Универзитет „Св. Кирил и Методиј“ во Скопје
ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО

Дипломска работа

Квантни компјутери и нивната улога во пробивањето на шифрирачките алгоритми

Изработил:
Андреј Станојковиќ

Ментор:
проф. д-р Весна Димитрова

Скопје, 2024

Тема	Квантни компјутери и нивната улога во пробивањето на шифрирачките алгоритми
Датум на одбрана	06.03.2024
Автор	Андреј Станојковиќ
Научна област	Криптографија
Ментор	д-р Весна Димитрова
Членови на комисија	д-р Христина Михајлоска Стефан Андонов

Содржина

Апстракт

Овој дипломски труд ги истражува основите концепти на квантното пресметување и квантните компјутери, објаснувајќи ги нивните основни принципи и механизми. Централната идеја зад квантното пресметување лежи во искористувањето на принципите на квантната физика, како што се суперпозицијата и испреплетеноста на квантните состојби.

Најпрво се објаснети овие клучни принципи на квантната механика, како и нејзината примена во различни области. Врз основа на овие принципи се изградени квантните компјутери во втората половина на минатиот век кои се надоградувале со текот на годините. Основната градбена единица на еден квантен компјутер е кјубитот кој е квантен еквивалент на класичниот бит. Опишани се некои операции кои можат да се применат врз кјубитите, како и позначајните квантни логички порти кои се користат за изградба на квантни кола. Потоа се споменати квантните алгоритми и нивната класификација во повеќе категории.

Како еден од најзначајните алгоритми за шифрирање се издвојува RSA криптосистемот кој има широка примена во денешните технологии. Од друга страна, развиен е алгоритамот на Шор, квантен алгоритам кој е голема закана за пробивање на RSA. Овие два алгоритми и нивните главни функционалности се детално опишани и имплементирани во програмскиот јазик Python.

Овој дипломски труд служи за на краток начин да претстави како подемот на квантните компјутери може да има сериозни негативни последици врз безбедноста на податоците, но и позитивни последици кои многу ќе го поедностават секојдневниот живот на човекот.

Клучни зборови: квантна механика, квантни компјутери, кјубит, квантни алгоритми, RSA криптосистем, алгоритамот на Шор

1. Вовед

Квантното пресметување стои во првите редови на технолошкиот напредок, подготвено да го револуционизира начинот на кој се обработуваат информациите и решаваат сложени проблеми. Традиционалните компјутери, засновани на класичната физика и бинарната логика, нè доведоа во дигиталната ера, но тие се соочуваат со инхерентни ограничувања кога ќе се соочат со одредени пресметковни предизвици. Квантното пресметување, од друга страна, ги користи принципите на квантната механика за да ја отклучи огромната пресметковна моќ и потенцијално да ги надмине овие ограничувања.

Концептот на квантен компјутер првпат е воведен од физичарот Ричард Фајнман во 1982 година, кој замислил уред способен да симулира квантни системи и ефикасно да решава сложени физички проблеми. [2] Во текот на изминатите неколку децении, постигнат е значителен напредок во разбирањето на теоретските основи и развојот на практични имплементации на квантното пресметување. Полето беше сведок на извонредни откритија, од раните демонстрации на квантните алгоритми до изградбата на сè пософистициран квантен хардвер.

Еден од најпознатите квантни алгоритми е алгоритамот на Шор, објавен од Питер Шор во 1994 година. Ова откритие има значителни импликации за криптографијата, бидејќи многу криптографски протоколи се потпираат на пресметковната тешкотија за разбивање на големи броеви. Потенцијалното влијание на квантното пресметување врз криптографијата поттикна интензивно истражување во пост-квантната криптографија, која е насочена кон развој на криптографски алгоритми отпорни на квантни напади.

Сепак, и покрај извонредниот напредок, квантното пресметување сè уште е во рана фаза, соочено со значителни предизвици на патот кон практичност и приспособливост. Квантните системи се неверојатно чувствителни на еколошки нарушувања и декохерентност, што може да доведе до грешки и губење на квантните информации. Развојот на стабилни и отпорни на грешки кјубити, имплементацијата на квантната корекција на толерантни грешки и подобрувањето на времето на кохерентност на квантните системи се активни области на истражување. [2][3]

2. Квантна механика

Квантната механика е фундаментална теорија во физиката која дава опис на физичките својства на природата на ниво на атоми и субатомски честички. Таа е основата на целата квантна физика, вклучувајќи ја квантната хемија, квантната теорија на поле, квантната технологија и квантната информатичка наука.

Класичната физика, множество теории што постоеле пред појавата на квантната механика, опишува многу аспекти на природата на обична (макроскопска) скала, но не е доволна за нивно опишување на мали (атомски и субатомски) размери. Повеќето теории во класичната физика може да се изведат од квантната механика како апроксимација која е валидна на големи (макроскопски) размери. [4][5]

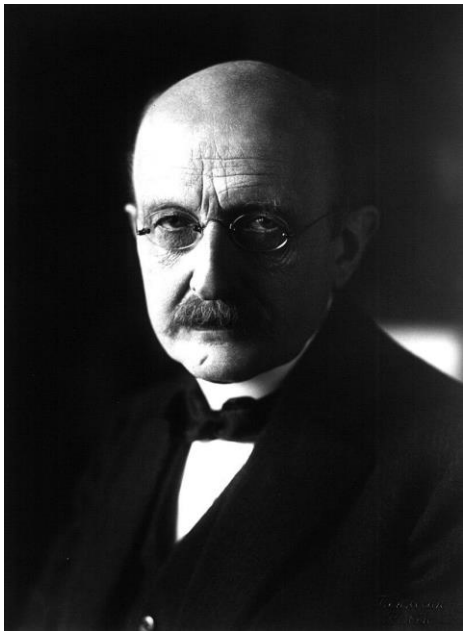
Терминот “quantum” потекнува од латинскиот јазик, каде што “quantus” значи „колку“ или „колку одлично“. Во 16 век, зборот “quantum” се користел за да се однесува на количина или квантитет. Сепак, неговата употреба во контекст на физиката и основните единици на енергија и материја се појавиле подоцна. [6]

2.1. Историја

Квантната механика почнала да се развива во првите децении на 20ти век и вклучува придонеси на многу познати физичари.

- Во 1900 година, Макс Планк (слика 1) ја предложил хипотезата дека енергијата се зрачи и се апсорбира во дискретни „кванти“ (или енергетски пакети). Според него, количините на енергија би можеле да се поделат на „елементи“ чија големина (E) би била пропорционална на нивната фреквенција (v): E = hv, каде h е Планкова константа.

- Во 1905 година, Алберт Ајнштајн ја протолкувал Планковата квантна хипотеза и ја искористил за да го објасни фотоелектричниот ефект, во кој светлина која сјае на одредени материјали може да исфрли електрони од материјалот. Ајнштајн понатаму ја развил оваа идеја за да покаже



Слика 1. Макс Планк, таткото на квантната теорија

дека електромагнетниот бран, како што е светлината, може да се опише и како честичка (подоцна наречена фотон).

- Нилс Бор, во 1913 година, предложил револуционерен модел на атомот заснован на идеите за квантизирани енергетски нивоа. Познат како Боров модел, тој ги опишал електроните кои орбитираат околу јадрото во одредени енергетски нивоа или обвивки. Овој модел успешно ги објасни дискретните емисиони спектри забележани во атомската спектроскопија.

- Во 1920-тите, бил постигнат значителен напредок во разбирањето на двојната природа на материјата и основните ограничувања во прецизното мерење и на положбата и на моментумот. Во 1923 година, францускиот физичар Луј де Броље ја изнел својата теорија за брановите на материјата наведувајќи дека честичките можат да покажат карактеристики на бранови и обратно. Надоврзувајќи се на пристапот на Де Броље, модерната квантна механика е родена во 1925 година, кога германските физичари Вернер Хајзенберг, Макс Борн и Пасквал Џордан развиле матрична механика, а австрискиот физичар Ервин Шродингер ја развил брановата механика.

- До 1930 година, квантната механика била дополнително обединета и формализирана од Дејвид Хилберт, Пол Дирак и Џон фон Њуман. Оттогаш навлегла во многу дисциплини, вклучувајќи ја квантната хемија, квантната електроника, квантната оптика и квантната информатичка наука. [4][5]

2.2. Основни концепти

Основните концепти на квантната механика опфаќаат низа принципи кои го објаснуваат однесувањето на материјата и енергијата на атомските и субатомските скали и објаснуваат феномени кои не се земени во предвид од класичната физика.

2.2.1. Квантизација

Квантизацијата (Quantization) се однесува на процесот на дискретизирање или претставување на континуирана физичка величина преку дискретни вредности. Со други зборови, тоа вклучува поделба на континуиран опсег на вредности на квантизирани нивоа или единици. Овој концепт е централен во различни области

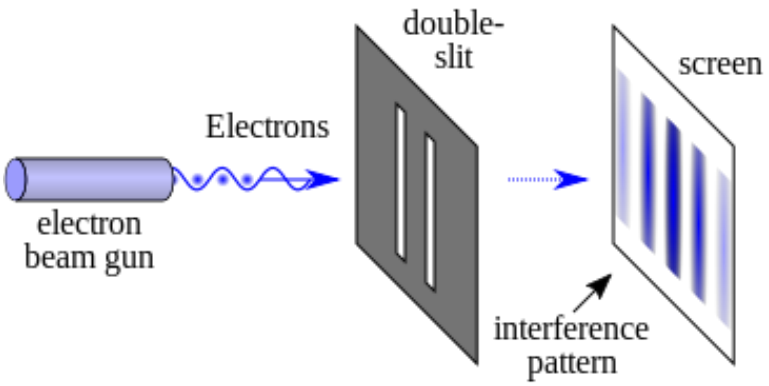
на физиката и инженерството, особено во квантната механика и дигиталните системи.

Во областа на квантната механика, квантизацијата е еден од основните аспекти. Се однесува на ограничување на одредени физички карактеристики, како што се енергијата, аголниот моментум и положбата, на специфични дискретни вредности наместо да им се дозволи да земат каква било континуирана вредност. Оваа дискретна природа на енергетските нивоа е особено очигледна во атомските и субатомските системи, каде што електроните можат да заземаат само одредени енергетски нивоа или состојби. На пример, кога се разгледуваат енергетските нивоа на електроните околу атомското јадро, квантизацијата наложува дека електроните можат да постојат само во специфични енергетски состојби, претставени со квантни броеви. Како што електронот преминува помеѓу овие квантизирани енергетски нивоа, тој емитира или апсорбира енергија во дискретни вредности, познати како фотони. [7][8]

2.2.2. Двојна природа на материјата

Двојната природа на материјата (Wave-particle Duality) е основен концепт во квантната механика кој претпоставува дека честичките, како што се електроните и фотоните, се однесуваат и како честички и како бранови. Овој концепт сугерира дека честичките можат да покажат својства на бранови, како интерференција и дифракција, но и својства на честички, како позиција и моментум. Однесувањето на честичките е опишано со бранови функции, кои ја претставуваат распределбата на веројатноста на својствата на честичката. Двојната природа е тесно поврзана со принципот на неопределеност кој е директна последица на својството честичките да покажуваат карактеристики и на честички и на бранови.

На слика 2 е прикажан експеримент кој го објаснува ова својство на честичките, познат како Double-Slit Experiment. Во овој експеримент, зрак од честички, како електрони или фотони, се пушта да помине низ плоча која има два блиско распоредени процепи и потоа се набљудува на екран зад плочата. Брановата природа на светлината предизвикува мешање на светлосните бранови кои поминуваат низ двата процепи создавајќи светли и темни ленти на екранот, додека апсорбирањето на екранот е во вид на дискретни точки, како поединечни честички. Друга верзија на овој експеримент вклучува детектори на процепите кои детектираат дека секој фотон поминува низ еден процеп (како честичка), а не низ двата процепи (како бран). [5][10]



Слика 2. Double-Slit Experiment

2.2.3. Суперпозиција

Суперпозицијата (Superposition) претпоставува дека еден квантен систем може да постои во повеќе состојби истовремено сè додека не се измери. Ова е спротивно на класичниот систем, каде еден објект постои во една единствена состојба во било кое време. Можните состојби во кои може да биде еден систем се претставени со неговата бранова функција. Овие состојби одговараат на различни својства, како што се положба, моментум или енергетско ниво. Суперпозиција вклучува комбинирање на две или повеќе квантни состојби со специфични коефициенти кои ја определуваат амплитудата и фазата на секоја состојба во суперпозицијата. На пример, квантен бит или кјубит е бит може да постои во суперпозиција од 0 и 1, што ги претставува двете вредности истовремено.

Еден од најпознатите експерименти кој ја објаснува суперпозицијата е Мачката на Шродингер. Во ова сценарио, се замислува дека мачката е истовремено жива и мртва сè додека не се направи набљудување што резултира во една дефинитивна состојба. На слика 3 е прикажана математичката равенка која ја објаснува суперпозицијата преку гореспоменатиот експеримент. Веројатноста за било која состојба е еднаква на апсолутната вредност на квадратот на соодветната амплитуда во равенката. Во оваа равенка, двете состојби имаат иста амплитуда од $\frac{1}{\sqrt{2}}$, која доколку се квадрира ќе даде $\frac{1}{2}$, т.е. 50% за мачката да биде во било која состојба. [11][12]

Слика 3. Математичка равенка за експериментот на Шродингер

2.2.4. Испреплетеност

Испреплетеност (Entanglement) се однесува на феномен во квантната физика каде што две или повеќе честички меѓусебно се поврзуваат или корелираат на таков начин што нивните индивидуални квантни состојби не можат да се опишат независно. Наместо тоа, квантните состојби на овие честички се поврзани заедно, без оглед на нивното физичко растојание. Ова значи дека состојбата на една честичка влијае на состојбата на другата (другите), дури и ако тие се оддалечени светлосни години, што го нарушува класичниот концепт на локалитет и брзината на светлината како горна граница за пренос на информации. [13][14]

2.2.5. Принцип на неопределеност

Принцип на неопределеност (Uncertainty Principle) е основен концепт во квантната механика формулиран од Вернер Хајзенберг во 1927 година. Тој вели дека одредени парови физички својства, како што се положбата и брзината на една честичка, не можат прецизно да се измерат во исто време. Колку попрецизно е познато едно својство, толку понепрецизно може да се одреди другото. Иако принципот на неопределеност е познат во квантната физика, сличен принцип важи и за проблемите во математиката и класичната физика, т.е. секој објект со својства слични на бранови ќе биде под влијание на овој принцип. [15][16]

2.2.6. Бранови функции

Брановата функција во квантната механика ја претставува квантната состојба на системот. Оваа математичка функција опфаќа важни информации за квантниот систем, вклучувајќи својства како моментум, време, позиција и спин. Во попрактична смисла, брановата функција го опишува однесувањето и карактеристиките на квантните честички, како што се електроните. Дава увид во веројатностите поврзани со различни аспекти на овие честички, како што се нивните позиции или моменти. Квадратот на големината на брановата функција ја дава густината на веројатноста, што укажува на веројатноста честичката да се најде во одредена состојба или локација. Исто така, обезбедува информации за распределбата на веројатноста на различни исходи кога се прават мерења на системот. [4][17]

2.3. Примена

Примените на квантната механика се обемни и покриваат широк опсег на полиња. Некои од клучните области каде што квантната механика наоѓа практична примена се:

- Квантно пресметување (Quantum Computing): Квантното пресметување ги користи принципите на квантната механика за да врши сложени пресметки поефикасно од класичните компјутери. Наместо класични битови, квантните компјутери користат кјубити, кои можат да бидат во суперпозиции на состојби. Квантните програмери се способни да манипулираат со суперпозицијата на кјубитите со цел да ги решат проблемите што класичното пресметување не може ефективно да ги направи, како што е пребарување во несортирани бази на податоци или факторизација на цели броеви. Квантните компјутери имаат потенцијал да направат револуција во полињата како што се криптографијата, оптимизацијата и симулацијата со решавање на проблеми кои моментално се нерешливи за класичните компјутери. [9]

- Квантна криптографија (Quantum Cryptography): Квантната криптографија ги користи принципите на квантната механика за да обезбеди комуникациски канали. Со искористување на квантните својства како што се дистрибуција на квантни клучеви (QKD) и квантна испреплетеност, квантната криптографија обезбедува сигурно средство за пренос на шифрирани информаци.

- Квантна комуникација и телепортација: Квантната механика овозможува безбедни комуникациски протоколи кои се отпорни на прислушување. Дополнително, концептот на квантна телепортација овозможува пренос на квантни информации помеѓу далечни локации преку искористување на испреплетеноста.

- Квантни сензори и метрологија: Квантните сензори и метролошките уреди ја користат чувствителноста и прецизноста што ги нуди квантната механика за мерење на физичките величини со исклучителна точност. Развиени се атомски часовници, магнетометри и квантни гравиметри, кои наоѓаат примена во навигацијата, геофизиката и прецизните мерења.

- Квантна хемија и наука за материјалите: Квантната механика обезбедува основа за разбирање на однесувањето на атомите, молекулите и материјалите. Квантната хемија користи пресметковни методи засновани на

квантна механика за проучување на хемиски реакции, молекуларни структури и електронски својства на материјалите.

- Квантна оптика и ласерска технологија: Квантната оптика ја истражува интеракцијата на светлината со материјата на квантно ниво. Има апликации во технологии како што се ласери, оптички влакна и фотонски уреди. Квантната механика овозможува развој на високо прецизни и ефикасни ласерски системи кои се користат во различни области, вклучувајќи ги телекомуникациите и медицината. [4][5][8]

3. Квантни компјутери

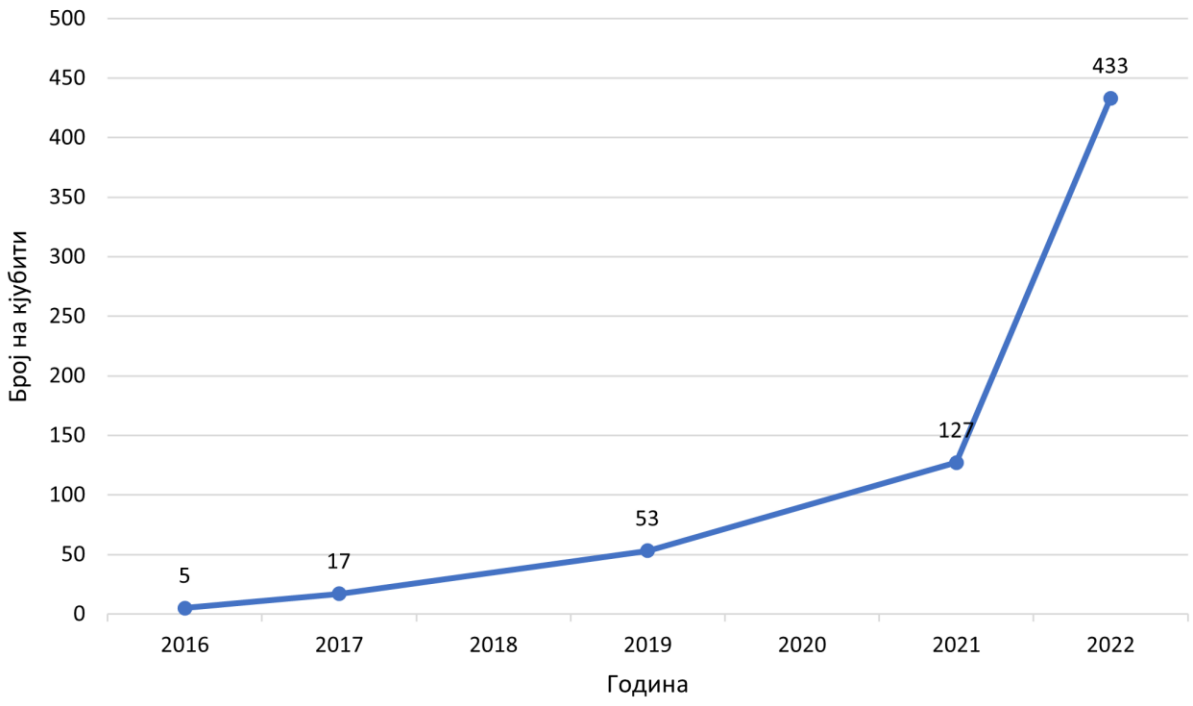
Квантното пресметување претставува револуционерен напредок во светот на обработката на информациите. За разлика од класичните компјутери кои се потпираат на битови како основна единица, квантните компјутери користат квантни битови или кјубити. Овие кјубити користејќи ги моќните својства на квантната механика, им овозможуваат на квантните компјутери да вршат одредени видови пресметки експоненцијално побрзо од нивните класични колеги.

Својството на суперпозиција им овозможува да истражуваат повеќе решенија за одреден проблем истовремено, што ги прави исклучително добри за задачи како разложување на големи броеви, оптимизирање на сложени системи и симулирање на квантна физика. Додека на класичните компјутери им требаат милиони години да факторизираат 300-цифрени броеви, на квантните им требаат часови. И покрај тоа што тие нема да ги заменат денешните компјутери, ќе можат да решат многу сложени статистички проблеми што денешните компјутери не можат. [18]

3.1. Историја

Почетоците на квантното процесирање датираат од 1980-тите години кога физичарот Ричард Фајнман го предложил моделот на квантен компјутер способен да симулира квантни системи и да решава сложени физички проблеми. Во 1994 година Питер Шор го претставил својот алгоритам со кој квантните компјутери ефикасно разложуваат големи цели броеви експоненцијално побрзо од традиционалните компјутери. Теоретски, алторитамот на Шор е способен да разбие многу криптосистеми кои се користат денес, но за тоа се потребни огромен број на кјубити. Во 1996 година, Лов Гровер претставил квантен алгоритам за пребарување во база на податоци кој е 4 пати побрз од пребарувањето со груба сила. Во 1998 година е изграден првиот квантен компјутер кој имал само 2 кјубити и со чија помош е решен алгоритамот на Гровер. Во 2001 година, IBM и Универзитетот во Стенфорд ја објавиле првата имплементација на алгоритамот на Шор со која 7-кјубитен процесор го факторира бројот 15 на неговите множители. Со ова започнува трката за градење на квантни компјутери кои имаат сè повеќе и повеќе кјубити. Како најголеми конкуренти се издвојуваат IBM кои во 2017 година го претставиле првиот комерцијално употреблив квантен компјутер (слика 4 и 5), и Google AI кои во 2019 година објавиле дека постигнале квантна надмоќ со 54-кјубитна машина изведувајќи пресметки невозможни за било кој класичен компјутер. [19][20]

Слика 4. Квантниот компјутер на IBM



Слика 5. Број на кјубити по години во најголемиот квантен процесор на IBM

3.2. Што е кјубит?

Дигиталните компјутери складираат и обработуваат информации користејќи битови кои можат да бидат или 0 или 1. Физички, бит може да биде сè што има две различни конфигурации: едната претставена со 0, а другата со 1. Во модерните компјутери и комуникации, битовите се претставени со отсуство или присуство на електричен сигнал кој кодира 0 и 1 соодветно. [21]

Квантен бит (кјубит) е секој бит направен од квантен систем, како електрон или фотон. Исто како и класичниот бит, кјубитот мора да има две различни состојби, една што претставува 0 и друга што претставува 1. Но, за разлика од класичниот бит, кјубитот може да биде во суперпозиција од двете состојби, со одредена веројатност да биде 0 и одредена веројатност да биде 1. Тоа значи дека еден кјубит ψ може да се претстави како линеарна комбинација од $|0\rangle$ и $|1\rangle$:

$$\psi = \alpha|0\rangle + \beta|1\rangle,$$

каде α и β се комплексни веројатносни амплитуди за секоја состојба. Кога ќе се измери овој кјубит, веројатноста за исход $|0\rangle$ со вредност 0 е $|\alpha|^2$, додека веројатноста за исход $|1\rangle$ со вредност 1 е $|\beta|^2$. Бидејќи апсолутните квадрати на амплитудите претставуваат веројатности, мора да важи следното:

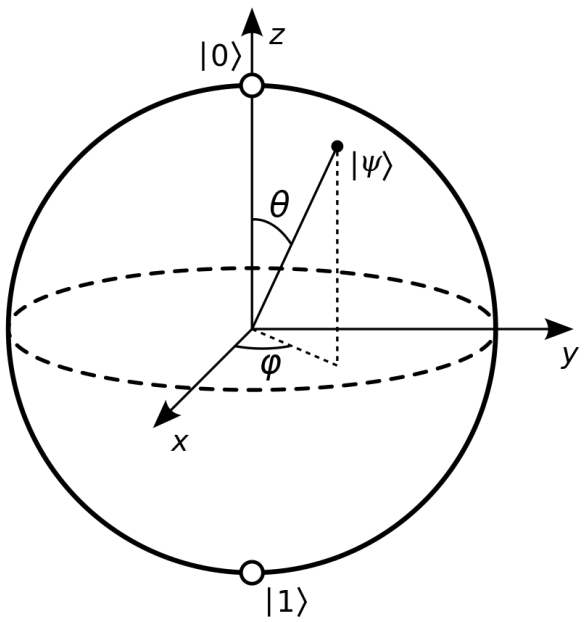
$$|\alpha|^2 + |\beta|^2 = 1.$$

На слика 6 може да се види кјубитот ψ претставен во сферата на Блох. [21][22] Според оваа сфера, амплитудите може да се изразат преку аглите θ и ϕ, т.е.

$$\alpha = \cos\left(\frac{\theta}{2}\right) \text{ и } \beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right).$$

Ако имаме два кјубити, тогаш тие можат да бидат во суперпозиција од четири состојби: 00, 01, 10 и 11, што се претставува како

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$



Слика 6. Сферата на Блох

За претставување на два кјубити потребни се 4 веројатности или амплитуди (a, b, c и d), за три кјубити се потребни 8. Значи, ако имаме n кјубити, ќе ни требаат 2^n броеви за да ја претставиме целокупната состојба на тој квантен систем. Со мало зголемување на бројот на кјубити ќе можеме да генерираме системи што можат да претставуваат огромен број на состојби што е незамисливо споредбено со класичните компјутери. Но дури и ако количината на информации потребни за да се опише суперпозицијата расте експоненцијално со бројот на кјубити, не можеме да пристапиме до сите овие информации заради фундаменталните лимити на квантната механика. Спинот на електрон во суперпозиција може да биде во сите правци, но кога ќе се измери, тој мора да биде во една насока или свртен нагоре или свртен надолу. Исто така, не можеме да го предвидиме резултатот од мерењето, тој е непредвидлив заснован на веројатноста поврзана со состојбата, има одредена веројатност да биде свртен надолу и одредена веројатност да биде свртен нагоре. Тоа значи, за да се искористи целосниот потенцијал на квантен компјутер, треба да развиеме квантни алгоритми кои ќе знаат да го искористат постоењето на огромна количина на информации зачувани во суперпозицијата на кјубити, но на крајот на пресметката да го оставиме системот во една од основните состојби што со сигурност можат да се детектираат. [23]

3.3. Операции на кјубити

Постојат различни видови на физички операции кои можат да се извршат на кјубити. Како најважни се издвојуваат: [22]

- Квантни логички порти се основни единици за квантно коло во квантен компјутер кои работат на множество кјубити (регистар). Математички, кјубитите се подложени на реверзибилна унитарна трансформација опишана со множење на унитарната матрица на квантната порта со векторот на квантната состојба. Резултатот од ова множење е нова квантна состојба.

- Квантно мерење е неповратна операција во која се добиваат информации за состојбата на еден кјубит. Резултат од мерењето на еден кјубит со состојба $\psi = \alpha|0\rangle + \beta|1\rangle$ ќе биде или $|0\rangle$ со веројатност $|\alpha|^2$ или $|1\rangle$ со веројатност $|\beta|^2$. Мерењето на состојбата на кјубитот ги менува вредностите на α и β. Ако се измери кјубит кој е испреплетен, тогаш мерењето може да ја промени состојбата на другите заплеткани кјубити.

- Иницијализација или ре-иницијализација до позната вредност, најчесто $|0\rangle$. Со оваа операција се менува квантната состојба (исто како мерењето). Иницијализацијата може да се имплементира логички (по мерење со примена на Паулиева-X порта доколку резултатот од мерењето е $|1\rangle$) или физички (доколку се работи за суперспроводлив фазен кјубит, со намалување на енергијата на квантниот систем до неговата основна состојба).

- Испраќање на кјубит преку квантен канал до оддалечен систем или машина, потенцијално како дел од квантна мрежа.

3.4. Квантни логички порти

Квантните логички порти се основните компоненти на квантните кола, исто како што класичките логички порти се за класичните кола. Тие вршат операции на еден или повеќе кјубити и се клучни во имплементацијата на квантните алгоритми. Квантните логички порти се разликуваат од класичните логички порти по тоа што прикажуваат суперпозиција, заплеткување и интерференција. Кјубитите може да се заплеткаат, при што нивните состојби се во корелација, дури и ако се оддалечени еден од друг. Тие исто така можат да влијаат едни на други, предизвикувајќи резултатот на квантната логичка порта да зависи од состојбите на сите кјубити во колото. [24]

За разлика од повеќето класични логички порти, квантните логички порти се реверзибилни. Една порта што дејствува на n кјубити е претставена со $2^n \times 2^n$ унитарна матрица[1]. Квантните состојби врз кои портата дејствува се вектори во 2^n комплексен простор. Доколку се измерат, тогаш основните вектори се можни резултати, а квантната состојба е линеарна комбинација на овие резултати. Најчесто користените квантни порти работат на простори од еден или два кјубити, исто како што работат и класичните логички порти. [25]
Векторската репрезентација на еден кјубит е

$$|a\rangle = v_0|0\rangle + v_1|1\rangle \rightarrow \begin{bmatrix} v_0 \\ v_1 \end{bmatrix}$$

каде v_0 и v_1 се веројатносните амплитуди на кјубитот. Вредноста 0 се претставува со векторот $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, а вредноста 1 со векторот $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

[1] Една инверзибилна комплексна квадратна матрица U е унитарна доколку нејзината инверзна матрица е еднаква на нејзината конјугирана транспонирана матрица, т.е. $U^{-1} = U^{\dagger}$.

Тенсор производот (се бележи со $\otimes$) служи за комбинирање на квантни состојби. Комбинираната состојба за регистарот е тенсорски производ од состојбите на составните кјубити. Со тоа, векторската репрезентација на два кјубити е

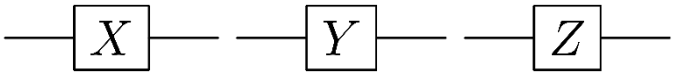
$$|ab\rangle = |a\rangle \otimes |b\rangle = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle \rightarrow \begin{bmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{bmatrix}$$

Со множење на унитарната матрица U, која претставува одредена порта, со векторот $|\psi_1\rangle$, кој ја претставува квантната состојба, се добива нова квантна состојба $|\psi_2\rangle$, т.е. $U|\psi_1\rangle = |\psi_2\rangle$.

3.4.1. Паулиеви (X, Y, Z) порти

Паулиевите порти се основните квантни логички порти за извршување на операции на еден кјубит. Тоа се три 2x2 матрици кои се претставуваат со X, Y и Z (слика 7). Тие претставуваат ротација околу x, y и z оските, соодветно, на сферата на Блох за π радијани.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



Слика 7. Паулиеви (X, Y, Z) квантни логички порти

Паулиевата X порта е квантен еквивалент на класичната НЕ порта која го мапира $|0\rangle$ во $|1\rangle$ и $|1\rangle$ во $|0\rangle$. Поради нејзината природа, оваа порта е наречена и променувач на состојбата на бит.

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle, \qquad X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

Паулиевата Y порта го мапира $|0\rangle$ во $i|1\rangle$ и $|1\rangle$ во $-i|0\rangle$ со што врши операции на промена на бит и промена на фаза на кјубитот. Паулиевата Z порта ја остава основната состојба $|0\rangle$ непроменета и го мапира $|1\rangle$ во $-|1\rangle$ со што врши операција на промена на фаза додавајќи фазно поместување од 180 степени на состојбата на кјубитот. [24][25][26]

3.4.2. Адамар (H) порта

Адамар (Hadamard) логичката порта е една од најчесто користените квантни логички порти. Дејствува на еден кјубит и служи за да го трансформира кјубитот од неговата моментална состојба во еднаква суперпозиција од двете можни состојби. Нејзината унитарна матрица и симбол се следните:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad —\boxed{H}—$$

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Адамар портата има едно својство кое е од витално значење за квантното пресметување. Ако имаме регистар со n кјубити во состојба $|0\rangle$ и примениме Адамар порта на секој кјубит, тогаш резултот е еднаква суперпозиција од сите цели броеви во опсегот од 0 до $2^n - 1$, т.е.

$$H|0\rangle \otimes H|0\rangle \otimes \ldots \otimes H|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle$$

каде $|j\rangle$ е резултантната состојба која ја претставува бинарната репрезентација на бројот j_{10}. На пример, во 7-кјубитен регистар, состојбата $|19\rangle$ одговара на резултантната состојба $|0010011\rangle$. Првите два бита (00) служат за пополнување, додека 10011_2 одговара на 19_{10}. [24][26]

3.4.3. Порти за промена на фаза (Z, S, T)

Портите за промена на фаза се фамилија од порти кои дејствуваат на еден кјубит и ги мапираат основните состојби $|0\rangle$ во $|0\rangle$ и $|1\rangle$ во $e^{i\varphi}|1\rangle$. Веројатноста да се измери $|0\rangle$ или $|1\rangle$ не се менува по примената на оваа порта, но сепак се менува фазата на квантната состојба. Ефектот од овие порти е ротирање на состојбата на кјубитот околу z-оската на сферата на Блох за φ радијани. Имаат примена во многу квантни алгоритми, како што се корекција на квантна грешка, подготовка на квантна состојба и квантна телепортација. [24][25]
Матрицата на овие порти е следната:

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

Во зависност од изборот на фазното поместување φ, може да има повеќе порти:

- $\varphi = \pi$: Ова ја претставува Паулиевата Z порта, којашто е објаснета погоре.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P(\pi)$$

- $\varphi = \frac{\pi}{2}$: Ова ја претставува S портата која ја ротира состојбата на кјубитот за $\frac{\pi}{2}$ радијани околу z-оската. Нејзината матрица е:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = P\left(\frac{\pi}{2}\right) = \sqrt{Z}$$

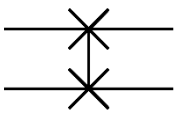
- $\varphi = \frac{\pi}{4}$: Ова ја претставува T портата која ја ротира состојбата на кјубитот за $\frac{\pi}{4}$ радијани околу z-оската. Нејзината матрица е:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{\sqrt{2}}{2}(1+i) \end{bmatrix} = P\left(\frac{\pi}{4}\right) = \sqrt{S} = \sqrt[4]{Z}$$

3.4.4. SWAP порта

SWAP портата е дво-кјубитна квантна логичка порта која е основен градежен блок во квантните алгоритми и игра важна улога во квантната обработка на информации. Оваа порта делува како порта за размена, што значи дека ја заменува состојбата на двата кјубита на кои работи. Исто така може да се искористи за да се смени редоследот на кјубитите во квантен регистар, што може да биде корисно за одредени квантни алгоритми. [24]
Матрицата и симболот на SWAP портата се дадени во продолжение:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

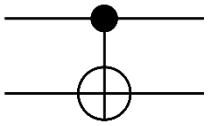


3.4.5. Контролирани квантни порти

За да се изведат нетривијални пресметки, често е неопходно да се смени операцијата која се применува на одредени кјубити во зависност од вредностите на други кјубити. Портите што ги спроведуваат овие операции се наречени контролирани порти. Има многу вакви порти, но најважни се: [26]

- Контролирана НЕ (CNOT) порта е дво-кјубитна квантна логичка порта која дејствува како условна НЕ порта, каде состојбата на целниот кјубит зависи од состојбата на контролниот кјубит. Оваа порта ја негира состојбата на вториот кјубит акко првиот кјубит е во состојба $|1\rangle$, инаку не прави ништо. Има голема примена во алгоритми за квантна телепортација и квантна корекција на грешка. Нејзините матрица, симбол и табела на состојби се прикажани на слика 8. [24]

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

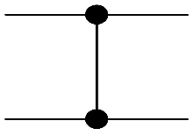


Влез	Излез
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Слика 8. Контролирана НЕ (CNOT) квантна логичка порта

- Контролирана Z (CZ) порта е дво-кјубитна квантна логичка порта која за разлика од CNOT портата, ја менува фазата наместо состојбата на целниот кјубит врз основа на контролниот кјубит. Ако контролниот кјубит е во состојба $|0\rangle$, тогаш CZ портата не влијае, но доколку е во состојба $|1\rangle$, тогаш CZ применува фазно поместување на целниот кјубит. Оваа порта е доста значајна во квантното процесирање бидејќи овозможува испреплетување на кјубити. [24]

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

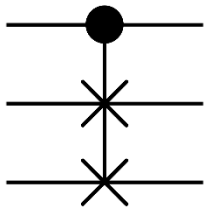


Влез	Излез
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

Слика 9. Контролирана Z (CZ) квантна логичка порта

- Контролирана SWAP (CSWAP, FREDKIN) е порта која дејствува врз три кјубити на тој начин што ги заменува (врши SWAP операција) на вториот и третиот кјубит акко првиот кјубит е во состојба $|1\rangle$. Генерализирана $n \times n$ FREDKIN порта не ги менува првите $n-2$ кјубити, а ги заменува состојбите на последните два кјубити само ако првите $n-2$ кјубити се во состојба $|1\rangle$. Може да се види дека оваа порта е реверзибилна, т.е. може да се дојде до почетната состојба доколку се примени истата порта на резултатот. [26][27]

$$CSWAP = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

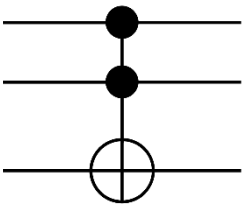


Влез	Излез
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|110\rangle$
$\|110\rangle$	$\|101\rangle$
$\|111\rangle$	$\|111\rangle$

Слика 10. Контролирана SWAP (CSWAP) квантна логичка порта

- Toffoli (Controlled-Controlled-NOT, CCNOT) е квантна логичка порта која дејстува на три кјубити. Оваа порта е пример за котролирана логичка порта која има повеќе од еден контролен кјубит. Оперира на тој начин што извршува НЕ операција на третиот (целниот) кјубит само ако првите два се во состојба $|1\rangle$, инаку не прави ништо. Оваа порта е клучна компонента во повеќе квантни алгоритми, како што се квантна корекција на грешка и квантни симулации, но и за изградбата на други квантни порти. [24][26]

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$



Влез	Излез
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|101\rangle$
$\|110\rangle$	$\|111\rangle$
$\|111\rangle$	$\|110\rangle$

Слика 11. Toffoli (CCNOT) квантна логичка порта

4. Квантни алгоритми

Класичен алгоритам е конечна низа од инструкции, или чекор-по-чекор процедура за решавање на проблем, каде што секој чекор или инструкција може да се изврши на класичен компјутер. Слично на ова, квантен алгоритам е чекор-по-чекор процедура, каде што секој од чекорите може да се изврши на квантен компјутер. Иако сите класични алгоритми може да се извршат и на квантен компјутер, терминот квантен алгоритам обично се користи за оние алгоритми кои се по природа квантни или користат некоја суштинска карактеристика на квантното пресметување како што е суперпозиција или испреплетеност.

Проблемите кои се нерешливи со класични компјутери остануваат нерешливи и со користење на квантните компјутери. Моќта на квантните алгоритми е тоа што тие би можеле да решат некои проблеми многу побрзо од класичните алгоритми бидејќи квантната суперпозиција и квантната испреплетеност кои ги користат квантните алгоритми не можат да бидат ефикасно симулирани на класичните компјутери.

Квантните алгоритми се претставуваат преку најкористениот модел за квантно пресметување, а тоа е моделот на квантно коло. Квантното коло, слично како класичното коло, се состои од квантни логички порти кои дејствуваат на фиксен број на кјубити и извршуваат операции како мерење или иницијализација на кјубити. Квантите алгоритми може да се категоризираат според главните техники кои ги користат (повраток на фаза, проценка на фаза, квантна Фуриева трансформација, квантно случајно движење, засилување на амплитудата), но и според типот на проблемот кој го решаваат. [28][29]

4.1. Алгоритми базирани на квантна Фуриева трансформација

Квантната Фуриева трансформација (QFT) е квантна алгоритамска постапка аналогна на класичната Фуриева трансформација, но дизајнирана да работи на квантни податоци користејќи ги принципите на квантната механика. Во класичното пресметување, Фуриевата трансформација се користи за анализа на фреквентните компоненти на сигналот, т.е. го трансформира сигналот од неговиот оригинален домен (како што е времето) во фреквентниот домен. Квантната Фуриева трансформација извршува слична задача, но работи на квантни состојби и е особено моќна за одредени типови на квантни алгоритми.

- Алгоритамот на Шор е квантен алгоритам кој служи за наоѓање на простите множители на цел број преку решавање на дискретниот логаритамски проблем. Се извршува во полиномно време, додека на најдобрите класични алгоритми им треба суперполиномно време[2]. Исто така, тој е еден од ретките квантни алгоритми што решава проблем на не-црна кутија[3] во полиномно време.

- Дојч-Јожа алгоритамот решава проблем на црна кутија што бара експоненцијално многу прашања до црната кутија за кој било детерминистички класичен компјутер, но може да се направи со едно барање од квантен компјутер. Алгоритмот одредува дали функцијата f е или константна (0 на сите влезови или 1 на сите влезови) или избалансирана (враќа 1 за половина од влезниот домен и 0 за другата половина). [30]

- Алгоритамот на Симон е еден од првите квантни алгоритми што покажал експоненцијално забрзување над најпознатите класични алгоритми за одреден проблем. Овој алгоритам го решава проблемот на Симон кој треба да одреди дали дадена функција $f: \{0,1\}^n \to \{0,1\}^n$ е еден-на-еден (секој влез се пресликува во единствен излез) или два-на-еден (секој излез одговара на точно два различни влеза). Со класичен компјутер, функцијата треба да се повика најмалку $2^{n-1}+1$ пати за да се дојде до заклучок, додека на квантниот алгоритам на Симон му требаат само $O(n)$ повици. Иако овој алгоритам нема директни примени, ги поставил темелите за подоцнежните квантни алгоритми, вклучувајќи го и алгоритамот на Шор. [31]

4.2. Алгоритми базирани на амплитудно засилување

Амплитудното засилување е техника која се користи во квантните алгоритми за да се зголеми веројатноста за добивање на посакуваниот исход додека се намалува веројатноста за несакани исходи. Обично доведува до квадратни забрзувања во однос на соодветните класични алгоритми. Оваа техника е воведена од Лов Гровер во 1996 година и е основна компонента на алгоритамот на Гровер. [28]

[2] Еден алгоритам се извршува во суперполиномно време доколку не е ограничен од горе со ниту еден полином.
[3] Црна кутија се однесува на систем или процес што може да се разгледува во однос на неговите влезови и излези, без да се земе во предвид неговата внатрешна функционалност.

- Алгоритамот на Гровер е квантен алгоритам кој служи за пребарување во неструктурирана база на податоци или неподредена листа. Доколку имаме N записи, со класичен алгоритам треба во просек $N/2$ повици, што има комплексност од $O(N)$. Со користење на алгоритамот на Гровер се постигнува квадратно забрзување, со што се намалува комплексноста на $O(\sqrt{N})$. [32]

- Алгоритамот за квантно броење е генерализација на алгоритамот за пребарување (алгоритамот на Гровер). Наместо само да открие дали постои одреден запис, наоѓа и колку пати тој запис се појавува во дадената структура. [33]

4.3. Алгоритми базирани на квантно случајно движење

Квантно случајно движење е квантна верзија на класичното случајно движење, што е математички модел кој опишува процес каде што ентитетот случајно преминува помеѓу различни состојби во низа од дискретни чекори. Во квантното движење, ентитетот ги следи принципите на квантната механика и може да се опише со квантна суперпозиција над состојбите. Оваа катерогија на алгоритми обезбедуваат полиномно забрзување за многу проблеми и експоненцијално забрзување за некои проблеми на црна кутија. [28]

- Проблемот на различни елементи утврдува дали сите елементи во одредена листа се различни. Во најлош случај, потребни се N повици за листа со големина N, но со користење на квантен компјутер, овој проблем може да се забрза. Постојат повеќе квантни алгоритми за решавање на овој проблем, но како најбрз се издвојува алгоритамот на Андрис Амбаинис на кој му требаат само $O(n^{2/3})$ повици. [34]

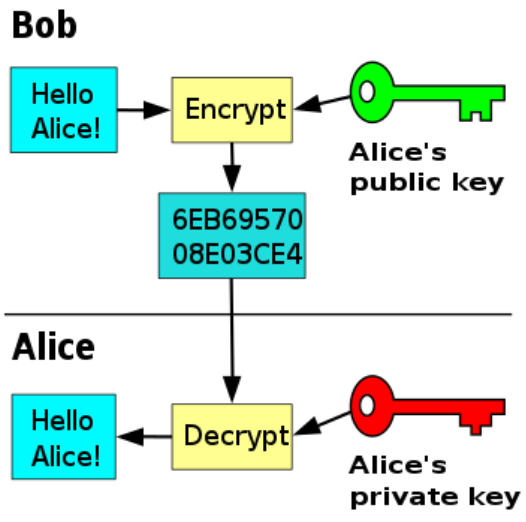
- Проблемот за наоѓање на триаголник утврдува дали одреден граф содржи триаголник (циклус со големина 3). Најефикасни квантни алгоритми се алгоритамот на Магниез, Санта и Сегеди со комплексност $O\left(n^{13/10}\right) = O(n^{1.3})$ [35] и алгоритамот на Беловс кој има комплексност од $O\left(n^{35/27}\right) = O(n^{1.296})$.

5. Криптографија со јавен клуч

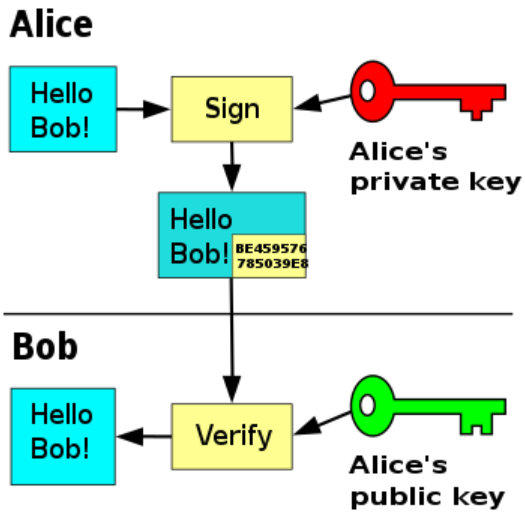
Криптографија со јавен клуч, или асиметрична криптографија е еден вид на криптографија која користи парови на клучеви за шифрирање и дешифрирање на податоци. Секој пар клучеви се состои од јавен клуч и соодветен приватен клуч. Овие парови се генерираат со криптографски алгоритми базирани на математички проблеми наречени еднонасочни функции. Јавниот клуч е криптографски клуч што може да го користи секое лице за шифрирање на порака така што пораката може да се дешифрира само од наменетиот примач со неговиот приватен клуч (слика 12).

Исто така, овој вид на криптографија се користи и во процесот на дигитално потпишување на пораки. Испраќачот го користи својот приватен клуч за да потпише одредена порака. Секој кој го има соодветниот јавен клуч може да потврди дали потписот се совпаѓа со пораката (слика 13).

Алгоритмите со јавен клуч се основни безбедносни концепти во современите криптосистеми, вклучувајќи апликации и протоколи кои нудат гаранција за доверливост и автентичност на електронските комуникации и складирањето податоци. Тие поддржуваат бројни интернет стандарди како што се TLS, SSH, S/MIME и PGP. Некои алгоритми обезбедуваат дистрибуција и тајност на клучот (Diffie-Hellman), некои обезбедуваат дигитални потписи, а некои ги обезбедуваат и двете (RSA). Во споредба со симетричното шифрирање, асиметричното е прилично побавно, па затоа денешните криптосистеми најчесто користат асиметрично шифрирање за безбедна размена на таен клуч кој потоа се користи за симетрично шифрирање. [36][37]



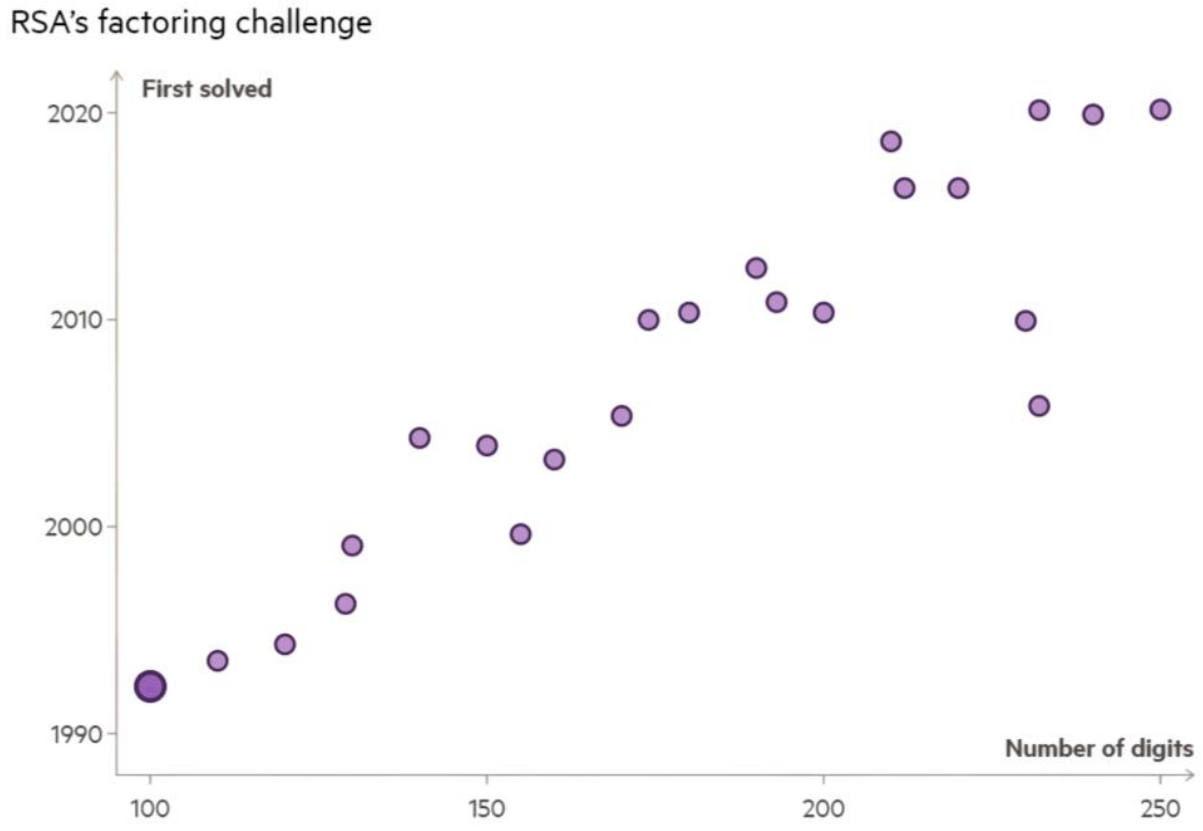
Слика 12. Шифрирање и дешифрирање



Слика 13. Дигитално потпишување

5.1. RSA криптосистем

RSA (Rivest Shamir Adleman) е криптосистем со јавен клуч кој е широко користен за безбеден пренос на податоци. Акронимот „RSA” доаѓа од презимињата на Ron Rivest, Adi Shamir и Leonard Adleman, тројцата научници кои го измислиле и јавно објавиле овој алгоритам во 1977 година. Основниот проблем брз кој се базира RSA е проблемот на факторизација на два броја, т.е. ако имаме n=pq, каде p и q се многу големи прости броеви, тогаш е речиси невозможно да се најдат p и q со помош на денешните компјутери. RSA е релативно бавен алгоритам и затоа вообичаено не се користи за директно шифрирање на податоци, туку за пренос на клучеви за криптографија со симетричен клуч. [38][39][40]



Слика 14. Разложување на големи броеви во текот на годините

5.1.1. Генерирање на клучеви

RSA користи јавен и приватен клуч. Јавниот клуч може секој да го знае и се користи за шифрирање на пораки, кои потоа се дешифрираат со помош на приватниот клуч. Овие клучеви се генерираат на следниот начин:

1. Одбери два различни големи прости броеви p и q.
2. Пресметај го нивниот производ $n = pq$.
3. Пресметај $\varphi(n) = (p-1)(q-1)$.
4. Одбери цел број e, т.ш. $1 < e < \varphi(n)$ и $НЗД(e, \varphi(n)) = 1$.
5. Пресметај d според формулата $d \equiv e^{-1} \bmod(\varphi(n))$.

Со овие пет чекори се добиваат јавниот клуч (n,e) и приватниот клуч (n,d) кои потоа се користат за шифрирање и дешифрирање на пораки.

5.1.2. Шифрирање и дешифрирање

За да може праќачот да испрати порака M до примачот, тој мора да го има јавниот клуч на примачот. Тој потоа ја претвора пораката M во број m таков што $1 \leq m \leq n$ со користење на претходно договорен протокол. На крај ја шифрира пораката m како $c \equiv m^e (\bmod n)$ и добиената вредност ја испраќа.

Примачот може лесно да ја дешифрира пораката c со користење на неговиот приватен клуч, т.е. $m \equiv c^d (\bmod n)$. Со тоа ќе ги добие бројот m и оригиналната порака M.

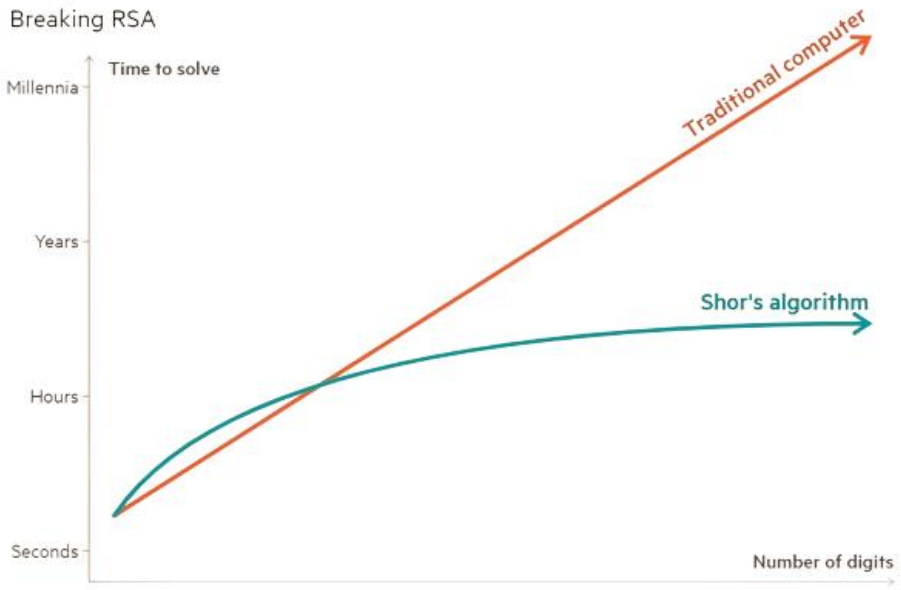
5.1.3. Пример за шифрирање и дешифрирање преку RSA алгоритамот

Нека $p = 47,\ q = 59$. Тогаш $n = pq = 47 \times 59 = 2773$ и $\varphi(2773) = 46 \times 58 = 2668$. Нека $e = 17$ со што се добива $d \equiv 17^{-1} (\bmod 2668)$, т.е. $d = 157$. Доколку сакаме да ја шифрираме пораката M = ITS ALL GREEK TO ME, користејќи ја шемата: празно место = 00, A = 01, B = 02, …, Z = 26, добиваме:
m = 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500.
Оваа порака се шифрира блок по блок со користење на јавниот клуч (2773, 17), т.е. $920^{17} (\bmod 2773) = 948$ и се добива
c = 0948 2342 1084 1444 2663 2390 0778 0774 0219 1655.
По слична постапка, примачот може да ја дешифрира добиената порака со помош на својот приватен клуч. [39][40]

6. Алгоритамот на Шор

Во 1994 година е претставен квантен алгоритам за факторизација на броеви од страна на американскиот математичар Питер Шор. Овој алгоритам овозможува ефикасна факторизација на големи сложени броеви на нивните прости множители. Има големо значење бидејќи има потенцијал да ги разбие широко користените шеми за шифрирање, како што е RSA, чија безбедност се заснова на претпоставката дека факторирањето на големи броеви е пресметковно неостварлива задача за класичните компјутери, особено кога се работи со многу големи броеви (слика 15). [41][42]

Алгоритамот на Шор ги користи уникатните својства на квантните компјутери, особено способноста на кјубитите да постојат во суперпозиција и да вршат повеќе пресметки истовремено, овозможувајќи му да работи побрзо од најпознатите класични алгоритми. Како и сите квантни компјутерски алгоритми, и овој алгоритам е веројатносен, т.е. го дава точниот одговор со голема веројатност, а веројатноста за неуспех може да се намали со повторување на алгоритамот. [43] Во практична смисла, доколку се создадат големи, толерантни на грешки квантни компјутери, овој алгоритам може да претставува значајна закана за класичните методи на шифрирање. Со ова се поттикнува развојот на пост-квантната криптографија, која има за цел да создаде алгоритми за шифрирање кои остануваат безбедни дури и во присуство на квантни компјутери. [41]



Слика 15. Време потребно да се пробие RSA со класичен компјутер и со алгоритамот на Шор

Алгоритамот на Шор се состои од два дела:

1. Редукција на проблемот на факторизација до проблем на наоѓање на ред.
2. Квантен алгоритам за решавање на проблемот за наоѓање на ред.

6.1. Класична редукција

Нека бројот кој треба да се факторизира е N. Потребно е N да биде сложен, непарен број и да не е во форма n^x. Доколку N исполнува еден од овие услови, тогаш е многу лесно да се најдат неговите множители. Со помош на следните чекори може да се направи факторизација на N:

1. Одбери случаен број $1 < a < N$.
2. Пресметај $НЗД(a, N)$.
3. Ако $НЗД(a, N) \neq 1$, тогаш a е нетривијален делител на N, а другиот е N/a и со тоа алгоритамот завршува.
4. Најди го редот r со користење на квантен алгоритам, т.ш. $a^r \equiv 1 \pmod N$.
5. Ако r е непарен врати се на чекор 1.
6. Пресметај $g = НЗД(N, a^{r/2} + 1)$. Доколку g е нетривијален делител, тогаш другиот делител е N/g и алгоритамот завршува, инаку врати се на чекор 1.

6.2. Квантен алгоритам за наоѓање на ред

Целта на квантниот алгоритам е да го најде редот r при дадени взаемно прости броеви N и $1 < a < N$, каде r е најмалиот позитивен цел број така што $a^r \equiv 1 \pmod N$. Овој алгоритам го користи својството на суперпозиција. Се дефинира квантна операција која како влез зема број x и пресметува a^x. Потоа друга операција го наоѓа остатокот k, таков што $a^x = mN + k$, за некој број m. Доколку како влез се даде суперпозиција од броеви и врз нив се применат претходно опишаните операции, тогаш се добива суперпозиција од различните броеви и нивните соодветни остатоци, т.е. [44]

$$|1\rangle + |2\rangle + |3\rangle + \cdots \rightarrow |1, a^1\rangle + |2, a^2\rangle + |3, a^3\rangle + \cdots \rightarrow |1, k_1\rangle + |2, k_2\rangle + |3, k_3\rangle + \cdots$$

Следен чекор е да се измери добиената суперпозиција за да се добие еден случајно одбран остаток k со што ќе се добие суперпозиција со исти остатоци., т.е.

$$|i, k\rangle + |j, k\rangle + |l, k\rangle + \cdots$$

Следно, го користиме својството: Ако $a^x = mN + k$, тогаш $a^{x+p} = sN + k$, каде $m \neq s$. Ова својство гарантира дека остатокот k ќе остане ист доколку експонентот x се зголеми или намали за p. Со ова се заклучува дека сите експоненти во последната добиена суперпозиција се разликуваат за период r, односно фреквенција $1/r$.

За да се добие периодот, се користи квантна Фуриева трансформација, која е дефинирана на следниот начин: [45]

$$|x\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} e^{\frac{2\pi i}{q} xy} |y\rangle = \frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} \omega^{xy} |y\rangle$$

каде $N^2 \leq q = 2^n < 2N^2$, за некое n. Доколку врз суперпозицијата од експонентите се примени квантната Фуриева трансормација, тогаш ќе се добие суперпозиција од фреквенции:

$$|i\rangle + |j\rangle + |l\rangle + \cdots = |x\rangle + |x + r\rangle + |x + 2r\rangle + \cdots \xrightarrow{QFT} |\frac{1}{r}\rangle + |\frac{2}{r}\rangle + |\frac{3}{r}\rangle + \cdots$$

Со мерење на резултантната суперпозиција повеќе пати, ќе се добијат повеќе фрекевенции кои имаат заеднички множител кој е еднаков на $1/r$. Од тука се добива бројот r, кој го претставува редот кој се бара. [46]

6.3. Факторизација на број со алгоритамот на Шор

Нека бројот кој сакаме да го факторизираме е $N = 357$. Најпрво одбираме број $a < N$, нека $a = 205$. Пресметуваме $НЗД(205, 357) = 1$, што значи дека може да се искористи квантниот алгоритам за наоѓање на ред. Поставуваме почетна суперпозиција од цели броеви и го применуваме операциите за степенување и наоѓање на остаток.

$$|1\rangle + |2\rangle + |3\rangle + |4\rangle + \cdots$$
$$\xrightarrow{205^x} |1, 205\rangle + |2, 42025\rangle + |3, 8615125\rangle + |4, 1766100625\rangle + \cdots$$
$$\xrightarrow{k} |1, 205\rangle + |2, 256\rangle + |3, 1\rangle + |4, 205\rangle + \cdots$$

Доколку ја измериме последно добиената суперпозиција, ќе се добие суперпозиција од броеви кои имаат ист остаток, нека $k = 205$. Со примена на квантната Фуриева

трансформација на оваа суперпозиција, се добиваат фреквенциите на почетните броеви, а со тоа и периодот (редот) $\mathrm{r} = 3$. Бидејќи r е непарен број, мора да се вратиме на почеток и да избереме нов број. Нека $\mathrm{a} = 152$. Со примена на квантниот алгоритам за наоѓање на ред добиваме $\mathrm{r} = 6$ и пресметуваме

$$\text{НЗД}\left(\mathrm{N}, \mathrm{a}^{\mathrm{r}/2} + 1\right) = \text{НЗД}(357, 152^3 + 1) = 357.$$

Со ова добиваме дека множителите на 357 се 357 и 1, кои се тривијални, што значи дека факторизацијата е неуспешна. Затоа одбираме нов број $\mathrm{a} = 52$. $\text{НЗД}(357, 52) = 1$ и $\mathrm{r} = 6$. $\text{НЗД}(357, 52^3 + 1) = 7$ е едниот множител на 357, додека другиот е $357/7 = 51$ и со тоа алгоритамот завршува. [47]

7. Практична имплементација

Во оваа глава ќе биде опишана практичната имплементација на RSA криптосистемот и алгоритамот на Шор. Овие два алгоритми ќе бидат имплементирани во програмскиот јазик Python, додека за алгоритамот на Шор дополнително ќе се користи библиотеката за симулација на квантни алгоритми, Qiskit.

7.1. Опис и основни карактеристики на Qiskit

Qiskit (Quantum Information Software Kit) е библиотека за развој на софтвер со отворен код. Служи за работа со квантни компјутери на ниво на кола, импулси и алгоритми. Обезбедува алатки за креирање и манипулирање на квантни програми и нивно извршување на прототипови на квантни уреди или на симулатори на локален компјутер. [49] Го следи моделот на колото за универзално квантно пресметување и може да се користи за кој било квантен хардвер. Основната верзија на Qiskit го користи програмскиот јазик Python, но истражувани се и верзии за Swift и JavaScript, чиј развој е запрен.

Qiskit е направен од елементи кои работат заедно за да овозможат квантно пресметување. Централната цел на Qiskit е да изгради софтверски пакет што ќе му олесни на секој да користи квантнен компјутер, без оглед на нивното ниво на вештина или област на интерес. Qiskit им овозможува на корисниците да дизајнираат алгоритми и апликации и да ги извршуваат на вистински квантни компјутери. Главните елементи кои го овозможуваат ова се:

- Елементот Terra е темелот врз кој е изграден Qiskit. Terra обезбедува алатки за креирање, визуелизација и оптимизација на квантни кола на (или блиску до) нивото на кодот на квантната машина, што овозможува процесите кои работат на квантен хардвер да бидат конструирани преку квантни порти.

- Елементот Aer обезбедува алатки за симулација на квантни алгоритми, како симулација на вектор на состојба, унитарна симулација и други. Со други зборови, Aer им овозможува на корисниците да го симулираат однесувањето на квантните кола на класичните компјутери.

- Елементот Ignis[4] обезбедува алатки за проверка на квантниот хардвер, детекција на шум и корекција на грешки, како и алатки кои овозможуваат пресметките да се извршуваат во присуство на шум.

- Елементот Aqua[5] е библиотека на Qiskit за квантни алгоритми и апликации. Вклучува разновидни претходно изградени квантни алгоритми за оптимизација, машинско учење, финансии и хемија. Aqua им овозможува на корисниците да експериментираат и да применуваат квантни алгоритми за проблеми од реалниот свет.

7.2. Имплементација на RSA во Python

Најпрво ја креираме функцијата rsa која служи за генерирање на јавен и приватен клуч со помош на два прости броја p и q (слика 16). За успешно енкриптирање и декриптирање на пораки без броеви и специјални знаци, може да се додаде услов кој ќе обезбеди модулот n да биде поголем од 26.

```
def rsa(p, q):
    if is_prime(p) == False or is_prime(q) == False:
        raise ValueError('Both numbers have to be prime.')

    n = p * q
    # if n < 26:
    #     raise ValueError('The product of p and q has to be greater than 26.')

    totient = (p - 1) * (q - 1)

    for e in range(2, totient):
        if numpy.gcd(e, totient) == 1:
            break

    d = 1
    while True:
        if d * e % totient == 1 and d != e and d != n:
            break
        d += 1

    return ((e, n), (d, n))
```

Слика 16. Имплементација на RSA во Python

[4] Од 6 декември 2021 година, Ignis е отфрлен и заменет со проектот Qiskit Experiments.
[5] Од 2 април 2021 година, Aqua е застарен и неговата поддршка завршува.

За енкриптирање и декриптирање се користат функциите encrypt и decrypt кои ги користат јавниот и приватниот клуч, соодветно (слика 17).

```
def encrypt(key, message):
    e, n = key
    encryption_map = {' ': '00', 'A': '01', 'B': '02', 'C': '03', 'D': '04', 'E': '05', 'F': '06', 'G': '07', 'H': '08',
                      'I': '09', 'J': '10', 'K': '11', 'L': '12', 'M': '13', 'N': '14', 'O': '15', 'P': '16', 'Q': '17',
                      'R': '18', 'S': '19', 'T': '20', 'U': '21', 'V': '22', 'W': '23', 'X': '24', 'Y': '25', 'Z': '26'}

    return ''.join([str(int(encryption_map[letter]) ** e % n).zfill(len(str(n))) for letter in message])

def decrypt(key, message):
    d, n = key
    decryption_map = {'00': ' ', '01': 'A', '02': 'B', '03': 'C', '04': 'D', '05': 'E', '06': 'F', '07': 'G', '08': 'H',
                      '09': 'I', '10': 'J', '11': 'K', '12': 'L', '13': 'M', '14': 'N', '15': 'O', '16': 'P', '17': 'Q',
                      '18': 'R', '19': 'S', '20': 'T', '21': 'U', '22': 'V', '23': 'W', '24': 'X', '25': 'Y', '26': 'Z'}

    message_blocks = [int(message[i : i + len(str(n))]) for i in range(0, len(message), len(str(n)))]
    return ''.join([decryption_map[str(number ** d % n).zfill(2)] for number in message_blocks])
```

Слика 17. Имплементација на функциите за енкриптирање и декриптирање

7.3. Градење на квантно коло за алгоритамот на Шор

При изградба на квантното коло, најпрво се дефинираат две функции: a_x_mod15 која служи за модуларна екпоненцијација (слика 18) и iqft која пресметува инверзна квантна Фуриева трансформација (слика 19).

```
def a_x_mod15(a, x):
    U = QuantumCircuit(4)
    for iteration in range(x):
        U.swap(2, 3)
        U.swap(1, 2)
        U.swap(0, 1)
        for q in range(4):
            U.x(q)

    U = U.to_gate()
    U.name = f'{a}^{x} mod 15'
    c_U = U.control()
    return c_U
```

Слика 18. Функција за модуларна експоненцијација

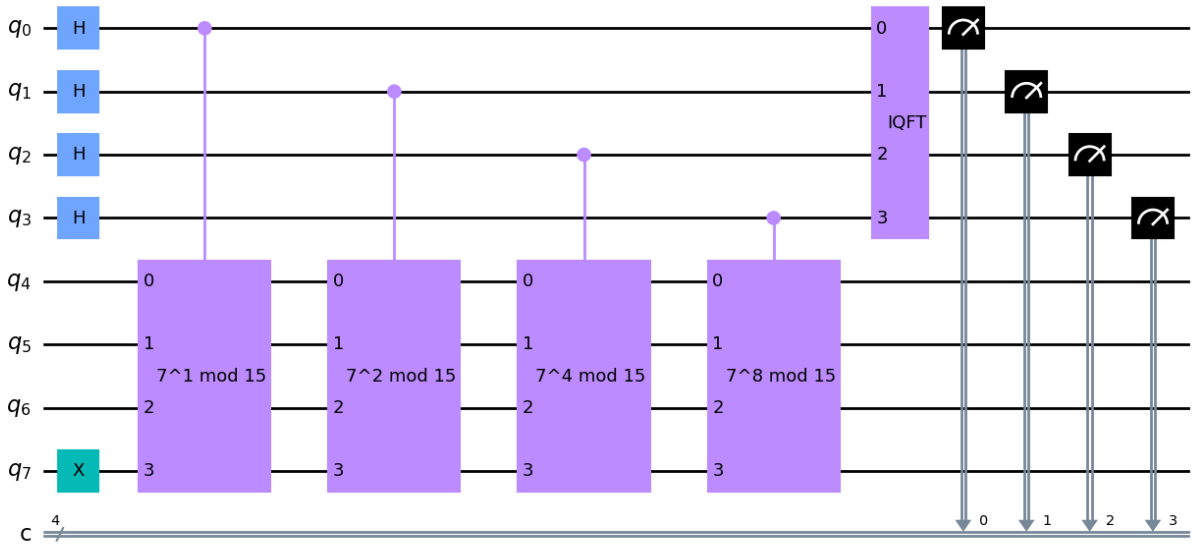
```
def iqft(n):
    qc = QuantumCircuit(n)

    for qubit in range(n//2):
        qc.swap(qubit, n-qubit-1)

    for j in range(n):
        for m in range(j):
            qc.cp(-numpy.pi/float(2**(j-m)), m, j)
        qc.h(j)

    qc.name = 'IQFT'
    return qc
```

Слика 19. Функција за инверзна Фуриева трансформација

Потоа се креира квантното коло со помош на функцијата create_circuit (слика 20) и на крај се мерат кјубитите.

```
def create_circuit(n_count, a):
    qc = QuantumCircuit(n_count + 4, n_count)

    for q in range(n_count):
        qc.h(q)

    qc.x(3 + n_count)

    for q in range(n_count):
        qc.append(a_x_mod15(a, 2**q), [q] + [i + n_count for i in range(4)])

    qc.append(iqft(n_count), range(n_count))

    qc.measure(range(n_count), range(n_count))
    return qc
```

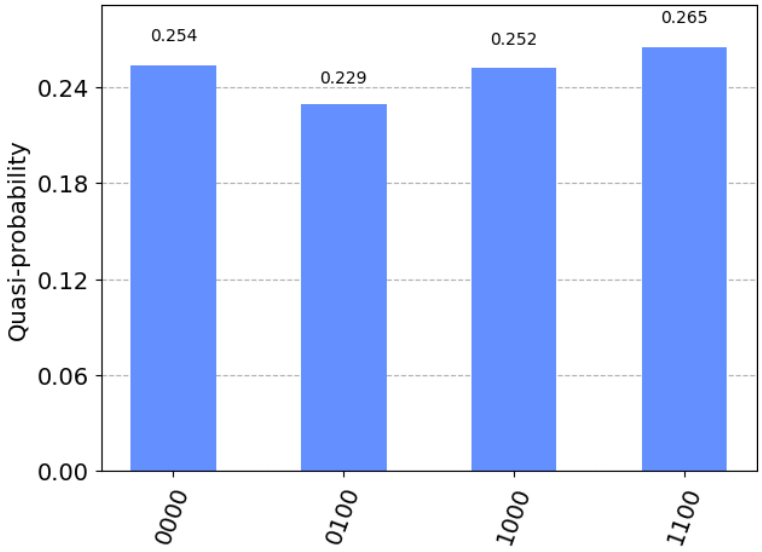
Слика 20. Функција за креирање на квантното коло



Слика 21. Квантно коло за алгоритамот на Шор

7.4. Наоѓање на период

Со мерење на резултантната суперпозиција, се добиваат резултати кои претставуваат фази на мерењето (слика 22).



Слика 22. Резултати од мерењето на суперпозицијата

На табелата на слика 23 може да се види процесот на извлекување на периодот r преку фазите. Може да се забележи дека овој алгоритам може да даде лоши резултати за периодот кога фазата е 0 или кога фазата и периодот не се взаемно прости. Затоа овој процес може да се повтори неколку пати сè додека не се добие период со кој успешно се разложува бројот N.

	Register Output	Phase	Fraction	Guess for r
0	0000(bin) = 0(dec)	0/16 = 0.00	0/1	1
1	0100(bin) = 4(dec)	4/16 = 0.25	1/4	4
2	1000(bin) = 8(dec)	8/16 = 0.50	1/2	2
3	1100(bin) = 12(dec)	12/16 = 0.75	3/4	4

Слика 23. Добивање на периодот r

7.5. Дешифрирање на порака преку алгоритамот на Шор

На слика 24 е дефинирана функцијата find_factors која како параметар прима број N кој треба да се разложи на два прости множители. Во оваа функција најпрво се одбира случајно а во опсегот [2, N) и се пресметува НЗД(a, N). Доколку овој број е делител на N, тогаш разложувањето е завршено. Инаку се креира квантно коло преку кое се наоѓаат фазите, периодот и можните фактори на N. Овој процес се повторува со нова вредност за a сè додека не се добијат делителите на бројот N.

```
def find_factors(N):
    a = numpy.random.randint(2, N)

    possible_factor = numpy.gcd(a, N)
    if possible_factor != 1:
        print(f'You have found a non-trivial factor of {N}.', end=' ')
        print(f'The factors are {possible_factor} and {int(N/possible_factor)}.')
        return (possible_factor, int(N/possible_factor))

    n = 4
    qc = create_circuit(n, a)
    backend = Aer.get_backend('qasm_simulator')
    counts = execute(qc, backend).result().get_counts()

    measured_phases = []
    for count in counts:
        measured_phases.append(int(count, 2) / (2**n_count))
```

```
    periods = set()
    for phase in measured_phases:
        period = Fraction(phase).denominator
        if period % 2 == 0:
            periods.add(period)

    factors = set()
    for period in periods:
        a_power_half = int(a**(period/2))
        guesses = [numpy.gcd(a_power_half + 1, N), numpy.gcd(a_power_half - 1, N)]
        for guess in guesses:
            if guess != 1 and guess != N and N % guess == 0:
                factors.add(guess)

    if len(factors):
        p = factors.pop()
        q = factors.pop() if len(factors) else N // p
        print(f'You have successfully factored {N} with a={a}. The factors are {p} and {q}.')
        return (p, q)
    else:
        print(f"Shor's Algorithm failed for a={a}. Choosing different 'a'.")
        return find_factors(N)
```

Слика 24. Функција на разложување на бројот N на прости множители

За тестирање на алгоритамот може да се искористи претходно шифрирана порака и јавен клуч со кој е шифрирана таа порака (слика 25).

```
message = '1445722405723480005404302833348'
public_key = (5, 851)

print('Results:')

p, q = find_factors(public_key[1])
public_key_shor, private_key_shor = rsa(p, q)

print(f'The private key is {private_key_shor}.')
print(f'The secret message is {decrypt(private_key_shor, message)}.')
```

```
Results:
Shor's Algorithm failed for a=658. Choosing different 'a'.
Shor's Algorithm failed for a=821. Choosing different 'a'.
Shor's Algorithm failed for a=846. Choosing different 'a'.
You have successfully factored 851 with a=574. The factors are 23 and 37.
The private key is (317, 851).
The secret message is PETER SHOR.
```

Слика 25. Тестирање на алгоритамот на Шор

8. Заклучок

Подемот на квантните компјутери доведува до промена на парадигмата во областа на криптографијата, менувајќи ги самите основи на конвенционалните методи за шифрирање. Импликациите на алгоритамот на Шор, способен за ефикасно разложување на големи броеви на квантен компјутер, преставуваат директна закана за широко користените криптографски протоколи повикувајќи на реевалуација на нашиот пристап за заштита на чувствителни информации.

Влијанието на квантните компјутери врз криптографските алгоритми се протега надвор од непосредните технолошки размислувања; има длабоки последици за глобалната сајбер безбедност и приватност. Ранливостите воведени со квантното пресметување бараат проактивен став, поттикнувајќи го развојот и имплементацијата на криптографски техники отпорни на квантните техники. Транзицијата кон пост-квантна криптографија станува критичен императив за заштита на дигиталната инфраструктура што го поткрепува нашиот меѓусебно поврзан свет.

Додека квантните компјутери претставуваат закана за постоечките криптографски алгоритми, тие исто така ги отвораат вратите за иновативни криптографски решенија. Дистрибуцијата на квантни клучеви (QKD) ги користи принципите на квантната механика за да обезбеди комуникациски канали. Осигурува дека секој обид за пресретнување или прислушкување на пораки ќе биде забележан, обезбедувајќи нова парадигма за безбедна комуникација.

Секојдневната еволуција на квантните компјутери и алгоритми бара иновативен и колаборативен пристап. Додека се движиме низ оваа еволуција, колективните напори на истражувачите, индустриските лидери и владите стануваат инструментални во обликувањето на безбедна иднина која може да ги издржи предизвиците наметнати од квантните достигнувања.

Користена литература

[1] R. P. Feynman, *Simulating Physics with Computers*, International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982
[2] https://www.sri.com/press/story/a-brief-introduction-to-quantum-computing/
[3] https://en.wikipedia.org/wiki/Quantum_computing
[4] https://www.britannica.com/science/quantum-mechanics-physics
[5] https://en.wikipedia.org/wiki/Quantum_mechanics
[6] https://www.vocabulary.com/dictionary/quantum
[7] https://www.mathworks.com/discovery/quantization.html#:~:text=Quantization%20is%20the%20process%20of,and%20range%20of%20a%20value.
[8] N. Zettili, *Quantum Mechanics: Concepts and Applications*, A John Wiley and Sons, Ltd, Publication, 2009
[9] https://en.wikipedia.org/wiki/Applications_of_quantum_mechanics
[10] A. Einstein, L. Infeld, *The Evolution of Physics: The Growth of Ideas from Early Concepts to Relativity and Quanta*, Cambridge University Press, 1938
[11] https://builtin.com/software-engineering-perspectives/superposition
[12] E. Schrödinger, *Die Naturwissenschaften*, Vol. 23, Issue 48, pp. 807-812, *Die gegenwärtige Situation in der Quantenmechanik*, November 1935
[13] https://en.wikipedia.org/wiki/Quantum_entanglement
[14] https://scienceexchange.caltech.edu/topics/quantum-science-explained/entanglement
[15] Heisenberg, W. *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*. Z. Physik 43, 172–198, 1927
[16] https://scienceexchange.caltech.edu/topics/quantum-science-explained/uncertainty-principle#:~:text=Formulated%20by%20the%20German%20physicist,about%20its%20speed%20and%20vice
[17] https://byjus.com/physics/wave-function/#:~:text=What%20is%20Wave%20Function%3F,Greek%20letter%20called%20psi%2C%20%F0%9D%9A%BF.
[18] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing
[19] https://medium.com/@markus.c.braun/a-brief-history-of-quantum-computing-a5babea5d0bd
[20] https://thequantuminsider.com/2020/05/26/history-of-quantum-computing/
[21] https://uwaterloo.ca/institute-for-quantum-computing/quantum-101/quantum-information-science-and-technology/what-qubit
[22] https://en.wikipedia.org/wiki/Qubit

[23] https://learn.microsoft.com/en-us/azure/quantum/concepts-multiple-qubits
[24] https://quantumpedia.uk/an-introduction-to-quantum-logic-gates-cee92ba9c1cc
[25] https://en.wikipedia.org/wiki/Quantum_logic_gate
[26] C.P. Williams, *Explorations in Quantum Computing*, Springer-Verlag London Limited, 2011
[27] J. Brown, *The Quest for the Quantum Computer*, Touchstone, 2000
[28] https://en.wikipedia.org/wiki/Quantum_algorithm#:~:text=Quantum%20algorithms%20are%20usually%20described,a%20fixed%20number%20of%20qubits.
[29] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010
[30] D. Deutch, R. Jozsa, *Rapid Solutions of Problems by Quantum Computation*, Royal Society of London, 1992
[31] D. Simon, *On the Power of Quantum Computation*, SIAM Journal on Computing, 1997
[32] L. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, Proceedings of the Annual ACM Symposium on Theory of Computing, 1996
[33] G. Brassard, P. Hoyer, A. Tapp, *Quantum Counting*, Lecture Notes in Quantum Counting, 1998
[34] A. Ambainis, *Quantum Walk Algorithm for Element Distinctness*, SIAM Journal on Computing, 2007
[35] F. Magniez, M. Santha, M. Szegedy, *Quantum Algorithms for the Triangle Problem*, SIAM Journal on Computing, 2007
[36] https://en.wikipedia.org/wiki/Public-key_cryptography
[37] https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography#:~:text=Asymmetric%20cryptography%2C%20also%20known%20as,from%20unauthorized%20access%20or%20use.
[38] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[39] http://www.cse.unt.edu/~tarau/teaching/PP/NumberTheoretical/RSA%20(cryptosystem).pdf
[40] R.L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 1977
[41] https://en.wikipedia.org/wiki/Shor%27s_algorithm
[42] P. W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, 1994
[43] https://www.quantiki.org/wiki/shors-factoring-algorithm
[44] https://www.qutube.nl/quantum-algorithms/shors-algorithm
[45] https://en.wikipedia.org/wiki/Quantum_Fourier_transform
[46] https://www.youtube.com/watch?v=FRZQ-efABeQ&ab_channel=minutephysics

[47] https://kaustubhrakhade.medium.com/shors-factoring-algorithm-94a0796a13b1
[48] https://www.classiq.io/insights/shors-algorithm-explained
[49] https://en.wikipedia.org/wiki/Qiskit
[50] https://medium.com/qiskit/applying-shors-algorithm-bbdfd6f05f7d
[51] https://github.com/Qiskit/textbook/blob/main/notebooks/ch-algorithms/shor.ipynb