*УДК 535.2*

***Репин В.А.***
***Магистрант***
***Кубанский государственный университет***
***Кулиш О.А.***
***Кандидат физико-математических наук, доцент***
***Кубанский государственный университет***

# АНАЛИЗ ХАРАКТЕРИСТИК ЭЛЕМЕНТОВ КВАНТОВО-КРИПТОГРАФИЧЕСКИХ СИСТЕМ

***Аннотация:*** *Основой конструкции установок квантовой криптографии являются два разбалансированных интерферометра Маха-Цендера, соединенных волоконно-оптической линией связи. Для приемлемой видности интерференции на выходе такой системы оба интерферометра должны быть идентичны с точностью до единиц микрометров, а расщепители излучения на входах и выходах интерферометров должны разделять интенсивность волны в соотношении 50:50. В квантово-криптографической установке будет возникать дрейф фазы, который необходимо свести к минимуму путем применения систем температурной стабилизации и компенсации набега фазы.*

***Ключевые слова:*** *квантовая криптография, фазовое кодирование, видность интерференции, дрейф фазы, детектирование фотонов, оптический разделитель.*

***Summary:*** *The basis of the design of quantum cryptography plants are two unbalanced Mach-Zehnder interferometers connected by a fiber-optic communication line. For an acceptable view of the interference at the output of such a system, both interferometers should be identical to within a few micrometers, and radiation splitters at the inputs and outputs of the interferometers should separate the wave intensity in a ratio of 50:50. In a quantum-cryptographic installation, phase drift will occur, which*

*must be minimized by applying temperature stabilization systems and compensating for phase incursion.*

***Keywords:*** *quantum cryptography, phase coding, visibility of interference, phase drift, photon detection, optical splitter.*

**Введение**

Одним из наиболее интенсивно развивающихся направлений криптографии в настоящее время является квантовая криптография, современный этап развития, который позиционируется, как создание оптических систем передачи квантовой информации. Безопасность информации, которая передается по квантово-криптографическому каналу связи, обусловлена физическими принципами квантовой механики.

Для передачи неопределенной последовательности бит, которую используют в качестве ключа в симметричных криптосистемах, разработаны оптические квантово-криптографические установки с фазовой модуляцией и последующим интерферометрическим детектированием фотонов. Базой конструкции квантово-криптографических установок с фазовым кодированием являются два разбалансированных интерферометра Маха-Цендера, соединенных волоконно-оптической линией связи [1].

Выделим главные условия, предъявляемые к оптическим элементам систем квантовой криптографии с фазовым кодированием. Элементы системы квантовой криптографии должны иметь малые потери мощности оптического излучения, так как в квантово-криптографических волоконно-оптических схемах нельзя использовать усилители. Из-за невозможности клонирования состояний квантовых систем следует, что использование усилителя дает такое же разрушающее воздействие при передаче по оптическому квантовому каналу, как и попытка перехвата сообщения [2]. Следовательно, требованием к квантово-криптографическим системам является малость потерь в передающем оптическом волокне, а также использование для регистрации фотонов

фотодетекторов, работающих в режиме счета единичных фотонов. Для всех существующих систем, основанных на инфракрасных фотонах и кварцевых световодах, минимальный уровень потерь оптического излучения составляет порядка 0,2 дБ/км.

Основная трудность в использовании волоконно-оптической квантово-криптографической системы с фазовым кодированием состоит в необходимости добиться полной идентичности всех компонентов двух интерферометров системы, что в принципе довольно трудно воиспроизвести на практике. Обратим внимание на зависимость видности интерференции от рассогласования оптических путей в интерферометре. Для оптических монохроматических волн видность интерференционной картины всегда равна 1. Свет от реального физического источника никогда не бывает строго монохроматическим, учитывая, что даже самая узкая спектральная линия имеет конечную ширину. Помимо этого, физический оптический источник имеет конечные размеры и состоит из огромного числа элементарных излучателей. Поэтому для адекватного описания интерференции рассматривают квазимонохроматический свет. То есть свет, состоящий из спектральных компонент, которые занимают частотный интервал $\Delta\nu$, малый по сравнению со средней частотой.

Расчеты дают понять, что при рассогласовании плеч волоконно-оптического интерферометра порядка длины волны оптического излучения, видность падает до 50%, следовательно это является очень низким показателем. Отсюда следует, в волоконно-оптических системах квантовой криптографии с фазовым кодированием оба интерферометра должны быть тождественным с точностью до долей длины волны.

В волоконно-оптических интерферометрах на четкость интерференции негативно влияет еще и дрейф фазы оптического излучения. Поэтому для нормальной работы оптической установки должна быть активная система компенсации дрейфа фазы и подстройка фазы каждый раз перед циклом передачи ключа. Так чтобы количество ошибок в сыром ключе не превышало

11% (максимально допустимое количество), ошибка в установке фазы должна быть менее 10 %.

Одной из основных проблем квантовой криптографии является то, что до сих пор невозможно создавать чистые однофотонные оптические импульсы. В основном источником света для квантовой криптографии является просто ослабленный аттенюатором луч лазера. Для такого типа света число фотонов в оптическом импульсе есть случайная величина с пуассоновским распределением. Это значит, что некоторые импульсы могут вообще не содержать фотонов, а в других может быть несколько фотонов. Из оптических импульсов с более чем одним фотоном информация может быть подслушана, а для очень слабых импульсов мало отношение сигнала к шуму. Для получения одиночных фотонов в современных волоконно-оптических системах используются импульсы лазерного излучения длительностью 30 пс, длиной волны 1,5 мкм и частотой импульсов 10 кГц.

При увеличении скорости передачи данных в волоконно-оптических квантово-криптографических системах появляются проблемы, которые связаны с детектированием единичных фотонов. В настоящий день многие квантово-криптографические системы работают на низкой частоте, потому что повышение частоты ведет к повышению процента ошибок при детектировании.

Для волоконно-оптической системы квантовой криптографии с фазовым кодированием важно соотношение потерь и коэффициентов разделения оптического сигнала в разветвителях. Неидеальность разделителя и неравные потери оптического излучения в плечах интерферометра Маха-Цендера существенно влияют на видность интерференционной картины.

На рисунке 1 показана система фазового кодирования на одном интерферометре с отражателями. Оптическое излучение лазера делится на два луча пластиной BS1, оба луча, пройдя через фазовые модуляторы $\varphi_А$ и $\varphi_Б$, интерферируют с помощью пластины BS2. В итоге интерференции оптическое излучение поступает на детекторы D1 или D2 в зависимости от внесенной

фазовыми модуляторами разности фаз. Согласно теории интерферометрии видность на детекторе D1 (рис. 1) выражается формулой [3]:

$$V_1 = 2\left(\frac{|r_1||t_2||t_A|}{|t_1||r_2||t_B|} + \frac{|t_1||r_2||t_B|}{|r_1||t_2||t_A|}\right)^{-1},$$

а на детекторе D2 формулой:

$$V_2 = 2\left(\frac{|r_1||r_2||t_A|}{|t_1||t_2||t_B|} + \frac{|t_1||t_2||t_B|}{|r_1||r_2||t_A|}\right)^{-1},$$

где $r_1, r_2, t_1, t_2$ - амплитудные коэффициенты отражения и пропускания разделителей луча $BS_1$ и $BS_2$. $t_A$, $t_B$ - коэффициенты поглощения в плечах интерферометра.

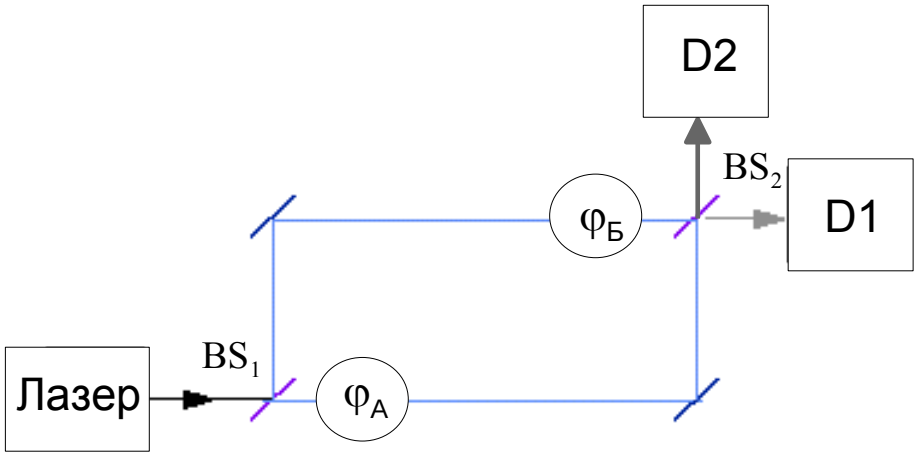


Рис. 1 Система фазового кодирования на одном интерферометре с отражателями.

Делитель $BS_2$ в схеме на рисунке 1 значительно более важен, чем делитель $BS_1$. Если $BS_2$ - идеальный делитель 50:50, то можно достичь единичной видности на обоих детекторах одновременно вне зависимости от несовершенства делителя $BS_1$. Условия достижения единичной видности на

обоих делителях $V_1 = V_2 = 1$ имеют вид:

$$|r_2|^2 = 0,5 \text{ и } \frac{|r_1||t_A|}{|t_1||t_B|} = 1.$$

Если $|r_2|^2 \neq 0,5$, то единичная видность может быть достигнута только на одном из детекторов. Поэтому разделитель оптического пучка, чей коэффициент разделения близок к 50:50 должен быть использован для сведения лучей, то есть в роли $BS_2$.

**Заключение**

В итоге получается, практическая реализация схемы с фазовым кодированием на двух разбалансированных волоконно-оптических интерферометрах Маха-Цендера сталкивается с рядом серьезных проблем. Как показывают расчеты для получения четкой интерференции на выходе системы оба интерферометра должны быть тождественны с точностью до единиц микрометров. В подобной системе будет возникать так же дрейф фазы, который необходимо свести к минимуму путем применения систем температурной стабилизации и компенсации набега фазы. Для приемлемой видности интерференции расщепители излучения на входах и выходах интерферометра должны разделять интенсивность волны пополам.

Решение проблем квантовой криптографии на элементной базе современной волоконной оптики является сложной задачей. Применение интегрально-оптической технологии позволяет создать оптические элементы (разветвители, интерферометры, поляризационные расщепители, фазовые модуляторы, брегговские волноводные отражатели, мультиплексоры) с требуемой точностью геометрических параметров, а также уменьшить размеры устройств, что значительно облегчает и упрощает их термостабилизацию. Хотя в интегрально-оптических волноводах потери излучения выше, чем в волокне, благодаря малым размерам интегрально-оптических устройств их применение в системах квантовой криптографии не требует значительного уменьшения длины квантовой линии связи. Помимо этого, интегрально-оптические схемы с

применением периодически поляризованного ниобата лития позволяют создать источники единичных фотонов и пар фотонов в перепутанных состояниях. Различные протоколы квантовой криптографии требуют построения сложных схем обработки сигналов, что также удобно реализовать на основе единой интегральной схемы.

**Список литературы:**


1. Бауместер Д., Экерт А., Цайлингер А. Физика квантовой информации. – М.: Постмаркет. – 2003. – 253 с.
2. Bennett C., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // J. of Cryptology. – 1992. – № 5 – P. 356-353.
3. Tittel W., Brendel J., Gisin B., Herzog T., Zbinden H., Gisin N. Experimental demonstration of quantum correlations over more than 10 km // Phys. Rev. A. – 1998. – V.57 – P. 3229-3232.