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: «Аналіз видів та способів генерації квантових таємних ключів»

Виконав (-ла):
студент (-ка) ІІ курсу, групи ТС-з71мп
Хорунжий Олександр Євгенійович _____

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

Рецензент:

_____

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

Київ – 2018

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-науковою 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

Хорунжому Олександру Євгенійовичу

1. Тема дисертації «Аналіз видів та способів генерації квантових таємних ключів», 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 квантові стани фотонів

4. Предмет дослідження методи генерації фотонів

5. Перелік завдань, які потрібно розробити

- Провести аналіз літератури по темі;
- Дослідити способи генерації заплутаних фотонів;

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 «Висновки»

7. Орієнтовний перелік публікацій

8. Дата видачі завдання 12 грудня 2017 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Огляд науково-технічної літератури	12.12.2017- 16.12.2017	виконано
2	Обгрунтування актуальності теми роботи	16.12.2017 - 24.02.2018	виконано
3	Написання першого розділу роботи	24.02.2018 – 15.05.2018	виконано
4	Написання другого розділу роботи	15.05.2018 – 03.06.2018	виконано
5	Написання третього розділу роботи	03.06.2018 – 24.08.2018	виконано
6	Написання четвертого розділу роботи	24.08.2018 – 27.09.2018	виконано
7	Написання висновків по роботі	27.09.2018 – 24.10.2018	виконано
8	Підготовка доповіді та демонстраційних матеріалів	24.10.2018 - 27.11.2018	виконано

Студент О. Є. Хорунжий

Науковий керівник дисертації О. О. Трубін

РЕФЕРАТ

Темою магістерської дисертації є аналіз видів та способів генерації квантових таємних ключів.

Робота містить 79 сторінок, зокрема 25 ілюстрацій, 5 таблиць та 28 джерел інформації.

Тема магістерської дисертації є актуальною, так як квантові закони дозволяють вивести методи захисту інформації в телекомунікаційних системах на якісно новий рівень.

Мета дисертації полягає в аналізі основних способів передачі одиничних фотонів, протоколів квантового розподілу ключа та визначенні основних проблем квантової криптографії на даний момент.

Об’єктом дослідження є квантові стани фотонів.

Предметом дослідження є методи генерації фотонів.

При виконанні роботи проводився аналіз протоколів квантового розподілу ключа.

У дисертації були запропоновані актуальні та найбільш безпечні способи створення квантових таємних ключів.

ABSTRACT

The theme of the master's thesis is to analyze the types and methods of generating quantum secret keys.

The work contains 79 pages, including 25 illustrations, 5 tables and 28 sources of information.

The topic of the master's thesis is relevant, since quantum laws allow the methods of information protection in telecommunication systems to be brought out to a qualitatively new level.

The purpose of the dissertation is to analyze the main methods of transmitting single photons, protocols of quantum development of the key and to determine the main problems of quantum cryptography at the moment.

The object of research is the quantum states of photons.

The subject of the research is the methods of photon generation.

In the course of the work, the analysis of protocols of quantum distribution of key was carried out.

The dissertation offered the most actual and most safe ways to create quantum secret keys.

РЕФЕРАТ

Темой магистерской диссертации является анализ видов и способов генерации квантовых тайных ключей.

Работа содержит 79 страниц, в том числе 25 иллюстраций, 5 таблиц и 28 источников информации.

Тема магистерской диссертации является актуальной, так как квантовые законы позволяют вывести методы защиты информации в телекоммуникационных системах на качественно новый уровень.

Цель диссертации состоит в анализе основных способов передачи единичных фотонов, протоколов квантового распределения ключа и определении основных проблем квантовой криптографии на данный момент.

Объектом исследования являются квантовые состояния фотонов.

Предметом исследования являются методы генерации фотонов.

При выполнении работы проводился анализ протоколов квантового распределения ключа.

В диссертации были предложены актуальные и наиболее безопасные способы создания квантовых тайных ключей.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ГФД – Газові фотонні детектори.

КРК – Квантове розподілення ключів;

ЛФД – Лавинні фотодіоди.

МКП – Мікроканальні пластини.

ПМД – Поляризаційна модова дисперсія.

ФЕП – Фотоелектронний помножувач.

ВСТУП

Формування квантової криптографії як науки почалося з дослідження С. Візнера [1]. Оскільки методи класичної криптографії не задовольняли зростаючим вимогам користувачів серед яких збільшення швидкості, рівня безпеки і захищеності всіх мережевих транзакцій. Громіздкі і не завжди надійні алгоритми засновані на законах математики вже не могли вирішити поставлені завдання. Ще одна проблема стосувалася області комп'ютерних технологій: потужність і швидкість обчислень обмежувалася законом Мура і мрія про суперкомп'ютери залишалася мрією.

Поставлену проблему вирішили два видатних і талановитих вчених, послідовники Візнера і творці квантової криптографії - Ч. Беннет і Ж. Бассард.

Ідея квантової криптографії є новою і революційною. Ч. Беннет і Ж. Бассард відкинули ідею створення алгоритмів на основі математичних законів і вирішили створити нову галузь криптографії засновану на незламних фізичних законах. Як відомо, будь-який математичний алгоритм захисту можна зруйнувати за допомогою іншого математичного інструменту або методом грубої сили (brute force) і великої потужності. Проти законів фізики ніякої панацеї немає.

Беннет і Бассард пропонують застосовувати для передачі сигналів частки світла - фотони. Ідея використання світлових імпульсів, в той час, була новаторською. Оптоволоконні технології входили в стадію розквіту і завжди користувалися попитом у користувачів мережі Інтернет. Вчені запропонували застосовувати не тільки ансамблі квантів світла, а також одиночні носії - фотони.

РОЗДІЛ 1. КВАНТОВА КРИПТОГРАФІЯ

1.1 Введення в криптографію

Криптографія - це мистецтво приховування інформації в послідовності бітів від будь-якого несанкціонованого доступу. Для досягнення цієї мети використовують шифрування: повідомлення за допомогою деякого алгоритму комбінується з додатковою секретною інформацією (ключем), в результаті чого виходить криптограма [2]. Довгий час способи розробки алгоритмів шифрування визначалися виключно хитрістю і винахідливістю їх авторів. І лише в XX столітті цією областю зацікавилися математики, а згодом - і фізики.

Для будь-якої системи передачі інформації характерні наступні дійові особи: об'єкти А і Б, що обмінюються інформацією (будемо називати їх Аліса і Боб - Аліса передає інформацію Бобу), і хтось Е, який намагається перехопити цю інформацію (надалі - Єва). Завдання полягає в тому, щоб виключити можливість розшифровки інформації Євою. Однак на практиці це жорстка вимога замінюється більш м'яким: необхідно зробити розшифровку повідомлення досить важкою для Єви.

Класичний підхід полягає в тому, що ключ, що використовується як для шифрування, так і для розшифровки повідомлення, повинен бути відомий тільки Алісі і Бобу. Такі системи називаються криптосистемами з закритим ключем. Надійність процедури шифрування доведена тільки для методу «одноразових блокнотів», запропонованого в 1917 році Гильбертом Вернама (Gilbert Vernam). Ідея його полягає в тому, що Аліса і Боб обмінюються набором загальних секретних ключів, кожен з яких використовується для шифрування тільки одного повідомлення. Ключі генеруються випадково і ніякої інформації не несуть. Процес шифрування полягає в тому, що кожен символ вихідного повідомлення

«складається» з відповідним символом ключа (так що ключ повинен бути досить довгим, а повідомлення - досить коротким). У «докомп'ютерний» час ключі зберігали в блокнотах з відривними листами (звідси і назва методу). Кожен лист блокнота знищувався після використання.

У застосуванні до систем телекомунікацій виникає проблема забезпечення секретності під час обміну ключами («блокнотами»), оскільки ключ повинен бути доставлений одержувачу повідомлення заздалегідь і з дотриманням суворої секретності. Інакше кажучи, конфіденційно обмінятися повідомленнями дозволяють ключі, але як обмінятися самими ключами із забезпеченням таємності? Сформульовану таким чином проблему називають проблемою поширення ключа.

Якщо використовується постійний закритий ключ, то розшифровка повідомлення залежить від обчислювальної потужності системи і часу. У США, наприклад, для шифрування використовується стандарт DES (Data Encryption Standard), розроблений в 1977 році. Він заснований на 56-бітному ключі, за допомогою якого можна закодувати 64 біт інформації. На цьому стандарті грунтується захист банківських транзакцій, паролів Unix-систем та інших секретних даних. Оскільки довжина ключа менше, ніж довжина кодованого повідомлення, то механізм захисту не є абсолютно надійним. Якщо спробувати вгадати ключ методом проб і помилок, потрібно перебрати 256 всіляких значень. І хоча цей обсяг обчислень дуже великий, в даний час вже є дані про можливість взлому подібних систем. Рекордний час становить 22 години 15 хвилин при розподіленої обробки інформації в комп'ютерній мережі.

Теорія шифрування з використанням відкритого ключа була створена Уетфілдом Діффі (Whitfield Diffie) і Мартіном Хеллманом (Martin Hellman) в 1976 р. У цій системі Боб має загальнодоступний код

для шифрування і закритий код для розшифровки повідомлень. Криптосистеми з відкритим ключем ґрунтуються на так званих односторонніх функціях: по деякому x легко вирахувати функцію f (x), але знаючи f (x) важко обчислити x.

Перший алгоритм, заснований на теорії Діффі-Хеллмана, був запропонований Роном Райвест (Ron Rivest), Еді Шамір (Adi Shamir) і Леонардом Едлману (Leonard Adleman) в 1977 р (RSA-алгоритм) [3]. Він заснований на розкладанні простого числа на множники. Відомо, що обчислити добуток двох простих чисел легко. У той же час, зворотна задача - розкладання числа на прості множники, досить трудомістка, оскільки час обчислень експоненціально зростає при збільшенні кількості бітів у вихідному числі. Хоча в даний час не опубліковані швидкі алгоритми розв'язання задачі розкладання числа на прості множники, не можна стверджувати, що вони не існують зовсім. Крім того, обчислювальна потужність комп'ютерних систем постійно зростає, тому складність завдання не означає її нерозв'язність. Так, компанія RSA, заснована вищепереліченими авторами алгоритму, пропонує всім бажаючим розкласти на прості множники представлені нею числа. Один з останніх звітів компанії присвячений розкладанню числа, що складається з 155 цифр. Це завдання вимагає 35,7 процесорних року, що приблизно еквівалентно 8000MIPS-років3; в реальному часі треба було 3,7 місяці завдяки розподіленої обробки інформації в комп'ютерній мережі.

Таким чином, на даний момент єдиним надійним методом шифрування є метод «одноразового блокнота», оскільки доведена його безумовна секретність, тобто секретність по відношенню до шпигуна, який має необмежений час і обчислювальну потужність. На шляху до досягнення такого рівня секретності, стоїть проблема поширення ключа: Аліса і Боб повинні обмінятися ключем, зберігши його в повному

секреті. Одним з її рішень є розроблений Чарльзом Беннет (Charles Bennett) і Джил Брассард (Gilles Brassard) протокол квантового розподілу ключа (quantum key distribution).

1.2 Квантовий розподіл ключа

Квантовий розподіл ключа [4] - метод передачі ключа, який використовує квантові явища для гарантії безпечної зв'язку. Цей метод дозволяє двом сторонам, з'єднаним з відкритого каналу зв'язку, створити загальний випадковий ключ, який відомий тільки їм, і використовувати його для шифрування і розшифрування повідомлень. Важливою і унікальною властивістю квантового розподілу ключа є можливість виявити присутність третьої сторони, яка намагається отримати інформацію про ключ. Тут використовується фундаментальний аспект квантової механіки: процес виміру квантової системи порушує її. Третя сторона, яка намагається отримати ключ, повинна виміряти надіслані через з'єднання квантові стани, що веде до їх зміни і появи аномалії. За допомогою квантової суперпозиції, квантової заплутаності і передачі даних в квантових станах можна здійснити канал зв'язку, який виявляє аномалії. Якщо кількість аномалій нижче певного порогу, то буде створено, ключ що гарантує безпеку (третя сторона не має інформації про це), інакше секретний ключ не буде створено і зв'язок припиняється.

Стан квантового об'єкта (тобто, грубо кажучи, об'єкта дуже малої маси і розмірів, наприклад, електрона або фотона) може бути визначено виміром. Однак відразу після виконання цього виміру квантовий об'єкт неминуче переходить в інший стан, причому передбачити цей стан неможливо. Отже, якщо в якості носіїв інформації використовувати квантові частинки, то спроба перехопити повідомлення призведе до зміни

стану частинок, що дозволить виявити порушення секретності передачі. Крім того, неможливо отримати повну інформацію про квантовий об'єкт, і отже, неможливо його скопіювати. Ці властивості квантових об'єктів роблять їх «невловимими».

Ідея використовувати квантові об'єкти для захисту інформації від підробки та несанкціонованого доступу вперше була висловлена Стефаном Вейснер (Stephen Weisner) в 1970 р Через 10 років Беннет і Брассард, які були знайомі з роботою Вейснер, запропонували використовувати квантові об'єкти для передачі секретного ключа. У 1984 р вони опублікували статтю, в якій описувався протокол квантового поширення ключа BB84.

Носіями інформації в протоколі BB84 є фотони, поляризовані під кутами 0, 45, 90, 135 градусів. Відповідно до законів квантової фізики, за допомогою вимірювання можна розрізнити лише два ортогональних станів: якщо відомо, що фотон поляризований або вертикально, або горизонтально, то шляхом вимірювання, можна встановити - як саме; те ж саме можна стверджувати щодо поляризації під кутами 45 і 135 градусів. Однак точно відрізнити вертикально поляризований фотон від фотона, поляризованого під кутом 45 градусів, неможливо.

Ці особливості поведінки квантових об'єктів лягли в основу протоколу квантового розподілу ключа. Щоб обмінятися ключем, Аліса і Боб роблять такі дії:

1) Аліса посилає Бобу фотон в одному з поляризованих станів (0, 45, 90, 135 градусів) і записує кут поляризації. Відлік кутів ведеться від напрямку "вертикально вгору" за годинниковою стрілкою. В реальних же системах перед процесом передачі ключа обладнання спеціально юстирується для забезпечення однакового режиму відліку на приймачі і передавачі (причому цю юстировку доводиться проводити періодично в

процесі передачі), а "просторове розташування" початку відліку кута – несуттєво;

2) Боб в своєму розпорядженні має два аналізатори: один розпізнає вертикально-горизонтальну поляризацію, інший - діагональну. Для кожного фотона Боб випадково вибирає один з аналізаторів і записує тип аналізатора і результат вимірювань;

3) По загальнодоступному каналу зв'язку Боб повідомляє Алісі, які аналізатори використовувалися, але не повідомляє, які результати були отримані;

4) Аліса по загальнодоступному каналу зв'язку повідомляє Бобу, які аналізатори він вибрав правильно. Ті фотони, для яких Боб невірно вибрав аналізатор, відкидаються.

Протокол для обміну ключем може виглядати, як показано на рис. 1.1.

Обозначение анализатора	Поляризация фотонов
+	Прямоугольный
x	Диагональный

Последовательность фотонов Алисы	|	/	/	—	\	|	|	—	—
Последовательность анализаторов Боба	+	x	+	+	x	x	x	+	x
Результаты измерений Боба	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	да	да		да	да			да	
Ключ	0	0		1	1			1	

Рисунок 1.1 Протокол BB84

Квантова передача включає шифрування інформації в квантові стани, або кубіти, на відміну від класичної передачі, що використовує біти. Як правило, використовуються фотони для квантових станів. Квантовий розподіл ключів використовує певні властивості квантових станів для забезпечення безпеки. Існує різні підходи квантового розподілу ключів, але вони можуть бути розділені на дві

основні категорії, в залежності від властивостей, які вони використовують.

Протокол підготовки та вимірювання.

На відміну від фізики, вимір є невід'ємною частиною квантової фізики. Вимірювання невідомого квантового стану змінює його в деякому роді. Це відомо як квантовий індетермінізм і лежить в основі результатів, таких як принцип невизначеності Гейзенберга і теореми про заборону клонування. Це може бути використано для того щоб виявити будь-які прослушки на зв'язку і, що більш важливо, для розрахунку кількості інформації, яка була перехоплена.

Протоколи засновані на заплутаності.

Квантові стани двох (або більше) окремих об'єктів можуть бути з'єднані таким чином, що вони будуть описуватися за допомогою комбінованого квантового стану, а не як індивідуальний об'єкт. Це називається заплутаністю і означає, що вимірювання на один об'єкт впливає і на інший. Якщо сплутана пара об'єктів є спільною між двома учасниками, то перехоплення будь-якого об'єкта змінює систему в цілому, розкриваючи присутність третіх осіб (і кількість інформації, яку вони отримали).

1.3 Фізична реалізація системи квантової криптографії

Розглянемо схему фізичної реалізації квантової криптографії [5] (рис. 1.2.)

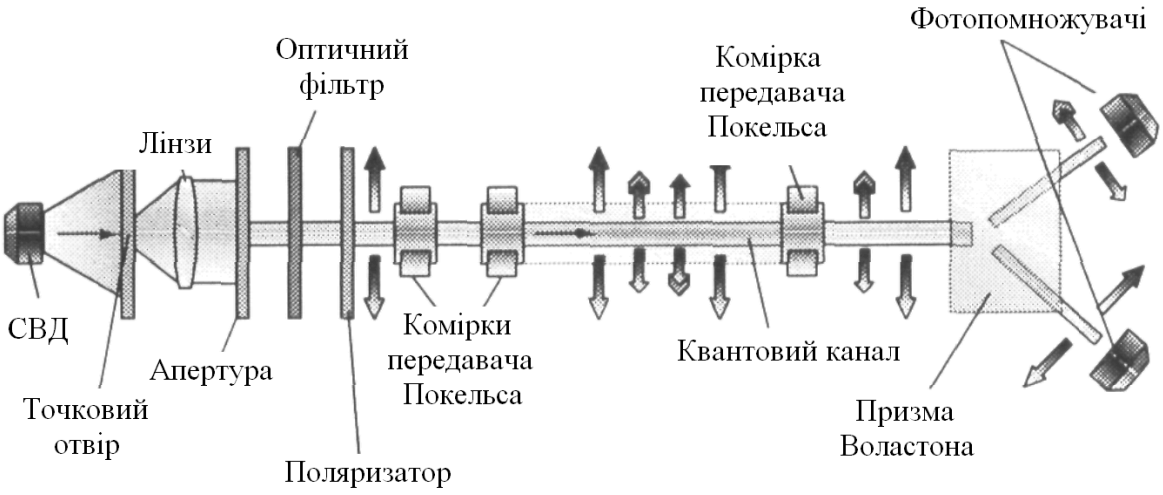

Рисунок 1.2 Схема фізичної реалізації квантової криптографії

Зліва знаходиться відправник, праворуч - одержувач. Для того, щоб передавач мав можливість імпульсно варіювати поляризацію квантового потоку, а приймач міг аналізувати імпульси поляризації, використовуються комірки Поккельса. Передавачем формується одне з чотирьох можливих станів поляризації. На комірки дані надходять у вигляді керуючих сигналів. Для організації каналу зв'язку зазвичай використовується волокно, а в якості джерела світла беруть лазер.

На стороні одержувача після комірки Поккельса розташована кальцитова призма, яка повинна розщеплювати пучок на дві складові, що вловлюються двома фотодетекторами (ФЕП), а ті, в свою чергу, вимірюють ортогональні складові поляризації. Спочатку необхідно вирішити проблему інтенсивності переданих імпульсів квантів, що виникає при їх формуванні. Якщо в імпульсі міститься 1000 квантів, існує ймовірність того, що 100 з них будуть відведені криптоаналітиків на свій приймач. Після чого, проводячи аналіз відкритих переговорів, він зможе отримати всі необхідні йому дані. З цього випливає, що ідеальний варіант, коли в імпульсі кількість квантів прагне до одного. Тоді будь-яка спроба перехопити частину квантів неминуче змінить стан всієї системи і

відповідно спровокує збільшення числа помилок у одержувача. У цій ситуації слід не розглядати прийняті дані, а заново повторити передачу. Однак, при спробах зробити канал більш надійним, чутливість приймача підвищується до максимуму, і перед фахівцями постає проблема «темнового» шуму. Це означає, що одержувач приймає сигнал, який не був відправлений адресантом. Щоб передача даних була надійною, логічні нулі і одиниці, з яких складається двійкове подання переданого повідомлення, представляються у вигляді не одного, а послідовності станів, що дозволяє виправляти одинарні і навіть кратні помилки.

Для подальшого збільшення відмовостійкості квантової криптосистеми використовується ефект Ейнштейна - Подільського - Розена, що виникає в тому випадку, якщо сферичним атомом були випроменені в протилежних напрямах два фотона. Початкова поляризація фотонів не визначена, але в силу симетрії їх поляризації завжди протилежні. Це визначає той факт, що поляризацію фотонів можна дізнатися тільки після вимірювання. Криптосхема на основі ефекту Ейнштейна - Подільського - Розена, що гарантує безпеку пересилання, була запропонована Екертом. Відправником генерується кілька фотонних пар, після чого один фотон з кожної пари він відкладає собі, а другий пересилає адресату. Тоді якщо ефективність реєстрації близько одиниці і на руках у відправника фотон з поляризацією «1», то у одержувача буде фотон з поляризацією «0» і навпаки. Тобто легальні користувачі завжди мають можливість отримати однакові псевдовипадковиі послідовності. Але на практиці виявляється, що ефективність реєстрації і вимірювання поляризації фотона дуже мала.

1.4 Практична реалізація системи квантової криптографії

У 1989 році Беннет і Брассар в Дослідницькому центрі IBM побудували першу працюючу квантово-криптографічний систему. Вона складалася з квантового каналу, що містить передавач Аліси на одному кінці і приймач Боба на іншому, розміщені на оптичній лаві довжиною близько метра в світлонепроникному півтораметровому кожусі розміром 0,5 × 0,5 м. Власне квантовий канал був вільний повітряний канал довжиною близько 32 см. Макет управлявся від персонального комп'ютера, який містив програмне уявлення користувачів Аліси і Боба, а також зловмисника. У тому ж році передача повідомлення за допомогою потоку фотонів через повітряне середовище на відстань 32 см з комп'ютера на комп'ютер завершилася успішно. Основна проблема при збільшенні відстані між приймачем і передавачем - збереження поляризації фотонів. На цьому заснована достовірність способу.

Створена за участю Женевського університету компанія GAP-Optique під керівництвом Ніколаса Гісіна поєднує теоретичні дослідження з практичною діяльністю. Першим результатом цих досліджень стала реалізація квантового каналу зв'язку за допомогою оптоволоконного кабелю довжиною 23 км, прокладеного по дну озера і з'єднує Женеву і Ніон. Тоді був згенерований секретний ключ, рівень помилок якого не перевищував 1,4%. Але все-таки величезним недоліком цієї схеми була надзвичайно мала швидкість передачі інформації. Пізніше фахівцям цієї фірми вдалося передати ключ на відстань 67 км з Женеви до Лозанни за допомогою майже промислового зразка апаратури. Але і цей рекорд був побитий корпорацією Mitsubishi Electric, яка передала квантовий ключ на відстань 87 км, правда, на швидкості в один байт в секунду.

Активні дослідження в галузі квантової криптографії ведуть IBM, GAP-Optique, Mitsubishi, Toshiba, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут, молода компанія MagiQ і холдинг QinetiQ, підтримуваний британським міністерством оборони. Зокрема, в національній лабораторії Лос-Аламоса була розроблена і почала широко експлуатуватися досвідчена лінія зв'язку, довжиною близько 48 кілометрів. Де на основі принципів квантової криптографії відбувається розподіл ключа, і швидкість розподілу може досягати кілька десятків кбіт / с.

У 2001 році Ендрю Шилдс і його колеги з TREL і Кембріджського університету створили діод, здатний випускати одиночні фотони. В основі нового світлодіода лежить «квантова точка» - мініатюрний шматочок напівпровідникового матеріалу діаметром 15 нм і товщиною 5 нм, який може при подачі на нього струму захоплювати лише по одній парі електронів і дірок. Це дало можливість передавати поляризовані фотони на більшу відстань. В ході експериментальної демонстрації вдалося передати зашифровані дані зі швидкістю 75 Кбіт / с - при тому, що більше половини фотонів втрачалося.

В Оксфордському університеті ставляться завдання підвищення швидкості передачі даних. Створюються квантово-криптографічні схеми, в яких використовуються квантові підсилювачі. Їх застосування сприяє подоланню обмеження швидкості в квантовому каналі і, як наслідок, розширення сфери практичного застосування подібних систем.

В Університеті Джона Хопкінса на квантовому каналі довжиною 1 км побудована обчислювальна мережа, в якій кожні 10 хвилин проводиться автоматичне підстроювання. В результаті цього, рівень помилки знижено до 0,5% при швидкості зв'язку 5 кбіт / с.

Міністерством оборони Великобританії підтримується дослідницька корпорація QinetiQ, яка є частиною колишнього британського агентства DERA (Defence Evaluation and Research Agency), яка спеціалізується на неядерних оборонних дослідженнях і активно удосконалює технологію квантового шифрування.

Дослідженнями в галузі квантової криптографії займається американська компанія Magiq Technologies з Нью-Йорка, що випустила прототип комерційної квантової кріптотехнології власної розробки. Основний продукт Magiq - засіб для розподілу ключа (quantum key distribution, QKD), яке названо Navajo (за назвою племені індіанців Навахо, мова яких під час Другої світової війни американці використовували для передачі секретних повідомлень, оскільки за межами США його ніхто не знав). Navajo здатний в реальному часі генерувати і поширювати ключі засобами квантових технологій і призначений для забезпечення захисту від внутрішніх і зовнішніх зловмисників.

У жовтні 2007 року на виборах в Швейцарії були повсюдно використані квантові мережі, починаючи виборчими дільницями і закінчуючи датацентрі ЦВК. Була використана техніка, яку ще в середині 90-х в Університеті Женеви розробив професор Ніколя жизень. Також одним з учасників створення такої системи була компанія Id Quantique.

У 2011 році в Токіо відбулася демонстрація проекту «Tokyo QKD Network», в ході якого розробляється квантове шифрування телекомунікаційних мереж. Була проведена пробна телеконференція на відстані в 45 км. Зв'язок в системі йде за звичайними оптоволоконними лініями. В майбутньому передбачається застосування для мобільного зв'язку.

1.5 Практична реалізація системи квантової криптографії

В теорії квантова комунікація ідеально безпечна. На практиці ж виявляється, що зараз існують різні лазівки, якими «квантові хакери» можуть скористатися, що було показано дослідницькими групами Хой-Квон Ло і Вадима Макарова [6].

Лазівки можуть виникнути і в джерелі, і в детекторі. Реальні джерела і детектори рідко повністю відповідають своїм ідеальним теоретичним прототипам, використовуваним при доказі безпеки квантової комунікації. Наприклад, в одному з видів детекторів gated detector ефективність детекції змінюється за допомогою зміщення напруги і, таким чином, залежить від часу. В ідеальній ситуації існує два детектора: один для нульового біта, а інший для одиниці, і важливо упевнитися в тому, що ефективність детектування в обох детекторів абсолютно однакова.

Група Хой-Квон Ло показала, що маленьке розбіжність у часі зміщення напруги може спричинити за собою значне неспівпадання ефективності детектування. Такий принцип атаки за допомогою тимчасового зсуву. І це тільки один з прикладів. Лазівки в системах КРК можуть бути різноманітними.

1.6 Висновки з розділу 1

Квантова криптографія - спосіб захисту комунікацій, який заснований на основних принципах квантової фізики. На відміну від традиційної криптографії, що використовує математичні методи для того, шоб забезпечити безпеку інформації, квантова криптографія заснована на

фізиці, де інформація переноситься за допомогою об'єктів квантової механіки.

Технологія квантової криптографії спирається на принципову невизначеність поведінки квантової системи, яка виражена в принципі невизначеності Гейзенберга, тобто неможливо одночасно отримати координати і імпульс частинки тавиміряти один параметр фотона, не спотворивши інший.

Використовуючи закони квантової фізики можна створити таку систему зв'язку, яка зможе заввжди виявляти підслуховування інформації.

РОЗДІЛ 2. СПОСОБИ ТА ПРИСТРОЇ ГЕНЕРАЦІЇ І ПЕРЕДАЧІ ОДИНОЧНИХ ФОТОНІВ

2.1 Фотонні детектори

У детекторах, які використовуються у фізиці атомного ядра і частинок, нерідко необхідна реєстрація фотонів невеликих енергій (у видимому або біля нього діапазоні довжин хвиль). Це, наприклад, черенковські детектори, сцинтилятори, детектори перехідного випромінювання [7]. Існують різні типи фотонних детекторів:

1. Вакуумні фотонні детектори [8]:
    а) Фотоелектронний помножувач;
    б) Мікроканальні пластини;
2. Газові фотонні детектори [9];
3. Твердотільні фотонні детектори [10]:
    а) PIN-фотодіоди;
    б) Лавинні фотодіоди;
    в) Мікропіксельні лавинні фотодіоди;
4. Гібридні фотонні детектори [11];

2.1.1 Вакуумні фотонні детектори

2.1.1.1 Фотоелектронний помножувач (ФЕП)

Перший фотоелектронний помножувач був створений на початку 1930-х років Л. Кубецким (так звана трубка Кубецким). Для фокусування і прискорення електронів в ній використовувалося магнітне поле. В сучасних ФЕП для цих цілей в основному використовується електростатичне поле. Вперше, в кінці 1930-х, фокусування і прискорення електронів застосував Я. Рейчман. З тих пір ФЕП широко використовуються у фізичному експерименті. У ФЕП фотони

потрапляють на фотокатод з якого за рахунок фотоефекту вибивають електрони. Електрони потім потрапляють на систему дінодов, де їх потік збільшується за рахунок вторинної електронної емісії. Струм в ланцюзі анода значно перевищує струм від фотокатода (фотострум). Коефіцієнт посилення в деяких ФЕП досягає 1011 (рис 2.1).

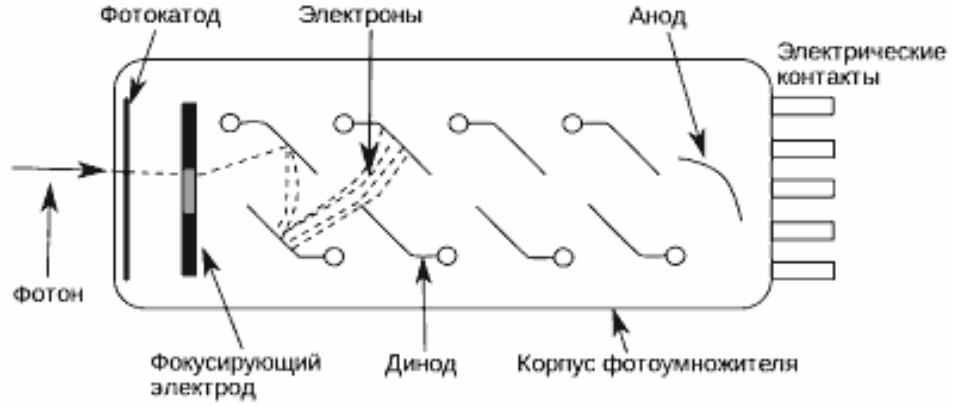

Рисунок 2.1 Фотоелектронний помножувач

Тривалість переднього фронту токового імпульсу на аноді зазвичай кілька наносекунд. На часовий простір ФЕП впливає також розкид часу прольоту електронів в дінодной системі. Для поліпшення тимчасових характеристик використовуються конструкції з невеликим шляхом прольоту електронів. "Звичайні" ФЕП чутливі навіть до відносно невеликим магнітних полів. Магнітне поле погіршують фокусування і в результаті зменшують коефіцієнт посилення. Для зменшення впливу магнітного поля використовують світлоланцюги, щоб направити світловий сигнал в область, де немає магнітного поля, або магнітні екрани. У світлоланцюгів світловий сигнал послаблюється і погіршуються тимчасові характеристики. Магнітні екрани можуть помітно підвищити вартість і, крім того, в магнітному екрані

відбуваються неконтрольовані втрати енергії частинками, які в сучасних детекторних комплексах повинні реєструватися в інших системах.

Для роботи в магнітних полях були сконструйовані ФЕП з сітковими дінодами. У таких ФЕП фотоелектрон, потрапивши на дінод, вибиває вторинні електрони, які спочатку летять вгору, а потім повертаються і проходять через отвір сіткового дінода, потрапляючи на наступний дінод. Відстань між фотокатодом і першим дінодамі кілька мм, а між дінодамі ~ 1 мм. Через невелику відстань між катодом і анодом тимчасові характеристики таких ФЕП хороші, чутливість до магнітних полів відносно невелика. Вони задовільно працюють до ~ 1.5 Тс. Коефіцієнт посилення ФЕП з сітковими дінодами ~ 106 (рис. 2.2).

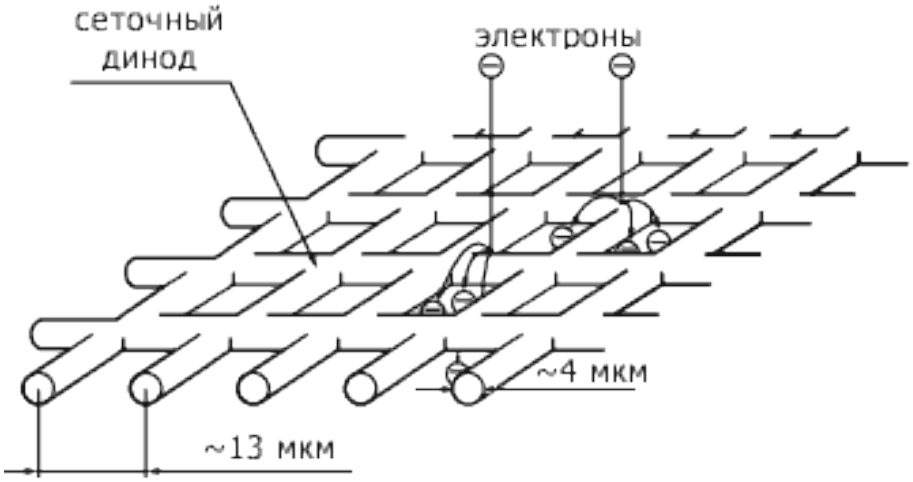

Рисунок 2.2 Фотоелектронний помножувач з сітковими дінодами

ФЕП з сітковими дінодами дозволяють отримувати двовимірну інформацію, якщо, наприклад, використовувати сенкціонований анод. Пластикові сцинтилятори з ФЕП з сітковими дінодами зокрема використовувалися в системі часу прольоту установки BELLE. Тимчасовий дозвіл системи склало 100 пс, що дозволило розрізняти π / K аж до енергії 1.2 ГеВ. Аерогельний черенковський детектор, в якому

також використовувалися ФЕП з сітковими дінодамі дозволив збільшити діапазон сепарації π / K аж до 3.5 ГеВ.

2.1.1.2 Мікроканальні пластини

Мікроканальні пластини (МКП) мають малі габарити, хороші тимчасове і просторове дозвіл, великий коефіцієнт посилення, меншу в порівнянні зі звичайними ФЕУ чутливість до магнітних полів. Так у мікроканальних пластин шевронного типу H8500 / H9500 посилення 106, тимчасовий дозвіл (FWHM) при рахунку окремих фотонів менше 30 пс. Вони не чутливі до аксіальним магнітним полях до 1.8 Тс (рис. 2.3).

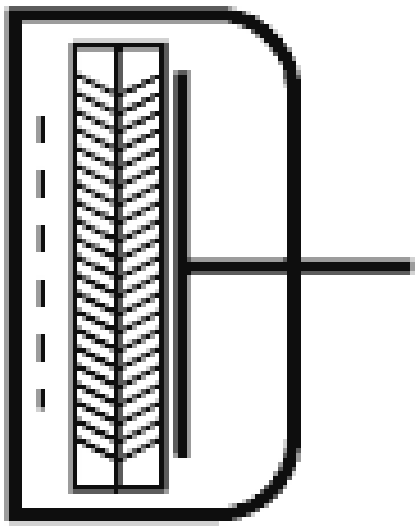

Рисунок 2.3 Мікроканальні пластини

2.1.2 Газові фотонні детектори

У газових фотонних детекторах фотоелектрон за рахунок ударної іонізації народжує в газоподібному середовищі лавину вторинних електронів. В принципі процеси множення і збору зарядів ідентичні

процесам, що відбувається в багатодротяних пропорційних камерах. Площа газових фотонних детекторів може бути великою з субміліметровою точністю локалізації. Тимчасовий дозвіл газових детекторів не гірше 1 нс. Вони можуть працювати в сильних магнітних полях.

Газові детектори чутливі до одиночних фотонів в спектральному діапазоні від ультрафіолетового до видимого світла. Вони мають високий коефіцієнт посилення (близько 105). Газові фотонні детектори часто використовуються для детектування черенковского випромінювання в RICH-детекторах. Так газові фотопомножувачі були використані в RICH-детекторі в детекторному комплексі ALICE.

Останнім часом великого поширення набули газові фотодетектори на основі ГЕУ. За принципом роботи ГФД на основі ГЕУ можна поділити на детектори з напівпрозорим і непрозорим фотокатодом (рис. 2.4). У першому варіанті катод фотодетектора є вхідний вікно, на яке нанесений напівпрозорий фоточутливий шар. Фотоелектрони, народжені на фотокатоде, рухаються в дрейфовому проміжку уздовж силових ліній і фокусуються в отвори ГЕУ. в яких під дією сильного електричного поля розвиваються електронні лавини. Таким чином, кожен отвір ГЕУ є незалежний пропорційний лічильник. Помітна частина електронів лавини виходить з отвору в газовий проміжок для посилення в подальшому усилительном каскаді. У варіанті з непрозорим фотокатодом вхідний вікно прозоро, катод виконується у вигляді сітки, а плівковий фотокатод наноситься прямо на електрод першого ГЕУ.

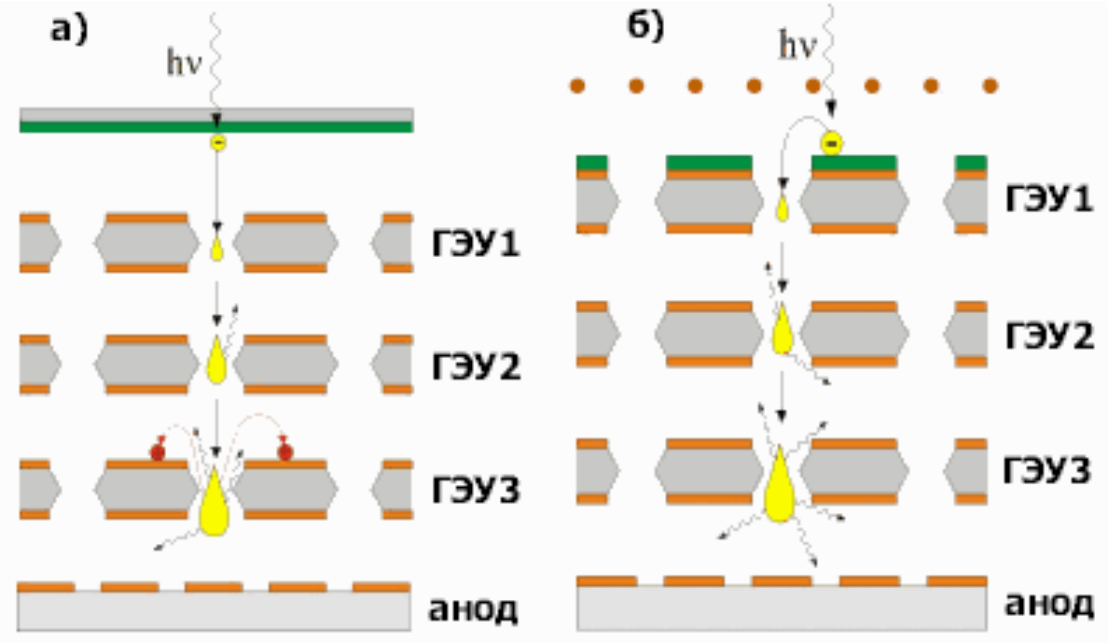

Рисунок 2.4 Газові фотонні детектори з: а) напівпрозорим фотокатодом; б) непрозорим фотокатодом

ГФД з непрозорим вхідним вікном були використані в RICH детекторі детекторного комплексу PHENIX. Важливим елементом класичного черенковського детектора кільцевого зображення (RICH детектора) є фокусуюче дзеркало, розташоване в кінці радіатора. Через геометричні обмеження на PHENIXe дзеркало було неможливо використовувати. Було вирішено замінити дзеркало фотонними детекторами, розташувавши його на шляху всіх частинок, які виникають під час зіткнень. У черенковський детекторі використовується газовий радіатор CF4. Цей детекторний модуль (HBD - Hadron Blind Detector) повинен був бути чутливий до ультрафіолету і "сліпий" до всіх адронів, що летять через нього. У ГЕУ як і в радіаторі також був використаний CF4.

Конструкція HBD виконана таким чином. На поверхню ГЕУ був напилюв тонкий шар CsI, який перетворив його у високоефективний фотокатод. (CsI має високу ефективність до ультрафіолету і в середовищі

CF4.) Електричне поле, необхідне для посилення в отворі ГЕМ було досить для того, щоб витягнути електрони з будь-якої точки поверхні ГЕМ і направити їх найближчим отвір. При цьому електрони, що з'являються в газі над фотокатодом в результаті іонізації, виробленої зарядженими частинками, віддалялися завдяки зворотному зміщення реалізованому між вхідним вікном (алюмінізірованний майлар товщиною 0.22 мм) і першим каскадом ГЕУ. Таким чином HBD, виправдовуючи свою назву, стає нечутливим до іонізуючого випромінювання.

2.1.3 Твердотільні фотонні детектори

У порівнянні з вакуумними і газовими фотонними детекторами твердотільні пристрої більш компактні, легкі, міцні, стійкі до магнітних полів, а часто і дешевші. З ними легко організувати пікселізацію, легко інтегрувати в великі системи Вони можуть працювати при низьких електричних потенціалах. Кремнієві фотодіоди широко використовуються у фізиці високих енергій в якості детекторів частинок, а також і в великій кількості додатків в якості детекторів фотонів. У своїй простій формі це діод з p-n переходом на яке подано зворотне зміщення. Фотони з енергіями більшими ширини забороненої зони вибувають з валентної зони в зону провідності електрони, залишаючи там дірки. Потім під дією прикладеного зворотного зсуву електрони і дірки рухаються до p і n контактів відповідно.

2.1.3.1 PIN-фотодіоди

Для збільшення збідненого (чутливої до появи іонізуючих частинок) області, тобто області, де немає вільних зарядів

використовують високолеговані напівпровідники. Такі діоди називаються pin-діодами. У них створюється n + -p-p +-перехід (+ означає сильне легування). Внутрішня частина напівпровідника (p-область) затиснута між двома сильно легованими n + і p + областями, де відбувається основна зміна потенціалу та електричне поле виникає майже по всій глибині зразка. Зворотне зміщення дозволяє збільшити товщину збідненої області. Так як в pin-діодах немає внутрішнього посилення, мінімальний детектований сигнал повинен містити не менше кількох сотень фотонів. Крім того, доводиться використовувати зарядо чутливі попередні, які вносять додаткові шуми. PIN-фотодіоди використовувалися в багатьох експериментах фізики високих енергій для зчитування сигналів від сцинтиляторів (CLEO, BELLE, BABAR, GLAST). Так PIN-фотодіоди використовувалися в електромагнітному калориметрі детекторного комплексу CLEO для реєстрації світла від кристалів CsI (Tl).

2.1.3.2 Лавинні фотодіоди

Збільшення чутливості твердотільних фотонних детекторів пов'язано з використанням лавинних фотодіодів (ЛФД). Лавинне множення досягається за рахунок збільшення напруги ЄСМ до величини, близької до пробійної. При цьому на p-n переході встановлюється дуже сильне електричне поле (E> 105 В / см). Під дією поля вільний носій заряду (електрон або дірка) набуває енергію, достатню для іонізації нейтрального атома і звільнення ще однієї електронно-діркової пари, причому такий процес може повторюватися неодноразово. Для розмноження дірок необхідна більша напруженість електричного поля, ніж для розмноження електронів. На самому p-n переході при подачі

відповідної напруги можливе досягнення стабільного множення електронів при тому, що лавинного множення дірок не відбувається. Як правило, максимальне посилення, яке можливо досягти в такій структурі, коливається від 10 до 200.

Розроблені і використовуються різні типи лавинних фотодіодів. Так в електромагнітному калориметрі ECAL детекторного комплексу CMS використовуються ЛФД чутливі до короткохвильової частини спектра (рис. 2.5). Фотони блакитного світла поглинаються в перших декількох мікронах кремнію, а ультрафіолетового - в частках мікрона, тому для реєстрації короткохвильової частини спектра ЛФД повинен мати в якості чутливої частини поверховий шар кремнію. Для цього спеціально створюється додатковий шар, в якому спочатку утворюється фотоелектрон, який йде вглиб до зони p-n переходу і потрапляє в зону лавинного множення

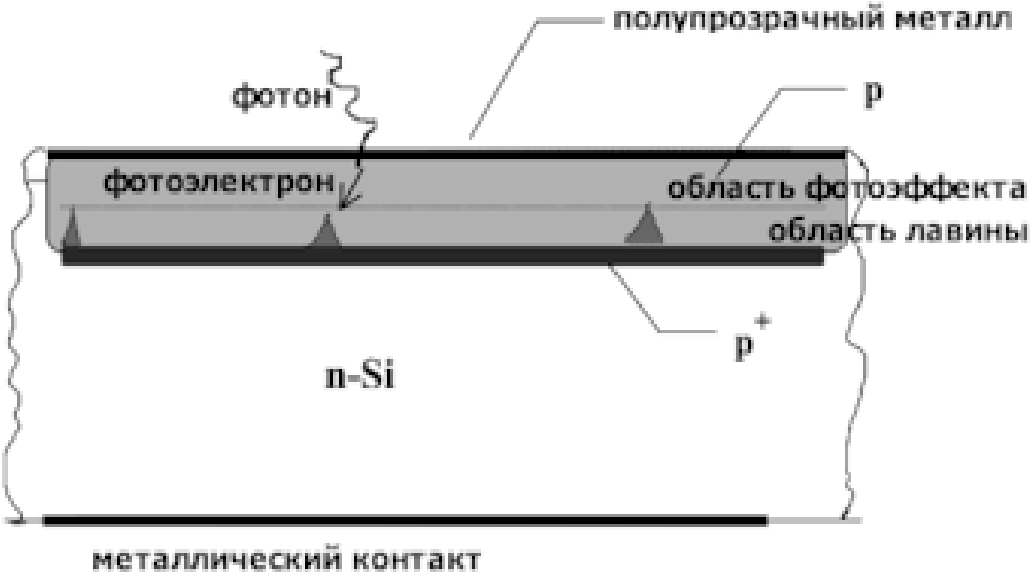

Рисунок 2.5 Лавинний фотодіод

Збільшити коефіцієнт множення звичайного лавинного фотодіода до 104 не вдається. При збільшенні зворотного зсуву в створенні лавини крім електронів починають брати участь і дірки, що призводить до

необмеженого росту лавини і, як наслідок, пробою p-n переходу. Поява лавинних фотодіодів з негативним зворотним зв'язком, яка гасить лавинний процес, дозволило створити лавинний фотодіод, що працює в так званому гейгеровському режимі. Напруга зворотного зсуву в такому діоді на кілька вольт вище напруги пробою. Такий фотодіод має високий коефіцієнт посилення (105-107). Однак при цьому мертвий час приладу стає великим (близько мікросекунд). Крім того, як і газорозрядних лічильниках Гейгера-Мюллера, такий детектор здатний реєструвати лише факт проходження іонізуючих частинок (в даному випадку фотоелектронів), але не їх кількість. Тобто він не може бути використаний в якості детектора реєструючого інтенсивність падаючого випромінювання. Розробка в кінці 90-х років кремнієвих мікропіксельних лавинних фотодіодів (MAPD або SiPM) вирішила цю проблему.

2.1.3.3 Мікропіксельні лавинні фотодіоди

У лавинних фотодіодах з піксельної структурою кожен піксель являє собою лічильник одиничних фотонів, але весь MAPD є аналоговий детектор, так як вихідний сигнал MAPD є сума сигналів з усіх пікселів, що спрацювали при поглинанні ними фотонів. Такі мікропіксельні лавинні фотодіоди здатні реєструвати малі інтенсивності світла (на рівні кількох десятків і навіть одиничних фотонів), при цьому володіючи високим коефіцієнтом внутрішнього посилення ~ 106 і навіть до ~ 108 (рис. 2.6).

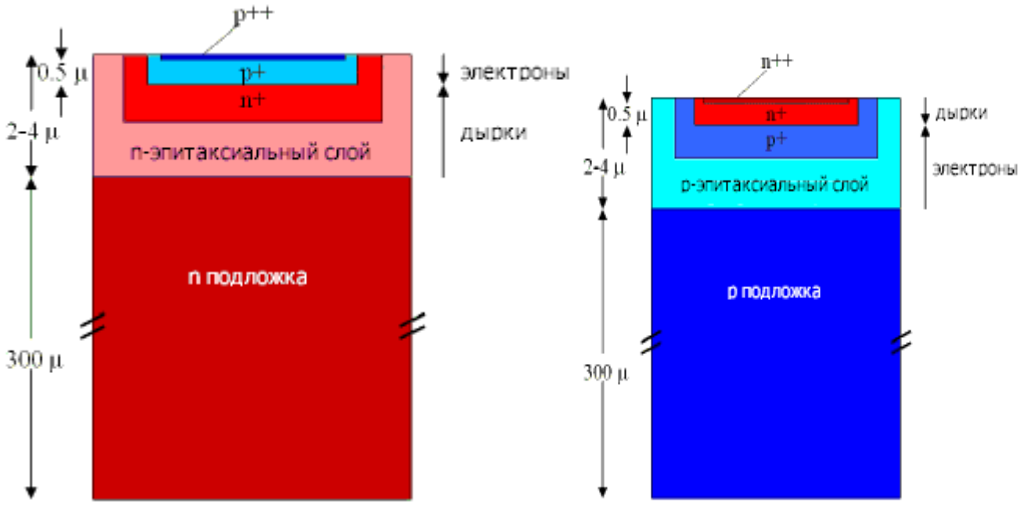

Рисунок 2.6 Спрощена схема одного пікселя MAPD, а) так звана p (n) - структура (в основному чутлива до синьої частини спектра, б) n (p) - структура (в основному чутлива до червоної частини спектра)

Лавинні фотодіоди з піксельної структурою мають малий розкид коефіцієнта посилення від пікселя до пікселя (близько 10%) і, як наслідок, низькі шуми; невисоку чутливість коефіцієнта посилення до зміни температури і напруги живлення; ефективні при реєстрації видимого світла на рівні вакуумних ФЕП; дозволяють реєстрацію наносекундних спалахів світла без спотворення форми детектованого імпульсу; можуть працювати, як в режимі рахунку імпульсів, так і в спектрометричному режимі; мають гарний тимчасовий дозвіл (десятки пікосекунд); не вимагають високої напруги живлення; нечутливі до магнітного поля; компактні.

2.1.4.3 Гібридні фотонні детектори

Гібридні фотонні детектори поєднують чутливість ФЕП з відмінним просторовим і енергетичним розрізненням кремнієвих детекторів. На рис. 2.7 показаний принцип дії гібридного детектора. Вилітає з фотокатода фотоелектрон прискорюється в електричному полі 12-20 кВ і потрапляє на сегментований анод - кремнієвий сенсор (лавинний діод). У кремнієвому сенсорі, поблизу його поверхні відбувається утворення електронно-доручених пар. Практично вся кінетична енергія фотоелектронів витрачається на створення електронно-діркових пар, тобто в залежності від прискорювальної напруги утворюється ~ 3000-5000 пар. Якщо в якості кремнієвого сенсора використовується лавинний діод, в ньому відбувається додаткове посилення в ~ 100 разів. В результаті коефіцієнт посилення гібридного фотонного детектора може досягти ~ 105, часовий простір десятки пс, в той час як у кращих ФЕП ~ 200 пс.

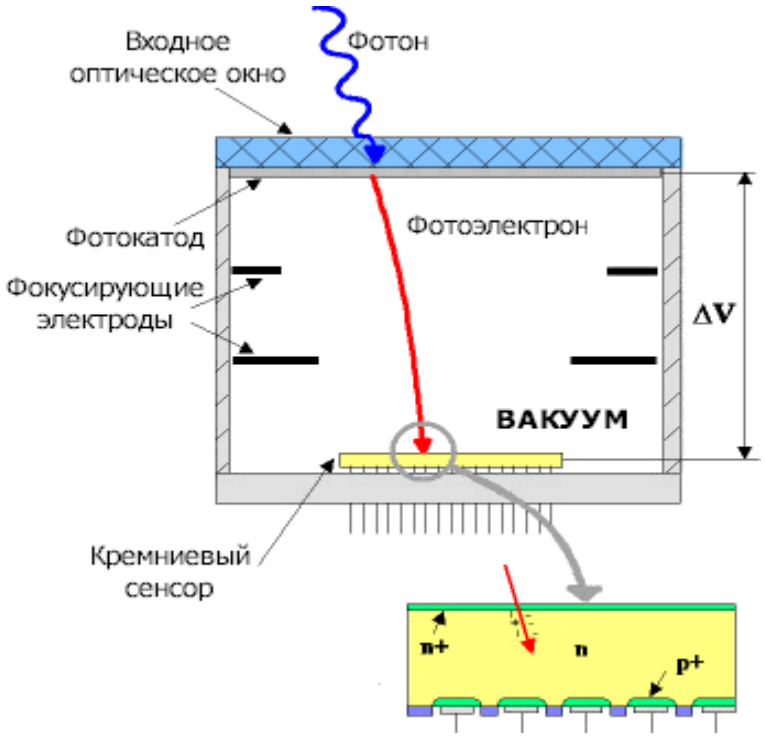

Рисунок 2.7 Принцип дії гібридного детектора

Гібридні фотонні детектори зокрема використовуються в адронному калориметр HCAL на CMS і в RICH-детекторі на LHCb. Кремнієвий сенсор являє з себе матрицю 32 × 32 пікселя, кожен має розміри 500 × 500 мкм2. На рис. 2.8 показаний кластер з трьох фотонних детекторів, на рис. 2.9 - накопичений набір даних черенковського кільця від негативних піонов з імпульсами 120 ГеВ / с проходячих через газовий радіатор C4F10. Коло - результ фіттірованія.

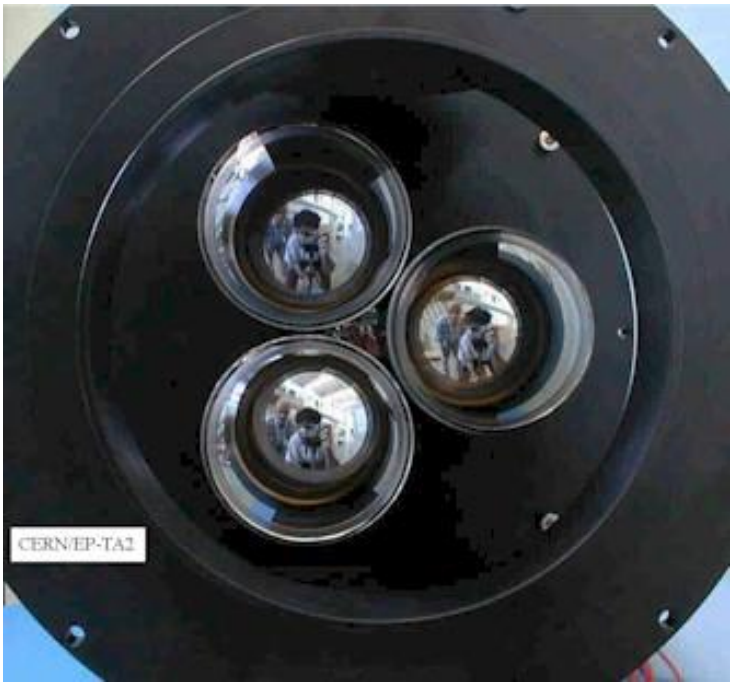

Рисунок 2.8 Кластер з трьох фотонних детекторів

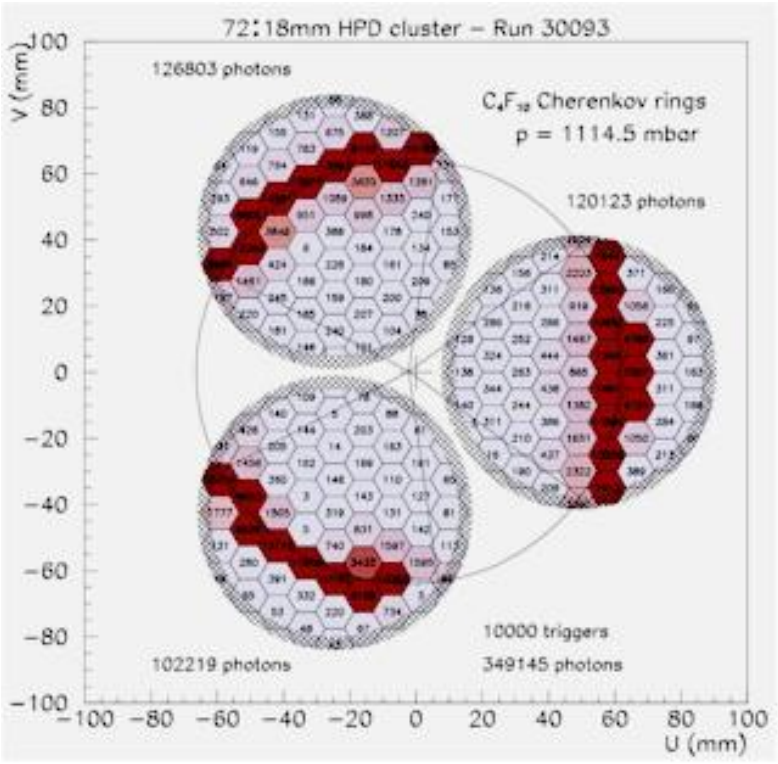

Рисунок 2.9 Накопичений набір даних черенковського кільця від негативних піонов з імпульсами 120 ГеВ / с проходячих через газовий радіатор C4F10

2.2 Кодування квантових станів

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

2.2.1 Поляризаційне кодування

Історично першою реалізацією системи квантового розподілу ключів була поляризационная схема кодування, що працює по протоколу BB84. Схема квантової криптографічного установки з поляризаційним кодуванням по протоколу BB84 з чотирма станами показана на рис. 2.10.

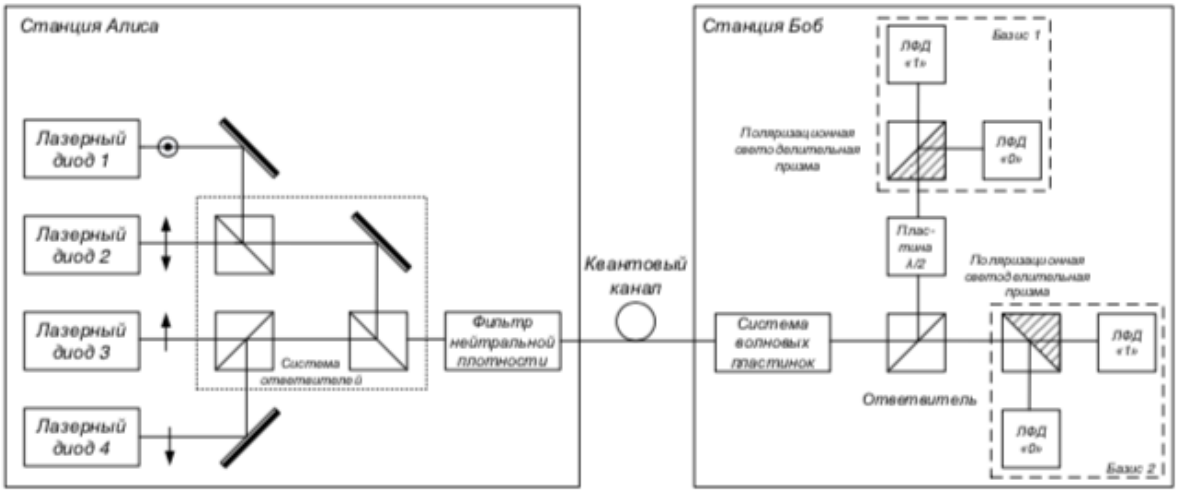

Рисунок 2.10 Схема квантової криптографічного установки з поляризаційним кодуванням

Станція Аліса, складається з четирѐх лазерних діодів, які випромінюють короткі імпульси світла тривалістю 1 нс. Поляризації фотонів становить -45^{o}, 0^{o}, $+45^{o}$ і 90^{o}. Для передачі одного біта активізується один з лазерних діодів. Потім імпульси послаблюються набором фільтрів для забезпечення умови однофотонності. Середня кількість фотонів в імпульсі вибирається менше одного $n < 1$. Після цього фотон випромінюється у напрямку до станції Боб. Важливою умовою правильного детектування інформації станцією Боб є збереження поляризації фотонів в волокні.

. Імпульси, досягаючи станції Боб, проходять через набір хвильових пластинок, використовуваних для відновлення вихідних поляризаційних станів шляхом компенсації змін, внесѐнних волокном. Потім імпульси досягають світлодільника, що здійснює напрямок фотона до лінійного або діагонального аналізатору. Передані фотони аналізуються в ортогональному базисі за допомогою поляризаційної світлороздільної призми і двох лавинних фотодіодів (ЛФД). Поляризація фотонів, які пройшли через хвильові платівки повертається на 45^{o} (з -45^{o} до 0^{o}). У той же час, інші фотони аналізуються другою системою «поляризаційна світлодільникова призма - ЛФД» в діагональному базисі.

Нехай є фотон, поляризований під кутом $+45^{o}$. Після того, як він залишає станцію Аліса, його поляризація випадковим чином перетворюється в оптичному волокні. В станції Боб система з хвильових пластинок повинна бути встановлена таким чином, щоб компенсувати зміну поляризації. Якщо фотон пройде на вихід світлодільника, відповідного лінійному базису поляризації, у нього будуть рівні ймовірності потрапити в один з фотодетекторів, що призведе до випадкового результату. З іншого боку, якщо буде обраний діагональний

базис, його поляризація буде повѐрнута на 45^{o}. Тоді світлодільник відобразить його з одиничною ймовірністю, що призведе до визначеного результату.

Замість використання чьотирьох лазерів станцією Аліса і двох поляризаційних світлодільникових призм станцією Боб, можливо також застосування активних поляризаційних модуляторів, таких як комірки Поккельса. Для кожного імпульсу світла модулятор активується за випадковим законом, приводячи поляризацію в один з чьотирьох станів, в той час як приймаюча сторона в випадковому порядку обертає поляризацію половини прийнятих імпульсів на 45^{o}.

Зауважимо, що поляризаційна модова дисперсія (ПМД) може привести до зміни поляризації фотонів, за умови, що час затримки між поляризаційними модами більше часу когерентності. Це вносить обмеження на типи лазерів, що використовуються станцією Аліса.

Антон Мюллер і його колеги з Женевського університету використовували подібну систему для проведення експериментів в галузі квантової криптографії [12]. Вони передавали ключ на відстань 1100 м, використовуючи фотони з довжиною хвилі 800 нм. Для збільшення максимальної дистанції передачі вони повторили експеримент з фотонами на довжині хвилі випромінювання 1300 нм [13] і передавали ключ на 23 км. Особливістю даного експерименту було використання в якості квантового каналу, який зв'язує станції Аліса з Боб, стандартного телекомунікаційного оптичного кабелю, який використовувався компанією Swisscom для проведення телефонних переговорів.

Результати цих експериментів показали, що зміни поляризації, що вносяться оптичним волокном, були нестабільні в часі. Незважаючи на те, що вони стабілізувалися на деякий час (порядку декількох хвилин), в випадковий момент поляризація різко змінювалася. Це означає, що

реальна квантова криптографічна система вимагає створення механізму активної компенсації поляризаційних змін. Незважаючи на наявність принципової можливості створення такого механізму, очевидно, що його практична реалізація дуже ускладнена.

Джеймс Френсон розробив систему автоматичного підстроювання поляризації, але не став займатися еѐ подальшим вдосконаленням [14]. Існують і інші способи автоматичного контролю поляризації, розроблені для когерентних волоконно-оптичних систем зв'язку. Цікаво те, що заміна стандартного волокна на волокно, що зберігає поляризацію, не вирішує проблему, так як такі волокна зберігають тільки два ортогональних стану поляризації, а в системах квантової криптографії використовуються чотири попарно неортогональних стану.

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

2.2.2 Фазове кодування

Нестабільність поляризації в системах з поляризаційним кодуванням сильно ускладнює їх створення. У зв'язку з цим був розроблений інший тип квантових криптографічних систем. Ідея кодування біт фазою фотонів була вперше згадана Беннеттом, коли він описував протокол з використанням двох станів [15]. Отримання квантових станів і подальший їх аналіз виробляються інтерферометрами, які можуть бути реалізовані одномодовими компонентами волоконної оптики. На рис. 2.11 показана волоконооптичну реалізація інтерферометра Маха-Цендера.

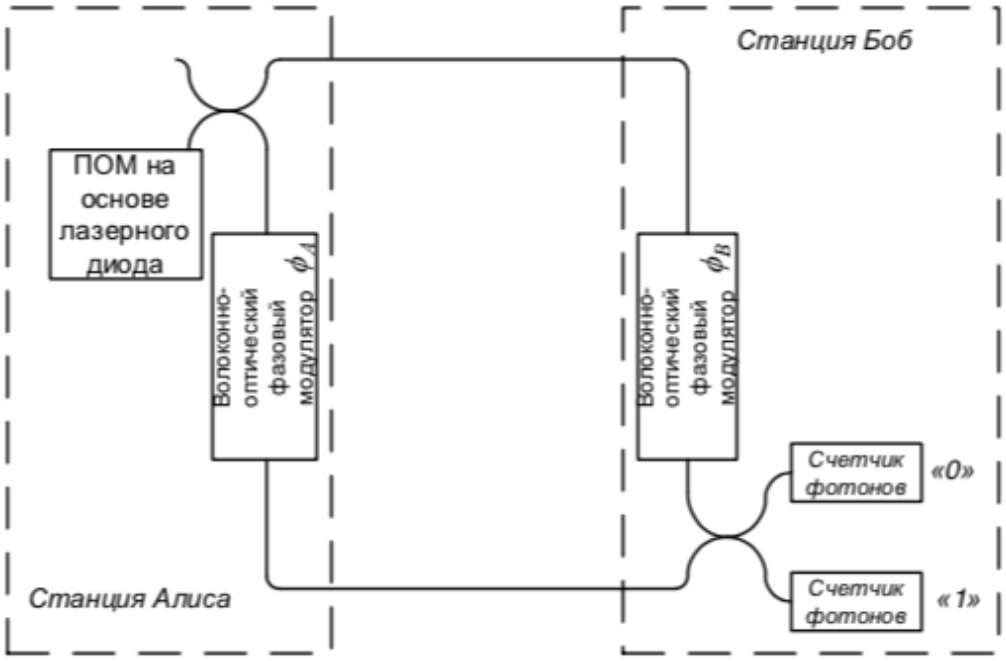

Рисунок 2.10 Інтерферометр Маха-Цендера

Інтерферометр виконаний з двох волоконно-оптичних разветвителей, соединѐнних між собою, і двох фазових модуляторів - по одному в кожному плечі. У таку систему можна ввести оптичне випромінювання, використовуючи класичний безперервний джерело, і спостерігати потужність оптичного випромінювання на виходах. У разі якщо довжина когерентності світла лазера більше різниці довжин плечей інтерферометра, можна отримати інтерференційну картину. Беручи до уваги фазовий зсув $\pi/2$, що відбувається на розгалужувачі, дії фазових модуляторів (φ_A і φ_B) і різницю довжин плечей (ΔL), потужність оптичного випромінювання на виході "0" визначається наступною формулою:

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

де k - хвильове число, а P - потужність джерела.

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

Описана вище поведінка інтерферометра справедлива для класичного оптичного випромінювання. Проте, інтерферометр працює аналогічно для випадку одиночних фотонів. Імовірність зареєструвати фотон на одному з виходів буде змінюватися зі зміною фази. Незважаючи на те, що фотон веде себе як частинка при реєстрації, він поширюється через інтерферометр як хвиля. Інтерферометр Маха-Цендера - це волоконно-оптичний варіант експерименту Юнга зі щілинами, в якому плечі інтерферометра аналогічні апертурою. Такий інтерферометр разом з однофотонним джерелом і з ЛФД може бути використаний в квантовій криптографії. Станція Аліса в такому випадку буде містити джерело, перший розгалужувач і перший фазовий модулятор, а станція Боб складатиметься з другого модулятора, розгалуджувача і ЛФД.

Розглянемо застосування до такої схеми протоколу BB84 з чотирма станами. Аліса може здійснювати один з четирѐх фазових зсувів $(0, \pi/2, \pi, 3\pi/2)$.Вона зіставляє значенням біта "0" - 0 та $\pi/2$, а значенням біта «1» - π і $3\pi/2$. У свою чергу, станція Боб робить вибір базису, в випадковому порядку зрушуючи фазу на 0 або $\pi/2$, и прирівнює біту, що

прийшов на фотодетектор, підключений до виходу "0" значення «0», а біту, що прийшов на фотодетектор, підключений до виходу "1" значення біта «1». Коли різниці фаз рівні 0 або π, то в станціях Аліса і Боб використовуються сумісні базиси і виходять цілком визначені результати. В таких випадках станція Аліса може визначити, в якій із фотодетекторов станції Боб попаде фотон, і, отже, вона може визначити значення біта. Зі свого боку, станція Боб може визначити, яка фаза була обрана станцією Аліса при передачі кожного фотона. У разі, коли різниця фаз приймає значення π/2 або 3π/2, сторони використовують несумісні базиси, і фотон випадковим чином потрапляє на один з фотодетекторов станції Боб. Всі можливі комбінації фазових станів наведені в таблиці 2.1.

Таблиця 2.1 Протокол BB84 з чотирма станами для фазового кодування.

Станция Алиса		Станция Боб		
Значение бита	φ_A	φ_B	$\varphi_A-\varphi_B$	Значение бита
0	0	0	0	0
0	0	π/2	3π/2	?
1	π	0	π	1
1	π	π/2	π/2	?
0	π/2	0	π/2	?
0	π/2	π/2	0	0
1	3π/2	0	3π/2	?
1	3π/2	π/2	π	1

Зауважимо, що для системи вкрай важливо зберігати стабільну різницю довжин плечей інтерферометра протягом сеансу передачі ключа. Ця різниця не повинна змінюватися більш ніж на частку довжини хвилі фотонів. Зміни довжини одного з плечей призведе до дрейфу фази і виразиться в помилках в переданому ключі. Незважаючи на те, що дана схема чудово працює в лабораторних умовах, на практиці не представляється можливим збереження довжин плечей в разі, коли користувачі відокремлені один від одного більш ніж на кілька метрів. Беннетт показав, як обійти цю проблему [28]. Він запропонував використовувати два незбалансованих інтерферометра Маха-Цендера, з'єднаних послідовно оптичним волокном.

Однак в комерційних реалізаціях систем квантового розподілу ключів застосовується ще більш складна і досконала схема кодування фазових станів. Дана схема являє собою розподілений інтерферометр з автоматичною компенсацією поляризаційних спотворень [16]. Типова структура реалізації комерційних систем представлена на малюнках рис. 2.13 – 2.14.

Рисунок 2.11 Схема приймально-передавального модуля системи Id 3000 Clavis

Рисунок 2.12 Схема кодуючого модуля системи Id 3000 Clavis

Як можна помітити, в одному блоці поєднані функції передавача і приймача. Однак функція кодування квантового стану фази фотона покладено на фазовий модулятор в другому блоці. Таким чином, схема зображена на рис. 2.12 є схемою пристрою Аліса в класичній інтерпретації протоколу BB84. За аналогічною схемою побудовано обладнання MagiQ QPN, вироблене компанією MagiQ Technologies. Різниця становить лише реалізація підсистеми синхронізації.

2.2.3 Часове кодуванням

Принципи побудови систем квантової криптографії використовуючих неортогональність часових інтервалів запропонував Сергій Молотков з інституту фізики твердого тіла РАН [17]. Для кодування «0» і «1» використовується стан лише з однієї просторово часовою формою, але зрушеною на різні часові інтервали в кожній посилці. За рахунок цього і досягається неортогональність.

Дана ідея дозволяє спростити волоконно-оптичну частину системи квантової криптографії і повністю відмовитися від застосування інтерферометрів. Запропонована схема дозволяє реалізувати більшість відомих протоколів квантової криптографії [18].

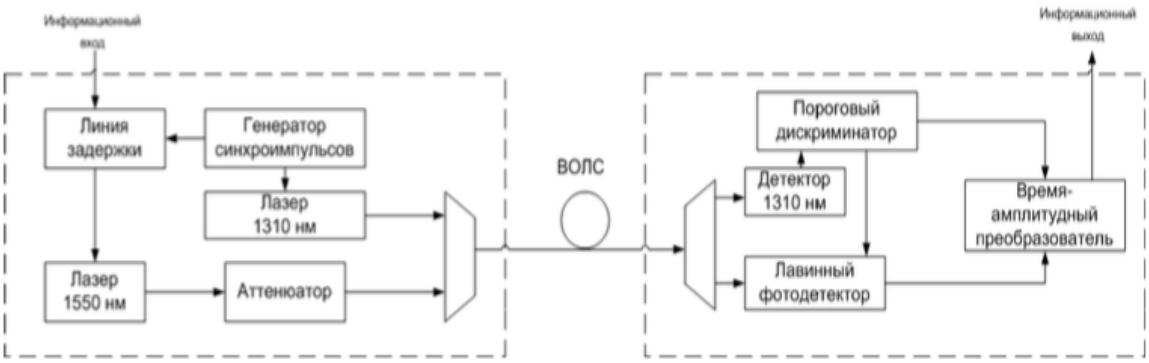

Рисунок 2.13 Схема оптоволоконної системи квантової криптографії на часових зсувах без інтерферометрів

В якості однофотонного стану використовується стан, зрушене щодо синхроімпульса, в кожній посилці на певну величину. Синхроімпульсом є короткий оптичний імпульс, що випромінюється лазером з довжиною хвилі 1310 нм. У реалізації використовуються два базису {+ (1), ×(1)} і {+ (2), ×(2)}. Всередині першого базису в кожному підбазисі {+ (1) і ×(1)}, стани для 0 - | 0_1 (+) і 1 - | 1_1 (+), відповідно, в підбазисі 0 - | 0_1 (x) і 1 - | 1_1 (x) - ортогональні. Між підбазисами +(1) і ×(1) стани попарно неортогональні, що досягається відповідними часовими зсувами. Аналогічно і для базису {+ (2), ×(2)}.

Стани в базисах відображені на малюнку 13. Дана реалізація еквівалентна протоколу BB84.

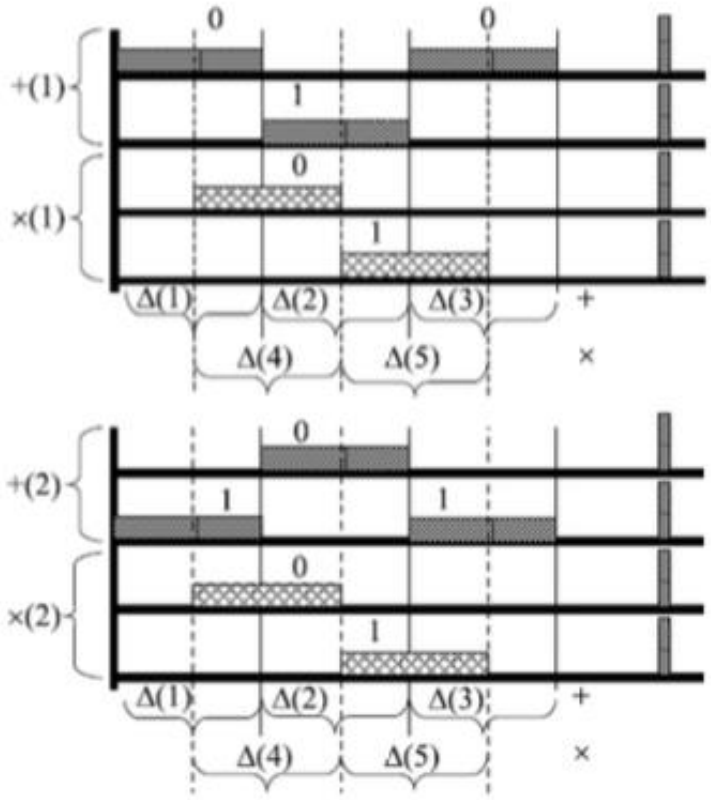

Рисунок 2.14 Квантові стани в базисах і підбазисах для схеми на часових зсувах при реалізації протоколу BB84

При роботі за протоколом BB84 спочатку випадково вибирається один з двох базисів - 1 або 2, потім також випадково всередині обраного базису вибирається один з підбазисів - + або. На наступному кроці вибирається безпосередньо значення біта «1» або «0». Відповідно для передачі біта «0» в першому базисі існує три варіанти послідовності часових зсувів. У другому базисі аналогічна картина при передачі біта «1». На приймальному кінці проводиться вимірювання станів в випадкові обрані інтервали часу Δ1 ... Δ5. Інтервали відраховуються від моменту прибуття синхроімпульсу. Після серії вимірювань одержувач повідомляє через відкритий канал номера посилок, де були зареєстровані факти спрацювання фотодетектора, користувач на передавальному кінці повідомляє який базис і підбазис були обрані. На відміну від

стандартного протоколу BB84 для узгодження базису потрібно пересилання двох біт класичної інформації замість одного.

Система з часовим кодуванням дозволяє реалізувати обмін ключами по протоколу B92 без зміни структурної схеми обладнання. Зміни торкнуться лише керуючої підсистеми, виконаної у вигляді програмного забезпечення.

2.3 Елементна база систем квантової криптографії

Елементна база, що застосовується в системах квантового розподілу ключів, являє собою набір високотехнологічних оптоелектронних модулів. До застосовуваним лазерів є високі вимоги по точності установки потужності, чистоті спектральних складових і тривалості генерації імпульсів. Для систем квантової криптографії розробляються спеціальні однофотонні джерела випромінювання на квантових точках [19]. Потужність випромінювання на довжині хвилі 1550 нм при частоті проходження імпульсів 5 МГц і одиничній середній кількості фотонів на імпульс становить -101 дБм. Для реєстрації такого слабкого випромінювання фотодетектори повинні володіти надвисокою чутливістю. На сьогоднішній день для реєстрації одиночних фотонів застосовують лавинні фотодіоди. Однак їх квантова ефективність в інфрачервоній області невелика і складає близько 10%. У кращих моделей квантова ефективність досягає 30- 70%, але вони вимагають азотного охолодження, що не дозволяє застосовувати їх поза лабораторій.

Для кодування поляризаційних станів застосовують комірки Поккельса і Керра, що працюють на основі однойменних електрооптичних ефектів. Для кодування фазових станів використовують оптичні фазові модулятори на основі ніобата літію. До обладнання,

керуючому електрооптичними пристроями, надходять високі вимоги по швидкості впливу. Висока інерційність оптичних атенюаторів не дозволяє досить точно контролювати рівень середньої кількості фотонів в кожному імпульсі.

2.4 Висновки з розділу 2

Основними джерелами одиночних фотонів є такі типи фотонних детекторів, як вакуумні, газові, твердотільні та гібридні. Ефективність детектора фотонного випромінювання залежить від матеріалу, з якого він зроблений, товщини стінок і енергії фотонів. Це пов'язано зі складним характером взаємодії випромінювання з речовиною.

Структури квантових систем розподілу ключа можуть бути засновані с поляризаційним, фазовим та часовим кодуванням. Але недосконаліть технологічного процесу виготовлення електрооптичних компонентів на сьогоднішній день не дозволяє вивести швидкісні показники квантово-криптографічних систем на якісно новий рівень.

РОЗДІЛ 3. ОСНОВНІ НАПРЯМКИ РОЗВИТКУ ТА ПРОБЛЕМИ КВАНТОВОЇ КРИПТОГРАФІЇ

3.1 Проблеми квантової криптографії

В даний час для секретної передачі повідомлення необхідно, щоб секретний ключ був випадковим, довжина ключа була не менша за довжину повідомлення та ключ використовувався тільки один раз. Ключова проблема в останньому, тому що жодна третя сторона не повинна отримати доступ до цієї інформації. Завдання безпечного обміну вирішується за допомогою квантового розподілу ключа (Quantum Key Distribution) [20].

Взагалі, квантова теорія інформації лежи на стику двох найбільш значних теорій XX століття: квантової механіки і теорії інформації. Вона працює з квантовомеханічними станами і розглядає їх здатність брати участь в перенесенні і обробці інформації. Під час появи цієї теорії були актуальні проблеми, пов'язані з сильним впливом квантового шуму, що вважався однозначно руйнівним чинником. Однак, при більш детальному вивченні цього явища з'ясувалося, що квантовий шум може надавати суттєву допомогу при передачі і обробці інформації: так, явище квантового розмивання частки по декількох точках простору має властивість інтерференції, здатній, в ряді випадків, принести суттєву користь.

Важливо відзначити, що при проведенні перших дослідів над елементарними частинками було виявлено, що їх поведінку дуже складно пов'язати з існуючими на той момент уявленнями про фізичні явища. Це призвело до того, що після формулювання нових законів, що описують поведінку елементарних частинок, цю частину фізики стали називати

квантовою теорією, а сформовану на той момент картину світу - класичною.

Одним з ключових законів квантової механіки є рівняння Шредінгера, яке описує зміну квантових станів у часі. Якщо враховувати, що Ерміта оператор H називається гамільтоніаном системи і саме він впливає на її еволюцію, то рівняння Шредінгера означає, що будь-яка еволюція квантової системи може бути представлена як дію деякого унітарного перетворення.

Найпростішим же прикладом нетривіального квантового об'єкта є система з двома базисними станами. Фізичними прикладами подібних систем можуть бути фотони з відповідними напрямками поляризації (вертикальної і горизонтальної), або напрямки спіна електрона (вгору і вниз). В цьому випадку відповідний гільбертовий простір буде двовимірним. Зазвичай, якщо не важлива конкретна природа дворівневої системи, її стани позначають 0 і 1. За аналогією з класичним бітом таку систему називають кубітом, що "означає квантовий біт".

Саме процедура вимірювання квантових станів відрізняє квантовий випадок проведення дослідів від класичного і дає можливість застосування квантової криптографії. У загальному випадку вимір квантової системи змінює її початковий стан, і це є найважливішою відмінністю квантової механіки від класичної.

Розглядаючи і порівнюючи квантову і класичну картини світу необхідно виділити кілька фундаментальних відмінностей.

Перше проявляється вже в самому визначенні квантової частинки і її стану. Подання про таку частку, як про деяке тіло, що має певні координати, розмір і масу, виявилися абсолютно неправильними, так як для деяких таких частинок не вдавалося навіть в принципі зрозуміти в якій точці простору вони знаходяться. Але прогноз поведінки таких

частинок виявився можливим, але тільки після відмови пояснити поведінку за допомогою "традиційних" характеристик. Характеристика стану елементарної частинки виражається в "хвильовій" функції, принципово новому об'єкті квантової картини світу.

Метод квантового розподілу ключа полягає в передачі окремих бітів коду за допомогою квантового стану елементарної частинки світла - фотона. Його надійність обумовлена фундаментальними законами квантової механіки, за якими навіть частина сигналу не можна забрати з передавальної лінії, так як неможливо поділити фотон на частини, а безпосереднє вбудовування в передавальну лінію неможливо, тому що квантовий стан не можна виміряти, не порушивши його, так як вимір одного сигналу рандомізує іншу складову.

У квантовій криптографії виділяють два основних напрямки розвитку систем розподілу ключів [21].

Перший напрямок базується на принципі неможливості абсолютно надійно розрізнити два неортогональних квантових стану самотньої частки, друге засновано на ефекті «переплутаних станів» [21].

Перша проблема носить фізичний характер. Використання в якості лінії передачі оптоволоконного кабелю обмежує відстань до 100 кілометрів і до 200-250 в лабораторії. Причина - втрата фотона через не ідеальность оптичного волокна [22]. Класичне рішення у вигляді підсилювача не відповідає законам квантового світу: зчитування сигналу з метою посилення неминуче змінить останній, тому підсилювач відрізняється від «шпигуна».

Рішенням є створення «квантового повторювача», який буде приймати сигнал НЕ прослуховуючи його. Для цієї мети передбачалося використовувати окремі атоми, але через практичну ненадійності, від цієї

ідеї відмовилися на користь атомних ансамблів, використання яких значно підвищує співвідношення сигнал / шум.

Друга проблема носить математичний характер. Розрахунок руху квантової частинки передбачає, що частка рухається за всіма можливими «альтернативними траєкторіями». В режимі суперпозиції [22]. Суперкомп'ютери, які розраховують рух мільярдів зірок, не здатні змоделювати взаємодію більше двох десятків квантових частинок.

Рішенням є створення так званого «квантового комп'ютера». Одна з перших теоритических моделей була запропонована Річардом Фейнманом в 1981 році. Проблема її практичної реалізації - одна з головних задач фізики 21-го століття, над якою працюють найбільші лабораторії світу.

Третя проблема полягає в збереженні квантового стану. Вона актуальна в ряді завдань, коли наявний квантовий стан світла необхідно використовувати не зараз, а, припустимо, через 100 мілісекунд. Для цього пропонують перенести цю інформацію в тверде тіло. Вирішити це завдання вдалося швейцарським фізикам в лабораторних умовах за допомогою домішкових іонів неодиму в кристалі. На практиці фізикам знадобиться більш високі значення ефективності і часу зберігання, а також можливість зчитування інформації за запитом. Для цього можна використовувати силікат ітрію, легований ізотопом європія і «заморожувати» стан атома під дією магнітних полів. Перспективність цього напрямку обумовлена дослідниками Австралійського національного університету [23].

Крім того, в даний момент, вчені виділяють необхідність приведення фотонів у взаємодію. Основа логіки на взаємодії бітів і їх зміні (на 0 або 1) при виконанні умовного оператора слабо вивчена в світі квантових частинок, надмалих розмір, великі швидкості і дуалізм яких

дозволяють фотонам практично не помічати один одного. Більш того, рішення саме цієї проблеми наблизить створення «квантового комп'ютера», появу яких, очікуть в найближчі 15-20 років.

3.2 Перспективи у розвитку квантової криптографії

З урахуванням викладених вище прикладних аспектів, а також з огляду на результати численних проведених наукових досліджень і розробок [2], можна з досить високою ймовірністю припустити наступний сценарій розвитку напрямків, які мають безпосереднє відношення до квантової криптографії.

У середньостроковій перспективі отримають розвиток спеціалізовані квантові комп'ютери, орієнтовані на рішення криптографічних завдань. Як вже зазначалося вище, для вирішення практично значимих завдань потрібно створити реєстр з числом кубітів, ефективно беручих участь в обчисленнях, до 1000. При цьому використання в квантовій обчислювальній системі кодів квантової корекції помилок зажадає істотного (приблизно на порядок) збільшення числа «запасних» (використовуваних тільки для корекції) кубітів. Тому для реалізації 1000 ефективно використовуваних («логічних») кубітів буде потрібно створення квантового регістра з істотно великою загальною кількістю кубітів.

Очікується, що для обслуговування 1000 кубітів за допомогою багатопроменевої лазерної системи, кріогенної системи і інших допоміжних систем не буде потрібно надмірно великих ресурсів. Подібна обчислювальна система зможе розміщуватися в приміщенні площею 50 - 100 м2, її енергоспоживання складе близько 100-200 кВт, причому

квантовий процесор буде споживати лише невелику частину цих ресурсів (1% або менше), а весь інший ресурс піде на допоміжні системи.

Особливу роль гратимуть розподілені квантові обчислювальні системи (квантові симулятори), які дозволять додатково підвищити ефективність моделювання складних процесів в різних областях науки, включаючи медицину і фармакологію, біологію та генну інженерію, матеріалознавство та ін.

У більш віддаленій перспективі можливо забезпечити поєднання окремих квантових обчислювальних систем в квантову мережу.

Отримає суттєвий розвиток область квантових комунікацій:

а) Засоби квантового розподілу криптографічних ключів можуть бути створені орієнтовно до 2020 року і будуть мати наступні характеристики:

- для волоконно-оптичного каналу зв'язку: швидкість вироблення ключів - 10 Гбіт / с при дальності до 200 км ;

- для атмосферного каналу зв'язку: швидкість вироблення ключів - 1 Гбіт / с при дальності до 2 км;

- для каналу розподілу ключів з Землі через низькоорбітальні космічні апарати: швидкість вироблення ключів - 1 кбіт / с при дальності до 1500 км.

б) У середньостроковій перспективі можуть бути створені квантові канали зв'язку, що виключають перехоплення інформації третьою стороною, з дальністю передачі інформації порядку 1000-3000 км в космічному просторі і близько 100 км в щільних шарах атмосфери зі швидкістю передачі інформації до 100 Мбіт / с. Інтеграція в ці мережі технологій квантового хеширування і квантового цифрового підпису дозволить вийти на новий рівень безпеки інформаційних технологій з розподіленою обробкою даних.

У середньостроковій перспективі можуть бути створені канали зв'язку на основі квантової телепортації, що забезпечують передачу до 107 кубіт (квантових станів) в секунду на відстань близько 1000 кілометрів в космічному просторі.

На базі каналів телепортації квантових станів в подальшому можуть бути створені квантові мережі, які зможуть використовуватися як для передачі квантової і класичної інформації, так і для організації розподілених квантових обчислень.

Один з можливих способів організації квантових мереж - мережі на основі квантових повторювачів (репітерів), ключовим елементом яких є квантова пам'ять. Повноцінні зразки квантової пам'яті, як основи квантових повторювачів, і зразки самих повторювачів можуть бути створені в найближчому десятилітті. Сполучення керованих джерел ЕП пар фотонів з квантової пам'яттю дозволять в перспективі 15 років створити квантові мережі, здатні об'єднувати квантові обчислювачі в єдину розподілену систему.

Квантова мережа високоточної синхронізації для захищених систем управління може бути створена в майбутньому десятилітті і буде підтримувати глобальне покриття навколоземного космічного простору і мати мережу з десяти вузлів (опорних станцій) по 1000 кубітів (атомів) в кожному, що забезпечить стабільність частоти до 10 -18, тобто в 100 разів краще наявних класичних аналогів. Зауважимо, що окремі технології, що входять до складу зазначених напрямків, такі, як квантова генерація випадкових чисел, можуть мати і вже мають самостійне прикладне значення.

3.3 Висновки з розділу 3

Аналізуючи описане вище, можна зрозуміти основні проблеми квантової криптографії і передачі квантового ключа. Ці проблеми грубо можна розділити на два класи: методологічні та технологічні.

До методологічних проблем можна віднести проблему таємності, підслуховування, можливості перехоплення і дешифрування повідомлень.

Технологічні проблеми і перспективи зростання довжини передачі визначаються, з одного боку, типом використовуваного кодування, а з іншого - тими труднощами процедури уточнення, які неминуче впливають на допустиму точність і надійність формування підсумкового секретного квантового ключа

Незважаючи на безліч невирішених завдань, квантова криптографія залишається найперспективнішим напрямом в області інформаційної безпеки, а квантові лінії зв'язку є найбезпечнішими для передачі секретного ключа. А завдяки безлічі інших переваг можна вважати, що найближчим часом вони замінять всі існуючі алгоритми шифрування інформації.

РОЗДІЛ 4. ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ КВАНТОВОЇ КРИПТОГРАФІЇ

Існує безліч протоколів квантової криптографії заснованих на передачі інформації за допомогою кодування в станах одиночних фотонів, наприклад: BB84, B92, BB84 (4 + 2), з шістьма станами, Гольденберга- Вайдман, Коаші -Імото і їх модифікації. Єдиний протокол, розроблений для кодування інформації в переплутаних станах - E91. Розглянемо більш докладно існуючі протоколи квантового розподілу ключів.

4.1 Квантовий протокол BB84

У протоколі BB84 використовуються 4 квантових стану фотонів, наприклад, напрямок вектора поляризації, одне з яких Аліса вибирає залежно від переданого біта: 90 ° або 135 ° для «1», 45 ° або 0 ° для «0». Одна пара квантових станів відповідає 0(0(+)) и 1(1(+)) і належить базису «+». Інша пара квантових станів відповідає 0(0(×)) и 1(1(×)) и належить базису «×».

Всередині обох базисів стану ортогональні, але стану з різних базисів є попарно неортогональної (неортогональної необхідна для детектування спроб с'єма інформації).

Квантові стану системи можна описати таким чином:

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

Тут стани 0_+ и 1_+ кодують значення «0» и «1» в базисі «+», а $0_\times$ і $1_\times$ кодують ті ж значення в базисі «×».Базиси повернені один відносно одного на 45° (рис. 4.1).

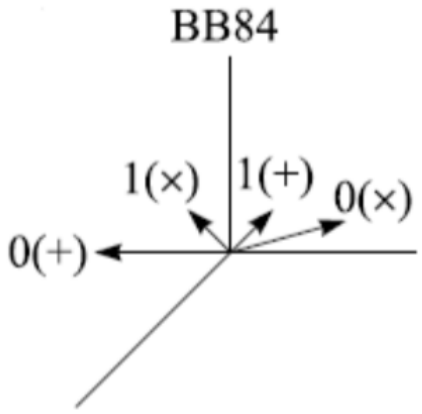

Рисунок 4.1 Стани поляризації фотонів, що використовуються в протоколі BB84

Етапи формування ключів:

1) Аліса випадковим чином вибирає один з базисів. Потім всередині базису випадково вибирає один зі станів, відповідне 0 або 1 і посилає фотони (рис. 4.2):

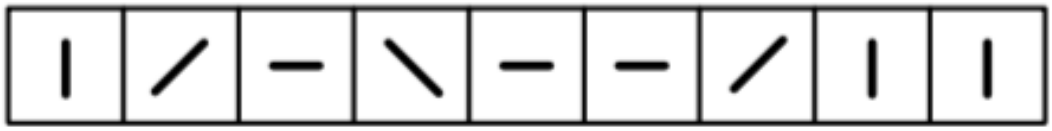

Рисунок 4.2 Фотони з різною поляризацією

2) Боб випадково і незалежно від Аліси вибирає для кожного вступника фотона: прямолінійний (+) або діагональний (⌭) базис (рис 4.3):

Рисунок 4.3 Обраний тип вимірювань

Потім Боб зберігає результати вимірювань (рис. 4.4):

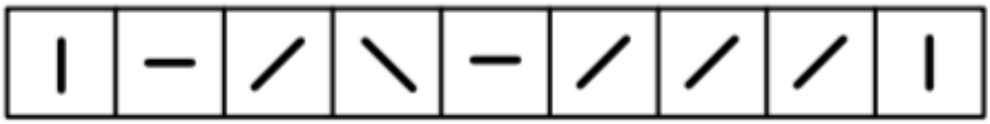

Рисунок 4.4 Результати вимірювань

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

4) Аліса повідомляє Бобу по відкритому загальнодоступному каналу зв'язку, які вимірювання були обрані відповідно до вихідним базисом Аліси (рис. 4.5):

Рисунок 4.5 Випадки правильних вимірів

5) далі користувачі залишають тільки ті випадки, в яких обрані базиси збіглися. Ці випадки переводять в біти (0 і 1), і отримують, таким чином, ключ (рис. 4.6):

Рисунок 4.5 Отримання ключової послідовності за результатами правильних вимірів

Число випадків, в яких обрані базиси збіглися, становитиме в середньому половину довжини вихідної послідовності, тобто $n = 1/2$

(приклад визначення кількості фотонів, прийнятих Бобом, показаний в таблиці 4.1).

Таблиця 4.1 Формування квантового ключа по протоколу BB84

Двоичный сигнал Алисы	0	1	0	1
Поляризационный код Алисы	↔	↕	↘	↙
Детектирование Бобом	⇹	⇹	⇹	⇹
Двоичный сигнал Боба	0	1	?	?

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

Однак ідеальних каналів зв'язку не існує і для формування секретного ключа необхідно провести додаткові процедури пошуку помилок і посилення секретності. При цьому для частини послідовності біт користувачів, в яких базиси збіглися, через відкритий загальнодоступний канал зв'язку випадковим чином розкриваються і порівнюються значення біт. Далі розкриті біти відкидаються. В ідеальному квантовому каналі (без шуму) досить виявити невідповідність в одній розкритій позиції для виявлення зловмисника. В реальній ситуації неможливо розрізнити помилки, які сталися через шум і через вплив зловмисника. Відомо, що якщо відсоток помилок QBER $\leq$ 11%, то користувачі з нерозкритої послідовності, після корекції помилок через відкритий загальнодоступний канал зв'язку і посилення секретності, можуть отримати секретний ключ, який буде у них однаковим і не буде

відомий Єві. Ключ, отриманий до додаткових операцій з послідовністю, називається "сирим" ключем.

При корекції помилок ефективним способом для узгодження послідовностей Аліси і Боба є їх «перемішування» для більш рівномірного розподілу помилок і розбиття на блоки розміром k, при якому ймовірність появи блоків з більш ніж однією помилкою нехтує мала. Для кожного такого блоку боку проводять перевірку на парність. Блоки з збігається парністю визнаються правильними, а що залишилися діляться на кілька дрібніших блоків, і перевірка на парність проводиться над кожним таким блоком, до тих пір, поки помилка не буде знайдена і виправлена. Процедура може бути повторена з блоками більш підходящого розміру. Найбільш дрібні блоки відкидаються при наявності в них помилки.

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

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

4.2 Квантовий протокол B92

У протоколі B92 [24] використовуються фотони, поляризовані в двох різних напрямках для подання нулів і одиниць ($|\varphi_0|\,i\,|\varphi_1|$, $|\varphi_0\varphi_{01}| \neq 0$). Фотони, поляризовані вздовж напрямку $+45^{o}$, несуть інформацію про одиничний біт, фотони, поляризовані вздовж напрямку 0^{o} (V) – про нульовий біт. Ці стани зручно для наочності зображати графічно (рис. 4.6).

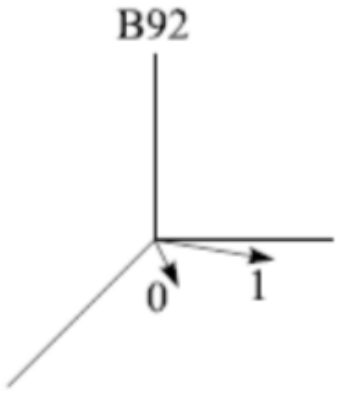

Рисунок 4.6 Поляризаційні стани, що використовуються в протоколі B92

Алгоритм роботи протоколу B92 (рис. 4.8).

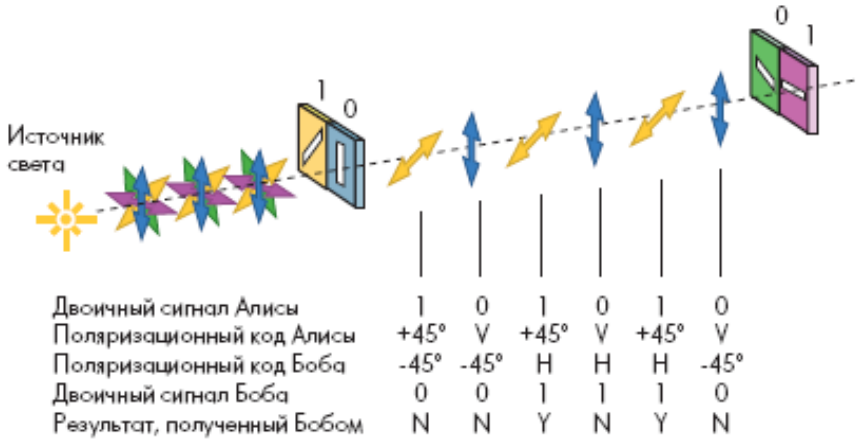

Рисунок 4.8 Формування квантового ключа по протоколу B92

Станція Аліса посилає фотони, поляризовані в напрямках 0 і $+45^{o}$, що представляють нулі і одиниці. Причому послідовність фотонів, що посилається станцією Аліса, випадково орієнтована. Станція Боб приймає фотони через фільтри орієнтовані під кутом 90^{o} і 135^{o} (-45^{o}). При цьому якщо фотон, переданий станцією Аліса, буде аналізувати станцією Боб за допомогою фільтра орієнтованого під кутом 90^{o} по відношенню до переданого фотону, то фотон не пройде через фільтр. Якщо ж цей кут складе 45^{o}, то фотон пройде через фільтр з ймовірністю 0,5.

Для визначення поляризації станція Боб аналізує прийняті нею фотони, використовуючи обраний випадковим чином один з двох неортогональних базисів «+» або «⌭». Якщо станція Боб аналізує надісланий фотон фільтром з ортогональним напрямком поляризації, то він не може точно визначити, яке значення цей фотон представляє: 1, відповідне фотону, який не проходить, або 0, відповідне фотону, який не проходить з ймовірністю 0,5. Якщо ж напрямки поляризації між надісланим фотоном і фільтром, неортогональні, то станція Боб може визначити, що прийнятий фотон відповідний 0. Якщо фотон був прийнятий вдало, то черговий біт ключа кодується 0 (якщо фотон був прийнятий фільтром, орієнтованим під кутом 135^{o}), або 1 (якщо фотон був прийнятий фільтром, орієнтованим у напрямку Н) (таблиця 4.2)

Таблиця 4.2 Формування квантового ключа по протоколу B92

Двоичный сигнал станции Алиса	1	0	1	0
Поляризационный код станции Алиса	⤢	↕	⤢	↕
Поляризационный код станции Боб	⤡	⤡	↔	↔
Двоичный сигнал станции Боб	0	0	1	1
Результат, полученный станцией Боб	-	-	+	-

У першій і четвертій колонці поляризації при передачі і прийомі ортогональні і результат детектування буде відсутній. В колонках 2 і 3 коди двійкові розряди збігаються і поляризації НЕ ортогональні. З цієї причини з імовірністю 50% може бути позитивний результат в будь-якому з цих випадків (і навіть в обох). У таблиці передбачається, що успішне детектування фотона відбувається для випадку, представленого в колонці 3. Саме цей біт стає першим бітом загального секретного ключа передавача і приймача. Звідсимінімальна кількість фотонів, яке може бути прийняте станцією Боб n = 1 / 4.

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

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

Для виявлення факту знімання інформації в даному протоколі використовують контроль помилок, аналогічний контролю помилок в

протоколі BB84. Тобто, станції Аліса і Боб звіряють випадково вибрані біти ключа. Якщо виявляються розбіжності, то можна говорити про несанкціоноване знімання інформації.

Розглянуті вище протоколи є основними. Однак існує ряд похідних протоколів. Наведемо деякі з них.

4.3 Протокол з шістьма станами

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

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

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

Таким чином, можна порахувати кількість фотонів, які будуть прийняті станцією Боб.

Таблиця 4.3 Формування квантового ключа по протоколу з шістьма станами

Двоичный сигнал станции Алиса	1	0	1	0	1	0
Поляризационный код станции Алиса	↙	↕	↔	↘	↺	↻
Детектирование станции Боб	✥	✥	✥	✥	✥	✥
Двоичный сигнал станции Боб	?	0	1	?	?	?

З таблиці 4.3 видно, що мінімальна кількість фотонів, яка буде

прийнята станцією Боб при детектуванні $n = 2/6 = 1/3$. Тобто при використанні протоколу з шістьма станами [25] буде прийнято близько 33% фотонів, які посилаються станцією Аліса.

4.4 Квантовий протокол BB84(4+2)

Даний протокол [26] є проміжним між протоколами BB84 і B92. У протоколі використовуються 4 квантових стану для кодування «0» і «1» в двох базисах. Стани в кожному базисі вибираються неортогональні, стани в різних базисах також попарно неортогональні. Це зручно представити графічно (рис. 4.9):

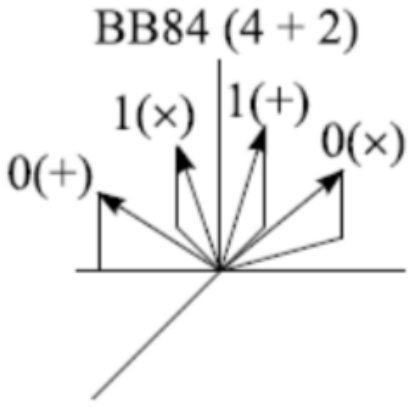

Рисунок 4.9 Поляризовані стани, що використовуються в протоколі BB84 (4 + 2)

Протокол реалізується в такий спосіб. Станція Аліса випадковим чином вибирає один з базисів. Усередині базису також випадковим чином вибираються стани 0 або 1, потім вони направляються в квантовий канал зв'язку. Станція Боб незалежно вибирає вимірювання двох типів (в різних базисах). Потім, після передачі досить довгої послідовності

користувачі через відкритий загальнодоступний канал зв'язку повідомляють, який базис був використаний в кожній посилці. Посилки, в яких базиси не збігалися, відкидаються. Для решти посилок станція Боб публічно відкриває номера тих посилок, де у нього були невизначені результати (такі посилки теж відкидаються). З решти посилок (з певним результатом) витягується секретний ключ шляхом процедури корекції помилок через відкритий канал і посилення секретності. Підрахунок кількості фотонів, прийнятих станцією Боб, представлений в таблиці 4.4.

Таблиця 4.4 Формування квантового ключа по протоколу BB84(4+2)

Двоичный сигнал станции Алиса	0	1	0	1	0	1	0	1
Поляризационный код станции Алиса	↔	↕	↘	↗	↔	↕	↘	↗
Детектирование станцией Боб	✕	✕	✕	✕	+	+	+	+
Двоичный сигнал станции Боб	0	?	?	1	0	?	?	1

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

4.5 Протокол Гольденберга-Вайдмана

У протоколі Гольденберга-Вайдмана [27] Аліса і Боб використовують для повідомлення два ортогональних стану:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle), \qquad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle),$$

кодуючі відповідно біти «0» і «1».

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

4.6 Протокол Коаши-Імото

Даний протокол [28] є модифікацією попереднього, але дозволяє відмовитися від випадкових часів передачі шляхом асимметризації інтерферометра, тобто розбиття світла в нерівній пропорції між коротким і довгим плечима. Крім того, різниця фаз між двома плечима інтерферометра становить π. Таким чином, два стану

$$|\psi_0\rangle = -i\sqrt{R}|a\rangle + \sqrt{T}|b\rangle \quad |\psi_1\rangle = \sqrt{R}|a\rangle - i\sqrt{T}|b\rangle$$

що кодують біти «0» і «1», визначаються відбивною R і пропускною T здібностями вхідного роздільник променів.

У разі асиметричної схеми, коли амплітуда ймовірності знаходження фотона в тому чи іншому плечі інтерферометра залежить від значення переданого біта, компенсація за рахунок фази не спрацьовує повністю. Тому при застосуванні Євою вищеописаної тактики існує ненульова ймовірність помилки детектування.

Провівши порівняльний аналіз наведених вище протоколів, з розрахунку кількості прийнятих фотонів, можна судити про те, що найбільш ефективним є BB84. Пізніше його модифікації спрямовані на зменшення відсотка помилок і кількості корисної інформації, яку теоретично може отримати зловмисник. Альтернативою у розвитку протоколу BB84 є протокол B92. Перевагою протоколу B92 перед BB84 є використання фотонів з двома типами поляризації (замість чотирьох), що дозволяє спростити схему реалізації, однак забезпечує меншу ефективність (зменшується кількість прийнятих фотонів), і гарантовану секретність ключа тільки на відстані до 20 км, тоді як BB84 - на відстані до 50 км. В даний час в комерційних системах розподілу ключа застосовується протокол BB84.

4.7 Протокол E91(EPR)

Протокол E91 був запропонований А. Екертом в 1991 році. Друга назва протоколу - EPR. так як він заснований на парадоксі Ейнштейна-Подольські-Розенберга. У протоколі пропонується використовувати, наприклад, пари фотонів, які народжуються в антисиметричних поляризаційних станах. Перехоплення одного з фотонів пари не приносить Єві ніякої інформації, але є для Аліси і Боба сигналом про те,

що їх розмову підслуховують.

Ефект EPR виникає, коли сферичний симетричний атом випромінює два фотона в протилежних напрямках в сторону двох спостерігачів. Фотони випромінюються з невизначеною поляризацією, але в силу симетрії їх поляризації завжди протилежні. Важливою особливістю цього ефекту є те, що поляризація фотонів стає відомою тільки після вимірювання. На основі EPR Екерт і запропонував протокол, який гарантує безпеку пересилання і зберігання ключа. Відправник генерує кілька EPR фотонних пар. один фотон з кожної пари він залишає для себе, другий посилає своєму партнеру. При цьому, якщо ефективність реєстрації близька до одиниці, при отриманні відправником значення поляризації 1, його партнер зареєструє значення 0 і навпаки. Ясно, що таким чином партнери щоразу, коли потрібно, можуть отримати ідентичні псевдовипадкові кодові послідовності.

Нехай спочатку створюється N максимально заплутаних EPR-пар фотонів, потім один фотон з кожної пари надсилається Алісі, а інший - Бобу. Три можливих квантових стану для цих EPR-пар є:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A |\frac{3\pi}{6}\rangle_B - |\frac{3\pi}{6}\rangle_A |0\rangle_B\right),$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|\frac{\pi}{6}\rangle_A |\frac{4\pi}{6}\rangle_B - |\frac{4\pi}{6}\rangle_A |\frac{\pi}{6}\rangle_B\right),$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left(|\frac{2\pi}{6}\rangle_A |\frac{5\pi}{6}\rangle_B - |\frac{5\pi}{6}\rangle_A |\frac{2\pi}{6}\rangle_B\right),$$

Це може бути записано в загальному вигляді як

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

Остання формула явно показує, що кожне з цих трьох станів кодує біти «0» і «1» в унікальному базисі. Потім Аліса і Боб здійснюють

вимірювання на своїх частинах розділених EPR-пар, застосовуючи відповідні проектори

$$P_1 = |0\rangle\langle 0|, \qquad P_2 = |\frac{\pi}{6}\rangle\langle\frac{\pi}{6}|, \quad P_3 = |\frac{3\pi}{6}\rangle\langle\frac{3\pi}{6}|.$$

Аліса записує виміряні біти, а Боб записує їх доповнення до 1. Результати вимірювань, в яких користувачі вибрали однакові базиси, формують сирий ключ. Для інших результатів Аліса і Боб проводять перевірку виконання нерівності Белла як тест на присутність Єви.

Експерименти по реалізації даного протоколу почалися нещодавно. Їх проведення стало можливим після отримання джерел переплутаних пар з високим ступенем кореляції і тривалим часом життя.

4.8 Висновки з розділу 4

В останні роки найбільша увага приділяється квантовому розподілу ключів, фактично вже існують досвідчені комерційні зразки таких систем. Тому детальний аналіз надійності КРК в даний час є важливою науковою проблемою.

Більшість із запропонованих КРК використовують для передачі бітів дворівневі квантові системи - кубіти. При цьому кожен кубіт кодує один біт інформації. Основними характеристиками таких протоколів є стійкість до різних стратегій атак підслуховування агента, а також ефективність протоколу, тобто відношення кількості біт, що використовуються для генерації ключа, до загальної кількості біт, переданих по квантовому каналу зв'язку.

ВИСНОВКИ

1. Квантова криптографія – метод забезпечення конфіденційності і цілісності інформації, який використовує принципи квантової фізики. Спроба вимірювання параметрів в квантовій системі вносить в неї порушення, руйнуючи вихідні сигнали, а значить, за рівнем шуму в каналі користувачі можуть розпізнати ступінь активності перехоплювача.
2. Джерела одиночних фотонів можуть генерерувати випромінювання в будь-яких довжинах хвиль, але мають свої недоліки. Основними проблемами при використанні ДОФ є температурний режим під час роботи та ймовірність того, що одночасно джерело може сгенерувати декілька фотонів
3. Основними проблемами квантової криптографії є проблема таємності, підслуховування, можливості перехоплення і дешифрування повідомлень. Також перспективи зростання довжини передачі, які в майбутньому впливають на надійність формування підсумкового секретного квантового ключа
4. Квантова криптографія є одним з найперспективнішим напрямів в області інформаційної безпеки. В свою чергу квантові лінії зв'язку є найбезпечнішими для передачі секретного ключа. Також є багато й інших переваг, завдяки яким у майбутньому квантова криптографія замінить всі існуючі алгоритми шифрування інформації.
5. Квантовий розподіл ключа - метод передачі ключа, який використовує квантові явища для гарантії безпечної зв'язку. Цей метод дозволяє двом сторонам, з'єднаним з відкритого каналу зв'язку, створити загальний випадковий ключ, який

відомий тільки їм, і використовувати його для шифрування і розшифрування повідомлень.

6. Протоколи КРК розділені на дві основні категорії: протоколи підготовки та вимірювання (вимірювання квантового стану призводить його до змін) та протоколи, засновані на заплутанності (квантові стани об’єктів можуть бути з’єднані так, що перехоплення будь-якого з них змінює систему в цілому).
7. Було зроблено детальний аналіз основних протоколів квантового розподілу ключа.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. S. Wiesner, "Conjugate coding", Sigact News 15, 78-88 (1983).
2. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии — 3-е изд. — М.: Диалог-МИФИ, 2011. — 176 с. — ISBN 978-5-9912-0182-7
3. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. — М.: Гелиос АРВ, 2002. — 240 с. — 3000 экз. — ISBN 5-85438-043-9.
4. Голубчиков Д. М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы.
5. Килин С. Я., Хорошко Д. Б., Низовцев А. П. «Квантовая криптография: идеи и практика»;
6. Румянцев К. Е., Плёнкин А. П. Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. 2014. № 10. С. 11 − 16.
7. In Particle detectors D. Chakraborty and T. Sumiyoshi. Photon detectors
8. Жигарев А. А., Шамаева Г. Т. Электронно-лучевые и фотоэлектронные приборы: Учебник для вузов. — М.: Высшая школа, 1982. — 463 с., ил.
9. Rachel Chechik and Amos Breskin. Advances in Gaseous Photomultipliers
10. А. Ф. Бузулуцков. Газовые фотодетекторы с твердыми фотокатодами
11. Bahaa E. A. Saleh, Malvin Carl Teich. Fundamentals of Photonics. ch17. Semiconductor photon detectors

12. A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", Europhysics Lett. 23, 383-388 (1993).

13. J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibers: experimental and practical limits", J. Mod. Opt. 41, 2405- 2412 (1994).

14. G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states", Physical Review Letters, Vol. 90, No. 22, 227901 (2003).

15. C.H. Bennett, "Quantum cryptography using any two non-orthogonal states", Phys. Rev. Lett. 68, 3121-3124 (1992).

16. M. Martinelli, "A universal compensator for polarization changes induced by birefringence on a retracting beam", Opt. Commun. 72, 341-344 (1989).

17. С.Н. Молотков. “Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы”, Письма в ЖЭТФ, Том 79, Выпуск 11.

18. С.Н. Молотков. “Мультиплексная квантовая криптография с временным кодированием без интерферометров”, Письма в ЖЭТФ, Том 79, Выпуск 9.

19. K.Alchalabi, D.Zimin, G.Kostorz, and H.Zogg. “Self-assembled semiconductor quantum dots with nearly uniform sizes” Phys. Rev. Lett. 90 (2003)

20. A. I. Lvovsky Squeezed light, section in book: Photonics Volume 1: Fundamentals of Photonics and Physics, D. Andrews, eds., Chapter 5: 121–164 Published by Wiley, West Sussex, United Kingdom, 2015

21. Холево А. С. Квантовые системы, каналы, информация. — М.:МЦНМО, 2010, -328 с.

22. Три главных квантовых прорыва. [Електронный ресурс]. — Режим доступу до журн.: http://slon.ru/future/3_glavnykh_kvantovykh_proryva_2013–869070.xhtml).

23. Создан квантовый накопитель с рекордным временем работы. [Електронный ресурс]. Режим доступу до журн.: http://zoom.cnews.ru/news/item/591505.

24. C.H. Bennett, "Quantum cryptography using any two non-orthogonal states", Phys. Rev. Lett. 68, 3121-3124 (1992).

25. D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States", Phys. Rev. Lett, Vol. 81, 3018 (1998).

26. B. Huttner, N. Imoto, N. Gisin, T. Mor, "Quantum Cryptography with Coherent States", Phys. Rev. A, Vol. 51, 1863—1869 (1995).

27. L. Goldenberg, L. Vaidman, "Quantum Cryptography Based On Orthogonal States", Phys. Rev. Lett., Vol. 75, 1239 (1995)

28. M. Koashi, N. Imoto, "Quantum Cryptography Based on Split Transmission of One- Bit Information in Two Steps", Phys. Rev. Lett., Vol. 79, 2383 (1997).