НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Сучасний стан досліджень квантових оптичних систем зв'язку»

Виконав:
студент ІІ курсу, групи ТС-з71мп
Тавер Станіслав Вячеславович _____

Керівник:
Доктор технічних наук, професор,
Трубін Олександр Олексійович _____

Рецензент:
Доктор технічних наук, доцент,
_____ _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2018 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійної програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Таверу Станіславу Вячеславовичу

1. Тема дисертації «Сучасний стан досліджень квантових оптичних систем зв'язку», науковий керівник дисертації Трубін Олександр Олексійовчи, д.т.н., професор, затверджені наказом по університету від «06» квітня 2018 р. №1105-с

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження архітектура квантової одно фотонної мережі

4. Предмет дослідження одиночні фотони

5. Перелік завдань, які потрібно розробити

- Огляд принципів побудови однофотонних систем зв’язку;
- Аналіз структури, принципів функціювання, застосування, переваг та недоліків протоколів передачі фотонів;
- Оптимальна схема мережі та протоколи, які забезпечують конфіденційність передачі;
- Можливість виявлення наявності в каналі перехоплювачів в каналі звязку;
- Прилад для виявлення перехоплювачів інформації в лінії зв’язку.

- 6. Орієнтовний перелік графічного (ілюстративного) матеріалу

- Плакат №1 «Тема, мета та завдання магістерської дисертації»
- Плакат №2 «Постановка задачі»
- Плакат №3 «Квантове розподілення ключа»
- Плакат №4 «Протоколи кодування»
- Плакат №5. «Опис роботи та застосування квантового рефлектометра»
- Плакат №6. «Висновки»
- 7. Орієнтовний перелік публікацій
- Заявка на патент від
- 8. Дата видачі завдання 10 вересня 2016 р.
- Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Огляд науково-технічної літератури, визначення недоліків досліджень та мети дипломної роботи	01.09.2016- 31.12.2016	
2	Вивчення квантових властивостей фотонів та однофотонних пристроїв для систем звязку	10.01.2017 - 29.02.2017	
3	Поглиблене вивчення квантових технологій зв'язку в курсе «Перспективні технології в телекомунікаційних системах»	01.03.2017 – 30.07.2017	
4	Вивчення станів фотонів та огляд пристроїв однофотонної мережі	01.08.2017 – 31.10.2017	
5	Огляд і аналіз методів кодування одиночних і заплутаних фотонів	01.11.2017 – 30.01.2018	
6	Розробка методів зондування мережі з використанням запутаних фотонів	01.02.2018 – 31.03.2018	
7	Використання методів зондування за допомогою заплутаних фотонів, розрахунки можливих втрат в середовищі передачі інформації	01.04.2018 – 30.04.2018	
8	Узагальнення результатів досліджень, підготовка звіту. Подання роботи та її захист	01.05.2018 - 20.05.2018	

- Студент С. В. Тавер
- Науковий керівник дисертації О. О. Трубін

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

КРК – квантове розподілення ключів;

ВК – виправлений ключ;

ПВК – перехоплений виправлений ключ;

ДОФ – джерело одиночних фотонів;

ІЧ – інфрачервоне;

ФЕП – фотоелектронний перемножував;

ЛФД – лавинний фотодіод;

ВАХ – вольт-амперна характеристика;

ЯП – ячейка Поккельса;

ПСД – поляризаційний світло дільник;

ФМ – фазовий модуль;

СР – короткоперіодичні надрешітки;

НЧ – низькі частоти.

ВСТУП

Розвиток людства і постійний обмін інформацією – основа прогресу. Обсяг та надійність передачі є основними показниками розвитку країни. Під час стрімкого розвитку технологій дуже важко уявити життя без засобів передачі інформації, не говорячи вже про науку та управлінську діяльність. В усі часи людство потребувало надійних та конфіденційних засоби передачі даних.

В останні два десятиліття минулого і на початку поточного століття відбувається зміна епохи індустріально-технологічного розвитку передових держав епохою інформаційно-технологічної. Яскравим проявом цього процесу є небачений за швидкістю і результатами прогрес у створенні нових методів і засобів телекомунікацій. Бурхливий розвиток технології виробництва систем і засобів зв'язку з практично необмеженої пропускною здатністю і дальністю передачі і масове їх використання по суті привели до інформаційно-технологічної революції і формування глобального інформаційного суспільства.

Телекомунікаційні системи вдосконалюються кожного дня, починаючи від звукових та візуальних пристроїв і закінчуючи системами автоматичного обміну, які забезпечують обмін інформацією на необмежені відстані в межах Землі.

Сьогодні телекомунікації - це одна з найбільш швидко високотехнологічних і наукомістких галузей світової економіки. Рівень розвитку технологічних розробок, виробництва і впровадження в різні сфери діяльності телекомунікаційних систем багато в чому формують позитивний образ передового суспільства. Такий розвиток подій став можливим завдяки широкому практичному використанню досягнень фундаментальних наук - перш за все фізики, хімії та математики, а також комп'ютерних технологій.

Збільшення обсягу і швидкості передачі інформації в високопродуктивних інтелектуальних мережах вимагає розробки відповідних

технічних засобів, серед яких оптика і оптичні методи передачі сигналів грають найважливішу роль.

РОЗДІЛ 1. ФІЗИКА КВАНТОВОЇ ІНФОРМАЦІЇ: ОСНОВНІ ПОНЯТТЯ

1.1. Історія розвитку та особливості оптичних систем зв’язку

Принцип суперпозиції грає центральну роль у всіх розглядах квантової інформації, як і в більшості уявних експериментів і парадоксів квантової механіки. Замість того, щоб вивчати його теоретично або визначати його абстрактно, ми обговоримо тут експеримент, який є квінтесенцією принципу квантової суперпозиції - експеримент з двома щілинами.

Згідно Фейнману, він «містить в собі серце квантової механіки». Необхідні складові цього експерименту - це джерело, діафрагма з двох щілин, і екран, на якому ми спостерігаємо інтерференційну картину. Природу цієї інтерференційної картини можна легко зрозуміти, якщо виходити з хвильових властивостей частинок, що вилітають з джерела. Тут можна помітити, що експеримент з двома щілинами проводився з частинками різних типів, від фотонів [2] і електронів [3] до нейтронів [4] і атомів [5]. З точки зору квантової механіки, стан на екрані - це когерентна суперпозиція

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\Psi_a\rangle + |\Psi_b\rangle), \qquad (1.1.1)$$

де $|\Psi_a\rangle$ та $|\Psi_b\rangle$ описують квантовий стан в тому випадку, якщо відкрита тільки щілина a чи щілина b.

Цікава властивість експерименту з двома щілинами, підтверджена у всіх експериментах, полягає в тому, що, інтерференційну картину можна зібрати по одній частці - тобто, встановивши настільки низьку інтенсивність джерела, що кожна частка буде інтерференціювати тільки сама з собою. В цьому випадку у нас з'являється спокуса запитати себе, через яку з двох щілин частка пролітає «насправді». Стандартна квантова механіка відповідає на це, що неможливо дати будь-якої розумну відповідь на питання «через яку щілину пролітає частинка?» Не використовуючи відповідні експериментальні методи, здатні дати відповідь на це питання.

Насправді, якби нам треба було поставити експеримент, який визначає, через яку щілину пролітає частинка, нам би довелося тим чи іншим чином взаємодіяти з часткою, що призвело б до декогерентності - тобто, до втрати інтерференції. Ми можемо спостерігати інтерференцію тільки тоді, коли навіть в принципі немає можливості дізнатися, через яку з щілин пролітає частинка. В якості невеликого застереження, зазначимо, що також невірно говорити, що частка пролітає через обидві щілини одночасно, хоча таке твердження можна нерідко почути.

Проблема тут в тому, що, з одного боку, це суперечливо, оскільки частка - це локалізований об'єкт, і, з іншого боку, таке твердження не несе сенсу з точки зору розглянутої операції. Відзначимо також, що можна отримати часткове знання про те, через яку з щілин пролітає частинка, за рахунок часткової втрати когерентності.

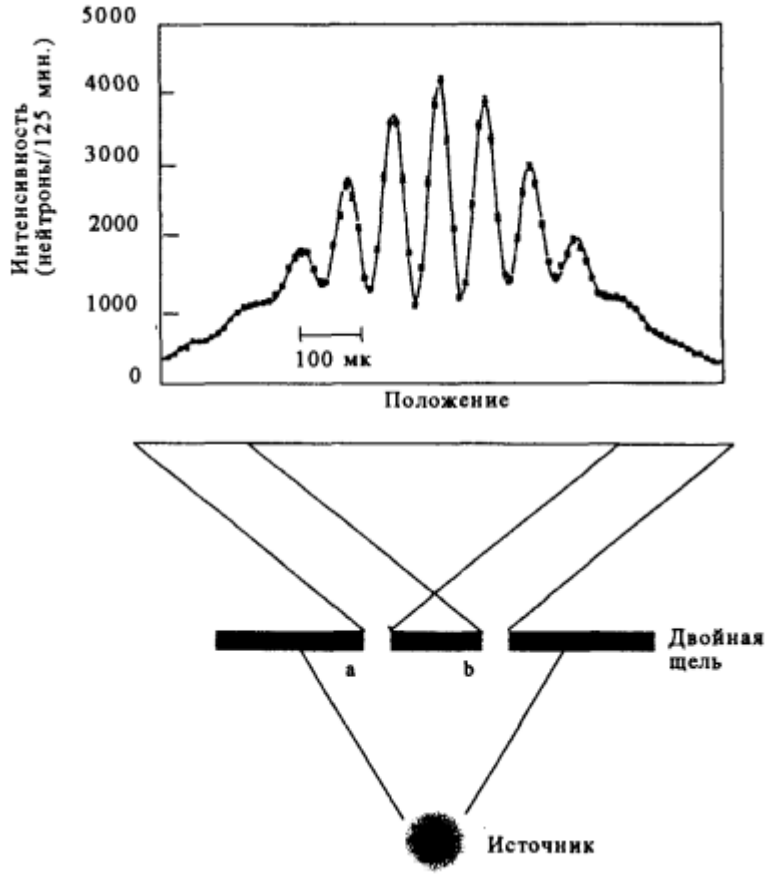

Рисунок. 1.1.1 Принцип експерименту з двома щілинами. Інтерференційна картина виникає в площині спостереження за двохщілистими

діафрагмами, навіть якщо інтенсивність джерела настільки мала, що в апараті одномоментно знаходиться тільки одна частинка. Показана тут інтерференційна картина була отримана в реальних експериментах на двох щілинах з нейтронами [4].

1.2. Кубіти

Найбільш фундаментальна величина в науці про інформацію - це біт. Це система, яка може приймати два значення, «0» і «1». У класичній реалізації, біт, який можна собі уявити, наприклад, просто механічним перемикачем, є система, що має два чітко помітних стани. Між ними повинен бути досить великий енергетичний бар'єр, щоб система не могла спонтанно переходити з одного стану в інший, що було б, очевидно, згубним ефектом.

Кубіт [6], квантовий аналог біта, отже, повинен також бути системою з двох станів: $|0\rangle$і $|1\rangle$. Кубітом може служити практично будь-яка квантова система, що має, щонайменше, два стани. Можна придумати безліч варіантів таких систем, і багато які з них вже були реалізовані експериментально. Найбільш необхідна риса квантових станів, які використовуються в якості бітів, - це властивості когерентності і суперпозиції. При цьому довільний стан виражається як

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (1.2.1)$$

Де $|\alpha|^2 + |\beta|^2 = 1$. Це означає не те, що значення кубіта лежить десь посередині між «0» і «1», але те, що кубіт знаходиться в когерентної суперпозиції двох станів, і, якщо ми його виміряємо, то знайдемо, що кубіт з ймовірністю $|\alpha|^2$ несе значення «0», і з імовірністю $|\beta|^2$ значення «1»:

$$p("0") = |\alpha|^2,\ p("1") = |\beta|^2 \qquad (1.2.2)$$

Незважаючи на те, що, за визначенням кубіта, його властивості здаються невизначеними, важливо розуміти, що (1.1) описує когерентну суперпозицію, а

не некогерентного суміш «0» і «1». Важлива відмінність між ними полягає в тому, що для когерентної суперпозиції завжди існує базис, в якому значення кубіта чітко визначено, тоді як некогерентна суміш - це суміш, яким би чином ми її не описували. Для простоти, розглянемо конкретний стан

$$|Q'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \qquad (1.2.3)$$

Це, очевидно, означає, що з 50% ймовірністю кубіт буде знайдений в стані або «0», або «1». Цікаво що в базисі, повернутому в гільбертовому просторі на 45%, значення кубіта чітко визначено. Цей факт можна побачити, застосувавши до кубіта відповідне перетворення. Одне з основних перетворень в науці про квантову інформацію - це так зване перетворення Ада- мара, яке діє на кубіт наступним чином:

$$H|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), H|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \qquad (1.2.4)$$

Застосувавши його до кубіти $|Q'\rangle$, отримаємо

$$H|Q'\rangle = |0\rangle \qquad (1.2.5)$$

тобто, певне значення кубіта. Це було б неможливо зробити з некогерентного сумішшю.

1.3. Перетворення одного кубіта

Можна зрозуміти одну з найбільш базових експериментальних операцій у фізиці квантової інформації, розглянувши дію простого дільника, який ділить промінь у відношенні 50/50. Такі дільники були реалізовані для частинок різних типів, не тільки для фотонів. Для довільного дільника, досліджуємо випадок двох вхідних мод і двох вихідних - так, як це показано на Рис. 1.3.1.

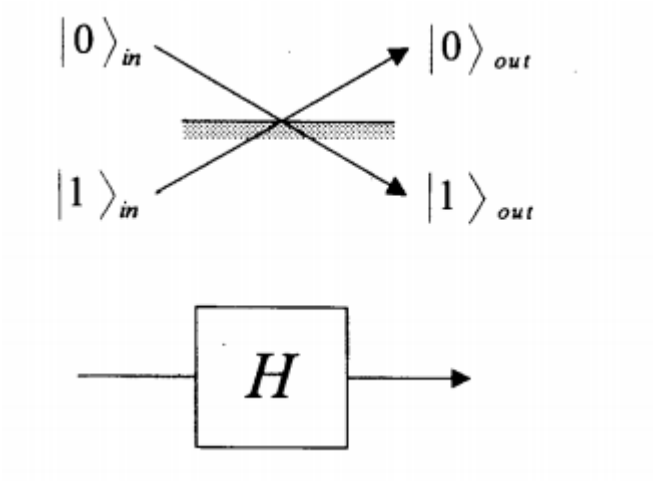

Рисунок. 1.3.1. Дільник 50/50 (вгорі) і відповідна діаграма, що позначає перетворення Адамара (знизу).

Частка, що падає згори або знизу на дільник 50/50, з'явиться або в верхньому, або в нижньому промені, що виходить, з однієї і тієї ж 50% ймовірністю. Тоді з умови квантової унітарності - тобто, з умови, що частинки не втрачаються, якщо дільник їх не поглинає, - ідуть певні фазові умови на дію подільника [7], з однією вільною фазою. Можна дуже просто описати фазову дію подільника, зафіксувавши фазові співвідношення так, що вона буде описуватися перетворенням Адамара (1.4).

Знову припустимо, що стан на вхід - це довільний кубіт:

$$|Q\rangle_{in} = \alpha|0\rangle_{in} + \beta|1\rangle_{in}. \qquad (1.3.1)$$

Для випадку однієї частинки це означає, що α - це амплітуда ймовірності виявити частинку, падаючу на дільник зверху, а β - амплітуда ймовірності виявити частинку, падаючу знизу. Тоді в результаті дії дільника виходить кінцевий стан:

$$|Q\rangle_{out} = H|Q\rangle_{in} = \frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle_{out} + (\alpha-\beta)|1\rangle_{out}), \qquad (1.3.2)$$

так що амплітуда ймовірності знайти частку в верхньому вихідному пучку дорівнює тепер $(\alpha + \beta)$, а амплітуда ймовірності знайти її в нижньому пучку дорівнює $(\alpha - \beta)$.

Зокрема, якщо α = 0 або β = 0, то видно, що частку можна з однаковою ймовірністю виявити в будь-якому з пучків. В іншому окремому випадку, α=β, частка буде обов'язково виявлена в верхньому пучку, і ніколи не буде виявлена в нижньому.

Цікаво і корисно розглянути послідовності таких дільників, оскільки вони здійснюють послідовності перетворень Адамара. Для двох послідовних перетворень використовується інтерферометр Маха-Цандера (Рис. 1.3.2) з двома однаковими дільниками.

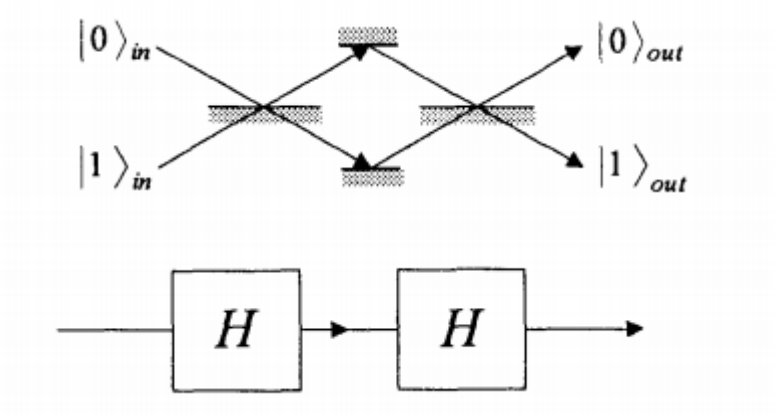

Рисунок. 1.3.2. Інтерферометр Маха-Цандера (вгорі) і послідовність з двох перетворень Адамара (внизу).

Зображені на малюнку дзеркала, потрібні тільки для того, щоб перенаправити пучки. Передбачається, що вони однаково діють на два пучка, і, отже, при аналізі їх можна не враховувати. Тоді повну дію інтерферометра можна описати просто як два послідовних перетворення Адамара, що діють на довільний стан на вході (1.3.2):

$$|Q\rangle_{out} = HH|Q\rangle_{in} = |Q\rangle_{in}. \qquad (1.3.3)$$

Відповідь випливає з того простого факту, що подвійне застосування перетворення Адамара (1.4) є тотожна операція. Це означає, що показаний на

Рис. 1.3.2 інтерферометр Маха-Цандера, дільник, в якому здійснюють перетворення Адамара, на виході відтворює той стан, який він отримує на вході. Розглянемо ще раз крайній окремий випадок, коли вхід складається тільки з одного пучка - тобто, припустимо, без втрати спільності, що $\alpha = 1$, а нижній пучок - порожній.

Тоді, згідно з (1.3.2), на виході частка буде обов'язково виявлена зверху. І, що цікаво, це станеться саме тому, що між дільниками частка була б з однаковою ймовірністю (з певною відносною фазою) виявлена в кожному з пучків. Саме інтерференція між двома амплітудами, що падають на останній дільник, призводить до того, що частка завжди виявляється в одному з пучків, що виходять і ніколи - в іншому.

Мовою квантової інформації, кубіт на виході інтерферометра Маха-Цандера матиме певне значення, якщо кубіт на вході буде також мати певне значення - і це тільки тому, що в проміжку між двома перетвореннями Адамара значення кубіта було максимально невизначено.

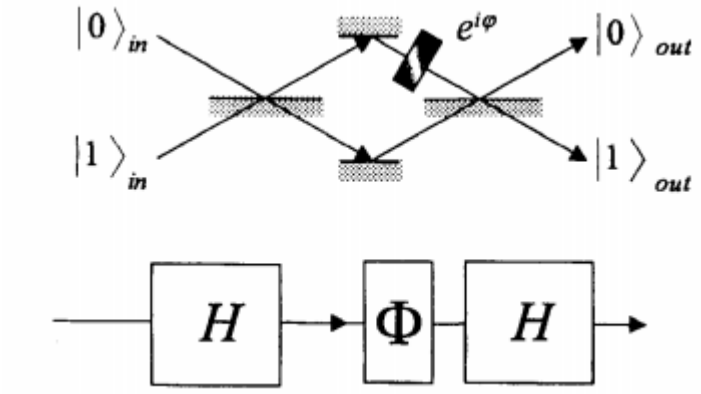

Рисунок. 1.3.3. Вгорі: інтерферометр Маха-Цандера з фазообертачем φ в одному з двох пучків. Це повністю змінює результат. Внизу: еквівалентне уявлення з перетвореннями Адамара і логічним елементом зсуву фази.

Ще одним важливим квантовим логічним елементом, крім елемента Адамара, є фазообертач. На Рис. 1.3.3 він додатково введен в інтерферометр Маха-Цандера. Його функція полягає в тому, щоб просто зробити зрушення фази φ у одного з двох пучків (без втрати спільності, припускаємо, що це

верхній пучок, оскільки важлива лише відносна фаза). У наших позначеннях, дію фазообертача можна описати унітарним перетворенням:

$$\Phi\big|0\rangle = e^{i\varphi}\big|0\rangle, \Phi|1\rangle = |1\rangle. \qquad (1.3.4)$$

Отже, кубіт на виході можна обчислити, послідовно застосовуючи всі відповідні перетворення до кубіту, який був на вході:

$$|Q\rangle_{out} = H\Phi H|Q\rangle_{in}. \qquad (1.3.5)$$

У випадку, коли є тільки один пучок на вході, а саме α= 1 і β = 0, тобто, $|Q\rangle_{in}$= 0. Тоді кінцевим є стан:

$$\text{НФН}|0\rangle = \frac{1}{2}\left(\left(e^{i\varphi}+1\right)|0\rangle + (e^{i\varphi}-1)|1\rangle\right). \qquad (1.3.6)$$

У цього виразу є дуже проста інтерпретація. Спочатку ми помічаємо, користуючись (1.3.6), що для φ= 0 значення кубіта визначине і дорівнює «0». З іншого боку, для φ = π до, значення кубіта строго дорівнює «1». Це показує, що фазовий зсув φ може перемикати стан вихідного кубіта між «0» і «1». У цілому, ймовірність, що кубіт має значення «0» є $P_0 = \cos^2(\varphi/2)$, а ймовірність, що він несе значення «1»дорівнює $P_1 = \sin^2(\varphi/2)$.

1.4. Змішування

Розглянемо джерело, яке випускає пару частинок так, що одна з них летить наліво, а інша - направо (джерело S на Рис. 1.4). Джерело таке, що частки випускаються з протилежними імпульсами. Якщо частка, що летить наліво (назвемо її часткою 1), виявлена в верхньому пучку, то частка 2, що летить направо, буде обов'язково виявлена в нижньому.

І навпаки, якщо частка 1 знайдена в нижньому пучку, то частка 2 буде обов'язково знайдена в верхньому. На мові кубітів це_означає, що дві частинки

несуть протилежні значення бітів. Якщо частка 1 несе «0», то частка 2 несе «1», і навпаки. Мовою квантової механіки, це двочастковий стан виду:

$$\frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + e^{i\chi}|1\rangle_1|0\rangle_2). \qquad (1.4.1)$$

Фаза χ визначається внутрішніми властивостями джерела, і ми припустимо для простоти, що $\chi = 0$. Рівняння 1.4.1) описує те, що називають переплутаним станом. Воно цікаве тим, що жоден з двох кубітів не несе певного значення, але, як випливає з виду квантового стану, як тільки один з двох кубітів буде вимірянний (результат буде абсолютно випадковим), то відразу виявиться, що інший несе певного значення . Кажуть, що в цьому проявляється загадка квантової нелокальності, так як під час вимірювання два кубіта можуть бути віддалені один від одного на довільно велику відстань.

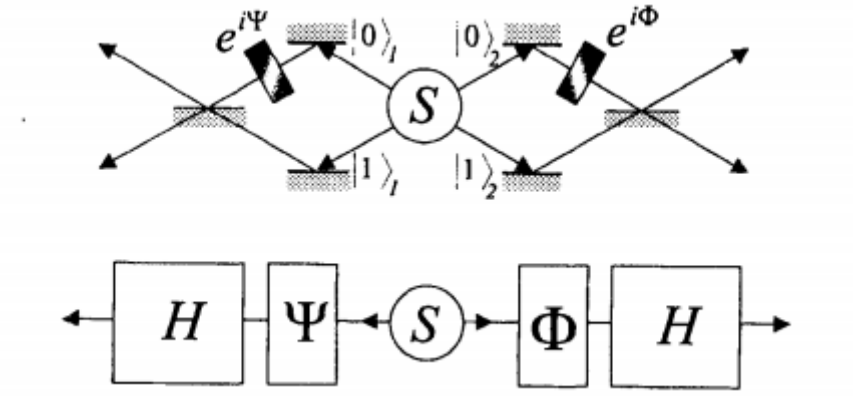

Рисунок. 1.4.1. Джерело випускає два кубіта в переплутаному стані. Вгорі: перевірка за допомогою двочасткового інтерферометра. Знизу: той самий принцип в термінах однофотонних логічних елементів.

Найцікавіша ситуація виникає тоді, коли обидва кубіта піддані фазовому зсуву і перетворенню Адамара, як показано на Рис. 1.4.1. Тоді, для детектування після обох перетворень Адамара - тобто, в разі перевірки за допомогою двочасткові інтерферометра [10] для детектування за дільниками, - з'являються цікаві нелокальних кореляції, що порушують нерівності Белла. Можна сказати, що суть такого порушення полягає в тому, що неможливо

пояснити кореляції між явищами, що спостерігаються на двох сторонах приладу на основі лише локальних властивостей кубітів.

Не можна зрозуміти квантові кореляції між ними, якщо вважати, що на детектор, реєструючий частку на одній заданій стороні, не впливає величина фази для іншої частинки, заданої як параметр. Є багато можливостей точно відобразити сенс нерівностей Белла, і можна їх формально представити багатьма способами.

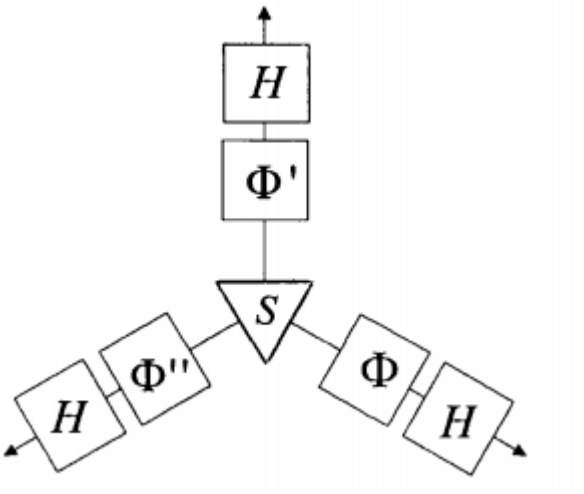

Рисунок. 1.4.2. Трьохчасткове переплутування. Тут ми показуємо тільки уявлення в термінах елементарних логічних елементів.

Дуже цікаве і дуже доречне з точки зору квантової механіки узагальнення - це досліджувати переплутування для більш ніж двох кубітів. Наприклад, розглянемо простий випадок змішування між трьома кубітами, як показано на Рис. 1.4.2. Припустимо, що джерело випускає три частки, по одній в кожному з показаних на малюнку приладів, у специфічній суперпозиції - в так званому стані Гринбергера-Хорна-Цайлінгер.

$$\frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3). \quad (1.4.2)$$

Цей квантовий стан має дуже специфічні властивості. Також як і в переплутуванні для двох частинок, жоден з трьох кубітів не несе сам по собі інформації, жоден з них не має чітко визначеного значення біта. Але як тільки

один з них буде виміряно, два інших придбають строго певне значення, якщо тільки вимірювання проводиться в базисі 0-1. І цей висновок не залежить від просторового розміщення трьох вимірів.

Найцікавіше те, що, якщо подивитися, на передбачувані станом ГХЦ, співвідношення між трьома вимірами, після проходження елементів зсуву фази і перетворень Адамара, то можна знайти велику кількість повних кореляцій для певних спільних наборів параметрів з цікавою властивістю, що неможливо зрозуміти навіть абсолютно точні кореляції в рамках локальної моделі. Це показує, що квантова механіка розходиться з локальним класичним поглядом на світ не тільки в області статистичних передбачень теорії, але також і для передбачень, які можна зробити з усією визначеністю.

1.5. Змішування і квантова непомітність

Щоб зрозуміти, як природу змішування, так і способи його створення, треба усвідомити, що стани загального вигляду (1.4.1) і (1.4.2) - це суперпозиції незалежних станів. Згадаймо обговорення явища дифракції на двох щілинах, де суперпозиція означала, що не існує способу сказати, яка з цих двох можливостей, які формують цю суперпозицію, має місце насправді. Це ж правило треба застосувати, щоб зрозуміти квантове переплутування. Наприклад, для стану:

$$\psi_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2). \quad (1.5.1)$$

Немає способу сказати, чи несе кубіт 1 значення «0» або «1», і, аналогічно, чи несе кубіт 2 значення «0» або «1». Але, якщо виміряти один кубіт, другий негайно прийме чітко визначене квантовий стан. Ці спостереження приводять нас прямо до умов того, як створювати і спостерігати переплутані квантові стани.

Є багато способів створити переплутані стани. По-перше, можна створити таке джерело, що, в силу його фізичного стану, з'являюись, квантові стану вже матимуть властивість нерозрізненості, яке обговорювалося вище. Це реалізується, наприклад, розпадом частинки зі спіном 0 на дві частинки зі спіном 1/2, зі збереженням внутрішнього моменту імпульсу. В цьому випадку спіни виникаючих частинок, повинні бути протилежними, і, якщо немає подальших механізмів, що дозволяють розрізнити можливості прямо на місці, квантовий стан є

$$\psi_{12} = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 + |\downarrow\rangle_1|\uparrow\rangle_2). \qquad (1.5.2)$$

де, наприклад, $|\uparrow\rangle_1$ позначає частку 1 зі спіном вгору.

Стан (1.5.2) має чудову властивість обертальної інваріантності - тобто, два спіни антипаралельні, щодо якого б напрямлення ми б їх не вимірювали. Друга можливість полягає в тому, що джерело може насправді створювати стани у вигляді індивідуальних компонент в суперпозиції, але стани, все одно, можна якимось чином розрізнити. Це відбувається, наприклад, при параметричному розсіянні, де стани фотонів вздовж певного обраного напрямку рівні:

$$|H\rangle_1|V\rangle_2 \text{ та } |V\rangle_1|H\rangle_2. \quad (1.5.3)$$

Це означає, що або фотон 1 поляризований горизонтально, а фотон 2 - вертикально, або фотон 1 поляризований вертикально, а фотон 2 - горизонтально. Проте, через різну швидкість світла всередині параметричного кристала-перетворювача, для горизонтально і вертикально поляризованих фотонів, часова кореляція між двома фотонами в цих двох випадках різна. Отже, за допомогою вимірювань в часі можна розрізнити два члена, і, через потенційну можливість розрізнити ці два випадки, не виникає переплутав стану.

Однак, навіть і в такій ситуації можна створити переплутування, зміщуючи два створених фотонних хвильових пакета один щодо одного таким чином, щоб вони перестали бути помітними завдяки своєму становищу в часі. Фактично це означає застосування техніки квантового стирання , в якій маркер - в даному випадку, відносний порядок у часі - стирається, так що виходить стан з квантовою нерозрізненістю яке є переплутаним:

$$\psi_{12}\frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 + e^{i\chi}|V\rangle_1|H\rangle_2) \qquad (1.5.4)$$

Третій засіб отримати переплутані стани - це спроектувати непереплутаний стан на переплутаний. Відзначимо, що переплутаний стан, ніколи не ортогонально жодній зі своїх компонент. Наприклад, розглянемо джерело, що створює непереплутаний стан:

$$|0\rangle_1|1\rangle_2 \qquad (1.5.5)$$

Припустимо, що цей стан тепер проходить через фільтр, описуваний оператором проектування

$$P = |\psi\rangle_{12}\langle\psi|_{12}\ , \quad (1.5.6)$$

Де $|\psi\rangle_{12}$ -це стан (1.5.1). Тоді з'являється наступний стан:

$$\frac{1}{2}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2)(\langle 0|_1\langle 1|_2 + \langle 1|_1\langle 0|_2)|0\rangle_1|1\rangle_2 =$$

$$= \frac{1}{2}(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2), \quad (1.5.7)$$

воно більш не нормовано на одиницю, тому що дія оператора призводить до втрати кубітів.

Тоді як кожен з обговорюваних вище методів може бути, в принципі, використаний для створення переплутаних станів, можливо також і створювати переплутування шляхом спостереження стану. Це, в цілому, означає, що у нас є

непереплутаний, або частково переплутаний стан в тому, чи іншому вигляді, а також процедура самого вимірювання, яка проектує квантові стани на переплутані, таким же чином, як це тільки що було описано.

1.6. Аргумент ЕПР і нерівність Белла.

Відразу після відкриття сучасної квантової механіки стало ясно, що вона містить нові, такі, що суперечать інтуїції риси. Найцікавіше тому свідчення - знаменитий діалог між Нільсом Бором і Альбертом Ейнштейном. Тоді як спочатку Ейнштейн стверджував, що квантова механіка неспроможна, пізніше він переформулював свої доводи, доводячи, що вона неповна.

У своїй ключовій статті Ейнштейн, Подільський і Розен (ЕПР) розглядають квантові системи, що складаються з таких двох частинок, що ні координата, ні імпульс кожної з частинок не визначені, але сума їх координат (тобто, їх центр мас) і різниця їх імпульсів (тобто, імпульс центру мас системи) визначено абсолютно точно. Тоді виходить, що вимір координати або імпульсу, скажімо, частки 1 негайно надає частці 2 точне значення координати або імпульсу без взаємодії з цією часткою.

Виходячи з того, що частинки 1 і 2 можуть бути рознесені на довільні відстані, ЕПР припускають, що вимір частки 1 не може насправді вплинути на частку 2 (умова локальності); і, отже, властивості частинки 2 не повинні залежати від вимірювання, проведеного над часткою 1. Вони вважають, що це означає, що координата і імпульс можуть одночасно бути визначеними певними властивостями квантової системи.

У своїй знаменитій відповіді Нільс Бор стверджує, що дві частинки в разі ЕПР завжди є частинами однієї квантової системи. І це значить, що вимір над однією з частинок змінює можливі передбачення, які можна зробити для всієї системи, а значить і для другої частки. Дискусію ЕПР-Бора довго вважали суто філософської, поки в 1951 році Давид Бом не ввів системи, переплутані по спіну, і в 1964 році Джон Белл [23] не показав, що, для таких переплутаних

систем, вимірювання корелюючих величин повинні в разі квантової механіки приводити до результатів, відмінним від того, що вийде, якщо припустити, що властивості системи існують до вимірювання і незалежно від нього.

Навіть незважаючи на те, що квантові передбачення підтверджені тепер у багатьох експериментах, зі строго логічної точки зору питання до сих пір не закрите, оскільки, через деякі «лазівки» в експериментах, до сих пір, в принципі, можливо логічно захищати точку зору локального реалізму.

Хід міркувань, що призводять до нерівності, еквівалентному початкового нерівності Белла.

Розглянемо джерело, що випускає два кубіта (Рис. 1.6.1) в переплутаному стані:

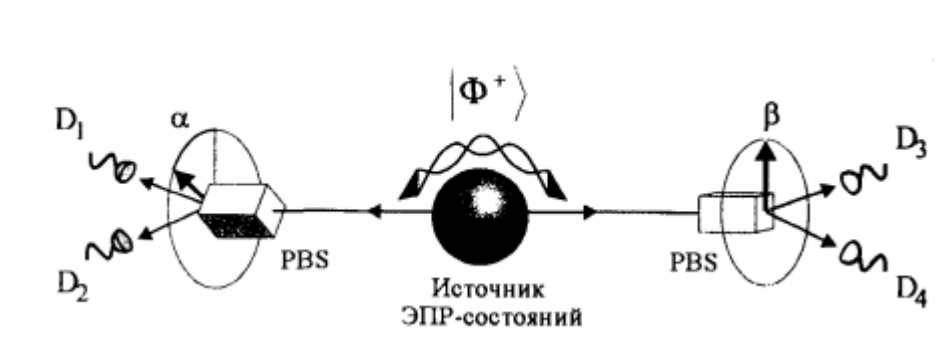

Рисунок. 1.6.1. Кореляційні вимірювання між подіями Аліси і Боба при різних виборах базисів детектування (позначених кутами α і β орієнтацій поляризаційних світлоподілювачів PBS) призводять до порушення нерівностей Белла.

Один кубіт надсилається Алісі (ліворуч на Рис. 1.6.1), а інший - Бобу (направо на Рис. 1.6.1). Аліса і Боб зроблять вимір поляризації, використовуючи поляризаційні подільники з двома однофотонними лічильниками на виході. Аліса з однаковою ймовірністю отримає результат вимірювання «0» або «1», відповідний детектування кубіта лічильником 1 або 2 відповідно. Це твердження залишиться вірним, в якому б поляризаційному базисі вона не робила вимір, і результат вимірювання буде абсолютно випадковим. Але, якщо

Боб вибере для вимірювання той же базис, він завжди отримає той самий результат.

Таким чином, дотримуючись першого кроку в міркуванні ЕПР, Аліса завжди зможе точно передбачити, який результат буде у Боба. На другому кроці застосовується гіпотеза локальності, тобто, припущення, що ніякий фізичний вплив не може моментально переміститись від приладу Аліси до приладу Боба, і значить, результат, який вимірюється Бобом повинен залежати тільки від властивостей його кубіта і приладу. Поєднуючи ці два кроки, Джон Белл досліджував можливі кореляції для випадку, коли Аліса і Боб вибирають базиси вимірювання під кутом один до одного. Можна побачити, що для трьох довільних кутів орієнтації α, β, γ, має виконуватися наступне співвідношення:

$$N(1_\alpha, 1_\beta) \leq N(1_\alpha, 1_\gamma) + N(1_\beta, 1_\gamma), \qquad (1.6.1)$$

де

$$N(1_\alpha, 1_\beta) = \frac{N_0}{2} cos^2(\alpha - \beta), \qquad (1.6.2)$$

є квантовомеханічне пророкування для числа випадків, в яких Аліса отримає «1» в своєму приладі, орієнтованому під кутом α, а Боб отримає «1» в своєму приладі, орієнтованому під кутом β і N_0- число пар, випущених джерелом. Це нерівність порушується прогнозами квантової механіки, наприклад, для таких кутів, що $(\alpha - \beta) = (\beta - \alpha)$= 30 °. Порушення нерівності означає, що, хоча б, одне з припущень, на яких заснована нерівність Белла, не узгоджується з квантовою механікою. Цей факт зазвичай вважають доказом нелокальності, хоча, звичайно, це не єдине можливе пояснення.

1.7. Зв'язування атомів і фотонів

Квантові мережі складаються з просторово рознесених вузлів, у яких можна побачити індивідуально керовані кубіти, і квантових комунікаційних

каналів, що з'єднують ці вузли. Обмін інформацією всередині мережі виконується шляхом пересилання кубітів по каналах.

Фізично такі мережі могли б складатися, наприклад, з кластерів або захоплених в пастки іонів, що представляють собою вузли, а також оптичних волокон або якихось пристроїв, що передають фотони, що забезпечувало б реалізацію квантових каналів, як показано на Рис.1.7.1.

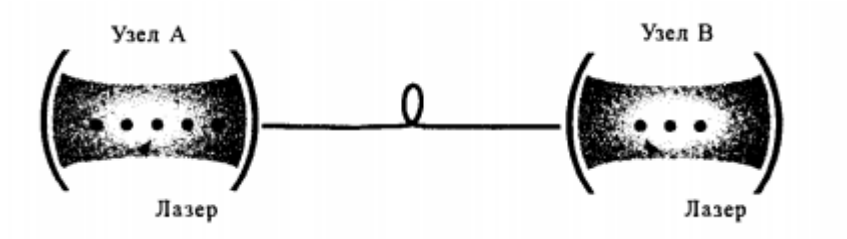

Рисунок. 1.7.1. Елемент квантової мережі. Атоми в високонадійних резонаторах використовуються для локального зберігання і маніпулювання квантовою інформацією між просторово розділеними «вузлами» мережі.

Для зберігання кубітів добре підходять атоми і іони, що знаходяться в довгоживучих внутрішніх станах. Нещодавно були запропоновані схеми для виконання квантових логічних операцій на атомах, в пастках або іонах, що дало привабливу можливість для виконання локальних маніпуляцій в межах атомних (іонних) вузлів. З іншого боку, для швидких і надійних способів передачі інформації на великі відстані, очевидно, саме фотони є кращими носіями кубітів. У цьому розділі ми розглянемо схему, в якій реалізується інтерфейс між атомами і фотонами, тобто між мережевими вузлами і комунікаційними каналами.

Така схема дозволяє здійснювати квантовий зв'язок з одиничною ефективністю (в принципі) між віддаленими атомами 1 і 2. Поєднання локальних квантових маніпуляцій з квантової зв'язком між мережевими вузлами відкриває можливість для нових різноманітних додатків – від криптографії на основі переплутаних станів і телепортації, до більш складних, таких як багаточастинкові засоби зв'язку і розподілені квантові обчислення.

Основна ідея цієї схеми, полягає в використанні сильної взаємодії між високоякісним оптичним резонатором і атомами, що утворюють окремий вузол квантової мережі. При впливі лазерних пучків можна перетворити внутрішній стан атома першого вузла в оптичний стан резонатора моди. Виникаючі при цьому фотони виходять з резонатора, поширюються як хвильової пакет по лінії передачі і потрапляють в резонатор другого вузла. В кінцевому рахунку, оптичний стан другого резонатора перетворюється на внутрішній стан атома.

При послідовному доступі до пари атомів (один атом в кожному вузлі) можна отримати багато-кубітові передачі, оскільки в процесі запису стану, зберігаються змішування між довільно розташованими атомами. Відмінна особливість цього протоколу полягає в тому, що керуючи взаємодією між атомом і резонатором, можна уникнути відображення хвильових пакетів від другого резонатора. Це досягається за допомогою ефективного виключення тих домінуючих втрат в каналі, які відповідали б за декогерентність в процесі передачі інформації.

1.8 Висновки з розділу 1

Майже кожен з нас отримує доступ до величезної кількості необхідних послуг, починаючи з передачі повідомлень і закінчуючи медіа контентом. Провайдери, які забезпечують доступ до мережі Intertet, в свою чергу мають величезні розповсюджені мережі. Основною задачею провайдерів є забезпечення якості зв’язку, та в першу чергу конфіденційності переданої інформації.

Створення елементної бази сучасних волоконно-оптичних систем передачі інформації (ВОСП) і технологій їх серійного виробництва засноване на практичному застосуванні таких відкриттів в області фізики і таких розділів математики, які ще зовсім недавно вважалися частиною так званої «чистої науки», на практичне використання яких не сподівалися не тільки широка громадськість, але і самі автори цих відкриттів. Насправді ж виявляється, що до

створення сучасних телекомунікаційних систем та комп'ютерних технологій причетні майже всі відомі фізики минулого і сьогодення: від Ньютона і Гюйгенса, Френеля і Декарта до більшості нобелівських лауреатів з фізики від М. Планка і А. Ейнштейна до А. М . Прохорова, Ч. Таунса, Н. Г. Басова і Ж. І. Алфьорова. В професійний лексикон фахівців, що працюють в області волоконно-оптичного зв'язку входять такі терміни, як кванти, електрони, фотони, фонони, ферміони і бозони, екситон і багато інших, які раніше в своїй діяльності використовували тільки професійній фізиці. Сучасні волоконно-оптичні системи передачі – це концентратор практичного використання самих глибинних досягнень фундаментальних наук.

РОЗДІЛ 2. КВАНТОВІ ОПТИЧНІ СИСТЕМИ ЗВ’ЯЗКУ

2.1. Квантова мережа

Квантова мережа – це мережа зв'язку, що захищає дані, які передаються з використанням фундаментальних законів квантової механіки. Є практичною реалізацією так званої квантової криптографії. Квантові мережі формують важливий елемент квантових обчислень і квантових систем криптографії. Вони допускають транспортування квантової інформації між фізично розділеними квантовими системами. У квантових мережах, що використовують в якості середовища передачі оптоволокно, важливу роль відіграє передача чистих квантових станів у вигляді фотонів на великі відстані.

Основним способом взаємодії квантових мереж на великих відстанях є використання оптичних мереж і фотонних кубітів. Оптичні мережі мають перевагу повторного використання існуючого оптоволокна. А вільні мережі можуть бути реалізовані так, що зможуть передавати квантову інформацію по повітрю або в вакуумі.

Оптичні мережі можуть бути реалізовані, використовуючи існуючі телекомунікації та телекомунікаційне обладнання. З боку відправника, джерело одиночних фотонів можна створити, сильно послабивши стандартний телекомунікаційний лазер, так що середнє число випускаються фотонів за імпульс буде менше одиниці. Щоб отримати цей ефект, використовується лавинний фотодіод. Також можуть використовуватися різні методи регулювання фази і поляризації, такі як роздільники променя і інтерферометри. У разі протоколів, заснованих на заплутуванні, заплутані фотони генеруються через спонтанне параметричне розсіяння. В обох випадках телекомунікаційне волокно може бути мультиплексним для відправлення не квантової синхронізації і керуючих сигналів.

2.1.1 Компоненти й конфіграція ВОСПІ

Мережі можна застосовувати не тільки у вигляді півдуплексної лінії передачі "із точки в точку" але волоконна оптика дає поштовх до створення дуплексних систем, у яких сигнали одночасно передаються по одному волокну в обох напрямках [6]. Практично важливим також є розподіл оптичного сигналу по волокнах між численними терміналами у мережі будь-якої топології. Багатотермінальна архітектура має багато застосувань. Найбільш важливим є локальна обчислювальна мережа (ЛОМ), що з’єднує численні вхідні і вихідні телекомунікаційні пристрої, розташовані на обмеженій території Наприклад, офісна ЛОМ з'єднує термінали, що розташовані у виробничих приміщеннях. Службовці через будь-який із терміналів можуть звертатися до баз даних, електронної картотеки, текстового процесора, комп’ютера, принтера, копіювальної машини. Комп'ютери можна безпосередньо об'єднати за допомогою ЛОМ.

У мережу також можна включати обладнання для організації відеоконференцій. Переваги волокон порівняно з провідниками полягають в кращі безпеці (надійність), меншому розмірі, низькій масі і великій широкосмужності. Наприклад, ЛОМ що є на заводі, використовують для контролю і керування обладнанням. Можна класифікувати "обплутане волокнами місто" як велику ЛОМ. Секретність волоконної передачі є перевагою такої багатотермінальної мережі. У цьому розділі розглянуто основні конфігурації мереж і компоненти для розподілу і керування сигналами, що передаються по оптичних кабелях 70 методами, які не настільки обмежені, як “єдиний оптичний канал” традиційної системи передачі, що з'єднує передавальний і приймальний пристрої. Розподільні мережі

Для розподілу оптичного випромінювання в кілька волоконних каналів або, навпаки, для об'єднання кількох оптичних сигналів для передачі по одному каналу потрібні такі пристрої, як відгалужувачі і розгалужувачі [13]. Розгалужувач (coupler) – пристрій, у якому відбувається як правило, однаковий

розподіл потужності вхідного сигналу між двома або більшим числом вихідних каналів (полюсів).

При зміні напрямку світлових потоків на протилежний, розгалужувач виконує роль об’єднувача (суматора). Відгалужувач – це узагальнення розгалужувача, в якому вихідна потужність розподіляється між вихідними каналами, не обов'язково у рівній мірі. Серед відгалужувачів широкого поширення набули спрямовані, що мають два вхідних і два вихідних полюси, причому ці пари полюсів між собою розв'язані. Такий відгалужувач здійснює функцію розподілу оптичної потужності (що надходить на один із вхідних каналів) тільки між вихідними каналами. При зворотному вмиканні пристрій також працює як спрямований відгалужувач (СВ).

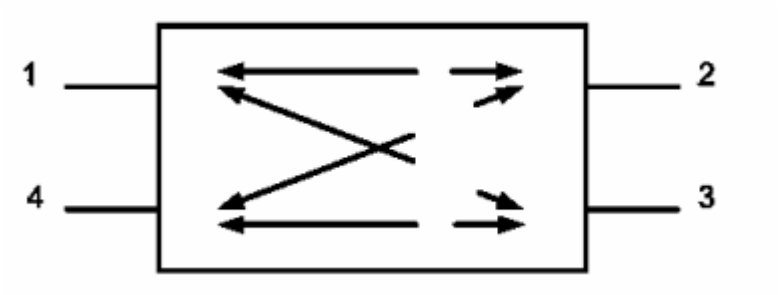

Рисунок 2.1.1.1 Чотириполюсний спрямованний відгалужувач

Спрямований відгалужувач є основним компонентом багатьох розподільних мереж. На рис.2.1.1.1 показано відгалужувач із чотирма (1-4) полюсами (Х- відгалужувач).

Нижче будуть описані відгалужувачі з більшою кількістю полюсів. Можливі напрямки розподілу потужності світла показано на рис.2.1.1.1 стрілками для опису параметрів відгалужувача приймемо, що на полюс 1 надходить потужність Р1, що ділитися між полюсами 2 і 3 у відповідній пропорції. В ідеалі жодна частка потужності не потрапляє на полюс 4 (що називають ізольованим), тому можемо прийняти, що потужність, що з'являється на полюсі 2Р2, дорівнює або більша, ніж потужність, що з’являється на полюсі

3Р3.Вводять такі параметри, що описують втрати відгалужувача, дБ. 1.Коефіцієнт передачі (throughput loss - втрати передачі):

$$\alpha_{\text{пер}} = -10 \lg P_2/P_1, \qquad (2.1.1.1)$$

визначає передачу потужності між вхідним полюсом 1 і одним із вихідних полюсів (в даному випадку 2).

Втрати відгалуження (tap loss):

$$\alpha_{\text{від}} = -10 \lg P_3/P_1, \qquad (2.1.1.2)$$

враховують передачу потужності між вхідним полюсом 1 і полюсом відгалуження.

Коефіцієнт спрямованості (directionality):

$$\alpha_{\text{спр}} = -10 \lg P_4/P_1, \qquad (2.1.1.3)$$

визначає передачу потужності між вхідним 1 та ізольованим 4 полюсами.

Внесені втрати (excess loss - додаткові втрати):

$$\alpha_{\text{вн}} = -10 \lg(P_2 + P_3)/P_4, \qquad (2.1.1.4)$$

оцінюють потужність, яка втрачається у відгалужувачі. Вона обумовлена випромінюванням, розсіюванням, поглинанням і зв'язком з ізольованим полюсом.

В ідеальному відгалужувачі потужність не потрапляє до ізольованого полюса 4. До того ж, він не має внутрішніх втрат потужності (авнутр= 0 дБ), так що загальна потужність, яка з'являється на полюсах 2 і 3, дорівнює потужності на вході (Р2 + Р3 = Р1) Якісні спрямовані відгалужувачі мають внесені втрати менші 1 дБ і коефіцієнт спрямованості більший за 40 дБ. Коефіцієнт розгалуження (splitting ratio) дорівнює відношенню потужностей на двох вихідних полюсах (Р2/Р3). Відгалужувачі часто описують у термінах втрат відгалуження. Наприклад, 10-ти децибельний відгалужувач - це пристрій, що

має втрати відгалуження у 10 дБ. У таблиці 3.5 наведено основні параметри кількох варіантів ідеальних відгалужувачів.

Таблиця 2.1.1.1 Параметри ідеальних спрямованних відгалжвачів

Позначення	$\alpha_{\text{пер}}$, дБ	$\alpha_{\text{від}}$, дБ	Коефіцієнт розгалудження
3дБ	3	3	1:1 або (50/50%)
6дБ	6	1,25	3:1 або (75/25%)
10дБ	10	0,46	9:1 або (90/10%)
12дБ	12	0,28	15:1 або (94/6%)

Для відгалужувача без втрат P2 = P1–P3, отже, коефіцієнт передачі (співвідношення 1) можна записати у вигляді:

$$\alpha_{\text{пер}} = -10\lg\left(1 - 10^{\frac{\alpha\text{від}}{10}}\right), \text{дБ} \qquad (2.1.1.5)$$

Це співвідношення пов'язує коефіцієнт передачі з втратами відгалуження. У наступному прикладі покажемо, як внесені втрати впливають на значення коефіцієнта передачі і втрати відгалуження. Якщо позначити через а’пер і а’від параметри ідеального СВ, який має заданий коефіцієнт розгалуження, тоді параметри реального СВ, що має такий самий коефіцієнт розгалуження і внесені втрати авн, можна записати у вигляді:

$$\alpha_{\text{пер}} = \alpha'_{\text{пер}} + \alpha_{\text{вн}}, \qquad (2.1.1.5\text{а})$$

$$\alpha_{\text{від}} = \alpha'_{\text{від}} + \alpha_{\text{вн}}, \qquad (2.1.1.5\text{б})$$

тобто втрати ідеального СВ слід збільшити на величину внесених втрат. Ці втрати на практиці вимірюються шляхом порівняння (вирахування) потужностей на виходах 2 і 3 при подачі потужності на вхід 1.

Оскільки втрати авн у рівняннях (2.1.1.1) є фактичними втратами, що вносяться при встановленні відгалужувача в тракт, їх часто називають надлишковими втратами. Стрілки на рис.2.1.1.1 свідчать, що такий відгалужувач є двоспрямованим. Будь-який із чотирьох полюсів може бути

вхідним. Можливі такі варіанти передачі: із 1 полюса до 2 і 3; із 2 - до 1 і 4; із 3 - до 4 і 1 і з 4 до 3 і 2. Спрямовані відгалужувачі звичайно виконують симетричними, так що втрати мають ті самі значення незалежно від того, який полюс обраний як вхідний.

2.1.2 Дуплексна мережа

При традиційній півдуплексній схемі передачі і прийому в обох напрямках для зв'язку "з точки в точку" використовуються пара волокон по яких передається інформація у протилежних напрямках. У повнодуплексній системі (з одночасною передачею в обох напрямках в одному волокні) економиться волокно, що важливо для довгих ліній передачі.

На рис.2.1.1.2 подано структурну схему повнодуплексної лінії з відгалужувачами, встановленими на кожній станції. При використанні в такому лінійному тракті ідеальних тридецибельних СВ між передавальним і приймальним обладнанням вносяться додаткові втрати 6 дБ. Внесені втрати і втрати у з'єднувачах, за допомогою яких приєднується кожний з полюсів реального відгалужувача, зменшують прийняту потужність ще більше.

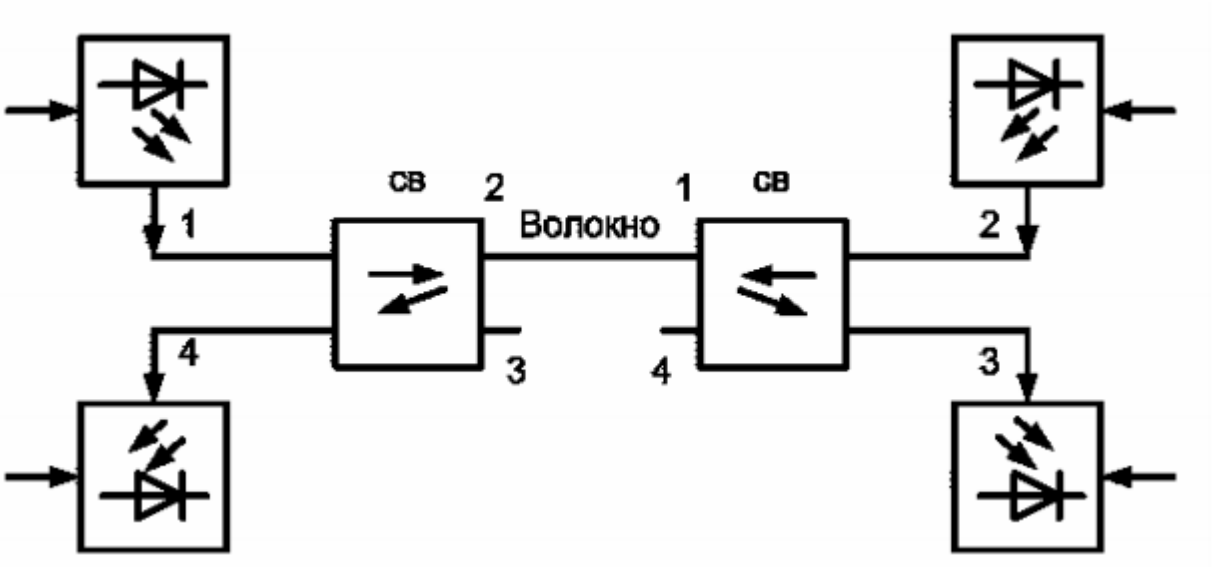

Рисунок 2.1.1.2 Структурна схема повнодуплексної системи передачі

2.1.3 Т-подібна мережа

Т-подібна мережа (рис.2.1.1.3) пов'язує велику кількість терміналів, кожний з яких має передавальний і приймальний пристрої. По магістральному волокну - шині (або шині даних) передається інформація між Т-подібними відгалужувачами, за допомогою яких забезпечується відведення частки потужності. Показаний на рис.2.1.1.3 Т-подібний відгалужувач (що складений з двох спрямованих Y - відгалужувачів) забезпечує дуплексний потік інформації у одноволоконній шині.

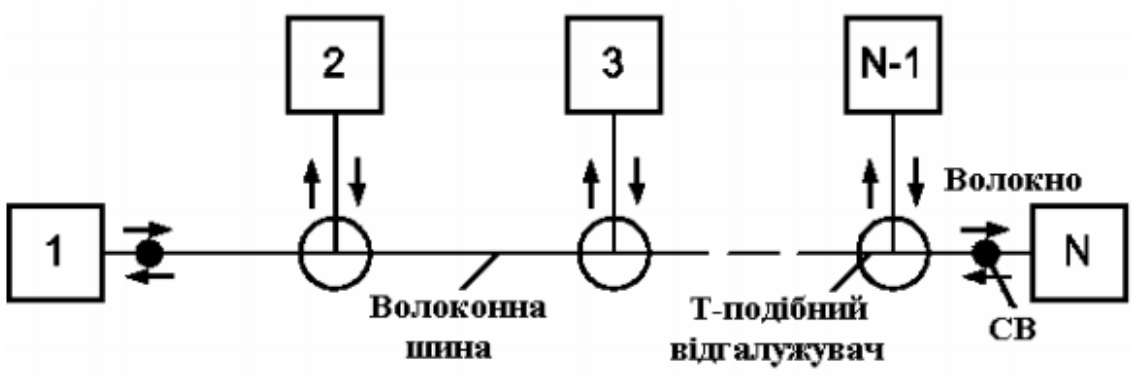

Рисунок 2.1.1.3 Структурна схема Т-подібної мережі з N терміналами

Багатотермінальна мережа потребує Т-подібного відгалужувача з великим коефіцієнтом розгалуження (переданна потужність набагато більша відведеної). Це гарантує, що сигнали, які надходять на приймальні пристрої, які розташовані на більшій відстані від передавального, будуть мати достатню потужність, щоб забезпечити задану якість передачі. Підрахуємо результуючі втрати між терміналами 1 і N, беручи до уваги, що кожний із приєднаних до волокна шини СВ, має коефіцієнт передачі 74 апер і втрати відгалуження авід. Сигнал має пройти через N - 1 СВ перш ніж потрапити у N-ий приймальний пристрій. Він приєднується до полюса відгалуження цього відгалужувача, так, що результуючі втрати розподілу:

$$\alpha = (N-1)\alpha_{\text{пер}} + \alpha_{\text{від}}, \text{дБ} \qquad (2.1.1.6)$$

Ясно, що результуючі втрати у мережі лінійно збільшуються при зростанні кількості терміналів. У реальній системі слід врахувати втрати в з'єднувачах, що використовуються для монтажу мережі. На кожному вході і виході СВ встановлюється з'єднувач, так що в тракті між терміналами 1 і N знаходяться 2N з'єднувачів. Якщо втрати в кожному із з'єднувачів дорівнюють аз, тоді в тракт вноситься додаткове згасання 2Nаз. Вони мають бути додані до формули (2.1.1.6), тобто результуючі втрати розподілу становлять

$$a = (N-1)\alpha_{\text{пер}} + a_{\text{зд}} + 2Na, \text{дБ} \qquad (2.1.1.7)$$

На рис. 2.1.1.4 показано результати розрахунків втрат для кількох варіантів розподільної мережі. Нижні графіки (див. рис.3.9) відповідають ідеальним СВ (відсутні втрати внесені відгалужувачами і з'єднувачами). Для верхніх графіків прийнято, що в реальній мережі авн = аз = 1 дБ. Як видно з рисунка, втрати стають неприпустимо великими при з'єднанні порівняно невеликої кількості терміналів (N=5).

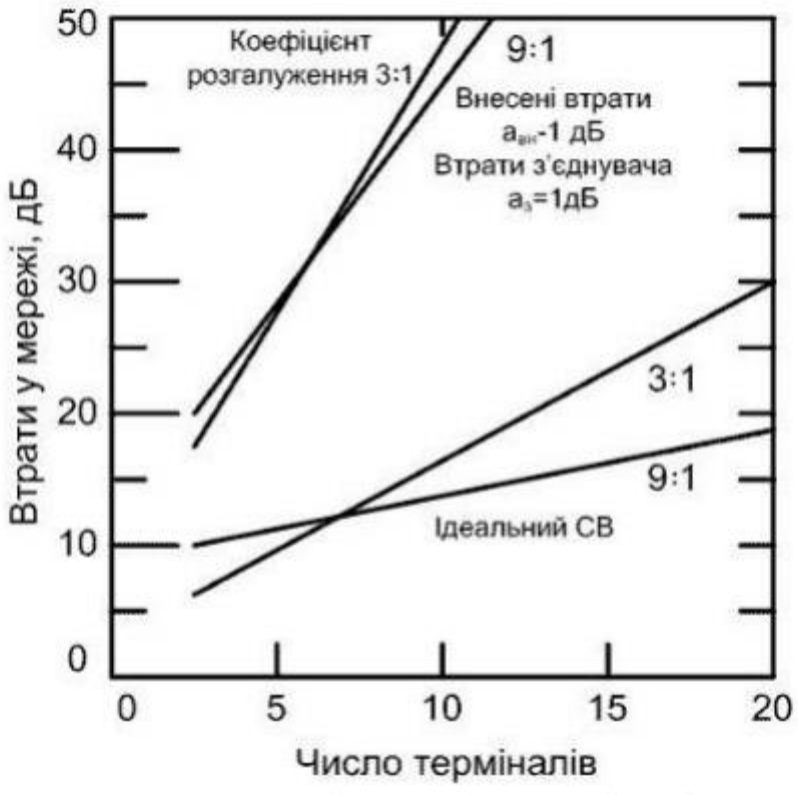

Рисунок 2.1.1.4 Залежність втрат розподілу від числа терміналів Т-подібної мережі

Крім втрат, Т-подібну мережу характеризують і такими параметрами, як динамічний діапазон приймальних пристроїв, стійкість до пошкоджень і легкість додавання нових терміналів. Розглянемо їх в Т-подібній мережі, на будь-який із терміналів надходить більша потужність від сусіднього термінала ніж від віддаленого.

Приймальний пристрій має бути здатним обробляти сигнали, що змінюються в широкому діапазоні рівнів оптичної потужності. Іншими словами, в даному випадку потрібний приймальний пристрій з великим динамічним діапазоном. Локальне пошкодження у Т-подібній мережі не призводить до припинення всього зв’язку.

Розрив волокна шини розділяє систему на дві частини з інформаційним потоком, що зберігається по обидві сторони від місця пошкодження. Пошкодження одного з Т-подібних відгалужувачів також розділяє мережу на дві працюючі ділянки і перериває зв'язок із терміналом, підключеним до мережі

через цей відгалужувач. Пошкодження в терміналі просто вимикає цей термінал, залишаючи іншу частину системи працювати в штатному режимі. Нові термінали можна додати до Т-подібної мережі простим розрізанням волокна шини і встановленням у місце розриву Т-подібного відгалужувача.

2.1.5 Зіркоподібна мережа

При великій кількості терміналів альтернативою Т-мережі є зіркоподібна (рис.2.1.1.5).

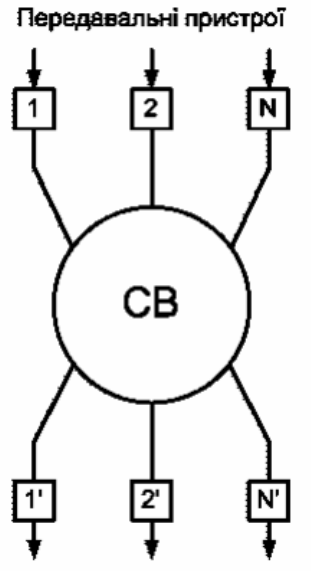

Рисунок 2.1.1.5 Структура зіркоподібної мережі

У цій мережі зіркоподібний передавальний відгалужувач зв’язує N терміналів. Відгалужувач має 2N полюсів. Він може розглядатися як спрямований відгалужувач із більше ніж чотирма полюсами. Зіркоподібний відгалужувач однаковою мірою розподіляє потужність із будь якого з полюсів передачі до кожного з полюсів прийому (рис.3.11). Ідеальна зірка розподіляє вхідну потужність між N полюсами без втрат. Ефективність передачі для кожного полюсу дорівнює 1/N, і відповідні внесені відгалужувачем втрати,

$$\alpha = -10\lg(1/N), \text{ дБ} \qquad (2.1.1.8)$$

Якщо для приєднання терміналів використовують два з'єднувачі, кожний із яких має втрати а, і внесені втрати складають авн, тоді результуючі втрати в розподільній мережі, що використовує зіркоподібний відгалужувач:

$$\alpha = -10\lg(1/N) + \alpha_{\text{вн}} + 2\alpha_{\text{з}}, \text{ дБ} \quad (2.1.1.9)$$

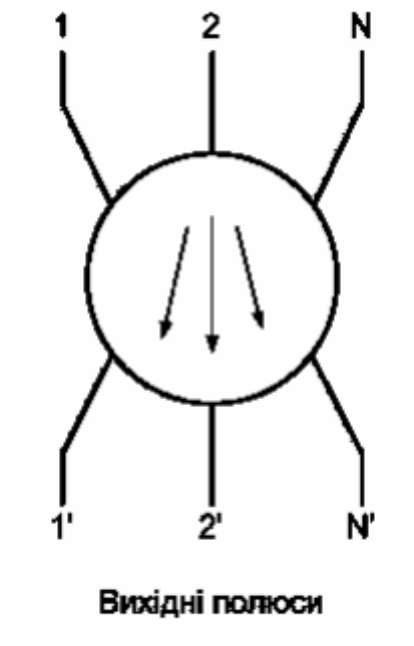

Рисунок 2.1.1.6 Структурна схема мережі з прохідним зіркоподібним відгалужувачем

Порівнюючи рис. 2.1.1.4 і рис. 2.1.1.7, бачимо різницю між втратами в зіркоподібній і Т-подібній мережах. Зірка забезпечує значно вищу ефективність, коли у мережі зв’язані більше ніж п'ять терміналів. Це відбувається тому, що зростання втрат у зіркоподібній мережі має логарифмічну залежність, тобто відбувається повільніше при збільшені N, ніж лінійне зростання втрат у Тподібній мережі. Для кожного нового термінала, що додається до Т-подібної мережі, сигнал має пройти ще через два з'єднувачі Y у зіркоподібній мережі, додавання термінала не збільшує число з'єднувачів, так що сигнал не повинен проходити через них, поширюючись від передавального до приймального пристрою.

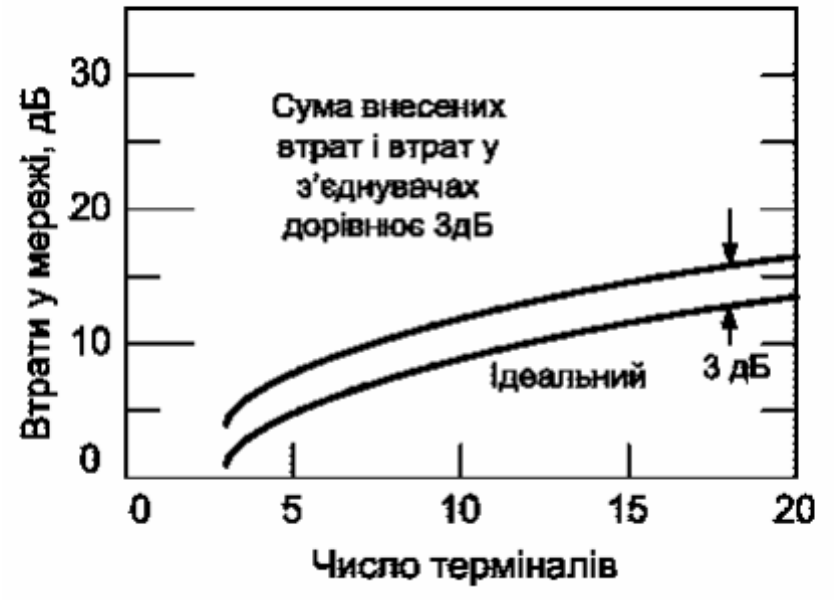

Рисунок 2.1.1.7 Залежність втрат розподілу від числа терміналів зіркоподібної мережі

Для систем з невеликим числом терміналів таке значення втрат в Тподібній мережі можна допустити, особливо, якщо втрати з'єднувача аз, мінімізовані за допомогою зрощування, зварюванням полюсів СВ з волоконною шиною. Отже Т-подібна мережа при кількості терміналів понад 10 є практично нездійснимою.

Навіщо тоді взагалі її розглядати? Справа в тому, що в такій мережі економиться оптичне волокно Якщо термінали розташовані на великій відстані один від одного на довгій трасі, тоді для організації Т-подібної мережі потрібно набагато менше волокна, ніж для зіркоподібної (де окремий кабель має прокладатися від центрального відгалужувача до кожного з терміналів) Для максимальної ефективності передачі зіркоподібний відгалужувач у мережі, що містить N терміналів, повинен мати 2N полюсів, тобто усі його полюси мають бути використані. Відгалужувач з числом полюсів більшим за 2N вносить більшу ніж потрібно кількість втрат у розподільну мережу. З цієї причини додавання нових терміналів до існуючої системи потребує нового зіркоподібного відгалужувача (з більшим числом полюсів).

У попередньому прикладі було прийнято, що новий зіркоподібний відгалужувач буде мати ненабагато більші внесені втрат, ніж старий. Таке припущення допустиме при додаванні тільки двох полюсів, оскільки внесені втрати практичних пристроїв збільшуються зі зростанням числа полюсів. Наприклад, внесені втрати можуть змінюватися з 1 дБ для 16 полюсів (N = 8) до 3 дБ для 128 полюсів (N = 64). У зіркоподібній мережі пошкодження кабелю гілки, що з’єднує термінал з відгалужувачем, перериває зв'язок із цим терміналом, проте вихід із ладу самого зіркоподібного відгалужувача перериває потік даних до всіх терміналів.

2.1.6 Кільцева мережа

Волокна можуть з'єднувати численні термінали в кільцеву мережу (рис. 2.1.1.8) [17], що фактично є послідовним з'єднанням незалежних ліній передачі "з точки в точку". Кожний вузол кільцевої мережі містить оптичні передавальний (ПП) і приймальний (ПрП) пристрої.

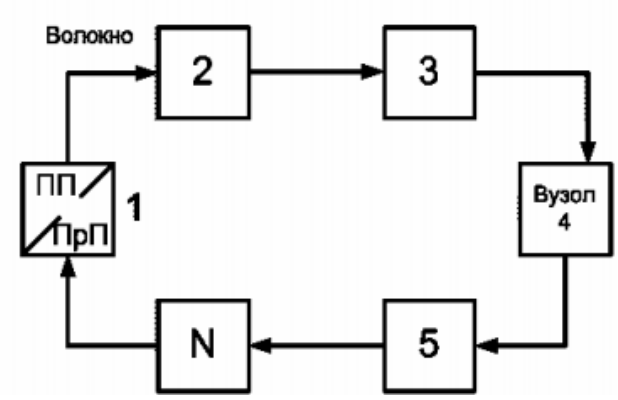

Рисунок 2.1.1.8 Структура кільцевої мережі

Функцією вузла є регенерація. Як тільки приймальний пристрій виявляє передане повідомлення, воно перетворюється до електричного еквіваленту, дані відновлюються (регенеруються), перетворюються в оптичний сигнал і передаються на наступну станцію.

У кільцевій мережі потужність з будь-якого оптичного передавального пристрою потрапляє тільки на один приймальний пристрій. Тут немає розподілу оптичної потужності між окремими станціями (на відміну від Т- і зіркоподібної мереж). З цієї причини кільце може зв'язати більшу кількість терміналів, ніж будь-яка з описаних вище конфігурацій мереж, тобто кільце не обмежене втратами в пристроях розподілу, як Т- і зіркоподібні мережі. Звичайно активні вузли кільцевої мережі значно складніші ніж пасивні вузли Т і зіркоподібних мереж.

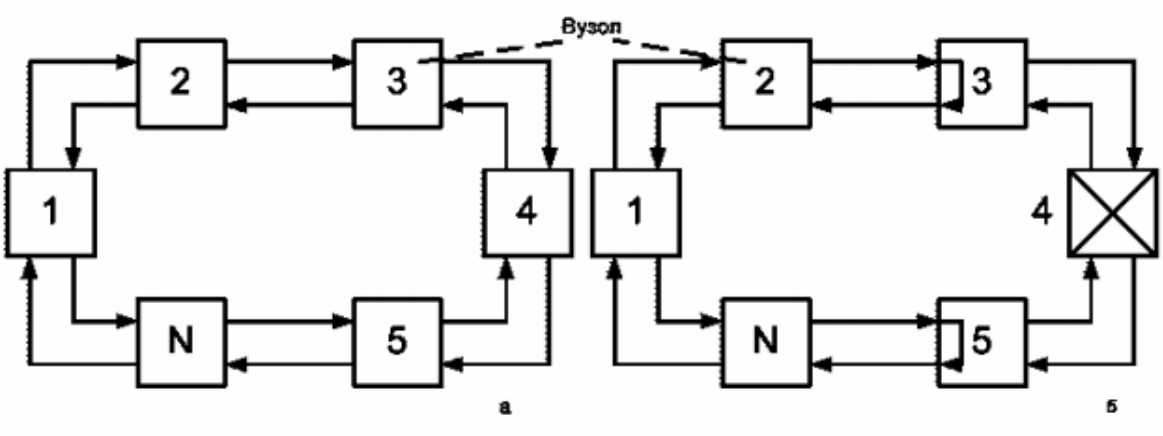

Рисунок 2.1.1.9 Структурна схема двонаправленого кільця: а- вихідна конфігурація, б- реконфігурована мережа при пошкодженні вузла 4

Якщо будь який вузол у кільці виходить із ладу, то це викликає перерив зв'язку всієї мережі. Система також перестає працювати при пошкодженні (обриві) будь-якого із сегментів волокна у кільці. Модифікація однонаправленого кільця може вирішити цю проблему. Наприклад, є можливість установити оптичний обхідний перемикач, щоб забезпечити оптичний обхід непрацездатного вузла, поки виконується його ремонт. Іншим варіантом є створення другого кільця, рис. 2.1.1.9 [17]. У другому кільці інформація передається в зустрічному напрямку. У звичайному режимі функціонує тільки основне кільце. Проте коли вузол або волокно виходить з ладу, мережа модифікується так, що інформація передається по кільцю, з якого виключений один або кілька сегментів. На рис.2.1.1.9,б показано шлях сигналу

в ситуації, коли сталося пошкодження вузла 4 і мережа реконфігурувалася у ЛОМ типу "розподілений інтерфейс передачі даних по волокну" (fiber distributed data interface - FDDI) використовується архітектура подвійного кільця.

2.1.7 Гібридні системи розподілу

Комбінації Т-подібної і зіркоподібної мереж забезпечують гнучкість при розробці багатотермінальних волоконних систем. У гібридній мережі, яка є комбінацією Т-подібної і зіркоподібної систем, зірка могла б з'єднувати близько розміщені термінали, а шина - більш віддалені. Може бути виконане пряме з'єднання між зіркою і Т-мережею.

Альтернативною є розробка активного ретранслятора для збільшення рівнів сигналів між зіркою і Т-мережею. На рис.2.1.1.10 показано гібридну мережу “зірка-зірка”, що використовує активний ретранслятор.

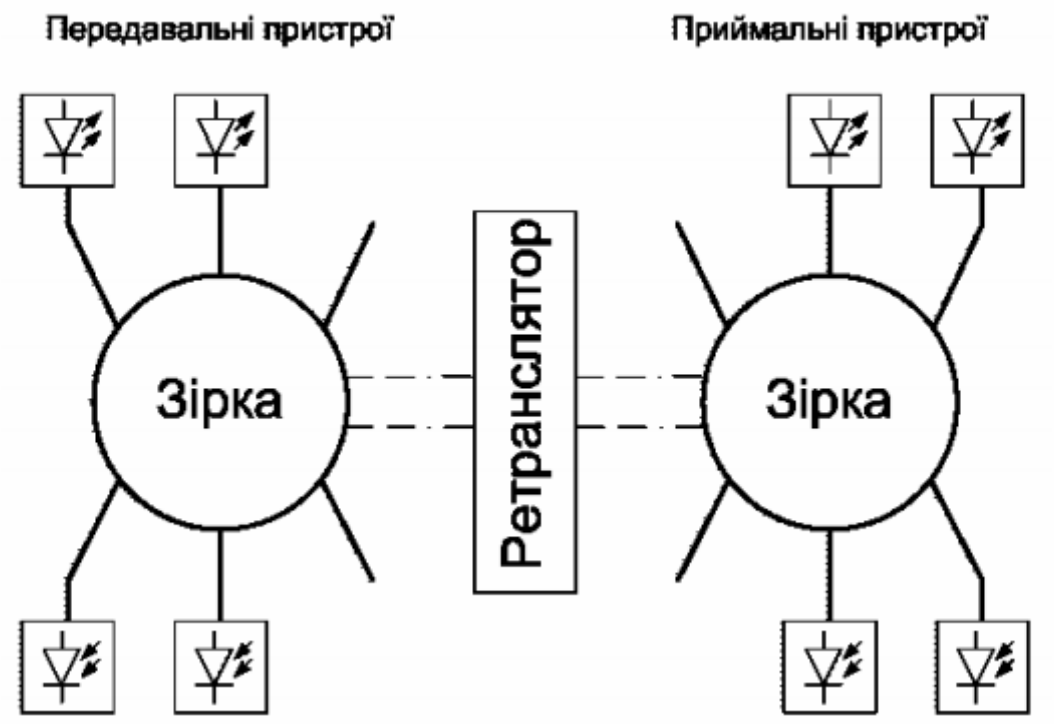

Рисунок 2.1.1.10 Структурна схема мережі типу «зірка-зірка»

2.1.8 Повнозв'язана мережа ("кожна з кожною")

Системи з N-терміналами можна створити безпосереднім з'єднанням кожного термінала з кожним, рис.2.1.1.11. У кожному передавальному пристрої світло від одного джерела подається в джгут із N - 1 волокон багатоволоконного кабелю. Щоб одержати найбільшу ефективність, площа випромінювальної поверхні джерела має дорівнювати площі джгута волокон. На кожний приймальний пристрій по одному з волокон надходить сигнал від кожного з віддалених передавальних пристроїв.

Світло з джгута волокон опромінює фотоприймач, активна поверхня якого має бути принаймні такого самого діаметра, як і у джгута. Хоча мережа з такою архітектурою потребує багато волокна, вона має деякі переваги. По-перше, тут можна використовувати джерела випромінювання з великою світловипромінювальною площею, (які забезпечують більшу потужність ніж джерело з малою площею, потрібну для збудження волокон малих розмірів).

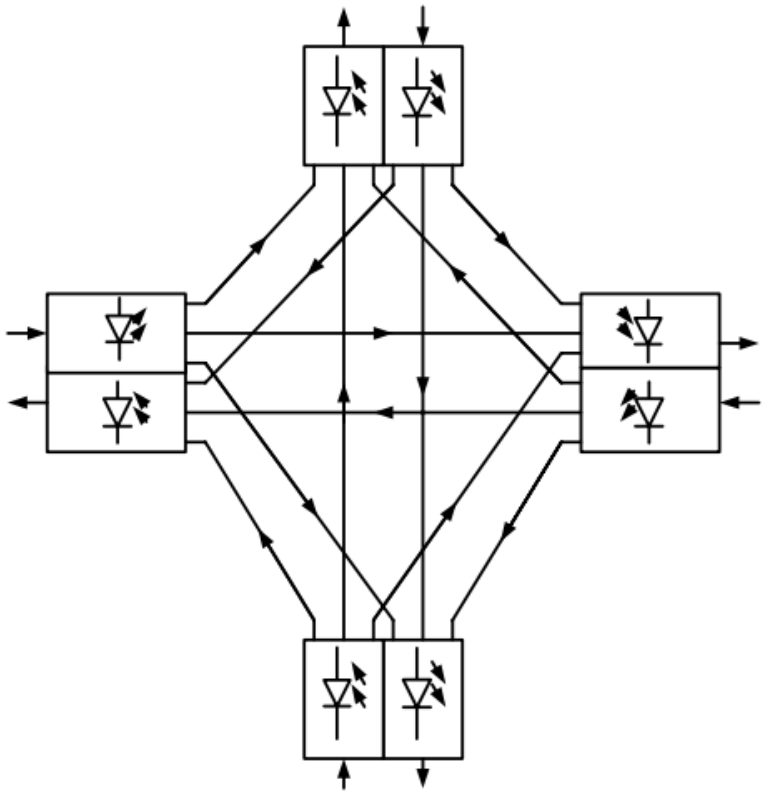

Рисунок 2.1.8.1 Повнов’язна мережа («кожна станція звя’язана з кожною»)

По друге, потужність, введена у волокно, не зазнає ослаблення через з'єднувачі або розподільні відгалужувачі як у Т-подібній, так і у зіркоподібних системах. Втрати передачі між терміналами будуть набагато нижчі ніж у Т - або в зіркоподібній. Деякі з волокон можна вимкнути, якщо не потрібно передавати сигнал між будь-якими терміналами.

Мультиволоконна мережа, що має певну складність, може бути більш економічним варіантом, ніж організація окремих "з точки в точку" ліній передачі між кожним із терміналів. У системі, що складається із ліній "з точки в точку", потрібно N - 1 передавальних і стільки ж приймальних пристроїв у кожному з терміналів при загальній кількості N(N-1) передавальних і N(N-1) приймальних пристроїв. Наприклад, чотиритермінальна двоточкова система потребує 12 передавальних і 12 приймальних пристроїв. Для мультиволоконної мережі, що використовує волоконний джгут, потрібно тільки чотири передавальних і чотири приймальних пристрої.

Розглянемо конструкції кількох чотириполюсних спрямованих відгалужувачів, що набули найбільше поширення в мережах ВОСПІ. Кожний із цих відгалужувачів використовує різні принципи відгалуження частини енергії.

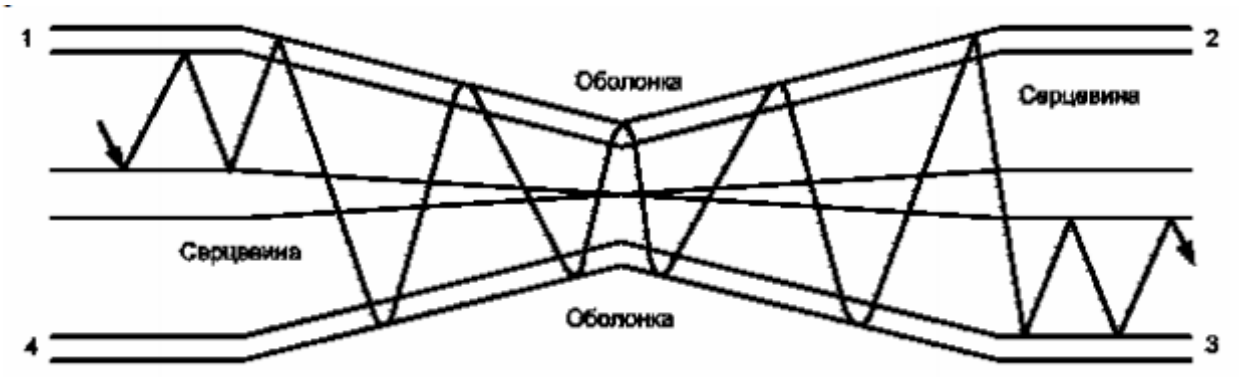

Рисунок 2.1.8.2 Повздовжній переріз біконічного спрямованого зварного відгалужувача

Конструкцію біконічного спрямованого відгалужувача, що виконується методом зварювання волокон, показано на рис. 2.1.1.12. Вона забезпечує малі

внесені втрати при великому діапазоні можливих значень коефіцієнта розгалуження. Метод виготовлення досить простий. Два одно-або багатомодові волокна скручують одне з одним з натягуванням, при нагріванні цього з'єднання волокна пом’якшуються, а їхні оболонки плавляться. Витягування пом’якшених волокон утворить біконічну плавну зміну поперечних розмірів волокон кожного з чотирьох полюсів.

У багатомодових волокнах зв'язок між волокнами виникає тому, що моди вищого порядку перестають відбиватися від поверхні розділу серцевина-оболонка, оскільки падають під кутом меншим за критичний, в звужених областях, як видно з рис. 2.1.1.12, ці моди утримуються повним внутрішнім відбиттям від зовнішньої поверхні оболонки, тобто перетворюються в моди оболонки. Промені, відповідні модам нижчого порядку йдуть під кутами, що 82 перевищують критичний кут, і не будуть перетворені в оболонкові.

Потужність, що зв'язана з цими модами, залишається в основному волокні. Оскільки зв'язані хвилеводи на рис. 2.1.1.12 мають однаковий матеріал оболонки, потужність мод вищого порядку буде переходити з оболонки одного волокна в оболонку іншого. Вихідні плавні зміни знову перетворюють моди оболонки в каналізовані серцевиною моди. Коефіцієнт розгалуження залежить від довжини області ділянки плавної зміни і товщини оболонки.

Робота одномодового біконічного відгалужувача пояснюється обміном енергії між полями, які швидко згасають і виникають в обох волокнах. Плавне потоншення волокон призводить до того, що дві серцевини наближаються одна до одної. Плавна зміна також зменшує діаметр серцевини волокон і, таким чином, знижує значення нормованої частоти (параметр V). Як випливає з рис. 2.1.1.11, зменшення параметра V збільшує розмір модової плями. Збільшений розмір плями і зменшена відстань між серцевинами збільшує область перекриття полів, які швидко згасають, що збільшує зв’язок між волокнами. При виготовленні одномодового спрямованого відгалужувача за методом механічного оброблення два оптичних волокна клиновидно вишліфовуються до

половини діаметра серцевини. Після склеювання цих волокон утворюється вихідний торець, зовнішній діаметр якого дорівнює діаметру волокна.

Цей вихідний торець склеюють (зварюють) з третім звуженим (або обшліфованим) волокном. Одномодовий відгалужувач має дуже велике практичне значення, тому більш докладно пояснимо принцип його дії. Використовуючи позначення рис.3.17, будемо вважати вхідним полюс 1, тоді зв'язок полюса 1 із полюсами 2 і 3 може бути зображений у вигляді:

$$P_2/P_1 = cos^2(\Delta\beta L),\ P_3/P_1 = sin^2(\Delta\beta L),\ (2.1.1.10)$$

де Δβ – коефіцієнт зв'язку між двома хвилеводами, рад/м, L – довжина волокна, уздовж якого існує зв'язок, м. Як видно з цих рівнянь, вхідна потужність ділиться між двома вихідними полюсами без втрат. У якісному відгалужувачі внесені втрати можуть становити усього кілька десятих часток децибела. Як випливає з попередніх рівнянь, уся потужність виходить з полюса 3, коли довжина області взаємодії:

$$L_{\text{вз}} = \pi/2\Delta\beta. \qquad (2.1.1.11)$$

Ця довжина названа довжиною зв'язку (довжиною взаємодії).

На рис. 2.1.1.13 наведено залежності потужності зв’язку від довжини області взаємодії. Відзначимо, що бажаний коефіцієнт розгалуження можна дістати добором потрібної довжини області зв'язку. Треба відзначити, що значення зв'язку періодично повторюється при збільшенні довжини взаємодії.

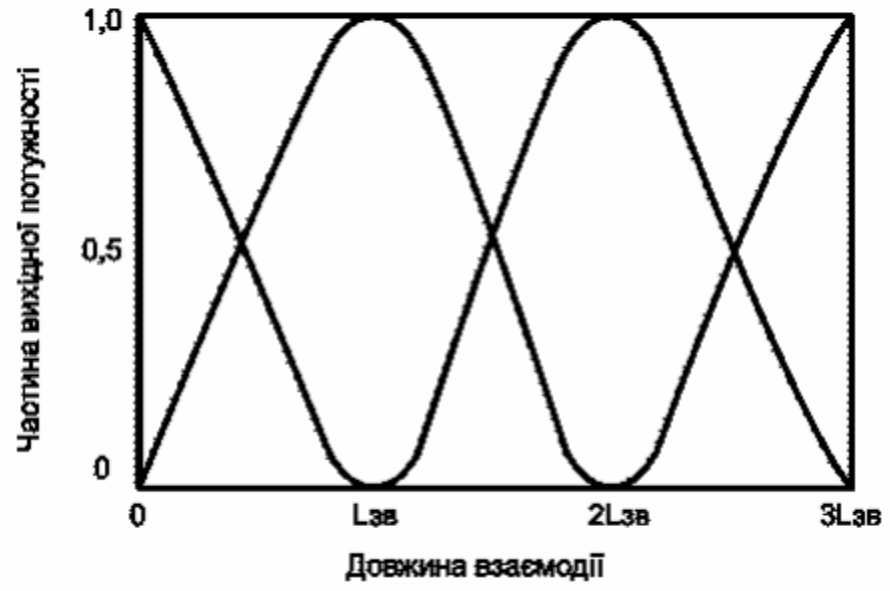

Рисунок 2.1.8.3 Залежності частини відгалужуваної потужності від довжини області взаємодії

Для створення чотириполюсного СВ можна використовувати метод зсуву торців волокон, рис. 2.1.1.14. Із вхідного полюса 1 у вихідний 2 проходить частина потужності, значення якої визначається розміром поперечного зсуву волокон.

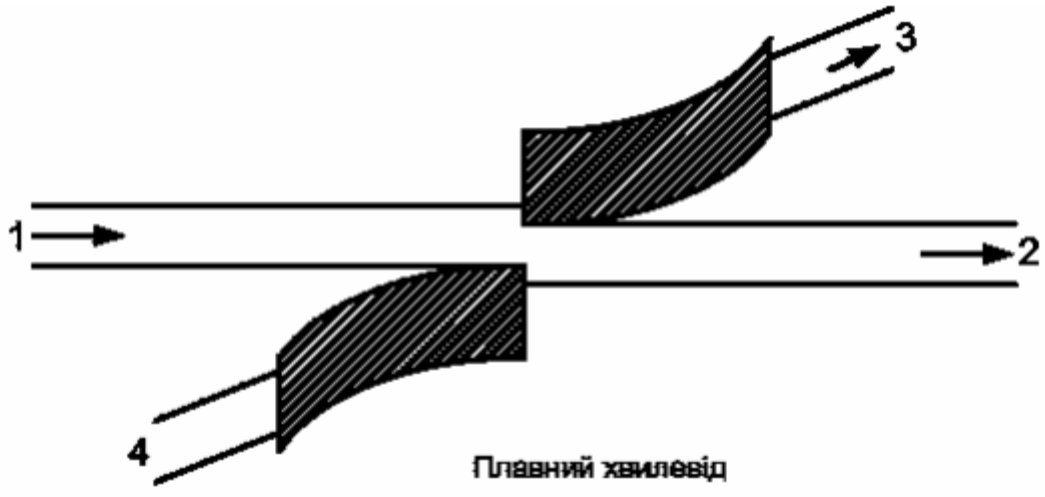

Рисунок 2.1.8.4 Поперечний переріз спрямованого відгалужувача типу «щільного з’єднання зі зсвом»

Крива на рис. 2.1.8.4 описує втрати в з'єднанні, що виникають при поперечному зсуві двох одномодових волокон. Частина світла з місця стику відгалужується в полюс 3 за допомогою планерного вигнутого пластмасового хвилеводу. Для точного установлення волокон у пластмасовому хвилеводі витравлюються канавки.

У традиційних оптичних системах в якості спрямованого відгалужувача використовують світлоділильні пристрої. Світлоділильна пластина, зображена на рис. 2.1.8.5а складається з тонкого частково відбивного покриття (діелектричного або металевого), нанесеного на прозорий прошарок. Від товщини і складу покриття залежить коефіцієнт розгалуження.

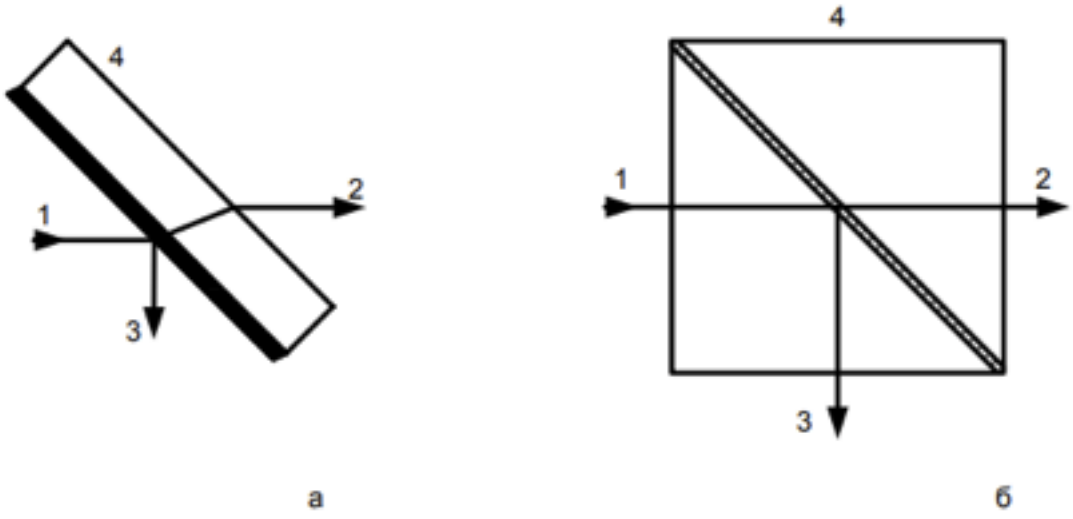

Рисунок 2.1.8.5 Хід променів спрямованих відгалужувачах світлоділильного типу: а-пластина, б-куб

Світлоділильна пластина зміщує передаваний пучок відносно падаючого пучка (поперечний зсув). Світлоділильний куб, що показаний на рис. 2.1.8.15б, усуває такий зсув. Куб складається з двох призм, розділених покриттям, що частково відбиває світло. Класичний світлоділильний пристрій не зручно використовувати для розділення потужності світла, що передається по волокну. Простір, що займає світлоділильний пристрій є еквівалентним зазору. Зазор між з'єднувальними волокнами призводить до великих втрат, тому що частина

розбіжних променів, що випромінюються передавальним волокном, не потрапляють у приймальне волокно. Колімування падаючих променів на світлоділильний пристрій і наступне фокусування (поділеного світла) у приймальне волокно вирішують цю проблему.

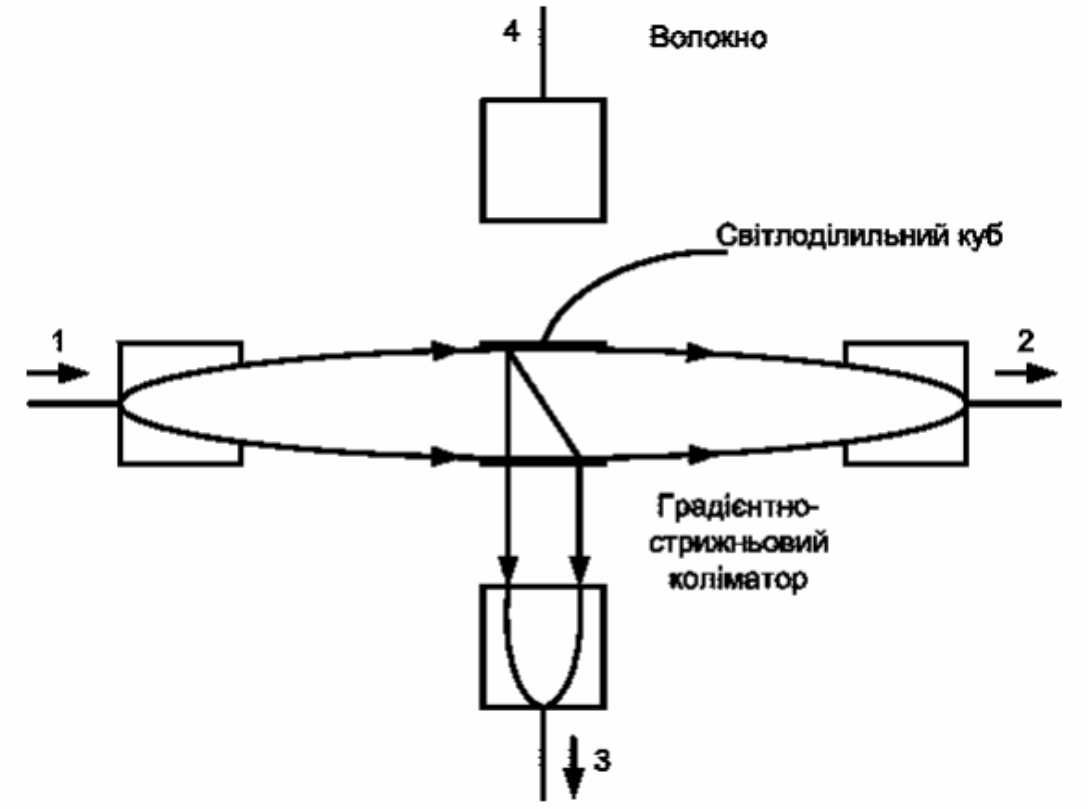

Рисунок 2.1.8.6 Конструкція спрямованого відгалужувача, що використовує градієнтно-стрижньові колімувальні лінії

На рис. 2.1.8.6 наведено конструкцію спрямованого відгалужувача світлоділильного типу, що використовує градієнтно-стрижневі лінзи (ГСЛ) для колімування і фокусування Світлоділильний куб вирівнює в лінію полюси 1 і 2 (і полюси 3 і 4). Ці полюси були б зміщені один відносно другого при використанні світлоділильної пластини Відгалужувач на рис. 2.1.8.6 також буде працездатний при заміні ГСЛ на звичайні сферичні лінзи.

2.1.9 Історія квантових обчислень та квантової інформації

Квантова інформація – новий напрямок сучасної фізики, що виник на межі дотику квантової фізики, оптики, теорії інформації та програмування, дискретної математики, лазерної фізики. Основні напрямки квантової інформації: квантові обчислення та квантові комп'ютери (quantum computing), квантова криптографія (quantum cryptography), квантова телепортація (quantum teleportation), проблеми спектроскопії поодиноких молекул та домішкових центрів. В області квантових обчислень та квантової інформації вивчають задачі з обробки інформації, які можуть бути виконані з використанням квантово-механічних систем.

20-ті рр.. XX століття вважають початком створення сучасної теорії квантової механіки. З цього часу вона стала невід'ємною частиною науки та з величезним успіхом застосовується до всього, що нас оточує, включаючи структуру атома, термоядерні реакції в зірках, надпровідники, структуру ДНК та елементарні частинки. Квантова механіка, основні ідеї якої першими сформулювали Нільс Бор, Ервін Шредінґер та Вернер Ґейзенберг, окрім апарату, який дозволяє розрахувати енергетичні стани атомів та молекул та обраховувати матричні елементи переходів між ними, містила «ідейну», філософську частину, яку зазвичай відносять до основ квантової механіки та яка не була використана до недавнього часу.

Саме ця частина квантової механіки пояснює незвичайність квантового світу. Найбільш повним є викладення цього аспекту в роботі Ервіна Шредінґера «Сучасний стан квантової механіки», яку було опубліковано в журналі Die Naturwissenschaften 29 листопада 1935 р. [5]. В ній, користуючись сучасною термінологією, обговорюється одна з проблем квантової інформації: що ми можемо дізн 4 усвідомленого Шредінгером стала необхідною під час інтерпретації експериментів, направлених на практичні застосування. Квантова механіка є математичною платформою для створення фізичних теорій.

Наприклад, квантова електродинаміка з надзвичайною точністю описує взаємодію атомів зі світлом.

Квантову електродинаміку побудовано на основі квантової механіки з додаванням специфічних правил. Зв’язок квантової механіки з конкретними фізичними теоріями схожа на зв’язок операційної системи комп’ютера з конкретною прикладною програмою: операційна система задає деякі базові параметри та режими роботи, проте не визначає, яким чином прикладні програми будуть виконувати свої специфічні задачі. Наприклад, на початку 80-х рр.. XX століття вчених зацікавило питання використання квантових ефектів для передачі сигналу зі швидкістю, що перевищує швидкість світла, що абсолютно заборонено загальною теорією відносності Ейнштейна.

Вирішення цієї проблеми зводиться до відповіді на запитання, чи можна копіювати невідомий квантовий стан. Якби копіювання було можливим, за допомогою квантових ефектів можна було б передавати сигнал зі швидкістю, більшою за швидкість світла. Однак, в загальному випадку копіювання квантового стану є неможливим в квантовій механіці.

Ця теорема про неможливість клонування (no-cloning theorem) є одним з перших результатів в області квантових обчислень та квантової інформації. З тих пір до неї було зроблено багато уточнень, тож тепер ми маємо концептуальні інструменти, що дозволяють зрозуміти, наскільки якісно може працювати пристрій квантового копіювання.

Інший історичний напрямок, що вніс вклад в розвиток квантових обчислень та квантової інформації, зародився в 70-х рр.. XX століття та пов’язаний з отриманням повного контролю над поодинокими квантовими системами. До цього часу зазвичай здійснювали контроль над об’ємним зразком. Наприклад, квантова механіка чудово пояснює надпровідність.

Проте оскільки надпровідник являє собою величезний порівняно з атомними масштабами зразок, ми можемо досліджувати лише незначну кількість аспектів його квантово-механічної природи. При цьому окремі квантові системи, з яких складається надпровідник, лишаються недоступними.

Такі пристрої, як 5 прискорювачі частинок, дозволяють отримувати обмежений доступ до окремих квантових систем, але не дають повного контролю над поодинокими квантовими системами. Починаючи з 70-х рр. було розроблено багато методів керування поодинокими квантовими системами, як наприклад, утримування одиночного атома а «атомній пастці», яке забезпечує його ізоляцію від оточуючого середовища та дозволяє з високою точністю досліджувати різноманітні а 6 «аналітичну машину» Беббіджа, запропонувавши в середині 30-х рр. XX століття універсальну машину Тьюрінга – повну можель класичного обчислення.

Сучасні комп'ютери не є машинами Тьюрінга, проте при цьому їх обчислювальна потужність еквівалентна (в технічному смислі) потужності машини Тьюрінга. Весь процес розвитку торкається лише розмірів та швидкодії, але не змінює основні принципи структури та роботи комп'ютера. Однак квантова механіка ставить питання про можливість подібних змін. Наразі ключовим фактором збільшення швидкодії обчислювальних машин є зменшення розміру транзисторів, які використовуються в сучасних процесорах.

В травні 2018 р. компанія Intel презентувала процесор Intel Cannon Lake на основі нанотехнології 10 нм (реалізовано в ноутбуці Lenovo Ideapad 330 з CPU Intel Core i3-8121U). Нещодавно корпорація IBM спільно з компаніями Samsung та GlobalFoundries анонсувала створення технології виробництва процесорів з топологією 5 нм. В масове виробництво така технологія буде впроваджена в 2020 р. Якщо розмір транзистора стає співвимірним з розмірами атома, виникає ефект так званого «квантового тунелювання», при якому електрони починають вільно проходити між полюсами транзисторів. Такі ефекти обумовлюють принципові обмеження в існуючих комп'ютерних технологіях.

Очевидно, що ера кремнієвої електроніки близька до завершення, на зміну нанотехнологіям приходять біотехнології, що оперують молекулами ДНК, та квантові технології, що оперують іонами, атомами та елементарними частинками. У витоків ідеї створення квантового комп'ютера стояв один з

найбільш яскравих фізиків-теоретиків – Річард Фейнман. В своїй роботі [2] він звернув увагу на те, що моделювання навіть простих фізичних систем на класичному комп’ютері потребує неймовірного об’єму обчислювальних ресурсів, що унеможливлює розв’язок задачі.

В той же час, завжди можна поставити фізичний експеримент з квантово-механічною системою й отримати шуканий результат. Квантовий комп’ютер, побудований на основі квантових частинок та який функціонує за квантовими законами, буде здатен реалізувати обчислення, які недоступні для класичних комп’ютерів або потребують надто багато часу навіть у випадку використання потужних обчислювальних ресурсів. 7 Це буде можливим, зокрема, завдяки ефекту «квантового паралелізму», про який йтиме мова нижче.

На початку 1990-х рр. кілька авторів займались пошуком задач, чий розв’язок за допомогою квантового комп’ютера є більш ефективним, ніж з використанням звичайного класичного комп’ютера. У 1994 р. Даніель Саймон зробив важливе відкриття, описавши ефективний квантовий алгоритм для розв’язку задачі, що не мала адекватних класичних альтернатив навіть за умови використання імовірнісних методів.

Це відкриття надихнуло Пітера Шора, який у 1994 р. запропонував алгоритм, що був не лише ефективним для реалізації на квантовому комп’ютері, але й дозволив вирішити фундаментальну задачу інформатики: розклад на множники простих цілих чисел [3]. Шор, застосовуючи метод квантового перетворення Фур’є, описав як розклад на множники, так і задачу знаходження дискретного логарифму. Зв'язок між квантовою механікою та теорією інформації виник після усвідомлення того факту, що такі прості властивості квантових систем, як невідворотне руйнування квантового стану під час вимірювань, можна використати в практиці квантової криптографії. Квантова криптографія об’єднує кілька ідей, з яких незмінною є ідея квантової передачі коду.

В цьому методі квантові стани використовуються для особливого завдання зв’язку: встановити в двох точках, що знаходяться на відстані, пару

ідентичних, проте випадкових послідовностей двійкових чисел таким чином, щоб вони залишались невідомими для третьої особи. Подібна випадкова послідовність може бути використана в якості криптографічного коду для забезпечення захищеного зв’язку. Принципи квантової механіки забезпечують абсолютне збереження квантової інформації, унеможливлюючи отримання її третім лицем.

На даний момент на ринку існують комерційні пристрої для створення квантових ліній зв’язку (QPN Security Gateway фірми MagiQ Technologies (США), криптосистеми Clavis та Cerberis фірми ID Quantique (Швейцарія)). У 2016 р. .Китай вивів на орбіту перший супутник квантового зв’язку Micius, у 2017 р. було повноцінно розгорнуто супутникову квантову комунікаційну систему. 8 Не дивлячись на значний інтерес до області квантової інформації, зусилля з побудови систем її обробки наразі мають невеликий успіх. Сучасна техніка для квантових обчислень представлена невеликими квантовими комп’ютерами, які здатні виконувати десятки операцій над невеликою кількістю квантових бітів (кубітів).

Було продемонстровано експериментальні прототипи пристроїв для реалізації квантової криптографії – способу секретного зв’язку на великих відстанях – й навіть на такому рівні, коли вони є корисними для реальних застосунків. Однак розробка технологій для реалізації крупномасштабної обробки квантової інформації залишається серйозним завданням для фізиків та інженерів, яке буде розв’язане в майбутньому. Фізика традиційно є дисципліною, де основну увагу зосереджено на розумінні «елементарних» об’єктів та простих систем, проте багато цікавих аспектів Природи проявляються лише зі зростанням розмірів та складності.

Такі явища частково досліджуються в хімії та інженерних науках, але, нажаль, специфічним методом. Квантові обчислення та квантова інформація - нові інструменти, які дозволять створити зв'язок між простим та відносно складним: у сфері обчислень та алгоритмів є систематичні засоби для побудови та вивчення таких систем. Застосування ідей з цих областей вже призвело до

появи нових поглядів на фізику, тому слід сподіватись, що в майбутньому такий підхід буде успішно застосовано в усіх розділах фізики.

2.1 Квантова криптографія

Квантова криптографія – розділ квантової інформатики, що вивчає методи захисту інформації шляхом використання квантових носіїв. Можливість подібного захисту забезпечується фундаментальною теоремою про неможливість клонування невідомого квантового стану.

Квантова теорія, що прийшла на зміну класичним уявленням про світ, принесла з собою цілий перелік обмежень на можливість маніпуляції фізичними об’єктами. Принцип невизначеності Ґейзенберга постулює неможливість одночасного вимірювання координати та імпульсу частинки з довільною точністю. Постулат про редукування хвильового пакету, висунутий фон Нейманом, вказує на неможливість в загальному випадку вимірювання квантової системи без руйнування її стану. Відкритий у 1982 р. принцип квантової неклонованості стверджує, що неможливо створити копію (клон) квантової системи як завгодно близько до оригіналу.

З практичної точки зору ці та подібні до них обмеження тривалий час мали негативний характер, показуючи, що при досягненні певної точності в роботі апаратури виникають додаткові складності, пов’язані з квантовою природою фізичних об’єктів, такі як «квантовий шум» оптичного каналу зв’язку, «квантовий шум» фотодетектора тощо. Тож дивовижним нововведенням стала ідея застосування квантових методів в таких застосунках, які потребують захисту від дій зловмисника, та обмеження можливостей останнього на основі фундаментальних квантових законів.

Таким чином, «негативні» властивості квантових систем, такі як чутливість відносно вимірювання, стають позитивними у випадку, коли з нею стикається зловмисник. Історично першою задачею такого типу була ідея створення «квантових грошей», захищених від підробки за допомогою

спеціальних маркерів, які неможливо скопіювати. Над цим завданням працював американський вчений Візнер в 70-ті рр. XX століття.

Проте його роботи так і не було опубліковано свого часу, тому народження нового напрямку зазвичай пов’язують з іменами 55 Ч. Беннета та Ж. Брассара, які запропонували використання дворівневої квантової системи для розподілу між двома користувачами секретного ключа, не доступного для зловмисника, що прослуховує канал зв’язку.

Однак у 80-ті рр.. цією проблемою займалось вузьке коло людей, оскільки основна ідея Беннета та Брассара (протокол BB84) була опублікована у 1984 р. в працях маловідомої конференції, після чого всі роботи у США за цією тематикою було засекречено. Широко відомими вони стали лише у 1991 р., коли англійський вчений А. Екерт опублікував абсолютно інший метод вирішення цієї проблеми – захищеного від перехоплення розподілу ключів. Метод, запропонований Екертом, спирався не лише на використання дворівневих квантових систем, а й на використання сильних квантових кореляцій (сплутування) між ними.

Дуже скоро після цього було опубліковано розсекречені результати групи Беннета з успішної експериментальної реалізації квантового розподілу ключів на поодиноких фотонах у відкритому просторі. З цього моменту новий науковий напрямок, який отримав назву квантової криптографії, став інтенсивно розвиватись, захоплюючи спеціалістів з різних областей – математичної теорії інформації, квантової оптики, фізики твердого тіла, квантової теорії тощо. Було запропоновано багато нових протоколів та випробувано різноманітні методи їх реалізації, виконана важлива робота з доведення безумовної захищеності квантових протоколів від перехоплення та розроблені комерційні квантові криптосистеми.

На черзі стоїть розробка глобальної супутникової криптографічної мережі та розширення наземних мереж на трансконтинентальні відстані за допомогою використання квантових повторювачів. У 2016 р. Китай вивів на орбіту перший супутник квантового зв’язку Micius, вже у 2017 р. було апробовано квантову

комунікаційну систему з його використанням: було здійснено сеанс зв’язку через супутник між китайською та австрійською Академіями наук.

2.1.1 Поняття про криптографію.

Історично під криптографією розуміли мистецтво тайнопису – перетворення тексту в незрозумілий шифр з метою захисту його від сторонніх очей. При цьому перетворення C f T = ( ) повинне бути оборотним, так щоб застосування оберненого перетворення ( ) 1 T f C − = дозволило отримати вихідний текст. Шифрування тексту може відбуватись як для захищеного збереження інформації, так і для секретного пересилання інформації до партнерів, що мають в наявності алгоритм дешифрування.

Таким чином, традиційно криптографія забезпечувала конфіденційність (confidentiality) інформації навіть за умови доступу сторонніх до її носіїв. В сучасному інформаційному світі, значною мірою пов’язаному з цифровою технікою, поняття криптографії розширилось, наразі воно пов’язане з комплексними методами захисту інформації, які окрім її конфіденційності забезпечують також її цілісність (data integrity) та проведення процедури аутентифікації (authentification). Цілісність інформації – це неможливість її непомітної зміни або повної підміни, аутентифікація – встановлення особистостей сторін, які вступають в обмін інформацією, або у встановленні джерела інформації.

Таким чином, захист інформації полягає в охороні законних користувачів, що здійснюють обмін інформацією, від дій зловмисника. В поняття захисту інформації іноді включають також захист законних користувачів один від одного, що є важливою вимогою в електронній торгівлі. Очевидно, що криптографія відрізняється від інших способів захисту своїми специфічними методами. Ще на початку 1990-х рр. криптографію визначали як науку, що вивчає математичні методи захисту інформації. Однак з виникненням квантової криптографії це визначення стало занадто вузьким. Тому криптографію будемо

визначати як науку, що вивчає методи захисту інформації, засновані виключно на варіюванні способу її запису. 57 7.2. Квантовий розподіл ключів. У 1949 р. С. Шеннон, спираючись на розроблену ним теорію інформації, довів теорему, що криптосистема є абсолютно секретною, якщо секретний код істинно випадковий та використовується лише один раз.

Однак на практиці реалізація такої системи наштовхується на серйозні труднощі, одна з них – створення та передача великого секретного коду, необхідного кожного разу, коли надсилається нове повідомлення. Вирішити цю проблему можна було б за наявності фізичного каналу, секретність якого забезпечується фізичними законами.

Саме такий канал представляє квантова фізика. Практичні можливості, які відкриває теорема про неклонованість квантового стану, призвели до розробки ряду суттєвих квантових криптографічних примітивів. Ми розглянемо найбільш важливий з них – квантовий розподіл ключів (КРК). КРК вирішує основну проблему симетричного шифрування – генерацію двох ідентичних реплік ключа для двох віддалених користувачів таким способом, що третя репліка ключа не може існувати в природі. Для передачі секретного повідомлення на практиці завжди застосовується комбінація КРК, симетричного шифрування та інших примітивів класичної криптографії [16].

Переваги КРК перед асиметричними технологіями розподілу ключів полягають в його безумовній захищеності, тобто за відсутності припущення про обчислювальні ресурси зловмисника. Крім того, безпека асиметричного шифрування має серйозну загрозу з боку квантових комп’ютерів, які з використанням алгоритму Шора можуть зламати такий шифр.

Теорія захищеного розподілу ключа з використанням квантових каналів зв’язку стрімко розвивалась протягом короткого часу. Ідея використання неклонованості та неможливості точного вимірювання невідомого одиночного квантового стану для створення секретних повідомлень була висловлена в роботі Візнера у 1983 р. [17]. Конкретні протоколи криптографії такого виду

були розроблені незалежно Беннетом та Брассаром [18] (BB84, B92) та Екертом [19].

Цих робіт виявилось достатньо для стимулювання серйозної експериментальної роботи, яка триває по сьогодні. 58 Справжня революція в області доведення захищеності КРК була розпочата Майєрсом наприкінці 90-х рр. [20], який довів, що протокол BB84 є абсолютно захищеним для достатньо низького детектованого рівня помилок у квантовому каналі. Наразі діяльність в області доведення захищеності протоколів розподілу ключа не можна вважати завершеною.

Досі існують важливі фундаментальні та практичні питання, пов’язані з неідеальними джерелами. Існує маса технічних питань (наприклад, використання слабких когерентних джерел), які заслуговують на теоретичний розгляд.

2.1.2 Змішані стани

Під час проведення перших дослідів над елементарними частинками було виявлено, що їх поведінку доволі важко описати, ґрунтуючись на вже існуючих представленнях про фізичні явища. Це призвело до того, що при формулюванні нових законів, описуючих поведінку елементарних частинок, цю частину фізики почали називати квантовою теорією, а ту частину фізики яка вже склалась – класичною.

Одна з головних відмінностей класичної фізики від квантової теорії проявляється вже в визначенні квантової частинки і її стану. Представлення частинки як тіла, що має визначені координати, розміри і масу, виявилось зовсім неправильним, так як для деяких таких частинок не вдавалося навіть зрозуміти, в якій точці простору вони знаходяться. Проте виявилось можливим передбачити поведінку таких частинок. Однак складність полягала в тому, що для пояснення цієї поведінки потрібно відмовитись від традиційних фізичних характеристик. Це призвело до того, що стан будь-якої елементарної частинки

(або системи) стало представлятися за допомогою "хвильової функції" - принципіально нового об'єкта квантової картини світу.

Для початку потрібно ввести поняття чистого квантового стану. Таким станом будемо називати вектор в гільбертовому просторі H з одиничною нормою. Під нормою вектора розуміється корінь з його скалярного квадрата $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$ $\psi \in$ H .

Для кожного чистого квантового стану $|\psi\rangle$ можна визначити відповідний йому оператор $\rho_\psi = |\psi\rangle\langle\psi|$, який називається оператором щільності. Даний оператор має ранг 1 і дорівнює одиниці, і він діє як проектор на чистий стан $|\psi\rangle$.

За допомогою операторів щільності вводиться загальне поняття квантового стану[1]. Змішаним квантовим станом називається статистична суміш декількох чистих станів:

$$\rho = \sum_\iota \rho_\iota |\psi_\iota\rangle\langle\psi_\iota|, \rho_\iota \geq 0 \ \forall_\iota, \ \sum_\iota \rho_\iota = 1. \qquad (1.1)$$

Очевидним є те що слід змішаного стану дорівнює одиниці. Його позитивна визначеність визначається таким чином:

$$\langle\varphi|\rho|\varphi\rangle = \sum_\iota \rho_\iota |\langle\varphi|\psi\rangle|^2 \geq 0 \quad \forall_{|\varphi\rangle} \in H \qquad (1.2)$$

Далі, будь-який ермітів оператор A, має спектральне розкладання:

$$\mathrm{A} = \sum_\iota \lambda_\iota |\lambda_\iota\rangle\langle\lambda_\iota| \qquad (1.3)$$

де власні значення λ_ι речові, а власні вектори $|\lambda_\iota\rangle$ нормовані і ортогональні. Це означає, що в будь-який позитивний ермітів оператор з одиничним слідом можна назвати оператором щільності деякого квантового стану: з позитивної

визначеності отримуємо позитивність всіх власних значень, а з умови одиничного сліду – сума власних значень дорівнює одиниці, з цього випливає, що така комбінація може трактуватись як статистична суміш.

Це приводить до загального визначення квантового стану: позитивний ермітів оператор в гільбертовому просторі H з одиничним слідом.

Квантові стани складають безліч операторів в просторі над H. Множину квантових станів прийнято позначати S(H). Крайніми точками цих станів є чисті квантові стани, які описуються операторами ранга 1.

Ключовий закон квантової механіки – рівняння Шредінгера, яке описує зміну квантових станів в часі. Традиційно в квантовій механіці рівняння описується:

$$\iota\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle \qquad (2.2.2.1)$$

де $\hbar$ - стала Планка і приблизно дорівнює $1{,}054 \cdot 10^{-34}$.

Ермітів оператор H називається гамільтаніоаном системи і саме він впливає на її еволюцію.

Відповідність між ермітовими і унітарними операторами:

$$U = e^{\iota H} \qquad (2.2.2.2)$$

Рівняння Шредінгера може бути записано в вигляді[2]:

$$|\psi'\rangle = U|\psi\rangle.$$

В подальшому саме цей вид рівняння Шредінгера приймається як найбільш прийнятний, він означає, що будь-яка еволюція квантової системи може бути представлена як дія унітарного перетворення.

2.1.3 Квантові вимірювання

Відмінність вимірів в квантовій теорії і класичній фізиці є те, що у випадку виміру квантової системи її початкове значення змінюється.

В будь-якому експерименті можна виділити дві стадії: підготовку стану та його вимірювання. Вимірювання не повинно давати точно очікуваний результат, в загальних випадках результат виміру – набір вихідних даних з деякими очікуваннями.

Неточні виміри. Досить часто на практиці зустрічається ситуація, коли результат вимірювань відомий неточно, тобто відомо, що результат відповідає деяким значенням, який належить деякій множині значень. Це трапляється через шум показників приладу, що в свою чергу не дає можливості достигнути необхідної точності. Така ситуація завжди має місце при вимірі неперервних змінних. В такому випадку результату виміру g_ι відповідає оператор $G_\iota = \sum_{S_\iota \epsilon \gamma_\iota} |S_\iota\rangle \langle S_\iota|$, а ймовірність виміру g_ι представляється виразом[3]:

$$\mathrm{p}_\iota = Tr\{G_\iota \rho\} \qquad (1.6)$$

де ρ – оператор щільності вимірюваної системи.

Після виміру система переходить в змішаний стан з оператором щільності.

Узагальнені виміри – в загальному випадку набору результатів вимірів $\{g_\iota\}$ відповідає набір позитивних операторів $\{G_\iota\}$, виконується розкладання одиниці $\sum_\iota G_\iota = 1$.

Вимір називається узагальненим і міра ймовірності є позитивно-операторною мірою. Отримання будь-якого результату виміру не завжди може надати однозначну відповідь про стан системи.

2.2. Оптичне поле

Фізичний об’єкт за допомогою якого реалізується квантова криптографія – оптичне поле, або електромагнітне поле оптичного діапазону. Послаблення або збудження оптичного поля може відбуватись порціями, а саме фотонами, енергія фотона $\hbar\omega$, де ω – частота, $\hbar = h/2\pi$ [3]. Оптичне поле представляється у вигляді набору його складових, а саме мод поля.

Мода поля - це стабільний стан електромагнітного поля всередині світловоду. Є одним з рішень рівнянь Максвелла для певної, заданої умовами структури. Моди поля в вільному просторі з граничними умовами на деякій поверхні, наприклад куб L^3- найпростіший випадок. В такому випадку поле представлено в вигляді разкладу по плоских бігучих хвилях. Під час розкладання кожна мода характеризується:

1) хвилевим вектором, який визначає направленість розповсюдження і частоту коливать. Проекції хвилевого вектора на грані куба кратні $2\pi/L$, згідно до умови періодичності[3].

2) направлення коливань вектора напруженості Е. Зважаючи на силу поперечного характера електромагнітної хвилі, існує два незалежних направлення коливань напруженості Е, які задаються двома одиничними векторами поляризації, які лежать в площині, перпендикулярній хвилевому вектору[3]. Нормуючий множник, вибраний таким чином, щоб амплітуди були безрозмірними. В класичній електродинаміці ці амплітуди є комплексними числами. В квантовій теорії оператори еквівалентні комутаційним співвідношенням для системи гармонічних осциляторів, які в свою чергу відповідають своїй моді.

Поле еквівалентного набору гармонічних осциляторів, повна енергія яких виражається:

$$H_n = \frac{1}{8\pi}\int((E^{(-)}(r,t)\cdot E^{(+)}(r,t)) + \text{ерм. опір.})dV = \sum_v \hbar\omega(a_v + a_v + 1/2),$$

де інтегрування виконується по об’єму квантування поля L^3, a_v – оператори породження або знищення фотонів.

Оптичне поле – моди плоскої біжучої хвилі, варто відмітити, що реальні об’єкти з якими мають справу в експериментах відрізняються один від одного поляризаційним індексом.

Світловий пучок з заданим хвильовим вектором еквівалентний двом гармонічним осциляторам або модам, відповідним двом ортогонально поляризованим коливанням електромагнітного поля.

2.2.1 Однофотонні оптичні імпульси

У випадку коли відомо, що об’єкт має один фотон, стан його задається суперпозицією двох однофотонних станів гармонічних осциляторів, які відповідають двом ортогональним поляризованим коливанням електромагнітного поля.

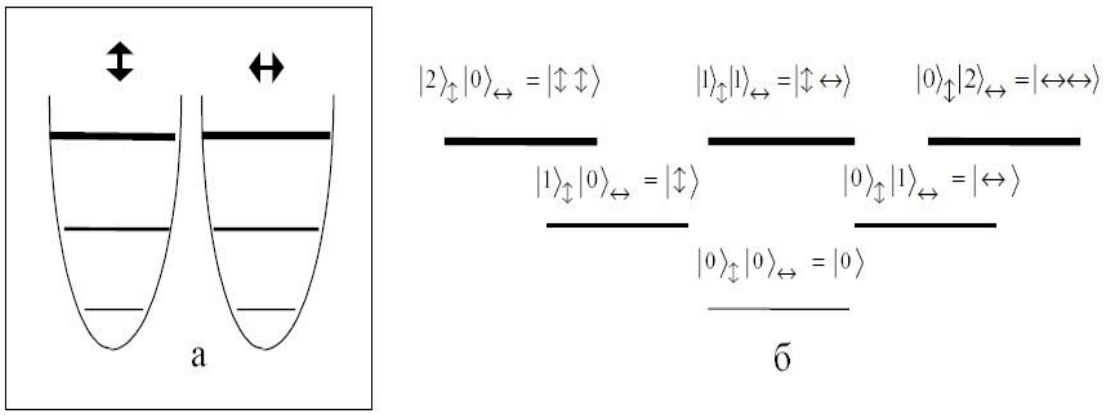

Рисунок 2.2.5.1 Світловий пучок з заданим хвильовим вектором

а) однофотонний стан пучка визначається суперпозицією двох породжених станів поляризованих фотонів;

б) двохфотонний стан пучка в загальному випадку є суперпозицією трьох енергетично породжених станів, два з яких - пара тотожно поляризованих фотонів, а одне – пара ортогонально поляризованих фотонів.

Коли мова йде про поляризаційні стани одного фотона – мають на увазі стан двохрівневої системи[3]:

$$\left|1_{\text{фотон}}\right\rangle = \mathrm{C}_{\leftrightarrow}\left|\leftrightarrow\right\rangle + C_{\updownarrow}|\updownarrow\rangle.$$

Під час проекційних вимірів детекторами одиночних фотонів, перед якими розміщені поляризатори, виділяючи горизонтальну або вертикальну поляризації, ймовірність відповідного вимірювання дорівнює $|C_{\leftrightarrow}|^2$ або $|C_{\updownarrow}|^2$. Якщо використовувати перед детекторами поляризатори, виділяючи поляризацію в 45° і 135°, то ймовірність їх спрацювання буде - $|C_{\leftrightarrow} + C_{\updownarrow}|^2$ або $|C_{\leftrightarrow} - C_{\updownarrow}|^2$ відповідно[3]. З цього випливає, що в діагональному базисі стан одного фотона можна еквівалентним шляхом представити в вигляді:

$$\left|1_{\text{фотон}}\right\rangle = \frac{(\mathrm{C}_{\leftrightarrow}+\mathrm{C}_{\updownarrow})}{\sqrt{2}}\left|\nearrow\right\rangle + \frac{(\mathrm{C}_{\leftrightarrow}-\mathrm{C}_{\updownarrow})}{\sqrt{2}}\ |\nwarrow|.$$

Поняття один фотон в розглянутому виникло як одне збудження об’єкта – світловий пучок з заданим хвильовим вектором, який складається з двох мод поля. Такий об’єкт є делокалізованим в просторі і не відповідає представленню про фотони, які локалізованих частинках, поширюваних у вільному середовищі зі швидкістю світла. Питання щодо локалізації фотона вирішується, беручи до уваги обставини в теоретичних міркуваннях про розповсюдження фотонів завжди присутнє поняття початкової (кінцевої) просторово-часовох точки, поява (зникнення) фотона.

Локальність зникнення фотонів можна спостерігати за допомогою детекторів незалежно від локальності реєстрованого поля. Локальність появи фотона можна спостерігати, використовуючи джерела такого ж розміру. Однак, зважаючи на геометричний фактор, таке джерело буде обов’язково збуджувати ряд делокалізованих мод поля і тим самим створювати польовий об’єкт, який вже локалізований в просторі.

Для прикладу квантого об’єкта, який складається з багатьох мод поля демонструючого розповсюдження локалізовані однофотонні імпульси світла. Світловий імпульс з заданим направленням хвильового вектора – багатоходовий об’єкт, створений з різночастотних мод поля. В залежності від розподілення амплітуд вхідних в нього мод, даний квантовий об’єкт може представляти собою різні по формі світлові імпульси, розповсюджувані в заданому направленні. До речі, чим ширше розподілення мод, тим більше локалізований відповідний імпульс світла.

Для визначення припустимо, що направлення розповсюдження імпульса співпадає з віссю z, то хвильові вектори плоских мод поля, що створюють імпульс, визначаються наступними декартовими компонентами[3]:

$$k_k = \left\{k_{kx} = 0, k_{ky} = 0, k_{kz} = \frac{2\pi}{L} m_z\right\} \qquad (2.2.5.1)$$

Стан данного об’єкта в загальному випадку може бути таким складним, яким може бути сукупність станів сукупності гармонічних осциляторів. Простий приклад стану, відповідному однофотонному збудженню мод поля: $|\psi_{\text{однофотонний імпульс}}\rangle = \sum_v c_v a_v + |0\rangle$,

де $|0\rangle$ - вакуумні стани мод поля, c_v - комплексні амплітуди, квадрати модулів яких визначають ймовірність виявити фотон в v - моді.

2.2.2 Когерентні і інші стани оптичних полів

Когерентний стан було відкрито Шредінгером (Schrqdinger, 1926) під час розгляду гармонічного осцилятора і визначалось як стан з мінімальною невизначеністю. Когерентні стани є важливими для опису квантового опису оптичної когерентності.

Сам термін когерентності в квантовій оптиці ввів Глаубер (Glauber, 1963). Хвильова функція, яка використовується для класичного описання

електромагнітного поля повинна мати мінімальну невизначеність для всіх відрізків часу[2]. Такою властивістю володіє хвильова функція основного стану зміщеного простого гармонічного осцилятора, яка представляє собою хвильовий пакет, що виконує синусоїдальні коливання в потенціальному полі.

Відповідний вектор стану представляє собою когерентний стан і позначається $|a\rangle$. В квантовому стані гармонічного осцилятора хвильовий пакет не розбігається, а його центр рухається по класичній траєкторії. З класичної точки зору електромагнітне поле складається з хвиль із зазданими значеннями амплітуди і фази. Але при квантово-маханічному описі поля цей опис повністю відрізняється. В нашому випадку займають місце флуктуації як амплітуди, так і фази поля. Електромагнітне поле в стані $|n\rangle$, заданим числом частинок має визначену амплітуду, але повністю невизначену фазу, тоді як поле в когерентному стані має однакові величини невизначеності для двох змінних.

Вектор стану $|\psi(t)\rangle$, повної системи задовольняє рівняння Шредінгера:

$$\frac{d}{dt}|\psi(t)\rangle = -\frac{i}{h}H|\psi(t)\rangle,$$

$$|\psi(t)\rangle = \prod_k \exp(a_k a_k^+ - a_k^+ a_k)\,|0\rangle_k,$$

де $|\psi(0)\rangle$, початкове значення є вакуумним $|0\rangle$. $\hat{\varepsilon}_{\mathbf{k}}$ одиничний ветор поляризації $E_к$ - напруженість електричного поля, $\hat{\varepsilon}_{\mathbf{k}}$ - частота.

$\alpha_{\mathbf{k}} = \frac{1}{\hbar \nu_{\mathbf{k}}} E_{\mathbf{k}} \int_0^{t'} dt' \int d\mathbf{r}\, \hat{\varepsilon}_{\mathbf{k}\mathbf{k}} \mathbf{J}_\nu(\mathbf{r},t) e^{i\nu_{\mathbf{k}}t' - i\mathbf{k}\cdot\mathbf{r}}$ стан поля $|\{\alpha_{\mathbf{k}}\}\rangle$ називається когерентним станом і позначається багатомодовий когерентний стан $|\{\alpha_{\mathbf{k}}\}\rangle = \prod_{\mathbf{k}} |\alpha_{\mathbf{k}}\rangle$, $|\alpha_{\mathbf{k}}\rangle = \exp\left(\alpha_{\mathbf{k}} a_{\mathbf{k}}^+ - \alpha_{\mathbf{k}}^* a_{\mathbf{k}}\right)|0\rangle_{\mathbf{k}}$ когерентний стан поля, як власний стан оператора знищення a, з власним значенням α.

$a|\alpha\rangle = \alpha|\alpha\rangle$, стан $|\alpha\rangle$ можна виразити через стан з заданим числом частинок $|n\rangle$ наступним чином: $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$, $|\alpha\rangle D(\alpha)|0\rangle$, $|\alpha\rangle = e^{\alpha a^+}|0\rangle e^{-|\alpha|^2/2}$,

$D(\alpha)=e^{-|\alpha|^2/2}e^{\alpha a^+}e^{-\alpha^* a}$ [4]. Згідно з виразом когерентний стан отримуємо в результаті використання оператора зміщення до вакуумного стану. Відповідно когерентний стан представляє собою зміщення основного стану гармонічного осцилятора. Для прикладу уявимо, що в момент часу t = 0 хвильова функція $\psi(q,t)$, $\Delta p\Delta q=(n+\frac{1}{2})\hbar$ має вигляд хвильового пакету з мінімальною невизначеністю, зміщеного в позитивну сторону направлення q на величину q0. $\psi(q,0)=(\frac{\nu}{\pi\hbar})^{1/4}\exp\left[-\frac{\nu}{2\hbar}(q-q_0)^2\right]$. Хвильова еволюція цього пакета заключається в тому, що в наступні моменти часу щільність ймовірності задається виразом[4] $|\psi(q,t)|^2=(\frac{\nu}{\pi\hbar})^{1/2}\exp\left[-\frac{\nu}{\hbar}(q-q_0\cos\nu t)^2\right]$.

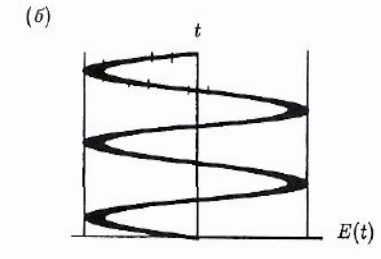

Рисунок 2.2.6.1 Хвильовий пакет з мінімальною невизначеністю в різні моменти часу в потенціальному полі гарнонічного осцилятора (а);відповідне електриче поле (б).

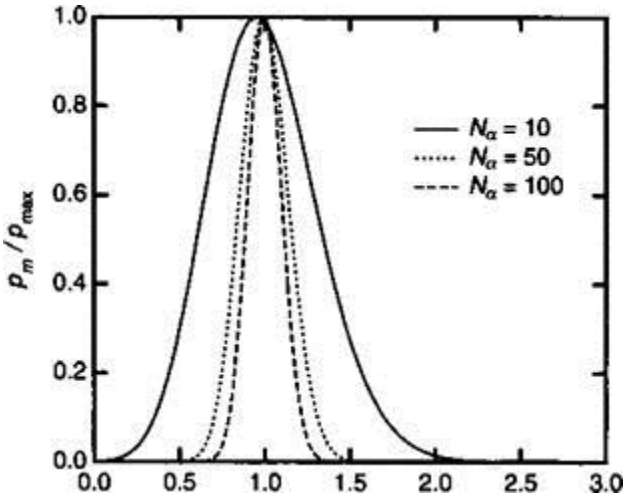

Рисунок 2.2.6.2. Розподілення фотонів

p(n) - в когерентному стані, $p(n) = \langle n|\alpha\rangle\langle\alpha|n\rangle = \frac{|\alpha|^2 n e^{-\langle n\rangle}}{n!} = \frac{\langle n\rangle^n e^{-\langle n\rangle}}{n!}$.

Гамильтоніан осцилятора при наявності квадратичного потенціалу

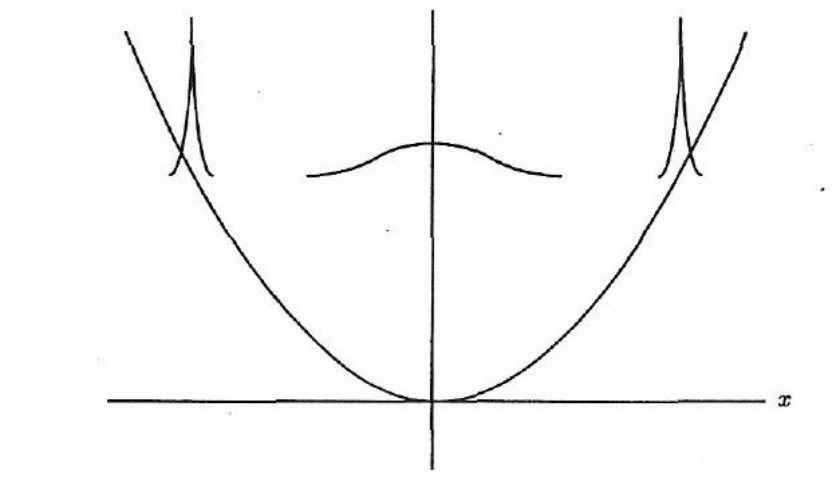

Рисунок 2.2.6.3. Еволюція стиснутого стану простого гармонічного осцилятора

Згідно з принципом невизначеності Гейзенберга зведення невизначеностей в визначенні середніх значень двох змінних A і B задається виразом $E(t) =$E$\hat{\varepsilon}(\alpha e^{-ivt} + \alpha^+ e^{ivt})$.

Кооперативний ефект – явище в багато частинній системі, зв’язане з когерентною взаємодією великої кількості частинок. Існують ефекти і явища, які залежать від стану і взаємодії групи атомів, при цьому групова і колективна поведінка атомної системи може бути відносно простою. Тоді досліджувати явище можливо шляхом сумування вкладів від індивідуальних атомів в загальне поле і гадати, що атоми діють майже незалежно один від одного. В інших випадках важливо враховувати вплив кожного атома на інші, оскільки це суттєво змінює поведінку кожного з них. Саме такі ефекти називають кооперативними.

Надтекучість і надпроводимість – це приклади кооперативних явищ, під час яких квантова когерентність проявляється в макроскопічних масштабах, а саме при участі електронно-фотонної взаємодії. Існують нерівноважні кооперативні явища, які виникають у відкритих системах, і їх існування

зв’язано з дисипацією енергії. Випромінювання лазера – приклад нерівномірного кооперативного явища, коли при достатньо високому ступені нерівномірності (потужність накачки) безструктурний стан системи стає нестійким до малих флуктуацій, шо супроводжується генерацією випромінювання.

2.3 Квантова інформатика

Квантова інформатика – наука нових ресурсів, які тільки відкриваються за допомогою квантових об’єктів для вирішення задач, в свою чергу відносяться до області «інформатика» - комунікації, захист, розрахунок. В свою чергу квантова інформатика ділиться на декілька підрозділів: квантова комунікація, квантова криптографія, квантові розрахунки.

В квантовій інформатиці є сенс замінити класичні об’єкти на квантові, але при цьому доведеться зіштовхнутись з рядом проблем. Наприклад, в класичному випадку не виникає ускладнень з нумерацією об’єктів для вибору: червона куля – з номером 1, оранжева -2, жовта -3 і так далі. Якшо припустити, що так само вчинимо з квантовими об’єктами в двохвимірному гільбертовому просторі, використовуючи, наприклад таблицю нумерації цих об’єктів:

Таблиця 2.2.7.1 Номерація об’єктів

Номер об’єкта (i)	1	2	3	4
Стан $\|\psi_i\rangle$	$\|0\rangle$	$\|+\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\|1\rangle$	$\|-\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$

Аліса створює ці об’єкти зі свого боку і передає їх Бобу. Боб отримує ці квантові об’єкти і намагається прочитати їх номер за допомогою вимірів. Саме на цьому етапі виникає проблема. Вибираючи в якості виміру будь-який з типів вимірів, він розуміє що не може розрізнити всі неортогональні стани. Так

вибираючи проекційний тип виміру,$P_{|0\rangle} = |0\rangle\langle 0|$, $P_{|1\rangle} = |1\rangle\langle 1|$, Боб буде отримувати наступні результати з ймовірністю[3]:

Таблиця 2.2.7.2 Номерація об’єктів

Номер об’єкта (i)	1	2		3	4	
Результат вимірювання $P_{\|k\rangle}$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
Ймовірність $\langle\psi_i\| P_{\|k\rangle}\|\psi_i\rangle$	1	1/2	1/2	1	1/2	1/2

Тобто достовірність відправлених станів буду лише для першого і третього об’єкта. Вибір проекційних операторів виміру в вигляді $P_{|+\rangle} = |+\rangle\langle +|$, $P_{|-\rangle} = |-\rangle\langle -|$ дозволить відрізнити другий і четвертий об’єкти, в той час як перший і третій буде неможливо відрізнити. Цим прикладом показано, що незважаючи на нескінченне число станів дворівневої системи, допустимих для розпізванання станів тільки два.

Квантова система з двома рівнями може переносити 1 біт інформації. Називається така система кубіт (квантовий біт). Зазвичай «дворівневими» називають квантові системи з двома рівнями енергії. В даному випадку система характеризується двома станами

Неможливість розрізнити неортогональні стани квантових систем показує, що квантові стани містять в собі засекречену інформацію, яку неможливо проявити під час виміру, з цього випливає, що вона може бути використана для криптографії і обчислень.

Неможливість розрізнити неортогональні стани призводить до принципового висновку. Якшо Боб отримав неортогональні повідомлення і міг розрізнити їх, то він би отримав можливість зробити безліч копій цих неортогональних станів. Неможливість зробити копію невідомого квантового

стану має назву теореми неможливості клонування невідомого квантового стану [3]. Загалом цю теорему виводять як наслідок лінійності квантової механіки.

Відсутність можливості клонування невідомих станів і еквівалентна неможливість ідеального розрізнення неортогональних станів не завжди негативні і їх можна використовувати.

З теореми неможливості клонування можна отримати оцінку для величини доступної квантової інформації в комунікаційній схемі[3]. Наприклад, нехай Аліса відправляє Бобу послідовність квантових систем в неортогональних станах з ймовірністю ρ та $1-\rho$. Якщо Боб, отримуючи неортогональні стани, може їх клонувати, то створюючи багаточасткові стани, він міг би їх розрізняти з більшою точністю, внаслідок того, що багаточасткові стани стають майже ортогональними. Відповідно, в цьому випадку він отримав можливість розрізняти неортогональні стани у відправленій послідовності. Величина доступної інформації дорівнювала б класичній. Хоча для довільних схем загальний спосіб підрахунку доступної квантової інформації невідомий, існує ряд граничних оцінок для такої величини. Однією з важливих є квантова ентропійна границя.

2.3.1 Переплутані квантові стани

Використання світлових сигналів викликає інтерес при вирішенні проблеми передачі квантової інформації. Визначення типу світлових полів володіє рядом властивостей, які безпосередньо використовуються в квантових комунікаційних протоколах, таких як квантова телепортація та квантове розподілення ключа. Ці поля розглядаються як квантові системи, спроба їх виміру призводить до збудження стану. Взагалі під некласичним розуміється світло, властивості якого неможливо описати класичним чином і виділити його відмінні сторони. Всі ці проблеми разом складають предмет квантової оптики.

З точки зору експеримента, властивості світлових полів можливо дослідити, аналізуючи властивості фотоку, які їм породжуються. При цьому аналогічно аналізувати їх середній потік і його флукрутацію. Відомо, що середній потік пропорційний інтенсивності світла, падаючого на фотодетектор. Флуктуацію фотоку можливо пояснити випадковістю породження фотоелектронів в процесі детектування, тому доволі довгий час їм не придавали особливого значення. Такі флуктуації називають пуасснонівськими або дробовим шумом. Існує співвідношення і критерії, які встановлюють зв'язок між характеристиками, які ми спостерігаємо, фоток і статистичні властивості світла.

Переплутування – це поняття, яке відноситься до двох чи більше адресуємих систем. Формально в квантовій механіці дві системи А і В можна розглядати як одну складову систему АВ з гільбертовим простором, що представляє собою пряме відтворення гільбертових просторових систем А і В. В загальному просторі відтворення вектора для системи А і вектор для системи В. такий вектор називається переплутаним станом систем А і В.

Переплутані стани створюються в результаті взаємодії двох систем А і В, але розглядаються і використовуються вже після закінчення взаємодії. Протягом 30 років переплутані стани успішно створюються в лабораторіях по всьому світу. Об’єктами для створення переплутаних станів служать різні частинки з різними степенями свободи, використовувані для кодування станів: фотони в поляризаційних, фазових, просторонних і інших станах, електронні і ядерні спіни в різних структурах і матеріалах, квантові стани надпровідних комірках та інші системи.

Найбільш широко використовуваним видом переплутування є поляризаційне переплутування – створення поляризаційного стану двох фотонів, які породжуються в нелінійному кристалі під дією оптичної накачки в процесі спонтанного параметричного розпаду. Фотони породжуються в синглетному стані $|\psi\rangle$, де $|0\rangle$ відповідає горизонтальній поляризації, а $|1\rangle$ – вертикальній[5].

Переплутані стани є необхідним квантовим ресурсом для реалізації протоколів квантової телепортації, надщільного квантового кодування, а також деяких протоколів квантової криптографії, наприклад, протокол Екерта. Переплутані стани лежать в основі квантових підрахунків і комп'ютерів. Є невід'ємною частиною у вивченні квантової теорії, через те, що вони призводять до ефектів, які не можна пояснити з точки зору локального реалізму в теорії ймовірності.

2.3.2 Основи криптографії

Квантова криптографія – розділ квантової інформатики, що вивчає методи захисту інформації шляхом використання квантових носіїв (фотонів). Можливість реалізації такого захисту реалізується теоремою про неможливість клонування невідомого стану квантового об'єкта [6].

Історично під криптографією розумілось мистецтво тайнопису, тобто перетворення осмисленого тексту в незрозумілий шифр з метою його захисту. Шифрування тексту може використовуватись для зберігання інформації, так і для секретної відправки кінцевому користувачу, який в свою чергу володіє алгоритмом дешифровки. Роблячи висновок, традиційна криптографія забезпечувала конфіденційність інформації навіть за умови доступу до неї сторонніх осіб. В 20 столітті криптографія перетворилась в окрему наукову дисципліну зі своїми науковими журналами, книгами та міжнародними конференціями [3]. В нащ час інформаційне суспільство в значній мірі зв'язано з цифровою технікою, а разом з цим поняття криптографія розширилось і зв'язується з комплексними методами захисту інформації, які, окрім конфіденційності, забезпечують її цілісність і проведення процедури аутентифікації. Цілісність – це неможливість її непомітно змінити або підмінити, аутентифікація – складається з встановлення особистості сторін, які вступають в обмін інформацією. Таким чином, захист інформації полягає в охороні законних користувачів, які обмінюються інформацією, від дій

зловмисника, який намагається прочитати інформацію або змінити її. В поняття захисту вкладено також захист законних користувачів один від одного, що є важливим в елетронній торгівлі.

Звісно, не кожний захист інформації має відношення до криптографії. Для забезпечення конфіденційності документи зберігають в сейфах, цілісність забезпечується підписами та печатками, а аутентифікація – за допомогою особистих даних. Криптографія відрізняється від інших способів специфічними методами. На початку 90-х років криптографію асоціювали з наукою, яка вивчала математичні методи захисту інформації. Після появи квантової криптографії це поняття стало «малим».

Під час використання простого методу шифрування – безпека буде втрачена, якшо зловмиснику стане відомий алгоритм шифрування. Історія показує, що при забезпеченні зв'язку між великими організаціями в секреті алгоритм шифрування тримати неможливо і періодично міняти – нерентабельно. Через це науковці прибігають до іншого прийому. У функції шифрування і дешифрування вводиться додаткова змінна – криптографічний ключ $C = f_e(T)$, $T = g_d(C)$, де e – ключ шифрування, а d - ключ дешифрування[3]. Алгоритми шифрування повинні задовольняти рівність $g_d(f_e(x)) = x$ для будь-якого x з безлічі значень початкового тексту для того, щоб дешифрований текст співпадав з початковим. Таким чином для забезпечення безпеки необхідно зберігати в секреті і періодично змінювати тільки декілька ключів, а самі алгоритми можна оприлюднювати. Інколи алгоритми спеціально публікують для знаходження критичних для безпеки недоліків.

2.4 Висновок з розділу 2

Квантова криптографія зарекомендувала себе як надійна система, яка не піддається поки що відомим методам дешифрування сторонніми особами. Може використовуватись в банківській та воєнній сфері. Завдяки відмінності

квантової теорії від класичної фізики стає можливо забезпечити повну безпеку передачі інформації по лінії зв’язку.

Сторонні особи, які будуть намагатись прослухати інформацію, можуть витягнути частину інформації, яка передається, але це не дасть ніякого результату, тому що сторонній користувач обов’язково змінить стан передаваємих частинок.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ КВАНТОВИХ КРИПТОГРАФІЧНИХ СИСТЕМ

3.1. Квантовий розподіл ключів

У 1949 р. С. Шеннон, спираючись на розроблену ним теорію інформації, довів теорему, що криптосистема є абсолютно секретною, якщо секретний код істинно випадковий та використовується лише один раз. Однак на практиці реалізація такої системи наштовхується на серйозні труднощі, одна з них – створення та передача великого секретного коду, необхідного кожного разу, коли надсилається нове повідомлення.

Вирішити цю проблему можна було б за наявності фізичного каналу, секретність якого забезпечується фізичними законами. Саме такий канал представляє квантова фізика. Практичні можливості, які відкриває теорема про неклонованість квантового стану, призвели до розробки ряду суттєвих квантових криптографічних примітивів. Ми розглянемо найбільш важливий з них – квантовий розподіл ключів (КРК).

КРК вирішує основну проблему симетричного шифрування – генерацію двох ідентичних реплік ключа для двох віддалених користувачів таким способом, що третя репліка ключа не може існувати в природі. Для передачі секретного повідомлення на практиці завжди застосовується комбінація КРК, симетричного шифрування та інших примітивів класичної криптографії [16]. Переваги КРК перед асиметричними технологіями розподілу ключів полягають в його безумовній захищеності, тобто за відсутності припущення про обчислювальні ресурси зловмисника.

Крім того, безпека асиметричного шифрування має серйозну загрозу з боку квантових комп’ютерів, які з використанням алгоритму Шора можуть зламати такий шифр. Теорія захищеного розподілу ключа з використанням квантових каналів зв’язку стрімко розвивалась протягом короткого часу. Ідея використання неклонованості та неможливості точного вимірювання

невідомого одиночного квантового стану для створення секретних повідомлень була висловлена в роботі Візнера у 1983 р. [17].

Конкретні протоколи криптографії такого виду були розроблені незалежно Беннетом та Брассаром [18] (BB84, B92) та Екертом [19]. Цих робіт виявилось достатньо для стимулювання серйозної експериментальної роботи, яка триває по сьогодні. 58 Справжня революція в області доведення захищеності КРК була розпочата Майєрсом наприкінці 90-х рр. [20], який довів, що протокол BB84 є абсолютно захищеним для достатньо низького детектованого рівня помилок у квантовому каналі.

Наразі діяльність в області доведення захищеності протоколів розподілу ключа не можна вважати завершеною. Досі існують важливі фундаментальні та практичні питання, пов’язані з неідеальними джерелами. Існує маса технічних питань (наприклад, використання слабких когерентних джерел), які заслуговують на теоретичний розгляд.

3.1.1 Захист за допомогою неортоганальних станів

Ідея використовувати неортогнальні квантові стани для кодування секретної інформації належить Стефану Візнеру, яких запропонував “Квантові гроші“, які неможливо підробити шляхом копіювання. Це так, бо неможливо копіювати неортоганальні квантові стани (чи любий невідомий квантовий стан). Щоб це побачити, розглянемо два нормованих стани |0) та |1), таких, що (0|1)^0. Припустимо, що існує клонуюча машина, яка діє в такий спосіб:

$$|0\rangle|\text{бланк}\rangle|\text{машина}\rangle \rightarrow |0\rangle|0\rangle|\text{машина}_0\rangle$$
$$|1\rangle|\text{бланк}\rangle|\text{машина}\rangle \rightarrow |1\rangle|1\rangle|\text{машина}_1\rangle,$$

де «бланк» позначає початковий стан частинки, яке після дії машини стає клоном, і де їхні стани відповідним чином нормовані. Операція клонування

повинна бути унітарною та застосовувати правила внутрішнього добутку, так що ми вимагаємо:

$$\langle 0|1\rangle = \langle 0|1\rangle\langle 0|1\rangle\langle \text{машина}_0|\text{машина}_1\rangle,$$

що можливо тільки при (0 | 1) = 0 (два стани взаємно ортогональні) або при $\langle 0|1\rangle$ = 1 (два стани невиразні і, отже, не можуть бути використані для кодування двох різних станів біта), що суперечить нашому вихідному припущенню. Таким чином, якщо хтось таємно готує випадкову послідовність станів типу |1⟩| 0⟩ | 1⟩| 1⟩..., де | 0⟩і | 1⟩ обрані випадково, то цю послідовність неможливо достовірно відтворити. Гроші Візнера з такими неклоніючими квантовими підписами зажадали б зберігання неортогональних квантових станів на банкнотах, що набагато важче, ніж пересилання неортогональних квантових станів із одного місця в інше. Ось чому ідея Візнера була адаптована до розподілу ключа. Чарльз Беннетт і Жиль Брассар запропонували використовувати неортогональні стани фотонів, щоб розподіляти криптографічні ключі. У будь-якого, хто підслуховує і намагається розрізнити неортогональні стани | 0) і [1), з'являється проблема. Припустимо, що Єва готує свій вимірювальний прилад в вихідному станів |m) і хоче відзначити |0) від |1), вона хоче виконати наступну унітарну операцію

$$|0\rangle|\mathrm{m}\rangle \rightarrow |0\rangle|\mathrm{m}_0\rangle$$
$$|1\rangle|\mathrm{m}\rangle \rightarrow |1\rangle|\mathrm{m}_1\rangle \ .$$

Умова унітарності означає, що (0 | 1) (m | m) = (m0 | m1) (m0 | m1), тобто, (m0 | m1) = 1, кінцевий стан вимірює приладу одне і теж в обох випадках. Два стани не обурені, але Єва не отримала ніякої інформації про закодованому значень біта. Більш про- ний вимір (але все ще не самого загального виду), що обурює вихідні стану, так що |0)->|0') і |1)->|1'),має вигляд

$$|0\rangle|\mathrm{m}\rangle \rightarrow |0'\rangle|\mathrm{m}_0\rangle$$
$$|1\rangle|\mathrm{m}\rangle \rightarrow |1'\rangle|\mathrm{m}_1\rangle \ .$$

Умова унітарності дає (0 | 1) = (0 '| 1') (m0 | m1). Мінімум (m0 | m1), який відповідає ситуації, коли у Єви з'являється найкращий шанс розрізнити два стану свого приладу, виходить при (0 '| 1') = 1, тобто, коли два стану | 0) і | 1) після взаємодії стають невиразними. Хоча тільки що описане вимір і не має найбільш загального вигляду, воно являє собою гарну ілюстрацію суперечливою зв'язку між інформацією, отриманою при вимірюванні, і обуренням вихідних станів. Протокол розподілу ключа, який використовує її, буде в деталях описаний пізніше.

3.1.2. Захист за допомогою заплутування.

Концептуальноє підставу для квантової криптографії, заснованої на переплутуванні, володіє зовсім інший природою, і включає в себе парадокс Зйнштейна-Подільського-Розена. У 1935 році Ейнштейн, разом з Борисом Подільським і Натаном Розеном (ЕПР), опуб- тріумфували статтю, в якій вони зробили начерк того, як повинна виглядати «правильна» фундаментальна теорія природи. Програма ЕПР включала в себе повноту («в повній теорії присутній злементов, відповідний кожному злементов реальності»), локальність («реальна фактична ситуація в системі А не залежить від того, що відбувається з системою В, просторово відокремленою від першої»), і визначала елемент фізичної реальності так: «якщо, не бунтували систему, ми можемо з упевненістю передбачити значення фізичної величини, то існує злементов фізичної реальності, відповідний зтой фізичної величиною». Потім ЕПР розглянули уявний експеримент на двох переплутаних частинках, который показав, що квантові стану не можуть у будь-яких ситуаціях бити повним описом фізичної реальності. Аргумент ЕПР, згодом видозміни Дзвідом Бомом, формується таким чином. Уявімо собі синглетное по спину стан двох частин зі спіном ½

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2)$$

де кет-вектори одиночних частинок | стрілка вгору) і [стрілка вниз) позначає спин вгору і спін вниз по відношенню до деякого внбранному напрямку. Цей стан сферично симетрично, і вибір напрямку не має значення. Дві частици, які ми позначимо A і B, випускаються одним джерелом і розлітаються в різні боки. Після того, як вони розлетяться досить далеко, так що вони вже не будуть один з одним взаємодіяти, ми можемо достовірно передбачити значення x-компоненти спина частинки A шляхом вимірювання x-компоненти спина частинки B. Дійсно, сумарний спин двох частинок дорівнює нулю, і компоненти спина двох частинок повинні володіти протилежними значеннями. Вимірювання, виконане на частці B не обурює частку A (з огляду на локальності), отже, x-компонента спина є елемент реальності згідно з критерієм ЕПР. Точно так же, завдяки сферичної симетрії, y, z і будь-які інші компоненти спина також є злементов реальності. Однак, оскільки не існує квантового стану частки зі спіном 1/2, в якому всі компоненти спина мали б певні значення, то квантове опис реальності неповно.

Програма ЕПР вимагала іншого опису квантової реальності, однак, аж до встановлення теореми Джона Белла (1964) не було ясно, чи можливо таке опис, і, якщо так, то чи призведе воно до інших прогнозам результатів зкспериментов. Белл показав, що припущення ЕПР про локальність, реальності і пів ноті несумісний з деякими прогнозами квантової механіки, що стосуються переплутаних частинок. Протиріччя виявляється шляхом виведення з програми ЕПР зкспериментально перевіряється нерівності, яке порушується в деяких прогнозах квантової механіки. Розширення оригінальної теореми Белла Джоном Клаузер і Майклом Хорном (1974) зробило можливими зкспериментальние тести програми ЕПР, і деякі з них були виконані. Експерименти підтвердили передбачення квантової механіки.

Яке зто все має відношення до захисту даних? Як не дивно, велика! Виявляється, що той самий трюк, який був використаний Беллом для перевірки

підстав квантової теорії, може захистити передачу даних від підслуховування! Можливо, зто буде звучати не так дивно, якщо ще раз згадати визначення злементов реальності згідно ЕПР: «якщо, не бунтували систему, ми можемо з упевненістю передбачити значення фізичної величини, то існує злементов фізичної реальності, відповідний зтой фізичної величиною». Якщо зта конкретна фізична реальність використовується для кодування двійкових значень криптографічного ключа, то все, чого хоче Подслушивающий агент - це злементов фізичної реальності, відповідний кодує змінної. Таким чином, квантова криптографія на основі змішування практично використовує квантове перепутіваніе і теорему Белла, показуючи, що межа між возвишення і приземленим дослідженням досить розмита.

3.1.3. Властивості зашумелних квантових каналів

Безвідносно до типу квантової зв'язку, висновок такий: досконалий квантовий канал (тобто квантовий канал без шуму) захищений. Будь-яке обурення в каналі є знак того, що хтось намагався туди проникнути. Таким чином, зашумлення сеанси зв'язку треба відкидати. На жаль, квантові канали зв'язку дуже тендітні, і на практиці неможливо уникнути деякої кількості цілком невинного шуму через взаємодію з оточенням. Поэтому, замість того, щоб отбрасівать будь-яку зашумленную передачу, «законні» користувачі повинні знайти процедуру для отримання секретного ключа, навіть в присутності деякої кількості шуму. Для початку, необхідно оцінити, скільки інформації могло витекти до підслуховувати одержувачу, як функцію параметрів, які вони можуть виміряти. Це кількість інформації може бути прийнятним, допустимим, або неприпустимим. Під допустимим ми маємо на увазі, що за допомогою деяких послідовних процедур, таких, як посилення секретності або квантове підсилення секретності, його можна зменшити до будь-якого бажаного прийнятного рівня, за рахунок більш короткого ключа. Існує, однак, поріг, і якщо занадто багато інформації витекло до одержувача, то

ніяке подальше посилення секретності неможливо, і сеанс зв'язку слід відкинути. Необхідність в більш точній критерії була вперше висунута Хаттнером і Екертом, з тих пір квантове підслуховування розвинулося в самостійну наукову область.

Якщо квантова передача по зашумленими каналах заснована на розподілі переплутаних частинок, то посилення квантової секретності визначає критерії захисту, з урахуванням самої загальної атаки, яку може провести Подслушивающий агент. Посилення квантової секретності перетворює частково переплутані частки (через підслуховування або будь-якого зовнішнього збурення) в повністю переплутані, і відомо, коли таке очищення квантового змішування можливо. Однак, з точки зору практики, технологія, необхідна для вьполненія квантового очищення, аналогічна тій, що вимагається для квантового комп'ютера, і, отже, поки недосяжна.

Література про зашите інформації секретності при передачі одиночних частинок досить обширна. На початку, обговорювалася тільки захист від так званих «некогерентних атак», при яких одержувач має справу з кожною частинкою окремо. Але квантова механіка допускає більш загальний і більш потужний тип атак, відомий як «когерентні атаки», при яких одержувачу дозволяється використовувати квантовий комп'ютер. Нещодавно були запропоновані засоби захисту від таких атак. Однак, чим більш потужними є розглянуті атак, тим жорсткішими мають бути умови захисту. Теж саме відноситься до оптимізації всього протоколу, яка критично важлива для практичних застосувань.

3.2. Протоколи квантового розподілення ключа

3.2.1. Протокол BB84

BB84 протокол, розроблений Чарльзом Беннетом и Жильем Брассаром, був запропонований в 1984 році і є першим протоколом квантового

розподілення ключа [7]. Протокол заснований на принципах квантової механіки, що робить його абсолютно безпечним при відсутності шуму в квантовому каналі зв’язку, і використовуючи частинки, що передаються і не допускають їх клонування. Виконання цих умов називається ідеальними умовами для квантоного розподілення ключа

Відсутність шуму дає змогу визначити, що квантові стани частинок не змінюються при розповсюдженні по квантових каналах зв’язку. Згадуючи класичну теорію інформації, початково вважається, що повідомлення завжди можна перехопити і прослухати, а також скопіювати його без зміни його змісту. Але якщо інформація зашифрована в неортогональних квантових станах, то стани фотонів з поляризацією 0°, 45°, 90°, 135°, то зловмиснику прочитати або скопіювати її повністю принципіально неможливо. Зловмисник не зможе отримати з повідомлення навіть частину інформації, не змінивши її випадковим чином, який з великою вірогідністю буде помічено легітимним користувачем каналу зв’язку.

Спочатку протокол BB84 був сформований для одиночних фотонів, хоча його можно перевести на інші реалізації кубітів. Для кодування інформації в протоколі використовується чотири стани поляризації, які створюють два базові неортогональні один для одного базиси ↔ і ↕, а також діагональний $|\nearrow\rangle = (|\leftrightarrow\rangle + |\updownarrow\rangle)/\sqrt{2}$, $|\nwarrow\rangle = (|\leftrightarrow\rangle - |\updownarrow\rangle)/\sqrt{2}$.

Суть полягає в тому, що один з користувачів, для прикладу, Аліса вибирає випадковим чином послідовність бітів і послідовність базисів, після цього посилає іншому користувачеві – Бобу – послідовність фотонів, кожен з яких кодує один біт з вибраної послідовності в базисі, відповідаючий порядковому номеру цього біта, стани ↔ і ↗ кодують 0, а ↕ і ↖ в 1.

Під час отримання фотонів Боб випадковим чином для кожного фотона незалежно від Аліси вибирає базис для виміру і аналогічним чином для кожного фотону інтерпретує результат своїх вимірів як двійковий 0 або 1. Згідно до законів квантової механіки, після виміру діагонального фотона в

прямокутному базисі його поляризація перетворюється в горизонтальну або вертикальну, зважаючи на результати виміру або навпаки, при цьому результат виміру буде випадковим. Таким чином Боб отримає результати, які співвпадають із станом відправлених фотонів в половині випадків, тобто коли він правильно вгадав базис.

Наступним кроком протоколу виконується за допомогою відкритого каналу зв'язку, Аліса і Боб можуть відкрито повідомляти один одному класичну інформацію. Припустимо, що класична інформація не змінюється при розповсюдженні по відкритому каналу. Це означає, що можливе пасивне підслуховування, тобто зловмисник може читати повідомлення двох сторін, але не може змінювати і відправляти повідомлення за них.

Таблиця 3.2.1.1 Реалізація протоколу BB84 за відсутності шуму

1. Случайные биты (Алиса)	0	1	1	0	1	1	0	0
2. Случайные базисы (Алиса)	⊗	⊗	⊗	⊕	⊕	⊗	⊗	⊕
3. Поляризация фотонов, передаваемых по *квантовому каналу*	↗	↘	↘	↔	↕	↘	↗	↔
4. Случайные базисы приема (Боб)	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕
5. Полученные Бобом биты	0	0	1	1	1	0	0	0
6. Боб сообщает Алисе базисы измерений (*классич. канал*)	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊕
7. Алиса сообщает, какие из них верны (*классич. канал*)			✓		✓			✓
8. Полученные общие биты (просеянный ключ)			1		1			0
9. Боб открывает часть битов					1			
10. Алиса подтверждает их					✓			
11. Полученный в итоге ключ (просеянный ключ после оценки ошибки, вызванной возможным подслушиванием)			1					0

В першу чергу Аліса і Боб визначають шляхом відкритого обміну повідомленнями, які фотони були успішно отримані, які з них були змінені Бобом в правильному базисі. Потім Аліса і Боб будуть мати однакові значення бітів, зашифрованих в цих фотонах, не дивлячись на те, що ця інформація ніколи не обговорювалась по відкритому каналу. Кожен з фотонів несе один біт випадкової інформації, яка відома Алісі та Бобу і більше нікому. Інформація про фотони у виміряних в неправильному базисі відкидаються, в результаті чого Аліса і Боб отримують просіяний ключ, який при відсутності прослуховування повинен бути однаковим в обох сторін.

Не пропускаючи факт того, що також можливе прослуховування, зловмисником буде виступати Ева, розглянемо приклад. Через випадковий вибір прямокутного або діагонального базиса вимірювання фотонів при обміні квантовими повідомленнями Ева змінює повідомлення таким чином, що Аліса і Боб знаходять зміни в бітах просіяного ключа, які за умови відсутності прослуховування повинні співпадати. Жоден вимір переданого фотона Евою, яка дізнається про початковий базис в фотоні лише після того, як зробить його вимір, не може дати більше ½ інформації про біт, кодуємий цим фотоном, будь-які зміни даючі b біт інформації, повинно давати неузгодженість з ймовірністю b/2, якщо виміряний фотон або його заміна в подальшому буде виміряна Бобом в початковому базисі. Такий спосіб підслуховування, коли Ева вимірює і передає далі всі перехвалені фотони в прямокутному базисі, дізнаючись в такому випадку правильну поляризацію половини фотонів і вносячи зміни в четверту частину фотонів, які будуть потім виміряні в початковому базисі.

Виходячи з вище сказаного, Аліса і Боб можуть перевірити наявності факту підслуховування, відкрито порівнюючи частину бітів, про які у них повинна бути однакова інформація, хоча це зробить біти непридатними для використання в секретному ключі.

Положення бітів під час цього порівняння повинні бути випадковою множиною правильно виміряних бітів так, щоб підслуховування більш ніж декількох бітів не могло уникнути виявлення Еви. Якшо всі біти порівнювальні

біти співпадають, Аліса і Боб роблять висновок, що підслуховування немає, і біти, які залишились, можна безпечно передавати в якості секретного ключа для наступного шифрування даних і передачі по відкритому каналу.

Коли ключ вже використаний, Аліса і Боб знову повторюють всю процедуру і отримують наступний секретний ключ.

3.2.2. Протокол B92

Протокол B92 був запропонований в 1992[8] році Чарльзом Беннетом, звідси і назва протоколу. Протокол був заснований на принципах невизначеності на відміну під протоколу E91. Носіями інформації дворівневої системи – кубіти. Особливість протоколу – використання двох неортогональних квантових станів.

Для генерації криптографічного ключа по протоколу B92 використовується та ж сама схема, що і для протоколу BB84, але замість чотирьох станів використовують тільки два неортогональні стани.

При зміні квантого біта на стороні Боба проводитmся випадковий вибір одного з двох базисів. Якщо при виборі прямолінійного базиса $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ результатом виміру виявилось $|\leftrightarrow\rangle$, Боб знає, що відправлявся стан $|\nearrow\rangle$ і записує його в свою послідовність 1. Аналогічно, якщо при виборі косокутного базиса $\{|\nearrow\rangle, |\nwarrow\rangle\}$ результатом виміру виявилось $|\nwarrow\rangle$, відправлявся стан $|\updownarrow\rangle$ і записує його як 0. Всі інші результати вважають нерезультативними і не враховують. В протоколі відсутня процедура погодження базисів, замість неї Боб повідомляє Алісі по відкритому каналу номер результативних вимірів, в подальшому по результатах генерується просіяний ключ. Ева, знаючи номер результативних вимірів, не в стані правильно визначити значення переданого біта через стан його кодування – неортогональний, тобто неможливо відрізнити.

На жаль, протокол B92 не зміг стати конкурентом для протоколу BB84 через свої недоліки. Існує ряд труднощів в реалізації протоколу:

1) Недосконалі джерела одиночних фотонів, а саме швидкість генерації;

2) Недосконалість детекторів одиночних фотонів – спрацювання датчика не тільки на фотони, але і на інші частинки;

3) Сучасні волоконно-оптичні лінії не гарантують досягання фотоном кінцевої точки;

4) Ціна встановлення такої системи приблизно оцінюється в сотні євро, але повсякденне використання такої системи не передбачається.

Незважаючи на недоліки перед іншими протоколами, протоколом B92 зручніше користуватись через простоту його реалізації. У зв'язку з цим були проведені експерименти по його реалізації. Вчені з Бразилії в своїй статті описали установку, за допомогою якої реалізували протокол. У висновку вони звернули увагу на проблеми, які виникли в процесі установки, і описали методи їх усунення. Так само група вчених з Китаю зібрали установку довжиною 2.2 метра і поставили експеримент по передачі інформації за допомогою протоколу B92 і відмітили, що для передачі фотона на великі відстані потрібно замінити протокол.

3.2.3. Протокол Екерта

Квантовий криптографічний протокол заснований на експерименті Енштейна-Подольского-Розена і узагальнений в теоремі Белла. Був запропонований польським фізиком Артуром Екертом в 1991 році[9]. Протокол заснований на властивостях заплутаних станів квантових частинок. Для цього Екерт використовував пару частинок – ЕПР пару.

В протоколі пропонується використовувати пару фотонів породжених в асиметричних поляризаційних станах. Перехоплення одного з пари фотонів не приносить Еві ніякого результату, але для Аліси і Боба є сигналом того, що канал прослуховується.

Ефект ЕПР виникає, коли сферично симетричний атом випромінює два фотона в протилежних направленнях в сторону спостерігачів. Фотони випромінюються з невизначеною поляризацією, але в силу симетрії їх поляризації завжи протилежні. Важливим фактором цього ефекту є те, що поляризація фотонів стає відомою тільки після вимірювання. На основі ЕПР Екерт запропонував протокол, який гарантує безпеку відправлення і зберігання ключа. Відправник генерує деяку кількість ЕПР фотонних пар. Один фотон з кожної пари він залишає собі, другий – відправляє. При цьому якщо ефективність реєстрації близька до одиниці, при отриманні відправником значення поляризації 1, його співбесідник зареєструє значення 0 або навпаки. Таким чином, співрозмовники кожного разу, коли потрібно, можуть отримати однакові псевдовипадкові кодові послідовності.

3.2.4. Шум і перехват інформації в каналі

В реальній ситуації в квантовому каналі зв’язку завжди є наявність шуму. Під шумом розуміють викривлення класичної інформації, закодованої в квантовому носії під час розповсюдження по квантовому каналі. Джерела шуму можуть мати різну фізичну природу. Наявність шуму в каналі призводить до того, що після виконання протоколу квантового розподілення ключів (КРК) випадкові послідовності, отримані Алісою та Бобом, будуть різнитись між собою [3]. Зрозуміло, що за наявності такого шуму, Ева може цим скористатись. Наприклад, Ева може замінити частину квантового каналу на менш шумний і провести свої виміри так, щоб загальний рівень шуму, контрольований Алісою і Бобом, не буде перевищено. В такому випадку Аліса і Боб не будуть знати, що їх прослуховують. Щоб забезпечити якомога мешний вплив шуму потрібно зробити аналіз:

1) Оцінка рівня шуму в просіяних ключах Аліси і Боба;

2) Способи, які може використати Ева для перехоплення повідомлення;

3) Теоретична оцінка величини інформації, якою буде володіти Ева в результаті перехоплення;

4) Процедури, що дозволяють оброблювати ключі Аліси і Боба таким чином, щоб вони не містили інформації, яку Ева перехопила – вторинна обробка ключа (корекція помилок).

Після етапу просіювання сирих ключів в схемі КРК, Аліса і Боб мають дві двійкові послідовності – просіяні ключі, які не співпадають в деяких позиціях через шум. Важливо визначити рівень шуму в отриманих просіяних ключах.

Позначимо довжину просіяного ключа N_s, а відношення неспівпадаючих бітів в просіяних ключах до довжини цього ключа Q. Цю величину Аліса і Боб можуть оцінити, виконуючи протокол визначення рівня шуму:

1) Аліса випадково вибирає послідовність номерів, менших N_s;

2) Аліса відправляє Бобу по класичному каналу цю послідовність разом зі значеннями бітів, маючих відповідні номери;

3) Боб порівнює значення бітів Аліси зі значеннями своїх бітів, маючих ті ж номери, вираховуючи кількість бітів, які не співпадають;

4) Аліса і Боб виключають скомпрометовані біти з послідовностей, отримуючи просіяні послідовності.

На стадії лабораторного тестування лінії КРК встановлюється робоче Q_0 і максимальне $Q_m > Q_0$ значення рівня шуму в квантовому каналі, відповідні довжині лінії КРК. Насправді лінії КРК на одиночних фотонах Q_0 і Q_m складають декілька відсотків при довжині лінії до 50 кілометрів. Перевищення шумом каналу максимального рівня Q_m розцінюється як перехоплення. В цьому випадку користувачі лінії КРК відмовляються від генерації ключа і займаються пошуком Еви в квантовому каналі.

3.2.5. Маскування перехоплення під шум. Види перехоплення

Задача перехоплювача Еви – отримати максимум інформації про ключ і не бути поміченою. Як відомо, будь-яка спроба перехоплення інформації призводить до збільшення рівня шуму в квантовому каналі. Насамперед Ева може використовувати різницю між робочим рівнем шуму Q_0 і максимальним рівнем Q_m. Якщо шум не перевищує максимальний рівень до робочого – перехоплення буде непомітним. Це найбільш реальний спосіб перехоплення через те, що вона потребує підключення до квантового каналу лише в одній точці. Під час аналізу захищеності лінії КРК роблять більш вагомі припущення щодо Еви. Передбачається, що Ева може володіти будь-якою технологією. В результаті у Еви вже є план перехоплення: Ева робить заміну шумного квантового каналу на ідеальний і перехоплює інформацію в цьому каналі, вносячи шум не більше Q_m. В такому випадку весь шум квантового каналу буде результатом перехоплення, що забезпечує Еві максимальну інформацію про кінцевий ключ.

Всі атаки на квантовий канал розділяються на два: основний клас – пов’язані з квантовою природою носія інформації, специфічні – недосконаліть апаратури. Атаки другого класу пов’язані з фізичною реалізацією криптографічної лінії [3].

Для перехоплення Ева повинна зробити квантові вимірювання. Квантове вимірювання може бути прямим – коли квантова система безпосередньо взаємодіє з вимірювальним пристроєм, або непрямим – коли квантова система взаємодіє з пробною системою, яка надалі піддається прямому виміру.

Відповідно по типу виміру атаки Еви розділяються на: прямі і непрямі. Також атаки Еви діляться відповідно до об’єкта виміру. Об’єктом виміру одного вимірювального процесу може бути окремий носій інформації в квантовому каналі. В цьому випадку атака – індивідуальна. У випадку, коли вимірюванню піддаються декілька носіїв – спільна атака. Когерентна атака є більш технічно складною, але інформативною.

У випадку непрямої атаки існує такий варіант, коли кожен носій вступає у взаємодію з окремою пробною системою, а подальші виміри йдуть над блоками з декількох пробних систем, такий тип атаки називається колективним.

При будь-якому методі перехоплення Ева в результаті отримує деяку кількість числової послідовності N_E. Без обмеження спільності можна рахувати, що її довжина співпадає з довжиною сирого ключа Аліси і Боба N_R - послідовність перехопленого сирого ключа. На стадії просіювання Еві доступна вся інформація, якою обмінюються Аліса і Боб по класичному каналу. Ева виключає з сирого ключа ті ж самі біти, що Аліса і Боб. Після чого Ева отримує перехоплений просіяний ключ, який несе часткову інформацію про просіяний ключ.

Аліса і Боб для того, щоб зробити непридатною інформацію про просіяний ключ Еви, використовують відомі криптографічні процедури корекції помилок і посилення секретності. Знаючи рівень шуму в просіяному ключі, Аліса і Боб проводять процедуру корекцій помилок і отримують ідентичні виправлені ключі (ВК). Ева, спостерігаючи за відкритим каналом, по якому Аліса і Боб узгоджують виправлення помилок, такой робить корекції в перехопленому ключі і отримує перехоплений виправлений ключ (ПВК).

Непряме індивідуальне перехоплення. На даний момент непрямі виміри окремих фотонів робили тільки з дуже малою вірогідністю успіху. Проте непрямі виміри більш інформативні, ніж прямі при тому ж самому рівні внесеного шуму, тому методи захисту криптографічного ключа повинні включати таку можливість перехоплення. При непрямому вимірі кубика S, який знаходиться у відомому стані, Ева проводить його у взаємодію з пробною системою P, яка має чотири квантові рівня. Пробна система початково підготовлена в чистому вигляді. Взаємодія описується унітарним перетворенням U в загальному просторі станів S і P. Параметри перетворення вибирають таким чином, щоб отримати максимум інформацію отриману при виміряному кубіті. Після взаємодії кубіт і пробна система переходять в стан пробної системи – тобто стан пробної системи корельовано із станом кубіта.

Після взаємодії кубіт продовжує рух по квантому каналу, а пробна система зберігається Евою до стадії погодження базисів. Така затримка в вимірі Р дає Еві можливість провести виміри з розрахунком відомостей, в якому базисі знаходився кубіт S до взаємодії. Квантова пам'ять – здатність зберігати квантову інформацію протягом декількох мілісекуд. Аналіз оптимальних параметрів взаємодії і оптимального виміру пробної системи пропонує наступний вираз для інформації Еви про виправлені ключі[3]:

$$I_E(Q) = \log_2(2 - (3 - \frac{2}{1-Q})^2). \qquad . \qquad (3.2.5.1)$$

На будь-якому рівні шуму інформація Еви при оптимальній непрямій атаці вище або дорівнює її інформації при прямій атаці проміжного базиса. В робочому рівні щуму близько 5%, це перевищення складає більше двох разів, тобто інформація Еви про ВК приблизно дорівнює 20%.

Колективне перехоплення. Під час атаки на ВВ84 Ева використовує взаємодію кожного кубіта, який протікає в квантовому каналі з окремою пробною системою. Вона зберігає всі пробні системи в квантовій памяті до стадії корекції помилок. Після цього Ева вимірює всі пробні системи, які залишились для отримання інформації про виправлений ключ. Колективний вимір всіх пробних систем забезпечить Еві потенційною багато інформації, якою Аліса і Боб обмінюються на стадії корекції помилок. Але параметри колективного виміру не були опубліковані. Обчислення верхньої границі цієї інформації не має інтересу через те, що обмежена зверху максимальноє інформацією, доступній Еві при когерентному перехопленні.

Когерентне перехоплення. Ева розглядає послідовність декількох кубітів, які розповсюджуються по квантовому каналі як одну квантову систему і намагається отримати максимальну інформацію про її стан.

Під час прямого когерентного перехоплення Ева проводить пряме колективне вимірювання декільков кубітів. Можливості перехоплення

обмежені кількістю одночасно знаходженості в квантовому каналі носія. Середня відстань між послідовними носіями значення сирого біта перевищує довжину криптографічної лінії, що робить такий вид перехвату неможливим. Поки що відсутні відомості про прямий когерентний перехват.

Під час непрямого перехоплення Ева має одну пробну систему з великою кількістю квантових рівнів. Пробна система по черзі взаємодіє зі всіма кубітами, які поширюються в квантовому каналі. Стан квантової системи зберігається в квантовій пам'яті до моменту закінчення стадії виправлення помилок. Далі Ева проводить виміри пробної системи з урахуванням всієї інформації, перехопленої в класичному каналі і отримує ПВК. Наразі вважається, що непряма когерентна атака найбільш ефективна, тому що забезпечує Еві максимум інформації про ВК. Але жоден протокол ефективної атаки не був опублікований. Всі атаки призводять до висновку їх ідентичності індивідуальним атакам в розумінні отриманої інформації.

3.3. Оптична реалізація квантових криптографічних систем

3.3.1. Джерела поодиноких фотонів.

Одним з основних можливих методів КРК є передача ключа за допомогою поодиноких фотонів, стани яких (поляризація, фаза тощо) задають значення бітів ключа. Безумовна секретність КРК, точніше, неможливість непомітного перехоплення інформації, забезпечується при цьому саме однофотонністю квантового носія інформації, оскільки будь-яке вимірювання його стану призводить до зміни останнього, роблячи неможливим клонування носія.

Якщо ж КРК здійснювати за допомогою багатофотонних імпульсів, кожен з яких утворений з фотонів з однаковими значеннями біту ключа, то вимірювання одного фотону, звичайно, змінить його стан. Проте решту фотонів можна буде використати для визначення біта, що передається. Саме тому

одним з ключових елементів цілого ряду квантових криптографічних систем є джерело одиночних фотонів (ДОФ).

В ідеалі ДОФ повинен генерувати цуг фотонів, випромінюючи в потрібні моменти часу (on demand) лише один фотон, причому випромінювані фотони мають бути абсолютно однаковими. Найбільш важливими з точки зору практичного використання характеристиками ДОФ є довжина хвилі λДОФ випромінюваних фотонів та частота їх повторення ωДОФ, оптимальні величини яких значним чином обумовлюються характеристиками інших складових частин криптографічної системи.

Вибір λДОФ зазвичай є компромісом між вимогами, що накладаються середовищем поширення фотонів, та можливостями існуючих детекторів. Дійсно, з одного боку, довжина хвилі генерованих одиночних фотонів має бути такою, щоб їх поглинання під час передачі від джерела до детектора було мінімальним, а з іншого боку – для даної довжини хвилі повинні бути наявні чутливі детектори. У випадку передачі ключа в повітрі довжина хвилі λДОФ повинна потрапляти у вікна прозорості атмосфери. Зазвичай з цією метою обирають вікна 750 – 800 нм та 850-900 нм, для яких існують комерційні високоефективні лавинні кремнієві детектори одиночних фотонів з низьким рівнем шуму, які добре працюють в діапазоні довжин хвиль 600 – 900 64 нм.

Під час використання для передачі ключа існуючих телекомунікаційних мереж на стандартному одномодовому оптоволокні оптимальними є довжини хвиль λДОФ≈1,31 мкм та λДОФ≈1,55 мкм, що забезпечують внаслідок малого поглинання (~0,35 дБ/км та 0,2 дБ/км відповідно) можливість передачі ключа на відстані порядку 100-150 км. В принципі, для таких довжин хвиль є комерційні лавинні детектори на структурах InGaAs-InP, проте їх характеристики недостатньо гарні для багатьох практичних застосувань квантової криптографії.

Для менших відстаней (< 10 км) у волоконних системах КРК можна використати ДОФ, які генерують фотони на довжинах хвиль ~ 840 нм, оскільки, не дивлячись на суттєво більші втрати в оптоволокні (~3 дБ/км), для їх реєстрації можна використати кремнієві лавинні детектори. Для забезпечення

високої швидкості передачі ключа частота повторення імпульсів ωДОФ=2π/ТДОФ, де ТДОФ – час між одиночними фотонами, має бути якомога більшою, проте вона обмежується згори величиною «мертвого» часу детектора, який використовується для реєстрації одиночних фотонів. Додатковими практичними вимогами до ДОФ є здатність до тривалої стабільної роботи, бажано при кімнатній температурі, простота практичного маніпулювання станами генерованих фотонів, їх збору та передачі у певному просторовому напрямку тощо.

Наразі в експериментальній та практичній квантовій криптографії в якості ДОФ широко використовуються різноманітні джерела світла, які, як правило, лише частково задовольняють вказаним вимогам. Джерела світла можна розділити на три основні групи, до яких відносяться ДОФ, засновані на використанні: 1) ослаблених лазерних імпульсів; 2) генерації корельованих пар фотонів в процесі параметричного розпаду в кристалах з квадратичною нелінійністю; 3) одиночних квантових систем (атомів, іонів, молекул, дефектів, квантових точок тощо). В багатьох лабораторіях світу широким фронтом проводяться роботи як з вдосконалення та оптимізації існуючих ДОФ, так і з розробки ДОФ нових типів 65 з метою створення джерел, характеристики яких більшою мірою задовольняли б вимогам КРК. Детальний огляд існуючих ДОФ наведено в роботах [21,22].

3.3.2. Детектування поодиноких фотонів

Неідеальна ефективність детектування одиночних фотонів являє собою один з основних джерел шумів у квантових криптографічних системах. На сьогодні існує кілька типів фотодетекторів, які здатні справитись із завданням реєстрації одиночних фотонів з різним ступенем ефективності: прилади з так званим внутрішнім механізмом підсилення (лавинні фотодіоди (ЛФД), фотоелектронні помножувачі (ФЕП), багатоканальні підсилювачі (ФЕП-БКП)) та пристрої, що використовують інші механізми ліку фотонів (гарячі електронні

болометри (ГЕБ), надпровідний перехід Джозефсона (НПД), сенсори граничного переходу (СГП), квантові точки (КТ)).

Наразі для цілей квантової інформації найбільш широко використовуються лавинні фотодетектори, які за більшістю своїх характеристик переважають над фотоелектронними помножувачами. На ринку детекторів одиночних фотонів представлені лише прилади з внутрішнім механізмом підсилення.

Детектори на надпровідних матеріалах та квантові точки з різних причин ще не вийшли за межі лабораторії. Як будь-який пристрій, детектор одиночних фотонів характеризується набором параметрів відносно ефективності реєстрації квантів світла. В Таблиці 7.3. наведено основні характеристики відомих детекторів одиночних фотонів. Квантовий вихід (quantum efficiency) – імовірність реєстрації одиночного фотону, або відношення кількості зареєстрованих фотонів до загальної кількості, що потрапила на детектор. Досягнення максимального значення цього параметра особливо важливе для фотонів з трьома довжинами хвиль: 810 нм, 1310 нм та 1550 нм, для яких затухання в оптоволокні сягає мінімальних значень.

Для цілей квантової криптографії значення цього параметру має наближуватись до 1. Частота темнових відліків (dark count rate) – кількість помилкових спрацювань детектора за одиницю часу за відсутності фотону. Ця величина є характеристикою власних шумів детектора. У квантовій криптографії цей 66 параметр дає вклад у рівень помилок.

Природно, що проблема зниження величини цього параметра є актуальною.

Таблиця 3.3.2.1 – Основні характеристики детекторів одиночних фотонів. QEmax – максимальний квантовий вихід, ND - частота темнових відліків, J - часові флуктуації, Rm - максимальна швидкість ліку, Res – можливість розділення кількості фотонів (число в дужках вказує на кількість фотонів). Дані з [16].

Тип	QE_{max}	N_D, кГц	J, нс	R_m, мГц	Res
Si-ЛФД	0,7 на 0,8 мкм	0,1	0,35	10	немає
InGaAs/InP- ЛФД	0,1 на 1,55 мкм	50	0,8	0,1	немає
ЛФД1	0,88 на 0,69 мкм	2	2	-	немає
ЛФД2	0,7 на 0,7 мкм	-	-	-	15
ФЕП	0,4 на 0,5 мкм	0,1	-	10	немає
ФЕП-МКП	0,2 на 0,5 мкм	2	0,025	10	немає
ГЕБ(Т=4К)	0,1 на 1,55 мкм	10^{-4}	0,018	1000	-
СПД(Т=0,2К)	0,5 на 0,2-0,5 мкм	10^{-3}	2	0,05	10
СГП(Т=0,1К)	0,2 на 0,2-1,8 мкм	10^{-6}	0,35	0,02	15
КТ	0,1 на 1,68 мкм	0,1	-	-	немає

Часові флуктуації (timing jitter) – параметр, що характеризує ступінь невизначеності приходу наступного фотону. Оскільки в квантовій криптографії важливу роль відіграє часова синхронізація між двома сторонами, які обмінюються фотонами в якості носіїв інформації, зростає необхідність у зменшенні величини цього параметру.

Максимальна частота ліку фотонів (maximum count rate) – величина, обернена до «мертвого» часу, протягом якого реєстрація наступного фотону є неможливою. Відповідно, для квантових комунікацій ця величина є характеристикою швидкості передачі інформації. 67 Розділення кількості фотонів (photon number resolving) – важлива характеристика, яка притаманна далеко не всім детекторам. В системах кантової криптографії для генерації одиночних фотонів часто використовують «ослаблені» лазерні імпульси.

В цьому випадку існує ненульова імовірність того, що в сигналі опиниться більше одного фотону, це буде можливим джерелом помилок та витоку інформації. Наразі в практичних застосуваннях квантової криптографії використовують ФЕП та ЛФД різних конфігурацій. Огляд детекторів одиночних фотонів представлено в роботах [22,23].

3.3.3. Середовища поширення фотонів

Середовища, в яких поширюються фотони, або квантові канали, не **є** ідеальними. Внесений ними шум «відкриває» вікно для прослуховування, оскільки, як було відмічено раніше, основні протоколи КРК є абсолютно захищеними лише за відсутності шуму в квантовому каналі. Тому знання про особливості поширення світла в таких каналах є необхідним для забезпечення стійкості квантових криптосистем.

Оптоволоконні лінії

Розглянемо деякі особливості оптичних волокон, які слід враховувати під час розробки квантових криптографічних систем. Випромінювання поширюється у волокні завдяки наявності профілю показника заломлення в напрямку, поперечному до осі оптоволокна. Світло утримується всередині волокна завдяки ефекту повного внутрішнього відбиття. При цьому у волокні можу існувати кілька мод (режимів поширення).

Моди, по суті, є різними розв’язками рівнянь Максвела для хвилеводу та визначаються частотою й поляризацією світла. Центральна оболонка оптоволокна називається серцевиною. Якщо серцевина достатньо велика, у волокні може існувати багато хвильових мод. Такі волокна називають багатомодовими й діаметр їх серцевини зазвичай дорівнює 50 мкм.

Окремий фотон буде взаємодіяти з таким набором як із незамкненою системою, а отже, багатомодове волокно не можна використовувати в якості квантового каналу. 68 Якщо діаметр серцевини малий порівняно з довжиною хвилі, у волокні поширюватиметься лише одна хвильова мода. Для

телекомунікаційних довжин хвиль (1,3 мкм та 1,5 мкм) типовий діаметр серцевини дорівнює 8 мкм. Одномодові волокна добре підходять для передачі одиночних фотонів.

Поляризаційні ефекти в одномодових волокнах.

Поляризаційні ефекти слугують джерелом помилок для будь-яких комунікаційних схем, як класичних, так і квантових. Ефект подвійного променезаломлення в сучасних оптичних волокнах доволі незначний, щоб здійснювати вплив на класичний канал зв’язку.

Натомість для квантового каналу навіть малий ефект подвійного променезаломлення може спричинити серйозні проблеми. Всі реалізації квантового зв’язку, засновані на оптичних волокнах, зіштовхуються з цією проблемою. Врахування поляризаційних ефектів важливе не лише для систем, заснованих на кодуванні поляризації, а й для тих, що побудовані на кодуванні фази.

Розглянемо детальніше три різних поляризаційних ефекти: двопроменезаломлення, дисперсію мод за поляризацією та залежність втрат від поляризації. Двопроменезаломлення. Навіть одномодовий хвилевод може підтримувати дві вироджені моди, переважно поляризовані в двох ортогональних напрямках. За ідеальних умов досконалої циліндричної геометрії та ізотропності речовини ортогонально поляризовані моди не взаємодіють між собою.

Однак в реальних умовах малі відхилення від циліндричної геометрії або малі флуктуації в анізотропії речовини (наприклад, викликані статичними напруженнями в серцевині волокна) викликають змішування двох поляризаційних станів, знімаючи виродження мод. Сталі поширення стають різними для мод, поляризованих у x- та y- напрямках. Ця властивість називається двопроменезаломленням мод. Існують оптичні волокна, в яких зберігаються стани поляризації. В таких волокнах примусово створюється сильне двопроменезаломлення, так що малі випадкові флуктуації суттєво не впливають на поляризацію.

Один зі способів створення сильного двопроменезаломлення – порушення циліндричної симетрії та створення волокна з еліптичною формою серцевини або підкладки. В іншому методі двопроменезаломлення 69 викликається статичними пружними напруженнями. Якщо ефект двопроменезаломлення є стійким в часі, його можна компенсувати.

Дисперсія мод по поляризації призводить до наявності двох різних групових швидкостей для ортогонально поляризованих мод. Дві групові швидкості локально створюються двопроменезаломленням. В оптичних волокнах локальна дисперсія приблизно дорівнює фазовій дисперсії. За порядком величини вона складає кілька пікосекунд на кілометр.

Оптичний імпульс локально розподіляється між «швидкою» та «повільною» модами. Проте оскільки ефект двопроменезаломлення малий, ці моди слабко взаємодіють. Навіть малі неоднорідності у хвилеводі викликають перекачування енергії від швидкої моди до повільної й навпаки.

Дисперсія мод по поляризації наростає пропорційно квадратному кореню з довжини волокна. Довжина взаємодії мод варіюється від кількох до сотень метрів залежно від типу волокна. В сучасних оптичних волокнах взаємодія мод штучно підсилюється в процесі виготовлення. Дисперсія поляризації описується статистичним розподілом затримок, викликана цим процесом деполяризація схожа на ефект втрати когерентності. Для запобігання цьому ефекту в квантових каналах зв’язку використовують лазерні імпульси з часом когерентності більшим за найбільший час затримки. Залежність втрат від поляризації є незначною в оптичних волокнах, проте вона може виявитись суттєвою в таких оптичних компонентах, як фазові модулятори. Зокрема, деякі оптичні хвилеводи підтримують лише одну поляризацію. Сама по собі залежність втрат від поляризації є стійкою, але за наявності ефекту двопроменезаломлення можуть виникати флуктуації.

Залежність втрат від поляризації не описується унітарним перетворенням в просторі станів поляризації. Зокрема, неортогональні стани можуть перетворитись на ортогональні з деякими втратами. Цю обставину

може бути використано для перехоплення інформації. Як вже було відмічено, поляризаційні ефекти в квантових лініях зв'язку можуть бути скомпенсовані.

Відкритий простір.

Фотони, які поширюються у відкритому просторі, не зазнають двопроменезаломлення, тому таке середовище краще підходить для поляризаційного кодування, ніж оптоволокно. Однак атмосфера призводить до інших шумових ефектів. Відкритий простір (земна атмосфера) надає широкі можливості для передачі фотонів з різними довжинами хвиль. В якості генераторів та приймачів випромінювання в цьому випадку також використовують лазери та фотодетектори (найпростіший приклад – пульт дистанційного керування).

Як і у випадку оптичного волокна, найбільша ефективність передачі досягається для фотонів певної енергії, для яких атмосфера дає «вікна прозорості». Найбільш прозорою атмосфера є для випромінювання з довжиною, більшою за 1 см. Нажаль, практична реалізація протоколів квантової криптографії з використанням фотонів сантиметрового діапазону є неможливою через малу величину енергії фотона, а отже, неможливість його ефективного детектування. Саме тому найкращими кандидатами є два спектральні вікна: 0,3 – 1,3 мкм та 1,5 – 1,8 мкм, тим більше, що генератори та приймачі фотонів в цих діапазонах розроблені й широко застосовуються під час передачі фотонів через оптичне волокно. Під час передачі фотонів через атмосферу існує чотири основних види втрат: *дифракційні втрати, статичні атмосферні втрати (розсіяння та поглинання), турбулентність атмосфери, оптичні втрати.*

Дифракційні втрати призводять до збільшення діаметра світлового пучка зі збільшенням відстані передачі

Статичні атмосферні втрати виникають й за відсутності турбулентності атмосфери й представляють собою процеси розсіяння та поглинання корисного сигналу. При цьому дощ або навіть легкий туман ускладнюють або роблять практично неможливою передачу сигналу. Затухання

сигналу в даному випадку залежить також від кута його поширення відносно зеніту й змінюється на 3-5° при зміні кута від 0° до 50°.

Турбулентність атмосфери може викликати ряд негативних ефектів: збільшення діаметра світлового пучка подібно до того, як це відбувається 71 внаслідок дифракційних втрат, відхилення світлового пучка, когерентні втрати, коливання інтенсивності пучка навколо середнього значення.

Оптичні втрати пов’язані з використанням телескопів для прийому та передачі сигналу: діаметр пучка, що приймається, може бути занадто великим, в результаті чого можливі втрати. У випадку одиночних фотонів додатковою проблемою є фонове випромінювання (Сонце, Місяць, світло зірок), тому важливим елементом практичних схем є синхронізація між приймачем та передавачем, щоб фотодетектор вмикався лише на короткий час в момент приходу чергового фотону для зменшення імовірності реєстрації сторонніх фотонів. Очевидно, що слабкі однофотонні сигнали будуть значною мірою відчувати вищевказані ефекти, внаслідок чого різко знизиться швидкість та відстань ефективної передачі. Для вирішення цієї проблеми було запропоновано схеми квантової криптографії, які використовують супутники на різних орбітах від 300 до 30000 км. Ефективність передачі в даному випадку зростає через те, що густина атмосфери спадає зі зростанням висоти над Землею й втрати при досягненні фотоном супутника на висоті 300 км порівняні зі втратами під час проходження 10-15 км біля поверхні планети.

3.4. Експерементальні криптосисетми КРК

3.4.1.Оптичні схеми з поляризаційним кодуванням

Вибір схеми кодування для експериментальної реалізації систем КРК визначається оптичними характеристиками каналу зв’язку. На Рис. 7.2 показано типову будову схеми КРК з поляризаційним кодуванням. Для здійснення поляризаційного кодування в таких схемах зазвичай використовуються комірки

Поккельса, для детектування поляризаційних станів фотонів – призми Глана. Компенсація стаціонарних поляризаційних втрат може здійснюватись шляхом уведення до схеми системи хвильових платівок.

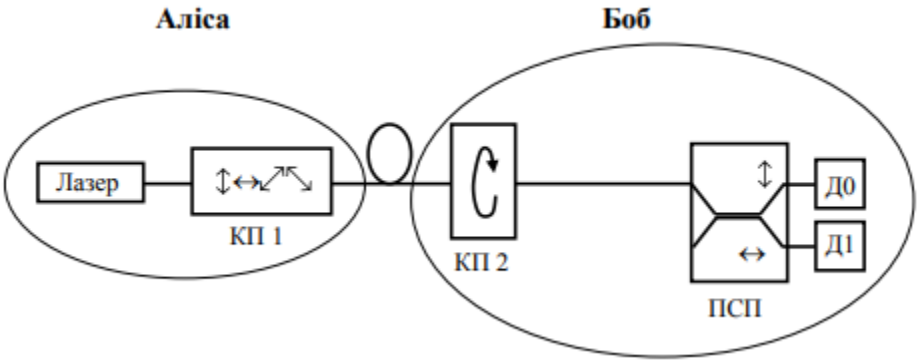

Рисунок 3.4.1 Типова схема КРК з використанням поляризаційного кодування КП- комірки Поккельса для кодування поляризаційного стану фотону, ПСП- поляризаційний світлоподілювач, який розкладає промінь на дві ортогональні компоненти, що реєструються дитекторами Д0 та Д1.

Поляризаційні схеми широко використовуються для передачі сигналу у вільному просторі, де зберігається поляризація фотонів, проте їх важче реалізувати в оптичних хвилеводах через ефекти деполяризації та випадкового флуктуаційного двопроменезаломлення. Деполяризація в таких випадках не є основною проблемою: її дію можна компенсувати шляхом використання джерела з високим ступенем когерентності. Часова шкала флуктуації двопроменезаломлення за стаціонарних умов зазвичай доволі повільна (1 год). Проте поряд з такими повільними флуктуаціями існують більш швидкі, які роблять передавання ключа неможливим. Електронна система компенсації має ПСП ↔ ↔ Лазер КП 1 КП 2 Д0 Д1 Аліса Боб 73 відслідковувати та виправляти поляризацію, зазвичай вона доволі громіздка й потребує додаткового узгодження між станціями передачі й прийому. Менше з тим, експериментальні доробки зі створення таких систем тривають і є доволі успішними [25, 26].

Оптичні схеми з фазовим кодуванням

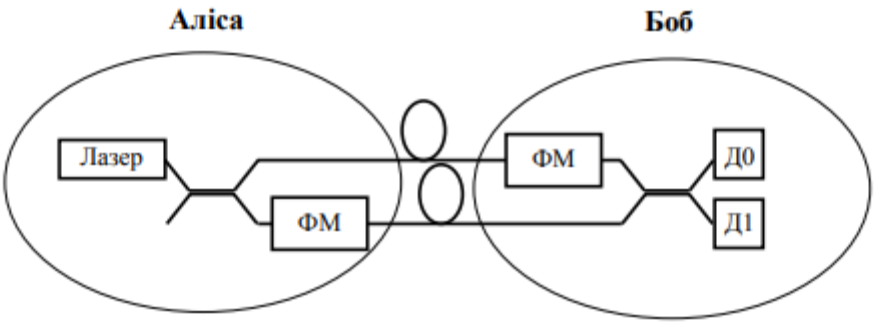

Рисунок 3.4.2 Типова схема КРК з використанням фазового кодування, ФП. Відносний вибір фази у двох фазових модуляторах (ФМ) створює інтерференційну картину.

Систему КРК можна реалізувати з використанням фазового кодування. Типову схему такого кодування представлено на Рис. 3.4.2. Вона являє собою інтерферометр Маха-Цендера з розширеною базою, з використанням двох фазових модуляторів (ФМ), які дозволяють здійснювати кодування та декодування.

Якщо Аліса використовує свій ФМ, щоб створювати зсув фаз величиною 0 або π (які відповідають значенню біта 0 або 1), то Боб отримає відлік або на Д0, або на Д1. Така схема еквівалентна поляризаційній схемі кодування, в якій використовуються лише дві поляризації. Для конфіденційності додається випадковий вибір базисів. Аліса повинна обрати один з чотирьох зсувів фаз: 0 або π, що відповідає базису ⊕ , π/2 або 3π/2, що відповідає базису ⊗ . Зі свого Лазер Д0 ФМ Д1 ФМ Аліса Боб 74 боку, Боб також обирає між нульовим зсувом фаз, тобто вимірюванням у базисі ⊕ , та зсувом фаз π/2, тобто вимірюванням у базисі ⊗ . Така схема буде еквівалента схемі на Рис. 3.4.2. в протоколі BB84. Нажаль, зберегти різницю фаз в інтеріерометрі з розширеною базою (з довжиною більше ніж 20 км) дуже важко. Тому з практичної точки зору краще використовувати схему фазового кодування з подвійним інтерферометром Маха-Цендера, як це, наприклад, було реалізовано в [27]. На

Рис. 3.4.3. показано схему фазового кодування з подвійним інтерферометром Маха-Цендера.

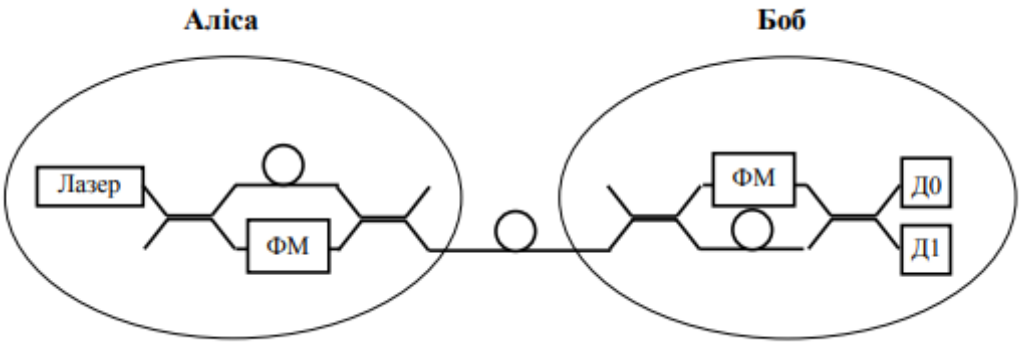

Рисунок 3.4.3 Типова схема КРК з фазовим кодування з використанням подвійного інтерферометра Маха-Цендера. Замість того, щоб проходити по двох різних шляхах, два імпульси по одному каналу, хоча й із затримкою в часі. Така схема збільшує стабільність інтерферометра, проте збільшє втрати на дБ в установці Боба.

Імпульс, генерований лазером Аліси, розділяється на дві частини, які поширюються коротким (К) та довгим (Д) шляхом. Після проходження через інтерферометр Боба з них формується три імпульси. Два з них, КК (короткийкороткий) та ДД (довгий-довгий) не важливі, оскільки не призводять до інтерференції. В той же час, центральний імпульс відповідає двом можливим шляхам: КД або ДК, які є ідентичними, а отже, інтерферують. Кодування та декодування в такій системі відбувається в базисах, аналогічних попередньому випадку. Така схема є більш стабільною, оскільки два когерентні вклади розділяються лише на кілька фемтосекунд, поширюються по одному каналу й не відчувають температурних або механічних флуктуацій.

Основний недолік схеми полягає у втраті половини сигналу в імпульсах ДД та КК. Аліса Боб Лазер Д0 ФМ Д1 ФМ 75 На сьогодні представлено значну кількість експериментальних реалізацій систем КРК, найпотужніша з яких дозволяє передавати 1 Мбіт/с (на відстань 20 км через оптичне волокно) та 10 кбіт/с (на відстань 100 км через волокно). Такі системи є спільною розробкою

University of Cambridge та компанії Toshiba й використовують протокол BB84. У 2007 р. Los Alamos National Laboratory (NIST), яка є провідним розробником квантових інформаційних систем, реалізувала передачу секретного ключа на відстань 148,7 км через оптоволокно, використовуючи протокол BB84. У серпні 2015 р. було реалізовано систему КРК на відстань 307 км, експеримент проведено University of Geneva та Corning Inc, потужність сигналу становила 12,7 кбіт/с.

У червні 2017 р. наукова група на чолі з Томасом Дженвейном (Thomas Jennewein) з Institute for Quantum Computing та University of Waterloo вперше продемонструвала роботу системи КРК між Землею та літаком, що знаходився в русі. Дослідники повідомили про передачу квантового ключа на відстань 3 – 10 км, потужність сигналу становила 868 кбіт. Також у червні 2017 р. в рамках проекту Quantum Experiments at Space Scale китайські вчені на чолі з Pan Jianwei з University of Science and Technology of China продемонстрували роботу системи КРК на заплутаних фотонних станах на відстань 1203 км між двома наземними станціями, започаткувавши створення міжконтинентальної мережі КРК. Фотони пересилали через супутник квантового зв’язку Micius, таким чином сумарний шлях фотонів становив від 1600 до 2400 км. Пізніше цього ж року було реалізовано сеанс квантового зв’язку для передачі зображень та відео між Китаєм (Бейінг) та Австрією (Вена).

Окрім експериментальних, існують також комерційні системи КРК. На ринку таку продукцію пропонує чотири компанії: ID Quantique (Швейцарія), MagiQ Technologies (США), QuintessenceLabs (Австралія) та SeQureNet (Франція). Деякі інші компанії також займаються активними науковими розробками, серед них компанії Toshiba, HP, IBM, Mitsubishi, NEC та NTT.

3.5 Висновок з розділу 3

Джерела одиночних фотонів на основі послаблених лазерних імпульсів просто в використанні, наявність широкого ряду лазерів працюючих при

кімнатних температурах і генеруючи випромінювання практично в будь-яких довжинах хвиль, легко маніпулювати, збирати і відправляти на потрібні детектори. Основними недоліками ДОФ є ймовірність того, що джерело може випустити декілька фотонів одночасно, а також температурний режим під час роботи приладу.

Традиційні пристрої детектування ФЕП і ЛФД є найбільш розповсюдженими в квантових системах, але не зважаючи на широке використання вони мають ряд недоліків пов’язаних не високою швидкодією внаслідок наявності в лінії шумів, тому ведуться досліди інших типів детекторів.

Поляризаційне і фазове кодування, які використовуються, але мають ряд недоліків, для усунення яких потрібні системи компенсації, яка буде неперервно відслідковувати і виправляти поляризації, що зробить систему на порядок громіздкою. На данний час ведеться вдосконалення методів кодування в квантових системах.

ВИСНОВОК

Оптичні системи передачі інформації є одним з найбільш перспективних сучасних напрямків в області техніки зв'язку. Вони увібрали в себе кращі досягнення мікроелектроніки, волоконної оптики, інтегральної оптоелектроніки, фізики і техніки напівпровідників.

Наукові проблеми освоєння оптичного діапазону зв'язку до теперішнього часу, в значній мірі, вирішені і подальший розвиток оптичних систем передачі інформації істотно залежить від рівня і стану технології виробництва оптичних і оптико-електронних компонент таких систем. Це не виключає можливості висунення і реалізації нових ідей в області фізики і техніки оптичних систем передачі інформації, заснованих на досить різноманітні властивості як оптичного випромінювання, так і застосовуваних в таких системах оптичних матеріалів, їх складних композицій і структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жиров О.А. Квантовая механика, Новосибирск, 2003. – 76 с. Смешанное состояние квантовых систем – стр. 15 – 16.

2. *Березин Ф. А., Шубин М. А.* Уравнение Шредингера.— М.: Изд-во МГУ.— 1983.— 392 с.

3. С.Я.Килин, Д.Б.Хорошко, А.П.Низовцев Квантовая криптография. - Минск: Белорусская наука, 2007. - 391 с.

4. Скалли М.О., Зубайри М.С. Квантовая оптика. М.:ФИЗМАТЛИТ, 2003 г.

5. Bell, J. On the Einstein Podolsky Rosen paradox / J. Bell //Physics.— 1964.— Vol. 1.— P. 195–200.

6. Харин, Ю. С. Математические основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев.— Минск: БГУ, 1999.

7. Bennett, C. H. Quantum cryptography: Public key distribution and coin tossing / C. H. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers and Systems and Signal Processing (Bangalore, India). —1984.— P. 175–179.

8. Bennett, C. H. Quantum cryptography using any two nonorthogonal states / C. H. Bennett // Phys. Rev. Lett. — 1992.— Vol. 68.— P. 3121.

9. Ekert, A. Quantum cryptography based on Bell’s theorem / A. Ekert // Phys. Rev. Lett. — 1991.— Vol. 67, № 6. — P. 661–663.

10. Basche, T. Photon antibunching in the fluorescence of a single dye molecule trapped in a solid / T. Basche, W. E. Moerner, M. Orrit, H. Talon // Phys. Rev. Lett. — 1992.— Vol. 69.— P. 1516–1519.

11. Килин, С. Я. Квантовая оптика: поля и их детектирование / С. Я. Килин.— Минск: Наука и техника, 1990; М.: Едиториал УРСС, 2003.

12. Берковский А. Г., Гаванин В. А., Зайдель И. Н., Вакуумные фотоэлектронные приборы, 2 изд., М.

13. Gisin, N. Towards practical and fast quantum

cryptography / N. Gisin, G. Ribordy, H. Zbinden et al. // arXiv:quant-ph/0411022.— 2004.

14. Ekert, A. K. Practical quantum cryptography based on two-photon interferometry / A. K. Ekert, J. G. Rarity, P. R. Tapster, G. M. Palma // Phys. Rev. Lett. — 1992.— Vol. 69.— P. 1293.

15. Muller, A. “Plug and play” systems for quantum cryptography / A. Muller, T. Herzog, B. Huttner et al. // Appl. Phys. Lett. — 1997.— Vol. 70.— P. 793.

16. Fuchs, C. A. Optimal eavesdropping in quantum cryptography. I. information bound and optimal strategy / C. A. Fuchs, N. Gisin, R. B. Griffiths et al. // Phys. Rev. A. — 1997.— Vol. 56, № 2.— P. 1163–1172.

17. Hirano, T. Quantum cryptography using pulsed homodyne detection / T. Hirano, H. Yamanaka, M. Ashikaga et al. // Phys. Rev. A. — 2003.— Vol. 68.— P. 042331.

18. Lorenz, S. Continuous variable quantum key distribution using polarization encoding and post selection / S. Lorenz, N. Korolkova, G. Leuchs // Appl. Phys. B. — 2004.— Vol. 79.— P. 273.

19. Grosshans, F. Continuous variable quantum cryptography / F. Grosshans, P. Grangier // Phys. Rev. Lett. — 2002.— Vol. 88, № 5.— P. 057902.

20. Тычинский В.П. Мощные газовые лазеры, УФН, т. 91, вып. 3, 1967, стр. 389 – 424.

21. Д.Бауместер. Физика квантовой информации, Москва: Постмаркет, 2002. – 376с.