Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)

Кафедра Фізичних основ електронної техніки
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

ОСНОВНІ ПОЛОЖЕННЯ КВАНТОВОЇ КРИПТОГРАФІЇ
(тема)

Виконав:
студент 2 курсу, групи ЛОЕТм-19-1
Коптяков О. В.
(прізвище, ініціали)

Спеціальність 152 «Метрологія та інформаційно-вимірювальна техніка»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо -наукова)

Освітня програма «Лазерна і оптоелектронна техніка»
(повна назва освітньої програми)

Керівник проф., зав. каф.ФОЕТ Мачехін Ю.П.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Мачехін Ю.П.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
Кафедра Фізичних основ електронної техніки
Рівень вищої освіти другий (магістерський)
Спеціальність 152 «Метрологія та інформаційно–вимірювальна техніка»
(код і повна назва)
Освітня програма «Лазерна і оптоелектронна техніка»
(повна назва)

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

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Коптякову Олексію Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Основні положення квантової криптографії
затверджена наказом по університету від " 27 " жовтня 2020 р. № 1451 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 17 грудня 2020р.
3. Вихідні дані до роботи Криптографічні протоколи. Протокол квантового шифрування BB84.

4. Перелік питань, що потрібно опрацювати в роботі
1. Задачі криптографії. 2. Способи шифрування даних. 3. Протоколи шифрування. 4. Проблеми, недоліки та тенденції розвитку квантової криптографії. 5. Застосування квантової криптографії на практиці.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

Схема структурна системи квантової криптографії – А4 – 1шт.

Схема структурна протокол ВВ84 – А4 – 1шт.

Демонстраційний матеріал – 12 шт.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Інформаційно тематичний пошук та огляд літературних джерел з квантової криптографії	02.11.2020 – 12.11.2020	Виконано
2	Ознайомлення з квантовими протоколами шифрування	13.11.2020 – 17.11.2020	Виконано
3	Фізична та практична реалізація системи квантового шифрування	17.11.2020 – 23.11.2020	Виконано
4	Оформлення пояснювальної записки	24.11.2020 – 03.12.2020	Виконано
5	Оформлення демонстраційної частини	04.12.2020 – 09.12.2020	Виконано
6	Проходження нормоконтролю та отримання рецензії на роботу	10.12.2020 – 14.12.2020	Виконано
7	Підготовка та захист атестаційної роботи	15.12.2020 – 22.12.2020	

Дата видачі завдання 2 листопада 2020 р.

Студент _____
(підпис)

Керівник роботи _____ проф. зав. каф.ФОЕТ Мачехін Ю.П.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до атестаційної роботи: 41 с., 11 рис., 4 табл., 2 додатки, 16 джерел.

КРИПТОГРАФІЯ, КВАНТОВА КРИПТОГРАФІЯ, ОДИНОЧНИЙ ФОТОН, ПРОТОКОЛ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ, КВАНТОВІ ПРОТОКОЛИ.

Об’єкт дослідження — протоколи квантового шифрування.

Мета роботи — ознайомлення з квантовими протоколами шифрування. Визначення проблем та недоліків квантової криптографії. Ознайомлення з фізичною та практичною реалізацією системи квантової криптографії.

Методи дослідження — теоретичний.

В аналітичному огляді літератури розглянуті задачі криптографії та основні технології передачі секретних даних, визначені способи та протоколи квантового шифрування даних.

Спираючись на розглянутий матеріал визначені проблеми, недоліки та основні тенденції розвитку квантової криптографії.

Проведено ознайомлення з фізичною та практичною реалізацією системи квантової криптографії.

ABSTRACT

Explanatory note to attestation work: 41 p., 11 fig., 4 tabl., 2 appendices, 16 sources.

CRYPTOGRAPHY, QUANTUM CRYPTOGRAPHY, SINGLE PHOTON, QUANTUM KEY DISTRIBUTION PROTOCOL, QUANTUM PROTOCOLS.

The object of research is quantum encryption protocols.

The purpose of the work is — introduction to quantum encryption protocols. Identification of problems and shortcomings of quantum cryptography. Knowledge of the physical and practical implementation of the quantum cryptography system.

Research methods — theoretical.

In the analytical review of the literature the tasks of cryptography and the main technologies of secret data transmission are developed, the methods and protocols of quantum data encryption are determined.

Verification when considering the material of certain problems, shortcomings and main trends in the development of quantum cryptography.

A knowledge of the physical and practical implementation of the quantum cryptography system was carried out.

РЕФЕРАТ

Пояснительная записка к аттестационной работе: 41 с., 11 рис., 4 табл., 2 прилож., 16 источн.

КРИПТОГРАФИЯ, КВАНТОВАЯ КРИПТОГРАФИЯ, ОДИНОЧНЫЙ ФОТОН, ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, КВАНТОВЫЕ ПРОТОКОЛЫ.

Объект исследования — протоколы квантового шифрования.

Цель работы — ознакомление с квантовыми протоколами шифрования. Определение проблем и недостатков квантовой криптографии. Ознакомление с физической и практической реализацией системы квантовой криптографии.

Методы исследования — теоретический.

В аналитическом обзоре литературы рассмотрены задачи криптографии и основные технологии передачи секретных данных, определенны способы и протоколы квантового шифрования данных.

Опираясь на рассматриваемый материал определенные проблемы, недостатки и основные тенденции развития квантовой криптографии.

Проведено ознакомление с физической и практической реализацией системы квантовой криптографии.

ЗМІСТ

ВСТУП

Квантова криптографія як наука зародилася в 1984 році, коли був розроблений перший протокол квантового розподілу ключів, названий BB84. Головною перевагою квантових криптографічних протоколів перед класичними є суворе теоретичне обґрунтування їх стійкості: якщо в класичній криптографії стійкість зводиться, як правило, до припущень про обчислювальних можливостях перехоплювача, то в квантової криптографії перехоплювач може робити все допустимі законами природи дії, і все одно у нього не буде можливості дізнатися секретний ключ, залишившись при цьому непоміченим.

Важливим для квантової криптографії властивістю квантової механіки є властивість колапсу хвильової функції [1], яке означає, що при вимірюванні квантово-механічної системи її вихідний стан змінюється. Тому не можливо достовірно розрізнити квантові стани з їх неортогональної набору. Саме ця властивість використовується в обґрунтуванні секретності квантової криптографії: при спробі підслухати передані стани з їх неортогональної набору перехоплювач неминуче вносить в них помилку, в результаті чого він може бути виявлений за додатковими перешкод на приймальній стороні.

Тому рішення про можливість секретного поширення ключів досягається легітимними користувачами на основі величини спостерігаються помилки на приймальній стороні: при наближенні значення цієї помилки до критичної величини (залежної від використовуваного протоколу) довжина секретного ключа в бітах прагне до нуля, і передача ключів стає неможливою.

Важливим результатом є знаходження точної величини критичної помилки для протоколу BB84, яка виявляється рівною приблизно 11%.

Експериментальна реалізація квантової криптографії натрапила на ряд технологічних труднощів, найбільш важливою з яких є складність генерації строго однофотонних квантових станів.

1 ОСНОВНІ ПОЛОЖЕННЯ КРИПТОГРАФІЇ

1.1 Задачі криптографії

Криптографія виникла як наука про методи шифрування, і довгий час саме шифрування залишалася єдиною проблемою, що вивчається криптографією.

Завдання передачі секретної інформації відома людству з давніх часів. З основних типів відомостей, для яких може бути важлива їх секретна передача, можна виділити наступні:

— важлива державна інформація;

— інформація, що містить військові секрети;

— комерційні дані;

— особиста конфіденційна інформація.

Результат великої кількості військових кампаній і фінансовий успіх багатьох корпорацій завжди був безпосередньо пов'язаний в тому числі з умінням передавати інформацію без її витоку до третіх осіб, що говорить про істотну цінності розвитку технологій секретної передачі даних.

Необхідність застосування криптографічних методів випливає з умов, в яких відбувається зберігання і обмін інформацією. В сучасних інформаційних системах дуже часто відбувається обмін даними в колективах, члени яких не довіряють один одному. Отже, метою застосування криптографічних методів є захист інформаційної системи від цілеспрямованих руйнівних впливів (атак) з боку противника.

Способи захисту істотно залежать від ситуації: від якого роду загрози необхідно захищатися, які можливості має противник.

Основні задачі криптографії:

— Забезпечення конфіденційності даних;

— Забезпечення цілісності даних

— Забезпечення аутентифікації.

— Забезпечення неможливості відмови від авторства

1.2 Основні технології передачі секретних даних

Можна виділити три основних технології передачі конфіденційної інформації:

1. Конструювання повністю секретного каналу зв'язку - цей метод виявляється найбільш складним, і його складність лише збільшується з розвитком технологій підслуховування.

2. Приховування самого факту передачі інформації. Цей метод отримав назву стенографії, і з тим або іншим успіхом використовувався в усі часи. З розширенням технологічного арсеналу застосування цього методу стає все простіше, однак з іншого боку у нього є істотні недоліки: так, важко забезпечити гарантії не потрапляння інформації третім особам, і при використанні одного і того ж способу стенографії протягом довгого часу велика ймовірність того, що передбачуваний перехоплювач також читає повідомлення, не виказуючи себе.

3. Відкрита передача повідомлення по відкритому каналу, але лише після спеціального перетворення — шифрування, мається на увазі неможливість отримання корисної інформації про повідомленні не повідомляючи певних даних — секретного ключа. Криптографія вивчає саме цей спосіб передачі секретної інформації [2].

1.3 Способи шифрування даних

Застосування шифрів почалося ще кілька тисячоліть тому [3], і за минулий час було винайдено величезну кількість технологій шифрування тій чи іншій мірі надійності. Розглянемо деякі найбільш відомі з найбільш ранніх способів захисту інформації.

Шифр «Сцітала».

Цей метод шифрування відомий ще з часів війни між Афінами і Спартою в V ст. до н.е. У ньому використовувалася спеціальна дощечка

круглої форми і певного радіуса, звана сціталой. На сціталу намотувалася стрічка, на якій (уздовж осі сцітали) писався текст. Потім стрічка розмотувалася і відправлялася одержувачу. Він, маючи в розпорядженні сціталу того ж радіуса, намотував на неї стрічку і читав повідомлення. А всім іншим повідомлення уявлялося лише нескладним набором символів, записаних в стовпчик.

Шифр Цезаря.

Цей спосіб шифрування полягає в тому, що кожна літера вихідного повідомлення замінюється третьою за рахунком буквою алфавіту, наступної за нею. Алфавіт в цьому випадку вважається циклічним, тобто за останній його буквою знову слід перша. Одержувач повідомлення може безпомилково відновити його вихідний текст, замінивши кожну букву третьої за рахунком до нього. Сам Цезар використовував зрушення на 3 позиції, в той час як більш загальна версія подібного шифру, званого шифром зсуву, може використовувати будь-яку величину зсуву: важливо лише, щоб її знали як відправник повідомлення, так і його одержувач.

Шифр заміни.

Цей спосіб шифрування є подальшим узагальненням шифру Цезаря: в ньому кожна буква замінюється на наступній за нею в алфавіті на деякому інтервалі, а буквою (або іншим символом), що виходить з вихідної з використанням спеціальної таблиці, відомої тільки передавальної і приймаючої сторони.

Відзначимо, що за сучасними мірками всі наведені методи шифрування можна назвати задовільними: при знанні самих методів шифрування їх дуже легко зламати. Для перших двох шифрів елементарно підібрати відповідно діаметр сцітали і величину зсуву, а в разі загального шифру заміни може допомогти знання статистики згадки різних букв мови, на якому відбувається спілкування [4].

1.4 Протоколи шифрування

Завдання передачі секретного повідомлення між двома абонентами — головне, але не єдине завдання криптографії. Існує ще ряд важливих завдань, близьких за технологіями їх вирішення. Узгоджені дії користувачів, що призводять до вирішення такого завдання, називаються криптографічним протоколом [5].

Протокол, розподілу ключів ставить собі за мету генерацію загального випадкового ключа між двома користувачами з умовою того, щоб він був відомий тільки їм і нікому іншому. Як буде показано в подальшому, наявність подібного ключа потрібної довжини практично означає можливість гарантовано секретної передачі даних. Таким чином, завдання генерації ключа можна вважати еквівалентної задачі передачі секретного повідомлення.

Протокол, підписання контракту, вирішує завдання, що виникає при підписанні угод віддаленими абонентами: два хто не довіряє один одному людини при підписанні контракту не хочуть допустити ситуацію, при якій один з абонентів отримав підпис іншого, а сам не підписався.

Протокол, аутентифікації працює з наступною задачею: при взаємодії двох осіб у кожного з них можуть виникнути побоювання, що їх співрозмовник — не той, за кого себе видає. Завдання аутентифікації полягає в тому, щоб переконати співрозмовника в своїй особистості.

Найбільш поширеною криптографічного завданням є пересилання секретних даних. Основних дійових осіб, що беруть участь в обміні інформацією, прийнято називати по іменах: зазвичай в книгах і статтях по криптографії передавальну сторону називають Алісою, приймаючу сторону - Бобом, а третю сторону яка, прагне перехопити повідомлення і отримати секретну інформацію — Євою.

2 ОСОБЛИВОСТІ КВАНТОВОЇ КРИПТОГРАФІЇ

2.1 Основні положення квантової криптографії

Квантова криптографія — це порівняно новий напрямок досліджень, що дозволяє застосовувати ефекти квантової фізики для створення секретних каналів передачі даних.

У квантової криптографії використовується фундаментальна особливість квантових систем [6], що полягає у принциповій неможливості точного детектування стану такої системи, яка приймає одне з набору декількох неортогональних станів. Це випливає з факту, що достовірно розрізнити подібні стану за один вимір не виходить. Наприклад, не можна визначити довжину відрізка в просторі тільки по його проекції на одну вісь, а більш одного виміру зробити неможливо, тому що після першого ж вимірювання система непередбачуваним чином змінює свій стан. Крім того, в квантовій механіці справедлива теорема про заборону точного клонування систем, що робить неможливим виготовлення декількох копій досліджуваної системи і подальше їх тестування.

Для початку розглянемо роботу ідеального квантового каналу, принцип дії якого передбачає, що приймально-передавальна апаратура і канали зв'язку ідеальні. В якості носіїв інформації в квантової криптографії, як правило, використовуються окремі фотони, або пов'язані фотонні пари. Значення «0» і «1» біт інформації кодуються різними напрямками поляризації фотонів. Для передачі сигналу відправник випадковим чином вибирає один з двох або в деяких схемах з трьох взаємно неортогональних базисів. При цьому однозначно правильне детектування сигналу можливо, якщо тільки одержувач правильно вгадав базис, в якому відправник підготував сигнал [7]. У разі якщо базис вгаданий невірно, результат вимірювання не визначений. На рис. 2.1 показано, що одержувач намагається детектувати сигнал 1_0 (квант, поляризований вздовж осі $Y_{\_0}$) в невірному базисі 1 (осі $X_{\_1}$, $Y_{\_1}$, повернені на 45°), в результаті він може отримати з однаковою ймовірністю

як «0», так і «1», тобто результат виміру повністю недостовірний.

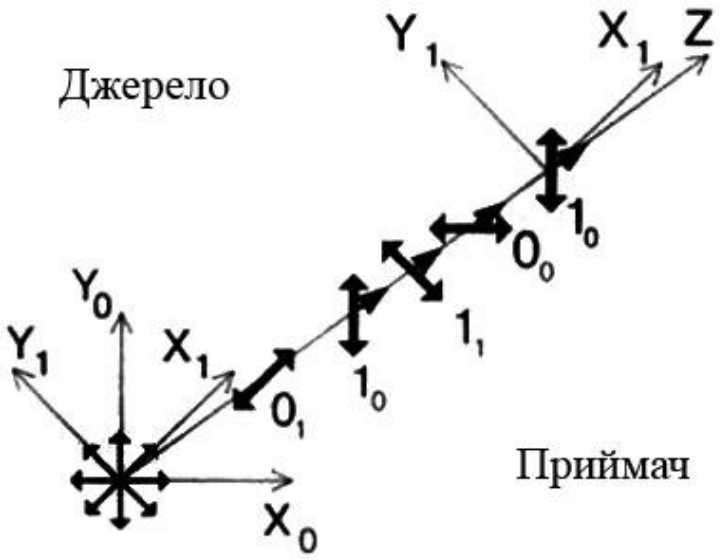

Рисунок 2.1 — Використання квантових ефектів
для секретної передачі даних

Оскільки відправник вибирає базис випадковим чином, одержувач неминуче буде помилятися у виборі базису детектування, і частина вимірювань виявиться невірною. Потім одержувач і відправник проводять обговорення результатів передачі з автентичного, але, можливо, несекретних каналу зв'язку. Що саме при цьому передається залежить від використаного квантового протоколу, але в будь-якому випадку зазначена інформація дозволяє кореспондентам виключити випадки, коли одержувач невірно вгадав базис, і не дає супротивникові жодних відомостей щодо правильно переданих даних.

Якщо противник спробує підслухати інформацію, передану через квантовий канал, то він, так само як і одержувач, буде неминуче помилятися у виборі базису. Оскільки квант, що несе інформацію, при детектуванні руйнується [7], противник випускає новий квант, поляризований тим чи іншим чином у використаному їм базисі. У певних випадках цей базис не

співпадатиме з тим, який використовувався, це призводить до спотворення даних. Наявність спотворень буде виявлено в ході порівнянні кореспондентами виробленого загального відрізка даних, і це буде означати спробу прослуховування.

Таким чином, системи квантової криптографії мають ряд принципових особливостей [8]:

— не можливо заздалегідь визначити, який з переданих бітів буде коректно прийнятий одержувачем;

— зниження швидкості передачі при використанні низькоенергетичних імпульсів .

Враховуючи особливості системи квантової криптографії, квантовий канал зв'язку малопридатний для передачі призначених для користувача даних, а більше підходить для вироблення ключа симетричного шифру, який буде використаний кореспондентами для шифрування даних, що передаються.

Базовим завданням криптографії є шифрування даних і аутентифікація відправника. Це легко виконати, якщо як відправник, так і одержувач мають псевдовипадкові послідовності біт, звані ключами.

Перед початком обміну кожен з учасників повинен отримати ключ, причому цю процедуру слід виконати з найвищим рівнем конфіденційності, так щоб жодна третя сторона не могла отримати доступ навіть до частини цієї інформації. Завдання безпечного пересилання ключів може бути вирішена за допомогою квантової розсилки ключів QKD (QuantumKeyDistribution).

Надійність методу будується на непорушності законів квантової механіки [6]. Зловмисник не може відвести частину сигналу з передавальної лінії, так як не можна поділити електромагнітний квант на частини. Будь-яка спроба зловмисника втрутитися в процес передачі викличе непомірно високий рівень помилок. Ступінь надійності в даній методиці вище, ніж в разі застосування алгоритмів з парними ключами (наприклад, RSA) [9]. Тут

ключ може генеруватися під час передачі по абсолютно відкритому оптичному каналу. Швидкість передачі даних при цій техніці не висока, але для передачі ключа вона і не потрібна. По суті квантова криптографія може замінити алгоритм Діффі-Хелмана, який в даний час часто використовується для пересилки секретних ключів шифрування по каналах зв'язку [10].

2.2 Протоколи квантового шифрування

У 1984 році були сформульовані принципи квантової криптографії і надані аргументи на користь секретності подібного способу розподілу ключів. Потім прийшов час для розвитку власне формалізму квантової криптографії: були описані необхідні дії легітимних користувачів, формалізовані дії перехоплювача, а також була доведена секретність першого протоколу квантового розподілу ключів, названого BB84 [3].

Основні факти квантової теорії інформації, на яких ґрунтується квантова криптографія — це пов'язані між собою твердження про неможливість копіювання довільних квантових станів і про неможливість достовірного розрізнення неортогональних станів. У поєднанні ці факти дають те, що попит розрізнення квантових станів з неортогональної набору, ведуть до перешкод, а значить, дії перехоплювача можуть бути детектованні за величиною помилки на приймальній стороні.

Важливо відзначити, що квантова криптографія не робить ніяких припущень про характер дій перехоплювача і обсязі доступних йому ресурсів. Це істотно відрізняє квантову криптографію від класичної, яка спирається на обмеження в обчислювальної потужності перехоплювача.

Неформально принцип дії всіх протоколів квантової криптографії можна описати так: відправник на кожному кроці посилає один зі станів з їх неортогональної набору, а одержувач виробляє такий вимір, що після додаткового обміну класичної інформацією між сторонами вони повинні мати бітові рядки, які повністю збігаються у разі ідеального каналу і

відсутності перехоплювача. Помилки ж у цих рядках можуть говорити як про не ідеальність каналу, так і про дії перехоплювача. При величині помилки, що перевищує певні межі, дія протоколу переривається, інакше легітимні користувачі можуть отримати повністю секретний ключ з їх (частково співпадаючих) бітових рядків.

На даний час існує багато протоколів квантової криптографії. Більшість з них засновані на передачі інформації за допомогою кодування в станах одиночних фотонів, наприклад: BB84, B92, BB84 (4+2), з шістьма станами, Гольденберга-Вайдмана, Коаші-Імото і їх модифікації [4]. Протокол E91 — розроблений для кодування інформації в переплутаних станах [11].

Розглянемо більш докладно існуючі протоколи квантового розподілу ключів.

2.2.1 Квантовий протокол BB84

Протокол BB84 [4] історично є першим протоколом квантового розподілу ключів, протоколом, безпека якого заснована на принципах квантової механіки, що робить його абсолютно безпечним за умови відсутності шуму в квантовому каналі зв’язку та використання таких станів частинок, які не допускають клонування. Спільне виконання цих двох умов будемо називати ідеальними умовами для протоколів КРК. Відсутність шуму в даному випадку означає, що квантові стани частинок не змінюються під час поширення квантовим каналом зв’язку. В класичній теорії інформації апріорі вважається, що повідомлення в принципі завжди можна підслухати та скопіювати без зміни бітів, що пересилаються. Однак, якщо інформацію зашифрувати в неортогональних квантових станах, таких, як, наприклад, стани поодиноких фотонів з поляризацією 0°, 45°, 90° та 135°, третя сторона принципово не зможе прочитати або скопіювати таку інформацію. Зловмисник не зможе отримати навіть часткову інформацію з повідомлення

без зміни його випадковим та неконтрольованим чином, що з великою імовірністю буде помічено користувачами каналу зв’язку.

Протокол BB84 формулюється на умові одиночних фотонів, хоча його легко узагальнити на будь-яку іншу реалізацію кубітів. Для кодування інформації в протоколі використовуються чотири поляризаційні стани фотонів [9], наприклад, напрямок вектору поляризації, однин з яких відправник вибирає в залежності від переданого біта: 90° або 135° для «1», 0° або 45° для «0» . Одна пара квантових станів відповідає 0(0(+)) та 1(1(+)) і належить базису «+». Інша пара квантових станів відповідає 0(0(x)) та 1(1(x)), належить базису «x».

Всередині обох базисів стани ортогональні, але стани з різних базисів є попарно неортогональними (неортогональність необхідна для детектування спроб підслуховування інформації). Квантові стани системи можнливо описати таким чином:

$$|0_\times\rangle = \frac{1}{\sqrt{2}}\left(|0_+\rangle + |1_+\rangle\right), \quad |1_\times\rangle = \frac{1}{\sqrt{2}}\left(|0_+\rangle - |1_+\rangle\right). \tag{2.1}$$

Стани $|0_+\rangle$ та $|1_+\rangle$ кодують значення «0» і «1» в базисі «+», а $|0_\times\rangle$ та $|1_\times\rangle$ кодують ті ж значення в базисі «×». Базиси повернені один відносно одного на 45° (рис. 2.2).

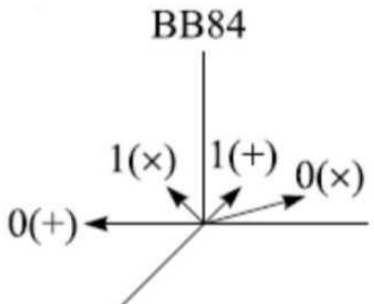

Рисунок 2.2 — Стани поляризації фотонів при використанні протоколу BB84

Етапи формування ключів:

1. Відправник випадково вибирає один з базисів. Після цього всередині базису випадково вибирає один зі станів, який відповідає «0» або «1» і відправляє фотони (рис. 2.3).

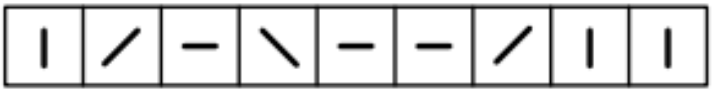

Рисунок 2.3 — Поляризація виправлених фотонів

2. Одержувач випадково і незалежно від відправника вибирає для кожного фотону: прямолінійний (+) або діагональний (×) базис (рис. 2.4 — 2.5).

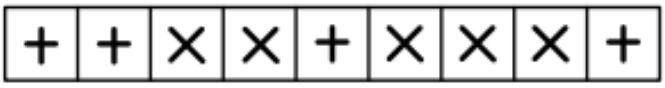

Рисунок 2.4 — Обраний базис для фотонів

Після цього одержувач зберігає результати вимірювань:

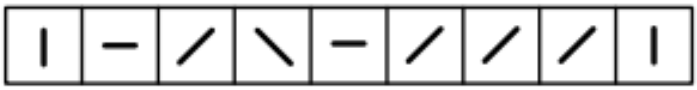

Рисунок 2.5 — Результати вимірювань

3. Одержувач по відкритому каналу зв'язку повідомляє, який тип вимірювань був використаний для кожного фотона, тобто який був обраний базис, але результати вимірювань не розголошуються.

4. Відправник повідомляє одержувачу по відкритому з каналу

зв'язку, які вимірювання були обрані відповідно до вихідного базису (рис. 2.6).

Рисунок 2.6 — Вихідний базис фотонів

5. Далі партнери залишають тільки ті випадки, в яких обрані базиси збіглися. Ці випадки переводять в біти (0 і 1), і отримують, таким чином, ключ (рис.2.7).

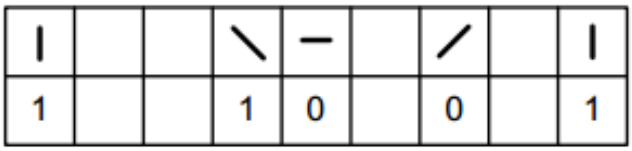

Рисунок 2.7 — Отриманий ключ за результатами вимірів

Число випадків, в яких обрані базиси збіглися, становитиме в середньому половину довжини вихідної послідовності, тобто $n = 1/2$ (приклад визначення кількості фотонів, прийнятих одержувачем, показаний в табл. 2.1).

Таблиця 2.1 — Формування квантового ключа за протоколом BB84

Двоїчний сигнал відправника	0	1	0	1
Поляризаційний код відправника	↔	↕	↘	↗
Детектування одержувача	✥	✥	✥	✥
Двоїчний сигнал одержувача	0	1	?	?

Отже, після передачі всіх станів і проведення вимірювань партнери мають по два рядки. Тут відбувається узгодження базисів: по відкритому

каналу партнери оголошують один одному свої рядки з вибором базисів, і вони викидають посилки, в яких їх базиси не співпали. Слід звернути увагу, що якщо базис, який використовується для посилки стану відправника, збігся з базисом виміру одержувача, то в разі відсутності перешкод в каналі зв'язку результати в їх бітових рядках на відповідній позиції збігатимуться, тому після етапу узгодження базисів в разі ідеального каналу і відсутності дій з боку перехоплювача партнери повинні володіти одними і тими ж бітовими рядками.

Однак, якщо в каналі були помилки або перехоплювач намагався підслухати інформацію, бітові рядки партнери можуть не збігатися, тому для перевірки вони повинні узгоджено розкрити приблизно половину своїх бітових рядків. Згідно центральної граничної теореми, помилка в розкритої бітової послідовності дає досить точну оцінку помилки у всій послідовності, і по ній можна досить точно оцінити ймовірність помилки в останніх позиціях. Якщо величина помилки виявляється більше деякої величини (параметра протоколу), передача даних припиняється: це означає, що перехоплювач має занадто великий інформацією про ключі. В іншому ж випадку перед партнерами стоїть завдання отримання загального секретного ключа.

Це завдання можна поділити на два етапи:

1) Корекція помилок;

2) Посиленням секретності

В результаті цих кроків у перехоплювача не повинно залишатися інформації про загальний бітовий рядок партнерів.

2.2.2 Квантовий протокол B92

У протоколі B92 [12] відправник посилає одержувачу фотони в одному з двох неортогональних станів ($|\varphi_0|$ і $|\varphi_1|$, $|\varphi_0\ \varphi_1| \neq 0$). Фотони, поляризовані вздовж напрямку +45°, несуть інформацію про одиничний біт, фотони, поляризовані вздовж напрямку 0°. Ці стани зображені графічно на рис. 2.8.

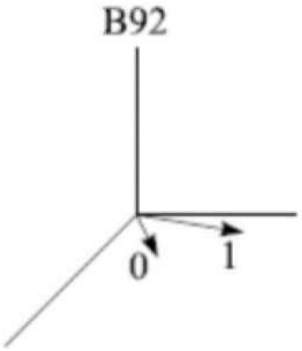

Рисунок 2.8 — Стани поляризації фотонів при використанні протоколу B92

Алгоритм роботи протоколу B92 (рис. 2.9).

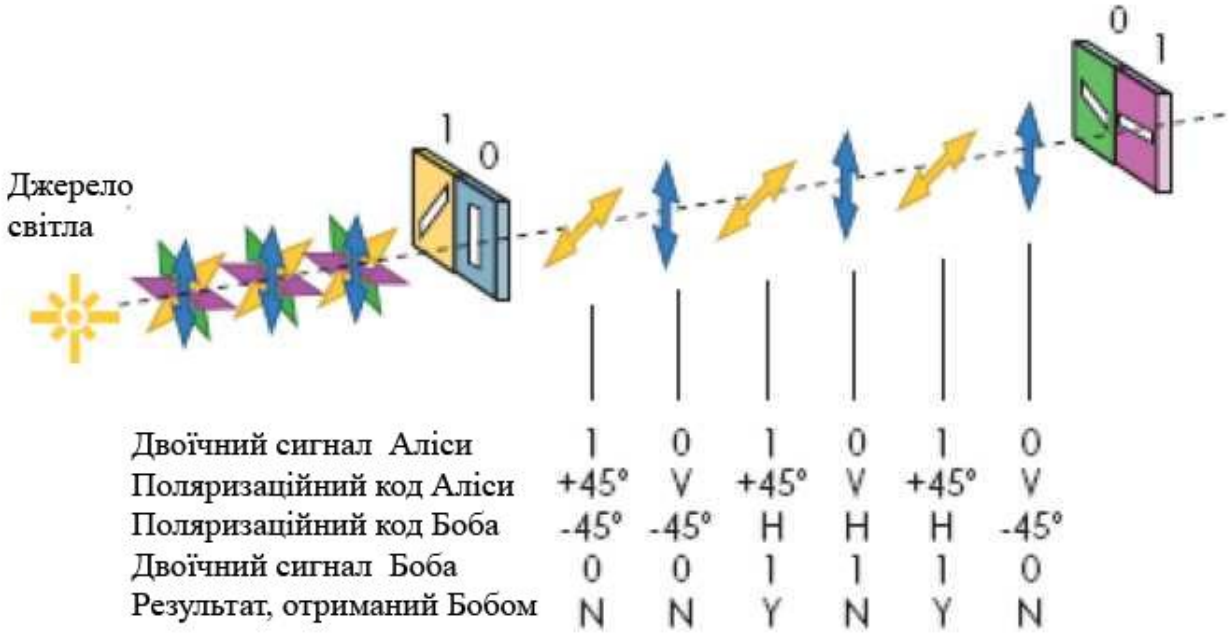

Рисунок 2.9 — Формування квантового ключа по протоколу B92

Відправник посилає фотони, поляризовані в напрямках 0 і 45°, що представляють нулі і одиниці. Причому послідовність фотонів, що посилається відправником, випадково орієнтована. Одержувач приймає фотони через фільтри орієнтовані під кутом 90° і 135° (– 45°). При цьому

якщо фотон, переданий відправником, буде проаналізоване одержувачем за допомогою фільтра орієнтованого під кутом 90° по відношенню до переданого фотону, то фотон не пройде через фільтр. Якщо ж цей кут складе 45°, то фотон пройде через фільтр з ймовірністю 0,5.

Для визначення поляризації одержувач аналізує прийняті нею фотони, використовуючи обраний випадковим чином один з двох неортогональних базисів «+» або «^». Якщо одержувач аналізує надісланий фотон фільтром з ортогональним напрямком поляризації, то він не може точно визначити, яке значення цей фотон представляє: 1, відповідне фотону, який не проходить, або 0, відповідне фотону, який не проходить з ймовірністю 0,5. Якщо ж напрямки поляризації між надісланим фотоном і фільтром, неортогональні, то одержувач може визначити, що прийнятий фотон відповідний «0». Якщо фотон був прийнятий вдало, то черговий біт ключа кодується «0» (якщо фотон був прийнятий фільтром, орієнтованим під кутом 135°), або «1» (якщо фотон був прийнятий фільтром, орієнтованим у напрямку Н) (таблиця 2.2)

Таблиця 2.2 Формування квантового ключа за протоколом B92

Двоїчний сигнал відправника	1	0	1	0
Поляризаційний код відправника	↗	↕	↗	↕
Поляризаційний код одержувача	↖↘	↖↘	↔	↔
Двоїчний сигнал одержувача	0	1	1	1
Результат, отриманий одержувачем	-	-	+	-

У 1 та 4 колонці поляризації при передачі і прийомі ортогональних, результат детектування буде відсутній. У колонках 2 і 3 коди двійкові розряди збігаються і поляризації не ортогональні. З цієї причини з імовірністю 50 % може бути позитивний результат в будь-якому з цих випадків (і навіть в обох). У таблиці передбачається, що успішне детектування фотона відбувається для випадку, представленого в колонці 3. Саме цей біт стає першим бітом загального секретного ключа передавача і

приймача. Звідси мінімальна кількість фотонів, яке може бути прийнятий одержувачем $n = 1/4$.

Тобто в результаті передачі такого ключа, близько 25 % фотонів будуть правильно детектовані одержувачем.

Після цього по відкритому каналу зв'язку одержувач може передати відправнику, які 25 фотонів з кожних 100 були нею отримані. Дана інформація і буде служити ключем до нового повідомлення. При цьому щоб зловмисник не дізнався інформацію про ключі, по відкритому каналу зв'язку можна передати інформацію тільки про те, які по порядку фотони були прийняті, не називаючи стану фільтрів і набутих значень поляризації. Після цього відправник може передавати повідомлення одержувачу зашифровані цим ключем.

Для виявлення факту знімання інформації в даному протоколі використовують контроль помилок, аналогічний контролю помилок в протоколі BB84. Тобто, станції партнери звіряють випадково вибрані біти ключа. Якщо виявляються розбіжності, то можна говорити про несанкціоноване знімання інформації.

2.2.3 Протокол з шістьма станами

Початково представляє протокол BB84, але ще з одним базисом, а саме:

$$|0_C\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right), \quad |1_C\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right). \qquad 2.2)$$

Відповідно до цього, існує ще два можливих напрямки поляризації для переданого фотона: правоциркулярний і лівоциркулярний.

Таким чином, можна порахувати кількість фотонів, які будуть прийняті одержувачем. (таблиця 2.3)

Таблиця 2.3 — Формування квантового ключа по протоколу з шістьма станами

Двоїчний сигнал відправника	1	0	1	0	1	0
Поляризаційний код відправника	↗	↕	↔	↘	↶	↷
Детектування одержувачем	✣	✣	✣	✣	✣	✣
Двоїчний сигнал одержувача	?	0	1	?	?	?

З таблиці видно, що мінімальна кількість фотонів, яка буде прийнята одержувачем при детектуванні n = 2/6= 1/3. Тобто при використанні протоколу з шістьма станами [4] буде прийнято близько 33 % фотонів, які посилаються відправником.

2.2.4 Квантовий протокол BB84(4+2)

Протокол BB84(4+2) [4] є проміжним між протоколами BB84 і B92. У протоколі використовуються чотири квантових стани для кодування «0» і «1» у двох базисах. Стани в кожному базисі вибираються неортогональні, стани в різних базисах також попарно неортогональні. Це зручно представити графічно (рис. 2.10).

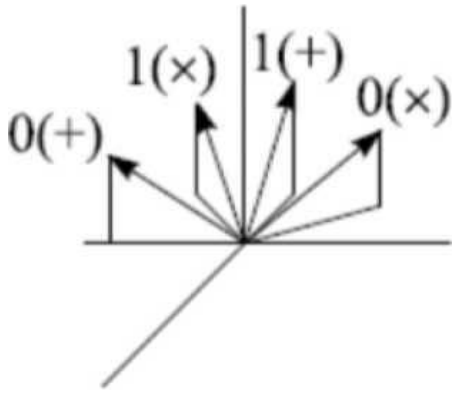

Рисунок 2.10 — Стани поляризації фотонів при використанні протоколу BB84 (4 + 2)

Протокол реалізується в такий спосіб. Відправник випадковим чином вибирає один з базисів. Усередині базису також випадковим чином вибираються стани «0» або «1», потім вони направляються в квантовий канал зв'язку. Одержувач незалежно вибирає вимірювання двох типів (в різних базисах). Потім, після передачі досить довгої послідовності користувачі через відкритий канал зв'язку повідомляють, який базис був використаний в кожній посилці. Посилки, в яких базиси не збігалися, відкидаються. Для решти посилок одержувач публічно відкриває номера тих посилок, де у нього були невизначені результати (такі посилки теж відкидаються). З решти посилок (з певним результатом) витягується секретний ключ шляхом процедури корекції помилок через відкритий канал і посилення секретності. Підрахунок кількості фотонів, прийнятих одержувачем, представлений в таблиці 2.4.

Таблиця 2.4 — Формування квантового ключа по протоколу

Двоїчний сигнал відправника	0	1	0	1	0	1	0	1
Поляризаційний код відправника	↔	↕	↘	↙	↔	↕	↘	↙
Детектування одержувача	⇵	⇵	⇵	⇵	⇆	⇆	⇆	⇆
Двоїчний сигнал одержувача	0	?	?	1	0	?	?	1

Таким чином, в результаті передачі ключа одержувачем будуть отримані 50 % фотонів, тобто $n = 1 / 2$.

2.2.5 Протокол Гольденберга-Вайдмана

Протокол Гольденберга-Вайдмана [4] оснований на використанні двох ортогональних станів.

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle + |b\rangle\right), \quad |\Psi_1\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle - |b\rangle\right). \tag{2.3}$$

Кодуючі відповідно біти «0» і «1».

Кожен з цих двох станів | φ_0 | і | φ_1 | є суперпозицією двох локалізованих нормалізованих хвильових пакетів |a| і |b|. відправник посилає пакети одержувачу по двох каналах різної довжини. В результаті цього хвильові пакети виявляються у одержувача в різні моменти часу. Хвильовий пакет |b| залишає відправника тільки після того, як хвильової пакет |a| вже досяг одержувача. Для цього можна використовувати інтерферометр з різною довжиною плечей. Одержувач затримує свій вимір до того моменту, як обидва хвильових пакета досягнуть його. Якщо час посилки |a| пакета відомо перехоплювача, то вона здатна перехопити інформацію, послявши одержувача в відповідний момент часу пакет, ідентичний з пакетом |a|, вимірявши потім надісланий відправником суперпозіційний стан і далі послявши одержувачу хвильовий пакет |b| з фазою, налаштованою відповідно до результату її вимірювань. Щоб попередити цю атаку, використовуються випадкові часи посилки.

2.2.6 Протокол Коаши-Імото

Даний протокол [4] є модифікацією протоколу Гольденберга-Вайдмана, але дозволяє відмовитися від випадкової передачі шляхом асимметризації інтерферометра, тобто розбиття світла в нерівній пропорції між коротким і довгим плечима. Крім того, різниця фаз між двома плечима інтерферометра становить π. Таким чином, два стани що кодують біти «0» і «1», визначаються відбивною R і пропускною T здібностями вхідного роздільник променів:

$$\left|\Psi_0\right\rangle = -i\sqrt{R}\left|a\right\rangle + \sqrt{T}\left|b\right\rangle, \quad \left|\Psi_1\right\rangle = \sqrt{R}\left|a\right\rangle - i\sqrt{T}\left|b\right\rangle. \tag{2.4}$$

У разі асиметричної схеми, коли амплітуда ймовірності знаходження фотона в тому чи іншому плечі інтерферометра залежить від значення

переданого біта, компенсація за рахунок фази не спрацьовує повністю. Тому при застосуванні перехоплювачем вказаної тактики існує ненульова ймовірність помилки детектування.

Виконуючи порівняльний аналіз наведених вище протоколів, з розрахунку кількості прийнятих фотонів, можна визначити, що найбільш ефективним є BB84. Подальші його модифікації спрямовані на зменшення відсотка помилок і кількості корисної інформації, яку теоретично може отримати зловмисник. Альтернативою у розвитку протоколу BB84 є протокол B92. Перевагою протоколу B92 є використання фотонів з двома типами поляризації (замість чотирьох) — це дозволяє спростити схему реалізації, однак зменшує ефективність (зменшується кількість прийнятих фотонів), і гарантовану секретність ключа тільки на відстані до 20 км, тоді як BB84 — на відстані до 50 км. Протокол BB84 застосовується в комерційних системах розподілу ключів.

2.2.7 Протокол E91 (EPR)

Протокол E91(EPR) заснований на парадоксі Ейнштейна–Подольського–Розена, був запропонований А. Екертом в 1991 році. У протоколі пропонується використовувати, пари фотонів, які утворюються в антисиметричних поляризаційних станах. Захоплення одного з фотонів пари не приносить Єві ніякої інформації, але дає можливість партнерам зафіксувати, що їх розмову підслуховують.

Ефект EPR виникає, у випадку коли сферичний симетричний атом випромінює два фотона з протилежних напрямків в сторону двох спостерігачів. Фотони випромінюються з невизначеною поляризацією, але в силу симетрії їх поляризації завжди протилежні. Важливою особливістю цього ефекту є те, що поляризація фотонів стає відомою тільки після вимірювання. На основі EPR був запропонований протокол, який гарантує безпеку пересилання і зберігання ключа. Відправник генерує кілька EPR

фотонних пар, один фотон з кожної пари він зберігає у себе, другий відправляє до отримувача. При цьому, якщо ефективність реєстрації близька до одиниці, при отриманні відправником значення поляризації 1, отримувач зареєструє значення 0 і навпаки. Ясно, що таким чином партнери щоразу, коли потрібно, можуть отримати ідентичні псевдовипадкові кодові послідовності.

Спочатку створюється максимальна кількість заплутаних EPR-пар фотонів, потім один фотон з кожної пари відправляється кожному з партнерів. Три можливих квантових стани для цих EPR-пар можливо визначити а формулами:

$$\left|\Psi_1\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|\frac{3\pi}{6}\right\rangle_B-\left|\frac{3\pi}{6}\right\rangle_A\left|0\right\rangle_B\right), \tag{2.5}$$

$$\left|\Psi_2\right\rangle=\frac{1}{\sqrt{2}}\left(\left|\frac{\pi}{6}\right\rangle_A\left|\frac{4\pi}{6}\right\rangle_B-\left|\frac{4\pi}{6}\right\rangle_A\left|\frac{\pi}{6}\right\rangle_B\right), \tag{2.6}$$

$$\left|\Psi_3\right\rangle=\frac{1}{\sqrt{2}}\left(\left|\frac{2\pi}{6}\right\rangle_A\left|\frac{5\pi}{6}\right\rangle_B-\left|\frac{5\pi}{6}\right\rangle_A\left|\frac{2\pi}{6}\right\rangle_B\right). \tag{2.7}$$

Загальний вигляд форми:

$$\left|\Psi_i\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|1_i\right\rangle_B-\left|1_i\right\rangle_A\left|0_i\right\rangle_B\right). \tag{2.8}$$

Формула 2.7 явно показує, що кожний з трьох станів кодує біти «0» і «1» в унікальному базисі. Потім партнери здійснюють вимірювання на своїх частинах розділених EPR-пар, застосовуючи відповідні проектори:

$$P_1=\left|0\right\rangle\left\langle 0\right|,\qquad P_2=\left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|,\qquad P_3=\left|\frac{3\pi}{6}\right\rangle\left\langle\frac{3\pi}{6}\right|. \tag{2.9}$$

Відправник записує виміряні біти, а одержувач записує їх доповнення до результатів вимірювань, в яких користувачі вибрали однакові базиси, формують сирий ключ. Для інших результатів партнери проводять перевірку виконання нерівності Белла як тест на присутність порушника.

Експериментальна реалізація даного протоколу розпочалася нещодавно. Проведення таких експериментів стало важливим отримання джерел переплутаних пар з високим ступенем кореляції і тривалим часом життя.

2.3 Проблеми квантової криптографії

При створенні практичних криптосистем, заснованих на квантовому розподілі ключа, доводиться стикатися з такими проблемами:

— низька швидкість передачі даних;

— передача даних здійснюється тільки на невеликі відстані;

— неможливо створити квантові повторювачі;

— інтенсивність квантових імпульсів;

— атаки зловмисників на квантовий канал змінює саме повідомлення.

Якщо квантів в імпульсі 1000, то є ймовірність того, що 100 квантів по шляху каналу буде відведено незаконному користувачеві на свій приймач. Тим самим, зловмисник може отримати потрібну йому інформацію, аналізуючи пізніше відкриті переговори між одержувачем і відправником. Будь-яка спроба відводу частини квантом незаконним користувачем призведе до істотного зростання помилок, в цьому випадку необхідна повторна передача повідомлення.

Незважаючи на дані проблеми, дуже великі і успіхи в цій сфері. Практичні роботи в галузі квантової криптології ведуть такі відомі компанії як IBM, Toshiba, GAP-Optique і інші. Створено також комерційна квантова криптосистема id 3000 Clavius Quantum Key Distribution System, яка

підтримує безпечний обмін ключами на відстані до 100 км, підтримує протокол BB84 і інше.

2.4 Недоліки квантової криптографії

На даний час основним недоліком квантової криптографії є потреба у тому щоб секретний ключ був випадковим. Довжина ключа не повинна бути меншою за довжину повідомлення, це обумовлено одноразовим використанням ключа.

Проблема передачі ключів через комунікаційний канал, який іноді називають розподілом ключів є проблемою, яка потребує окремого обговорення. Для досягнення конфіденційності ключа під час спілкування, сам ключ слід розглядати як повідомлення яке зашифроване за допомогою іншого набору ключів. Це звичайно призводить до проблеми спілкування, появи другого набору ключі. Це не викликає надії на розумне вирішення проблеми розподілу ключів шляхом існуючих методів шифрування повідомлень та розшифровки.

В даний час широко використовуються криптографічні системи які гібридні за своєю природою — частково симетричні, а частково асиметричні. Частина повідомлення зашифрована за допомогою одного ключа, і цей ключ передається через шифрування-дешифрування асиметричною системою. З двох клавіш в асиметричній системі одна — це відкритий ключ, що використовується для шифрування оригінального повідомлення, а другий — це закритий ключ, який використовується для розшифровки. Приватний ключ ніколи не передається і тому цей спосіб розподілу ключів цілком безпечний.

У будь-якій операційній системі довжина ключа вибирається так щоб він був доступний достатній запас часу.

Поява концепції квантових комп'ютерів і прогрес у реалізації такого комп’ютера обіцяє наявність величезної обчислювальної потужності та подальшого розвитку у шифруванні ключа.

Одночасний прогрес відбувається у криптоаналізі. Криптоаналіз — наука про розрив шифру. Петро Шор лабораторії Белл запатентував алгоритм для вирішення досі категоризованих як важкі проблеми розкладання на множники та дискретний логарифм у поліноміальному часі за допомогою квантових комп’ютерів. В результаті присутній асиметрії криптографічні системи не зможуть забезпечити належної безпеки в найближчому майбутньому. Люди вивчають абсолютно різні галузі технологій у пошуку безпечної системи розподілу ключів.

Однак та сама квантова теорія, яка обіцяє швидкість в квантових комп'ютерах, забезпечує альтернативний підхід для абсолютної безпеки. Квантові біти або qbits або Qubits, як воліють називати це деякі автори, є одним із таких технологія з обіцянками на майбутнє.

Для кубітів зручно використовувати атоми з неспареним електроном на зовнішній орбіті, де можливі надтонкі (hyperfine) енергетичні переходи (ті ж самі, що використовуються в атомних годинниках). Найбільш зручні тут атоми цезію, літію або рубідію.

Однак створити масив таких атомів-кубітів, привести їх все в потрібний стан і утримати в ньому — непроста технологічна задача.

Перш за все необхідно позбутися від зайвого тепла, оскільки тепловий шум не дозволить контролювати стану атомів. Для того щоб довести кубіти до температури, близької до абсолютного нуля, використовується лазерне охолодження, тобто опромінення лазером певної довжини хвилі, який змушує атоми поглинати і випускати фотони, що впливає на їх момент і, отже, на температуру.

Друга проблема — утримати атоми на місці. Вчені підвішують їх у оптичних пастках, які представляють собою серії перехресних лазерних променів, на перетині яких утворюються стоячі електромагнітні хвилі.

В даний час в різних країнах розробляються десятки різних типів квантових обчислювальних пристроїв, заснованих на різних типах кубітів, призначених для вирішення різних типів завдань.

Однак говорити про початок квантової ери в обчислювальній техніці можна буде не раніше, ніж квантові комп'ютери покажуть свою перевагу над звичайними комп'ютерами в рішенні будь-яких завдань, тобто продемонструють квантову «надбавку» в швидкості обчислень — квантову перевагу.

Поки жодна квантова обчислювальна машина не показала абсолютного квантового переваги.

Завдання безпечного обміну нині вирішується за допомогою квантового розподілу ключа (Quantum Key Distribution) [12].

Метод квантового розподілу ключа полягає в передачі окремих бітів коду за допомогою квантового стану фотона [14]. Надійність квантового розподілу ключа обумовлена фундаментальними законами квантової механіки, за якими навіть частина сигналу не можливо вилучити з лінії зв’язку, це обумовлено не можливістю поділу фотона на частини, а безпосередня інтеграція в лінію передач є не можливою

2.5 Тенденції розвитку квантової криптографії

У квантовій криптографії виділяють три потенціальних напрямки розвитку систем розподілу ключів [14].

1. Базується на принципі неможливості фактично розрізнити два неортогональних квантових станів одного фотону.

2. Засноване на ефекті «переплутаних станів» [14].

3. Засноване на збереженні квантового стану.

Квантова криптографія тільки наближається до повноцінного практичного застосування. До розробки нових технологій квантової криптографії підключились не тільки найбільші всесвітньо відомі інститути, а й приватні компанії, які тільки розпочинають свою діяльність. Зацікавленість одночасно всесвітньо відомих інститутів та приватних компаній свідчить про те, що ринок квантових криптографічних систем знаходиться на стадії формування.

У літературі відсутній опис впливу параметрів функціональних вузлів на характеристики ефективності системної квантової криптографії [13]. Тісним способом з цією проблемою пов'язана відсутність загально-признанних методик дослідження (зміни) параметрів системи квантового розподілу ключів у цілому, а також усіх функціональних вузлів, що знаходяться в складі системи.

Слабо вивчений вплив не ідеальності характеристик компонентів на умовах несанкціонованого зчитування інформації. Для виключення можливостей несанкціонованого доступу в системах, що працюють на одночасних станах, вимагається розробити промислові образи однофотонних джерел виведення. Для реалізації системи, працюючих на сплутаних станах, необхідне створення джерел оптичного вилучення нового класу, що дозволяють формувати сплутанні фотонні пари.

Квантова криптографія — є дуже перспективною наукою, це обумовлено рівнем технологій, котрі в ній застосовуються. Квантова криптографія повинна забезпечити високий рівень захисту інформації, такий рівень захисту є дуже важливим для великих корпорацій та державних структур.

3 РЕАЛІЗАЦІЯ КВАНТОВОГО ШИФРУВАННЯ

3.1 Фізична реалізація системи квантової криптографії

Фінальним продуктом будь-якої системи квантової криптографії є секретні ключі. Для реального застосування їх секретність повинна бути строго доведена. Оскільки система квантової криптографії є розподіленим пристроєм, то крім атак під час передачі фотонів по лінії зв'язку, можливі атаки активного зондування по лінії зв'язку на прийомну і передавальну апаратури, до яких перехоплювач не має прямого доступу (наприклад, можуть зчитуватися стани фазових модуляторів, що дає однозначну інформацію про переданий стан). Таким чином, секретність ключів досягається, як вибором квантового протоколу, так і технічною реалізацією системи, тобто протокол повинен забезпечувати секретність ключів при атаках на квантовий канал зв'язку — без прямого і непрямого доступу до передавальної і приймальної апаратури. З іншого боку, система квантової криптографії повинна забезпечувати захист і від атак на апаратуру через канал. Відзначимо, що багато відомих системи уразливі при атаках активного зондування [14].

Розглянемо схему фізичної реалізації квантової криптографії [5] (рис. 3.1)

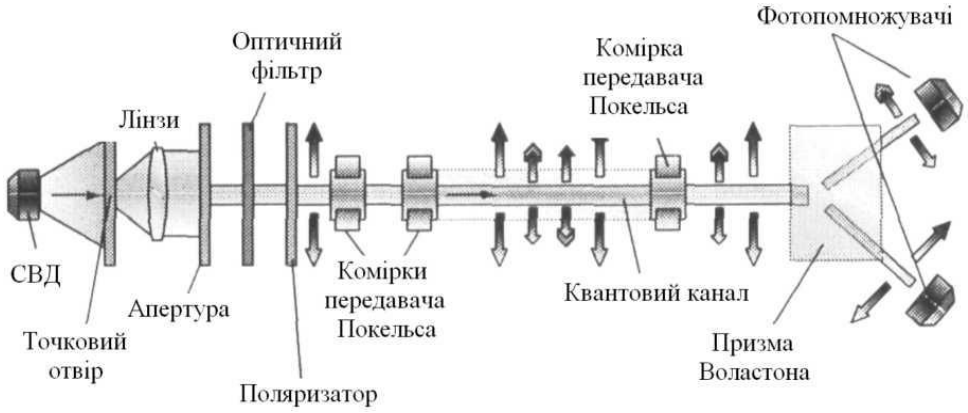

Рисунок 3.1 — Схема структурна: «Фізична реалізація квантової криптографії»

Використання комірок Поккельса дало можливість відправнику імпульсно варіювати поляризацію фотонів, а одержувачу аналізувати імпульси поляризації. Відправник зазвичай формує один із чотирьох станів поляризації.

На комірки дані надходять у вигляді керуючих сигналів. У якості каналу зв'язку прийнято використовувати оптоволокно, а джерелом світла виступає лазер. Між одержувачем і коміркою Поккельса розташована кальцитова призма, яка дозволяє розділити пучок випромінювання на дві складові, що в свою чергу забезпечує більш точне вимірювання ортогональні складові поляризації.

Першою при формуванні імпульсів виникає проблема вирішення інтенсивності переданих імпульсів фотонів. Якщо в імпульсі міститься 1000 фотонів, то існує ймовірність того, що 100 з них будуть перехоплені. Аналізуючи цей факт, збільшується вірогідність, що на відкритих переговорах перехоплювач зможе отримати всі необхідні йому дані. Тому зазначимо, що ідеальним варіантом передачі буде та передача в котрій кількість фотонів прагне до одного.

Кожна спроба перехоплення фотонів неминуче змінює стан всієї системи, цей факт сприяє збільшенню кількості помилок в одержувача.

У разі збільшенні детектованих помилок у прийнятих даних слід не враховувати цю передачу, а повторити передачу заново. Однак, при спробах зробити канал більш достовірним, чутливість приймача збільшується до максимуму, цей факт сприяє появлені «темнового» шуму. Це означає, що одержувач приймає вже спотворений сигнал. Для підвищення надійності передачі даних, логічні «0» та «1», представляються у вигляді послідовності станів, це дозволяє виправляти одинарні і навіть кратні помилки.

Для збільшення стійкості квантової криптосистеми використовується ефект Ейнштейна-Подільського-Розена, який виникає, якщо сферичним атомом буде випромінені фотони у двох протилежних напрямках. Початкова поляризація фотонів є не визначеною, але в силу симетрії їх поляризації

завжди протилежні. Базуючись на квантовій невизначеності можно стверджувати, що поляризацію фотонів можливо визначити лише після вимірювання [15]. Відправником генерується кілька фотонних пар, після чого один фотон з кожної пари він залишає у себе, а другий комплект відправляє одержувачу. Якщо ефективність реєстрації близька до одиниці і у відправника зберігається фотон з поляризацією «1», то у одержувача буде фотон з поляризацією «0» і навпаки. Тобто партнери завжди мають можливість отримати однакові псевдовипадкові послідовності. Але практичні дослідження виявили, що ефективність реєстрації і вимірювання поляризації фотона дуже мала.

3.2 Практична реалізація системи квантової криптографії

На даний час дослідження щодо безпечної прямої передачі повідомлень (без шифрування) за допомогою квантових систем стають все більш активними, однак така технологія ще не досягла потрібного ступеня надійності, необхідної для її практичного застосування. Тому питання про заміну існуючих мереж передачі даних на захищені квантові мережі поки не варто.

Так, запропоновані квантові протоколи прямого зв'язку, з одного боку, не володіють необхідним рівнем стійкості проти деяких видів атак, а з іншого боку, ці протоколи взагалі не можуть бути реалізовані практично, або реалізуються з неприйнятно низькою швидкістю передачі кубітів.

Однак технологія квантового розподілу ключів, в разі, якщо не потрібна висока швидкість їх генерації, вже зараз може бути інтегрована в існуючу інфраструктуру мереж передачі даних. Так, більшість віртуальних приватних мереж, широко поширених у всьому світі, використовують захищений протокол IPSec, що вимагає шифрування всього потоку обміну даними на рівні IP. Ключі для такого шифрування можна розподілити по окремій квантової мережі.

З 2002 року американською компанією BBN Technologies у співпраці з Гарвардським і Бостонським університетами виконується п'ятирічний проект, метою якого є розробка Відзначимо, що цей проект фінансується американським оборонним агентством DARPA (Defense Advanced Research Projects Agency). До теперішнього часу вже створена експериментальна квантова мережа між зазначеними вище організаціями (максимальна відстань між якими 19,6 км), що складається з десяти вузлів квантового розподілу ключів. При передачі ключа по протоколам BB84 і B92 між BBN Technologies і Гарвардським університетом (близько 10 км) досягнутий мінімальний рівень помилок в 3%. Відзначимо, що це значно менше тих 25 %, які вніс би перехоплювач при стратегії перехоплення всіх пересилаються фотонів в протоколі BB84. Таким чином, захищений проти атаки повного перехоплення протокол BB84 вже реалізований практично. Однак швидкість передачі невисока — близько 1000 біт/с, що обумовлено в першу чергу недосконалістю випромінювачів і детекторів фотонів. Проте, технологічне обладнання для систем квантової криптографії постійно вдосконалюється, тому інтегровані мережі, мабуть, вже близькі до впровадження в комерційну експлуатацію.

Активні дослідження в галузі систем квантової криптографії ведуть IBM, GAP-Optique, Mitsubishi, Toshiba, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут, приватна компанія MagiQ і холдинг QinetiQ. Зокрема, в національній лабораторії Лос-Аламоса була розроблена і почала широко використовуватися для досліджень лінія зв'язку, довжиною близько 48 км.

ВИСНОВКИ

Квантова криптографія — є надійним методом забезпечення конфіденційності і безпеки передачі інформації. Цей факт обумовлений використанням принципів квантової фізики. Спроба зчитування та вимірювання параметрів в квантовій системі неминуче вносить помилки, вихідний сигнал руйнується, отже, за рівнем шуму та кількістю помилок в каналі користувачі можуть розпізнати ступінь активності перехоплювача.

В якості носіїв інформації у системах квантової інформації використовуються одиночні фотони. На даний час джерела одиночних фотонів дозволяють генерувати фотони у будь-якому діапазоні довжин хвиль, але джерела випромінювання мають свої недоліки. Основною проблемою при використанні джерела одиночних фотонів є підтримка постійного температурного режиму під час роботи та ймовірність того, що одночасно джерело може згенерувати декілька фотонів

Основні проблеми квантової криптографії:

— проблема таємності;

— підслуховування;

— можливості перехоплення і дешифрування повідомлень.

Квантова криптографія — є дуже перспективною наукою, це обумовлено рівнем технологій, котрі в ній застосовуються. Квантова криптографія повинна забезпечити високий рівень захисту інформації, такий рівень захисту є дуже важливим для великих корпорацій та державних структур.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Wiesner S. Conjugate coding. // Sigact News. 1983. № 15. P. 78—88.

2. Основы современной криптографии. 3-е изд. / Баричев С. Г., Гончаров В. В., Серов Р. Е. Москва: Диалог-МИФИ, 2011. 176 с.

3. История криптографии. Часть I. / Бабаш А.В., Шанкин Г.П., Москва: Гелиос АРВ, 2002. 240 с.

4. Квантовая криптография: принципы, протоколы, системы. / Голубчиков Д. М., Румянцев К. Е. // Таганрогский технологический институт Южного федерального университета Таганрог: ТТИ ЮФУ, 2008. 37 с.

5. Криптографические методы защиты информации / Т. В. Кузьминов. Новосибирск: Наука. 1997. С. 44.

6. Квантовая теория / Д. Бом. Москва: Физматлит, 1965. С. 732.

7. Запутанные квантовые состояния атомных систем / И. В. Баргатин, Б. А. Гришанин, В. Н. Задков // УФН. 2001. Т. 171, № 6. С. 625.

8. Квантовая информация / С. Я. Килин // УФН. 1999. Т. 169. С. 507.

9. Quantum cryptography with entangled photons / T. Jennewein, C. Simon, G. Weihs et al. // Phys. Rev. Lett. 2000. Vol. 84. P. 4729 — 4732.

10. Оптическая когерентность и статистика фотонов / Р. Глаубер // Квантовая оптика и квантовая радиофизика, под ред. О. В. Богданкевича, О. Н. Крохина. Москва: Мир, 1966.

11. Quantum cryptography with coherent states / B. Huttner, N. Imoto, N. Gisin, T. Mor // Phys.Rev.A. 1995. Vol. 51. P. 1863.

12. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack / N. LËutkenhaus, M. Jahma // New J. Phys. 2002. Vol. 4. P. 44.

13. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в опто-волоконные телекоммуникационные системы / С. Н. Молотков // Письма в ЖЭТФ. 2004. Т. 79. С. 691—704.

14. Quantum key distribution with high loss: Toward global secure communication / W.-Y. Hwang // Phys. Rev. Lett. 2003. Vol. 91. P. 057901.

15 Физико-математические основы измерений в нелинейных динамических системах / Ю. П. Мачехин, Ю. С. Курской, А. С. Гнатенко // Радиотехника. 2018. № Вып. 192. С. 102—105.

16. Методичні рекомендації та вимоги щодо оформлення пояснювальної записки атестаційної роботи / Упоряд.: О.С. Гнатенко, А.І. Крючков, Н.М. Чернишова. Харків: ХНУРЕ, 2018. 44 с.