Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)
Кафедра _____Безпеки інформаційних технологій____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____перший(магістерський)_____

_____Криптосистеми з квантовим розподілом ключів_____

Виконав:
студент 2 курсу, групи БДІРм-20-1
Скічко Данило Володимирович_____
(прізвище, ініціали)
Спеціальність ___125 Кібербезпека _____
(код і повна назва спеціальності)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)
Керівник проф Халімов Г.З._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З.__
(підпис) (прізвище, ініціали)

2021

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Скічко Данилу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Криптосистеми з квантовим розподілом ключів
_____
_____
затверджена наказом по університету від 8. 11. 2021 р. 1684_Ст
2. Термін подання студентом роботи до екзаменаційної комісії 15 - 12 2021 р.
3. Вихідні дані до роботи дослідження криптосистем із квантовим розподілом ключів, оцінка складності реалізації криптосистем з квантовим розподілом ключів, аналіз та оцінка сучасних моделей реалізації квантових комп'ютерів та алгоритмів заснованих на квантовій теорії
_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі _____
Теоретичні та технічні особливості роботи квантових комп'ютерів
Сфери використування квантових комп'ютерів
Аналіз та оцінка квантових протоколів розподілу ключів
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5. включається до завдання за рішенням випускової кафедри)
презентаційний матеріал у вигляді слайдів

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	01.09.2021	виконано
2	Робота з джерелами за тематикою роботи	1.09.2021-1.10.2021	виконано
3	Вивчення основних понять квантової механіки	01.10.2021-20.10.2021	виконано
4	Вивчення основних понять квантових обчислень	20.10.2021 – 5.11.2021	виконано
5	Аналіз квантових обчислень у криптографії	5.11.2021 – 15.11.2021	виконано
6	Аналіз квантових протоколів розподілення ключів	15.11.2021 – 20.11.2021	виконано
7	Теоретичний аналіз квантових криптосистем	20.11.2021 – 25.11.2021	виконано
8	Оформлення пояснювальної записки	25.11.2021 – 13.12.2021	виконано

Дата видачі завдання __01_ _____09_____2021 р.

Студент _____
(підпис)

Керівник роботи _____ _____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до атестаційної роботи магістра: 64 с., 2 табл., 18 рис., 28 джерел.

Об’єкт дослідження – криптосистемі з квантовим розподілом ключа та їх ефективність. Методи дослідження - теоретичний, аксіоматичний та конкретний аналіз. Результатом роботи є висновки щодо криптосистем з квантовим розподілом ключа, квантового комп’ютеру та припущення щодо подальших шляхів їх розвитку.

Мета диплома полягає в дослідженні поточного стану розвитку криптосистем з квантовим розподілом ключа, квантових обчислень та квантового комп’ютеру. Оцінка погроз впливу квантового комп’ютеру на сучасну криптографію та на класичні алгоритми розподілу ключа.

У даній роботі розкрита теоретична база щодо квантових обчислень та квантових комп’ютерів. Досліджено архітектуру квантового комп’ютеру та принципи його роботи. Розглянуті основні принципи квантової теорії і квантової механіки, які є основою роботи квантових обчислень. Проведено теоретичне порівняння класичного комп’ютера та його обчислювальних можливостей щодо сучасного стану квантового комп’ютеру та його обчислювальних можливостей. Розглянуті та розібрані сучасні квантові алгоритми з квантовим розподілом ключів такі, як: BB84, BB92 та надані приклади криптосистем у яких ці алгоритми можуть знайти застосування.

КВАНТОВИЙ КОМП’ЮТЕР, КУБІТИ, КВАНТОВІ ОБЧИСЛЕННЯ, КВАНТОВА ІНФОРМАЦІЯ, КВАНТОВІ СХЕМИ, ПОСТ КВАНТОВА КРИПТОГРАФІЯ.

ABSTRACT

The report on pre-certification practice contains: 64 pp., 2 table, 18 pictures 28 sources

The object of research is cryptosystems with quantum key distribution and their efficiency. Research methods - theoretical, axiomatic and specific analysis. The result is conclusions about cryptosystems with quantum key distribution, quantum computer and assumptions about further ways of their development.

The subject of research is to study the current state of development of cryptosystems with quantum key distribution, quantum computing and quantum computer. Assess the threats of the quantum computer to modern cryptography and classical key distribution algorithms.

This paper reveals the theoretical basis for quantum computing and quantum computers. The architecture of the quantum computer and the principles of its operation are studied. The basic principles of quantum theory and quantum mechanics, which are the basis of quantum computing, are considered. A theoretical comparison of the classical computer and its computing capabilities in relation to the current state of the quantum computer and its computing capabilities. Modern quantum algorithms with quantum key distribution such as: BB84, BB92 and examples of cryptosystems in which these algorithms can be used are considered and analyzed.

QUANTUM COMPUTER, QUBITS, QUANTUM CALCULATION, QUANTUM INFORMATION, QUANTUM SCHEMES, POST QUANTUM CRYPTOGRAPHY.

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ECC - Elliptic curve cryptography

RSA - Rivest, Shamir та Adleman.

АЛП - Арифметико-логічний пристрій

БК - Блок керування - блок процесора, що служить для керування АЛП за допомогою команд.

ЕПР-пара - Пара кубітів у стані названному у честь Ейнштейна, Подольського та Розена

QKD - Quantum Key Distribution

ЗМІСТ

ВСТУП

У сучасному світі, комп'ютерні системи займають особливе місце. Обчислювальна техніка приймає участь майже в кожній сфері нашого життя і безпосередньо впливає на неї. З часів початку застосування перших комп'ютерів щодня збільшувалася необхідність збільшення обчислювальної потужності останніх. Спочатку, нарощування потужність обчислювальних пристроїв здійснювалося шляхом накопичення обчислювальних ресурсів (застосування більш досконалих типів центральних обчислювальних процесорів і т.д.), проте зараз дослідники починають говорити про те, що нескінченно накопичувати ресурси неможливо, і скоро ми зіткнемося з необхідністю застосування нових підходів до обчислювальної. техніки в цілому. Узагальнюючи, вони говорять про те, що незабаром на зміну методу накопичення ресурсів повинен прийти метод зміни підходів до обробки та обчислення даних. Теорія про квантові комп'ютери, застосовує у своїй основі закони квантової механіки і дозволяє вивести новий рівень сучасну обчислювальну техніку.

Захист інформації у цифровому середовищі є однією з головних проблем сучасного світу. Нарощування потужностей комп'ютера призводить до того, що алгоритми та стратегії захисту втрачають свою ефективність пропорційно зростанню потужностей. Найпростішим прикладом є той факт, що зловмисник, маючи потужний обчислювальний потенціал, має ймовірність швидше підібрати пароль простим методом перебору. Маючи в своєму розпорядженні квантовий комп'ютер зловмисник вже становить серйозну загрозу алгоритмам заснованих на проблемах факторизації простих чисел, завдання дискретного логарифмування і т.д.

Варто зауважити, що квантовий комп'ютер перевищує обчислювальної потужності звичний нам комп'ютер, заснований на архітектурі фон Неймана

тільки в певному класі завдань. У більшості випадків, при спробі використовувати його для повсякденних завдань, він може навіть показувати продуктивність на порядок нижче, ніж стандартний комп'ютер архітектури фон Неймана

Один з перспективних алгоритмів, які показують можливості квантового комп'ютера - це алгоритм пошуку Гровера. Припустимо, що потрібно знайти один елемент зі списку, що складається з N елементів. Застосування класичного комп'ютера передбачає, що вам необхідно перевірити як мінімум N/2 елементів. У найгіршому випадку - усі N. Застосування квантового комп'ютера дозволить знайти потрібний елемент після перевірки приблизно $\sqrt{(N)}$ елементів. Таким чином, за підрахунками, класичний комп'ютер знадобиться близько тижня для вирішення рівняння, тоді як квантовий комп'ютер знайде елемент за одну секунду.

У криптографії, розподіл ключів відіграє значну роль. Встановлення захищеного каналу передачі повідомлень є основою для обміну даними для застосування наступних протоколів, в яких можливе застосування сеансового ключа. Застосування та реалізація подібних протоколів не обмежується використанням тільки в системах, заснованих на класичному комп'ютері, однак також можуть знайти своє застосування та реалізацію у світі квантових комп'ютерів. У роботі будуть розглянуті протоколи розподілу ключів у квантовому каналі зв'язку, які дозволяють сторонам узгодити загальний секрет, цим встановивши захищений канал зв'язку.

1 АКТУАЛЬНИЙ СТАН КВАНТОВОГО КОМ’ЮТЕРА

1.1 Представлення класичного комп’ютера архітектурі фон Неймана

Архітектура фон Неймана була вперше представлена у 1945 році. Його представлення комп'ютерної архітектри складалося з:

1) Арифметико-логічного пристрою
2) Блоку управління
3) Системи шин
4) Блоку пам'яті
5) Блоки введення-виводу

Схема класичного комп’ютеру фон Неймановської архітектури представлена на рис. 1.1.

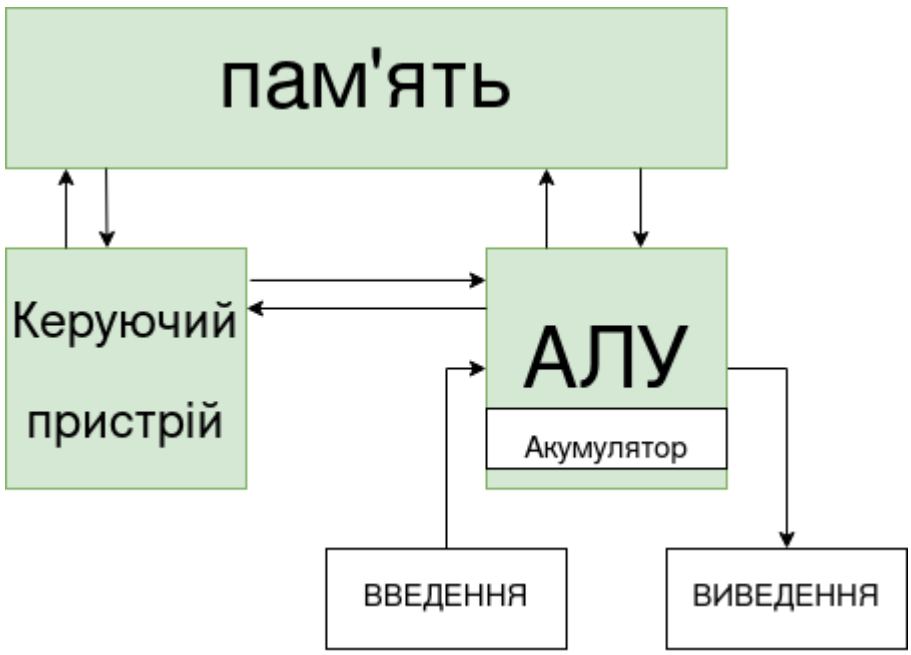


Рисунок 1.1 – Схематичне представлення архітектури класичного комп’ютера згідно фон Нейману

Джон фон Нейман сформулював свої принципи на основі того, що комп'ютер - програмований пристрій. Комп'ютер, за його визначенням - це сукупність спеціальних пристроїв для збирання, зберігання та обробки інформації, що функціонують під контролем програм, де програма - це сутність що містить інструкції, написані мовою, яку розуміє комп'ютер. [6, 21]

Арифметико-логічний пристрій разом з блоком управління формує центральний процесор. Блок управління контролює Арифметико-логічний пристрій за допомогою команд, які передаються через систему шин, що дозволяє зчитувати нові команди і записувати результати виконання команди назад в систему шин. Пам'ять і блок вводу-виводу повідомляється з системою шин, тим самим дозволяючи зберігати інформацію у пам'яті і зчитувати її в міру необхідності так само, як і її зміна, внаслідок реакції на зовнішні фактори.

Структурно, блок управління складається з: дешифратора команд (операцій), регістру команд, вузла формування (обчислення) поточної виконавчої адреси, лічильника команд.[5]

Центральний процесор фон Неймановської архітектури складається з п'яти спеціальних регістрів, які використовує для обробки вхідних даних:

1) Програмний лічильник. Тримає в пам'яті адресу до наступної команди, яку потрібно витягти з блоку пам'яті

2) Реєстр адресів пам'яті, який містить адресу поточної команди

3) Регістр пам'яті - містить дані, які були знайдені за адресою, що міститься в регістрі адрес пам'яті

4) Регістр поточної інструкції - містить у собі команду, яка була декодована та виконана

5) Акумулятор - спеціальний тип регістру, який використовується Арифметико-логічним пристроєм, для того, щоб містити дані, що знаходяться в обробці, а також результати обчислень

Також, фон Нейманом були представлені основні принципи, яким має

відповідати архітектура комп'ютера:

1) Принцип бінарного кодування - принцип, згідно з яким вся інформація, яка входить до комп'ютера, повинна бути закодована з використанням бінарних сигналів

2) Принцип програмного контролю - принцип, згідно з яким програма - це набір команд, які виконуються центральним процесором одна за одною, та у певній послідовності

3) Принцип однорідності пам'яті - принцип, який свідчить, що програма і дані зберігаються у тому самому блоці пам'яті. Крім того, комп'ютер не розділяє комірки пам'яті з командами програми, від осередків пам'яті з даними. Над даними та командами можуть бути проведені одні й ті самі операції

4) Принцип адресації - принцип, який визначає, що структурно, блок пам'яті складається з осередків, і кожна з осередків доступна центрального процесора у час. Однак, можливо, можна давати імена певним областям пам'яті, для того, щоб значення, які зберігаються в цих областях могли бути отримані під час виконання програми

5) Принцип дискретності - принцип, який свідчить, що комп'ютерний пристрій має обробляти команди дискретно, тобто центральний процесор повинен зчитувати команди з блоку пам'яті по одній за раз (треба брати до уваги, що в даному контексті принцип сформований з світла того, що центральний процесор складається з одного обчислювального ядра)[5]

1.2 Машина Тюрінга

Машина Тюрінга була вперше описана Аланом Тюрінгом у 1936 році. По суті це абстракція над обчислювальним пристроєм, яка була сформована для того, щоб допомогти вивчити межі того, що може бути обчислено даним пристроєм. Сьогодні, машина Тюрінга, є основоположною обчислювальною та

теоретичною моделлю у комп'ютерних науках. Схематичне представлення машини Тюрінга представлено не рис.1.2

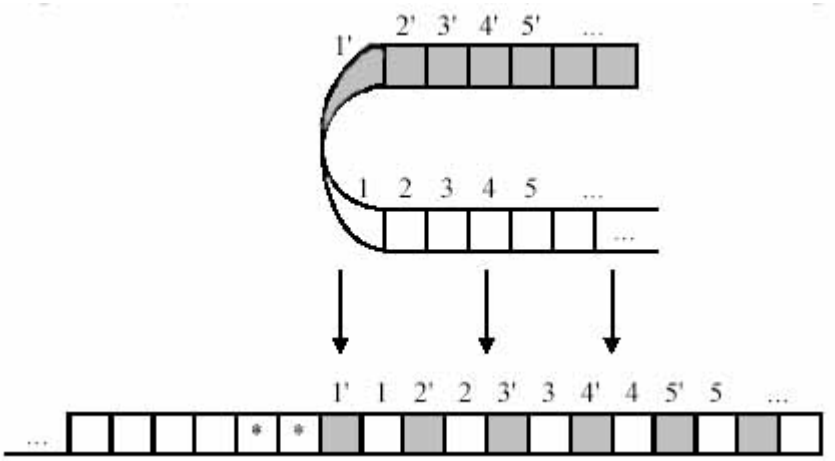


Рисунок 1.2. – Схематичне представлення машини Тюрінга як нескінченної двомірної стрічки станів

Машина Тюрінга – це машина, яка здатна перебувати в кінцевому наборі станів від q1 до qn. Стани представлені односпрямованою нескінченною стрічкою єдиного виміру, яка розділена на прямокутні області, кожна з яких може містити тільки один символ. [1,13,5] У будь-який момент машина Тюрінга може сканувати прямокутну область стрічки, яка може бути або порожньою, або містити символ від S1 до Sm, де S1 = 0, S2 = 1.

Поточний стан машини Тюрінга повністю визначається поточним станом символу S (названим конфігурацією), який сканується в даний момент. Це називається "станом визначеності". Ця множина машин, кожна з яких визначається станом сканування можна сопоставити з машинами з декількома можливими наступними станами, кожне з которих визначається рішеннями зовнішніх пристроїв або результатів операторів. Машина Тюрінга здатна на три можливі операції:

1) Вивести Si, перейти на одну область вліво і увійти в стан Qj

2) Вивести Si, перейти на одну область вправо та увійти в стан Qj

3) Вивести Si, не переходити нікуди і увійти в стан Qj

1.3 Квантова машина Тюрінга

Квантова машина Тюрінга (quantum Turing machine) - це абстрактна машина, яка використовується для моделювання процесів та ефектів, що протікають у квантових комп'ютерах.

Квантова машина Тьюринга узагальнює класичну машину Тьюринга таким чином, що внутрішні стани класичної машини тьюрінга замінюються чистими або змішаними станами з Гільбертого простору. [1,13]

Таким чином, основні відмінності від класичної машини Тьюрінга наступні:

1) Набір станів Q замінено на Гільбертовий простір

2) Порожня область стрічки замінена на нульовий вектор

3) Стан ініціалізації q0 може бути як змішаним, так і чистим.

4) Набір станів F, які є фінальними можливими станами системи, є підмножиною Гільбертового простору.

Також однією з головних відмінностей є те, що факт зчитування стану може спричинити зміну вихідного результату з певною часткою ймовірності. Причина цього лежить у законах квантової теорії, де факт спостереження може впливати на результати вимірюваних явищ та процесів.

1.4 Представлення квантового комп’ютера архітектури фон Неймана

Коли розробляється такий незвичний тип обчислювальної машини, як квантовий комп'ютер, то найкраще ґрунтуватися на вже існуючих архітектурах, які успішно реалізовані в класичних комп'ютерах, для того, щоб уникнути фундаментальних відмінностей. Крім того, масштабованість апаратної частини квантового комп'ютера – це одне з найскладніших завдань, з яким стикаються дослідники. [1,13]

Для полегшення завдання масштабованості та розробки новітньої архітектури - була запропонована квантова модель архітектури фон Неймана, яка поєднує класичну архітектуру фон Неймана з вимогами, що висуваються до реалізації квантового комп'ютера (DiVincenzo's criteria). Як наслідок, така архітектура значно полегшує питання масштабованості всієї системи загалом.

Схематичне зображення квантового комп'ютера фон Неймановської архітектури представлено малюнку *1*. Так, як і будь-якому іншому квантовому комп'ютеру - йому буде потрібно модуль, який відповідатиме управління внутрішніми процесами, що протікають у квантовому комп'ютері. Квантова шина дозволяє пересувати квантову інформацію між різними частинами системи квантового комп'ютера. Маніпуляції з квантовими даними протікають у квантовому арифметичному логічному модулі, який є одним з найважливіших елементів системи, так як операції над квантовими гейтами протікають саме тут. Квантові дані, які пройшли або очікують на обробку зберігаються в квантовій пам'яті, яка повинна бути реалізована на основі багатошарової технології, яка зможе забезпечити високу ємність накопичувача. Вхідні та вихідні інтерфейси системи повинні функціонувати як будь-який інший інтерфейс у класичному комп'ютері, тобто стан кубіту має бути чітко визначено як на вході, так і на виході системи [1,13]. Подібна необхідність виникає через те, що саме з інтерфейсом проходить взаємодія користувача, або будь-якої іншої класичної системи.

2 АРХІТЕКТУРА КВАНТОВОГО КОМП'ЮТЕРА. АКТУАЛЬНИЙ СТАН ТА ПРИНЦИПИ РОБОТИ

2.1 Історія розробки квантового комп'ютера

Історія квантового комп'ютера і квантових обчислень бере свій початок на початку двадцятого століття, коли фізика відчувала кризу, яка полягала в тому, що деякі явища вона просто не могла пояснити своїми законами. Дані явища не узгоджувалися з жодним із існуючих законів, і у фізиків створювалося враження, що вони щось упускають. Якесь проміжне ланка, яке було непросто виявити служило джерелом парадоксів і тоді не з'ясовних явищ.

Спочатку, цю проблему вирішили розширенням існуючих теорій та встановлення деяких припущень, які могли потенційно мати місце у класичній фізиці. Але одночасно з удосконаленням знань про атом і теорію радіації та її джерел, здобування набували все більш заплутаного характеру. До 1920 року фізика існувала в такому стані і постійно відчувала на собі наслідки цих заплутаних і часом абсурдних припущень, поки не було започатковано новий напрям - квантової механіки.

Квантову механіку можна справедливо назвати математичним фундаментом, у якому будуються фізичні теорії. Наприклад, існує теорія, звана "квантова електродинаміка", яка визначає взаємодію атомів та світла. Квантова електродинаміка побудована з урахуванням фундаментальних теорій квантової механіки з додаванням спеціальних правил, які стосуються особливостям атомів та його взаємодії, які описані квантової механікою.[13]

Взаємозв'язок між квантовою механікою та певною фізичною теорією можна порівняти із взаємозв'язком операційної системи з додатками, які на ній запущені. Операційна система встановлює базові параметри та закони, але в

жодному разі не втручається безпосередньо в роботу програм, які на цій операційній системі запущені.[1,13]

Закони квантової механіки надзвичайно прості, але навіть люди, які вивчають її роками, не можуть не погодитись, що вони абсолютно не інтуїтивні. Перші дослідники квантової теорії, квантових обчислень та квантової інформаційної теорії просто намагалися краще розібратися в природі явищ, яку ця теорія описує. Одне з сучасних завдань квантової теорії полягає у розробці та відточуванні практик, інструментів і теорій, які допоможуть більш інтуїтивно підходити до питання квантової теорії та зробити її більш передбачуваною для людського розуму.

З часом квантова механіка і квантова теорія набувала все більшого інтересу в наукових колах, тим самим змушуючи фізиків задаватися питаннями, як наприклад: чи можливо передавати сигнал швидше за швидкість світла? Теорія відносності Ейнштейна цілком явно каже, що ні. Однак, квантова механіка потенційно давала зрозуміти, що якщо стан квантового стану системи можливий, значить має бути можливе відтворення повної копії будь-де[13]. Однак, приблизно в той же час вчені дійшли висновку, що це не можливо і започаткували так звану "теорему про заборону клонування", яка й досі набуває уточнень та доповнень.

Незабаром після того, як Тюрінг вивів свою знамениту машину, а Джон фон Нейман побудував теоретичну модель того, як повинен, і в якому вигляді, виглядатиме класичний комп'ютер - був зібраний перший прототип. З кожним роком комп'ютерні потужності зростали, і зростають до цього дня з такою швидкістю, що ще в 1965 році Гордон Мур вивів знаменитий "закон Мура", в якому йдеться, що комп'ютерні потужності подвоюватимуться кожні два роки. Закон став відомим через те, що прогрес обчислювальної техніки дійсно дотримувався його аж до сьогодні. На жаль, крім прогресу, "закон Мура" також говорить, що обчислювальні ресурси мають межу, яка буде досягнута в перші два десятиліття двадцять першого століття. Процеси, створені задля зменшення

складових частин коипьютера, почали втрачати свою ефективність через наближення до фізичних кордонів допустимих розмірів компонентів. Через постійне зменшення, квантові ефекти почали втручатися у працездатність електронних компонентів систем класичного комп'ютера.

Одне з можливих рішень, які дозволять переступити через закон Мура - це підійти до вирішення проблеми з іншого боку. Одна з можливих парадигм альтернативного підходу лежала в тому, щоб почати використовувати квантову механіку для обчислень замість принципів, побудованих на класичній фізиці. Як виявилося, класичний комп'ютер може проводити симуляцію процесів, що протікають у квантовому комп'ютері. Однак, згодом з'ясувалося, що класичний комп'ютер і близько не може наблизитися до ефективності, яку в теорії може запропонувати квантовий комп'ютер. Квантовий комп'ютер має настільки велику перевагу перед класичним, що деякі дослідники дуже сумніваються в тому, що прірва у продуктивності може бути колись покрита.[1,13]

У 1982 році, Річард Фейман припустив, що експерименти щодо симуляції квантових комп'ютерів за допомогою класичних - не ефективні. Натомість, він припустив, що зібравши комп'ютер, який по-справжньому використовує принципи квантової механіки, дозволить вирішити цю проблему. У 1990 року, відразу кілька команд незалежних дослідників почали втілювати його ідею життя, цим реальному прикладі показуючи, що побудувати квантовий комп'ютер складно, але цілком реально. Пізніше, багато хто почав задаватися питанням: які саме завдання квантовий комп'ютер вирішує краще за класичний? Найчастіше дослідники не знають, оскільки клас завдань, які здатний вирішувати квантовий комп'ютер залежить від реалізованих алгоритмів. А реалізувати якісний алгоритм для квантового комп'ютера, який крім того, буде в рази ефективніший за аналоги, реалізовані на класичних системах - складно. Розробка алгоритмів для квантових комп'ютерів є проблемою з двох причин:

1) Людський розум звик до класичного світу, де все підпорядковується простим і зрозумілим фізичним законам класичної фізики. Якщо розробляти в такому ключі алгоритм для квантової системи - то в кращому випадку, вийде класичний алгоритм, який працює на квантовому комп'ютері. Щоб досягти позитивного результату, слід брати до уваги квантову природу та намагатися використовувати квантові закони якнайчастіше, при реалізації алгоритму[1,13]

2) Мало розробити аналог алгоритму в квантовій середовищі, але необхідно зробити аналог, який буде ще й краще, ніж реалізація на класичному комп'ютері. Найчастіше це складно у світі класичного комп'ютера, а у світі квантової механіки і поготів

Концепція інформації Шеннона та його теорема про джерело шифрування показала скільки інформації можна пропустити по виділеному каналу без втрат. Для забезпечення цілісності Шеннон ввів коди корекції помилок, які могли використовуватися для захисту інформації від спотворення.

Квантова теорія інформації, у свою чергу, пішла шляхом, аналогічним Шеннону. В 1995 Бен Шумахер, ввів аналог теореми про джерело шифрування (або теореми безшумного шифрування) для квантового середовища. У процесі Шумахер визначив фундаментальні сьогодні поняття квантового біта або кубіту (qbit) як матеріальної фізичної сутності. За аналогією з класичним комп'ютером, була виведена теорема про корекцію помилок у квантовому каналі зв'язку, що дозволяє зберігати цілісність інформації при проходженні по цьому квантовому каналу зв'язку. Також, згодом з'ясувалося, що квантовими каналами зв'язку також можлива передача класичних бітів через кубіт шляхом надщільного кодування.

2.2 Кубіт

Біт - це фундаментальна концепція у світі класичного комп'ютера та інформації у класичному вигляді. Квантова обробка інформації і квантовий

комп'ютер побудовані на трохи іншій концепції, яка має схожість з концепцією класичного комп'ютера. Ця концепція називається "квантовий біт" або скорочено "qbit".[1,13]

Qbit найчастіше розглядається як математична сутність та об'єкт. Проте, оскільки витоки цього поняття лежать у сфері квантової механіки, кубит можна також описувати фізичними законами квантової механіки. У цій роботі кубіт буде розглянутий переважно як математична сутність, оскільки мова йдеться не про фізику квантових об'єктів, а про застосування їх для формування сутності схожої з традиційним бітом інформації у квантовому світі.

Так само як і в класичному комп'ютері, кубіт приймає стани "1" і "0", проте, на відміну від класичного біта, у нього є третій, так званий проміжний стан невизначеності. У цьому вся стані кубіт не приймає значення ні "1" ні "0", а має певну можливість стати або "1" чи "0", при спробі виміряти його. Цей стан називають "суперпозицією". Кінцеві стани, які може приймати кубіт, позначають у нотації Дірака - $|0\rangle$ і $|1\rangle$. Дане позначення є загальноприйнятими в квантовій механіці і кодує деякий вектор-стовпець або вектор рядок у більш простий вигляд, яким зручніше оперувати.

В нотації Дірака вектор в ряд позначається як "бра", а вектор в стовпець як "кет". Перетворення вектору "кет" показано на рис. 2.1.

Суперпозиція, у свою чергу, описується як[13]

$$|\gamma\rangle = \alpha|0\rangle + \beta|1\rangle$$

де α і β є комплексними числами, які відповідають наступній умові:

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

Формула зветься - "Правило Борна". Ця умова виводиться з факту, що квантові сутності мають математичну 2-у норму і все ще повинні задовольняти умови теорії ймовірності, де сума всіх можливих результатів події повинна дорівнювати "1".

Якщо з іншого боку, то стан кубіту – це вектор двовимірного простору комплексної площини. Особливі стани - $|0\rangle$ і $|1\rangle$ називають "числовими базисами станів". Ці базиси формують ортонормальні базиси у комплексному

$$|\alpha\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}; \ |\beta\rangle = \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}$$

$$\begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{bmatrix} |\beta\rangle = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{bmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 * \beta_1 + \alpha_2 * \beta_2 \\ \alpha_3 * \beta_1 + \alpha_4 * \beta_2 \end{pmatrix}$$

$$|\alpha\rangle|\beta\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 * \beta_1 \\ \alpha_1 * \beta_2 \\ \alpha_2 * \beta_1 \\ \alpha_2 * \beta_2 \end{pmatrix}$$

$$\langle\alpha|\beta\rangle = \begin{pmatrix} \alpha_1, & \alpha_2 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \alpha_1 * \beta_1 + \alpha_2 * \beta_2$$

векторному просторі.

Рисунок 2.1 – Представлення вектору "кет" у нотації Дірака як вектор-стовпець

Для знаходження стану біта в класичній системі ми просто його вимірюємо. Класичний комп'ютер робить це щоразу, коли зчитує інформацію з вінчестера чи оперативної пам'яті. Даний підхід не може бути застосовний до кубітів та області квантових обчислень в цілому. Ми не можемо вимірювати кубит, щоб дізнатися про його квантовий стан. Але з цією проблемою допоможуть аргументи α і β. Тобто у нас немає виміряного кубіта, але у нас є вірогідність прийняття кубітом одного чи другого стану.

Коли ми вимірюємо кубіт, ми можемо отримати або "0" із ймовірністю $|\alpha|^2$, або "1" з ймовірністю $|\beta|^2$. Так як це ймовірність, то їх сума повинна дорівнювати "1". Дані ймовірності зазвичай є результатом великої кількості експериментів над квантовими частинками, які грають роль кубіта.[13]

У реальному світі, найчастіше ми можемо простежити залежність теоретичного об'єкта, з його у представленням у реальному світі. До квантової теорії, однак, це є вірним. Поточний стан квантової системи не може бути передбачено явно. Однак, існує безліч неявних взаємозв'язків, які дозволяють маніпулювати станом кубітів, змінюючи їх таким чином, щоб результат вимірювання системи залежало від деяких параметрів поточного стану системи. Ці стани, у свою чергу, мають експериментально доведені особливості, які забезпечують унікальні властивості квантових комп'ютерів.[1]

Найчастіше, стан суперпозиції кубіту вводить у повне нерозуміння, тому що людині складно уявити як щось може одночасно бути у двох станах і в той же час не бути в жодному з них зовсім. Класичний біт - це як монета: у монети дві сторони, і лише два можливі стани, якщо її підкинути. Кубіт, у свою чергу, є монетою, яка перебуває у стані між двома станами рівно до тих пір, як хтось не спробує подивитися якою стороною монета впала. У квантовій механиці, кубіт, який веде себе як вищеописана монета, можна було б описати так:

$$\frac{1}{\sqrt{(2)}}|0\rangle + \frac{1}{\sqrt{(2)}}|1\rangle$$

Таким чином, кубіт має рівну ймовірність на результат $|0\rangle$ і $|1\rangle$

Незважаючи на свою дивність і незвичайну поведінку - кубіт цілком реальний фізичний об'єкт, який ми моделюємо математично і маємо з цього корисні властивості. Поведінка кубітів не була виведена з формул, а була доведена чистими та множинними експериментами. Також, завдяки цим експериментам стало ясно, що кубіт може бути використаний у багатьох системах (наприклад у системі розподілу ключів по квантовому каналу). Щоб отримати уявлення про те, в якому вигляді кубіт існує в реальному світі, потрібно навести кілька прикладів реальних прикладів фізичних об'єктів, які можуть грати роль кубітів:

1) Фотон, який має два стани поляризації по деякому базису

2) Електрон атому, який має два стани орбіти

Якщо кубіт представлений електроном на орбіті деякого атома, то ймовірність прийняття електроном будь-якого стану після вимірювання може бути змінена шляхом опромінення атома певним типом енергії. Подібним чином можна маніпулювати ймовірностями прийняття кубітом станів $|0\rangle$ та $|1\rangle$

Оскільки

$|\alpha|^2 + |\beta|^2 = 1$, то константи α і β (комплексні числа) можна висловити у полярній системі координат

$$c_0 = r_0 e^{i\phi_0}$$

$$c_1 = r_1 e^{i\phi_1}$$

При підстановці у формулу, що визначає суперпозицію, отримуємо:

$$|\psi\rangle = r_0 e^{i\phi_0}|\mathbf{0}\rangle + r_1 e^{i\phi_1}|\mathbf{1}\rangle \;=\; e^{i\gamma}(\cos\frac{\theta}{2}|\mathbf{0}\rangle + e^{i\phi}\sin\frac{\theta}{2}|\mathbf{1}\rangle)$$

У даних формулах θ, ϕ, γ - реальні числа, які можна ігнорувати, тому що $e^{i\gamma}$ не має жодного впливу на результат, і тому ми можемо записати :

$$|\psi\rangle = \cos\frac{\theta}{2}|\mathbf{0}\rangle + e^{i\phi}\sin\frac{\theta}{2}|\mathbf{1}\rangle$$

У формулі вище числа θ і ϕ визначають точку на поверхні тривимірної сфери, як показано на малюнку. Ця сфера називається "Сферою Блоха".

Ця сфера дозволяє візуалізувати стан одного кубіту, і є частим об'єктом у дослідженні квантового комп'ютера і квантових обчислень в цілому. "Сфера Блоха" допомагає візуалізувати більшість операцій, які можна здійснити над одним кубітом.

Виходячи з того, що на поверхні "Сфери Блоха" може бути визначено нескінченна множина точок - нескінченна кількість станів системи кубіту може мати власну унікальну точку на поверхні.[1,13]

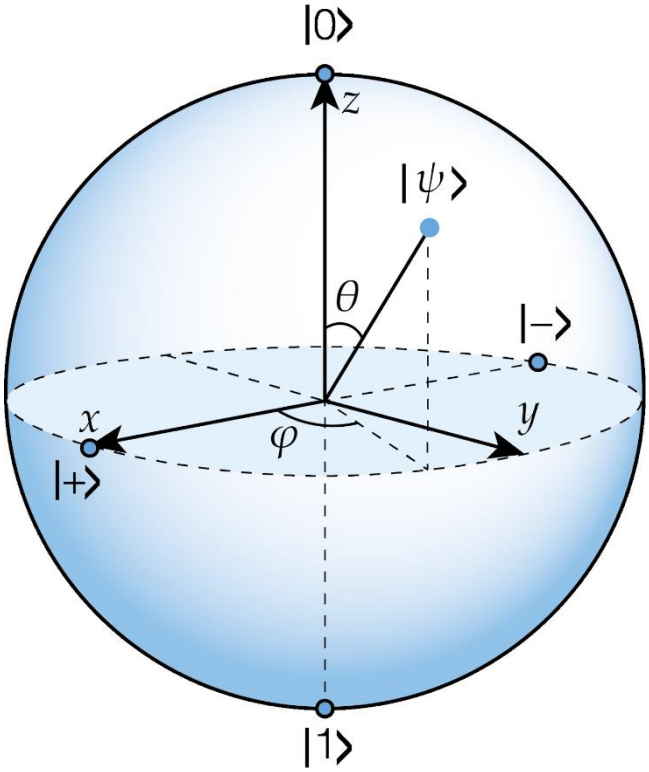


Рисунок 2.2 – Сфера Блоха с описаним станом кубіту $|\psi\rangle$

Узагальнюючи: виміряний кубит містить у собі один біт інформації. Проте, є цікаве питання, на яке немає відповіді. Яка кількість інформації міститься в незміряному кубіті? Це більше філософське питання, і зазвичай інформацію, що міститься в незміряних кубітах називають "прихованою інформацією", і приймають як природне явище (наприклад амплітуди вірогідностей). У природі кубіти не піддаються жодним вимірам, проте вони містять деяку " приховану " інформацію про свій стан.

2.3 Декілька кубіт

Якщо припустити, що у нас є два класичні біти, то це означає, що система з двох класичних бітів може приймати чотири можливі стани 00, 01, 10, 11.

Відповідно, якщо взяти два кубіти, то дана система буде також мати 4 можливі стани $|\mathbf{00}\rangle, |\mathbf{01}\rangle, |\mathbf{10}\rangle, |\mathbf{11}\rangle$. Пара кубітів може також існувати у суперпозиції всіх чотирьох станів одночасно. Саме з цієї причини квантовий стан двох кубітів, як і одного кубіта описується коефіцієнтом, який називається "амплітудою ймовірності". Таким чином загальний стан системи з двох кубів у суперпозиції буде дорівнювати.[1,13]

$$|\gamma\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Також як і у випадку з одним кубітом, результат вимірювання виникатиме з деякою ймовірністю, яка знаходиться в прямій залежності від коефіцієнта "амплітуди ймовірності". Оскільки ми знаємо, що сума всіх ймовірностей має дорівнювати 1, можна записати:

$$\sum_{x\in\{0,1\}^2} |a_x|^2 = 1$$

У системах, що складаються з кількох кубів, досить важливе значення має так званий стан "Белла"

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Даний вираз описує два кінцеві стани системи з кількох кубітів, де кожен стан може наступити з рівною ймовірністю після вимірювання. Це, здавалося б непримітне вираз має дуже важливу роль у квантової механиці та у квантових обчисленнях загалом, оскільки є ключовим елементом принципів квантової телепортації та квантового надщільного кодування.[1,13]

Стан Белла має унікальну властивість, яка свідчить, що при вимірі першого кубіту системи, є рівна ймовірність того, що кубіт прийме або стан 1, або стан 0. Вимірювання другого кубіту завжди дасть результат ідентичний тому, що був отриманий при вимірюванні першого кубіту. Таким чином, вимірювання другого біта та його результат залежний або пов'язаний з результатами вимірювання першого кубіту.

Також, виявляється, що цей взаємозв'язок зберігається навіть після застосування деяких операцій спочатку до першого, а потім і до другого кубіту.

Для опису системи з 3 класичних бітів, потрібно надати 3 класичні біти, щоб представити всю систему. У разі системи з 3 кубіт, потрібно надати 8 амплітуд ймовірностей, щоб описати всю систему та її можливі варіації. Таким чином 3 біти класичного комп'ютера несуть у собі 3 біти інформації, тоді як 3 кубіти потенційно несуть у собі 8 значень амплітуд ймовірностей.

Узагальнюючи, можна сказати, що системи, побудовані із застосуванням двох і більше кубітів, повинні бути описані із застосуванням 2^n векторів станів. Таким чином, можна провести уявний експеримент, в якому ми візьмемо квантову систему, що складається з 500 кубітів і спробуємо її описати. Для того, щоб описати подібну систему, нам потрібно врахувати кожен можливий варіант комбінацій, яку дана система може приймати. Для цього нам потрібно небагато чим, а 2^{500} амплітуд станів. Це просто величезна кількість коефіцієнтів не може зберегти жоден існуючий комп'ютер, тому що атомів у всесвіті приблизно та ж кількість, скільки амплітуд ймовірностей у нашій експериментальній системі. Якщо розглядати коефіцієнти як потенційну корисну інформацію, це покаже нам потенціал величезної обчислювальної потужності, яку зберігає у собі кубіт і система, що з кількох кубітів.

2.4 Однокубітні квантові гейти

Зміни, що відбуваються на квантовому рівні, можуть бути описані мовою квантової обробки інформації або квантових обчислень. Аналогічно тому, як класичний комп'ютер побудований на базі мікросхем та логічних операторів або як їх називають "гейтів", квантовий комп'ютер побудований на базі квантових схем та квантових гейтів, які допомагають переносити та маніпулювати даними на квантовому рівні, використовуючи закони квантової механіки.[1,13]

Як уже було сказано, класичний комп'ютер у своїй роботі використовує дроти та логічні гейти, для перенесення та маніпуляції з інформацією. Наприклад, класичний біт інформації, пропущений через логічний гейт "НЕ", змінить свій стан протилежне від поточного (наприклад 1 -> 0, 0 -> 1). Однак, чи можливо реалізувати класичний гейт "НЕ" для кубитів і квантового комп'ютера. Уявімо, що у нас є певний процес, який зможе змінити квантовий стан кубіту з $|0\rangle$ до $|1\rangle$ і навпаки. Подібний процес був відмінним кандидатом для реалізації гейту "НЕ" у полі квантових обчислень та обробки інформації. Однак, опис процесу, який буде проведений над станом системи кубіту, нічого нам не говорить про те, що станеться із суперпозицією базисних станів кубіту.

Квантовий гейт "НЕ" функціонує лінійно. Він бере стан суперпозиції кубіту:

$$\alpha|0\rangle + \beta|1\rangle$$

І міняє місцями коефіцієнти амплітуд ймовірностей системи:

$$\alpha|1\rangle + \beta|0\rangle$$

Чому квантовий гейт функціонує лінійно і не має лінійної природи - це дуже цікаве питання, відповідь на яке зовсім не очевидна. Шляхом досліджень, з'ясувалося, що лінійна поведінка квантових систем – це загальна властивість усіх квантових систем, яка підтверджена обчисленнями. Крім того, не лінійна поведінка квантової системи може призвести до парадоксу.

Гейт "НЕ" квантової системи може бути легко описаний за допомогою матриці

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Також представимо вектор-стовпець, що описує ймовірні вектори системи кубіту $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Де відповідно верхнє значення представляє амплітуду ймовірності стану системи $|0\rangle$, а нижнє відповідно $|1\rangle$

Враховуючи описаний раніше гейт "НЕ" та вектор-стовпець амплітуд станів квантового стану кубиту, перемножимо матрицю, що описує гейт "НЕ" та вектор-стовпець амплітуд

$$X\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

Таким чином, гейт "НЕ" змінює місцями амплітудні вектори стану кубіту, що описують стан системи.

Подібно можна припустити, що у квантових обчисленнях гейти реалізуються матрицями. Однак, у подібного підходу є одне обмеження, яке полягає в тому, що матриця, що описує гейт повинна бути унітарною (тобто множення матриці, що описує гейт на сполучено-транспоновану їй же - має дорівнювати одиничній матриці). Це правило є єдиним обмеженням, яке застосовується до квантових гейтів. Що логічно повідомляє нам про те, що будь-яка унітарна матриця є правильно описаним квантовим гейтом, який може змінювати стан системи кубіту. На відміну від класичних систем, де може існувати тільки один не тривіальний гейт для одного біта - "НЕ", в квантових системах, і в квантових обчисленнях зокрема може існувати багато не тривіальних однокубітних квантових гейтів. Як приклад таких гейтів можна навести гейт, який позначають Z:

$$Z \equiv \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Який залишає ймовірність стану $|0\rangle$ системи не змінним, і звертає знак стану $|\mathbf{1}\rangle$, щоб отримати $-|1\rangle$.

Зокрема гейта Z, існує ще один досить популярний гейт, який зветься "Перетворення Адамара"

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Цей гейт ще часто називають "квадратним коренем гейту НЕ". Перетворювання Адамара перетворює$|0\rangle$ в $(|0\rangle + |1\rangle)/\sqrt{2}$, а $|1\rangle$ у свою чергу обертається $(|0\rangle - |1\rangle)/\sqrt{2}$.

Перетворення Адамара є одним із найважливіших перетворень у квантовій обробці інформації, і варто візуалізувати це перетворення на сферу Блоха.

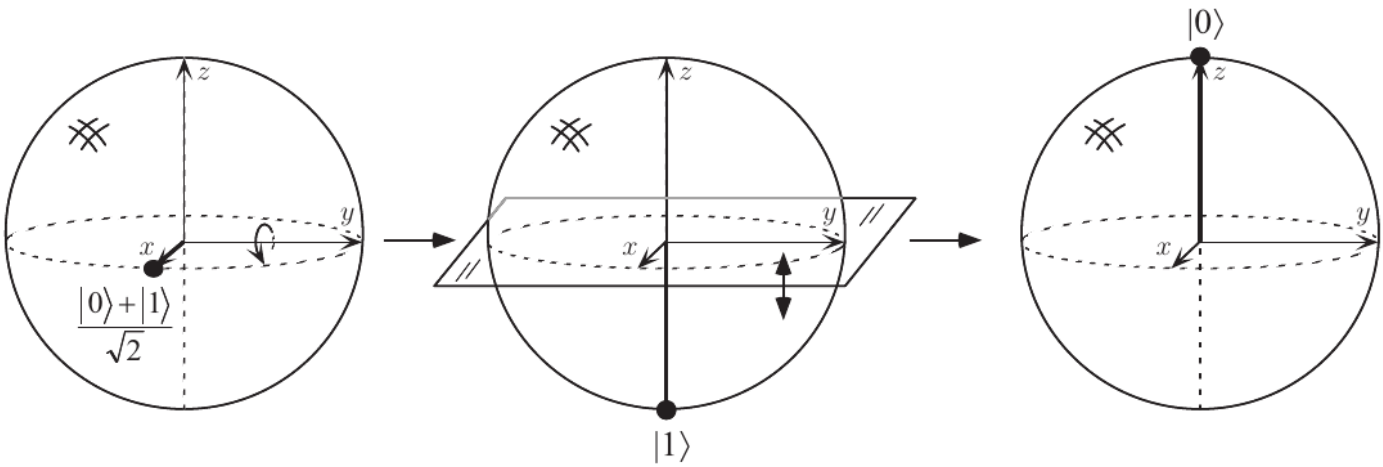


Рисунок 2.3 – Представлення однокубітного гейта " Перетворення Адамара " на сфері Блоха

На рисунку 2.3 показано, що перетворення Адамара є відповідальним як за поворот так і за відображення сфери. [13] Узагальнюючи, можна сказати, що перетворення Адамара не що інше як поворот сфери Блоха на 90 градусів навколо осі y, за яким слідує оборот усієї сфери на 180 градусів навколо осі x

Знову ж таки звертаючись до сфери Блоху та векторної природи квантових обчислень та спостережень, будь-який квантовий однокубітний гейт можна представити у вигляді декомпозії більш простих елементів, для перетворення однокубітного гейту на продукт обертання сфери Блоха по одній із трьох осей.

Ще декілька прикладів однокубітних квантових гейтів може буди знайдено на рис. 2.4

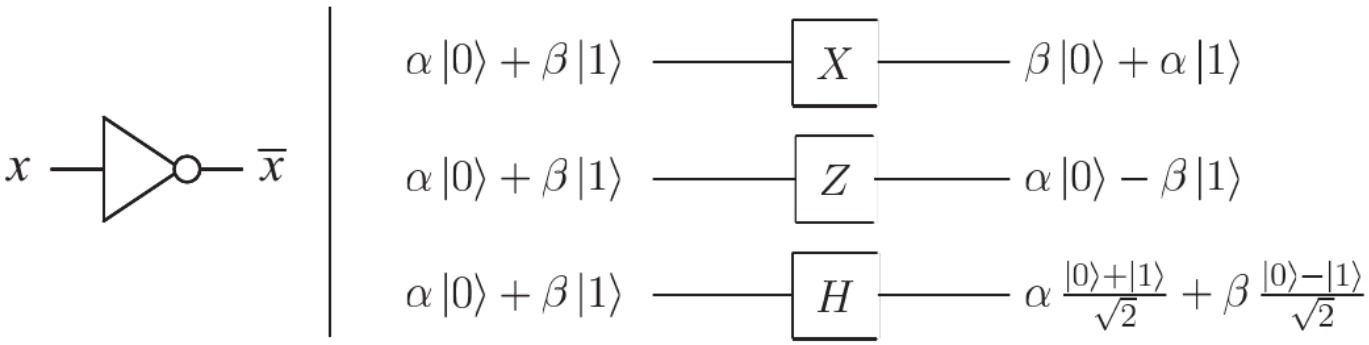


Рисунок 2.4 – Порівняння класичного гейта одного біта із гейтами для одного кубіта

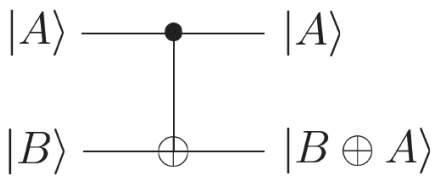
2.5 Багатокубітні квантові гейти

Крім однокубітних гейтів, також є багатокубітні, де логічні операції застосовуються до кількох кубитів одночасно. Досить важливий теоретичний результат полягає в тому, що будь-яка операція з бітами може бути проведена із застосуванням лише одного гейту "НЕ І" (NAND), який є універсальним. Наприклад, у порівнянні з гейтом "виключне або" (XOR), який навіть після об'єднання з гейтом "НЕ" (NOT), не настільки універсальний.

Прототипом багатокубітного логічного квантового гейта є "контрольоване-НЕ" (controlled NOT, CNOT). Даний гейт передбачає два кубіти на вході, звані кубітом контролю і цільовим кубітом відповідно. Схематичне представлення показано на рис 2.5

Наступний приклад описує роботу даного гейту:

- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- $|11\rangle \rightarrow |10\rangle$

Рисунок 2.5 – Схематичний опис гейта "контрольоване-НЕ"

Якщо контрольний кубіт перебуває у стані 0 – цільовий кубит не змінюється. Якщо стан контрольного кубіту 1 - цільовий кубіт змінюють свій стан на протилежний бази.

Ще один спосіб визначення гейту "контрольоване-НЕ" полягає в зображенні його як класичного гейта "виключне або". Адже:

$$|A, B\rangle \rightarrow |A, B \oplus A\rangle$$

Так як було виявлено, що гейт "контрольоване-НЕ" може бути представлений через узагальнений гейт "виключне або", то логічним буде питання про те, чи можливе представлення інших квантових гейтів у вигляді узагальнень або уявлень класичних гейтів (також як квантовий гейт "НЕ" за своєю природою є аналогом класичного гейту "НЕ" і може бути їм представлений). Як виявилося – це не можливо. Причина тому полягає в тому, що гейт "Виключає АБО" і "НЕ І" є не оборотними. Не оборотні гейти, - це ті гейти, у яких неможливо визначити вхідні параметри, виходячи з отриманого результату.

2.6 Квантові схеми

Проста квантова схема, представлена на малюнку, містить три квантові гейти. Схеми читають зліва направо. Кожна лінія в схема представляє дрот. Дрот - це не завжди є представленням звичайного фізичного дроту. У квантових схемах, дрот може представляти діапазон течії часу або фізичну частинку (також як фотон є частинкою світла, яка пересувається від однієї точки до іншої через простір). Схема представлена на рис 2.6 виконує просту, але дуже корисну роботу: ця схема змінює місцями стан двох кубіт.

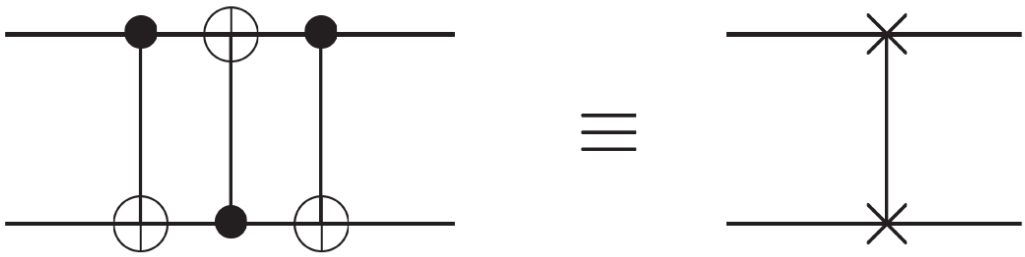


Рисунок 2.6 – представлення схеми, яка виконує роботу по зміну стану двох кубітів

Щоб простежити те, як саме ця схема міняє місцями стану двох кубів, можна представити операції схеми квантовим перетворенням:

$$|a, b\rangle \rightarrow |a, a \oplus b\rangle \rightarrow |a \oplus (a \oplus b), a \oplus b\rangle \rightarrow |b, a \oplus b\rangle = |b, a\rangle$$

Варто зауважити, що схема міняє місцями стану кубитів, але не вносить у ці стани відхилень

Класичні схеми дозволяють до реалізації багато операцій, на які квантові схеми не здатні. Наприклад:

1) У квантових схемах не можна реалізувати цикли (які за своєю природою є результатом роботи однієї частини схеми, який потім передається в іншу частину схеми).

2) Особливістю класичних схем є властивість об'єднувати дроти. Ця операція називається "FANIN" та визначає кількість входів, які можуть бути у

конкретного гейту. Досягається це за допомогою формування одного дроту, що є конкатинацією кількох гейтів "АБО". Як було сказано раніше, дана операція необоротна (ми не можемо судити про входи по результату). Що означає, що операція не унітарна і не може бути реалізована або застосована у квантових обчисленнях чи квантових схемах

3) Класична операція "FANOUT", в якій проводиться кілька копій одного біта також не дозволена в квантових схемах, тому що скопіювати стан кубіту не можливо, не змінюючи його стан

Одним з найпопулярніших багатокубітних квантових гейтів є "контрольоване-U" (controlled-U), де U - будь-яка унітарна матриця, що працює з декількома кубітами інформації. "Контрольоване-U" (рис 2.7) є по своїй суті новою версією "контрольоване-НЕ". Цей гейт приймає на вхід один контрольний кубіт (на малюнку представлений чорною точкою), і n цільових кубітів (на малюнку представлені як U). Якщо контрольний кубіт приймає стан 0 - нічого не відбувається, але якщо контрольний кубит приймає стан 1 - то гейт U застосовується до кубитів, що подаються на вхід. Гейтом U може бути будь-який багатокубітний гейт. Наприклад на малюнку 2 схемою представлений гейт "контрольоване-НЕ".

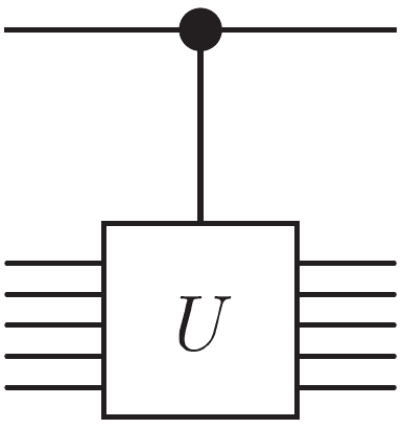


Рисунок 2.7 – Квантова схема представлення гейту "Контрольоване-U"

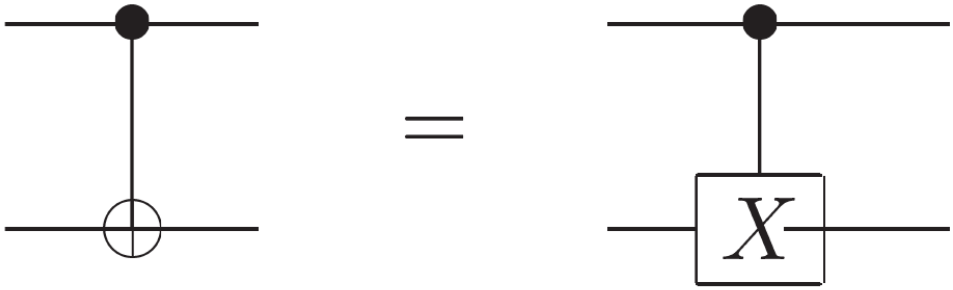


Рисунок 2.8 – Квантова схема представлення гейту "контрольоване-НЕ".

Таким чином, квантові схеми застосовуються для опису роботи гейтів. Це дозволяє простежити процеси наочно з структурної точки зору. Ще однією досить важливою та широко застосовною операцією, яку має сенс описати квантовою схемою – це операція вимірювання кубіту [1,13]. Операція вимірювання кубіту представляється літерою "M" і показана на рисунку 2.9

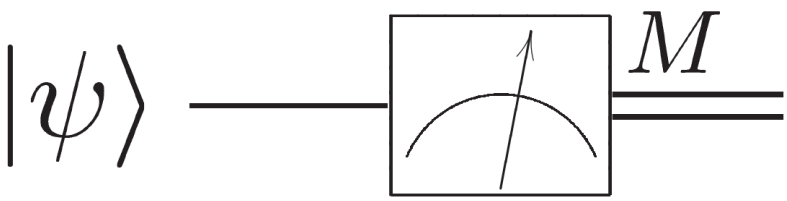


Рисунок 2.9 – Квантова схема процесу вимірювання стану одного кубіту

Операція вимірювання конвертує стан кубіту $|\gamma >= \alpha|0\rangle + \beta|1\rangle$ в один з його можливих класичних станів "M", ґрунтуючись на ймовірності прийняття кубитом кожного з них (0 з ймовірністю $|\alpha|^2$ або 1 з ймовірністю $|\beta|^2$) (подвійний результат операції вимірювання).

Квантові схеми можуть бути моделлю будь-якого квантового процесу, включаючи, але не обмежуючись обчисленнями, передачею інформації і навіть описом квантових шумів і перешкод.

2.7 Схема станів Белла

Для того щоб скопіювати інформацію одного кубіта в інший, треба просто застосувати CNOT, де контрольований біт буде в стані | 0⟩ (рис 2.10).

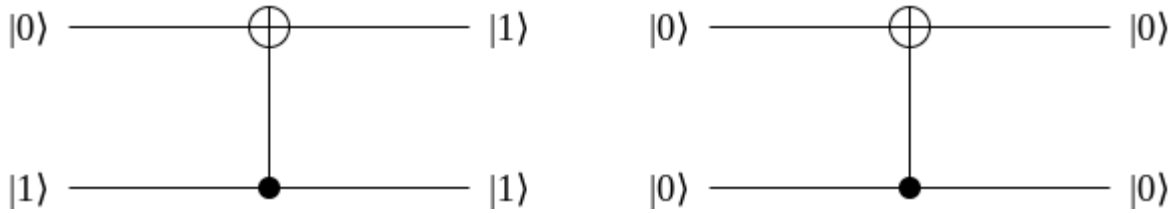
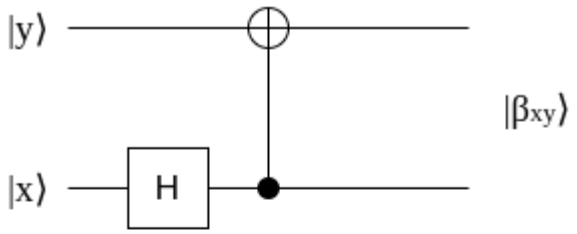


Рисунок 2.10 - Використання CNOT гейту для копіювання інформації

Але якщо потрібно привести два кубіта в стан Белла, тоді перед CNOT гейтом застосовується до контролюючого біту гейт H (рис. 2.11). В такому випадку отримується наступні можливі корелюємі стани кубітів:[13]



Вхід, $\|xy\rangle$	Вихід, $\|\beta_{xy}\rangle$
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

Рисунок 2.11 - Квантова схема для створення станів Белла

Як видно з хвильової функції яка описує стан системи з двох кубіт в стані ЕПР-пари - ці кубіти настільки тісно пов'язані, що результат вимірювання одного з них повідомляє про стан другого.

2.8 Пост квантова криптографія

Пост квантовою криптографією (або квантово стійкою криптографією) називають алгоритми, які стійкі до атак, що проводяться за допомогою квантового комп'ютера. Головна проблема полягає в тому, що багато популярних алгоритмів у своїй основі використовують три основні класи складних математичних проблем:

1) Факторизація простого числа
2) Дискретне логорифмування
3) Дискретне логорифмування порядку точки елептичної кривої

Усі ці проблеми можуть бути вирішені на квантовому комп'ютері середньої потужності, застосовуючи алгоритм Шора за детермінований час. Сьогодні, навіть маючи на руках інформацію про те, що квантові комп'ютери не перебувають у тому стані обчислювальної потужності, яка б дозволила їм повсюдно зламувати існуючі криптосистеми [4], багато криптографів вже зараз починають готуватися до часів, коли квантові обчислення будуть представляти реальну загрозу сучасним криптосистемам.

Варто зазначити, що найбільшу загрозу квантові комп'ютери становлять асиметричним крипто-алгоритмам. Більшість симетричних крипто-алгоритмів та хеш функцій вважаються відносно стійкими до атак із використанням квантових комп'ютерів. Саме тому пост квантова симетрична криптографія навряд буде сильно відрізнятиметься від поточної.

Розглянемо вразливість одного з найпоширенішого на сьогоднішній день криптографічного протоколу – TLS/SSL. Цей протокол на сьогоднішній день є

одним з найбільш використовуваних для обміну інформацією між клієнтом і сервером. Обмін даними між клієнтом та сервером може існувати відносно майже будь-якого сервісу, який використовують мережу Інтернет, що означає: потенційна загроза квантових обчислень щодо цього протоколу загрожує катастрофічними наслідками. Залежно від версії протоколу та підтримуваних шифрів, TLS/SSL включає використання RSA і протоколу розподілу ключа на еліптичній кривій Діффі-Хеллмана. І RSA і Діффі-Хеллман уразливі до атак за допомогою квантових комп'ютерів середньої потужності із застосуванням алгоритму Шора. Таким чином, уразливості для сучасної реалізації TLS/SSL можна узагальнити у два пункти:

1) Проблема розподілу ключів: сервер і клієнт повинні якимось чином згенерувати сесійний ключ (наприклад, за допомогою ECDH) не передаючи його відкритим каналом зв'язку. Сесійний ключ буде використовуватися для встановлення захищеного каналу зв'язку. У ході розвитку квантових комп'ютерів, стійкість криптосистем розподілу ключів буде знижуватися тим самим наражаючи на небезпеку стійкість захищеного каналу зв'язку

2) Проблема автентифікації: в ході цього кроку, сервер (або опціонально клієнт) доводить справжність повідомлення шляхом надання сертифіката, який включає підпис (наприклад RSA або ECDSA). Ця вразливість потенційно може призвести до проведення так званої атаки "людина посередині", де зловмисник, за допомогою застосування квантового комп'ютера, отримає приватний ключ і видає себе за власника сертифіката під час спілкування з клієнтом або сервером.

Першу з вищезгаданих проблем у майбутньому можна буде вирішити застосуванням криптосистем із квантовим розподілом ключа.

У майбутньому, необхідно, щоб квантово-стійкі алгоритми зайняли своє місце в подібному TLS протоколі і замінили застарілі і менш стійкі аналоги (RSA, ECDH, RCDSA).

Поки що, багато дослідників радять використовувати так звані "гібридні" схеми, в яких традиційні алгоритми існують поруч із квантовими. Гібридні схеми можуть знайти своє застосування доти, доки класичні алгоритми та криптосистеми повністю не доведуть свою ефективність та стійкість у застосуванні в пост квантовій ері.

3 КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ

3.1 Основні відомості що до квантового розподілу ключів

Особливе місце застосування квантових обчислень знайшлося в криптографії. Якщо узагальнювати, то криптографія - це вирішення проблеми комунікації двох сторін, які, можливо, абсолютно один одному не довіряють. Найчастіше вирішення даної проблеми включає підпис повідомлень, що відправляються, або їх шифрування. Або й те, й інше. Крім того, варто взяти до уваги, що канал, яким проходить комунікація - за умовчанням не вважається безпечним, тому що завжди є ймовірність того, що третя сторона (зловмисник, який зацікавлений у даних, що передаються) отримає доступ до інформації, що передається.

Здебільшого, криптографічні алгоритми, які передбачають встановлення захищеного каналу між сторонами, допомагають забезпечити вироблення загального секрету або сесійного ключа обом сторонам, без безпосередньої передачі частини секрету незахищеним каналом зв'язку. Одним з найпопулярніших алгоритмів вироблення загального секрету (протоколом розподілом ключів) в класичних комп'ютерних системах є алгоритм Діффі-Хеллмена, який повз все інше знайшов своє застосування в протоколі TLS/SSL.

Одним із ранніх відкриттів квантових обчислень стало те, що квантова механіка та принципи квантових обчислень можуть бути використані у протоколах розподілу ключів. Подібну процедуру назвали "квантовий розподіл ключів" або "процедура розподілу ключів по квантовим каналам зв'язку".

Основною ідеєю протоколів квантового розподілу ключів було використання одного з основних принципів квантової механіки, які свідчили, що спостереження за станом системи змушує спостерігаєму систему порушити свій стан. Таким чином, ґрунтуючись на цьому принципі, можна сказати, що

якщо зловмисник спробує втрутитися у передачу інформації по квантовому каналу зв'язку, його присутність буде розкрито, ґрунтуючись на порушеннях у каналі квантової передачі.

Квантовий розподіл ключів (Quantum key distribution) - це протокол, забезпечення безпечного каналу зв’язку , що дозволяє сторонам згенерувати сеансові ключі, обмінюючись даними тільки по публічному каналу зв'язку. Сеансовий ключ може бути використаний для генерації вхідних даних для інших протоколів. Однак, маючи на руках загальний секрет, вони мають можливість встановити між собою захищений канал зв'язку для подальшої взаємодії.

Вочевидь, що у квантових каналах зв'язку використовуватимуться кубіти (а не класичні біти і протоколи) які мають працювати із застосуванням квантових каналів зв'язку та мають ґрунтуватися на фундаментальних принципах квантової механіки. Безпека сеансового ключа може бути забезпечена лише в тому випадку, якщо відсоткове співвідношення перешкод у квантовому каналі не перевищує певного порогового значення. При підвищенні порога допустимих перешкод можна зробити висновок, що третя сторона намагається втрутитися у взаємодію сторін. Таким чином, безпека сеансового ключа забезпечується властивостями квантової механіки та квантової системи загалом.

Узагальнюючи: основна ідея, що стоїть за квантовим розподілом ключів, полягає в тому, що третя сторона (зловмисник) не може отримати жодної інформації про кубіти, що передаються по каналу, не порушивши їх стан (суперпозиція кубіту трансформується в один із ймовірних станів при спробі вимірювання). Також, дотримуючись теореми про заборону клонування (яка забороняє повністю копіювати стан системи) третя сторона (зловмисник) не може скопіювати кубіти, що передаються квантовим каналом.

Варто зробити пояснення про те, як саме кубіти вимірюються, і як саме вимірювання кубітів неправильним базисом може викликати перешкоди в

каналі. Кубіт повинен бути виміряний з застосування збігаючого за напрямком базису. Якщо при вимірі буде застосований не збігається базис - в такому випадку стан системи всього кубіту буде схильним до зміни, що згодом виллється в перешкоди в каналі.

У квантових протоколах розподілу ключів зазвичай використовуються ідея про передачу не ортогональних станів кубитів між сторонами Аліси та Боба. Вимірюючи перешкоди та похибки в переданих станах, вони визначають порогове значення можливих перешкод у квантовому каналі.

3.2 Протокол bb84

У 1984 році Чарльз Беннетт та Жіль Брассар запропонували новий квантовий протокол розподілу ключа BB84. Як і інші протоколи, його метою є створення нового сеансового ключа, який надалі можна використовувати в класичній симетричній криптографії. Однак особливістю протоколу є використання окремих положень квантової фізики для гарантії захисту ключа від перехоплення зловмисником. [13]

До початку чергового сеансу протоколу передбачається, що Аліса і Боб, як учасники протоколу, мають:

1) Квантовий канал зв'язку (наприклад, оптоволокно)

2) Класичний канал зв'язку

Протокол гарантує, що втручання зловмисника в протокол можна помітити доти, доки зловмисник зможе контролювати і читання, і запис всіх каналах спілкування відразу (контроль класичного каналу із квантовим одразу). Протокол складається з наступних етапів:

1) передача Алісою та прийом Бобом фотона по квантовому каналу зв'язку;

2) передача Бобом інформації про використані аналізатори (за яким базисом був зчитаний фотон);

3) передача Алісою інформації про збіг обраних аналізаторів та вихідних поляризацій.

У першій частині протоколу, Аліса бере одиничний фотон і поляризує під одним із чотирьох кутів: 0, 45, 90 або 135. Говоритимемо, що Аліса спочатку обрала базис поляризації (+ або X), а потім обрала в цьому базисі один із двох напрямків поляризації:

1) $0^\circ \rightarrow$ або $90^\circ \uparrow$ у першому базисі (+);

2) $45^\circ \nearrow$ або $135^\circ \nwarrow$ у другому базисі (X)

З погляду квантової фізики, ми можемо вважати, що ми маємо систему з двома базовими станами: $|0\rangle$ і $|1\rangle$. Стан системи у будь-який момент часу можна записати як $|\psi\rangle = \cos\alpha|0\rangle + \sin\beta|1\rangle$. Оскільки чотири обрані Алісою можливі вихідні стани неортогональні між собою (точніше, не все попарно), то із законів квантової фізики випливають два важливі моменти:

1) неможливість клонувати стан фотона;

2) неможливість достовірно відрізнити неортогональні стани один від одного

Будемо вважати, що Аліса використовує дві незалежні випадкові величини X_A і Aз ентропією по 1 біт кожна, щоб отримати нову випадкову величину $Y_A = f(X_A; A)$, що передається в канал зв'язку.

1) $H(A) = 1$ біт, вибір базису поляризації (+ або ×);

2) $H(X) = 1$біт, саме повідомлення, вибір одного з двох напрямків поляризації в базисі.

Єва може спробувати стати посередині каналу і щось з фотоном зробити. Може спробувати просто знищити фотон або надіслати замість нього випадковий. Хоча останнє призведе до того, що Аліса та Боб не зможуть

згенерувати загальний сеансовий ключ, корисну інформацію Єва з цього не витягне.

Єва може спробувати пропустити фотон через один із поляризаторів і спробувати зловити фотон детектором. Якби Єва точно знала, що у фотона може бути тільки два ортогональні стани (наприклад, вертикальна ↑ або горизонтальна → поляризація), то вона могла б вставити на шляху фотона вертикальний поляризатор ↑ і за наявності сигналу на детекторі визначити, чи була поляризація фотона вертикальною (1, є сигнал) або горизонтальною (0, фотон через поляризатор не пройшов і сигналу немає). Проблема Єви в тому, що у фотона не два стани, а чотири. І жодне становище одного поляризатора та єдиного детектора не допоможе Єві точно визначити, який із цих чотирьох станів прийняв фотон. А пропустити фотон через два детектори не вдасться. По-перше, якщо фотон пройшов вертикальний поляризатор, то якою б вихідною не була поляризація (↖,↑,↗), після поляризатора вона стане вертикальною ↑ (друга складова зітреться). По-друге, детектор, перетворюючи фотон в електричний сигнал, тим самим знищує його, що ускладнює його подальші вимірювання.[13]

Крім того, двох або навіть чотирьох детекторів для одного фотона мало. Відрізнити між собою неортогональні поляризації ↑ і ↖ можна лише статистично, тому що кожна з них проходитиме і вертикальний ↑, і діагональний ↖ поляризатори, але з різними ймовірностями (100% і 50%).

З погляду квантової фізики, Єва може спробувати провести вимірювання властивостей фотона, що призведе до колапсу хвильової функції фотона. Тобто після дії оператора вимірювання на хвильову функцію фотона вона неминуче змінюється, що призведе до перешкод у каналі зв'язку, які можуть виявити Аліса та Боб. Неможливість достовірно відрізнити неортогональні стани заважає Єві отримати повну інформацію про стан об'єкта, а заборона клонування заважає повторити вимір із дублікатом системи.

З погляду теорії інформації, ми можемо розглянути фактично передаваємий стан фотона як деяку випадкову величину Y_A. Єва використовує випадкову величину E (вибір пари ортогональних напрямів поляризатора - + або ×) для отримання величини Y_E як результату вимірювання Y_A. При цьому для кожного заданого вихідного стану Єва отримує на виході:

1) аналогічний стан з ймовірністю 50% (імовірність вибору пари ортогональних напрямків поляризатора, що збігаються з обраними Алісою);

2) один з двох неортогональних оригінальних станів, з ймовірністю 25% кожен.

Таким чином, умовна ентропія величини Y', виміряної Євою, щодо величини Y, переданої Алісою, дорівнює:

$$H(Y_E|Y_A) = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{4}\log_2\frac{1}{4} - \frac{1}{4}\log_2\frac{1}{4} = 1{,}5\text{біт}.$$

І взаємна інформація між цими величинами дорівнює:

$$I(Y_E; Y_A) = H(Y_E) - H(Y_E|Y_A) = 0{,}5\text{біт}$$

Що становить 25% від ентропії, що передається по каналу випадкової величини Y_E. Якщо розглядати величину X_E, яку Єва намагається відновити з прийнятої нею величини Y_E, то з погляду теорії інформації ситуація ще гірша:

1) при вгаданому базисі поляризатора Єва отримує вихідну величину:

$X_E = X_A$

2) при невгаданому базисі ще в половині випадків криптоаналітик отримує вихідну величину (через випадкове проходження фотона через неправильний поляризатор).

Виходить, що умовна ентропія відновлюваної Євою послідовності X_E щодо вихідної X_A дорівнює:

$$H(X_E|X_A) = -\frac{3}{4}\log\frac{3}{4} - \frac{1}{4}\log\frac{1}{4} \approx 0{,}81\text{біт}.$$

І взаємна інформація:

$$I(X_E; X_A) = H(X_E) - H(X_E|X_A) \approx 0{,}19\text{біт}.$$

Що становить ≈ 19 від ентропії вихідної випадкової величини X_A. Оптимальним алгоритмом подальших дій Єви буде надіслати Бобу фотон в отриманій поляризації (передати далі канал отриману випадкову величину Y_E). Тобто якщо Єва використовувала вертикальний поляризатор ↑і детектор зафіксував наявність фотона, то передавати фотон у вертикальній поляризації ↑ , а не намагатися вводити додаткову випадковість і передавати ↖ або ↗

Боб, аналогічно діям Єви (хоча це швидше Єва намагається імітувати Боба), випадково вибирає ортогональну пару напрямків поляризації (+ або ×) і ставить на шляху фотона поляризатор (↑ або ↖) та детектор. У разі сигналу на детекторі він записує одиницю, у разі відсутності - нуль.

Можна сміливо сказати, що Боб, як і Єва, вводить нову випадкову величину B (характеризує вибір базису поляризації Бобом) й у результаті вимірів отримує нову випадкову величину X_B. Причому Бобу поки невідомо, чи використовував він оригінальний сигнал Y_A переданий Алісою, або підроблений сигнал Y_E , переданий Євою:

1) $X_{B1} = f(Y_A, B)$;

2) $X_{B2} = f(Y_E, B)$;

Далі Боб повідомляє по відкритому класичному каналу зв'язку, які саме базиси поляризації використовувалися для кожного с кубітів, а Аліса вказує, які з них збіглися з спочатку обраними. У цьому самі виміряні значення (пройшов фотон через поляризатор чи ні) Боб залишає у секреті.

Можна сказати, що Аліса та Боб публікують значення згенерованих ними випадкових величин A та B. Приблизно в половині випадків ці значення збігатимуться (коли Аліса підтверджує правильність вибору базису

поляризації). Для фотонів, у яких значення A і B збіглися, збігатимуться і значення X_A і X_{B1}. Тобто:

1) $H(X_{B1}|X_A; A = B) = 0$біт

2) $I(X_{B1}; X_A|A = B) = 1$біт

Для тих фотонів, для яких Боб вибрав неправильний базис поляризації, значення X_{B1} і X_A будуть незалежними випадковими величинами (бо, наприклад, при вихідній діагональній поляризації фотон пройде і через вертикальну, і через горизонтальну щілини з ймовірністю 50%):

1) $H(X_{B1}|X_A; A \neq B) = 1$біт

2) $I(X_{B1}; X_A|A \neq B) = 0$ біт

Розглянемо випадок, коли Єва втрутилася у процес передачі інформації між Алісою та Бобом і відправляє Бобу вже свої фотони, але не має можливості змінювати інформацію, якою Аліса та Боб обмінюються за класичним каналом зв'язку. Як і раніше, Боб відправляє Алісі обрані базиси поляризації (значення B), а Аліса вказує, які з них збіглися з обраними нею значеннями A.

Таблиця 3.1 – Результати взаємодії Аліси і Боба за квантовим каналом зв’язку із втручанням Єви (зловмисника)

Базис Аліси	Базис Єви	Базис Боба	Результат взаємодії
X	X	X	Прийнято без помилок
X	X	+	Відхиллено
X	+	+	Прийнято з помилками

X	+	+	Відхиллено

Але тепер для того, щоб Боб отримав коректне значення X_{B2} ($X_{B2} = X_A$), повинні бути виконані всі наступні умови для кожного фотона.

1) Єва повинна вгадати базис поляризації Аліси ($E = A$)

2) Боб повинен вгадати базис поляризації Єви ($B = E$)

Розглянемо без обмеження спільності варіант, коли Аліса використала діагональну поляризацію. (табл. 3.1)

При цьому Боб і Аліса будуть впевнені, що в першому та третьому випадках (які з їхньої точки зору нічим не відрізняються) Боб коректно відновив поляризацію фотонів. Оскільки всі ці рядки рівно ймовірні, то виходить, що у Боба та Аліси після вибору тільки фотонів з вгаданим базисами (як вони впевнені) тільки половина поляризацій (значень X_A і X_B) співпадатиме. При цьому Єва знатиме ці значення. Кількість відомих Єві біт загальної послідовності і частка помилок у ній перебувають у лінійній залежності від кількості перехоплених Євою бітів.[13]

Незалежно від наявності чи відсутності Єви, Аліса та Боб змушені використовувати заздалегідь узгоджену процедуру виправлення помилок. Код корекції помилок, що використовується, з одного боку, повинен виправляти помилки, викликані фізичними особливостями квантового каналу. Але з іншого боку, якщо код виправлятиме занадто багато помилок, то він приховає від нас потенційний факт наявності Єви. Доведено, що існують такі методи виправлення помилок, які дозволяють безпечно (без небезпеки розкрити інформацію Єві) виправити від 7,5% (Майєрз, 2001) до 11% помилок (Ватанабе, Матсумото, Уйематсу).[13]

Цікавим є також варіант, коли Єва може змінювати інформацію, що передається не тільки по квантовому, але й по класичному каналу зв'язку. У цьому випадку багато залежить від того, в який бік (від імені якого) Єва може підробляти повідомлення. У найнегативнішому сценарії, коли Єва може видати себе і за Алісу, і за Боба, матиме місце повноцінна атака "людина посередені" (MITM), від якої неможливо захиститися жодним способом, якщо не використовувати додаткові захищені канали зв'язку або не ґрунтуватися на інформації, переданій наперед. Проте це буде вже зовсім інший протокол.

3.3 Протокол bb92

У 1992 році один з авторів протоколу BB84 - Чарльз Беннет висунув ідею, що учасникам не обов'язково використовувати чотири різні варіанти поляризації, а досить двох, але неортагональних варіанти поляризації. Наприклад 0 градусів та 45 градусів.

Для кожного біта, який передається в канал, виконується наступний порядок дій:

1) Аліса поляризує фотон залежно від біта b_i і передає кубит квантовим каналом зв'язку Бобу:

$b_i = 0$; Аліса поляризує фотон під 0 градусів

$b_i = 1$; Аліса поляризує фотон під 45 градусів

2) Боб, випадковим чином вибирає базис поляризації з ортогональних до 0 і 45 градусів (тобто з 90 і 135) і намагається зчитати фотон, що передається по квантовому каналу зв'язку. Якщо зчитати фотон вийшло, то Боб робить висновок про обрану Алісою поляризацію і кодований біт b_i

1) Якщо Боб успішно зчитав фотон на поляризації в 135 градусів, то Аліса обрала поляризацію в 0 градусів і відповідно $b_i = 0$

2) Якщо Боб успішно зчитал фотон на поляризації в 90 градусів, то Аліса обрала поляризацію в 45 градусів і відповідно $b_i = 1$

Принцип, який лежить за цим, полягає в тому, що Боб не може зчитати ортогонально поляризований вектор, тому успішно зчитаний фотон завжди буде говорити про те, який конкретно біт був переданий.

Боб за класичним каналом зв'язку повідомляє Алісі, чи вдалося зчитати фотон чи ні. Якщо так, то біт приймається учасниками за переданий

3.4 Протокол bb84(4+2)

Протокол bb84(4+2) є результатом об’єднання протоколів bb84 із протоколом bb92. Їх об’єднання було результатом спроби протидії так званій PSN атаці. Основна ідея протоколу наступна: якщо Єва (зловмисник) теоретично може перехватити інформацію що до коректних базисів поляризації, та після цього використати скопійовані фотони (PSN атака) за для обчислення ключу (і повного взлому протоколу), має сенс використовувати такі базиси поляризації, де кути поляризації неортогональні (тобто так само як у протоколі bb92).

Для кожного біта, який передається в канал, виконується наступний порядок дій:

1) Аліса обирає базис поляризації із неортогональними один до одного кутів поляризації (наприклад 0 та 45 градусів)
2) Аліса та Боб проводять взаємодію згідно протоколу bb92 у обраному базису

Таким чином, якщо Єва намагається відтворити послідовність бітів за допомогою скопійованих раніше фотонів – буде вірогідність того (1/2), що відтворити фотон не вийде.

3.5 Порівняння протоколів bb84 та bb84(4+2)

Як було сказано раніше, основною перевагою протоколу bb(4+2) перед bb84 була його теоретична стійкість до PNS атак.

Атака PNS – потужна атака, призначена для використання багатофотонної вразливості яка дозволяла повністю відтворити розподілені ключі без введення помилок у канал зв’язку (тобто присутність зловмисника буде непомічена). Для проведення атаки, Єва повинна втрутитись у передачу, та замінити відрізок каналу між Євою та Бобом на квантовий канал телепортації. Цій канал дозволяє використовувати властивості квантової механіки та передавати фотон від Єви до Бобу без жодних втрат та помилок. Для кожного імпульсу, який генерується Алісою, Єва виконує спеціальне квантове вимірювання без втрат для знаходження кількості фотонів у кожному імпульсі. Якщо кількість фотонів 1 – Єва блокує сигнал. У інших випадках Єва квантує фотони та зберігає іх у своїй квантовій пам’яті. Після перехвату базисів по відкритому каналу, Єва обробляє збережені фотони та відтворює послідовність біт ключа.

Протокол bb84(4+2) у свою чергу адоптує принципи впроваджені у протоколі bb92 та використовує пари неортогональних один до одного кутів у базисі, тим самим зробив точне відновлення передаваємого стану Євою – неможливим

Одним з самих важливих переваг перед bb84 є те, що bb84(4+2) зберігає свою секретність що до довжин оптоволоконної лінії (десь 150 кілометрів), у той же час, протокол bb84 може запровадити безпечність лише на довжину у 50 кілометрів. Тобто узагальнюючи основні відміни bb84(4+2) перед bb84 є:

1) Стійкість до PNS атак
2) Використання двох пар неортогональних базисів
3) Покращені показники безпечної передачі фотону
4) Покращенні показники виявлення порушника у каналі

3.6 Практичне дослідження протоколу bb84 на базі установки EDU-QCRY1

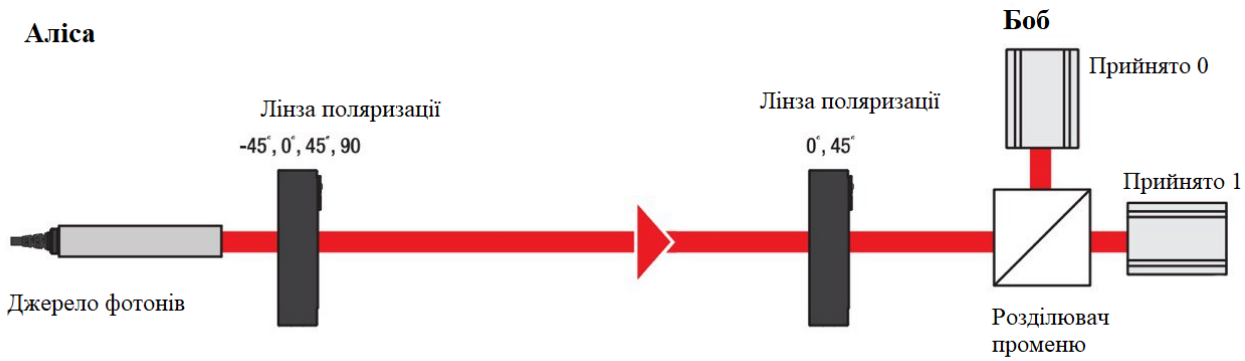


Рисунок 3.1 – Схематичне уявлення установки EDU-QCRY1

Установка EDU-QCRY1 складається з двох ключових компонентів (рис. 3.1):

1) Модель відправника Аліси. Складається з лазерного діод-випромінювача підключеного до електронного контролеру (джерело фотонів) та лінзи поляризатора

2) Модель приймача Боба. Складається з лінзи поляризатора, куба за для розподілу лазерного сигналу та двох детекторів із електронним контролером прийому. Один детектор відповідає за успішне проходження фотону через лінзу та куб поляризації. Другий детектор відповідає за не проходження фотону через лінзу та куб розподілу сигналу. Відповідно перший детектор відповідає за біт 0, а другий за біт 1

Опціонально, у схему взаємодії може бути додана модель порушника (Єви), яка виконує втручання в квантовий канал взаємодії та додає помилки у вимірювання (якщо Єва обирає неправильний базис – приймаюча сторона не може обробити результат).

На рис. 3.1 представлена модель відправника сигналу, де 1 – електронний контролер випромінювача, 2 – лазерний діод-випромінювач, 3 - лінза поляризатора.

На рис 3.2 представлена модель приймача сигналу, де 1 – лінза поляризатора, 2 – електронний контролер прийому, 3 – куб за для розподілу лазерного сигналу, 4- детектор прийому фотона, який відповідає біту 0 (тобто не прийому сигналу), 5 - детектор прийому фотона, який відповідає біту 1

Для проведення взаємодії між Алісою та Бобом згідно протоколу bb84, перш за все ми повинні:

1) Обрати базис за яким фотони будуть поляризуватися: оберемо базис + у якому ми маємо два доступних кути для поляризації – 0 та 90. На лінзі поляризації відправника виставляємо значення 90.
2) Наступним кроком буде обрання аналогічного базису на стороні приймача фотона (Боба). Оберемо базис + та виставимо лінзу поляризатора у положення 0 (рис 3.3)
3) Далі випускаємо фотон відправника через лінзу поляризатора та бачимо, що приймач №4 (рис 3.2) приймає сигнал (світлодіод моргає). Таким чином ми успішно прийняли біт 1.
4) Повторюємо шаги 1-3 n разів, змінюючи базиси поляризації на стороні Аліси (рис 3.4) та Боба де n – кількість бітів у ключі, записуючи базис та направлення поляризації кожного фотона. У нашому випадку ключ буду довжиною 8 біт.
5) Після передачі останнього фотону, Боб по відкритому каналу повинен передати Алісі індекс кожного прийнятого фотону та обраний базис поляризації. Аліса ж повинна у відповіді указати у яких випадках базис

фотону був обран коректно (базис Аліси збігається із базисом Боба). Однак, так як ми використовуємо тестову модель і ми виставляли базиси Аліси та Боба однаковими навпродовж усієї передачи, приймаємо за факт те, що усі передані фотони були прийняті у коректному базисі. У реальних умовах взаємодії, Боб обирає базис випадково та приблизно у половині випадків базис буде збігатися.

6) Формуємо таблицю прийому-передачі фотонів у якої вказуємо базиси, обрані Алісою, базиси обрані Бобом, кути поляризації та прийняті біти

Таблиця 3.2 – Результати прийому-передачі фотонів

Базис Аліси	Кут поляризації Аліси	Переданий Алісою біт	Базис Боба	Кут поляризації Боба	Прийнятий Бобом біт
+	0	0	+	0	0
+	90	1	+	0	1
X	45	1	X	45	1
X	-45	0	X	45	0
+	0	0	+	0	0
+	90	1	+	0	1
X	45	1	X	45	1
X	-45	0	X	45	0

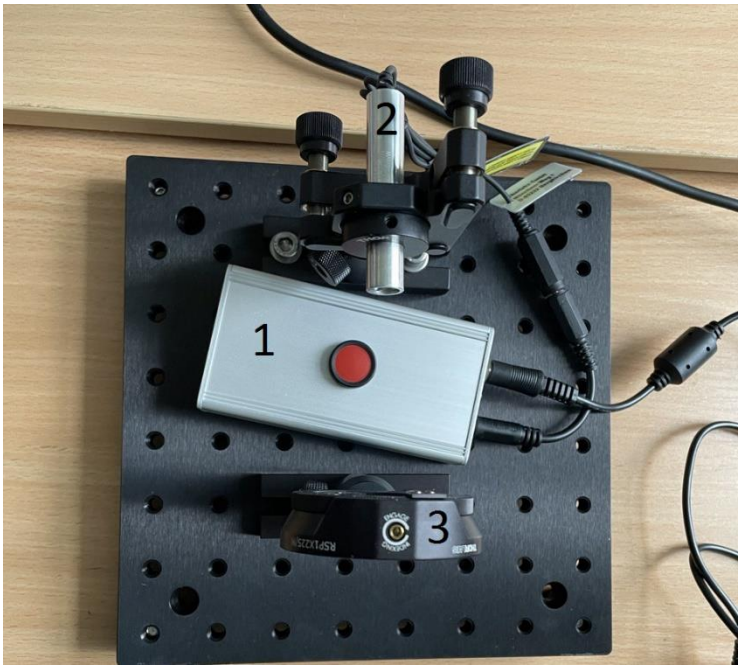


Рисунок 3.2 – Модель відправника Аліси

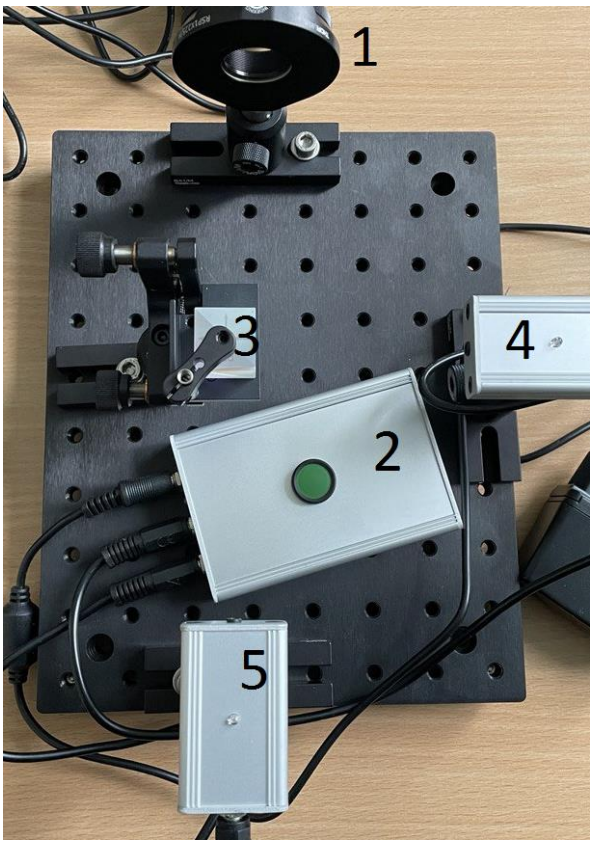


Рисунок 3.3 – Модель приймача Боба

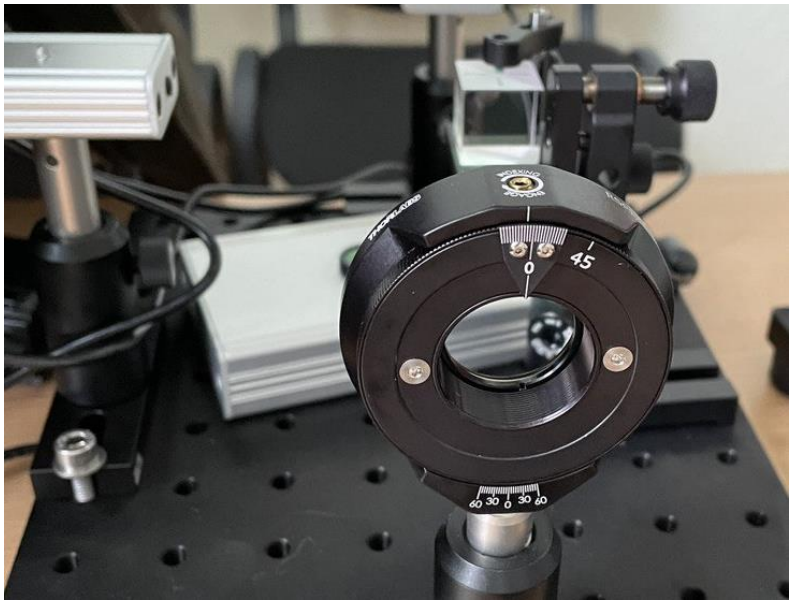


Рисунок 3.4 – Обрання базису на стороні приймача (Боба)

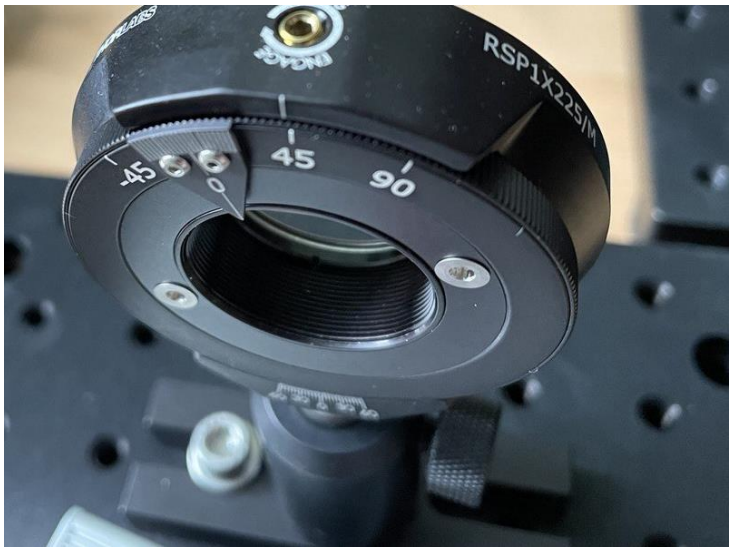


Рисунок 3.5 – Обрання базису та кута поляризації на стороні відправника (Аліси)

У ході експерименту було проведено моделювання роботи алгоритму bb84 та взаємодії його учасників (Алісі і Боба), які успішно згенерували сесійний у вигляді послідовності бітів 01100110. Однак, ця система може служити лише експериментальною моделлю, і не може бути використана у реальних умовах. У реальних умовах Аліса і Боб будуть значно віддалені один від іншого та Боб не буде знати об

обраних базисах Аліси.

3.7 Недоліки квантових протоколів розподілу ключів

Підсумовуючи, можна сказати, що квантові протоколи розподілу ключів (а саме ними поки що й обмежується вся відома на сьогоднішній день квантова криптографія) мають як певні переваги, так і фатальні недоліки, що ускладнюють їх використання (і ставить під питання саму цю необхідність).[1]

1)Будь-які квантові протоколи (як і взагалі будь-які квантові обчислення) вимагають оригінального та дорогого обладнання

2) Квантові канали зв'язку – це завжди фізичні канали зв'язку. У них є максимальна довжина каналу та певний рівень помилок. Для квантових каналів (на сьогодні) повторювачів не існує, які дозволили б збільшити довжину безумовно квантової передачі даних.

3) Жоден квантовий протокол (нині) неспроможний обходитися без додаткового класичного каналу зв'язку. Для такого зв'язку потрібні мінімум такий самий рівень захисту, як і при використанні, наприклад, криптографії з відкритим ключем.

4) Для всіх протоколів особливу проблему представляє не лише доказ коректності (що є дуже нетривіальною справою у разі сумлінних перешкод), а й інженерне завдання щодо реалізації протоколу в залізі.

Ми можемо точно сказати, що протоколи bb84, bb92 - безпечні лише в тому випадку, якщо Єва (зловмисник) намагатиметься перехоплювати по одному кубіту інформації за раз. Складність у тому, що Єва може зчитувати набір кубітів за один раз. У цьому випадку Єва формує у себе блоки кубітів, які надалі можна обробити. Для того, щоб спробувати вирішити цю проблему, сторона, що відправляє, може використовувати квантові коди корекції, що дозволяють скоригувати t кубіт, де t - кількість неправильних кубіт в блоці, сформованому Євою (кубіти, які змінили свій квантовий стан через спроб Єви визначити ймовірні амплітуди) . Це дозволить Бобу позбутися та відкинути кубіти, стан яких

було змінено Євою (що збільшить стабільність протоколу загалом). Однак, це рішення можна тільки застосувати за наявності перешкодостійкого, стабільного квантового комп'ютера, який зможе на ходу кодувати і декодувати кубіти.[1,13,7]

Узагальнюючи, можна сказати, що квантові протоколи розподілу ключів не набудуть своєї заслуженої популярності доти, доки розробка перешкодостійкого квантового комп'ютера не буде завершена. Більш глибоке розуміння квантової механіки та її законів, які застосовуються до світів обчислень та криптографії в цілому, є ключовим фактором у розкритті та початку загального застосування квантових алгоритмів, включаючи протоколи розподілу ключів по квантовому каналу.

ВИСНОВКИ

Сучасна криптографія розвивається разом із технологіями обчислювальної техніки, що безпосередньо впливає на криптографію загалом. Чим більша потенційна обчислювальна потужність, тим вища ймовірність того, що буде місце алгоритм (або група алгоритмів), які за детерміноване час зможуть уявити загрозу сучасним криптографічним алгоритмам. Грунтуючись на складних математичних завданнях (проблеми факторизації, дискретного логарифмування тощо) – криптографія намітила собі шлях, обмежений розвитком обчислювальної техніки та методів обробки інформації. Квантові комп'ютери, у свою чергу, кілька десятиліть тому почали вносити хаос і невпевненість у сучасні криптоалгоритми та їх стійкість. Середньостатистичний квантовий комп'ютер у теорії мав потенціал вирішувати складні математичні завдання, які лежать в основі сучасних криптоалгоритмів не просто за детермінований час, а буквально миттєво (коли найпотужніші класичні комп'ютери минали роки).

Поява пост-квантової криптографії, як явної міри запобігання неминучій загрозі, була неминучою і логічною. Якщо атакуюча сторона потенційно буде використовувати потенціал квантових обчислень і квантові комп'ютери для обробки, то є сенс спробувати побудувати захист на тих же законах у вигляді певної кількості протоколів (наприклад, класична симетрична криптографія вже має стійкість до квантових алгоритмів). Багато протоколів і алгоритмів починають купувати аналоги, засновані на квантовій теорії та квантових обчисленнях. Таким чином дослідники вживають заходів для запобігання криптографічній катастрофі.

Багато вчених вважають побоювання у тому, що квантові обчислення зламають все й одразу не більше ніж перебільшенням, оскільки до появи повністю функціонального, завадостійкого та стабільного квантового

комп'ютера в лабораторії – пройдуть роки (якщо не десятиліття). До отримання доступу до цієї технології звичайних людей взагалі годі й говорити. Не відомо коли квантовий комп'ютер вийде (і чи взагалі вийде) на ринок. Тому перехід у квантову еру обчислень не буде лавиноподібним, а буде радше вкрай східчастим. Тому в дослідників залишається ще час винахід способів захисту від квантових обчислень.

Одним з результатів досліджень, спрямованих на адаптацію квантових алгоритмів та розвитку пост-квантової криптографії було винахід протоколів квантового розподілу ключів (розподіл ключів по квантовому каналу зв'язку) або QKD (quantum key distribution). Тоді як звичайні протоколи розподілу ключів ґрунтуються на трьох фундаментально складних математичних обчислювальних задачах, протоколи квантового розподілу ключів намагаються використати та застосовувати особливості поведінки елементарних частинок у квантовій механіці та квантових системах загалом. Квантові алгоритми розподілу ключів оперують квантовими сутностями (кубіт, суперпозиція) та використовують теорію ймовірності для того, щоб визначати успішність взаємодії.

Протоколи QKD (quantum key distribution) активно використовують принципи та закони квантової теорії, застосовуючи їх особливості у процесі роботи. Таким чином QKD застосували одну з найкорисніших властивостей квантової механіки, де факт спостереження за системою вносить зміни в цю систему. Будь-яка спроба виміряти систему або визначити вторинні параметри може призвести до зміни стану. Стосовно алгоритмів QKD ця особливість буквально говорить - якщо хтось встане між стороною, що відправляє, і приймаючою, намагаючись вимірювати проходять по каналу кубити (які є системою в суперпозиції, у ймовірностях якої відправна сторона закодувала інформацію), то стан кубіту може постраждати і сторона, що приймає. вважає кубит невірно і відкине його на фінальному етапі узгодження як перешкоду у каналі або помилку зчитування. Таким чином, якщо кількість помилок у каналі

перевищуватиме певний поріг, то й Аліса та Боб можуть з певною впевненістю припустити, що хтось чи щось намагається перехопити інформацію. Тим самим зловмисника буде розкрито. Таким чином, протоколи QKD забезпечують свою захищеність за рахунок застосування квантової механіки та квантових обчислень, тим самим забезпечуючи виживання протоколу в пост-квантову еру.

Однак, як би не було багато плюсів у квантових протоколів та криптосистем (QKD зокрема), також існує безліч проблем, більшість яких пов'язані з рівнем розвитку квантових технологій на сьогоднішній день. Обладнання квантового каналу буде не виправдано дорого, а дальність дії подібного каналу буде суворо обмежена, оскільки поки що не існує повторювачів, які могли б продовжити передачу кубітів (заборона клонування стану кубіту).

Наступне впровадження QKD в криптосистеми знову ж таки не виправдано, так як для успішного кодування і декодування кубитів з подальшою обробкою, необхідно мати повністю функціонуючий квантовий комп'ютер, не схильний до перешкод. Тому не сьогоднішній день крипто алгоритми засновані на квантових технологіях (включаючи квантовий розподіл ключів) ще не знаходяться на рівні практичного застосування і можуть тільки запропонувати теоретичну базу, що підтверджує їхню безпеку

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Aaronson Scott. Quantum Computing Since Democritus / Scott Aaronson. — Cambridge University Press, 2013. — 398 с.
2. Copeland B. Jack. The Essential Turing / B. Jack Copeland. — Clarendon Press, 2004. — 622 с.
3. Algorithms for quantum computation: discrete logarithms and factoring / Proceedings 35th Annual Symposium on Foundations of Computer Science. — Santa Fe 20-22 лист. 1994 р. — IEEE Shor P.W. 1994. — 124–134 с.
4. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. — Харків: Форт, 2013. — 880 с.
5. Leeuwen J. V. Handbook of Theoretical Computer Science, Volume A / J. V. Leeuwen. 1994. — Elsiever / MIT Press. — 1010 с.
6. Michael Sipser. Introduction to the Theory of Computation (2nd ed.). / Michael Sipser, 2006. — USA: Thomson Course Technology. p. 421 с.
7. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / Peter W. Shor. 1996. — 28 с.
8. Горбенко Ю. І. Аналіз можливостей квантових комп’ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя / Восточно-Европейский журнал передовых технологий. — Харків, 2014. — Том 6, №1(67). — С. 8–15.
9. The quantum algorithm zoo. [Електронний ресурс] / S. Jordan. — 2011. — Режим доступу до журн.: http://math.nist.gov/quantum/zoo/
10. Abhijit Das. Computational Number Theory / Abhijit Das. — CRC Press, 2016. — 614 с.
11. Karmarkar, N. A new polynomial-time algorithm for linear programming. / Karmarkar, N. — Combinatorica, 1984. — 395 с.

12. Agrawal Manindra. PRIMES is in P / Manindra Agrawal, Neeraj Kayal, Nitin Saxena. — Department of Computer Science & Engineering Indian Institute of Technology Kanpur, 2002. — 9 с.
13. Nielsen Michael. Quantum Computation and Quantum Information (2nd ed.) / Michael Nielsen, Isaac Chuang. — Cambridge University Press, 2010. — 665 с.
14. Michael R. Garey. Computers and Intractability: A Guide to the Theory of NP-Completeness / Michael R. Garey, David S. Johnson. — W. H. Freeman, 1979. — 338 с.
15. Sato Takayuki. Complexity and Completeness of Finding Another Solution and Its Application to Puzzles / Sato Takayuki, Seta Takahiro. — International Symposium on Algorithms, 1987. — 8 с.
16. A New Golden Age for Computer Architecture: Domain-Specific Hardware/Software Co-Design, Enhanced Security, Open Instruction Sets, and Agile Chip Development / International Symposium on Computer Architecture. — John L. Hennessy David A. Patterson, 2018. — 27-29 с.
17. Computational complexity of probabilistic Turing machines, SIAM Journal on Computing [Електронний ресурс] / J. Gill, 2006. — 21 с. — Режим доступу до журн. : https://epubs.siam.org/doi/pdf/10.1137/0206049
18. Quantum Complexity Theory, SIAM Journal on Computing [Електронний ресурс] / Ethan Bernstein, Umesh Vazirani, 1997. — 1411-1473 с. — Режим доступу до журн. : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.655.1186&rep=rep1&type=pdf
19. Bennett Charles H. Relative to a Random Oracle A, P^A != NP^A != co-NP^A with Probability 1", SIAM Journal on Computing [Електронний ресурс] / Charles H. Bennett, John Gill, 1981. — 96-113 с. — Режим доступу до журн. :

https://pdfs.semanticscholar.org/6f4d/2abf44adf686e4d88dd956d969fb921cc60f.pdf?_ga=2.259262858.1845783001.1590726583-1440781742.1590726583

20. Brandl Matthias F. A Quantum von Neumann Architecture for Large-Scale Quantum Computing / Matthias F. Brandl. — Institut f¨ur Experimentalphysik, Universit¨at Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria, 2017. — 44 с.
21. Tanenbaum A. S. Structured Computer Organization (5th edition) / A. S. Tanenbaum. — Pearson, 2005. — 757 с.
22. DiVincenzo D.P. The physical implementation of quantum computation / D.P. DiVincenzo, IBM, 2000. — 9 с.
23. Hawking Stephen. A Brief History of Time: From the Big Bang to Black Holes / Stephen Hawking. — Bantam Books, 2016. — 245 с.
24. Feynman R. The Feynman Lectures on Physics, Vol. 3. / Richard Feynman, Leighton, Robert Sands, 1964. — California Institute of Technology. — 400 с.
25. Einstein A. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? / A. Einstein, B. Podolsky, N. Rosen. — Institute for Advanced Study, 1935. — 777-780 с.
26. Hammond William F. Continued Fractions and the Euclidean Algorithm, Lecture notes prepared for MATH 326 / William F. Hammond. — Department of Mathematics and Statistics University at Albany, 1997. — 15 с.
27. Hartnett Kevin. “Does Neven's Law Describe Quantum Computing's Rise?”, Quanta Magazine [Електронний ресурс] / Kevin Hartnett. — 2019. — Режим доступу до журн. : https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/#
28. Laarhoven Thijs. Solving the Shortest Vector Problem in Lattices Faster Using Quantum Search / Thijs Laarhoven, Michele Mosca, Joop van de Pol. — 2013. — 19 с.

ВІДОМІСТЬ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Позначення	Найменування	Дод. відомості
		Текстові документи	
1	ГЮІК.ХХХ1684Ст.14ПЗ	Пояснювальна записка	64 стор.
		Графічні документи	
2		Слайд-презентація	слайд
3		Інші документи	
		Електронна версія ПЗ	1
		Рецензія	1 с.
		Відгук	1 с.

					ГЮІК.ХХХ1684Ст.14ВД			
Змін.	Арк	Номер докум.	Підп	Дата				
Розроб.		Скічко Д. В.			Криптосистеми з квантовим розподілом ключів	Літ	Аркуш	Аркушів
Перевір.		Халімов Г.З				У		
Н.контр.		Шевченко Л.П.				ХНУРЕ Кафедра БІТ		
Затв.		Халімов Г.З.						