Дипломска работа

Квантни компјутери и нивната улога во пробивањето на шифрирачките алгоритми

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

Кандидат:
Андреј Станојковиќ 186039

Ментор:
Проф. др. Весна Димитрова

Вовед

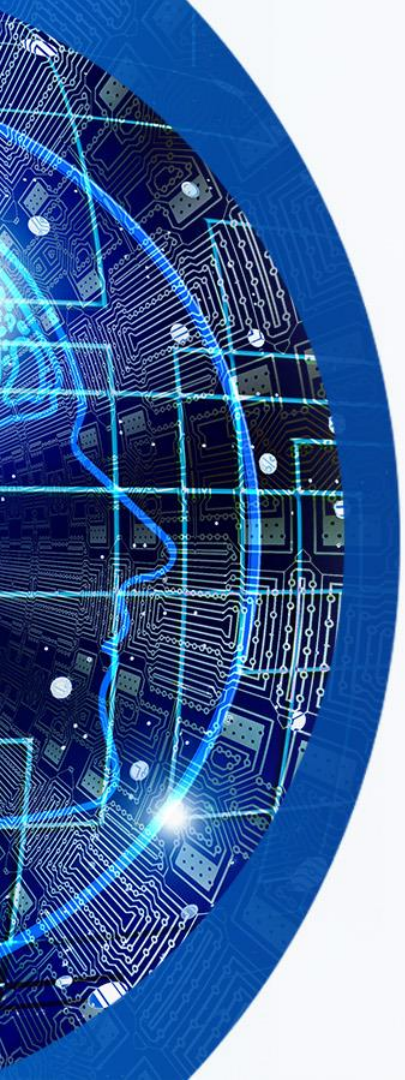
- Развој на квантното пресметување
- Воведување на концептот на квантен компјутер од Ричард Фајнман во 1982 година
- Објавување на алгоритамот на Шор во 1994 година
- Развој на пост-квантна криптографија како одговор на алгоритамот на Шор

Квантна механика

- Фундаментална теорија во физиката
- Дава опис на физичките својства на природата на атомско и субатомско ниво
- Терминот “quantum” потекнува од латинскиот “quantus”, што значи „колку“ или „колку одлично“

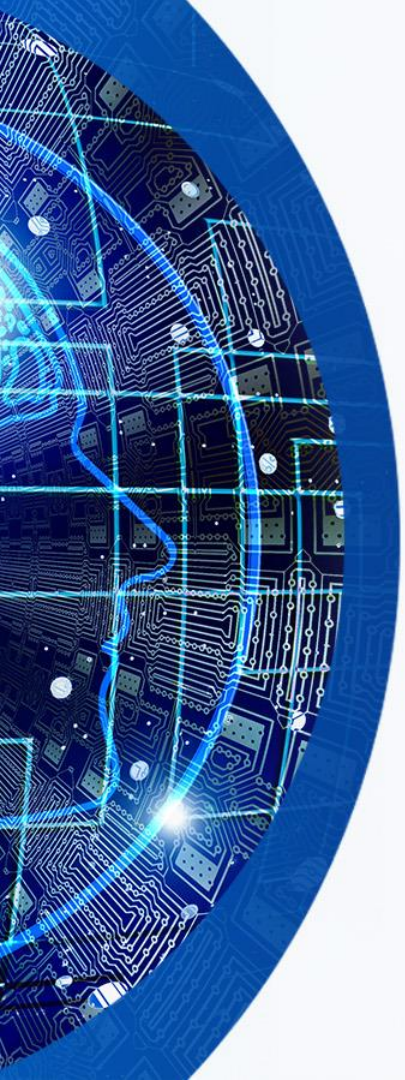
Историја

1900	• Макс Планк ја предложил хипотезата дека енергијата се зрачи и апсорбира во дискретни „кванти“
1905	• Алберт Ајнштајн го објаснил фотоелектричниот ефект
1913	• Нилс Бор предложил модел на атомот заснован на идеите за квантизирани енергетски нивоа
1923	• Луј де Броље ја објавил теоријата дека честичките може да покажат карактеристики на бранови и обратно
1925	• Хајзенберг, Борн и Џордан развиле матрична механика, додека Шродингер ја развил брановата механика
1930	• Квантната механика била дополнително обединета и формализирана од Хилберт, Дирак и фон Њуман



Основни концепти

- Квантизација
- Двојна природа на материјата
- Суперпозиција
- Испреплетеност
- Принцип на неопределеност
- Бранови функции



Примена

- Квантно пресметување
- Квантна криптографија
- Квантна комуникација и телепортација
- Квантни сензори и метрологија
- Квантна хемија и наука за материјалите
- Квантна оптика и ласерска технологија

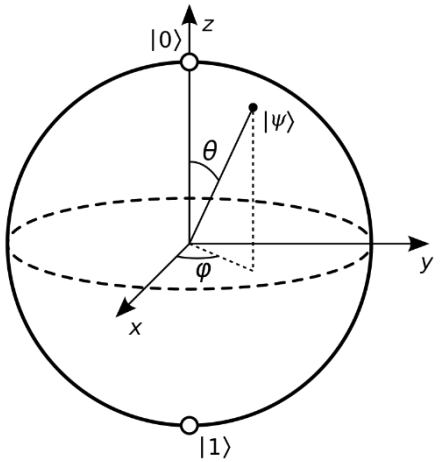
Квантни компјутери

- Користат квантни битови – кјубити
- Експоненцијално побрзи од класичните компјутери
- Способни да истражуваат повеќе решенија за одреден проблем истовремено
- Нема да ги заменат денешните компјутери

Историја

1982	• Ричард Фајнман го предложил моделот на квантен компјутер способен да симулира квантни системи
1994	• Питер Шор го претставил својот алгоритам за разложување на големи цели броеви
1996	• Лов Гровер претставил квантен алгоритам за пребарување во база на податоци
1998	• Изграден е првиот квантен компјутер со само 2 кјубити
2001	• IBM и универзитетот во Стенфорд ја објавиле првата имплементација на алгоритамот на Шор
2017	• IBM го претставиле првиот комерцијално употреблив квантен компјутер
2019	• Google AI објавиле дека постигнале квантна надмоќ со 54-кјубитна машина

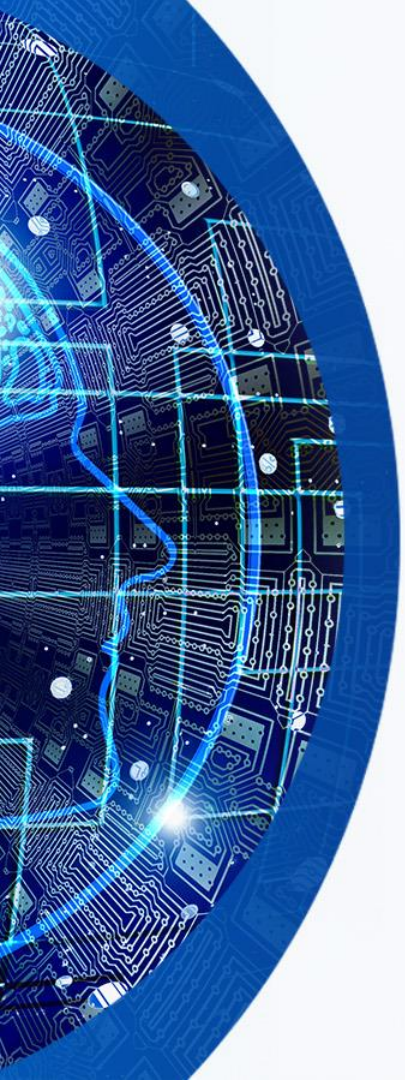
Кјубит



- Има две различни состојби, 0 и 1
- За разлика од класичниот бит, кјубитот може да биде во суперпозиција од двете состојби
- Линеарна комбинација од $|0\rangle$ и $|1\rangle$, т.е. $\psi = \alpha|0\rangle + \beta|1\rangle$, каде α и β се комплексни веројатносни амплитуди, т.ш. $|\alpha|^2 + |\beta|^2 = 1$
- $\alpha = \cos\left(\frac{\theta}{2}\right)$ и $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$
- За два кјубити: $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

Операции на кјубити

- Квантни логички порти – основни компоненти на квантните кола кои вршат операции на еден или повеќе кјубити
- Квантно мерење – неповратна операција преку која се добиваат информации за состојбата на еден кјубит
- Иницијализација или ре-иницијализација до позната вредност, најчесто $|0\rangle$
- Испраќање на кјубит преку квантен канал



Квантни логички порти

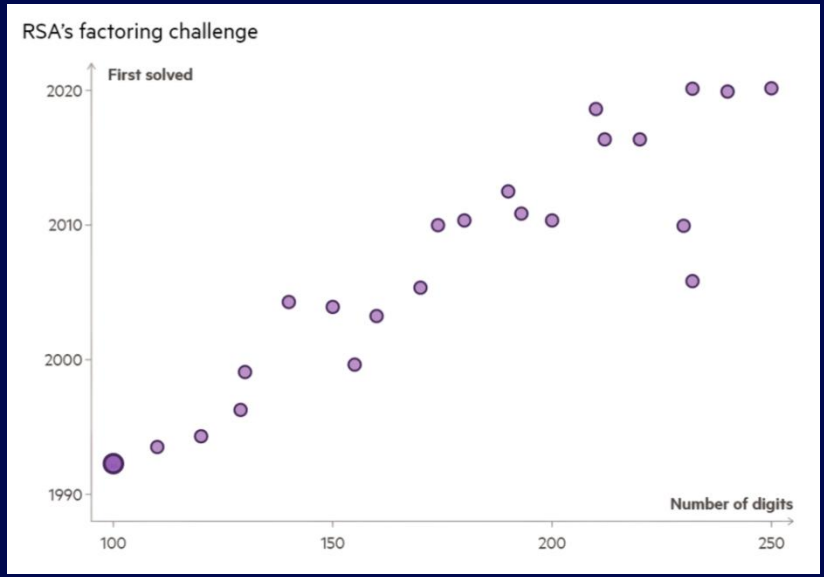
- Паулиеви (X, Y, Z) порти
- Адамар (H) порта
- Порти за промена на фаза (Z, S, T)
- SWAP порта
- Контролирани квантни порти (CNOT, CZ, CSWAP, CCNOT)

Квантни алгоритми

- Чекор-по-чекор процедура која се извршува на квантен компјутер
- Модел на квантно коло
- Алгоритми базирани на квантна Фуриева трансформација
- Алгоритми базирани на амплитудно засилување
- Алгоритми базирани на квантно случајно движење

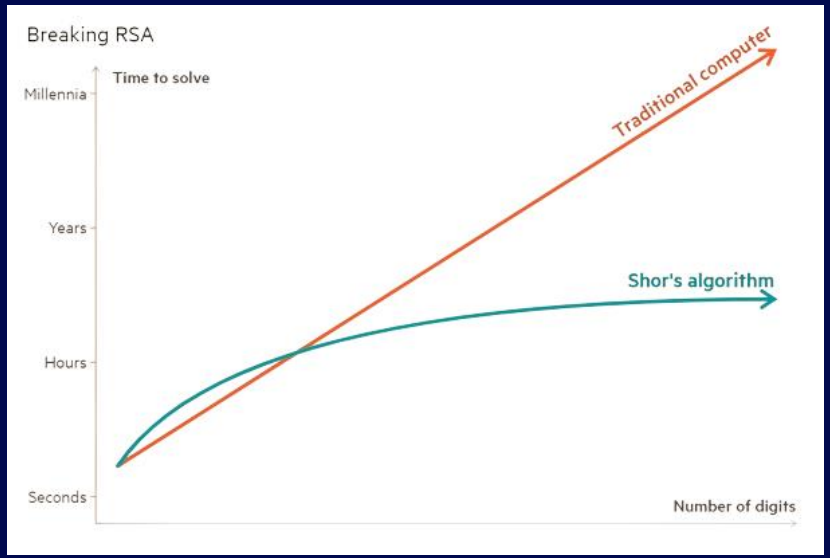
RSA криптосистем

- Криптографија со јавен клуч
- Ron Rivest, Adi Shamir и Leonard Adleman – 1977 година
- Се базира на проблемот на факторизација на големи броеви
- Вообичаено се користи за пренос на клучеви за криптографија со симетричен клуч



Алгоритамот на Шор

- Квантен алгоритам за факторизација на големи броеви
- Потенцијал да ги разбие широко користените шеми за шифрирање
- Веројатносен алгоритам



Алгоритамот на Шор

1. Класична редукција – постапка за разложување на даден број
2. Квантен алгоритам за наоѓање на ред
   - целта е да го најде редот r при дадени N и a, т.ш. $a^r \equiv 1 \pmod N$
   - го користи својството на суперпозиција
   - $|1\rangle + |2\rangle + |3\rangle + \cdots \rightarrow |1, a^1\rangle + |2, a^2\rangle + |3, a^3\rangle + \cdots \rightarrow |1, k_1\rangle + |2, k_2\rangle + |3, k_3\rangle + \cdots$, каде $a^x = mN + k$ за некое m
   - со мерење на добиената суперпозиција се добива $|i, k\rangle + |j, k\rangle + |l, k\rangle + \cdots$
   - со користење на својството: $a^x = mN + k \Longrightarrow a^{x+p} = sN + k$, се добива:

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

Quantum Information Softwate Kit – Qiskit

- Python библиотека за развој на софтвер со отворен код
- Нуди алатки за креирање и манипулирање на квантни програми
- Изградба на софтверски пакет за користење на квантен компјутер
- Главни елементи: Terra, Aer, Ignis и Aqua

Практична имплементација

Заклучок

- Промена на парадигмата во областа на криптографијата
- Директна закана за широко користените криптографски протоколи
- Длабоки последици за глобалната сајбер безбедност и приватност
- Дистрибуција на квантни клучеви (QKD)
- Колективни напори на истражувачите, индустриските лидери и владите за развивање на безбедна иднина

Прашања?