^a a g^b ale vďaka problému diskrétneho algoritmu, vedomosť g^a a g^b neznamená, že by ktokoľvek dokázal získať a alebo b. A vlastnosti polí neumožňujú nikomu pomocou g^a a g^b aby s ľahkosťou získal g^{ab}. [2]

1.3.3.3 ElGamal

Šifrovací systém ElGamal je založený na výmene kľúčov, ktorú popisuje Diffie-Hellman. Tento šifrovací systém je takisto založený na probléme hľadania diskrétneho logaritmu na cyklickej grupe. [19] [20]

Funguje na základe troch komponent:

1. Generovanie kľúča
    a. Alica si vyberie veľké číslo q a cyklickú grupu F_q
    b. Z cyklickej grupy F_q si vyberie číslo g a číslo a také, že ich najväčší spoločný deliteľ je 1
    c. Potom vypočíta $h = g^a$
    d. Potom uverejní F, h, q a g ako svoj verejný kľúč a ponechá si a ako súkromný kľúč
2. Šifrovanie správy m pomocou uverejneného kľúča
    a. Bob si vyberie číslo k z cyklickej grupy F
    b. Vypočíta $p = g^k$ a $s = h^k = g^{ak}$
    c. Ďalej vynásobí s a m
    d. Bob odošle $s*m$ a p

3. Alica dešifruje správu
    a. Vypočíta $t = p^a = g^{ak}$
    b. Vypočíta *(s*m) / t* aby získala m, keďže $s = t$

1.3.3.4 DSA

DSA (Digital Signature Algorithm) je založený na probléme diskrétneho logaritmu a modulárneho umocňovania. Na rozdiel od RSA, tento algoritmus nemôže byť využitý na šifrovanie alebo výmenu kľúčov, ale iba na funkciu pre digitálne podpisy.

DSA vypočíta hash správy, potom vygeneruje pseudonáhodné číslo *k* a vypočíta podpis, ktorý pozostáva z dvoch čísiel *r* a *s,* kde *r* sa vypočíta z *k* a *s* sa vypočíta z hashu správy + exponentu súkromného kľúča + čísla *k.* Vďaka náhodnosti čísla *k* je podpis nedeterministický. [5] [10] [21]

DSA algoritmus poskytuje nasledujúce výhody:

- Nepopierateľnosť – Odosielateľ nemôže poprieť, že správu odoslal.
- Overenie správy – pomocou správneho kľúča sa dá overiť pôvod odosielateľa.
- Overenie integrity – Nie je možné so správou nijako manipulovať

1.3.3.5 ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) je komplexnejší než DSA a jeho kľúče sa generujú pomocou eliptických kriviek, vďaka čomu sú kľúče menšie, ako klasické kľúče DSA. Kryptografia eliptických kriviek je typ kryptografie, založený na algebrickej štruktúre eliptických kriviek nad konečnými telesami. Využíva sa hlavne na generovanie pseudonáhodných čísiel a digitálnych podpisov. ECDSA je vďaka menšej dĺžke svojich podpisov efektívnejší, než iné algoritmy na digitálne podpisovanie, zatiaľ čo si zachováva takú istú úroveň bezpečnosti. [22]

1.3.4 Využitie asymetrickej kryptografie

Okrem už spomínaných využití asymetrickej kryptografie, v kombinácii so symetrickou kryptografiou, pri zabezpečení webových stránok, sú využitia asymetrickej kryptografie podľa [23] a [24] nasledovné:

- Asymetrická kryptografia sa využíva pri HTTPS, pre bezpečné pripojenie k webovým stránkam.

- SSH algoritmy, ktoré slúžia na bezpečné pripojenie k vzdialenému serveru.
- Digitálne podpisy
- Takisto sa využíva na bezpečné posielanie emailov pomocou protokolu PGP.
- Ďalšie využitie algoritmu RSA je pri VPN, kde slúži na bezpečnú komunikáciu medzi VPN klientom a VPN serverom.
- Asymetrická kryptografia tiež slúži na zabezpečenie chráneného prenosu správ pri chatovaní cez internet.
- Kryptomeny využívajú asymetrickú kryptografiu na to, aby zabezpečil to, že iba vlastník peňaženky z nej môže vyberať alebo posielať peniaze.

1.4 Kvantová kryptografia

Kvantová kryptografia prináša šifrovanie na vyššiu úroveň, s použitím princípov kvantovej fyziky, ako napríklad kvantové mechanizmy, ktoré šifrujú a prenášajú informácie bezpečne takým spôsobom, že ich nikto nedokáže prelomiť. Kvantová kryptografia je tiež známa ako kvantová distribúcia kľúčov (Quantum Key Distribution - QKD). [25]

1.4.1 Kvantová distribúcia kľúčov

Kvantová distribúcia kľúčov využíva kvantovú fyziku, na zabezpečenie distribúcie symetrických kľúčov. Funguje na báze posielania fotónov (častíc svetla), cez optické spojenie. Jednotlivé protokoly QKD sú navrhnuté tak, že každé nežiaduce pozorovanie týchto fotónov, naruší samotný prevod. Toto vedie k chybám pri prenose, čo legitímni užívatelia dokážu spozorovať. Toto umožňuje overenie bezpečnosti takto distribuovaných kľúčov. Prvý protokol kvantovej distribúcie kľúčov, s názvom BB84, vznikol v roku 1984. [26]

1.4.1.1 Protokol BB84

Charles Bennet a Gilles Brassard vyvinuli prvý protokol kvantovej distribúcie kľúčov, zvaný BB84. Tento protokol je založený na polarizácii fotónov. Rozlišujú sa dva stavy polarizácie: priamočiara báza, ktorá zahŕňa horizontálnu a vertikálnu orientáciu a diagonálna báza, ktorá zahŕňa orientáciu otočenú buď o + 45° alebo o -45°.

1. Alica si vyberie reťazec N náhodných klasických bitov $X_1 \ldots X_N$
2. Alica si vyberie náhodnú postupnosť polarizačných stavov, kde si môže vybrať buď priamočiaru bázu (*R*) alebo diagonálnu bázu (*D*). Tieto bázy sú vzájomne nezávis-

lé. To znamená že meranie v jednej z báz neodhaľuje informácie o bite, ktorý je zakódovaný v inej báze.

3. Alica zašifruje jej reťazec bitov do súboru fotónov s polarizáciou podľa vybraných báz.
4. Keď Bob dostane tento súbor fotónov, náhodne a nezávisle od Alice sa rozhodne pre každý fotón, či ho zmeria v priamočiarej báze alebo v diagonálnej báze, aby získal klasické bity. Po tomto kroku majú aj Alica aj Bob klasický reťazec bitov, ktorý sa zapisuje ako $X = (X_1 \ldots X_N)$ pre Alicu a $Y = (Y_1 \ldots Y_N)$ pre Boba.
5. Bob potom zverejní bázy, ktoré zvolil na zmeranie fotónov, ktoré mu poslala Alica. Alica tieto bázy porovná s bázami, ktoré použila ona a povie, ktoré bázy zvolil Bob správne. Bity, pre ktoré boli zvolené šifrovacie a meracie bázy nezhodné, sú vyradené. Tomuto kroku sa v angličtine hovorí „sifting“, teda preosievanie.
6. Ďalším krokom je odhad parametrov, kedy Bob zverejní niektoré náhodné bity svojho kľúča. V prípade nenarušenej komunikácie by tieto bity mali byť také isté, ako má Alica, ktorá ich v takomto prípade potvrdí. Ak je chybovosť príliš vysoká, tak pravdepodobne prišlo k narušeniu komunikácie a Alica a Bob tento protokol preruša. Zverejnené bity sú po tomto kroku zahodené, keďže sú verejne prístupné narušiteľovi.
7. Ďalším krokom je oprava chýb. Alica pošle potrebné informácie k oprave, cez klasický verejný kanál Bobovi. Po tomto kroku majú Alica a Bob rovnaké kľúče.
8. Posledným krokom je zvýšenie utajenia, kedy sú z kľúča odstránené všetky bity, ktoré boli zverejnené a vznikne tak kratší, ale úplne utajený reťazec bitov, ktorý je výsledným kľúčom.

Na základe tohto protokolu vzniklo mnoho ďalších QKD protokolov, ktoré využívajú polarizáciu fotónov a ktoré sa považujú za varianty BB84. Napríklad BB92 protokol, SARG04 protokol, alebo Six-State protokol(SSP). [27] [28] [29]

1.4.1.2 Protokol E91

Nový typ QKD protokolov, ktorý využíva kvantové previazanie vznikol v roku 1991. Kvantové previazanie je stav, kedy dve častice sú previazané tak, že keď sa zmeria stav jednej častice, tak na druhej častici bude okamžite nameraný presne opačný stav. Na vzdialenosti týchto dvoch častíc nezáleží. Pred meraním je nemožné určiť, v akom stave častice sú. Toto musí byť komunikované cez verejný komunikačný kanál.

Generovanie kľúča vyzerá pri tomto protokole takto:

1. Vygeneruje sa pár maximálne previazaných častíc a prvý z nich sa pošle Alici, a druhý Bobovi.
2. Alica zmeria stav svojich častíc pomocou otočenia ich bázy buď o 0°, 45° alebo 22.5°, zatiaľ čo Bob zmeria stav svojich častíc pomocou otočenia ich bázy buď o 0°, -22.5° alebo 22.5°. Každý z nich si zaznamenáva svoje merania a pomocou klasického komunikačného kanálu si dajú vedieť, aké rotácie bázy použili na svoje merania.
3. Svoje merania potom rozdelia do dvoch skupín: jedna z nich je G_1, do ktorej patria merania, pri ktorých zvolili iné rotácie bázy, a G_2, kde zvolili tie isté rotácie bázy.
4. Skupina G_1 slúži na detekciu narušiteľov. Kedy si Bob a Alica pošlú výsledky meraní, pri ktorých zvolili iné bázy, a vypočítajú pomocou korelačných koeficientov meraní hodnotu *S*, za použitia Bellovej nerovnosti, kedy by *S* malo vyjsť $2\sqrt{2}$. Ak táto hodnota nevyjde, znamená to že komunikácia bola narušená a Alica a Bob protokol prerušia.
5. Ak je kanál bezpečný, tak merania zo skupiny G_2, pri ktorých zvolili rovnaké rotačné bázy, sa použijú ako súkromný kľúč.

Tieto dva protokoly sú základom kvantovej distribúcie kľúčov, na základe ktorých vznikli ďalšie a modernejšie protokoly. Kvantová kryptografia je dôležitou súčasťou zabezpečenia komunikácie v budúcnosti, kedy klasické šifry budú prelomené pomocou kvantových počítačov. [30]

2 KVANTOVÉ POČÍTANIE

Slovo kvantový popisuje minimálne množstvo fyzickej kvantity, ktoré môže existovať popri fyzikálnych zákonoch v prírode. Popisuje vlastnosti častíc, ktoré tvoria svetlo a hmotu, ktoré sa správajú celkom inak, než bežné objekty, s pravdepodobnosťou ako hlavným motorom ich správania. [31]

2.1 Kvantový bit

2.1.1 Klasický bit

Klasické počítače používajú binárnu sústavu (1 alebo 0), aby uchovávali a manipulovali s dátami. Bit môže mať vždy iba jeden z dvoch stavov: buď 1 alebo 0. Je buď zapnutý, alebo vypnutý. Vďaka tomu, že bit môže reprezentovať iba jeden z dvoch stavov, môžeme vypočítať, koľko bitov je potrebných na adresovanie určitého množstva dát. Napríklad, 1 bit môže teoreticky obsahovať buď 1 alebo 0, čiže dva bity informácií, ale vo výsledku vždy bude obsahovať iba jeden z daných stavov. A to pred, počas, aj po jeho pozorovaní. [32]

2.1.2 Bit a qubit

Zatiaľ čo bit je základný koncept klasickej informatiky, kvantová informatika je postavená na podobnom koncepte, ktorý sa nazýva kvantový bit, alebo skrátene, qubit. Kvantové bity sú, na rozdiel od bitov, často reprezentované ako matematické objekty. Platí, že kvantové bity, tak isto ako obyčajné bity, sú realizované ako fyzické systémy, ale reprezentácia v abstraktnej podobe pomáha zostaviť všeobecnú teóriu kvantových výpočtov a kvantovej informácie, ktorých realizácia nezávisí od konkrétneho systému. Presne ako klasický bit, má qubit svoj stav. Buď $|0\rangle$ alebo $|1\rangle$, ktoré korešpondujú so stavmi 0 a 1, pri klasickom bite. Spôsob zápisu „$|\ \rangle$“ je nazývaný Diracova notácia, a je to štandardný zápis v stavoch kvantovej mechaniky. [18]

2.1.3 Superpozícia

Rozdiel medzi bitmi a qubitmi je, že qubit môže byť aj v stave inom, než je $|0\rangle$ a $|1\rangle$. Je totiž tiež možné, aby vytvoril lineárnu kombináciu stavov, tiež nazývanú superpozícia. Tento stav je kombináciou stavov $|0\rangle$ a $|1\rangle$. Ak označíme tento stav ako $|\psi\rangle$, tak superpozícia sa dá zapísať takto:

$$(1): |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

V rovnici (1) predstavujú α a β komplexné čísla a reprezentujú amplitúdy pravdepodobnosti. Inými slovami, stav qubitu je vektor v dvojdimenzionálnom komplexnom vektorovom priestore. Jednotlivé stavy $|0\rangle$ a $|1\rangle$ sú známe ako stavy výpočtovej bázy. Aj keď môže qubit byť v superpozícii stavov $|0\rangle$ a $|1\rangle$, keď sa zmeria, nájde sa buď v stave $|0\rangle$ alebo v stave $|1\rangle$. [18] [33] [34]

Pri bite je možné jednoznačne určiť, či je v stave 0 alebo 1. Počítače toto robia neustále keď sa snažia získať informácie z pamäti. Pri kvantových počítačoch sa nedá určiť ich kvantový stav, teda hodnoty α a β. Na miesto toho, kvantová mechanika hovorí, že je možné získať iba obmedzené informácie o danom kvantovom stave. Keď sa meria qubit, vyjde buď výsledok $|0\rangle$, s pravdepodobnosťou $|\alpha|^2$ alebo výsledok $|1\rangle$, s pravdepodobnosťou $|\beta|^2$. Samozrejme, $|\alpha|^2 + |\beta|^2 = 1$, keďže pravdepodobnosť sa musí rovnať jednej. Geometricky, sa toto dá interpretovať ako podmienka, že stav qubitu musí byť normalizovaný na dĺžku 1, a teda, vo všeobecnosti, stav qubitu je jednotkový vektor v dvojdimenzionálnom komplexnom vektorovom priestore, tiež nazývanom ako Hilbertov priestor. [33] [35]

2.2 Viacero kvantových bitov

Ak sa k jednému qubitu pridá ďalší, tak keby to boli obyčajné bity, tak by mohli byť v štyroch stavoch, 00, 01, 10 a 11. Systém s dvomi kvantovými bitmi má tiež štyri možné stavy, $|00\rangle$, $|01\rangle$, $|10\rangle$ a $|11\rangle$. Dva qubity môžu tiež byť v superpozícii týchto štyroch stavov. To znamená, že kvantový stav dvoch kvantových bitov zahŕňa priradenie komplexného koeficientu, nazývaného amplitúda pravdepodobnosti. Kvantový stav systému s *n* qubitmi je definovaný 2^n amplitúdami. [33]

2.2.1 Interferencia

Výsledkom superpozície je interferencia. Stavy kvantových bitov sa navzájom môžu rušiť, pretože každý stav je popísaný amplitúdou pravdepodobnosti. Konštruktívna interferencia amplitúdu zvyšuje, zatiaľ čo pri deštruktívnej interferencii dochádza k vzájomnému rušeniu amplitúdy. Tento jav sa využíva pri kvantových algoritmoch a spolu s kvantovým previazaním umožňuje kvantovým počítačom obrovské zrýchlenie oproti počítačom klasickým. [36]

2.2.2 Kvantové previazanie

Viacero kvantových bitov môže mať vlastnosť kvantového previazania. Previazané kvantové bity spolu vždy korelujú, aby vytvorili jeden systém. Aj keď by boli od seba nekonečne vzdialené, meranie jedného kvantového bitu umožňuje poznať stav toho druhého bez toho, aby musel byť meraný. Tento jav je potrebný na efektívne kvantové počítanie a využíva sa pri kvantových algoritmoch, ako napríklad pri Shorovom alebo Groverovom algoritme. [36]

2.2.3 Kvantová Fourierova transformácia

Fourierova transformácia sa využíva pri klasických počítačoch, napríklad pri spracovávaní signálov alebo teórii komplexnosti. Kvantová Fourierova transformácia je kvantovou implementáciou diskrétnej Fourierovej transformácie na amplitúdach pravdepodobnosti. Jej hlavnou úlohou je, že medzi kvantovými bitmi vyvoláva kvantovú interferenciu, ktorá je buď konštruktívna alebo deštruktívna. Týmto uvádza register do stavov, v ktorých jeho hodnoty budú namerané s rôznymi pravdepodobnosťami.

Kvantová Fourierova transformácia je súčasťou mnohých kvantových algoritmov, napríklad Shorovho faktorizačného algoritmu. [37] [38]

2.3 Typy kvantových bitov

2.3.1 Supravodivé kvantové bity

Tieto qubity sú tvorené zo supravodivých elektrických obvodov a používajú ich spoločnosti IBM a Google. Supravodiče sú materiály, ktoré sa pri ochladení menia z normálneho stavu do supravodivého, kde nie je žiadny odpor prúdeniu elektrického prúdu. Medzi výhody takýchto kvantových bitov patrí rýchly prevádzkový čas. To znamená, že oproti iným druhom kvantových bitov, môžu byť výpočty vykonávané rýchlejšie.

Hlavnou nevýhodou takýchto qubitov je, že sa veľmi rýchlo dostanú do stavu dekoherencie, čo je strata kvantových vlastností daného qubitu. Ich životnosť je veľmi krátka. [39]

2.3.2 Zachytené atómy a ióny

Keď sú zachytené lasermi atómy alebo ióny (nabité atómy), tak sa správajú ako kvantové bity. Spoločnosti, využívajúce takéto qubity, sú napríklad Ion Q, Alpine Quantum Technologies alebo Eleqtron. Takéto kvantové bity doslova zachytávajú ióny pomocou magnetic-

kých polí a držia ich na jednom mieste. Najvzdialenejší elektrón obiehajúci jadro atómu demonštruje stav superpozície a využíva sa ako kvantový bit.

Hlavnou výhodou takýchto kvantových bitov je, že sú odolnejšie než iné druhy qubitov. Dokážu pracovať aj za izbovej teploty, ale najlepší výkon podávajú pri teplote do 4 kelvinov.

Oproti supravodivým qubitom sú o niečo pomalšie a ich údržba je náročnejšia, keďže ióny musia byť udržiavané vo vákuu. [39]

2.3.3 Fotónové kvantové bity

Fotónové qubity využívajú častice svetla, aby prenášali a spracovávali informácie. Jednotlivé kvantové bity sú samostatné fotóny. Počítač s fotónmi pracuje pomocou zrkadiel, rozdeľovačov lúčov a fázových meničov.

Veľkou výhodou fotónových qubitov je, že môžu pracovať v izbovej teplote a sú tiež menej citlivé na prostredie, čo znamená že si svoje kvantové vlastnosti uchovávajú na dlhšiu dobu. Ďalšou výhodou je, že sa dajú integrovať do optických systémov. Toto by mohlo znamenať prepojenie viacero kvantových počítačov cez optické siete, aby vytvorili jeden kvantový počítač s milión a viac kvantovými bitmi.

Nevýhoda je, že konštrukcia systému, ktorý by využíval veľké množstvo takýchto qubitov je zatiaľ náročná. [39]

2.4 Hadamardovo hradlo

Hadamardovo hradlo je jednoqubitové hradlo, ktoré aplikuje Hadamardovu transformáciu na jeden qubit. To spôsobí, že sa z $|0\rangle$ stane $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ a z $|1\rangle$ sa stane $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$, čiže vznikne superpozícia týchto základných stavov. Toto hradlo sa využíva pri kvantových algoritmoch, ako napríklad Deutsch-Joza algoritmus alebo Groverov algoritmus. [40]

2.5 Kvantový počítač

Kvantové počítače využívajú vlastnosti kvantovej mechaniky na robenie výpočtov rýchlejšie a efektívnejšie, než súčasné počítače. Využívajú k tomu vlastnosti, ako je superpozícia a kvantové previazanie, pomocou ktorých je možné dosiahnuť exponenciálne množstvo paralelizmu. [41]

Kvantové počítanie spája prvky kvantovej mechaniky, informačnej teórie a aspekty počítačovej vedy. Veľa zaujímavých problémov sa na klasickom počítači nedá vyriešiť z dôvodu nedostatku výkonnosti. Kvantové počítače prinášajú nové algoritmy, pre ktoré tieto problémy sú riešiteľné. [33] [41]

V súčasnosti sú kvantové počítače veľmi citlivé. Teplo, elektromagnetické polia a kolízie s molekulami vzduchu môžu zapríčiniť, aby kvantový bit stratil svoje kvantové vlastnosti. Tento proces je zvaný tiež kvantová dekoherencia a spôsobuje zlyhanie celého systému. V súčasnosti je možné vykonať iba desiatky operácií na kvantových počítačoch predtým, než nastane pri kvantových bitoch dekoherencia. Kvantové počítače musia kvantové bity ochraňovať pomocou fyzickej izolácie, chladenia alebo kontrolovaným prísunom energie. Každá odchýlka od očakávanej výstupnej hodnoty je nežiaduca a nazýva sa všeobecne šum. Na korekciu chýb je potrebné veľké množstvo dodatočných kvantových bitov. Tejto korekcii sa tiež hovorí kvantová korekcia chýb. [42] [43]

2.6 Kvantová korekcia chýb

Kvantová korekcia chýb je jediný spôsob, ako do veľkej miery znížiť množstvo chýb, pri kvantových počítačoch. Pri tomto postupe sa využíva veľké množstvo prebytočných kvantových bitov a kód, pre kvantovú korekciu chýb, ktorý využíva tento nadbytok qubitov, aby zaistil stále qubity s veľmi malými mierami chybovosti. Takéto kvantové bity sa nazývajú qubity odolné voči chybám alebo aj logické qubity. Stav týchto nadbytočných kvantových bitov sa pravidelne kontroluje a klasický počítač vyhodnotí, či je daný qubit chybný. Vďaka tejto informácii sa daná chyba môže opraviť. Cieľom kvantovej korekcie chýb je zabezpečiť kvantovým algoritmom úplne bezchybné fungovanie. [44]

2.7 Typy kvantových počítačov

2.7.1 Kvantový žíhací počítač

Kvantový žíhací počítač je najjednoduchší na zloženie, ale takisto je najmenej výkonný z kvantových počítačov. Súčasné klasické počítače tento druh kvantového počítača dokážu predbehnúť vo výkonnosti, pri všedných úlohách, ako je napríklad hranie hier, písanie emailov, tvorba videa a podobne. Kde kvantový žíhací počítač vyniká, je v schopnosti faktorizácie čísiel a pri riešení optimalizačných problémov. S takýmto typom kvantového počítača prišla spoločnosť D-Wave. Táto spoločnosť bola prvou na svete, ktorá dala do pre-

daja počítače využívajúce kvantové výpočty. Čip, ktorý pracuje na základe kvantového žíhania, má značne obmedzenú funkcionalitu. Ako už bolo spomenuté, takýto čip funguje pre kvantové výpočty, ktoré riešia optimalizačné úlohy. V prípade kvantových žíhacích počítačov, panuje vo vedeckej oblasti konsenzus, že takýto typ kvantového počítača nemá žiadne známe výhody, oproti konvenčným počítačom. [45] [46]

2.7.2 Analógový kvantový počítač

Analógový kvantový počítač je rýchlejší a ponúka značné výpočtové výhody oproti klasickým počítačom. Na takomto kvantovom počítači pracuje niekoľko spoločností, vrátane Google, Microsoft, IBM Q, Rigetti, Honeywell a IonQ. Táto forma kvantového počítača je veľmi komplikovaná na zostavenie, ale ponúka veľké pokroky v riešení problémov v kvantovej chémii, materiálnej vede, kvantovej dynamike, vzorkovaní a problémov optimalizácie. Analógový kvantový počítač môže byť použitý na prelomenie súčasných šifrovacích štandardov, za použitia napríklad Shorovho alebo Groverovho algoritmu. [45]

2.7.3 Univerzálny kvantový počítač

Univerzálny kvantový počítač je najkomplexnejší na zloženie, ale zároveň najviac výkonný. Mal by mať viac než 100 000 qubitov a má obrovské energetické nároky na fungovanie. Okrem toho, univerzálny kvantový počítač potrebuje kryogénny chladiaci systém, aby zachoval teplotu absolútnej nuly, na jeho správne fungovanie. Firma IBM navrhuje čip pre takýto druh kvantového počítača a takisto robí v tejto oblasti veľa výskumu pre software aj hardware. Zatiaľ sa nevie, na čom pracujú iné firmy, ale s veľkou pravdepodobnosťou budú v tejto oblasti zainteresované aj firmy Google a Microsoft. Univerzálne kvantové počítače môžu byť použité na strojové učenie, kvantovú dynamiku, problémy optimalizácie, kvantovú biochémiu a podobne. Takýto počítač dokáže prelomiť určité typy šifrovania rýchlejšie, než akýkoľvek iný počítač. [45]

2.8 Využitie kvantových počítačov

V predchádzajúcich podkapitolách bolo vysvetlené, čo sú kvantové počítače a ich typy. V tejto podkapitole sa preberá, prečo sú vlastne kvantové počítače dôležité pre rozvoj ľudstva a v akých oblastiach môžu ľudstvu pomôcť.

2.8.1 Strojové učenie a umelá inteligencia

S príchodom kvantových počítačov sa v niektorých prípadoch exponenciálne zvýši výkonnosť výpočtových zariadení. Umelá inteligencia a strojové učenie sa v širokej škále používajú už v súčasnosti, napríklad pri rozpoznávaní hlasu, obrazu alebo textu. Pre klasické počítače je veľmi náročné tieto veci vykonávať rýchlo a presne. Kvantové počítače môžu pomôcť riešiť tieto komplexné problémy omnoho efektívnejšie. [47]

2.8.2 Kybernetická bezpečnosť

V súčasnosti je online svet, s narastajúcim počtom kybernetických útokov, veľmi zraniteľný. Kvantové počítanie za pomoci strojového učenia môže pomôcť pri vynaliezaní rôznych techník a nástrojov, na obranu proti kybernetickým hrozbám. Takisto môže pomôcť vymyslieť nové šifrovacie metódy. [47]

2.8.3 Biologické a chemické inžinierstvo

Táto oblasť zahŕňa manipuláciu a objavovanie molekúl. Súčasťou toho je aj skúmanie pohybu a interakcie subatomárnych častíc (kvantová mechanika). Jednou z motivácií Richarda Feynmana postaviť kvantový počítač, bola práve simulácia kvantovej mechaniky. Tým, ako sa molekuly stávajú komplexnejšími, počet ich možných konfigurácií exponenciálne rastie, čím sa z tohto problému stáva kombinatorický príklad, ktorý je vhodný pre kvantové počítače. Niektoré existujúce kvantové počítače už dokázali simulovať niektoré jednoduché chemické reakcie, vďaka čomu bude možné v budúcnosti simulovať čoraz zložitejšie chemické procesy. Kvantové počítače preto budú dôležité pri objavovaní nových materiálov a vývoji nových liekov. [47] [48]

Toto sú len niektoré z možných využití kvantových počítačov. Medzi ďalšie využitia, patrí napríklad lepšia schopnosť predpovedať počasie, vylepšenie procesu výroby alebo využitie v oblasti financií. [47]

2.9 Súčasné kvantové počítače

2.9.1 IBM

Najnovší kvantový čip od IBM, predstavený 15. novembra 2021, obsahuje 127 kvantových bitov, čo z neho robí prvé zariadenie s trojciferným počtom kvantových bitov. Tento čip sa nazýva *Eagle* a je iba prvým krokom v pláne tejto firmy, ktorá plánuje v roku 2022 vyrobiť

433-qubitový kvantový procesor, nasledovaný ďalším, s 1121 kvantovými bitmi zvaným *Condor* v roku 2023. Cieľ tejto spoločnosti je zostaviť kvantový počítač s miliónom kvantových bitov. Dátum pre tento ambiciózny cieľ doposiaľ nešpecifikovali.[1] [49] [50]

2.9.2 Google

V roku 2019 spoločnosť Google vyhlásila kvantovú nadradenosť, keď ich kvantový počítač s procesorom zvaným *Sycamore*, ktorý obsahuje 53 kvantových bitov, vykonal výpočet, ktorý je na klasickom počítači veľmi náročné vykonať. Google tvrdí, že ich kvantový počítač urobil tento výpočet za 200 sekúnd, pri čom klasickému superpočítaču by to trvalo vyše 10 000 rokov. Toto tvrdenie konkurencia Google vyvrátila. IBM tvrdí, že daný výpočet by superpočítaču trval 2.5 dňa.

Spoločnosť Google chce do konca aktuálneho desaťročia, teda do roku 2029, postaviť kvantový počítač s 1 000 000 kvantovými bitmi. Spoločnosť si myslí, že im takýto prístroj dokáže pomôcť vyriešiť klimatickú krízu, hladomor a vývoj v oblasti medicíny. V roku 2021, preto Google otvoril areál *Quantum AI* v Santa Barbare, ktorý obsahuje kvantové dátové centrum, laboratórium na výskum hardware pre kvantové počítače a továrne na výrobu kvantových čipov.[2] [51]

2.9.3 D-Wave

Spoločnosť D-Wave je prvou spoločnosťou na svete, ktorá priniesla na trh funkčný kvantový počítač v roku 2011. Táto spoločnosť sa zameriava na kvantový žíhací počítač. Takýto kvantový počítač je vhodný iba pre určité matematické príklady. Aj v minulých rokoch, kedy konkurenčné spoločnosti pracovali na vývoji primitívnych analógových a univerzálnych kvantových počítačov, D-Wave zostalo pri kvantových žíhacích počítačoch. Postupne zlepšili svoje prístroje a momentálne predávajú, najmenej v jednej oblasti, najvýkonnejší kvantový počítač na svete. Nedávno D-Wave oznámil, že plánuje zostrojiť kvantový univerzálny počítač a ponúkne zákazníkom možnosť na ňom, spolu s ich najnovším žíhacím počítačom, spúšťať výpočty cez cloud.

---

[1] https://www.science.org/content/article/ibm-promises-1000-qubit-quantum-computer-milestone-2023

[2] https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor

Spoločnosť tvrdí, že jej cieľom je zostaviť 60-qubitový kvantový počítač do roku 2023 až 2024. Nasledovať bude 1000 qubitový počítač, kde najmenej 4 qubity budú logické.[3] [52]

[3] https://fortune.com/2021/10/05/quantum-computer-d-wave-google-ibm-gate-model/

3 KVANTOVÉ ALGORITMY

Kvantový algoritmus je taký, ktorý môže byť spustený na kvantovom počítači, a využíva vlastnosti kvantovej mechaniky. Kvantové algoritmy sú považované za oveľa rýchlejšie, než tie klasické. Toto zrýchlenie je možné vďaka tomu, že namiesto spúšťania daného algoritmu iba s jedným vstupom, ako sa to robí klasicky, môže byť algoritmus spustený s využitím kvantového paralelizmu a superpozície na všetkých možných vstupoch naraz. [53]

Kvantových algoritmov, ktoré sú lepšie než tie klasické, je pomerne málo. Toto je z dôvodu, že vymýšľanie dobrých kvantových algoritmov je pomerne ťažké. Existujú na to minimálne dva dôvody. Prvým z nich je, že vymýšľanie či už klasických alebo kvantových algoritmov nie je tak celkom jednoduché. Dokonca aj algoritmy na riešenie jednoduchých problémov nie sú jednoduché na vymyslenie. Kvantové algoritmy sú o to ťažšie vymyslieť, pretože sa vyžaduje, aby boli lepšie než tie klasické. Druhý dôvod je, že ľudská intuícia je oveľa lepšie adaptovaná na klasický svet než na ten kvantový. [33]

3.1 Prvé kvantové algoritmy

3.1.1 Deutschov algoritmus

V roku 1985 vydal David Deutsch, jeden zo zakladateľov kvantového počítania, prelomový článok, ktorý popisoval kvantové Turingove stroje a kvantové počítanie. Tento článok obsahoval aj prvý algoritmus, ktorý dokazoval, že kvantové algoritmy môžu byť oveľa rýchlejšie, než tie klasické. [53]

Deutschov algoritmus spája kvantový paralelizmus s vlastnosťou kvantovej mechaniky zvanej interferencia. Jedná sa o najjednoduchší kvantový algoritmus, ktorého cieľom je určiť, či je funkcia $f: \{0,1\} \rightarrow \{0,1\}$ konštantná alebo vyvážená, pri jedinom vyčíslení danej funkcie, bez znalosti, ako je funkcia definovaná. Táto funkcia je konštantná, ak $f(0) = f(1)$ a vyvážená, ak $f(0) \neq f(1)$. Tento problém je v reálnom svete v podstate nevyužiteľný, ale dokázalo sa na ňom to, že kvantové počítače môžu riešiť problémy rýchlejšie, než tie klasické. [33] [54]

Klasický počítač by totiž na vyriešenie tohto problému potreboval vyčísliť f pre jeden vstup, a potom pre druhý. Čiže, na určenie výsledku potrebuje dve operácie. Pri kvantovom počítači, pomocou superpozície stavov, je možné vyčísliť obidva vstupy naraz. [54]

3.1.2 Deutsch-Joza algoritmus

Deutsch-Jozov algoritmus je generalizáciou Deutschovho algoritmu. Tento algoritmus pomáha určiť, či je funkcia od $\{0,1\}^n$ do $\{0,1\}$ konštantná alebo vyvážená. Premisa je tá istá, ale tentokrát má funkcia viacero vstupov. Ak je funkcia konštantná, tak je výsledok rovnaký pre všetky vstupné hodnoty x. Ak je funkcia vyvážená, tak $f(x) = 0$ pre polovicu výstupov a $f(x) = 1$ pre druhú polovicu výstupov. Pri Deutschovom algoritme stačilo dať do superpozície dva možné vstupy. Pri tomto algoritme je potrebné do superpozície dať všetkých 2^n možných vstupov. [53] [54]

3.1.3 Simonov algoritmus

Simonov algoritmus bol prvý kvantový algoritmus, ktorý dokázal exponenciálne zrýchlenie oproti klasickým počítačom. Zatiaľ čo na klasickom počítači je tento problém riešiteľný v exponenciálnom čase, na kvantových počítačoch sa dá vyriešiť v čase polynomiálnom. Na rozdiel od predchádzajúcich algoritmov, musí Simonov algoritmus byť spustený niekoľkokrát po sebe.

Tento algoritmus rieši Boolovu funkciu typu f: $\{0,1\}^n \rightarrow \{0,1\}^n$, ktorá je predaná v čiernej skrinke. Ďalej, existuje skrytý binárny reťazec s taký, že $f(x) = f(y)$ presne vtedy, keď $y = x$ alebo $y = x \oplus s$, kde $\oplus$ reprezentuje výlučný logický súčet (XOR). Hodnoty funkcie f sa opakujú v určitom vzorci a ten vzorec je určený reťazcom s. Reťazec s sa nazýva periódou funkcie f. Cieľom Simonovho algoritmu je určiť s.

Tento algoritmus inšpiroval Petera Shora, ktorý vymyslel Shorov faktorizačný algoritmus, ktorý tiež využíva koncept hľadania periódy vo funkcii. [54] [55]

3.2 Kvantové algoritmy v kryptografii

Algoritmy, ktoré boli doteraz spomenuté, sú prvé kvantové algoritmy, ktorých účelom bolo dokázať výhodu kvantových počítačov v riešení komplexných problémov, oproti klasickým počítačom. Nasledujú algoritmy, ktoré majú využitie v oblasti modernej kryptografie a môžu ohroziť bezpečnosť najpoužívanejších kryptografických systémov.

3.2.1 Shorov faktorizačný algoritmus

V roku 1994, Peter Shor vynašiel kvantové algoritmy na faktorizáciu vysokých čísiel a riešenie diskrétneho logaritmu, pomocou ktorých je možné prelomiť Rivest-Shamir-

Adleman (RSA) kryptosystém, s verejným kľúčom a výmenu kľúčov Diffie-Hellman, pomocou kvantových počítačov. [1]

Shorov algoritmus na faktorizáciu celých čísel je postup, ktorý pracuje v polynomiálnom čase, čím takmer exponenciálne zrýchľuje aktuálne riešenie problému faktorizácie. Shorov algoritmus tento problém rieši pomocou kvantového paralelizmu. Algoritmus hľadá prvočíselné súčinitele nepriamo. Faktorizáciu premieňa na problém hľadania periódy určitej periodickej funkcie. [25] [56]

Za použitia kvantových počítačov, s dostatkom stálych kvantových bitov, Shorov algoritmus dokáže faktorizovať veľmi vysoké čísla v sekundách až minútach. Shorov algoritmus umožňuje kvantovým počítačom faktorizovať oveľa rýchlejšie, použitím vzorca, ktorý náhodne skúsi trafiť jedno z prvočísiel a zmení ho na oveľa presnejší tip, pomocou ktorého rýchlo nájde jednotlivé správne prvočísla. Shorov algoritmus používa matematickú väzbu medzi danými dvomi prvočíslami takým spôsobom, aby drasticky eliminoval počet pokusov potrebných na ich uhádnutie. Stále je potrebné veľké množstvo pokusov, ale ak sa tieto pokusy robia s využitím kvantovej vlastnosti superpozície, môžu byť tieto pokusy vygenerované takmer okamžite. Medzi všetkými týmito pokusmi sú aj správne prvočísla. [32]

Predpokladá sa, že iné algoritmy vymyslené po Shorovom, budú ešte rýchlejšie a efektívnejšie, než Shorov algoritmus. Napríklad algoritmus GEECM je v niektorých prípadoch ešte rýchlejší, než ten Shorov. To znamená, že Shorov algoritmus je iba spodnou priečkou v rýchlej faktorizácii čísiel. Je veľmi pravdepodobné, že tento problém sa dá vyriešiť ešte rýchlejšie alebo za použitia menšieho počtu qubitov, ako Shor predpokladal. [32]

3.2.2 Groverov algoritmus

Groverov algoritmus je jedným z najdiskutovanejších a najobľúbenejších kvantových algoritmov. Tento algoritmus patrí medzi kvantové vyhľadávacie algoritmy. V podstate dokázal, že nájdenie hľadaného prvku v neusporiadanej dátovej štruktúre, môže byť do značnej miery urýchlené použitím kvantových počítačov. Grover povedal, že namiesto potreby rátania všetkých *N* možností po jednom, lineárne, tak ako na klasickom počítači, na kvantovom počítači by stačilo rátať $\sqrt{N}$ možností, k dosiahnutiu výsledku s použitím kvantového počítača s *log(N) + 1* kvantovými bitmi. Groverov algoritmus vedie ku štvornásobnému zrýchleniu oproti klasickým vyhľadávacím algoritmom. [32]

Ak má matematický problém 1 000 000 možných riešení, klasický počítač by potreboval v najhoršom prípade 1 000 000 operácií, aby našiel správne riešenie. Groverov algoritmus dokázal, že kvantové počítače so 7 qubitmi (log(1000000) + 1) by toto riešenie našili pri najviac 1000 operáciách. [32]

II. PRAKTICKÁ ČÁST

4 PREHĽAD KVANTOVÝCH ALGORITMOV

Táto kapitola obsahuje charakterizáciu vybraných kvantových algoritmov, ktoré ohrozujú niektoré šifrovacie systémy modernej kryptografie. Algoritmy sú vždy popísané s ohľadom na niekoľko kritérií, a to popularita, druh, časová zložitosť, implementácia, funkcionalita a šifry, ktoré daný algoritmus ohrozuje. V prípade, že bol algoritmus implementovaný, sú pri jednotlivých algoritmoch uvedené aj ukážky kódu v jazyku python.

4.1 Shorov faktorizačný algoritmus

Popularita

Články Petera Shora, v ktorých predstavuje svoje algoritmy, s názvami *Algorithms for quantum computation: discrete logarithms and factoring*, a *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, boli dohromady citované 20 315 krát, z čoho prvý článok, z roku 1994, bol citovaný 8455 krát a druhý, z roku 1999, 11 842 krát. Ide o zatiaľ najpopulárnejšie a najznámejšie kvantové algoritmy. Z týchto dvoch algoritmov sa väčšina pozornosti upriamuje na faktorizačný algoritmus. [57]

Druh

Tento algoritmus slúži na prvočíselný rozklad veľkých čísiel. Tento problém sa považoval za veľmi náročný, a pri číslach s tisíc alebo viac ciframi, sa považovalo, až do objavenia tohto algoritmu, za nemožné ho vyriešiť. [58]

Časová zložitosť

Oproti klasickým počítačom, ktoré dokážu faktorizovať pri časovej zložitosti e, Shorov faktorizačný algoritmus to dokáže pri časovej zložitosti $\log N$, čo predstavuje exponenciálne zrýchlenie oproti klasickým algoritmom. [59]

Implementácia

Shorov faktorizačný algoritmus bol zatiaľ úspešne implementovaný iba na kvantových počítačoch s veľmi malým počtom kvantových bitov. Problém pri implementovaní Shorovho algoritmu na kvantovom počítači s väčším počtom kvantových bitov, je v tom, že vzniká obrovský šum, ktorý spôsobuje veľké problémy pre stabilitu a spoľahlivosť systému. Prvýkrát sa to podarilo firme IBM v roku 2001, kedy bol tento algoritmus úspešne spustený na 7-qubitovom systéme a podarilo sa pomocou neho rozložiť na prvočísla číslo

15. V roku 2012 bolo, pomocou Shorovho algoritmu na kvantovom počítači, faktorizované číslo 21.

Na prelomenie súčasných najpoužívanejších šifrovacích systémov s verejným kľúčom by Shorov algoritmus potreboval kvantový počítač s aspoň 4000 veľmi stabilnými kvantovými bitmi. [31] [32]

Funkcionalita

Shorov algoritmus slúži na nájdenie súčiniteľov obrovského čísla N, a funguje podľa [60] takto:

1. Vygeneruje sa pseudo-náhodné číslo *g*, ktoré je menšie než N
2. Pomocou Euklidovho algoritmu sa zistí najväčší spoločný deliteľ *N* a *g.* Ak je tento deliteľ väčší než 1, tak bol nájdený súčiniteľ, ktorým vydelíme *N*, a tak je nájdený aj druhý súčiniteľ. Ak je deliteľ 1, tak sa pokračuje.
3. Pomocou kvantovej mechaniky sa nájde také *p*, pre ktoré platí, že $g^{p/2} \pm 1$, majú najväčší spoločný deliteľ s *N* väčší ako 1, a teda našli sa hľadané súčinitele. Musí platiť aj to, že *p* je párne.
   3.1. V podstate sa hľadá *p*, pre ktoré platí, že $g^p = m*N+1$, kde *m* značí násobok čísla *N*. Na to je potrebné využiť kvantový počítač, ktorý umocní *g* na akúkoľvek hodnotu, a potom vypočíta o koľko je výsledná hodnota väčšia než *N*.
   3.2. Ak sa začne so superpozíciou všetkých čísel až po *N*, tak kvantový počítač vráti superpozíciu g^1, g^2, g^3... a potom superpozíciu rozdielov medzi týmito číslami a *N*.
   3.3. Ak sa zmeria stav superpozície týchto rozdielov, výsledkom bude jeden z nich. Toto spôsobí, že v kvantovom stave zostane superpozícia tých výsledkov, pri ktorých po umocnení a odrátaní od *N*, vychádza presne ten rozdiel, ktorý vyšiel ako výsledok merania. O týchto výsledkoch s istotou platí, že sú od seba vzdialené o periódu *p*, teda o frekvenciu *1/p*.
   3.4. Ďalší krok je na túto superpozíciu uplatniť kvantovú Fourierovu transformáciu, ktorá túto frekvenciu zachytí, a výsledkom bude superpozícia násobkov frekvencie *1/p*, teda $|1/p\rangle + |2/p\rangle + |3/p\rangle + |4/p\rangle$...
   3.5. Ďalším krokom je zmerať túto superpozíciu. Výsledkom tohto merania bude jedna z hodnôt tejto superpozície. Napríklad $|5/p\rangle$. Potom sa toto meranie zopakuje, a výsledkom bude napríklad $|2/p\rangle$. Tento krok sa opakuje dovtedy, pokiaľ nebude možné vypočítať hodnotu 1/p.

4. Potom sa vypočíta $g^{p/2} + 1$ a zistí sa, či nevyšlo samotné číslo *N*. Ak áno, tak sa musí zvoliť iné číslo *g*. Ak nie, tak sa pomocou Euklidovho algoritmu spočíta najväčší spoločný deliteľ tohto čísla a čísla *N*. Ak je výsledok väčší ako 1, tak vyšiel prvý súčiniteľ obrovského čísla *N*.
5. Ďalej sa vypočíta $g^{p/2} - 1$ a opäť sa využije Euklidovho algoritmu na zistenie druhého spoločného deliteľa s *N*.

Šifry, ktoré ohrozuje

Úspešne implementovaný Shorov faktorizačný algoritmus na univerzálnom kvantovom počítači, by ohrozil veľkú časť modernej asymetrickej kryptografie. Medzi hlavné šifrovacie systémy, ktoré sú v ohrození patrí RSA, čo je jeden z najpoužívanejších šifrovacích systémov súčasnosti.

Ukážka kódu

Qiskit je open-source nástroj od IBM, pre vývoj softvéru pre prácu s kvantovými počítačmi. Program, ktorý sa mi podarilo vďaka tomuto nástroju spustiť na simulovanom kvantovom počítači cez API, úspešne zfaktorizoval číslo 15. Shorov algoritmus bol implementovaný v programovacom jazyku python, a vďaka Qiskit, ktoré má zabudovanú funkciu pre tento algoritmus zvanú *Shor(N)*, ktorá vypočíta súčinitele čísla *N*, je programovanie a simulácia daného algoritmu veľmi jednoduchá. Stačí vložiť knižnice, vyvinuté od IBM nazvané Qiskit, získať API kľúč od IBM Quantum a zavolať ich implementáciu Shorovho algoritmu. Na Obrázku 1 je znázornený upravený kód Shorovho algoritmu, ktorý som prebral z [61]. Obrázok 2 zobrazuje výstup tohto algoritmu, kde je správny výsledok faktorizácie čísla 15. Na Obrázku 3 je znázornený priebeh algoritmu na simulátore kvantových zariadení, s názvom *ibmq_qasm_simulator*.

Kód v jazyku python vyzerá takto:

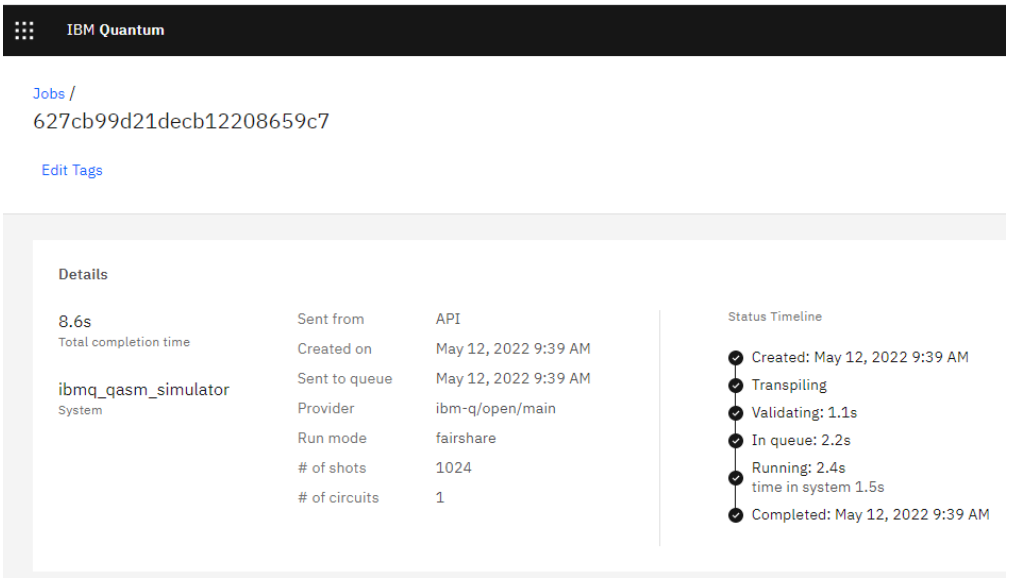
```
from qiskit import IBMQ
from qiskit.utils import QuantumInstance
from qiskit.algorithms import Shor

N = 15
IBMQ.enable_account('f887c6623d9abfc2d38bfde60567aac46d2e923d447faed8d97edb9ce81c
fe10e50b3bc4ba11b49ae1beafcbd73b488d2a014beca0ef6b65b64bc425f89e8dc4')
provider = IBMQ.get_provider(hub='ibm-q')

backend = provider.get_backend('ibmq_qasm_simulator')

quantum_instance = QuantumInstance(backend, shots=1024,
skip_qobj_validation=False)
shor = Shor(quantum_instance=quantum_instance)
result = shor.factor(N)

print(result)
```

Obrázok 1 Implementácia Shorovho algoritmu v pythone

S výstupom :

```
{'factors': [[3,5]], 'successful_counts': 2, 'total_counts': 4}
```

Obrázok 2 Výstup Shorovho faktorizačného algoritmu



Obrázok 3 Ukážka priebehu programu na simulátore kvantových zariadení

4.2 Groverov algoritmus

Popularita

Groverov kvantový algoritmus bol prvý krát popísaný v roku 1996 v článku nazvanom „A fast quantum mechanical algorithm for database search“. Odvtedy bol citovaný 7541 krát. Ide o druhý najznámejší a najpopulárnejší kvantový algoritmus. [62]

Druh

Groverov algoritmus je vyhľadávací. Nájde jedinečný prvok v neusporiadanej databáze. Ide o pravdepodobnostný algoritmus, čiže vracia výsledok ktorý je s vysokou pravdepodobnosťou správny. Táto pravdepodobnosť sa dá zvýšiť pomocou opakovania tohto algoritmu. [63]

Časová zložitosť

Zatiaľ čo klasický počítač by pri tomto hľadaní musel spraviť N krokov, Groverov algoritmus to zvládne za $\sqrt{N}$, čo z neho robí najrýchlejší kvantový algoritmus na vyhľadávanie v neusporiadanej databáze. Oproti klasickým algoritmom je štyrikrát rýchlejší, čo nie je exponenciálne zrýchlenie, ale ak je N vysoké číslo, tak je toto zrýchlenie značné. [63]

Implementácia

Tak isto ako Shorov algoritmus, aj Groverov algoritmus bol implementovaný na kvantových počítačoch s malým počtom kvantových bitov. Bol implementovaný na zariadeniach firmy IBM na 2-qubitovom, 3-qubitovom a 4-qubitovom kvantovom systéme. Teoreticky by mal Groverov algoritmus pri 3 iteráciách dosahovať presnosti 96%. Po testovaní algoritmu na zariadení IBM Q5 (s 5 kvantovými bitmi), sa preukázalo, že reálna presnosť bola niekde okolo 7%. Toto dokazuje, že existuje obrovská medzera medzi súčasnými kvantovými počítačmi, a teoretickým maximálnym výkonom takýchto zariadení. [64]

Funkcionalita

Groverov algoritmus rieši tento problém:

Nech má systém $N = 2^n$ stavov, ktoré sú označené $S_1, S_2 \ldots S_N$. Tieto 2^n stavov je reprezentovaných ako n-bitové reťazce. Ďalej nech existuje jedinečný stav S_v, pre ktorý platí že funkcia $f(S_v) = 1$, zatiaľ čo pre všetky ostatné S je funkcia $f(S) = 0$. Cieľom je nájsť stav S_v.

Priebeh algoritmu vyzerá takto:

1. Inicializácia systému do stavu superpozície využitím Hadamardovho hradla: $\left(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}} \ldots \frac{1}{\sqrt{N}}\right)$ teda pre každý stav N je rovnaká amplitúda.
2. Tento krok sa opakuje $O(\sqrt{N})$ krát.
    a. Nech je systém v akomkoľvek stave, v prípade $f(S) = 1$, fázovo sa otočí jeho amplitúda. Ak je $f(S) = 0$, stav zostáva nezmenený.
    b. Aplikuje sa rozptylová transformácia D, ktorá je definovaná takto:

$$D_{ij} = \frac{2}{N} \; ak \; i \neq j \; \& \; D_{ii} = -1 + \frac{2}{N}$$

Toto je známe ako fáza zosilnenia, všetky amplitúdy sa otočia podľa priemernej amplitúdy $\frac{1}{\sqrt{N}}$. Tým, že amplitúda nášho požadovaného výsledku bola premenená a všetky ostatné zostali také isté, toto otočenie zvýši amplitúdu nášho požadovaného výsledku, zatiaľ čo zmenší amplitúdy všetkých ostatných stavov.

3. Meranie výsledného stavu. Toto bude stav S_v s pravdepodobnosťou minimálne 50%.

Slučka v kroku č. 2 je najdôležitejšou časťou tohto algoritmu. Pre každú iteráciu tejto slučky sa amplitúda požadovaného stavu zvýši o $O(\frac{1}{\sqrt{N}})$. Ako výsledok, po $O(\sqrt{N})$ opakovaniach tejto slučky amplitúda, a teda pravdepodobnosť dosiahnutia požadovaného výsledku stúpa na O(1). [65]

Šifry, ktoré ohrozuje

Vďaka svojej rýchlej schopnosti vyhľadávania je Groverov algoritmus a jeho variácie, hrozbou pre niektoré symetrické šifry, ako napríklad AES a niektoré hashovacie funkcie. [32]

Ukážka kódu

Táto implementácia Groverovho algoritmu využíva framework Qiskit od IBM, ktorý umožňuje pomocou API prístup k reálnym kvantovým zariadeniam cez internet.

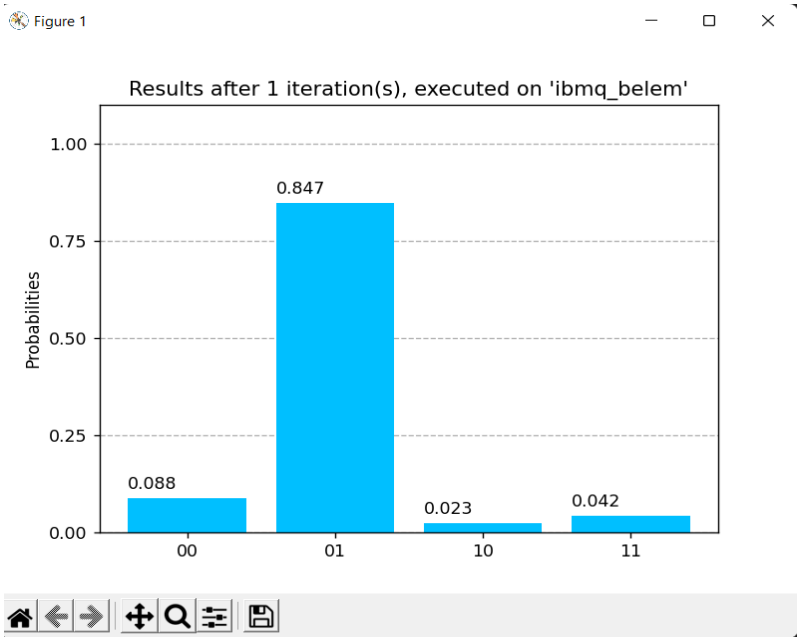
Program počíta s n-qubitovým registrom. Tento program (Obrázok 4) bol spustený pre n = 2, n = 3 a n = 4. Obrázok 5 zobrazuje výstup Groverovho algoritmu pri jednom opakovaní pre n = 2 v grafe, zatiaľ čo na Obrázku 6 je tento výstup zobrazený v konzole programu. Pri n = 2 vyšiel správny výsledok (01), pri 2000 meraniach, 1693 krát, teda s pravdepodobnosťou okolo 85%. Na Obrázku 7 je znázornený priebeh programu na kvantovom zariadení *ibmq_belem*. Pri n = 3, ktorý bežal na kvantovom zariadení *ibmq_quinto* vyšiel, pri hľadaní výsledku 000, správny výsledok s pravdepodobnosťou okolo 46%. Pre n = 4, pri 3 iteráciách a hľadaní čísla 0000, toto číslo vychádza iba v 11% prípadoch a začína byť ťažké rozoznať správny výsledok od nesprávnych výsledkov. Toto značí, že Groverov algoritmus zatiaľ nemôže byť naplno využitý kvôli praktickým limitom doterajších kvantových zariadení.

Pôvodný kód, pred jeho upravením, je z [66]. V ukážke je zobrazená najdôležitejšia časť kódu, a to inicializácia parametrov a spúšťanie kódu na dostupnom kvantovom zariadení, spolu so zobrazením výsledkov.

```
# veľkosť klasických a kvantových registrov
n = 4

 # veľkosť prehľadávaného priestoru
N = 2**n

 # ideálny počet opakovaní
k = floor(pi/4*sqrt(N))

 # simulácia na kvantovom počítači
IBMQ.enable_account('f887c6623d9abfc2d38bfde60567aac46d2e923d447faed8d97edb9ce81c
fe10e50b3bc4ba11b49ae1beafcbd73b488d2a014beca0ef6b65b64bc425f89e8dc4')
provider = IBMQ.get_provider(hub='ibm-q')
backend = least_busy(provider.backends(filters=lambda x:
                                       x.configuration().n_qubits >= n and
                                       not x.configuration().simulator and
                                       x.status().operational==True))
x.status().operational==True))
s = randrange(N)
s = bst(n,s)

print("BACKEND: " + str(backend))
print("SEARCHING FOR |" + s + ">")
print("REQUIRED ITERATIONS: " + str(k))

grc = QuantumCircuit(n,n)

 # vytvorenie počiatočnej superpozície
grc += gn(n,"h")

 # opakovanie až pokial nedosiahne ideálny počet opakovaní
for iteration in range(k):
    grc += grover_iteration(n,s)

 # meranie na konci
grc.measure(list(range(n)),list(range(n)))

 # počet meraní
shots = 2000

job_grc = execute(grc, backend, shots=shots)
job_monitor(job_grc)
result = job_grc.result()
comment = "executed on '" + str(backend) + "'"

counts = result.get_counts(grc)
print("RESULTS: " + str(counts))

show_results(counts,shots,k,comment)
```

Obrázok 4 Implementácia Groverovho algoritmu v pythone

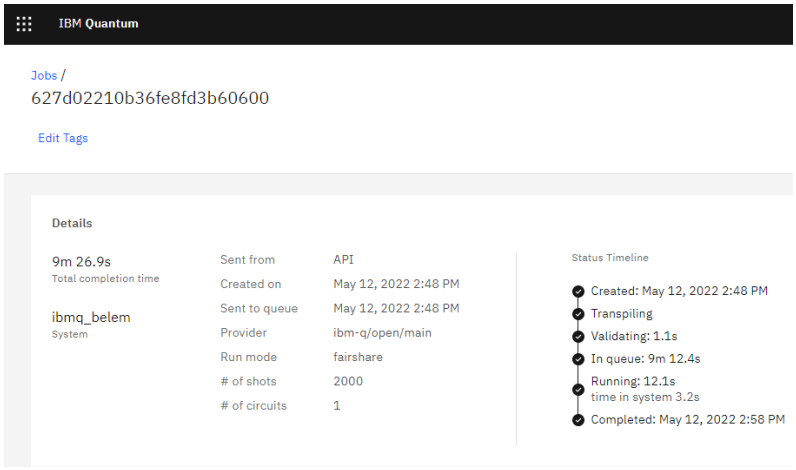
S výsledkom pre n = 2:



Obrázok 5 Výstup Groverovho algoritmu pre n = 2 v grafe

```
RESULTS: {'00': 177, '01': 1693, '10': 46, '11': 84}
```

Obrázok 6 Výsledok Groverovho algoritmu pre n = 2 v konzole



Obrázok 7 Ukážka priebehu programu pre n = 2 na kvantovom zariadení

4.3 Shorov algoritmus pre diskrétny logaritmus

Popularita

Tento algoritmus bol predstavený spolu s Shorovým faktorizačným algoritmom, je o niečo menej populárny. Je to tretí najznámejší kvantový algoritmus.

Druh

Ide o algoritmus, ktorý rieši problém diskrétneho logaritmu, na ktorom je založená veľká časť modernej kryptografie. Tento algoritmus sa dá využiť aj na prelomenie kryptografie založenej na eliptických krivkách.

Časová zložitosť

Podľa Petera Shora, sú obi dva jeho algoritmy schopné riešiť dané problémy v polynomiálnom čase.

Implementácia

Shorov algoritmus pre diskrétny logaritmus zatiaľ nebol implementovaný na žiadnom kvantovom zariadení, ani na žiadnom simulátore takýchto zariadení.

Funkcionalita

Peter Shor problém diskrétneho logaritmu popisuje takto:

Ak existuje prvočíslo p, generátor g z multiplikatívnej skupiny (mod p) a x (mod p), cieľom je nájsť také r, pre ktoré platí, že $g^r \equiv x(mod\ p)$.

Algoritmus funguje takto:

1. Najprv si algoritmus zvolí čísla a a b(mod p-1).
2. Algoritmus vypočíta $g^a x^{-b}(mod\ p)$.
3. Použije sa Fourierova transformácia pre $a \rightarrow c$, $b \rightarrow d$.
4. Vypočíta sa pravdepodobnosť že výstupom bude $|c, d, y\rangle$ kde $y \equiv g^k(mod\ p)$:
   $\left|\frac{1}{(p-1)q}\sum_{\substack{a,b \\ a-rb\equiv k}} \exp\left(\frac{2\pi i}{q}(ac+bd)\right)\right|^2$.
5. V tejto rovnici sa nahradí $a \equiv k + rb(mod\ p-1)$ z čoho vznikne:
   $\left|\frac{1}{(p-1)^2}\sum_{b=0}^{p-2} \exp\left(\frac{2\pi i}{p-1}(kc+b(d+rc))\right)\right|^2$.

6. Tento výpočet dá, ako výsledok, náhodnú hodnotu *c* (mod *p-1*) a zodpovedajúcu hodnotu $d \equiv -rc\,(mod\,p-1)$ Ak sú hodnoty *c* a *p-1* relatívne prvočísla, je možné získať hodnotu *r* pomocou delenia.

Počet opakovaní tohto algoritmu, pre získanie *r* s veľkou pravdepodobnosťou, je polynomiálny v $log\ p$.

Šifry, ktoré ohrozuje

Tento algoritmus ohrozuje nie len asymetrické šifry založené na diskrétnom logaritme, ale aj šifry založené na eliptických krivkách. Medzi najznámejšie ohrozené šifry patrí, podľa zdrojov [32] a [58]:

- ECDSA
- Diffie-Hellman
- ECDH(Elliptic Curve Diffie-Hellman)
- ElGamal

4.4 Simonov algoritmus pre útok na CBC-MAC

Popularita

Tento vedecký článok, ktorý vyšiel v roku 2016 a bol citovaný 75 krát. [67]

Druh

Simonov algoritmus slúži na nájdenie periódy funkcie predanej v čiernej skrinke. Pri tomto využití Simonovho algoritmu autormi Thomasom Santolim a Christianom Schaffnerom, je tento kvantový algoritmus použitý na útok na šifru CBC-MAC, ktorá slúži na zabezpečenie správ. [68]

Časová zložitosť

Časová zložitosť Simonovho algoritmu je O(*N*). [68]

Implementácia

Simonov algoritmus môže byť implementovaný pomocou nástroja Qiskit, avšak jeho využitie pre útok na daný kryptografický systém zatiaľ implementované nebolo. Preto pre tento konkrétny prípad využitia tohto kvantového algoritmu, zatiaľ implementácia neexistuje.

Funkcionalita

Cieľom overenia integrity správ, je možnosť komunikujúcich zistiť, či správa prichádza od očakávaného odosielateľa a že nebola počas prenosu nijako upravovaná. [68]

Komunikujúce strany, ktoré zdieľajú súkromný kľúč, môžu použiť kódy na zabezpečenie správ (Message Authentication Codes - MAC), aby tohto dosiahli. Odosielateľ pošle kľúč *k* a správu *m* do algoritmu *MAC(k,m)*, ktorý vygeneruje tag *t*, pre danú správu, a pošle príjemcovi pár *m* a *t*. Príjemca pomocou kľúča *k* môže overiť, či ide o platný tag pre správu *m*. [68]

CBC-MAC je efektívny spôsob vytvárania kódov pre zabezpečenie správ, založený na pseudonáhodnej permutácii. Používateľ, ktorý chce poslať správu *m* dĺžky *L* môže vypočítať tag *t*: $CBC^L(k,m)$ a poslať dvojicu *m* a *t* prijímateľovi, ktorý môže overiť či $t = CBC^L(k,m)$. [68]

Pri tomto využití Simonovho algoritmu je možné vytvoriť falošný tag pre danú správu.

Prvým krokom tohto útoku sa predpokladá, že pseudonáhodná permutácia F_k sa nahradí celkom náhodnou permutáciou π.

Cieľom je vytvoriť tag pre správu s prefixom $\alpha_1 \in \{0,1\}^n$ a vybrať nejaké $\alpha_0 \neq \alpha_1$. Pre j = 1...*L*, platí: $g_j: \{0,1\}^{n+1} \to \{0,1\}^n$,

$$b \parallel x \mapsto \mathrm{CBC}_\pi^L\left(\alpha_b \| 0^{(j-1)n} \| x \parallel 0^{(L-j-1)n}\right) = \pi^{L-j}\left(\pi^j(\alpha_b) \oplus x\right)$$

Pri jednom volaní operátora $U_{\mathrm{CBC}_\pi^L}$ sa dá vytvoriť jednotný operátor U_{g_j} pre $j = 1 \dots L-1$.

Kvantový počítač tieto operátory môže využiť na generáciu tagu pre správu podľa [68] takto:

1. Pre $j = 1 \dots L-1$, sa spustí Simonov algoritmus na U_{g_j} s cieľom nájsť $z^j := \pi^j(\alpha_0) \oplus \pi^j(\alpha_1)^g$. V tomto kroku sú všetky procesy na superpozíciách správ $m_1 \| m_2 \| \dots \| m_L$ také, že pre aspoň jedno $i \in \{1 \dots L\}^h$ platí, že $m_i = 0^n$.
2. Priradí sa $t_0 := \mathrm{CBC}_\pi^L\left(\alpha_0 \parallel 0^{(L-1)n}\right) = \pi^L(\alpha_0)$ a $t_1 := \mathrm{CBC}_\pi^L\left(\alpha_1 \parallel 0^{(L-1)n}\right) = \pi^L(\alpha_1)$.
3. Ak je *L* párne, sfalšuje sa $(m,t) := (\alpha_1 \| z^1 \| z^2 \parallel \cdots \parallel z^{L-1}, t_0)$. Ak je nepárne, sfalšuje sa $(m,t) := (\alpha_1 \| z^1 \| z^2 \parallel \cdots \parallel z^{L-1}, t_1)$.

Šifry, ktoré ohrozuje

Toto využitie Simonovho algoritmu sa sústreďuje na útok na systém zabezpečenia správ CBC-MAC. [68]

4.5 GEECM

Popularita

Článok, v ktorom bol tento algoritmus predstavený vyšiel v roku 2017. Vydali ho autori a matematici Daniel J. Bernstein, Nadia Heninger, Paul Lou a Luke Valenta. Od jeho vydania bol tento článok citovaný 68 krát. Tým, že je tento algoritmus pomerne nový, je o ňom veľmi málo informácií. [69]

Druh

Tento algoritmus slúži na faktorizáciu čísiel. [70]

Časová zložitosť

Tento algoritmus je v niektorých prípadoch ešte rýchlejší než Shorov algoritmus. Autori presne rýchlosť svojho algoritmu nešpecifikovali. [70]

Implementácia

Tento algoritmus zatiaľ nebol úspešne implementovaný na žiadnom kvantovom zariadení a zatiaľ zostáva iba v teoretickej rovine. [70]

Funkcionalita

Podľa autorov tohto algoritmu je najlepší spôsob riešenia faktorizačného problému, vziať najefektívnejšie klasické algoritmy na nájdenie prvočísiel a urýchliť ich, pomocou kvantového počítania. Konkrétne je tento kvantový algoritmus založený na algoritme ECM (Elliptic Curve Method), ktorý nájde prvočísla $p \leq y$ s použitím $2^{(lg\ y)^{1/2+o(1)}}$ operácií. Vylepšený variant ECM je EECM (ECM s využitím Edwardových kriviek).

EECM si vyberie Edwardovu krivku $x^2 + y^2 = 1 + \mathrm{d}x^2 + y^2$ nad bodom *Q*, inak povedané Edwardova krivka so známym nenulovým bodom *P*. EECM si tiež vyberá veľké celé číslo *s* a používa Edwardove sčítacie pravidlo, aby vypočítal *s*-tý násobok *P* na danej krivke. Konkrétne súradnicu *x*, ktorá je reprezentovaná ako zlomok celých čísel. Výsledkom tohto algoritmu je čitateľ tohto zlomku. Celkovo tento výpočet zaberie $(7 + \mathrm{o}(1))$ lg s násobení.

GEECM (Grover plus EECM) využíva Groverov algoritmus aby rýchlejšie našiel výsledok týchto výpočtov, čo tento algoritmus zrýchli tak, že namiesto $L^{\sqrt{2}+o(1)}$ operácií, stačí urobiť $L^{1+o(1)}$ operácií, kde $L = \sqrt{logy\ log\ logy}$. Pre ten istý počet operácií, GEECM zvyšuje *log y* o faktor *2+o(I)*, čo takmer zdvojnásobuje počet prvočísiel, ktoré algoritmus môže nájsť. [70]

Šifry, ktoré ohrozuje

Keďže sa tento algoritmus zaoberá faktorizáciou, tak ako Shorov faktorizačný algoritmus, ohrozuje presne tú istú šifru, a tou je RSA. [70]

4.6 Zvyšné kvantové algoritmy

Kvantových algoritmov, ktoré ohrozujú modernú kryptografiu je v súčasnosti veľké množstvo a každý rok sú objavované nové techniky ako tieto algoritmy ešte zrýchliť. Veľká časť z týchto algoritmov stavia na základe Shorových kvantových algoritmov a na Groverovom algoritme. Je zrejmé, že tieto najpopulárnejšie algoritmy sú len spodnou priečkou v oblasti kvantových kryptoanalytických algoritmov a v budúcnosti sa určite vyvinú ďalšie a rýchlejšie kvantové algoritmy, ktoré sa budú dať efektívne využiť na modernú kryptografiu.

4.7 Simulácie kvantových počítačov

S narastajúcim vývojom techniky a vývojom kvantových počítačov s narastajúcim počtom kvantových bitov, sa stáva myšlienka univerzálneho kvantového počítača so 100 000 a viac kvantovými bitmi realizovateľnou. Kým sa ale takýto počítač podarí zrealizovať, existujú v súčasnosti simulátory kvantových počítačov, na ktorých sa dajú kvantové algoritmy spustiť. Tieto simulátory majú oproti teoretickým kvantovým počítačom obmedzené výpočtové schopnosti. V tejto bakalárskej práci bol už jeden z takýchto simulátorov ukázaný, pri spustení Shorovho a Groverovho algoritmu pomocou IBM Quantum API, zvanej Qiskit v kapitolách 4.1 a 4.2, pri ukážkach kódov daných algoritmov. Tento open-source nástroj umožňuje spúšťať simulácie kvantových algoritmov na kvantových procesoroch alebo na simulátoroch takýchto zariadení. Podobný nástroj je prístupný aj od spoločnosti Google, s názvom Quantum Engine API, pomocou ktorého je možné využívať kvantového procesoru alebo simulátoru spoločnosti Google. Tento nástroj nie je zadarmo, na rozdiel od API firmy IBM. Podobný software ponúka aj firma D-Wave, s názvom Ocean. Týmto

firma umožňuje používateľom riešiť určité ťažké problémy na kvantových počítačoch. [71] [72] [73]

Aj keď majú tieto simulátory a počiatočné kvantové stroje obmedzený výkon a nemôžu presne simulovať správanie kvantových zariadení, sú vhodné na pochopenie fungovania kvantových počítačov a kvantových algoritmov, ktoré môžu v budúcnosti do značnej miery ohroziť bezpečnosť modernej kryptografie.

5 KVANTOVÉ ALGORITMY V MODERNEJ KRYPTOGRAFII

V tejto kapitole sú popísané konkrétne dopady kvantových algoritmov, ktoré boli podrobne charakterizované v kapitole 4. Skúmajú sa ich dopady na symetrickú a asymetrickú kryptografiu.

5.1 Symetrická kryptografia

Groverov algoritmus využíva vlastnosti kvantovej mechaniky na to, aby oslabil tradičné symetrické šifry. Obzvlášť tie, ktoré používajú menšie veľkosti kľúča. Bezpečnosť týchto kľúčov klesá na polovicu. To znamená, že kľúč symetrickej šifry s bezpečnosťou 128 bitov, by bol bezpečný ako 64-bitový kľúč. Toto zníženie ich bezpečnosti síce nie je úplným prelomením týchto kryptosystémov, ale je to značné zníženie ochrany takýchto systémov. 128-bitové kľúče budú síce stále považované za dosť silné na to, aby neboli ihneď prelomené, ale s rýchlym vývojom technológií bude ich bezpečnosť iba dočasná. 256 a viacbitové kľúče sú v čase písania tejto bakalárskej práce považované za bezpečné a odolné proti kvantovým počítačom.

Experti odporúčajú, aby sa symetrické kľúče zdvojnásobili, aby si zanechali svoju relatívnu ochranu v post-kvantovom svete. [32] [74]

5.1.1 Ohrozené symetrické šifry

Nižšie je uvedený zoznam šifier, ktoré sa môžu považovať v blízkej dobe za ohrozené, podľa [32]:

1. AES-128
2. DES, 3DES, DESX
3. CAST
4. IDEA
5. SAFER Kuznyechik
6. Serpent-128, Serpent-192

5.2 Asymetrická kryptografia

Všetky asymetrické šifry, ktoré sa v súčasnosti využívajú, sú založené na dvoch matematických problémoch. Prvým z nich je faktorizácia obrovských čísiel a druhým je výpočet

diskrétneho logaritmu. Obi dva tieto matematické problémy majú podobnú stavbu a môžu byť vyriešené pomocou Shorových kvantových algoritmov. [32]

5.2.1 RSA

Shorov algoritmus potrebuje *(2*n) + 3* veľmi stabilných kvantových bitov na prelomenie asymetrických kľúčov, kde *n* je počet bitov daného asymetrického kľúča. To znamená, že na prelomenie RSA kľúča, ktorý má 2048 bitov, by bolo potrebných 4099 stabilných kvantových bitov. Na prelomenie kľúča s 4096 bitmi by bolo potrebných 8195 stabilných qubitov.

RSA sa využíva pri zabezpečení internetových spojení ako súčasť SSL. Prelomenie tejto šifry by znamenalo ohrozenie celej komunikácie medzi webovou stránkou a klientom. Mohli by byť zneužité osobné informácie, finančné údaje, zdravotné údaje a podobne. Ďalší problém by nastal pri zabezpečení komunikácie cez internet, keďže tieto šifry sa využívajú pri zabezpečení komunikácie cez email a na zabezpečenie posielania textových správ cez internet. Ďalším príkladom dopadov Shorovho algoritmu na modernú kryptografiu je zabezpečenie VPN, ktoré takisto spolieha na asymetrickú šifru RSA. [32] [75]

5.2.2 DSA a ECDSA

DSA sa používa na zabezpečenie komunikácie cez internet a ECDSA je využívané pri TSL, čo je nástupca SSL, pri zabezpečovaní bezpečného spojenia medzi internetovými stránkami a internetovými prehliadačmi. Zabezpečenie HTTPS, ktoré slúži na bezpečné posielanie dát medzi prehliadačom a stránkou, je taktiež zabezpečované pomocou ECDSA.

Ďalším príkladom využitia ECDSA sú aplikácie na posielanie správ cez internet. Preto má prelomenie týchto šifrovacích systémov pomocou Shorových algoritmov obrovský dopad na súčasné kryptografické systémy.

Jednou z ďalších zasiahnutých oblastí by boli kryptomeny, keďže asymetrická šifra ECDSA sa používa na zabezpečenie Bitcoinu.

5.2.3 Elliptic Curve Diffie-Hellman

160-bitové eliptické krivky môžu byť prelomené kvantovým zariadením s 1000 kvantovými bitmi. [76]

Diffie-Hellman s využitím eliptických kriviek je ďalším z kryptosystémov, ktoré kvantové počítače prelomia. Táto šifra sa využíva v rôznych aplikáciách na vytvorenie bezpečných kľúčov.

5.3 Ďalšie ohrozené šifry

Okrem spomínaných šifrovacích systémov budú podľa [32], ako dôsledok príchodu kvantových počítačov, prelomené aj nasledujúce kryptografické systémy:

1. PKI (Public key infrastructure): Infraštruktúra správy a distribúcie verejných kľúčov.
2. Hardvérový bezpečnostný modul
3. Smartcards
4. Zabezpečenie Wi-Fi
5. Klasické generátory náhodných čísiel
6. Väčšina dvojfaktorového overovania, ktoré spolieha na digitálne certifikáty

5.4 Bezpečné šifry

S príchodom kvantových počítačov bude prelomených mnoho široko používaných šifier, zatiaľ čo niekoľko z nich nebude priamo prelomených, ale oslabených. Mnoho kryptografických systémov, naopak, zostane neohrozených. Medzi takéto systémy patria podľa [32]:

1. AES s bezpečnými dĺžkami kľúčov
2. Symetrické hashovacie systémy ako SHA-2, SHA-3, ak sa použije bezpečná dĺžka hashov
3. Prúdová šifra SHAKE
4. Super singular Isogeny Diffie-Hellman (SIDH) výmena kľúčov
5. Kvantová distribúcia kľúčov (QKD)
6. Post-kvantové kryptografické systémy
7. Kvantové generátory náhodných čísiel

5.5 Alternatíva k ohrozeným šifrám

Groverov algoritmus pri symetrických šifrách v podstate skracuje bezpečnosť ich kľúčov na polovicu. Pri týchto šifrách sa odporúča zvýšiť veľkosť kľúčov, čím sa dá dosiahnuť odolnosť voči kvantovým počítačom.

Pri asymetrických šifrách, ktoré s príchodom kvantových počítačov budú prelomené, zostáva tieto šifry nahradiť za bezpečnejšie šifrovacie systémy, ktoré kvantové počítače nedokážu prelomiť. Medzi tieto šifry patria RSA, Diffie-Hellman a ECDH(Elliptic curve Diffie-Hellman), DSA a ECDSA. Riešením, k prelomeniu týchto kryptografických systémov, sa venuje oblasť kryptografie s názvom post-kvantová kryptografia.

6 POST-KVANTOVÁ KRYPTOGRAFIA

Post-kvantová kryptografia sa zaoberá kryptografickými systémami, ktoré sú bezpečné proti plne funkčným kvantovým počítačom, s implementovanými kvantovými algoritmami, pri čom je rozdiel medzi post-kvantovou a kvantovou kryptografiou. Kvantová kryptografia sa, ale aj tak, považuje za súčasť post-kvantovej kryptografie. [1]

6.1 Kvantová a post-kvantová kryptografia

Kvantová kryptografia (QKD) bola vysvetlená na konci prvej kapitoly, v sekcii 1.4.1 tejto bakalárskej práce. Väčšinou sa zaoberá distribúciou kľúčov medzi dvomi užívateľmi, Alicou a Bobom. Medzi týmito dvomi odvetviami kryptografie sú podľa [1] tri zásadné rozdiely:

1. Zatiaľ čo kvantová kryptografia sa zaoberá iba jednou úlohou, post-kvantová kryptografia sa zaoberá širším spektrom kryptografie. Menovite bezpečnou komunikáciou, čo znamená napríklad digitálne podpisovanie s verejným kľúčom alebo šifrovanie s verejným kľúčom napríklad pri zabezpečení elektronických volieb.
2. Post-kvantová kryptografia zahŕňa systémy, ktoré majú svoju bezpečnosť dokázanú, ale aj systémy, pri ktorých sa bezpečnosť iba predpokladá. Kvantová kryptografia takéto systémy odmieta.
3. Post-kvantová kryptografia obsahuje množstvo systémov, ktoré môžu byť použité na zabezpečenie väčšej časti súčasnej komunikácie cez internet. Alica a Bob síce musia poslať určité dáta a vykonať pár výpočtov, ale nepotrebujú žiadny nový hardware. Kvantová kryptografia vyžaduje nový hardware pre pripojenie na internet, ktorý je v súčasnej dobe veľmi drahý.

6.2 Odvetvia post-kvantovej kryptografie

Post-kvantová kryptografia sa v súčasnosti sústredí na tieto odvetvia:

1. Kryptografia založená na hashovacích funkciách
2. Kryptografia založená na mriežke
3. Kryptografia založená na kódoch
4. Kryptografia využívajúca polynomiálne rovnice

6.2.1 Kryptografia založená na hashovacích funkciách

Digitálne podpisy sa stali dôležitou súčasťou pre zabezpečenie internetu. Doteraz sa na toto zabezpečenie používali šifry DSA, ECDSA a RSA, ktoré s príchodom kvantových počítačov budú prelomené. Alternatívou k nim sú podpisové schémy založené na hashovacích funkciách. [76]

6.2.1.1 Merkleho podpisová schéma (MSS)

Tieto funkcie boli vymyslené Ralphom Merklem, ktorý začal s jednorazovými podpisovými schémami, konkrétne s Lamport a Diffieho schémou a neskôr WOTS schémou. Tieto schémy samotné sú vhodné iba pre jednorazové použitie. Merkle predstavil nový prístup, s využitím hashového binárneho stromu, ktorý redukuje platnosť mnoho jednorazových verifikačných kľúčov do jedného verejného kľúča. Každý uzol tohto stromu obsahuje hash, ktorý sa používa na podpisovanie. Prvý uzol tejto hierarchie sa nazýva koreň tohto stromu a slúži ako verejný kľúč, pomocou ktorého sa dajú overiť hashe na listoch tohto stromu.

V súčasnosti sú podpisy založené na hashovacích funkciách najsľubnejšou alternatívou k RSA a podpisom založeným na eliptických krivkách. [1] [76]

6.2.2 Kryptografia založená na mriežke

Toto je forma kryptografie s verejným kľúčom, ktorá nemá slabiny RSA. Namiesto násobenia prvočísiel, pri kryptografii založenej na mriežke sa násobia matice. Tieto kryptografické systémy sú založené na náročných problémoch mriežkových problémov. Ich základom je problém najkratšieho vektoru (SVP). Vstupom tohto problému je mriežka reprezentovaná ľubovoľnou bázou a cieľom je nájsť v nej najkratší nenulový vektor. [76]

V nasledujúcich podkapitolách sú predstavené príklady algoritmov založených na mriežke.

6.2.2.1 Ajtai a Dwork

V roku 1997 našli Ajtai a Dwork prvé spojenie medzi najhorším a priemerným prípadom SVP. Tvrdili, že ich kryptosystém je bezpečný, ale v to v roku 1998 vyvrátili Nguyen a Ster. Kľúč tohto kryptosystému je veľmi dlhý a spôsobuje zväčšovanie správy, čo z neho nerobí vhodného kandidáta na post-kvantové obdobie. [76]

6.2.2.2 Goldreich-Goldwasser-Halevi

Tento kryptosystém vyšiel v roku 1997 a využíva problému najbližšieho vektoru (CVP), ktorý je NP-ťažký. Je efektívnejší než Ajtai-Dwork, avšak v roku 1999 bola objavená obrovská slabina tohto systému, ktorou je, že časti správy sa dajú odhaliť pomocou riešenia jednotlivých prípadov CVP. [76]

6.2.2.3 NTRU

NTRU bol publikovaný v roku 1996 a používa sa aj na šifrovanie, aj na digitálne podpisovanie. Spolieha sa na náročnosť faktorizovania určitých polynómov, čím sa stáva odolným proti Shorovmu algoritmu. Aby získal post-kvantovú bezpečnosť, NTRU vyžaduje 12881 bitové kľúče.

V roku 2016 Bernstein vydal novú verziu NTRU nazývanú NTRU Prime. Táto verzia je zabezpečená voči mnohým slabinám mriežkových šifrových systémov. Ide o najefektívnejší a najbezpečnejší algoritmus z kryptografie založenej na mriežke, čo z neho robí vhodného kandidáta na budúce využitie v modernej kryptografii. [76]

6.2.3 Kryptografia založená na kódoch

Kryptografia založená na kódoch predstavuje systémy, ktoré využívajú takzvaný *error correcting code*, teda kód na opravu chýb. Prvým systémom s verejným kľúčom založeným na kódoch bol McEliece v roku 1978. [76]

6.2.3.1 McEliece

Tento kryptosystém je založený na probléme dekódovania náhodného lineárneho kódu. Zatiaľ nebol prelomený. Jediným problémom je obrovská veľkosť kľúča (100kB až niekoľko MB). McEliece je rýchly s veľmi nízkou zložitosťou. Funguje tak, že sa do kódového slova vloží určitý počet chýb. Príjemca potom tajne tento kód vygeneruje ako náhodný Goppa kód, ktorý dokáže efektívne odstrániť vložené chyby. McEliece využíva na generovanie kódu generujúce matice. Od jeho vytvorenia bol McEliece niekoľkokrát upravovaný a vylepšovaný. S jedným takýmto vylepšením prišiel Niederreiter. [1] [76]

6.2.3.2 Niederreiter

Kryptosystém Niederreiter je variantom McEliece, ale namiesto generujúcich matíc využíva kontrolné matice a namiesto kódových slov posiela syndrómy. Tieto dva kryptografické systémy sú rovnako bezpečné.

Najväčším problémom týchto systémov je dĺžka kľúčov. Avšak niektoré kryptografické systémy, ktoré sa snažili tieto verejné kľúče o niečo zmenšiť, boli prelomené. Preto jedinými odporúčanými systémami zostávajú McEliece a Niederreiter. [1] [74] [77]

6.2.4 Kryptografia využívajúca polynomiálne rovnice

Tento typ kryptografie je založený na mnohorozmerných polynómoch nad konečnými poľami. Problém riešenia mnohorozmerných polynómov je NP-úplný problém, čo je jeden z dôvodov, prečo sú tieto kryptografické systémy vhodným kandidátom pre post-kvantové systémy. Tento typ kryptografie môže byť využitý aj pre šifrovanie, aj pre digitálne podpisovanie. [78]

6.2.4.1 Rainbow

Rainbow poskytuje celkom malé podpisy, pozostávajúce iba z niekoľko stoviek bitov, ktoré sú oveľa kratšie, než pri ostatných post-kvantových kryptografických schémach. Keďže Rainbow využíva jednoduché operácie nad malými konečnými poľami, je generácia týchto podpisov a ich overenie nesmierne efektívna.

National Institute of Standards and Technology v roku 2020 zaradil medzi top 3 post-kvantové podpisové schémy. Toto je jasným dôkazom toho, že ide o veľmi kvalitného kandidáta pre nahradenie, v budúcnosti prelomených, asymetrických šifrovacích systémov. [79]

ZÁVĚR

Na konci 20. storočia bolo publikovaných niekoľko kvantových algoritmov, ktoré sú hrozbou modernej kryptografie. Kvantové algoritmy zatiaľ predstavujú hrozbu iba v teoretickej rovine, pretože zatiaľ existujú iba kvantové zariadenia s malým počtom kvantových bitov, ktoré nedokážu využiť silu týchto kvantových algoritmov naplno. Simulácie takýchto algoritmov sa dajú spustiť na súčasných superpočítačoch, ale tie kvantové algoritmy nedokážu využiť do takej miery, aby to predstavovalo hrozbu pre súčasnú kryptografiu.

Ak by bol zostavený kvantový počítač so 100 000 a viac stabilnými kvantovými bitmi, znamenalo by to pravdepodobne koniec súčasnej podoby modernej kryptografie. Bolo by nevyhnutne potrebné vymeniť všetky asymetrické šifrovacie systémy, ktoré sa v súčasnosti vo veľkej miere používajú a zvýšiť veľkosť kľúčov pre dnes používané symetrické šifrovacie systémy.

Toto ale neznamená, že by bola kryptografia mŕtva. Práve naopak. Existuje totiž oblasť kryptografie, ktorá sa zaoberá skúmaním šifrovacích algoritmov a protokolov, ktoré sú odolné proti útokom s plne funkčným univerzálnym kvantovým počítačom. Táto veda sa nazýva post-kvantová kryptografia. Každý rok prichádza s novými algoritmami a šifrovacími systémami, ktoré tvoria najvhodnejších kandidátov na nahradenie šifier, ktoré sú ohrozené kvantovými počítačmi.

V tejto práci boli v teoretickej časti popísané základné pojmy kryptológie a modernej kryptografie, spolu s podrobným popisom základných šifrovacích algoritmov, ktoré ohrozujú kvantové počítače. Ďalej boli predstavené kvantové počítače spolu s ich jednotlivými typmi a ich možným využitím. Nasledovalo predstavenie kvantových algoritmov, ktoré dokázali exponenciálne zrýchlenie oproti klasickým počítačom. V poslednej časti teoretickej časti boli predstavené kvantové algoritmy, ktoré ohrozujú niektoré šifrovacie systémy modernej kryptografie.

V praktickej časti boli tieto algoritmy podrobne charakterizované a kategorizované. Pri Shorovom faktorizačnom algoritme a pri Groverovom algoritme sa mi podarilo spustiť tieto algoritmy na kvantových zariadeniach alebo na simulátoroch takýchto zariadení, pomocou API od IBM s názvom Qiskit. Nasledoval prehľad dopadov týchto algoritmov na symetrickú a asymetrickú kryptografiu, pričom v závere tejto kapitoly bola predstavená alternatíva k prelomeným šifrám v podobe post-kvantovej kryptografie. Táto oblasť kryptografie je podrobnejšie predstavená v poslednej kapitole tejto bakalárskej práce, kde sú

uvedené jednotlivé oblasti, ktorými sa táto disciplína zaoberá a z každej oblasti boli uvedené príklady jednotlivých šifrovacích algoritmov z týchto jednotlivých oblastí, ktoré tvoria vhodných kandidátov na nahradenie ohrozených šifier, ktoré sa používajú v súčasnosti.

SEZNAM POUŽITÉ LITERATURY.

[1] BERNSTEIN, Daniel J., Johannes A. BUCHMANN a Erik DAHMEN, ed. *Post-quantum cryptography*. Berlin: Springer, 2009. ISBN 978-3-540-88701-0.

[2] SWENSON, Christopher. *Modern cryptanalysis: techniques for advanced code breaking*. Indianapolis: Wiley, 2008. ISBN 9780470135938.

[3] Cryptanalysis. In: *Techopedia* [online]. 2022 [cit. 2022-04-15]. Dostupné z: https://www.techopedia.com/definition/1769/cryptanalysis

[4] STINSON, Douglas Robert a Maura B. PATERSON. *Cryptography: theory and practice*. Fourth edition. Boca Raton, 2019. Textbooks in mathematics (CRC Press). ISBN 978-1-1381-9701-5.

[5] KATZ, Jonathan a Yehuda LINDELL. Introduction to *modern* cryptography. Second edition. Boca Raton: CRC Press/Taylor & Francis Group, 2015. Chapman & Hall/CRC cryptography and network security. ISBN 9781466570269.

[6] A quick guide to modern cryptography. *In: InfoWorld [*online]. 2021 [cit. 2022-05-01]. Dostupné z: https://www.infoworld.com/article/3641388/a-quick-guide-to-modern-cryptography.html

[7] What is a cryptographic key? | Keys and SSL encryption. In: *Cloudflare* [online]. 2022 [cit. 2022-04-12]. Dostupné z: https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/

[8] MENEZES, Alfred J., Paul C. van OORSCHOT a Scott A. VANSTONE. *Handbook of applied cryptography*. Boca Raton: CRC, 1997. CRC Press series on discrete mathematics and its applications. ISBN 08-493-8523-7.

[9] Symmetric cryptography. In: *IBM* [online]. 2021 [cit. 2022-05-16]. Dostupné z: https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-symmetric-cryptography

[10] STALLINGS, William. *Cryptography and Network Security: Principles and Practice, Sixth Edition*. 6th ed. USA: Pearson Education, Inc., 2014. ISBN 978-0-13-335469-0.

[11] MOGOLLON, Manuel. *Cryptography and Security Services: Mechanisms and*

Applications. University of Dallas, USA: CyberTech Publishing, 2007. ISBN 978-1-59904-839-0.

[12] AUMASSON, Jean-Philippe. *Serious cryptography: a practical introduction to modern encryption*. San Francisco: No Starch Press, 2018. ISBN 978-1-59327-826-7.

[13] Advanced Encryption Standard (AES). In: *GeeksforGeeks* [online]. 2022 [cit. 2022-05-16]. Dostupné z: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

[14] What Is AES Encryption and How Does It Work?. In: *Simplilearn* [online]. 2022 [cit. 2022-04-16]. Dostupné z: https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption#what_are_the_applications_of_aes

[15] Meltdown - chyba v moderních procesorech 5. leden 2018. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2018 [cit. 2022-04-16]. Dostupné z: https://www.nukib.cz/cs/infoservis/hrozby/1464-meltdown-chyba-v-modernich-procesorech/

[16] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 1. vyd. v českém jazyce. Praha: Dokořán, 2003. Aliter. ISBN 8072034995.

[17] What is Asymmetric Encryption? Understand with Simple Examples. In: *Savvy Security* [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://cheapsslsecurity.com/blog/what-is-asymmetric-encryption-understand-with-simple-examples/

[18] MCMAHON, David. *Quantum computing expained*. Hoboken, New Jersey, USA: John Wiley & Sons, Inc., 2008. ISBN 978-0-470-09699-4.

[19] What is the El Gamal encryption?. In: *Educative* [online]. 2022 [cit. 2022-04-20]. Dostupné z: https://www.educative.io/edpresso/what-is-the-el-gamal-encryption

[20] ElGamal Encryption Algorithm. In: *GeeksforGeeks* [online]. 2021 [cit. 2022-05-16]. Dostupné z: https://www.geeksforgeeks.org/elgamal-encryption-algorithm/

[21] Digital Signature Algorithm (DSA) in Cryptography: How It Works and Advantages. In: *Simplilearn* [online]. 2022 [cit. 2022-05-16]. Dostupné z: https://www.simplilearn.com/tutorials/cryptography-tutorial/digital-signature-algorithm#what_is_the_dsa_algorithm,%20https://cryptobook.nakov.com/digital-signatures

[22] Elliptic Curve Digital Signature Algorithm (ECDSA). In: *Encryption Consulting* [online]. c2018-2022 [cit. 2022-04-21]. Dostupné z: https://www.encryptionconsulting.com/education-center/what-is-ecdsa/

[23] Asymmetric Encryption. In: *TEACH COMPUTER SCIENCE* [online]. 2022 [cit. 2022-05-16]. Dostupné z: https://teachcomputerscience.com/asymmetric-encryption/

[24] What is RSA encryption and how does it work?. In: *Comparitech* [online]. 2021 [cit. 2022-05-16]. Dostupné z: https://www.comparitech.com/blog/information-security/rsa-encryption/

[25] KUMAR, Neeraj. Limitations and Future Applications of Quantum Cryptography. USA: IGI Global, 2021. ISBN 9781799866794.

[26] Quantum Key Distribution. *In: IDQ [online]. 2022* [cit. 2022-04-25]. Dostupné z: https://www.idquantique.com/quantum-safe-security/quantum-key-distribution/

[27] DJORDJEVIC, Ivan B. Physical-Layer *Security* and Quantum Key Distribution. Cham, Switzerland: Springer Nature Switzerland AG, 2019. ISBN 978-3-030-27565-5.

[28] WOLF, Ramona. Quantum *Key Distribution: An Introduction with* Exercises. Cham (Switzerland): Springer Nature Switzerland AG, 2021. ISBN 978-3-030-73991-1.

[29] GRASSELLI, Federico. *Quantum Cryptography: From Key Distribution to Conference* Key Agreement. Cham (Switzerland): Springer Nature Switzerland AG, 2021. ISBN 978-3-030-64359-1.

[30] Fundamentals of Quantum *Key Distribution — BB84, B92 & E91 protocols. In*: Medium [online]. 2021 [cit. 2022-04-26]. Dostupné z: https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead

[31] CLEGG, Brian. Quantum computing: the transformative technology of the qubit revolution. *London*: Icon Books, 2021. ISBN 978–178578–707–2.

[32] GRIMES, Roger A. *Cryptography Apocalypse: Preparing for the Day When Quantum* Computing Breaks Today's Crypto. USA: Wiley, 2020. ISBN 978-1-107-01446-6.

[33] NIELSEN, Michael A. *a Isaac L. CHUANG. Quantum computation and quantum information. 10th Anniversary* ed. Cambridge: Cambridge University Press, 2010. ISBN 9781107002173.

[34] HAGOUEL, Paul Isaac a Ioannis G. KARAFYLLIDIS. Quantum *computers: Registers, gates* and algorithms. 2012 28th International Conference on Microelectronics Proceedings. IEEE, 2012, 15-21. ISBN 978-1-4673-0237-1. Dostupné z: doi:10.1109/MIEL.2012.6222789

[35] Applied Quantum Cryptography. Berlin: Springer, 2010. ISBN 978-3-642-04831-9.

[36] *What is a* qubit?. In: Microsoft Azure [online]. 2022 [cit. 2022-03-16]. Dostupné z: https://azure.microsoft.com/en-us/overview/what-is-a-qubit/#superposition-interference-entanglement

[37] Quantum Fourier Transform. In: Qiskit [*online].* 2022 [cit. 2022-05-16]. Dostupné z: https://qiskit.org/textbook/ch-algorithms/quantum-fourier-transform.html

[38] Kvantová Fourierova transformace. In: *Matematicko-fyzikální* fakulta Univerzita Karlova [online]. 2001 [cit. 2022-05-16]. Dostupné z: https://www2.karlin.mff.cuni.cz/~holub/soubory/qc/node21.html

[39] The Many Faces of a *Qubit. In: Quantum* Computing Inc. [online]. [cit. 2022-04-17]. Dostupné z: https://www.quantumcomputinginc.com/blog/the-many-faces-of-a-qubit/

[40] Hadamard gate. In: Quantum Inspire [online]. *2022 [cit.* 2022-05-16]. Dostupné z: https://www.quantum-inspire.com/kbase/hadamard/

[41] PERRY, Riley Tipton. *Quantum Computing* from the Ground Up. Singapore: World Scientific Publishing, 2012. ISBN 978-981-4412-11-7.

[42] What is a quantum *computer?*. *In: New Scientist* [online]. [cit. 2022-05-16]. Dostupné z: https://www.newscientist.com/question/what-is-a-quantum-computer/

[43] EDMUNDS, Claire. Q-CTRL. In: YouTube [*online].* [cit. 2022-05-16]. Dostupné z: https://www.youtube.com/watch?v=AUAkoEiutOE

[44] GRUMBLING, Emily a Mark HOROWITZ. *Quantum* Computing: Progress and Prospects. USA: The National Academies Press, 2019. ISBN 978-0-309-47972-1.

[45] Understanding the 3 types of quantum *computers* and what it means to you. In: Secured2 [online]. 2020 [cit. 2022-04-21]. Dostupné z: https://secured2.com/understanding-the-3-types-of-quantum-computers-and-what-it-means-to-you/

[46] RøNNOW, Troels F., Zhihui WANG, Joshua JOB et al. Defining and detecting quantum speedup. Science. 2014, 345(6195), 420-424. ISSN 0036-8075. Dostupné z: doi:10.1126/science.1252319

[47] Top Applications Of Quantum Computing Everyone *Should* Know About. In: Analytics India Magazine [online]. 2020 [cit. 2022-04-17]. Dostupné z: https://analyticsindiamag.com/top-applications-of-quantum-computing-everyone-should-know-about/

[48] Quantum Computing Is Coming. What Can It Do?. In: Harvard Business Review [online]. 2021 [cit. 2022-05-17]. Dostupné z: https://hbr.org/2021/07/quantum-computing-is-coming-what-can-it-do

[49] First quantum computer to pack 100 *qubits* enters crowded race. In: Nature [online]. 2021 [cit. 2022-04-18]. Dostupné z: https://www.nature.com/articles/d41586-021-03476-5

[50] IBM promises 1000-qubit quantum computer—a *milestone*—by 2023. In: Science [online]. 2020 [cit. 2022-05-17]. Dostupné z: https://www.science.org/content/article/ibm-promises-1000-qubit-quantum-computer-milestone-2023

[51] Google wants to build a useful *quantum* computer by 2029. In: The Verge [online]. 2021 [cit. 2022-05-17]. Dostupné z:

https://www.theverge.com/2021/5/19/22443453/google-quantum-computer-2029-decade-commercial-useful-qubits-quantum-transistor

[52] D-Wave took its own path in *quantum* computing. Now it's joining the crowd. In: Fortune [online]. 2021 [cit. 2022-04-20]. Dostupné z: https://fortune.com/2021/10/05/quantum-computer-d-wave-google-ibm-gate-model/

[53] BERNHARDT, Chris. Quantum computing for *everyone*. Cambridge, Massachusetts: The MIT Press, 2019. ISBN 978-026-2039-253.

[54] YANOFSKY, Noson S. a Mirco *A*. MANNUCCI. Quantum Computing for Computer Scientists. USA: Cambridge University Press, 2008. ISBN 978-0-521-879965.

[55] LIPTON, Richard J. a Kenneth *W*. REGAN. Quantum algorithms via linear algebra: a primer. Cambridge, Massachusetts: The MIT Press, 2014, 1 online zdroj (xii, 192 pages). ISBN 9780262323567. Dostupné také z: https://proxy.k.utb.cz/login?url=http://ieeexplore.ieee.org/servlet/opac?bknumber=7008157

[56] SHOR, Peter W. Polynomial-Time Algorithms *for* Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing. 1997, 26(5), 1484-1509. ISSN 0097-5397. Dostupné z: doi:10.1137/S0097539795293172

[57] Google Študovňa. In: Google Scholar *[*online]. [cit. 2022-05-18]. Dostupné z: https://scholar.google.sk/scholar?hl=sk&as_sdt=0%2C5&q=peter+shor&btnG=

[58] SHOR, Peter W. Algorithms for *quantum* computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press, 1994, 124-134. ISBN 0-8186-6580-7. Dostupné z: doi:10.1109/SFCS.1994.365700

[59] Using Shor's Algorithm to Achieve Factor *Decomposition*. In: Huawei HiQ [online]. 2019 [cit. 2022-05-01]. Dostupné z: https://hiqsimulator.readthedocs.io/en/latest/examples/examples.ShorAlgorithm.html

[60] REICH, Henry. Minutephysics. In: *YouTube* [online]. [cit. 2022-05-10]. Dostupné z: https://www.youtube.com/watch?v=FRZQ-efABeQ&t=280s

[61] Shor's Algorithm With Code. In: *Quantum* Computing UK [online]. 2022 [cit. 2022-05-17]. Dostupné z: https://quantumcomputinguk.org/tutorials/shors-algorithm-with-code

[62] Lov Grover. In: Google Scholar *[*online]. [cit. 2022-05-18]. Dostupné z: https://scholar.google.sk/scholar?hl=sk&as_sdt=0%2C5&q=lov+grover&btnG=

[63] Grover's search algorithm. In: Quantiki *[*online]. 2015 [cit. 2022-04-25]. Dostupné z: https://www.quantiki.org/wiki/grovers-search-algorithm

[64] MANDVIWALLA, Aamir, Keita OHSHIRO a *Bo* JI. Implementing Grover's Algorithm on the IBM Quantum Computers. 2018 IEEE International Conference on Big Data (Big Data). IEEE, 2018, 2531-2537. ISBN 978-1-5386-5035-6. Dostupné z: doi:10.1109/BigData.2018.8622457

[65] GROVER, Lov K. Quantum Mechanics *Helps* in Searching for a Needle in a Haystack. Physical Review Letters. 1997, 79(2)*, 325-328. ISSN 0031-9007*. Dostupné z: doi:10.1103/PhysRevLett.79.325

[66] Information Security in the Quantum Era *Threats* to modern cryptography: Grover's algorithm [online]. In: . 2020 [cit. *2022-05-17]. Dostupné z:* https://www.researchgate.net/publication/342378356_Information_Security_in_the_Quantum_Era_Threats_to_modern_cryptography_Grover's_algorithm

[67] Simon's algorithm attack. In: Google *Scholar* [online]. [cit. 2022-05-18]. Dostupné z: https://scholar.google.com/scholar?*hl=sk&as*_sdt=0%2C5&q=simons+algorithm+attack&btnG=

[68] SANTOLI, Thomas a Christian SCHAFFNER. *Using* Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Information and Computation. 2017, 17, 65-78. *ISSN 15337146.* Dostupné z: doi:10.26421/QIC17.1-2-4

[69] Post-quantum RSA. In: Google Scholar *[*online]. [cit. 2022-05-18]. Dostupné z: https://scholar.google.com/scholar?hl=*sk&as_sdt*=0%2C5&q=Post-quantum+RSA&oq=Post-quantum+RSA

[70] BERNSTEIN, Daniel J., Nadia HENINGER*,* Paul LOU a Luke VALENTA. Post-

quantum RSA. Post-Quantum Cryptography. Cham: Springer International Publishing, *2017, 311-329.* Lecture Notes in Computer Science. ISBN 978-3-319-59878-9. Dostupné z: doi:10.1007/978-3-319-59879-6_18

[71] Quantum Engine API. In: Google *Quantum* AI [online]. 2022 [cit. 2022-05-18]. Dostupné z: https://quantumai.google/*cirq*/google/engine

[72] D-Wave Ocean Software Documentation. In: *D-Wave* Ocean Software Documentation [online]. [cit. 2022-05-18]. Dostupné z: https://docs.*ocean*.dwavesys.com/en/stable/#

[73] The most popular quantum computing SDK. In: Qiskit [online]. [cit. 2022-05-18]. Dostupné z: https://qiskit.org/overview

[74] BERNSTEIN, Daniel J. a Tanja *LANGE*. Post-quantum cryptography. Nature. 2017, 549(7671), 188-194. ISSN 0028-0836. Dostupné *z: doi:10.1038/nature23461*

[75] RSA Is Dead — We Just *Haven't* Accepted It Yet. In: Forbes [online]. 2021 [cit. 2022-05-17]. *Dostupné z: https://*www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-just-haventaccepted-ityet/?sh=72781aa15d22

[76] MAVROEIDIS, Vasileios, Kamer VISHI, Mateusz D. a Audun JøSANG. The Impact of Quantum Computing on Present Cryptography. International Journal *of Advanced Computer* Science and Applications. 2018, 9(3). ISSN 21565570. Dostupné z: doi:10.14569/IJACSA.2018.090354

[77] LANGE, Tanja a Rainer STEINWANDT, *ed*. Post-Quantum cryptography: 9th International conference, PQCrypto 2018 Fort Lauderdale, FL, USA, April *9-11, 2018 Proceedings*. Cham: Springer, 2018. ISBN 978-3-319-79062-6.

[78] Multivariate cryptography. In: Fandom [online*]*. [cit. 2022-05-17]. Dostupné z: https://cryptography.fandom.com/wiki/Multivariate_cryptography

[79] Rainbow Signature. In: PQCRainbow [online*]*. 2020 [cit. 2022-05-17]. Dostupné z: https://www.pqcrainbow.org/

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ψ Stav qubitu

α Amplitúda pravdepodobnosti

β Amplitúda pravdepodobnosti

$\oplus$ XOR

$^{\circ}$ Stupne otočenia

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBSAH CD

- fulltext.pdf
- prilohy.zip