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)

КОДУВАННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ФЕМТОСЕКУНДНИХ ЛАЗЕРІВ
(тема)

Виконала:
студентка 2 курсу, групи ЛОЕТм-18-1
Сівні В.Б
(прізвище, ініціали)

Спеціальності 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)

2019 р.

Харківський національний університет радіоелектроніки

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

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____20___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Сівні Валерії Богдановні
(прізвище, ім'я, по батькові)

1. Тема роботи Кодування інформації за допомогою фемтосекундних лазерів

затверджена наказом по університету від "30 "жовтня 2019 р. № 1576 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 18.12.2019 р.
3. Вихідні дані до роботи Оптичний діапозон передачі інформації. Постійна Больцмана, температура переходу скла в тверду фазу, коефіцієнт стисливості, показник заломлення серцевини волокна, довжина хвилі.

4. Перелік питань, що потрібно опрацювати в роботі 1. Фізичні основи квантового кодування. 2. Основні напрямки розвитку квантової криптографії. 3. Методи квантового кодування. 4. Типові структури квантових систем розподілу ключів. 5. Кодування інформації за допомогою фемтосекундного лазера. 6. Розрахунок загасання випромінювання в волокні і відкритих системах.

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

Схема оптична структурна система з поляризаційним кодування– А4 – 1шт.

Схема оптична структурна квантовий розподіл ключів на переплутаних фотонах– А4 – 1 шт.

Демонстраційний матеріал – 11 шт.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Інформаційно-тематичний пошук інформації о кодуванні	04.11.19 –14.11.19	Виконано
2	Порівняння характеристик кодування інформації	15.11.19 – 17.11.19	Виконано
3	Розробка та моделювання оптичної схеми фемтосекудного лазера	18.11.19 – 22.11.19	Виконано
4	Розрахунок загасання випромінювання в волокні і відкритих системах	23.11.19 – 30.11.19	Виконано
5	Оформлення пояснювальної записки	01.12.19 – 07.12.19	Виконано
6	Оформлення графічної та демонстраційної частин	08.12.19 – 11.12.19	Виконано
7	Проходження нормоконтролю та отримання рецензії на роботу	12.12.19 – 16.12.19	Виконано
8	Підготовка та захист атестаційної роботи	17.12.19 – 19.12.19	

Дата видачі завдання 03 листопада 2019р.

Студент _____
(підпис)

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

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 67 с., 19 рис., 2 табл., 2 додатки, 19 джерел.

КВАНТОВІ СИСТЕМИ ЗВ'ЯЗКУ, ФЕМТОСЕКУНДНИЙ ЛАЗЕР, ПОЛЯРИЗАЦІЯ, КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ, ВОЛОКНО, ОДНОФОТОННИЙ СИГНАЛ, КОЕФІЦІЄНТ ЗГАСАННЯ.

Об'єкт дослідження – кодування інформації за допомогою фемтосекундного лазеру.

Мета роботи – розвиток оптичних методів кодування інформації. та дослідження принципів оптичного кодування інформації і можливість застосування фемтосекундних лазерів в оптичному кодуванні.

Метод дослідження – теоретичний з використанням електронно обчислювальних машин .

У першій частині роботи розглянуто історію квантової криптографії та перший пристрій квантової криптографії. Елементи теорії інформації(теорема Шеннона-Котельникова). Основні напрямки розвитку квантової криптографії. Описано протокол BB84.

У другій частині роботи розглянуто методи квантового кодування,а також структури систем з полярізаційним, фазовим, часовим кодуванням. Приведенно установки з використанням фемтосекундного лазеру.

У третій частині роботи розглянуто можливості застосування фемтосекундний лазер. Використання фемтосекундного лазера та розраховано загасання випромінювання в волокні і відкритих системах.

ABSTRACT

Explanatory note of the performance appraisal: 67 pp., 19 figures, 2 tables, 2 appendices, 19 sources.

QUANTUM COMMUNICATION SYSTEMS, FEMTOSECOND LASER, POLARIZATION, QUANTUM KEY DISTRIBUTION, FIBER, SINGLE SIGNAL, EXTINGUISHING COEFFICIENT.

The object of study is to encode information using a femtosecond laser.

The purpose of the work is to develop optical methods of encoding information. and the study of the principles of optical information encoding and the possibility of using femtosecond lasers in optical encoding.

The research method is theoretical using electronic computers.

The first part deals with the history of quantum cryptography and the first device for quantum cryptography. Elements of information theory (Shannon-Kotelnikov theorem). Basic directions of development of quantum cryptography. BB84 protocol is described.

The second part of the paper deals with the methods of quantum coding, as well as the structure of systems with polarization, phase, time coding. The settings using a femtosecond laser are given.

In the third part of the paper the possibilities of using a femtosecond laser are considered. Using a femtosecond laser and calculated attenuation of radiation in the fiber and open systems.

РЕФЕРАТ

Пояснительная записка аттестационной работы: 67 с., 19 рис., 2 табл., 2 приложения, 19 источников.

КВАНТОВЫЕ СИСТЕМЫ СВЯЗИ, ФЕМТОСЕКУНДНЫЙ ЛАЗЕР, ПОЛЯРИЗАЦИЯ, КВАНТОВОЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ВОЛОКНО, ОДНОФОТОННЫЙ СИГНАЛ, КОЭФФИЦИЕНТ ЗАТУХАНИЯ

Объект исследования – кодирование информации с помощью фемтосекундного лазера.

Цель работы – развитие оптических методов кодирования информации. и исследования принципыв оптического кодирования информации и возможности применения фемтосекундных лазеров в оптической кодировке.

Метод исследования – теоретический с использованием электронно-вычислительных машин.

В первой части работы рассмотрена история квантовой криптографии и первое устройство квантовой криптографии. Элементы теории информации (теорема Шеннона-Котельникова). Основные направления развития квантовой криптографии. Описаны протокол BB84.

Во второй части работы рассмотрены методы квантового кодирования, а также структуры систем с поляризацийним, фазовым, временным кодированием. Приведение установки с использованием фемтосекундного лазера.

В третьей части работы рассмотрены возможности применения фемтосекундный лазер. Использование фемтосекундного лазера и рассчитан затухания излучения в волокне и открытых системах.

ЗМІСТ

ВСТУП

Розвиток лазерної фізики в останні 30 років було в значній мірі ознаменовано інтенсивними розробками і впровадженням лазерів, що генерують імпульси тривалістю від декількох одиниць до декількох сотень фемтосекунд (1 фс = 10^{-15} с). Для видимого і інфрачервоного діапазонів довжин хвиль електромагнітного випромінювання такі імпульси є гранично короткими з точки зору порівнянності тривалості імпульсу з періодом світлового коливання. Так, наприклад, довжині хвилі λ = 600 нм (помаранчевий колір) відповідає період світлового коливання T = 2 фс в вакуумі.

Фемтосекундне лазерне випромінювання є певною мірою унікальним з тієї точки зору, що тривалість імпульсів не перевищує або навіть суттєво менше часів, що характеризують фазові переходи в речовинах, швидкості хімічних і біологічних реакцій. Даний факт дав поштовх до інтенсивного розвитку різних методів діагностики фізичних, хімічних і біологічних процесів з надвисоким тимчасовим дозволом. У 1999 році американський вчений єгипетського походження Ахмед Зевейл був удостоєний Нобелівської премії з хімії за дослідження перехідних станів, що виникають під час хімічних реакцій, з використанням фемтосекундною техніки.

Варто відзначити, що генерація гранично коротких лазерних імпульсів забезпечує не тільки надвисокий дозвіл за часом, але і по частоті, коли фемтосекундний лазер працює в режимі синхронізації мод, що в частотному поданні означає формування в широкому діапазоні довжин хвиль еквідистантним послідовності спектральних компонент, так званої, оптичної гребінки. У 2005 році Нобелівська премія з фізики за внесок в розвиток лазерної точної спектроскопії, включаючи техніку прецизійного розрахунку світлового зрушення в оптичних стандартах частоти (оптичних гребінок) була присуджена американцеві Джону Холу і німцеві Теодору Хеншо.

Крім цього, можливість генерації імпульсів фемтосекундної тривалості знімає істотне обмеження на швидкість обробки інформації: сучасні логічні елементи і мікропроцесори на їх основі, де управління здійснюється електричним струмом, працюють на характерних частотах порядку декількох гігагерц. У той час, як перехід до оптичного діапазону довжин хвиль електромагнітного випромінювання дозволяє в ряді випадків управляти характеристиками середовища, а, отже, і поширенням сигналів через останню, зі швидкостями, порівнянними з тривалістю лазерних імпульсів. В даний час є експериментальні підтвердження сказаного: фемтосекундного лазерне збудження оптично прозорого середовища приводить до зміни її показника заломлення на часовій шкалі порядку сотень фемтосекунд і, отже, до фазово-амплітудних змін оптичних сигналів, що поширюються в даному середовищі, на тих же часах. Це так зване повністю оптичне перемикання. Необхідно відзначити, що часи близько 100 фс є гранично короткими в разі управління хвильовими імпульсами видимого та ближнього інфрачервоного діапазонів.

Важливою перевагою фемтосекундного лазерного випромінювання є також те, що тривалість імпульсів коротше характерних часів термічних процесів в речовинах (десятки і сотні пикосекунд). З практичної точки зору це дозволяє здійснювати лазерну обробку (наприклад, свердління і різання) твердотільних матеріалів в умовах, коли теплові втрати мінімізовані, а, отже, з максимальною прецизійністю і чистотою в практично повній відсутності крапель з розплаву [1].

Метою данной атестаційної роботи є розвиток оптичних методів кодування інформації. Для досягнення мети в роботі були поставлені такі завдання: дослідити принципи оптичного кодування інформації та переваги застосування фемтосекундних лазерів в оптичному кодуванні;

1 ФІЗИЧНІ ОСНОВИ КВАНТОВОГО КОДУВАННЯ

1.1 Загальна схема передачі сигналу

Інформація в енергетичній формі реалізується у вигляді сигналів. «Сигнал» – це фізичний процес (електричний, акустичний, електромагнітний і ін.), що несе повідомлення. «Повідомлення» є сукупність сигналів, що містять інформацію. «Дані» є інформація в формалізованому вигляді, що дозволяє реєструвати її на фізичному носії і здійснювати обробку і передачу інформації за допомогою технічних засобів.

Теорія інформації на основі різних статистичних (імовірнісних) моделей процесу передачі інформації дозволяє сформулювати оптимальні способи перетворення і обробки сигналів для їх найбільш вірогідного відтворення в кінцевому пристрої системи джерела – одержувачі інформації (рис. 1.1).

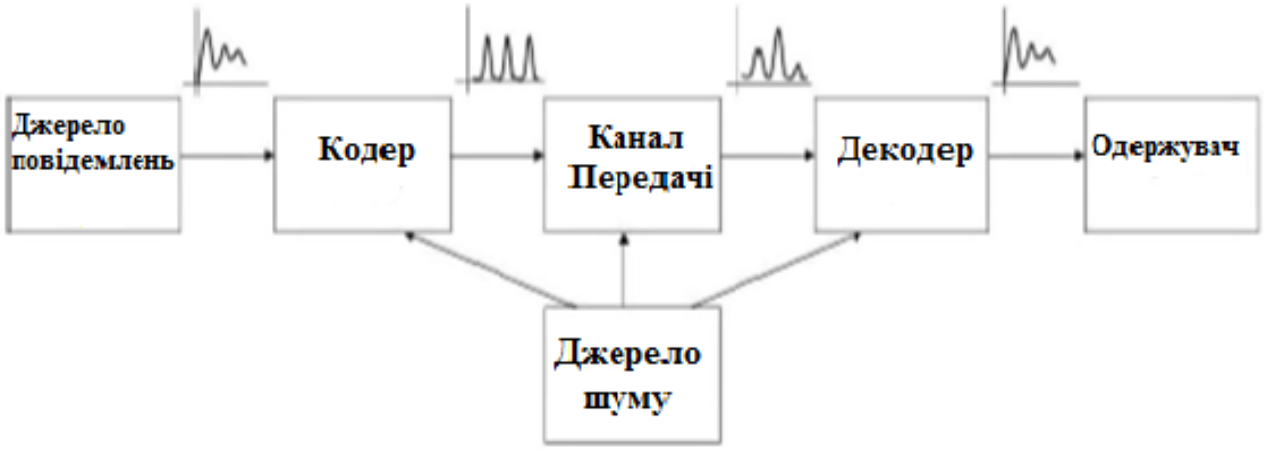


Рисунок 1.1 – Загальна схема системи передачі інформації

Процес передачі інформації неминуче супроводжується різними випадковими дестабілізуючими діями, тобто шумами. Створення системи передачі сигналів, стійкої до впливу шумів різної природи (адитивних, мультиплікативних і ін.), і є основним завданням розробників таких систем, при цьому істотну роль грає вибір способу кодування сигналів, що

поширюються в каналі передачі. Одним з головних наслідків сучасної теорії інформації є твердження, що найбільш достовірне відтворення сигналу на виході системи передачі забезпечується саме при дискретному («цифровому») кодуванні сигналів. При певних вимогах до дискретного перетворення сигналів в кінцевому пристрої системи можна відновити вхідну послідовність сигналів з будь-якою точністю.

1.2 Елементи теорії інформації

1.2.1 Теорема Шеннона

Теорема Шеннона, де швидкість C передачі інформації дорівнює відношенню обсягу I переданої інформації до часу T передачі:

$$C = \frac{I}{T} \ \textit{біт/с} \ . \qquad (1.1)$$

Теорема Шеннона показує залежність швидкості передачі інформації від технічних характеристик системи передачі: ширини B смуги переданих частот і відносини сигнал / шум (S/N) в крайовому пристрої цієї системи:

$$C = B \log_2(1 + \frac{S}{N}), \qquad (1.2)$$

де S/N – відношення середньоквадратичної потужності сигналу до середньоквадратичної потужності шуму на виході системи передачі.

Очевидно, що пропускна здатність системи передачі інформації прямо пропорційна ширині B смуги частот передачі. Наприклад, в телефонії при передачі аналогового звукового сигналу величина B = 8 кГц, а при передачі цього телефонного сигналу в цифровій формі, при восьми знаках двійкового коду (відповідних 256 рівнями квантування величини сигналу), смуга частот

передачі в 8 разів ширше, B = 64 кбіт/с. Аналоговий аудіо-сигнал має смугу частот B = 22,05 кГц і для його високоякісної цифрової передачі, при 16 розрядах в двійковому коді, потрібна смуга частот B = 2,03 Мбіт/с. Звичайне ТВ – зображення переноситься аналоговим сигналом в смузі частот B = 4 МГц, а при 256 рівнях квантування величини сигналу B = 32 Мбіт/с. Смуга частот передачі в цифровому телебаченні високої чіткості (ТВЧ) дорівнює 504,3 Мбіт/с.

1.2.2 Теорема Шеннона-Котельникова (теорема відліків)

Дана теорема визначає необхідні умови дискретного перетворення (кодування) сигналів, при якому вибіркові значення сигналу містять повну інформацію про сигнал в будь-який момент часу. Якщо задана періодична функція $f(t) = f(t \pm NT)$, де N = 1,2, ... і T – період, з обмеженим (максимальна кутова частота спектра дорівнює ω_c) фур'є-спектром, вона представляється кінцевим рядом Фур'є:

$$f(t) = \sum_{k=1}^{n} C_k \cos(k\omega_1 t - \varphi_k), \qquad (1.3)$$

де C_k і φ_k – коефіцієнти Фур'є,

$\omega_I = 2\pi/T$;

$n = \omega_I / \omega_c$.

Можна показати, що така функція представляється поруч її вибіркових значень з ваговими коефіцієнтами виду функцій відліків ($\sin\varphi/\varphi$):

$$f(t) = \sum_{k=1}^{\infty} f(k\tau) \frac{\sin \omega_c (t - k\tau)}{\omega_c (t - k\tau)} \ . \qquad (1.4)$$

На підставі останньої формули теорема Шеннона-Котельникова стверджує: передача неперервної функції може бути зведена до передачі її окремих вибіркових значень (відліків) або кодових комбінацій, що містять інформацію про величину відліків, з тактовою частотою не менш, ніж $2F_c$. Точний вид функції $f(t)$ в будь-який момент часу відновлюється по її вибірковими значеннями $f(k\tau)$ (рис. 1.2).

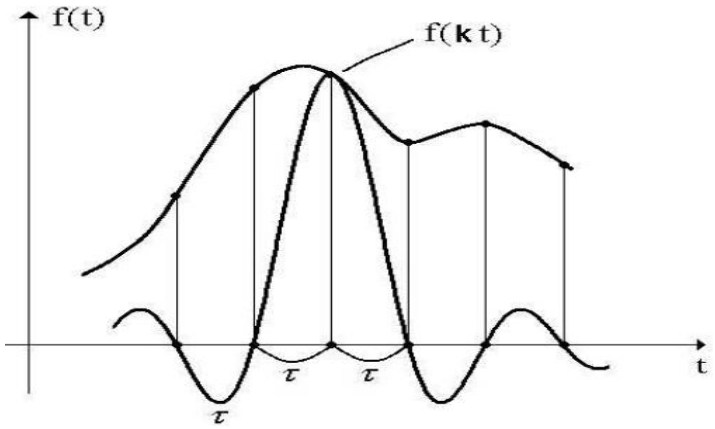


Рисунок 1.2 – Іллюстрація теореми відліків

При множенні величин вибірок на відповідні функції відліків (виду sinφ/φ) і підсумовуванні досить великого числа членів нескінченної низки, нулі функцій відліків збігаються з моментами відліків [2].

1.3 Природа секретності квантового каналу зв'язку

При переході від сигналів, де інформація кодується імпульсами, що містять тисячі фотонів, до сигналів, де середнє число фотонів, що припадають на один імпульс, менше одиниці (близько 0,1), вступають в дію закони квантової фізики. Саме на використанні цих законів в поєднанні з процедурами класичної криптографії заснована природа секретності квантового каналу зв'язку (ККЗ). У квантово-криптографічному апараті можна застосувати принцип невизначеності Гейзенберга, згідно з яким

спроба провести вимірювання в квантовій системі вносить в неї порушення, і отримана в результаті такого виміру інформація визначається прийнятою стороною як дезінформація. Процес вимірювань в квантовій фізиці характеризується тим, що він може активно вносити зміни в стан квантового об'єкта, і йому притаманні певні стандартні квантові обмеження. Слід виділити обмеження, пов'язані з неможливістю одночасного вимірювання взаємо доповнюючих параметрів цієї системи. Ми не можемо одночасно виміряти енергію і поляризацію фотона. Дослідження показали, що спроба перехоплення інформації з квантового каналу зв'язку неминуче призводить до внесення в нього перешкод, які виявляються законними користувачами цього каналу. Квантова криптографія використовує цей факт для забезпечення можливості двом сторонам, які раніше не зустрічалися і не обмінювалися ніякою попередньою секретною інформацією, здійснювати між собою зв'язок в обстановці повної секретності без остраху бути підслуханими зловмисником (рис. 1.3).

.

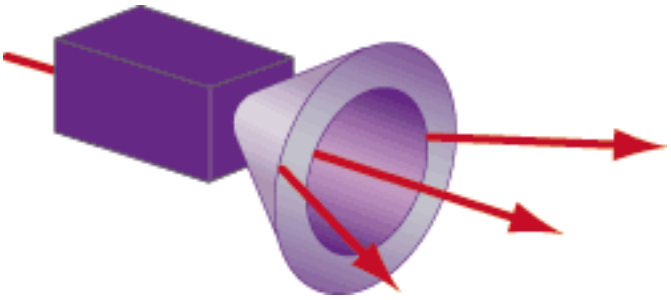


Рисунок 1.3 – Поширення поодиноких фотоні в квантово-оптичному каналі зв’язку

Технологія квантової криптографії спирається на принципову невизначеність поведінки квантової системи – неможливо одночасно отримати координати і імпульс частинки, а також виміряти один параметр фотона, що не спотворив інший. Це фундаментальні властивісті природи у фізиці відомі як принцип невизначеності Гейзенберга, сформульований в

1927 року.

Згідно з цим принципом, спроба вимірювання взаємопов'язаних параметрів в квантовій системі вносить в неї порушення, і отримана в результаті такого виміру інформація визначається прийнятої стороною як дезінформація.

Якщо намагатися щось зробити з фотоном – виміряти поляризацію (напрям обертання) або довжину хвилі (колір), то його стан зміниться.

Дві квантові величини не можуть бути виміряні одночасно з необхідною точністю, і вимір одного виду поляризації рандомізує іншу складову. Якщо відправник і одержувач не домовилися між собою, який вид поляризації брати за основу, одержувач може зруйнувати посланий відправником сигнал, не отримавши ніякої корисної інформації.

Завдяки цьому можлива побудова каналів передачі даних, захищених від підслуховування: одержувач завжди зможе визначити, чи не перехоплена ця інформація, і при позитивній відповіді повторити передачу з іншим ключем.

Відправник кодує відправлені дані, задаючи певні квантові стани, а одержувач реєструє ці стани. Потім одержувач і відправник спільно обговорюють результати спостережень. У підсумку можна бути впевненим, що передана і прийнята кодові послідовності тотожні. Обговорення результатів стосується помилок, внесених шумами або зловмисником, і ні в якій мірі не розкриває вмісту повідомлення. Може обговорюватися парність повідомлення, але не окремі біти. При передачі даних контролюється поляризація фотонів [3].

1.4 Історія квантової криптографії

Стівен Візнер (Stephen Wiesner), будучи студентом Колумбійського університету, в 1970 подав статтю з теорії кодування в журнал IEEE Information Theory, але вона не була опублікована, так як викладені в ній

припущення здавалися фантастичними, а не науковими. Саме в ньому була описана ідея можливості використання квантових станів для захисту грошових банкнот. Візнер запропонував в кожну банкноту вмонтувати 20 так званих світових пасток, і поміщати в кожну з них по одному фотону, поляризованому в строго визначеному стані. Кожна банкнота маркувалася спеціальним серійним номером, який укладав інформацію про становище поляризаційного фотонного фільтра. В результаті цього при застосуванні відмінного від заданого фільтра комбінація поляризованих фотонів стиралася. Але на той момент технологічний розвиток не дозволяв навіть міркувати про такі можливості. Однак в 1983 році його робота «Поєднане кодування» була опублікована в SIGACT News і отримала високу оцінку в наукових колах.

Надалі на основі принципів роботи Візнера С. вчені Чарльз Беннет (Charles Bennett) з фірми IBM і Жиль Брассард (Gilles Brassard) з Монреальського університету розробили спосіб кодування і передачі повідомлень. Ними була зроблена доповідь на тему «Квантова криптографія: Розподіл ключа і підкидання монет» на конференції IEEE International Conference on Computers, Systems, and Signal Processing. Описаний в роботі протокол згодом визнаний першим і базовим протоколом квантової криптографії і був названий на честь його творців BB84. Для кодування інформації протокол використовує чотири квантових стану мікросистеми, формуючи два сполучених базису.

В 1991 році відбулося опублікування результатів робіт Артур Екерта, який працював над протоколом квантової криптографії, заснованому на заплутаних станах. В основу покладені принципи парадоксу Ейнштейна-Подільський-Розенберга, зокрема принцип нелокальності заплутаних квантових об'єктів.

Протягом двадцяти п'яти років, квантова криптографія пройшла шлях від теоретичних досліджень і докази основних теорій до комерційних систем, що використовують оптичне волокно для передачі на відстань десятків кілометрів.

У першій експериментальній демонстрації установки квантового розподілу ключів проведеної в 1989 в лабораторних умовах, передача здійснювалася через відкритий простір на відстань тридцяти сантиметрів. Далі ці експерименти були проведені з використанням оптичного волокна в якості середовища поширення. Після перших експериментів Мюллера та інших, в Женеві, з використанням оптоволокна довжиною 1,1 км, в 1995 р. відстань передачі було збільшено до 23 км через оптичне волокно, прокладене під водою. Приблизно в той же час, Таунсенд з British Telecom була продемонстрована передача на 30 км. Пізніше, продовживши тестування систем з використанням різних конфігурацій оптичних мереж, збільшив дальність до 50 км. Експерименти з передачі на цю ж відстань були пізніше повторені Хьюзом і ін. В Лос-Аламосі. У 2001 р. Хіскетом та ін. в Сполученому Королівстві була здійснена передача на відстань 80 км. В 2004 – 2005 роках дві групи в Японії і одна в Сполученому Королівстві повідомили про здійснення експериментів по квантовому розподілу ключів і інтерференції одиночних фотонів на відстань понад 100 км. Перші експерименти по передачі на відстань 122 км проводилися вченими з Toshiba в Кембриджі з використанням детекторів на основі лавинних фотодіодів (ЛФД). Рекорд по дальності передачі інформації належить об'єднанню вчених Лос-Аламоса і Національного інституту стандартів і технологій і становить 184 км. У ньому використовувалися однофотонні приймачі, що охолоджуються до температур близьких до нульових за Кельвіном.

Перша презентація комерційної системи квантової криптографії сталася на виставці CeBIT-2002, де швейцарські інженери компанії GAP-Optique (www.gap-optique.unige.ch) з Женевського університету представили першу систему квантового розподілу ключів (QKD – Quantum Key Distribution). Вченим вдалося створити досить компактний і надійний пристрій. Система розташовувалася в двох 19-дюймових блоках і могла працювати без настройки відразу після підключення до персонального комп'ютера. З його допомогою було встановлено двостороння наземна і повітряний волоконно-

оптичний зв'язок між містами Женева і Лузаном, відстань між якими становить 67 км. Джерелом фотонів служив інфрачервоний лазер з довжиною хвилі 1550 нм. Швидкість передачі даних була невисока, але для передачі ключа шифру (довжина від 27,9 кбіт до 117,6 кбіт) велика швидкість і не була потрібна.

У наступні роки до проектування і виготовлення систем квантової криптографії підключилися такі комерційні монстри як Toshiba, NEC, IBM, Hewlett Packard, Mitsubishi, NTT. Але поряд з ними з'являлися на ринку і маленькі, але високотехнологічні компанії: MagiQ (www.magiqtech.com), Id Quantique (www.idquantique.com), Smart Quantum (www.smartquantum.com). У липні 2005 в гонці за збільшення відстані передачі ключа вперед вийшли інженери Toshiba, представивши на ринку системи здатні передати ключ на 122 км. Однак, як і у конкурентів, швидкість генерації ключа в 1,9 кбіт/с залишала бажати кращого. Виробники в теперішній час прагнуть до розробки інтегрованих систем – новинкою від Id Quantique, є система Vectis, що використовує квантовий розподіл ключів для створення VPN тунелів, кодуванняя даних на канальному рівні за допомогою шифру AES. Ключ може бути 128, 196 або 256-бітної довжини і змінюється з частотою до 100 Гц. Максимальна дистанція для даної системи складає 100 км. Всі перераховані вище компанії виробляють системи кодування інформацій по бітових ключах в фазових станах фотонів. З часів перших реалізацій, схеми побудови систем квантового розподілу ключів значно ускладнилися.

Британські фізики з комерційного підрозділу QinetiQ Британської оборонної дослідної лабораторії та німецькі фізики з Мюнхенського університету Людвіга-Максиміліана вперше здійснили передачу ключа на відстань 23,4 км безпосередньо через повітряний простір без використання оптичного волокна. В експерименті для кодування криптографічної інформації використовувалися поляризації фотонів – одна для передачі двійкового символу «0» і протилежна для символу «1». Експеримент проводився в горах Південної Німеччини. Слабкий імпульсний сигнал

посилався вночі з однієї гірської вершини (2 950 м) на іншу (2 244 м), де знаходився лічильник фотонів.

Керівник проекту Джон Реріті (John Rarity) з QinetiQ вважав, що вже в 2005 році буде проведено експеримент з відправкою криптографічного ключа на низькоорбітальних супутників, а до 2009 року з їх допомогою можна буде відправляти секретні дані в будь-яку точку планети. Зазначалося, що для цього доведеться подолати ряд технічних перешкод. По-перше, необхідно поліпшити стійкість системи до неминучої втрати фотонів при їх посилці на відстані в тисячі кілометрів. По-друге, існуючі супутники не оснащені відповідним обладнанням для пересилання криптографічних даних по квантовому протоколу, так що буде потрібно конструювання та запуск абсолютно нових супутників.

Дослідники з Північно-західного університету (Еванстон, штат Іллінойс) продемонстрували технологію, що дозволяє передавати на невелику відстань шифрування повідомлення зі швидкістю 250 Мбіт/с. Вчені запропонували метод квантового кодування самих даних, а не тільки одного ключа. У цій моделі враховується кут поляризації кожного переданого фотона, Тому будь-яка спроба декодувати повідомлення призводить до такої зашумленості каналу, що будь-яка розшифровка стає неможливою. Модель наступного покоління зможе працювати практично на магістральній швидкості Інтернету близько 2,5 Гбіт/с. За словами одного з розробників, професора Премії Кумара (Prem Kumar), "ще нікому не вдавалося виконувати квантове шифрування на таких швидкостях". Вчені вже отримали кілька патентів на свої розробки і зараз працюють разом зі своїми промисловими партнерами Telcordia Technologies і BBN Technologies над подальшим удосконаленням системи. Спочатку розрахований на п'ять років проект був підтриманий грантом DARPA (the Defense Advanced Research Projects Agency) в 4,7 мільйона доларів. Результатом даного проекту стала система квантового кодування AlphaEta.

Група Річарда Хьюгс (Richard Hughes) з Лос-Аламоса займається розробками супутникових оптичних ліній зв'язку (ОЛС). Для реалізації переваг квантової криптографії фотони повинні проходити через атмосферу без поглинання і зміни поляризації. Для запобігання поглинання дослідники вибирають довжину хвилі в 770 нм, що відповідає мінімальному поглинанню випромінювання молекулами атмосфери. Сигнал з більшою довжиною хвилі також слабо поглинається, але більш схильний до турбулентності, яка викликає зміну локального показника заломлення повітряного середовища і, зважаючи на це, зміну поляризації фотонів. Вченим доводиться вирішувати і побічні завдання. Супутник, поряд з фотонами, що несуть повідомлення, може прийняти і фотони фонового випромінювання, що виходить як від Сонця, так і відбитого Землею або Місяцем. Тому застосовуються надвузьконправлені приймачі, а також фільтри для відбору фотонів певної довжини хвилі. Крім того, фотоприймач чутливий до прийому фотонів протягом 5 нс періодично з інтервалом в 1 мкс. Це повинно бути погоджено з параметрами передавача. Такі хитрощі знову обумовлюють вплив турбулентності. Навіть при збереженні поляризації, внаслідок турбулентності може змінитися швидкість передачі фотонів, приводячи до фазового тремтіння.

З метою компенсації фазового тремтіння попереду кожного фотона висилається світловий імпульс. Цей синхронізуючий імпульс, піддається такому ж, як наступний за ним фотон, впливу атмосфери. Тому незалежно від моменту отримання імпульсу приймач супутника знає, що через 100 нс потрібно відкритися для прийому інформаційного фотона. Зміна показника заломлення внаслідок турбулентності викликає догляд променя від антени. Тому для направлення потоку фотонів передаюча система відстежує слабке віддзеркалення від синхроімпульсів. Групою Хьюгс здійснена передача повідомлення по квантовому криптографічному каналу через повітряне середовище на відстань в 500 м на телескоп діаметром 3,5 дюйма. Прийнятий фотон потрапляє на розподільник, який направляє його на той чи інший

фільтр. Після цього ключ контролювався на наявність помилок. Реально, навіть при відсутності перехоплення, рівень помилок досягав 1,6 % через наявність шуму, фонових фотонів і неузгодженості. Це несуттєво, оскільки при перехопленні рівень помилок зазвичай більше 25 %.

Пізніше групою Хьюгс було передано повідомлення по квантовому каналу через повітряне середовище на відстань 2 км. При випробуваннях сигнали передавалися горизонтально, поблизу поверхні Землі, де щільність повітря і флуктуації інтенсивності максимальні. Тому відстань в 2 км поблизу поверхні Землі еквівалентні 300 км, що відокремлює Низькоорбітальний штучний супутник від Землі.

Таким чином, менш ніж за 50 років квантова криптографія пройшла шлях від ідеї до втілення в комерційну систему квантового розподілу ключів. Діюча апаратура дозволяє розподіляти ключі через квантовий канал на відстань, яка перевищує 100 км (рекорд 184 км), зі швидкостями достатніми для передачі ключів шифрування, але не достатніми для поточного шифрування магістральних каналів за допомогою шифру Вернама. Основними споживачами систем квантової криптографії в першу чергу виступають міністерства оборони, міністерства закордонних справ і великі комерційні об'єднання. На даний момент висока вартість квантових систем розподілу ключів обмежує їх масове застосування для організації конфіденційного зв'язку між невеликими і середніми фірмами і приватними особами.

1.5 Перший пристрій квантової криптографії

У 1989 р Беннет і Брассард в Дослідницькому центрі компанії IBM побудували першу працюючу квантово-криптографічну систему. Вона складалася з квантового каналу, що містить передавальний апарат Аліси на одному кінці і прийомний апарат Боба на іншому, розміщених на оптичній лаві довжиною близько 1 м, в світлонепроникному кожусі розмірами 1,5 м ×

0,5 м × 0,5 м. Він представляв собою вільний повітряний канал довжиною близько 32 см. Під час функціонування макет керувався від персонального комп'ютера, який містив програмне уявлення користувачів Аліси і Боба, а також зловмисника.

Надійність збереження в таємниці переданих повідомлень в значній мірі залежить від інтенсивності використаних для передачі спалахів світла. Слабкі спалахи ускладнюють перехоплення повідомлень, але призводять до збільшення числа помилок у вимірі правильної поляризації у законного користувача. Посилення ж інтенсивності спалахів полегшує можливість перехоплення шляхом розщеплення вихідного пучка світла або одиночного фотона на два: одного, що направляється законному одержувачу, і іншого, аналізованого зловмисником. Аліса і Боб можуть використовувати для виправлення помилок коди, що виправляють помилки, обговорюючи результати кодування по відкритому каналу (рис. 1.4).

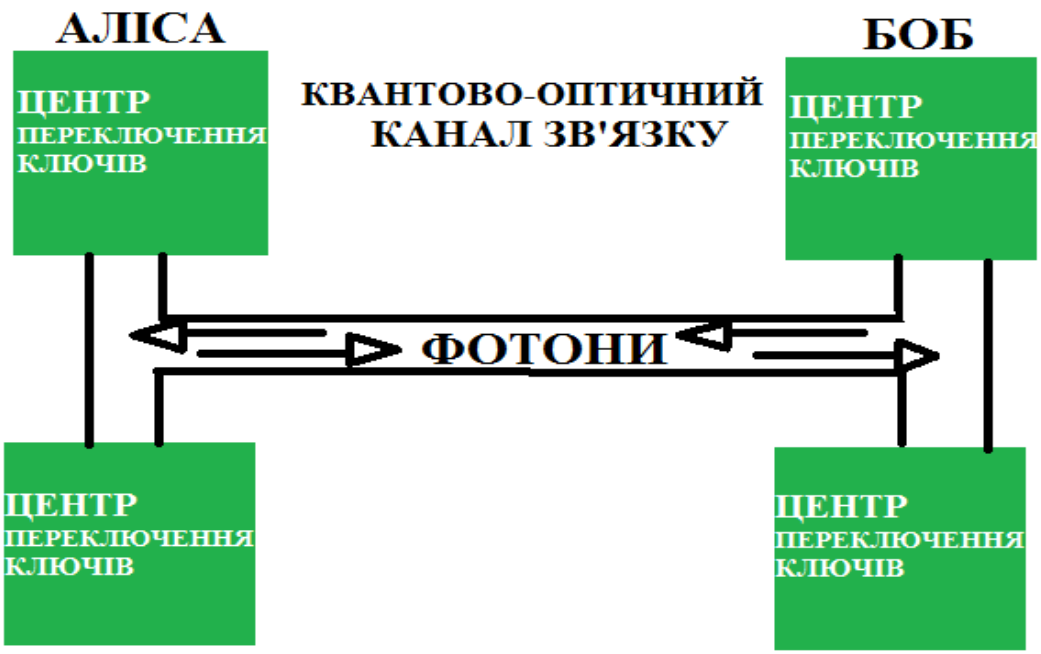


Рисунок 1.4 – Перша квантово-криптографічна схема

Система складається з квантового каналу і спеціального устаткування на обох кінцях схеми.

Однак при цьому частина інформації може потрапити до зловмисника. Проте Аліса і Боб, знаючи інтенсивність спалахів світла і кількість виявлених і виправлених помилок, можуть оцінити кількість інформації, що потрапляє до зловмисника.

1.6 Основні напрямки розвитку квантової криптографії

У квантовій криптографії виділилися два основних напрямки розвитку систем розподілу ключів. Перший напрямок заснований на кодуванні квантового стану одиночної частинки і базується на принципі неможливості розрізнити абсолютно надійно два неортогональних квантових стану.

Довільний стан будь-якої дворівневої квантово-механічної системи можна представити у вигляді лінійної суперпозиції:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.5}$$

її власних станів 0 та 1 з комплексними коефіцієнтами α і β, причому:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.6}$$

Захищеність першого напрямку ґрунтується на теоремі про заборону клонування невідомого квантового стану. Завдяки унітарності і лінійності квантової механіки, неможливо створити точну копію невідомого квантового стану без впливу на початковий стан. Нехай, наприклад, відправник (назвемо його Аліса) і одержувач (Боб) використовують для передачі інформації дворівневі квантові системи, кодуючи стан цих систем. Якщо зловмисник (Єва) перехоплює носій інформації, посланий Алісою, вимірює його стан і пересилає далі Бобу, то стан цього носія буде іншим, ніж до вимірювання. Таким чином, підслуховування квантового каналу призводить до помилок передачі, які можуть бути виявлені легальними користувачами. Основним

протоколом квантової криптографії на одночастотних станах є протокол BB84 [2].

1.7 Протокол BB84

У протоколі BB84 використовуються 4 квантових стани фотонів, наприклад, напрямок вектора поляризації, одне з яких Аліса вибирає залежно від переданого біта: 90° або 135° для «1», 45° або 0° для «0». Одна пара квантових станів відповідає 0 (| 0 (+) >) і 1 (| 1 (*x*)>) і належить базису «+». Інша пара квантових станів відповідає 0 (| 0 (*x*) >) і 1 (| 1 (*x*) >) і належить базису «*x*». В середині обох базисів стани ортогональні, але стани з різних базисів є попарно не ортогональними (не ортогональність необхідна для детектування спроб знімання інформації).

Квантові стани системи можна описати таким чином:

$$\begin{aligned} |0_x\rangle &= \frac{1}{\sqrt{2}}(|0_x\rangle + |1_x\rangle), \\ |1_x\rangle &= \frac{1}{\sqrt{2}}(|0_x\rangle - |1_x\rangle). \end{aligned} \tag{1.7}$$

Тут стани $|0\rangle$ і $|1\rangle$ кодуються значеннями «0» та «1» в базисі «+», а $|0_x\rangle$ і $|1_x\rangle$ кодуються цими же значеннями в базисі «*x*». Базиси повернуті друг відносно одного на 45° (рис. 1.5).

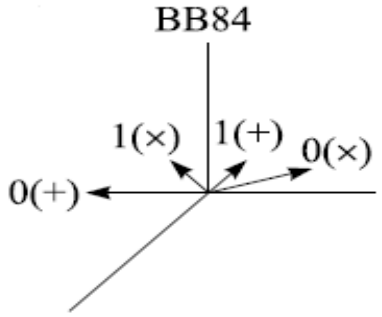


Рисунок 1.5 – Стан поляризованних фотонів, використованні в протоколі BB84

Етапи формування ключів.

1. Аліса випадковим чином вибирає один з базисів. Потім всередині базису випадково вибирає один зі станів, відповідне (0) або (1) і посилає фотони (рис. 1.6).

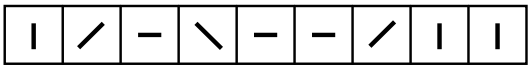


Рисунок 1.6 – Фотони з різною поляризацією

2. Боб випадково і незалежно від Аліси вибирає для кожного вступника фотона: прямолінійний (+) або діагональний (х) базис (рис. 1.7).

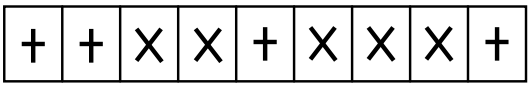


Рисунок 1.7 – Обраний тип вимірюваня

Потім Боб зберігає результати вимірювань (рис. 1.8).

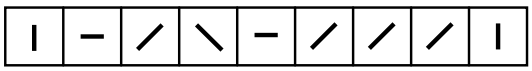


Рисунок 1.8 – Результати вимірювань

3. Боб по відкритому загальнодоступному каналу зв'язку повідомляє, який тип вимірювань був використаний для кожного фотона, тобто який був обраний базис, але результати вимірювань залишаються в секреті.

4. Аліса повідомляє Бобу по відкритому загальнодоступному каналу зв'язку, які вимірювання були обрані відповідно до вихідного базису Аліси (рис.1.9).

Рисунок 1.9 – Випадки правильних вимірів

5. Далі користувачі залишають тільки ті випадки, в яких обрані базиси збіглися. Ці випадки переводять в біти (0 і 1), і отримують, таким чином, ключ (рис.1.10).

Рисунок 1.10 – Отримання ключової послідовності за результатами правильних вимірів

Число випадків, в яких обрані базиси збіглися, становитиме в середньому половину довжини вихідної послідовності (приклад визначення кількості фотонів, прийнятих Бобом, показаний в таблиці 1.1).

Таблиця 1.1 – Формування квантового ключа по протоколу BB84

Двійковий сигнал Аліси	0	1	0	1
Поляризаційний код Аліси	↔	↕	⤡	⤢
Детектування Бобом	✣	✣	✣	✣
Двійковий сигнал Боба	0	1	?	?

Таким чином, в результаті передачі ключа Бобом в разі відсутності перешкоди спотворень будуть правильно зареєстровані в середньому 50 % фотонів.

Однак ідеальних каналів зв'язку не існує і для формування секретного

ключа необхідно провести додаткові процедури пошуку помилок і посилення секретності. При цьому для частини послідовності біт користувачів, в яких базиси збіглися, через відкритий загальнодоступний канал зв'язку випадковим чином розкриваються і порівнюються значення біт. Далі розкриті біти відкидаються. В ідеальному квантовому каналі (без шуму) досить виявити невідповідність в одній розкритій позиції для виявлення зловмисника. В реальній ситуації неможливо розрізнити помилки, які сталися через шум і вплив зловмисника. Відомо, що якщо відсоток помилок QBER ≤ 11 %, то користувачі з нерозкритою послідовностю, після корекції помилок через відкритий загальнодоступний канал зв'язку і посилення секретності, можуть отримати секретний ключ, який буде у них однаковим і не буде відомий Єві. Ключ, отриманий до додаткових операцій з послідовністю, називається "сирим" ключем.

При корекції помилок ефективним способом для узгодження послідовностей Аліси і Боба є їх «перемішування» для більш рівномірного розподілу помилок і розбиття на блоки розміром k, при якому ймовірність появи блоків з більш ніж однією помилкою дуже незначна. Для кожного такого блоку сторони проводять перевірку парності. Сторони, в яких збігається парність визнаються правильними, а що залишилися діляться на кілька дрібніших частин, і перевірка парності проводиться над кожною такою частиною, поки помилка не виявиться і буде виправлена. Процедура може бути повторена з блоками більш підходящого розміру. Найбільш дрібні блоки відкидаються при наявності в них помилки.

Коли в якомусь блоці кількість помилок виявиться парною, то навіть з оптимальним розміром блоку деякі з них можуть бути не виявлені. Для їх виключення виробляють перемішування послідовності біт, розбиття її на блоки і порівняння їх парності проводиться ще кілька разів, кожен раз зі зменшенням розміру блоків, до тих пір, поки Аліса і Боб не прийдуть до висновку, що ймовірністю помилки в отриманій послідовності можна знехтувати.

В результаті всіх цих дій Аліса і Боб отримують ідентичні послідовності біт. Ці біти і є ключем, за допомогою якого користувачі отримують можливість кодувати і декодувати секретну інформацію і обмінюватися нею по незахищеному від знімання інформації каналу зв'язку.

1.8 Приймачі випромінювання в квантових лініях

Найбільш відомі у відкритій літературі приймачі випромінювання, що працюють в режимі лічильників квантів. В першу чергу - це лавинні фотодіоди. Як відомо, лавинні фотодіоди - високочутливі напівпровідникові прилади, що перетворюють світло в електричний сигнал за рахунок фотоефекту. Їх можна розглядати в якості фотоприймачів, що забезпечують внутрішнє посилення за допомогою ефекту лавинного множення. З функціональної точки зору вони є твердотільними аналогами фотопомножувачів. Лавинні фотодіоди мають більшу чутливість у порівнянні з іншими напівпровідниковими фотоприймача, що дозволяє використовувати їх для реєстрації малих світлових потужностей (1 нВТ).

При подачі сильного зворотнього зсуву (близького до напруги лавинного пробою, зазвичай порядку декількох сотень вольт для кремнієвих приладів), відбувається посилення фотоструму (приблизно в 100 разів) за рахунок ударної іонізації (лавинного множення) генерованих світлом носіїв заряду. Суть процесу в тому, що енергія утворена під дією світла електрона збільшується під дією зовнішнього прикладеного поля і може перевищити поріг іонізації речовини, так що зіткнення такого «гарячого» електрона з електроном з валентної зони може привести до виникнення нової електрон-діркової пари, носії заряду якої також будуть прискорюватися полем і можуть стати причиною утворення все нових і нових носіїв заряду.

Існує ряд формул для коефіцієнта лавинного множення (M), досить об'єктивною є наступна:

$$M = \frac{1}{1 - \int_0^L a(x)dx}, \tag{1.8}$$

де L – довжина області просторового заряду,

α – коефіцієнт ударної іонізації для електронів (і дірок).

Цей коефіцієнт сильно залежить від прикладеної напруги, температури і профілю легірування. Звідси виникає вимога у відмінній стабілізації напруги живлення і температури, або врахування температури задаючою напругу схемою. Ще одна емпірична формула показує сильну залежність коефіцієнта лавинного множення (M) від прикладеного зворотної напруги:

$$M = \left(\frac{1}{1 - \left(\frac{U}{U_b} \right)} \right)^n, \tag{1.9}$$

де U_b – напруга пробою.

Показник ступеня n приймає значення від 2 до 6, в залежності від характеристик матеріалу і структури *p-n* перехода.

Виходячи з того, що в загальному випадку зі зростанням зворотного напруги зростає і коефіцієнт посилення, існує ряд технологій, що дозволяють підвищити напругу пробою до більш ніж 1500 вольт, і отримати, таким чином, посилення більш ніж в 1000 разів. Слід мати на увазі, що просте підвищення напруженості поля без вжиття додаткових заходів може привести до збільшення шумів. І це необхідно врахувати при проектуванні квантових ліній зв'язку. Слід враховувати і інженерне протиріччя: вимога забезпечити максимально можливу дальність зв'язку і максимальне співвідношення сигнал / шум.

Якщо потрібні дуже високі коефіцієнти посилення (10^5 – 10^6), можлива експлуатація деяких типів ЛФД (лавинних фотодіодів) при напрузі вище

пробійної. В цьому випадку потрібно подавати на фотодіод обмежені по току швидко спадають імпульси. Для цього можуть використовуватися активні і пасивні стабілізатори струму. Прилади, що діють таким чином, працюють в режимі Гейгера (Geiger mode). Цей режим застосовується для створення однофотонних детекторів (за умови, що шуми досить малі).

Типове застосування ЛФД – лазерні далекоміри і волоконні лінії зв'язку. Серед нових застосувань можна назвати позитронно-емісійну томографію і фізику елементарних частинок. В даний час вже з'являються комерційні зразки масивів лавинних фотодіодів.

Сфера застосування і ефективність ЛФД залежать від багатьох факторів. Найбільш важливими є:

– квантова ефективність, яка показує, яка частка падаючих фотонів приводить до утворення носіїв заряду і виникнення струму;

– сумарний струм витоку, який складається з темнового струму і шумів.

Електронні шуми можуть бути двох типів: послідовні і паралельні. Перші є наслідком дробових флуктуацій і в основному пропорційні ємності ЛФД, тоді як паралельні пов'язані з механічними коливаннями приладу і поверхневими струмами витоку. Іншим джерелом шуму є фактор надлишкового шуму (excess noise factor) – F. У ньому описуються статистичні шуми, які притаманні стохастичному процесу лавинного множення M в ЛФД. Зазвичай він виражається в такий спосіб:

$$F = kM + (2 - \frac{1}{M})(1 - k), \qquad (1.10)$$

де k – співвідношення коефіцієнтів ударної іонізації для дірок і електронів.

Таким чином, збільшення асиметрії коефіцієнтів іонізації приводить до зменшення цих перешкод. До цього прагнуть на практиці, так як $F(M)$ вносить основний вклад в обмеження роздільної здатності приладів по енергії.

Обмеження на швидкість роботи накладають ємності, час транзиту електронів і дірок і час лавинного множення. Ємність збільшується з ростом площі переходів і зменшенням товщини. Час транзиту електронів і дірок зростає зі збільшенням товщини, що змушує йти на компроміс між ємністю і часом. Затримки, пов'язані з лавинним множенням визначаються структурою діодів, застосовуваними матеріалами, існує залежність від *k*. Таким чином, при розробці методу захисту від несанкціонованого доступів особливу увагу треба звернути на швидкодію джерел випромінювання і рівень власних шумів.

Для створення малошумливих приладів може бути використаний широкий круг напівпровідників:

– кремній використовується для роботи в ближньому ІЧ-діапазоні, при цьому має малі шуми, пов'язані з множенням носіїв;

– германій приймає інфрачервоні хвилі довжиною до 1.7 мкм, але прилади на його основі мають помітні шуми;

– InGaAs забезпечує прийом хвиль довжиною від 1.6 мкм, при цьому маючи менші, ніж у германію шуми. Зазвичай цей матеріал використовується для виготовлення лавинних фотодіодів на гетероструктурах, також включають InP як підкладку і другого компонента для створення гетероструктури. Ця система має робочий діапазон в межах 0,7 мкм – 0,9 мкм. У InGaAs високий коефіцієнт поглинання на довжинах хвиль, використовуваних в телекомунікації через волоконно-оптичні лінії зв'язку, таким чином, досить навіть мікронних шарів InGaAs для повного поглинання випромінювання. Ці матеріали забезпечують невеликі затримки і малі шуми, що дозволяє отримати пристрої з смугою частот понад 100 ГГц для простої InP / InGaAs системи і до 400 ГГц для InGaAs на кремнію.. Це робить можливим передачу даних на швидкості, що перевищує 10 Гбит / с;

– діоди на основі нітриду галію використовуються для роботи в ультрафіолетовому діапазоні хвиль;

– HgCdTe застосовується для виготовлення діодів, що працюють в інфрачервоній частині спектра, зазвичай максимальна довжина хвилі становить приблизно 14 мкм. При цьому вони потребують охолодження для скорочення темпових струмів. Така система здатна забезпечити дуже низький рівень перешкод [4]

2 МЕТОДИ КВАНТОВОГО КОДУВАННЯ

2.1 Типові структури квантових систем розподілу ключів

У системах квантової криптографії в даний час застосовують три види кодування квантових станів: поляризаційне, фазове і кодування тимчасовими зрушеннями. Нижче більш докладно розглянемо типові структури квантових систем розподілу ключів, що реалізують кожний з видів кодування

2.1.1 Структура системи з полярізаційним кодування

Історично першою реалізацією системи квантового розподілу ключів була поляризаційна схема кодування, що працює по протоколу BB84.

Схема квантової криптографічної установки з поляризаційним кодуванням по протоколу BB84 і чотирма станами показана на рисунку 2.1

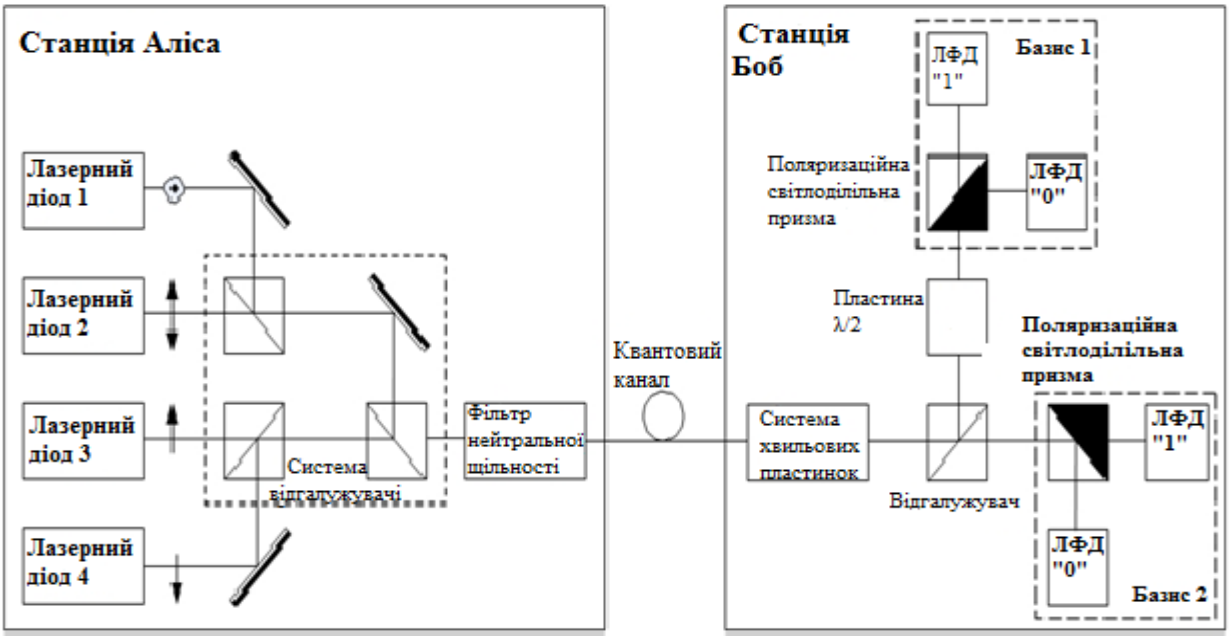


Рисунок 2.1 – Схема квантової криптографічної установки з поляризаційним кодуванням

Станція Аліса, складається з чотирьох лазерних діодів, які випромінюють короткі імпульси світла тривалістю 1 нс. Поляризації фотонів

становить -45°, 0°, +45° и 90°. Для передачі одного біта активізується один з лазерних діодів. Потім імпульси послаблюються набором фільтрів для забезпечення умови однофотонності. Середня кількість фотонів в імпульсі вибирається менше $n<1$. Після цього фотон випромінюється у напрямку до станції Боб. Важливою умовою правильного детектування інформації станцією Боб є збереження поляризації фотонів в волокні. Імпульси, досягаючи станції Боб, проходять через набір хвильових пластинок, використовуваних для відновлення вихідних поляризаційних станів шляхом компенсації змін, внесених волокном. Потім імпульси досягають світлодільника, що здійснює напрямок фотона до лінійного або діагонального аналізатору. Передані фотони аналізуються в ортогональному базисі за допомогою поляризаційної світлоділільної призми і двох лавинних фотодіодів (ЛФД). Поляризація фотонів, які пройшли через хвильові платівки повертається на 45° (з – 45° до 0°). У той же час, інші фотони аналізуються другою системою «поляризационная світлороздільна призма – ЛФД» в діагональному базисі. Нехай є фотон, поляризований під кутом 45°. Після того, як він залишає станцію Аліса, його поляризація випадковим чином перетворюється в оптичному волокні. В станції Боб система з хвильових пластинок повинна бути встановлена таким чином, щоб компенсувати зміну поляризації. Якщо фотон пройде на вихід світлодільника, відповідний лінійному базису поляризації, у нього будуть рівні ймовірності потрапити в один з фотодетекторов, що призведе до випадкового результату. З іншого боку, якщо буде обраний діагональний базис, його поляризація буде повернена на 45°. Тоді світлодільник відобразить його з одиничною ймовірністю, що призведе до певного результату. Замість використання чотирьох лазерів станцією Аліса і двох поляризаційних світлоділільних призм станцією Боб, можливо також застосування активних поляризаційних модуляторів, таких як комірки Поккельса. Для кожного імпульсу світла модулятор активується за випадковим законом, приводячи поляризацію в одному з четирьох станів, в той час як приймаюча сторона в випадковому

порядку обертає поляризацію половини прийнятих імпульсів на 45^{o}.При чому, поляризаційна модова дисперсія (ПМД) може привести до зміни поляризації фотонів, за умови, що час затримки між поляризаційними модами більше часу когерентності. Це вносить обмеження на типи лазерів, що використовуються станцією Аліса.

Антон Мюллер і його колеги з Женевського університету використали подібну систему для проведення експериментів в галузі квантової криптографії. Вони передавали ключ на відстань 1100 м, використовуючи фотони з довжиною хвилі 800 нм. Для збільшення максимальної дистанції передачі вони повторили експеримент з фотонами на довжині хвилі випромінювання 1300 нм і передавали ключ на 23 км. Особливістю даного експерименту було використання в якості квантового каналу, який зв'язує станції Аліса з Боб, стандартного телекомунікаційного оптичного кабелю, який використовувався компанією Swisscom для проведення телефонних переговорів.

Результати цих експериментів показали, що зміни поляризації, що вносяться оптичним волокном, були нестабільні в часі. Незважаючи на те, що вони стабілізувалися на деякий час (порядку декількох хвилин), в випадковий момент поляризація різко змінювалася. Це означає, що реальна квантова криптографічна система вимагає створення механізму активної компенсації поляризаційних змін. Незважаючи на наявність принципової можливості створення такого механізму, очевидно, що його практична реалізація дуже ускладнена.

Джеймс Френсон розробив систему автоматичного підстроювання поляризації, але не став займатися її подальшим вдосконаленням. Існують і інші способи автоматичного контролю поляризації, розроблені для когерентних волоконно-оптичних систем зв'язку. Цікаво те, що заміна стандартного волокна на волокно, що зберігає поляризацію, не вирішує проблему, так як такі волокна зберігають тільки два ортогональних стану поляризації, а в системах квантової криптографії використовуються чотири

попарно неортогональних стану. З цих причин, поляризаційне кодування не є оптимальним методом кодування при побудові волоконно-оптичних систем квантової криптографії.

2.1.2 Структура системи з фазовим кодуванням

Нестабільність поляризації в системах з поляризаційним кодуванням сильно ускладнює (хоча і не унеможливлює) їх створення. У зв'язку з цим був розроблений інший тип квантових криптографічних систем. Ідея кодування біт фазою фотонів була вперше згадана Беннеттом, коли він описував протокол з використанням двох станів. Отримання квантових станів і подальший їх аналіз виробляються інтерферометрами, які можуть бути реалізовані одномодовими компонентами волоконної оптики. На рисунку 2.2 показана волоконооптичну реалізація інтерферометра Маха-Цендер.

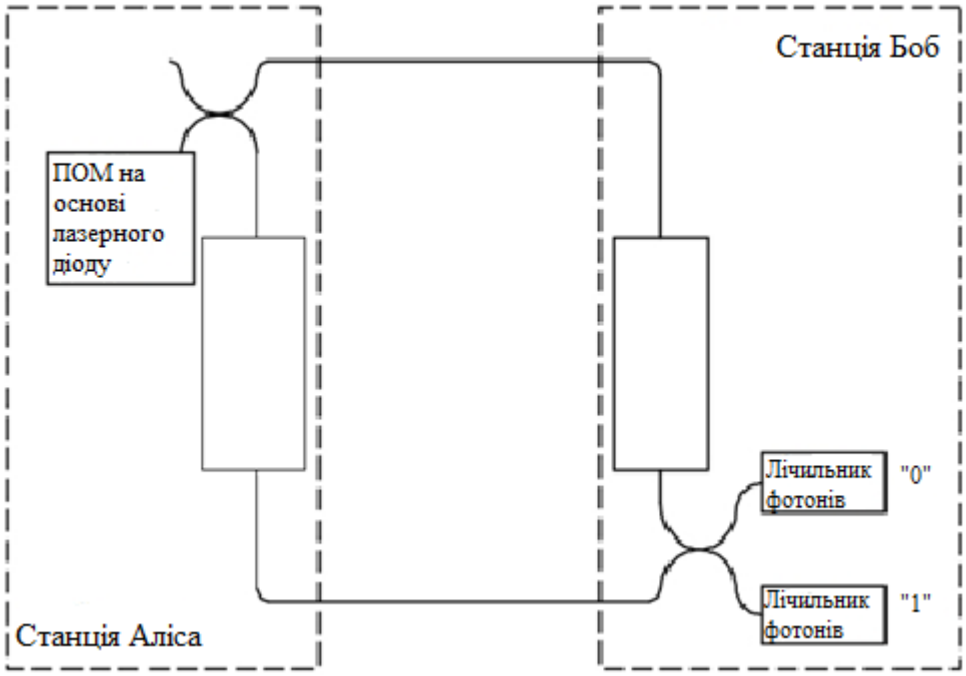


Рисунок 2.2 – Інтерферометр Маха-Цендера

Інтерферометр виконаний з двох волоконно-оптичних відгалужувачів, з'єднаних між собою, і двох фазових модуляторів – по одному в кожному

плечі. У таку систему можна ввести оптичне випромінювання, використовуючи класичне безперервне джерело, і спостерігати потужність оптичного випромінювання на виходах. У разі, якщо довжина когерентності світла лазера більше різниці довжин плечей інтерферометра, можна отримати інтерференційну картину. Беручи до уваги фазовий зсув $\pi 2$, що відбувається на розгалужувачі, дії фазових модуляторів (φ_A і φ_B) і різниця довжин плечей (ΔL), потужність оптичного випромінювання на виході "0" визначається наступною формулою:

$$P_0 = \overline{P} \cdot \cos^2\left(\frac{\varphi_A - \varphi_B + k\Delta L}{2}\right), \qquad (2.1)$$

де k – хвильове число;

P – потужність джерела.

Якщо різниця фаз складає $\pi/2 + \nu\pi$, де n – ціле число, то на виході "0" утворюється деструктивна інтерференція. Тому потужність оптичного випромінювання, що реєструється на виході "0", досягає мінімуму і все оптичне випромінювання реєструється на виході "1". Коли різниця фаз складає $\nu\pi$, ситуація зворотна – на виході "0" спостерігається конструктивна інтерференція, в той час як потужність на виході "1" досягає мінімуму. У разі появи помилки оптичне випромінювання може бути зареєстроване на обох виходах. Цей пристрій працює як оптичний перемикач. Необхідно відзначити, що вкрай важливим є збереження постійної і малої різниці довжин плечей для одержання стійкої інтерференції.

Описана вище поведінка інтерферометра справедливо для класичного оптичного випромінювання. Проте, інтерферометр працює аналогічно для випадку одиночних фотонів. Ймовірність зареєструвати фотон на одному з виходів буде змінюватися зі зміною фази. Незважаючи на те, що фотон веде себе як частинка при реєстрації, він поширюється через інтерферометр як хвиля. Інтерферометр Маха-Цендера – це волоконно-оптичний варіант

експерименту Юнга зі щілинами, в якому плечі інтерферометра аналогічні апертурою. Такий інтерферометр разом з однофотоним джерелом і з ЛФД може бути використаний в квантовій криптографії. Станція Аліса в такому випадку буде містити джерело, перший розгалужувач і перший фазовий модулятор, а станція Боб складатиметься з другого модулятора, розгалуджувача і ЛФД.

Розглянемо застосування до такої схеми протоколу BB84 з чотирьма станами. Аліса може здійснювати один з чотирьох фазових зрушень (0, $\pi/2$, π, $3\pi/2$. Вона зіставляє значенням біта «0» – 0^o і $\pi/2$, а значення біта «1» -π і $3\pi/2$. У свою чергу, станція Боб робить вибір базису, в випадковому порядку зрушуючи фазу на 0 або $\pi/2$, і привласнює біту, що прийшов на фотодетектор, приєднаний до виходу "0" значення «0», а біту, що прийшов на фотодетектор, приєднаний до виходу "1" значення біта «1». Коли різниці фаз рівні 0 або π, то в станціях Аліса і Боб використовуються сумісні базиси і виходять цілком певні результати. У таких випадках станція Аліса може визначити, в якій із фотодетекторов станції Боб потрапить фотон, і, отже, вона може визначити значення біта. Зі свого боку, станція Боб може визначити, яка фаза була обрана станцією Аліса при передачі кожного фотона. У разі, коли різниця фаз приймає значення $\pi/2$ або $3\pi/2$, сторони використовують несумісні базиси, і фотон випадковим чином потрапляє на один з фотодетекторов станції Боб. Всі можливі комбінації фазових станів наведені в таблиці 2.1.

Зауважимо, що для системи вкрай важливо зберігати стабільну різницю довжин плечей інтерферометра протягом сеансу передачі ключа. Ця різниця не повинна змінюватися більш ніж на частку довжини хвилі фотонів. Зміни довжини одного з плечей приведуть до дрейфу фази і виразяться в помилках в переданому ключі.

Таблиця 2.1 – Ілюстрація протоколу BB84 з чотирьма станами для фазового кодування

Станція Аліса		Станція Боб		
Значення біта	φ_A	φ_B	φ_A- φ_B	Значення біта
0	0	0	0	0
0	0	π/2	3π/2	?
1	π	0	π	1
1	π	π/2	π/2	?
0	π/2	0	π/2	?
0	π/2	π/2	0	0
1	3π/2	0	3π/2	?
1	3π/2	π/2	π	1

Незважаючи на те, що дана схема чудово працює в лабораторних умовах, на практиці не представляється можливим збереження довжин плечей в разі, коли користувачі відокремлені один від одного більш ніж на кілька метрів. Беннетт показав, як обійти цю проблему. Він запропонував використовувати два незбалансованих інтерферометра Маха-Цендера, з'єднаних послідовно оптичним волокном.

Однак в комерційних реалізаціях систем квантового розподілу ключів застосовується ще більш складна і досконала схема кодування фазових станів. Дана схема являє собою розподілений интерферометр з автоматичною компенсацією поляризаційних спотворень.

2.1.3 Структура системи з часовим кодуванням

Принципи побудови систем квантової криптографії використовують неортогональні тимчасові інтервали, які запропонував Сергій Молотков з інституту фізики твердого тіла РАН. Для кодування «0» і «1» використовується стан лише з однією просторовою тимчасовою формою, але

зрушеною на різні часові інтервали в кожній посилці. За рахунок цього і досягається неортогональність.

Дана ідея дозволяє спростити волоконно-оптичну частину системи квантової криптографії і повністю відмовитися від застосування інтерферометрів. Запропонована схема дозволяє реалізувати більшість відомих протоколів квантової криптографії (рис. 2.3).

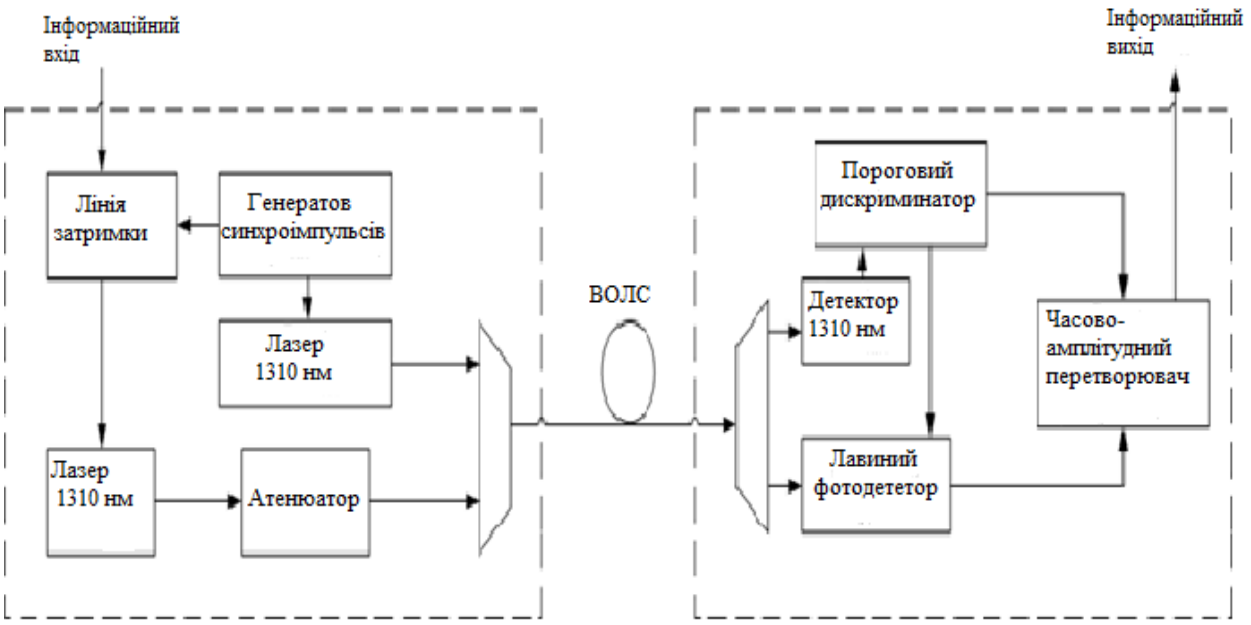


Рисунок 2.3 – Схема оптоволоконної системи квантової криптографії на тимчасових зрушеннях без інтерферометрів

Як однофотонний стан використовується стан, зрушений щодо синхроімпульса, в кожній посилці на певну величину. Синхроімпульсом є короткий оптичний імпульс, що випромінюється лазером з довжиною хвилі 1310 нм. У реалізації використовуються два базису {{+(1), ×(1)} і {+(2), ×(2)}. Всередині першого базису в кожному подбазисі {+(1) і ×(1)}, стан для 0 – |01(+)> і 1 – |11(+), відповідно, в подбазисі 0 – $|0_1(\times)$ × і 1 – $|1_1(\times)>$ – ортогональні. Між підбазисами +(1) і ×(1) стан попарно неортогональний, що досягається відповідними тимчасовими зсувами. Аналогічно і для базису {+(2), ×(2)}.

2.2 Елементна база систем квантової криптографії

Елементна база, що застосовується в системах квантового розподілу ключів, являє собою набір високотехнологічних оптоелектронних модулів. До застосовуваних лазерів пред'являються високі вимоги по точності установки потужності, чистоті спектральних складових і тривалості імпульсів, що генеруються. Для систем квантової криптографії розробляються спеціальні однофотонні джерела випромінювання на квантових точках. Потужність випромінювання на довжині хвилі 1550 нм при частоті проходження імпульсів 5 МГц і одиничному середній кількості фотонів на імпульс становить – 101 дБм. Для реєстрації такого слабкого випромінювання фотодетектори повинні володіти надвисокою чутливістю. На сьогоднішній день для реєстрації одиночних фотонів застосовують лавинні фотодіоди. Однак їх квантова ефективність в інфрачервоній області невелика і складає близько 10 %. У кращих моделей квантова ефективність досягає 3070 %, але вони вимагають азотного охолодження, що не дозволяє застосовувати їх поза лабораторій. Для кодування поляризаційних станів застосовують комірки Поккельса і Керра, що працюють на основі однойменних електрооптичних ефектів. Для кодування фазових станів використовують оптичні фазові модулятори на основі ніобата літію. До обладнання, керуючому електрооптичними пристроями, пред'являються високі вимоги по швидкості впливу. Висока інерційність оптичних атенюаторів не дозволяє досить точно контролювати рівень середньої кількості фотонів в кожному імпульсі. Недосконалість технологічного процесу виготовлення електрооптичних компонентів на сьогоднішній день не дозволяє вивести швидкісні показники квантово-криптографічних систем на якісно новий рівень [5].

2.3 Однофотонні випромінювачі

Випромінювач одиночних фотонів (або однофотонний випромінювач) – це абсолютна межа мініатюризації випромінювачів світла. Визначимо, що він представляє собою: випромінювач одиночних фотонів (ВОФ) – це квантове джерело, в якому під дією керуючого сигналу (і тільки під дією цього сигналу) випромінюється один (і тільки один) фотон. Випромінювання ВОФ характеризується некласичною суб-пуассонівською статистикою, а ідеальний випромінювач одиночних фотонів генерує однофотонні фоковські стани (світловий потік з нульовим шумом). ВОФ може бути реалізований тільки на основі ізольованої квантової системи: одиночного атома, молекули, штучного атома (напівпровідникової квантової точки). Створення ефективних ВОФ є складною науково-технічною проблемою, що включає в себе рішення трьох завдань: локалізація та ізоляція квантової системи; ефективне накачування ізольованою квантовою системою; збору випромінювання.

Випромінювачі одиночних фотонів можуть знайти застосування в системах квантової криптографії і квантових обчислень. Вони також необхідні для прецизійної спектроскопії і створення еталонів оптичної потужності. До теперішнього моменту однофотонне випромінювання (з оптичним лазерним накачуванням) продемонстровано на цілому ряді об'єктів: одиночних атомах і іонах, одиночних молекулах, центрах забарвлення і одиночних напівпровідникових квантових точках. Перевагою напівпровідникових квантових точок є можливість створення випромінювача одиночних фотонів з струмовим накачуванням у вигляді надмініатюрного світлодіода, тобто повністю твердотільного компактного випромінювача. Такий випромінювач реалізований в Інституті фізики напівпровідників СО РАН спільно з берлінським Інститутом фізики твердого тіла (ФТТ). ВОФ містить бреггівський вертикальний мікрорезонатор, який використовується для збільшення зовнішньої квантової ефективності, і шар квантових точок InGaAs низької щільності. На одному квадратному мікроні в середньому

розміщується одна квантова точка. Інжекція струму в шар (поверхність) з квантовими точками здійснюється через оксидну апертуру з субмікронним внутрішнім діаметром, що забезпечує струмове збудження лише однієї квантової точки. Спектр випромінювання містить єдину вузьку лінію, що відповідає рекомбінації екситона, локалізованого в одиночній квантової точці [6].

2.4 Установки з використанням фемтосекундного лазеру

2.4.1 Універсальна фемтосекундна лазерна система PHAROS

PHAROS представляє собою інтегровану фемтосекундну лазерну систему, яка поєднуватиме в собі імпульси з енергією декількох міліджоулей і високою середньою потужністю. Механічна конструкція і оптична схема PHAROS оптимізовані під промислове виробництво, наприклад, точну механічну обробку. [7].

Володіючи самими компактними розмірами серед конкурентів, вбудованою системою температурної стабілізації і герметичній конструкцією, PHAROS можна вбудовувати в промислові системи обробки матеріалів. Використання твердотільних лазерних діодів для накачування кристала Yb (іттербій) значно знижує витрати на технічне обслуговування і збільшує термін служби лазерної системи (рис. 2.4)

Рисунок 2.4 – Універсальна фемтосекундна лазерна система PHAROS

Більшість вихідних параметрів фемтосекундної лазерної системи PHAROS можна регулювати за допомогою пульта управління або ПК, за лічені секунди налаштувавши лазер для роботи в конкретній галузі застосування. Регульованість вихідних параметрів дозволяє використовувати фемтосекундну систему PHAROS в тих областях, де зазвичай потрібні лазери різних класів. Параметри: тривалість імпульсу (190 фс – 10 пс), частота проходження імпульсів 1 кГц – 1000 кГц, енергія імпульсу (до 2 мДж) і середня потужність (до 20 Вт). Вихідної потужності достатньо для обробки на високій швидкості більшості матеріалів. Система комплектується зовнішнім пультом управління для інтеграції її в промислових установках для обробки матеріалів.

Компактна і міцна оптомеханічна конструкція фемтосекундної системи PHAROS складається модулів в термостабілізованих і герметичних корпусах, які забезпечують стабільне функціонування лазера в мінливих умовах роботи, а також з легкістю знімаються. Фемтосекундна система PHAROS поставляється з розширеним пакетом програм для надійної автоматичної роботи і інтеграції в різні системи обробки матеріалів.

У PHAROS застосовується стандартна методика посилення чірпірованного імпульсу, яка включає в себе модуль осцилятора, регенеративного підсилювача і імпульсного розширювача або компресора.

Серед основних особливостей системи слід виділити.

1. Змінна тривалість імпульсу в діапазоні 190 фс – 20 пс.
2. Енергія в імпульсі до 2 мДж.
3. Вихідна потужність до 20 Вт.
4. Змінна частота проходження імпульсів в діапазоні 1 кГц – 1000 кГц.
5. Селектор імпульсів для виведення необхідної послідовності.
6. Міцний і надійний корпус індустріального класу.
7. Автоматизований генератор гармонік (515, 343, 257, 206 нм).
8. Опциональна стабілізація.
9. Можливість синхронізації генератора із зовнішнім джерелом.

Фемтосекундна лазерна система PHAROS заснована по стандартній методиці посилення чірпірованного імпульсу, яка передбачає використання модулів осцилятора, регенеративного підсилювача і розширювача або компресора імпульсів. Осцилятор з пасивною синхронізацією мод видає потужність більше 700 мВт з тривалістю імпульсу менше 80 фс. В якості активного середовища, в регенеративному підсилювачі використовується кристал Yb: KGW. Підсилювач неколінеарно накачується одним або двома (PHAROS, відповідно, на 6 Вт – 15 Вт) модулями накачування – надяскравими діодами оригінальної конструкції компанії Light Conversion, потужність випромінювання яких сягає 60 Вт. Для роботи підсилювача і опціонального пристрою для контролю частоти повторення (pulse-picker) при частоті проходження імпульсів до 200 кГц (з можливістю її підвищення до 1 МГц) використовуються дві комірки Поккельса з малими втратами. Модуль розширювача або компресора імпульсів побудований на основі звичайної пропускної дифракційної решітки, яка демонструє високу ефективність і відмінні можливості з передачі енергії. Всі робочі параметри вузлів системи регулюються з блоку дистанційного керування або ПК, підключеного через USB інтерфейс.

Сфери застосування фемтосекундною системи.

1. Мікрообрабка.
2. Мікро- та наноструктурування.
3. Формування решіток Брегга і хвилеводів.
4. Багатофотонні полімеризація.
5. Нелінійна оптика.
6. Спектроскопія з часовим розширенням.
7. Біомедицина.
8. Мікроскопія [7].

2.4.2 Компактна універсальна фемтосекундна лазерна система CARBIDE

CARBIDE являє собою лазерну систему високої потужності з подвоєною енергією імпульсу промислового класу (для мікрообробки). Система має вихідну потужність до 40 Вт і енергію імпульсу до 800 мкДж. Даний лазер увібрав в себе найкраще від лазерної системи PHAROS: широкий діапазон зміни частоти проходження імпульсів від 60 кГц до 2000 кГц з вбудованим селектором імпульсів і контрольовану тривалість імпульсів в діапазоні від 290 фс до 10 пс (рис. 2.5).

Основні параметри системи.

1. Змінна тривалість імпульсу в діапазоні 290 фс – 10 пс.
2. Енергія в імпульсі до 800 мкДж.
3. Вихідна потужність до 40 Вт.
4. Змінна частота проходження імпульсів в діапазоні 60 кГц – 2000 кГц.
5. Селектор імпульсів для виведення необхідної послідовності.
6. Міцний і надійний корпус індустріального класу.
7. Повітряне або водяне охлоджування.
8. Автоматизований генератор гармонік (515, 343, 257 нм).
9. Аппаратний інтерфейс, підвищуючий гнучкість системи.

Рисунок 2.5 – Ультракомпактна універсальна фемтосекундна лазерна система CARBIDE

Також CARBIDE має ряд нових технологічних особливостей, однією з яких є покращений дизайн резонатора, що підтримує більш швидкий прогрів лазерної системи, що особливо важливо в медичних цілях. Вбудований в порожнину резонатора селектор імпульсів дозволяє знизити загальну вартість і енергоспоживання. Керуюча електроніка, сучасні драйвери лазерних діодів і вбудований комп'ютер забезпечують більш низький рівень електромагнітних шумів. Інші невеликі, але важливі поліпшення дозволили підвищити ефективність перетворення змінного струму, що надходить в джерело живлення, в більш високу середню вихідну потужність лазера.

Сфери використання:

– мікрообрабка;

– мікро- і наноструктурування;

– мікроскопія;

– багатофотонная полімеризація;

– нелінійная оптика;

– спектроскопія з часовим розширенням;

– біомедицина [7].

2.5 Сьогодення та майбутнє квантової криптографії

Перераховані вище проблеми реальних систем квантової комунікації вимагають прийняття спеціальних заходів. Вирішити проблему багатофотонного імпульсу можна шляхом зміни способу кодування сигналу. Наприклад, запропоновані схеми, в яких число фотонів в імпульсі (тобто його енергія) є одним з параметрів стану квантової системи та його зміна при «відведенні» частини квантів, які стають явними.

Для боротьби з помилками системи використовуються різні коди корекції, а для зниження значущості перехоплених бітів – процедура посилення секретності. Крім того, можуть прийматися додаткові заходи захисту чисто технічного характеру. Так, труднощі перехоплення сигналу

можна істотно збільшити, розвести його на кілька шляхів поширення, як в інтерферометрі Маха-Цендера. Можливі й більш складні схеми, в яких розпаралеледьний сигнал мультиплексується з часом в один канал зв'язку. Ці заходи ніяк не обмежують теоретичну можливість перехоплення даних, але надзвичайно ускладнюють практичне здійснення такого перехоплення, роблячи його технічно неможливим на даний момент часу.

На шляху практичної реалізації систем квантової комунікації виникає ряд таких технічних труднощів, як розробка стабільних джерел одиночних фотонів і детекторів одиночних фотонів, які були б працездатні в звичайному діапазоні температур і не потребували охолодження рідкими газами. Крім того, для реального використання важливим є створення так званих plug & play-систем, які починають працювати відразу після включення і не потребують складного юстирування апаратури. Всі ці завдання необхідно вирішити, щоб перейти від експериментальних установок до промислових зразків.

В даний час вже кілька фірм (наприклад, компанії id Quantique, Magic Technologies) пропонують перші комерційні системи квантового розподілу ключів. Ці системи мають подібні характеристики: використання оптоволокна як середовища передачі, максимальна дальність зв'язку в кілька десятків кілометрів і невисока швидкість вироблення ключа (порядку одиниць кілобіт в секунду). З технічної точки зору ці системи ще дуже далекі від досконалості. Основна незручність в їх використанні: необхідність застосування складної фізичної апаратури, яка повинна бути заздалегідь розміщена у кореспондентів, і обмеження середовища передачі даних оптичними каналами. Це робить установку каналу «на вимогу» практично неможливою: як, наприклад, встановити апаратуру на низькоорбітальних супутників, якщо він був запущений без неї або стара апаратура вийшла з ладу?

Очевидно, що за масовістю застосування системи квантової комунікації ще дуже нескоро зможуть наблизитися до асиметричної криптографії:

принаймні до тих пір, поки можливий прорив в квантових обчисленнях або в теорії обчислювальної складності не змінить ситуацію. Швидше за все, цей процес займе не один десяток років, і цілком ймовірно, що ми станемо свідками поступового проникнення квантової криптографії на ринок засобів захисту інформації, починаючи з верхніх сегментів цього ринку. Однак вже зараз системи квантової комунікації можуть знайти застосування для захисту особливо важливих каналів зв'язку або інформаційних магістралей між великими центрами обробки даних, тобто там, де надзвичайно високі вимоги до стійкості або дуже великий трафік.

Активні дослідження в галузі квантової криптографії ведуть GAP-Optique, Mitsubishi, Toshiba, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут, молода компанія MagiQ і холдинг QinetiQ, підтримуваний британським міністерством оборони.

Квантова криптографія як сегмент ринку тільки починає формуватися, і тут поки на рівних можуть грати і світові комп'ютерні корпорації, і невеликі початківці компанії

На закінчення хотілося б сказати, що останні розробки в галузі квантової криптографії дозволяють створювати системи, що забезпечують практично 100 % захисту ключа і ключової інформації. Використовуються всі кращі досягнення щодо захисту інформації як з класичної криптографії, так і з новітньої "квантової" області, що дозволяє отримувати результати, що перевершують всі відомі криптографічні системи. Можна з упевненістю говорити, що в найближчому майбутньому весь криптографічний захист інформації і розподіл ключів будуть базуватися на квантово-криптографічних системах [2].

3 КОДУВАННЯ ІНФОРМАЦІЇ З ДОПОМОГОЮ ФЕМТОСЕКУНДНОГО ЛАЗЕРА

3.1 Фемтосекундний лазер – широкі можливості застосування

Слово «унікальні» давно стало характеристикою властивостей фемтосекундних лазерів. Унікальні характеристики випромінювання фемтосекундних лазерів обумовлюють їх широке застосування в різних областях науки, включаючи фундаментальну. Вражаючі успіхи досягнуті в техніці, медицині, хімії та біології [10].

Не будемо шукати відповіді на меті висвітлити усе різноманіття отриманих на сьогоднішній день результатів. Відзначимо лише принципові моменти, яким зобов'язано це різноманіття. Розвиток лазерів ультракоротких імпульсів, а в даний час отримані імпульси близько 5×10^{-15}с, ініціює застосування, засновані на використанні мінімальної тривалості імпульсу. Це перш за все дослідження надшвидкопротікаючих процесів оточуючого світу, в тому числі світу, створеного руками людини. Для переважної більшості досліджуваних часових процесів імпульси фемтосекундної тривалості є фактично дельтафункцією.

Особливий інтерес фемтосекундні лазери представляють для метрології. Унікальна особливість генерації суперконтиніума в режимі самосинхронізації поздовжніх мод, коли може бути забезпечена їх еквідистантність не гірше, ніж 10^{-16}, відкриває можливість створення частотної "гребінки" (comb) [2]. За допомогою цієї прецизійної "гребінки" можна здійснити не тільки синхронізацію еталонів, що працюють на різних частотах, але і вимірювати абсолютні значення оптичних частот.

Другим принциповим моментом є використання фемтосекундних лазерів в ролі задаючих генераторів одночасно з методом посилення частотномодульованих імпульсів для створення надпотужних лазерних систем тераватного (10^{12} Вт) і петаватного (10^{15} Вт) рівня – CPA-лазерні системи (абревіатура від англіських слів “chirp pulse amplification” [1]).

Поява СРА-лазерних систем стало поворотним моментом у розвитку лазерної техніки, що дало абсолютно нові, раніше недоступні можливості для дослідницької практики. Завдяки їм, тераваттні потужності досягаються на установках настільного типу. На їх основі, створені прискорювачі часток з розмірами від міліметрів до сантиметрів замість розмірів від метрів до сотень метрів для традиційних прискорювачів. Створено компактні надшвидкодіючі джерела іонізуючого випромінювання. СРА-лазери не тільки використовуються в нанотехнологіях, але і отримали самостійний розвиток, який називається фемтотехнологією.

В Інституті плазмової електроніки і нових методів прискорення ННЦ ХФТІ створено фемтосекундний лазер, що генерує на довжині хвилі 800 нм імпульси тривалістю 17,3 фс. На рис. 3.1 показаний зовнішній вигляд фемтосекундного лазера (два ракурсу). В останній модифікації лазерної установки він розміщений в окремому герметичному корпусі (рис. 3.1, лівий).

Рисунок 3.1 – Зовнішній вигляд фемтосекундного лазера (два ракурси)

При створенні фемтосекундного лазера було вжито заходів щодо максимального зменшення вібрацій на конструкцію лазера, здійснений контроль і підтримання температури, вологості і вмістом пилу в робочому обсязі. Загальний робочий об'єм, в якому знаходився фемтосекундний лазер,

обмежувався обсягом "чистої кімнати". Оптична схема фемтосекундного лазера представлена на рисунку. 3.2

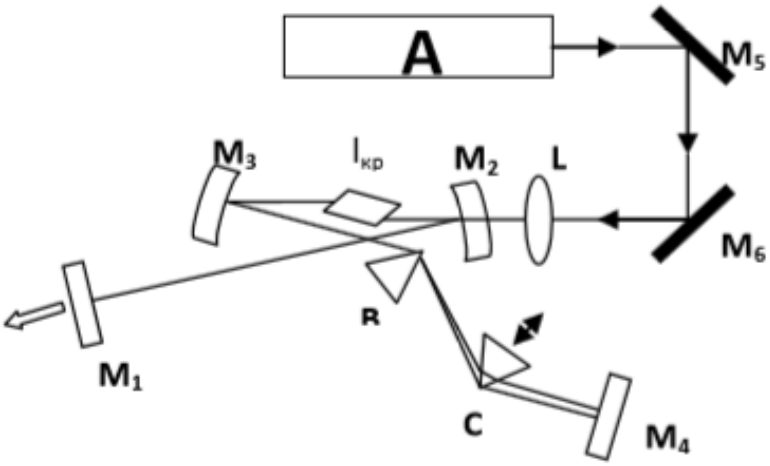


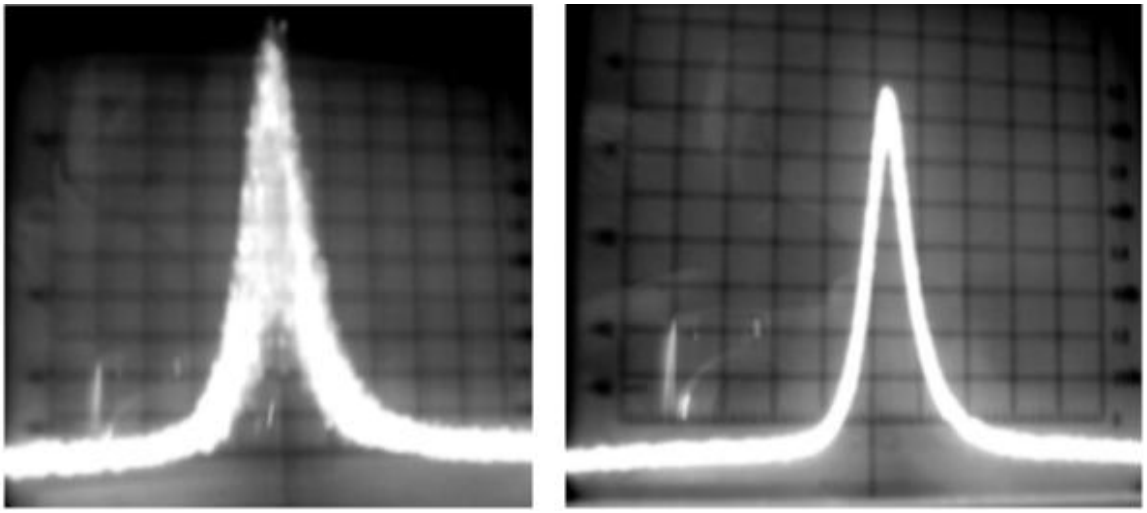
Рисунок 3.2 – Оптична схема фемтосекундного лазера

До складу приведеної системи входять: M_1 і M_4 – вихідний і "глухе" дзеркала; M_2 і M_3 – сферичні дзеркала фокусучого плеча резонатора, в якому знаходиться Ti-Sa кристал $l_{кр}$; M_5 і M_6 – напрямні дзеркала Ar лазера накачування; L – лінза, фокусуюча випромінювання накачування в Ti-Sa кристал; R і C – призми компенсатора дисперсії групової швидкості (ДГС).

Вимоги до довжини Ti-Sa кристала визначаються з необхідності зменшення дисперсії третього порядку. При зменшенні довжини кристала досягається зменшення тривалості імпульсів і збільшення ширини спектра випромінювання лазера, що дуже важливо при використанні фемтосекундного лазера для метрологічних цілей. У нашому випадку довжина Ti-Sa кристала складала величину 5 мм, що забезпечувало ширину спектра випромінювання лазера до 90 нм.

Чудовою особливістю роботи фемтосекундного лазера в режимі самосинхроніізації є отримання стабільної "гребінки" еквідистантних поздовжніх мод. На рисунку 3.3 (а, б) показаний спектр биття поздовжніх мод

лазера на частоті $\Delta f = c/2L = 96,2$ МГц, де c – швидкість світа, L – довжина резонатора лазера.



а) б)

а) спектр биття лазера, працюючого в режимі неперервної генерації, при зміні фази генеруючих мод випадковим чином;

б) спектр биття лазера, працюючого в режимі синхронизації мод.

Рисунок 3.3 – Зображення спектра биття поздовжніх мод лазера

На рисунку 3.3, а сигнал биття флуктуює по частоті і по амплітуді. На рисунку 3.3, б показаний спектр биття лазера, працюючого в режимі синхронізації мод. Тут сигнал стабільний по частоті і амплітуді, а спостережувана ширина спектра сигналу відповідає роздільній здатності аналізатора спектра. Справжня ширина спектра сигналу биття на кілька порядків величини менше спостережуваного на екрані аналізатора спектра.

Прикладом застосування еквідистантної "гребінки" може служити робота, де описана методика вимірювання АЧХ широкосмугових фотоприймачів в діапазоні частот 200 10^9 Гц з точністю 2 % і представлені результати вимірювання АЧХ високошвидкісного фотодіода S5972 фірми “Hamamatsu”.

Характеристики фемтосекундного лазера надають підстави вважати про широкі можливості їх застосування в різних областях науки і техніки. Особливо слід підкреслити привабливість їх реалізації в метрології [4].

3.2 Використання фемтосекундного лазера

Унікальні властивості фемтосекудних лазерів визначають їх найширші застосування в різних облястях науки, техніки і медицини. Ефективність практичного використання ультракоротких імпульсів (УКІ) може і бути обумовлена мінімальною тривалістю імпульсу і пов'язаної з нею малою часовою когерентністю, максимальними піковою потужністю і интесивністю, великими тимчасовою когерентністю і середньою потужністю цуга УКІ. Нижче перераховані основні застосування УКІ із зазначенням ключового параметра характеристики випромінювання. Розглянемо всі можливі застосування, які пов'язані з граничними параметрами випромінювання та реалізовані останнім часом.

Використання в науці.

1. Застосування, засновані на мінімальної тривалості імпульсу:

– нелінійная оптика;

– волоконна оптика, оптичні солітони;

– дослідження надшвидких явищ методом збудження зондування;

– двух- і трьохфотонна мікроскопія;

– фемтохімія;

– терагерцові пучки і когерентна тимчасова Фур'є-спектроскопія.

2. Застосування, засновані на високій когерентності безперервної послідовності УКІ:

– прецизійна спектроскопія, включаючи багатофотонні переходи;

– абсолютні вимірювання оптичних частот, оптичні стандарти частоти;

3. Застосування, засновані на високих потужностях, інтесивності і напруженості полів в світловій хвилі:

– лазерна плазма, джерела рентгенівського випромінювання;

– релятивістський режим взаємодії випромінювання з речовиною;

– прискорення електронів;

– спрямовані пучки ренгенівського і γ-випронінювання;

– експерменти по нелінійній квантовій електродинаміці;

– ініціювання фотоядерних реакцій, швидкий підпал термоядерної реакції.

4. Застосування, пов'язані з високою потужністю імпульсів тривалістю кілька світлових періодів:

– генерація вищих гармонік до рентгенівського діапазону;

– генерація імпульсів і м'якого ренгенівського випромінювання аттосекундної тривалості.

Використання в техніці.

1. Надшвидкодіюча оптоелектроніка; осцилографи з субпікосекундним дозволом.

2. Контроль елементів мікроелектроніці.

3. Волоконно-оптична зв'язок зі швидкістю передачі інформації, приблизно 1 Тбит/с.

4. Прецизійна обробка матеріалів.

5. Системи зображення на терагерцових частотах.

6. Поділ ізотопів.

Використання в медицині.

1. Оптична когерентна томографія.

2. Прецизійна хірургія.

3. Виготовлення кардіологічних мікропротезів.

4. Двухфотонная фотодинамічна терапія [12].

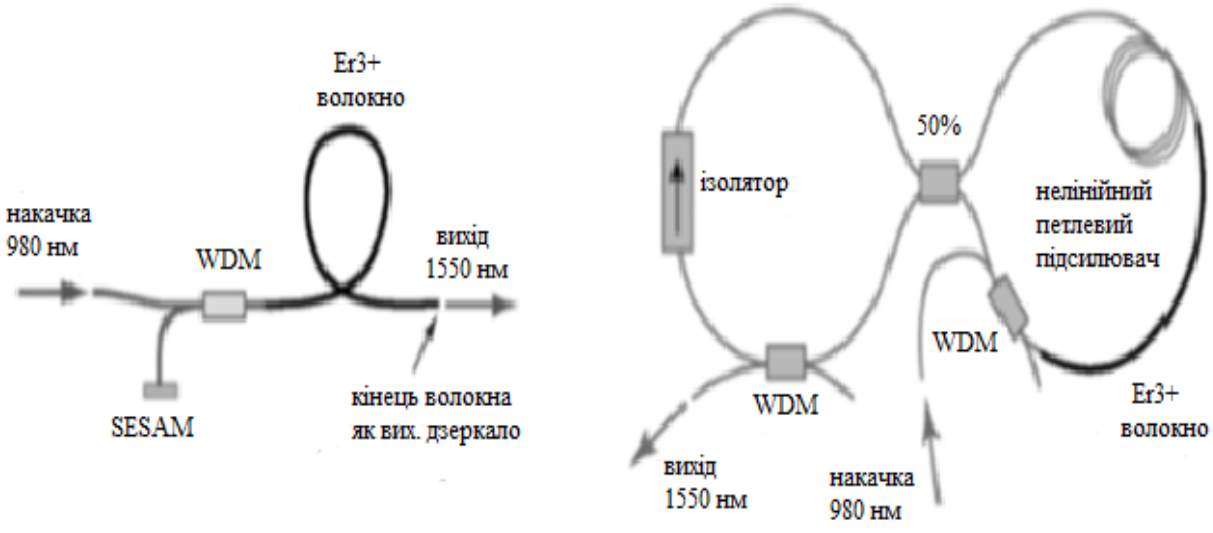
3.3 Волоконні лазери з синхронізацією мод

З ростом числа застосувань лазерів ультракоротких імпульсів, виникає необхідність в компактних, надійних, малошумливих джерелах фемтосекундних імпульсів. Одним з таких джерел є фемтосекундні волоконні лазери, засновані на волокнах, легованих ербієм.

Фемтосекундні волоконні лазери допускають стійку і стабільну роботу без необхідності постійного налаштування системи. Компактність, низька вартість і стабільність фемтосекундних волоконних лазерів надає можливість кожній дослідній лабораторії мати фемтосекундне джерело без необхідності покупки додаткового дорогого і складного устаткування. Фемтосекундні волоконні лазери з довжиною хвилі 1550 нм використовуються в оптичній телекомунікації, так як ця довжина хвилі добре узгоджуватися з вікном прозорості кварцових оптичних кабелів.

Перша генерація фемтосекундних імпульсів з використанням волоконного лазера була здійснена в 1990 році. Мінімальна тривалість лазерів на волокні досягає приблизно 10 фс. В даний час велика кількість комерційних фірм у всьому світі випускає волоконні лазери з тривалістю імпульсів від 100 фс до 1 пс. Найбільш поширеними фемтосекундними волоконними лазерами є Er-лазери. У порівнянні з титан-сапфіровим лазером вони мають такі переваги: 1) більш компактні; 2) менш дорогі; 3) генерація на довжині хвилі 1,55 мкм потрапляє у вікно прозорості оптичних ліній зв'язку.

На рисунку 3.4 представлені дві основні оптичні схеми, які використовуються в волоконних фемтосекундних лазерах. Лазер, побудований за схемою на рис. 3.4, а використовує лінійний резонатор Фабрі-Перо, а за схемою на рис. 3.4, б – кільцевий резонатор. Лазери, що використовують кільцевой резонатор, більш чутливі до якості волокна і температурі, але дозволяють генерувати фемтосекундні імпульси без використання насичувального поглинача, що значно спрощує конструкцію лазера.



а) б)

а) лазер з лінійним резонатором і насичувальним поглиначем;

б) кільцевій лазер з пасивною синхронізацією мод.

Рисунок 3.4 – Схема волоконного лазера з синхронізацією мод

Як лінійна, так і нелінійна зміна поляризації випромінювання, що поширюється через оптичне волокно, є основою генерації фемтосекундних імпульсів більшості волоконних лазерів [13].

3.4 Розрахунок загасання випромінювання в волокні і відкритих системах

Перспективним являється використання фемтосекундних лазерів ІЧ-діапозону для рішення задач квантової криптографії. Далі в роботі приведений розрахунок дозволяючий оцінити дальність передачі сигналу без проміжного посилення.

Відсутність систем проміжного посилення сигналу є обов’язковою умовою створення систем квантового кодування, так як посилення сигналу, який несе квантову заплутаність, веде до його порушення.

Втрати потужності оптичного сигналу при його поширенні в оптичному волокні обумовлені різними механізмами взаємодії світлових хвиль з матеріалом серцевини і оболонки волокна. Основними причинами втрат в світловодах є розсіювання і поглинання енергії.

Поглинання світла в оптичних волокнах визначається:

– власним поглинанням матеріалу світловода;

– поглинанням домішок;

– поглинанням на атомних дефектах;

Власне поглинання матеріалу світловода обумовлено коливальними смугами в ультрафіолетовій і найближчій інфрачервоній області. Їх вплив може поширюватися на довжину хвилі $\lambda = 0,7 - 1,1$ мкм. При домішковому поглинанні основну роль грають іони металів: заліза, хрому, міді та гідроксильної групи.

Атомні дефекти виникають при тепловій обробці або опроміненні оптичного волокна. Ця складова втрат може бути значно зменшена і навіть зведена до нуля при виборі матеріалу оптичного волокна.

При монтажі кабелю можуть створюватися вигини світловода, його деформація, що призводить до додаткових втрат. Повне ослаблення енергії при передачі через оптичне волокно визначиться як сума всіх перерахованих вище складових:

$$\alpha_K = \alpha_p + \alpha_n + \alpha_{доп}, \qquad (3.1)$$

де α_K – загасання оптичного волокна, дБ км

α_p – загасання оптичного волокна, яке визначається втратами на розсіюванні, дБ/км;

α_n – загасання оптичного волокна, яке визначається втратами на поглинанні, дБ/км;

$\alpha_{доп}$ – додаткові втрати, дБ/км.

Однією з основних характеристик оптичного волокна є коефіцієнт ослаблення (загасання) – це величина загасання на одиницю довжини волокна і виражається в дБ/км. Коефіцієнт загасання в оптичному волокні обумовлюється власними втратами волокна і виражається у вигляді:

$$\alpha = \alpha_p + \alpha_n, \tag{3.2}$$

де α_p і α_n – коефіцієнти загасання оптичного волокна за рахунок розсіювання і поглинання енергії в волок.

З вищесказаного випливає, що α залежить від довжини хвилі переданого випромінювання. Чим коротше довжина хвилі, тим вище розсіювання світла. Між максимальними значеннями α знаходяться вікна прозорості, в яких ослаблення порівняно невелике. Збільшення α на довжинах хвиль більше 1,8 мкм обумовлені інфрачервоним поглинанням.

Розрахунок складової коефіцієнта втрат за рахунок розсіювання. Загасання на розсіюванні обумовлене неоднорідностями матеріалу і тепловими флуктуаціями показника заломлення. Величина a_p визначається за формулою:

$$\alpha_p = 4,34 \cdot \frac{8 \cdot \pi^3}{3 \cdot \lambda^4} \cdot (n_1^2 - 1) \cdot K \cdot T \cdot \chi \cdot 10^3, \text{ дБ/км} \tag{3.3}$$

де K – постійна Больцмана, $K = 1,38 \cdot 10^{-23}$, Дж/К;

T – температура переходу скла в тверду фазу, $T = 1500°$, К;

χ – коефіцієнт стисливості, $\chi = 8,1 \cdot 10^{-11}$, м^2/н;

n_1 – показник заломлення серцевини волокна;

λ – довжина хвилі, мкм.

Підставивши всі значення в формулу, ми отримаємо:

$$\alpha_p = 4,34 \cdot \frac{8 \cdot \pi^3}{3 \cdot \lambda^4} \cdot (n_1{}^2 - 1) \cdot K \cdot T \cdot \chi \cdot 10^3 = 4,35 \cdot \frac{8 \cdot 3,14^3}{3 \cdot \ 1,55 \cdot 10^{-6}{}^4} \cdot$$
$$\cdot (1,46085458^2 - 1) \cdot 1,38 \cdot 10^{-23} \cdot 1500 \cdot 8,1 \cdot 10^{-11} \cdot 10^3 = 0,118311. \quad (3.4)$$

Розрахунок складової коефіцієнта втрат за рахунок поглинання. Загасання на поглинанні пов'язано з втратами на діелектричну поляризацію і істотно залежить від властивостей матеріалу оптичного волокна. Величина α_n визначається за формулою:

$$\alpha_n = \frac{\pi n_1 t_\delta}{\lambda} \cdot 4,34 \cdot 10^3, \text{ дБ / км} \quad (3.5)$$

де t_δ – тангенс кута діелектричних втрат світловода, $t_\delta = 2,4 \cdot 10^{-12}$

Підставивши значення в формулу, отримаємо:

$$\alpha_n = \frac{\pi n_1 t_\delta}{\lambda} \cdot 4,34 \cdot 10^3 = \frac{3,14 \cdot 1,46085458 \cdot 2,4 \cdot 10^{-12}}{1,55} \cdot 4,34 \cdot 10^3 =$$
$$= 0,03082 \quad (3.6)$$

Отже, сумарний коефіцієнт загасання в оптичному кабелі може бути розрахований за формулою:

$$\alpha = \alpha_p + \alpha_n = 0,149131, \text{ дБ / км} \quad (3.7)$$

Облік молекулярного розсіювання має сенс тільки на коротких хвилях, починаючи ж з довжини хвилі 0,55 мкм втрати на молекулярному розсіюванні зазвичай не враховують. У відкритих оптичних системах зв'язку світло поширюється у вільному середовищі – в атмосфері або в космічному просторі. При обліку тільки дифракційних ефектів розбіжність світла

потужністю P_R випромінювання, що падає на фотоприймач, описується рівнянням дальності:

$$P_R \approx 0,45 \frac{P_A \tau d^2 D^2}{R^2 \lambda^2}, \tag{3.8}$$

де P_A – потужність випромінювання;

τ – коефіцієнт пропускання середовища поширення;

d и D – лінійна апертура (діаметр дзеркал), відповідно, передавальною і приймальною оптичних систем;

R – відстань;

λ – довжина хвилі випромінювання.

Числовий коефіцієнт відповідає розмірностям зазначених величин в системі СІ.

Коефіцієнт пропускання атмосфери дорівнює:

$$\tau = e^{-\alpha R}. \tag{3.9}$$

де коефіцієнт α дорівнює сумі коефіцієнта поглинання Бугера α_B і коефіцієнта розсіювання α_S

$$\alpha = \alpha_B + \alpha_S. \tag{3.10}$$

Коефіцієнт поглинання α_B для атмосфери помітно залежить від довжини хвилі випромінювання, і досягає мінімуму лише в кількох «вікнах прозорості» в околицях довжин хвиль 0,4 мкм – 0,8; 1,5; 2; 3,5; 10,5 мкм. Коефіцієнт розсіювання α_S дорівнює сумі коефіцієнтів розсіювання Релея α_{SR} і розсіювання Мі α_{SM}:

$$\alpha_S = \alpha_{SR} + \alpha_{SM}. \tag{3.11}$$

Розсіювання Релея є розсіювання світла на частинках, розміри яких набагато менше довжини світлової хвилі, і його вплив найбільш помітно в області коротких довжин хвиль,

$$\alpha_{SR} = 0,83\frac{NA^3}{\lambda^4}, \tag{3.12}$$

де A – площа поперечного перерізу частинок-розсіювачів,

N – щільність розсіювачів.

Емпірична формула для коефіцієнта розсіювання Мі (розсіювання на частинках розмірами набагато більшими, ніж λ) має вигляд:

$$\alpha_{SM} = \frac{3,9}{\gamma}\left(\frac{\lambda}{0,55}\right)^{-0,58\gamma^{1/3}}, \tag{3.13}$$

де γ – метеорологічна дальність бачення, км.

Коефіцієнт молекулярного розсіювання $\tau_p(\lambda)$, при оптичній товщині $\sigma_p(\lambda)$ = 1,327 10^{-4}, км$^{-1}$ дорівнює $\tau_p(\lambda)$ =0,0011 (при λ = 1,55 мкм) [14]. Ослаблення випромінювання з міжнародного коду видимості на довжині траси 50 км при дуже чистому повітрі становить 0,19 дБ/км [15].

Енергетичні втрати оптичних сигналів, зумовлені молекулярним розсіюванням, можуть бути визначені з великою точністю, якщо відомо розподіл щільності по висоті. Зазвичай прийнято вважати, що до висот 30 км досить добре виконується умова стандартної моделі атмосфери. На великих висотах щільність атмосфери може істотно змінюватися в залежності від місця і часу, відповідно будуть змінюватися і коефіцієнти молекулярного розсіювання. Однак при будь-якій зміні завжди залишається той факт, що

енергетичними втратами за рахунок релеєвського розсіювання в інфрачервоній області можна знехтувати.

На дальність і надійність відкритих систем зв'язку в атмосфері помітно впливають метеорологічні умови: туман, дощ, сніг, дим, турбулентність атмосфери та ін. Для великих відстаней (кілометри і більше), внаслідок явищ рефракції і розсіювання, ускладнюється проблема точного наведення світлового променя на фотоприймальну систему, а також впливу фону (розсіяне випромінювання, небесні світила). Сучасні наземні відкриті системи зв'язку великої, понад 10 км, протяжності діють, в основному, в діапазоні довжин хвиль близько 10,6 мкм в режимі когерентного фотодетектування сигналу. Більш перспективно, з точки зору дальності зв'язку, застосування таких систем в космосі. У міських умовах, при дальності зв'язку близько 1 км, зручний діапазон довжин хвиль передачі сигналів знаходиться в області 0,8 мкм – 0,9 мкм [14].

Очевидно, що слабкі однофотонні сигнали будуть в значній мірі схильні до описаних перешкод, тому різко знизиться швидкість і відстань ефективної передачі. Щоб вирішити цю проблему були запропоновані схеми квантової криптографії, що використовують супутники на різних орбітах від 300 км до 30000 км. Ефективність передачі в даному випадку зростає через те, що щільність атмосфери падає з ростом висоти над Землею і втрати при досягненні фотоном супутника, що знаходиться на 300-кілометровій орбіті можна порівняти з втратами при проходженні 10 км – 15 км у поверхні планети.

ВИСНОВКИ

Метою данной атестаційної роботи є розвиток оптичних методів кодування інформації. Для досягнення мети в роботі були поставлені такі завдання: дослідити принципи оптичного кодування інформації та можливість застосування фемтосекундних лазерів в оптичному кодуванні.

В процесі виконанні атестаційної роботи було досліджено фізичні та математичні основи оптичного кодування інформації. Розібрано основні теореми теорії інформації: теорему Шенонна та теорему Котельнікова.

Аналіз публікайції показав, що до перспективних методів кодування відноситься квантова криптографія. До переваг цього методу можна віднести фізичний принцип шифрування інформації (традиційні методи криптографії основані на математичних алгоритмах) та квантова заплутаність станів, що суттєво зменшує вирогідність несанкціонованого перехоплення та декодування. Розглянуто типові структури квантових систем розподілу ключів, а саме поляризаційна, фазова та часова системи кодування.

У работі в якості джерела світла систем кодування запропоновано застосування фемтосекундного лазера. Розглянуто принцип роботи та схему використання фемтосекундного лазера, унікальні властивості та приклади застосування в різних областях науки, техніки і медицини. Продемонстровано дві установки з використанням фемтосекундного лазеру PHAROS та CARBIDE.

Виконано розрахунки розповсюдження оптичного імпульсу у відкритому середовищі та оптичному волокні. Розраховано коефіцієнт затухання сигналу в атмосфері та хвилеводах. При довжині хвилі $\lambda = 1,55$ мкм отримані такі результати: у волоконно-оптичних лініях зв'язку: $\alpha = 0,149131$ дБ/км; у атмосфері: $\alpha = 0,19$ дБ/км.

Результати роботи свідчать про перспективність використання фемтосекундних лзерів у системах квантової криптографії.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Головань Л. А., Заботнов С. В. Измерение длительности фемтосекундных лазерных импульсов: учеб. пособ. Москва: МГУ имени М.В. Ломоносова, 2014 г. 32 с.

2. «Оптичні інформаційні системи» для студентів усіх форм навчання спеціалізацій: лазерна і оптоелектронна техніка, фотоніка та оптоінформатика. Конспект лекцій з дисципліни ХНУРЕ / Курський Ю.С., Харків, 2017. 62 с.

3. Курочкин В.Л. Экспериментальная установка для квантовой криптографии с одиночными поляризованными фотонами // Журн. технической физики. 2005. Т. 75, № 12. С. 54 – 58.

4. Волосатова Т. М., Чичварин Н. В. Моделирование квантовых линий связи, // Вопросы кибербезопасности Т 11, №3. 2015.

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

6. Гайслер В. А. Фотоны поштучно // «Наука в Сибири», 2010. № 50. С. 8.

7. Фемтосекундные Yb:KGW лазеры PHAROS Light Conversion // ООО «Промэнерголаб». 2005-019 URL: https://www.czl.ru/catalog/lasers/light-conversions-pharos/pharos.html (дата звернення: 25.11.2019).

9. Крюков П.Г., Лазеры ультракоротких импульсов // Квантовая электроника, 2001, Т. 31. С. 95 – 119.

10. Поврозин А.И., Онищенко И.Н. Фемтосекундный лазер – широкие возможности применения // Журн. метрологія. Харьков, 2014, С. 8.

11. Udem T., Reithert J .// Optics Lrtts, 1999, Т 24. P. 881.

12. Крылов В. Н., Смолянская О. А., Фемтосекундная оптика и фемтотехнологии: Методические материалы к экспериментальному практикуму.СПб: СПбГУ ИТМО, 2009. 83с.

13. Гнатенко А. С. Обеспечение синхронизации мод в волоконных кольцевых лазерах // Журнал нано- та електронної фізики 2018. Т 10, № 2, С. 8.

14. Дмитриев А. Л. Оптические системы передачи информации: учеб. СПб.: СПбГУИТМО, 2007. 96 с.

15. Расчет атмосферного канала // ЦНИТ. URL: http://www.novsu.ru/file/1207543 (дата звернення: 23.11.2019).

16. Данные о распространении радиоволн, требуемые для разработки наземных оптических линий для связи в свободном пространстве / Рек. МСЭ-R P.181,. 2007. 17 с.

17. Juan Yin, Yuan Cao, Yu-Huai Li Satellite-based entanglement distribution over 1200 kilometers / Science. 2017. P. 24.

18. Способ генерации секретных ключей с помощью перепутанных по времени фотонных пар: пат. 2566335 Россия, ООО «ЛОЭП» / Проценко И.Е., Сайгин М. Ю., Фирсов В. В.– №2014113183/08; заявл. 04.04.2014; опубл. 10.10.2015.

19. Wei Zhang, Dong-Sheng Ding Quantum Secure Direct Communication with Quantum Memory // Physical Review Letters. 2017. Vol. 118.