Санкт-Петербургский Государственный Технический Университет
Радиофизический факультет
Кафедра квантовой электроники

Диссертация допущена к защите зав. кафедрой
_____ В.И. Дудкин
"_____"_____ 2000 г.

ДИССЕРТАЦИЯ

на соискание ученой степени

МАГИСТРА

Тема: *Оценка защищённости практической квантово-криптографической системы на основе волоконно-оптических линий связи от несанкционированного доступа*

Направление: 553100 - Техническая физика
Магистерская программа: 553110 - Оптическая физика и квантовая электроника

Выполнил студент гр. 6093 _____ А.В.Вахитов
Руководитель, к.т.н., доц. _____ В.И.Тарханов

Санкт-Петербург

2000

Реферат

В данной работе исследуется новая стратегия несанкционированного доступа к квантово-криптографическим системам, исключающая необходимость прямого взаимодействия с передаваемыми квантовыми состояниями. Это позволяет нарушителю избежать наведения ошибок в передаче, по количеству которых легальные пользователи могут обнаружить его присутствие. В качестве объекта подслушивания рассмотрены волоконно-оптические схемы на фазовых состояниях. Сущность метода состоит в сканировании параметров передающей и/или приёмной аппаратуры путём измерения характеристик отражённых от неё мощных световых импульсов. Указываются границы применимости данного метода. Оценивается вид и количество информации, приобретаемое лицом, осуществляющим несанкционированный доступ, в зависимости от различных параметров сканирующего сигнала и аппаратуры. Предлагаются меры защиты от данного вида атаки. Представлена разработанная схема установки для осуществления модельного эксперимента по подслушиванию, а также результаты успешных предварительных измерений. В работе приведён также короткий обзор литературы по существующим методам, протоколам и схемам квантовой криптографии.

Abstract

The thesis describes a new strategy of eavesdropping on quantum cryptographic systems, which eliminates the need of immediate interaction with transmitted quantum states. It allows the eavesdropper to avoid inducing transmission errors that disclose her presence to the legal users. As an object of the eavesdropping, phase state fiberoptic schemes are considered. In this eavesdropping strategy, parameters of transmitting and/or receiving apparatus are interrogated by external high-power light pulses. Applicability conditions of this method are given. Type and amount of information learned by the eavesdropper is estimated, depending on the parameters of the interrogating pulse and apparatus. The thesis suggests security measures against this kind of attack. Experimental setup for eaveadropping experiment is proposed and results of successful preliminary measurements are presented. Also, the thesis contains a short review of existing methods, protocols and schemes of quantum cryptography.

Оглавление

Введение

Квантовая криптография - весьма динамично развивающаяся ветвь современной криптографической науки, сулящая много новых перспектив в традиционных областях применения - дипломатической связи, военном деле, бизнесе и других областях, требующих передачи секретной информации. В экспериментальных и теоретических работах по квантовой криптографии, проводимых до сегодняшнего дня, рассматривалось множество разнообразных схем и протоколов обмена, а также устойчивость этих схем и протоколов по отношению к различным приёмам несанкционированного доступа. Среди рассмотренных уже приёмов много довольно сложных, практически нереализуемых в рамках технологии обозримого будущего. Однако до самого последнего времени игнорировалась одна из возможных стратегий несанкционированного доступа к информации в квантово-криптографических системах, целиком основанная на эксплуатации паразитных свойств реальных оптических схем, а именно, отражательных потерь оптических компонентов. Оказывается, что при использовании этих свойств, для широкого класса схем квантовой криптографии возможно осуществление доступа к абонентам системы извне, через общий оптический канал, этих абонентов соединяющий, в результате чего успешно обходится часть ограничений квантовой механики, обеспечивающих секретность этих систем. Поэтому насущной задачей является исследование этой стратегии несанкционированного доступа и выработка защитных мер против неё, чему и посвящена данная диссертация.

Задачей настоящей диссертационной работы являлось:

1. Теоретическое исследование стратегии несанкционированного доступа к абонентам через общий оптический канал связи на примере квантово-криптографических систем на основе волоконно-оптических линий связи с использованием протоколов обмена BB84 и B92 на фазовых состояниях.
2. Выработка возможных мер защиты от данного вида атаки.

3. Разработка схемы экспериментальной установки для реализации данной стратегии, а также подготовительные измерения на оптической части квантово-криптографической установки NTNU.

Работа над данной магистерской диссертацией выполнялась на базе Норвежского Университета Науки и Технологии (NTNU) в г. Трондхейм, Норвегия, в рамках ФЦП "Интеграция" (грант № А0147/13.5/778/2000 "Оптика и лазерная физика: развитие фундаментальных проблем квантовой оптики"). Финансирование работы осуществлялось Норвежским Советом по Исследованиям (NFR).

Принципы, протоколы и схемы квантовой криптографии

Введение. История и основополагающие принципы квантовой криптографии

С древнейших времен люди изыскивали способы коммуникации, которые бы обеспечивали сохранение передаваемой информации в тайне от третьих лиц, что было актуально для нужд дипломатии, торговли, военного дела и любовной переписки. Для этого применялись разнообразные виды кодирования информации. Все они обеспечивали секретность передаваемой информации в той или иной мере, однако ни один из них не давал абсолютной защиты. В 1918 г. Вернамом был изобретён шифр, для которого позднее, в конце 40-х гг., было проведено доказательство абсолютной секретности. Условия этой секретности являются, собственно, главным недостатком этого шифра: требуется абсолютно случайный ключ такой же длины, как и передаваемое сообщение, причём использоваться этот ключ должен всего лишь один раз. Следовательно, перед тем, как передать тайное сообщение, нужно вначале передать по каналу, весьма надёжно защищённому от несанкционированного доступа, такой же длины сообщение, содержащее секретный ключ. Такая система оказывается громоздкой, неудобной в использовании и дорогой, из-за чего применяется крайне редко.

В 70-х гг. была изобретена т.н. система криптографии с открытым ключом, в которой существует два ключа: один для зашифровки сообщений, оглашаемый публично, а другой для расшифровки, хранимый в тайне. Данная система используется сейчас практически повсеместно, хотя её секретность так и не была никем строго доказана (как, впрочем, не доказано и обратное). Эта система основана на специального вида функциях, вычисление которых в одном направлении не представляет трудностей, а в обратном - весьма

затруднено. В частности, проблема вычисления секретного ключа при наличии публичного сводится к проблеме факторизации больших чисел, которая считается трудноразрешимой до сегодняшнего времени. Однако, в связи с ожидаемым появлением на свет квантовых компьютеров, для которых уже разработаны алгоритмы быстрой факторизации, системы с публичным ключом могут потерять свою эффективность. Поэтому возникла потребность в криптографических системах, основанных на других принципах.

Работа "Сопряжённое кодирование" [1], которую написал Stephen Wiesner из Колумбийского университета, поначалу мало кем замеченная и даже не опубликованная, положила начало новому направлению в криптографической науке - квантовой криптографии. В ней, благодаря законам квантовой механики, стало возможным распространение между двумя или более абонентами секретного ключа, удовлетворяющего всем требованиям, предъявляемым шифром Вернама, что означает абсолютную секретность передаваемой информации. В 1984 г. Bennett и Brassard запатентовали первый протокол обмена для квантово-криптографической системы, известный как BB84 [2]. С этого момента интерес к квантовой криптографии в мире начал расти чрезвычайно быстро, и на сегодняшний день проведено уже огромное количество исследований, затрагивающих самые различные её аспекты.

По формулировке авторов BB84, квантовая криптография - это метод, позволяющий двум пользователям, не обладающим изначально никакими общими для них секретными данными, договориться о случайном ключе, который будет секретным от третьего лица, осуществляющего несанкционированный доступ к их коммуникациям [3].

В криптографической науке выработалась своя традиционная терминология, несколько специфически звучащая на первый взгляд, однако весьма удобная на практике. Так, легальных пользователей по традиции называют "Алиса" и "Боб", тогда как лицо, осуществляющее несанкционированный доступ, называют "Ева". Мы не будем отступать от канонов и сохраним эту терминологию в настоящей работе.

Главными квантово-механическими принципами, составляющими основу для квантовой криптографии, являются [4]:

1. *Невозможность различить абсолютно надёжно два неортогональных квантовых состояния*

   Произвольное состояние любой двухуровневой квантово-механической системы можно представить в виде линейной суперпозиции её собственных состояний $|0\rangle$ и $|1\rangle$ с комплексными коэффициентами:

   $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

   где $|\alpha|^2 + |\beta|^2 = 1$. Законы квантовой механики не позволяют абсолютно надёжно различить два квантовых состояния

   $|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$

   и

   $|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$,

   если не выполнено $\langle\Psi_1|\Psi_2\rangle = 0$, т.е. состояния ортогональны.

2. *Теорема запрета на клонирование*

   Благодаря унитарности и линейности квантовой механики, невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние. Пусть, например, Алиса и Боб используют для передачи информации двухуровневые квантовые системы, кодируя биты данных состояниями этих систем. Если Ева перехватывает носитель информации, посланный Алисой, измеряет его состояние и пересылает далее Бобу, то состояние этого носителя будет иным, чем при измерении. Таким образом, подслушивание квантового канала наводит ошибки передачи, которые могут быть обнаружены легальными пользователями.

3. *Квантовое запутывание*

   Две квантово-механические системы (даже разделённые пространственно) могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое на одной из систем, определит результат измерения этой величины на другой. Этот эффект называется квантовым

запутыванием. Ни одна из запутанных систем не находится в определённом состоянии, поэтому запутанное состояние не может быть записано как прямое произведение состояний подсистем. Синглетное состояние двух частиц со спином 1/2 может служить примером запутанного состояния:

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

Измерение, проведённое на одной из двух подсистем, даст с равной вероятностью $|0\rangle$ или $|1\rangle$, а состояние другой подсистемы будет противоположным (т.е. $|0\rangle$, если результат измерения на первой системе был $|1\rangle$, и наоборот).

4. *Причинность и суперпозиция*

   Причинность, исходно не являющаяся ингредиентом нерелятивистской квантовой механики, может быть тем не менее использована для квантовой криптографии совместно с принципом суперпозиции: если две системы, состояния которых образуют некую суперпозицию, разделены во времени, не будучи связаны причинностью, то нельзя определить суперпозиционное состояние, проводя измерения на каждой из систем последовательно.

Процесс коммуникации будет рассмотрен подробно на примере протокола BB84, как исторически первого и наиболее популярного в настоящее время. Остальные протоколы будут описаны весьма кратко. Что же касается конкретных схем квантово-криптографических установок, то здесь будут рассмотрены лишь те из них, подслушивание которых является предметом настоящего исследования, а именно, волоконно-оптические схемы, использующие протоколы обмена BB84 и B92 на фазовых состояниях.

Протокол BB84

Первый протокол обмена для квантовой криптографии под названием BB84 [2] изобрели Bennett и Brassard в 1984 году. Он использует для кодирования информации четыре квантовых состояния двухуровневой системы, формирующие два сопряжённых базиса (обозначенных здесь буквенными индексами A и B):

$|0_A\rangle$,

$|1_A\rangle$,

$|0_B\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$,

$|1_B\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle - |1_A\rangle)$.

Здесь состояния $|0_A\rangle$ и $|1_A\rangle$ кодируют значения “0” и "1" в базисе *A*, а $|0_B\rangle$ и $|1_B\rangle$ кодируют те же значения в базисе *B*. Можно представить их как поляризационные состояния частицы со спином 1/2: $|0_A\rangle$ и $|1_A\rangle$ соответствуют горизонтальному (0^0) и вертикальному (90^0) направлениям поляризации, а $|0_B\rangle$ и $|1_B\rangle$ - двум диагональным, а именно $+45^0$ и -45^0 (получаются из $|0_A\rangle$ и $|1_A\rangle$ путём поворота системы координат на 45^0). Два состояния, принадлежащие к одному и тому же базису, являются ортогональными, то есть их можно различить надёжно при условии, что измерения проводятся в том же самом базисе. Однако, измерение в неправильном базисе (т.е., к примеру, попытка определить, какой из двух поляризаций - 0^0 или 90^0 – обладает частица, которая на самом деле поляризована под углом $+45^0$), даст абсолютно случайный результат.

Вначале мы опишем протокол в предположении отсутствия шума в квантовом канале, затем модифицируем описание, принимая шум во внимание. Обмен информацией осуществляется в две стадии: сперва по квантовому каналу, затем

по обычному каналу, открытому для подслушивания (например, через Интернет).

На первой стадии Алиса выбирает случайно и с равной вероятностью одно из четырех квантовых состояний $|0_A\rangle$, $|0_B\rangle$, $|1_A\rangle$, $|1_B\rangle$, и пересылает его Бобу по квантовому каналу, фиксируя в своих записях значение бита данных и базис, в котором он закодирован. Боб производит измерение переданного состояния, в одном из двух возможных базисов A или B, выбранном независимо от Алисы, случайно и с равной вероятностью, также записывая результат измерений и выбранный базис. Если базис, выбранный Бобом для измерения, совпадает с базисом, выбранным Алисой для передачи, то биты данных у Алисы и Боба будут идентичны; в противном случае они совпадут с вероятностью 1/2. Алиса и Боб повторяют эту процедуру N раз, в результате чего каждый из них будет обладать строкой бит длиной N. Так как выбор базисов осуществлялся пользователями случайно и независимо, то примерно в 50% случаев они выберут различные базисы для передачи и детектирования.

На второй стадии Алиса и Боб общаются по открытому каналу, который, однако, должен обладать тем свойством, что Ева не может *изменять* передаваемые между ними сообщения. Алиса и Боб сообщают друг другу использованные ими при передаче значения базисов, и договариваются исключать из своих данных те биты, для которых базисы передачи и детектирования не совпадали. Результирующая строка бит называется сырым ключом.

Представим себе, что Ева осуществляет подслушивание квантового канала, перехватывая носители информации, посланные Алисой, осуществляя измерение их состояния и пересылая их далее Бобу. Эта стратегия носит название “перехват/регенерация”. Будем рассматривать здесь лишь те случаи, в которых Алиса и Боб выбрали одинаковые базисы (остальные биты будут исключены из конечного ключа в любом случае). Поскольку Ева вынуждена выбирать базисы для детектирования случайно и независимо от Боба и Алисы, то приблизительно в 50% случаев базисы Евы и Боба будут не совпадать. При

этом результаты измерений Боба будут случайными, но примерно на 50% совпадающими с данными Алисы. Таким образом, измерения Боба будут давать правильный результат с вероятностью 1/2 + 1/2 * 1/2 = 3/4, в то время как в отсутствие Евы они бы давали правильный результат всегда.

Это означает, что для осуществления теста на присутствие Евы Алиса и Боб должны сравнить публично некоторое случайно выбранное подмножество своих данных (разумеется, не используя затем биты данных из этого подмножества). Если ошибки присутствуют, значит, Ева осуществляла подслушивание; в этом случае полученные данные отбрасываются и процесс передачи начинается с самого начала. Если ошибок нет, оставшиеся биты формируют финальный секретный ключ.

Существует, однако, ещё один способ подслушивания, известный как "расщепление луча". Принципиальная особенность его состоит в том, что Алиса и Боб не в состоянии определить наличие такого рода подслушивания в канале. Известно, что при используемом повсеместно способе получения одиночных фотонов, а именно, ослаблении лазерного излучения до средней интенсивности $\mu \leq 1$ фотона на импульс, определенная доля выходного излучения будет содержать более одного фотона в импульсе (это определяется пуассоновской статистикой, которой подчиняется излучение лазера). Таким образом, поставив на пути фотонов обыкновенный делитель, Ева может получить некоторую информацию о ключе, и не внося ошибок в передачу. Эта возможность учитывается Алисой и Бобом в процессе получения финального секретного ключа: они исключают из своих данных количество бит, соответствующее объёму информации, который может получить Ева в результате выполнения этой атаки.

Сказанное выше для второй стадии имеет силу лишь для идеального, бесшумного квантового канала. Но в реальном канале всегда присутствуют шумы, поэтому некоторое несоответствие в данных Алисы и Боба будет всегда, даже в отсутствие подслушивания. Так как Алиса и Боб не могут различить ошибки, имеющие причиной подслушивание, и ошибки, вызванные

естественными шумами канала, то им приходится предположить, что *все* ошибки передачи вызваны присутствием Евы. При этом стадия обмена по открытому каналу усложняется [3, 27].

Сначала Алиса и Боб извлекают сырой ключ как описано выше, при этом, разумеется, удаляются те битые интервалы, где Бобу не удалось продетектировать частицу вообще (например, из-за неидеального детектора, или из-за несовершенства применяемого способа генерации одиночных фотонов). Надо сказать, что в реальных системах таких интервалов большинство.

Далее Алиса и Боб производят оценку процента ошибок в сыром ключе, публично сравнивая выбранное ими случайно подмножество данных, которое, конечно же, будет исключено из дальнейшего рассмотрения. Если процент ошибок превосходит некоторый заданный уровень, то для Алисы и Боба будет невозможным придти к общему секретному ключу. В этом случае все данные отбрасываются и процесс передачи начинается заново. Если же этот уровень не превышен, то Алиса и Боб переходят к коррекции ошибок.

Целью здесь является удалить все ошибки из сырого ключа и придти к общей, свободной от ошибок кодовой последовательности (которая будет, однако, лишь частично секретной, благодаря тому, что некоторая информация будет утекать к Еве во время самого процесса коррекции). Для начала, Алиса и Боб производят некоторую случайную перестановку своих данных с целью рандомизации положения ошибок. После этого строки разбиваются на блоки длиной l, причём эта длина выбирается так, что вероятность обнаружить более одной ошибки в одном и том же блоке достаточно мала (l выбирается исходя из оцененного процента ошибок в сыром ключе). Для каждого из блоков производится проверка чётности, после чего исключается последний бит каждого из сравниваемых блоков. Если чётности у Алисы и Боба не совпадают, то внутри блока производится бинарный поиск местоположения ошибочного бита, с исключением последних бит сравниваемых субблоков. Найденный ошибочный бит также удаляется. Весь процесс (перестановка, разбиение на

блоки и проверка чётности) повторяется нужное количество раз, после чего производятся те же самые действия, но уже с проверкой чётности в случайно выбранных подмножествах и исключением случайно выбранного бита. Наконец, если ни одной ошибки не было обнаружено в течение некоторого количества последовательных итераций, Алиса и Боб заключают, что с очень высокой вероятностью оставшиеся данные не содержат ошибок.
Как уже сказано выше, данные , оставшиеся после коррекции ошибок, будут только частично секретными. Следующая процедура служит для того, чтобы извлечь из этих данных финальный секретный ключ. Основываясь на проценте ошибок в сыром ключе, определяется максимальное число бит *k*, известное Еве из общего количества оставшихся бит *n*. Пусть также *s* - параметр секретности, значение которого выбирается пользователями произвольно. Алиса и Боб выбирают публично $n - k - s$ случайных подмножеств своих данных. Чётности этих подмножеств они не раскрывают - эти чётности и составляют финальный секретный ключ. Можно показать, что общая информация, которую Ева может иметь о финальном ключе, составляет менее чем $2^{-s}/\ln 2$ бит [2].

Другие протоколы квантовой криптографии

Для большинства протоколов будет описан только процесс обмена по квантовому каналу, так как вторая стадия коммуникации в основном одинакова.

- Протокол B92 [5]

  Введён Беннеттом в 1992 г. Им было показано, что в принципе любые два неортогональных состояния могут быть использованы для квантовой криптографии. Пусть $|\psi_0\rangle$ и $|\psi_1\rangle$ - два неортогональных квантовых состояния, кодирующие биты ”0” и ”1”, соответственно. Их произведение есть $0 < \|\langle\psi_0|\psi_1\rangle\|^2 < 1$. Алиса посылает Бобу случайно выбранное состояние, после чего Боб применяет к нему случайным образом один из двух

несовместимых операторов проектирования:

$P_0 = 1 - |\psi_1\rangle\langle\psi_1|$, или

$P_1 = 1 - |\psi_0\rangle\langle\psi_0|$.

P_0 однозначно уничтожает $|\psi_1\rangle$, но даёт положительный результат с вероятностью $1 - \|\langle\psi_0|\psi_1\rangle\|^2 > 0$ будучи применён к $|\psi_0\rangle$, и наоборот для P_1. Таким образом, результат измерения может быть $|\psi_0\rangle$, $|\psi_1\rangle$ или двусмысленным (нуль может получится в результате воздействия i-того проектора на i-тое состояние, либо же любого проектора на вакуумное состояние - отсутствие фотона, и все эти случаи различить невозможно). На стадии обмена по открытому каналу Алиса и Боб исключают двусмысленные результаты, и после этого, в отсутствие подслушивания, примерно $\left(1 - \|\langle\psi_0|\psi_1\rangle\|^2\right)/2$ их данных будут абсолютно коррелированы.

- Протокол 4+2 [6]

  Этот протокол объединяет идеи из BB84 и B92. Биты "0" и "1" могут быть закодированы в двух базисах, но два состояния внутри одного базиса не ортогональны.

- Протокол с шестью состояниями [8]

  Исходно это тот же самый протокол, что и BB84, но ещё с одним базисом, а именно:

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

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

  В соответствии с этим, существует ещё два возможных направления поляризации для переданного фотона – право- и левоциркулярное.

- Протокол ЭПР [7]

  Экертом был предложен протокол, основанный на квантовом запутывании. Вначале создаётся N максимально запутанных ЭПР-пар фотонов, затем один фотон из каждой пары посылается Алисе, а другой - Бобу. Три возможных

квантовых состояния для этих ЭПР-пар есть [27]:

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

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

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

что может быть записано в общем виде как

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

Последняя формула явно показывает, что каждое из этих трёх состояний кодирует биты "0" и "1" в уникальном базисе.

Затем Алиса и Боб осуществляют измерения на своих частях разделённых ЭПР-пар, применяя соответствующие проекторы

$$P_1 = |0\rangle\langle 0|$$

$$P_2 = \left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|$$

$$P_3 = \left|\frac{3\pi}{6}\right\rangle\left\langle\frac{3\pi}{6}\right|.$$

Алиса записывает измеренные биты, а Боб записывает их дополнения до 1. Результаты измерений, в которых пользователи выбрали одинаковые базисы, формируют сырой ключ. Для остальных результатов Алиса и Боб проводят проверку выполнения неравенства Белла как тест на присутствие Евы (Ева здесь интерпретируется как скрытый параметр).

- Протокол Гольденберга-Вайдмана [9]

  Алиса и Боб используют для сообщения два ортогональных состояния:

  $$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle + |b\rangle\right),$$

  $$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle - |b\rangle\right),$$

  кодирующие биты ”0” and ”1”,соответственно. Каждое из двух состояний

$|\psi_0\rangle$ и $|\psi_1\rangle$ является суперпозицией двух локализованных нормализованных волновых пакетов, $|a\rangle$ и $|b\rangle$, которые Алиса посылает Бобу по двум каналам различной длины, в результате чего они оказываются у Боба в разные моменты времени: волновой пакет $|b\rangle$ покидает Алису только после того, как волновой пакет $|a\rangle$ уже достиг Боба. Для этого можно использовать интерферометр с разной длиной плеч. Боб задерживает своё измерение до того момента, как оба волновых пакета достигнут его. Если время посылки $|a\rangle$ пакета известно Еве, то она способна перехватить информацию, послав Бобу в соответствующий момент времени пакет, идентичный с $|a\rangle$, измерив затем посланное Алисой суперпозиционное состояние и далее послав Бобу волновой пакет $|b\rangle$ с фазой, настроенной согласно результату её измерений. Чтобы предупредить эту атаку, используются случайные времена посылки.

- Протокол Коаши-Имото [10]

  Этот протокол является модификацией предыдущего, но позволяет отказаться от случайных времён передачи путём асимметризации интерферометра, т.е. разбиения света в неравной пропорции между коротким и длинным плечами. Кроме того, разность фаз между двумя плечами интерферометра составляет π. Таким образом, два состояния, кодирующие биты "0" и "1", есть

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

  $|\psi_1\rangle = \sqrt{R}|a\rangle - i\sqrt{T}|b\rangle$,

  где R и T - отражательная и пропускательная способности входного лучерасщепителя, соответственно. В случае асимметричной схемы, когда амплитуда вероятности нахождения фотона в том или ином плече интерферометра зависит от значения передаваемого бита, компенсация за счёт фазы не срабатывает полностью, и при применении Евой вышеописанной тактики существует ненулевая вероятность ошибки детектирования.

Наиболее популярные волоконно-оптические квантово-криптографические системы, использующие протоколы обмена BB84 и B92 на фазовых состояниях

В данном подразделе будут описаны схемы, получившие наибольшее распространение в квантовой криптографии, а именно схема Тауншенда и классический и усовершенствованный варианты схемы "plug-n-play".

- Схема, реализованная Таунсендом [29], состоит из интерферометра Маха-Цендера, включающего в себя передающую часть, приёмную часть и канал передачи, источника одиночных фотонов, представляющего собой лазер с сильным аттенюатором на выходе, и двух детекторов на основе лавинных фотодиодов, стоящих на выходах D0 и D1 (рис.1). Приёмная и передающая части реализованы на двух оптических ответвителях (объединителях) каждая: обычном и поляризационном. Импульсы с лазера Алисы делятся на входном ответвителе и проходят в два плеча интерферометра, в одном из которых (длинном) происходит задержка, а в другом (коротком) - модуляция по фазе в соответствии с передаваемым значением бита и базисом. Сигналы из обоих плеч объединяются на выходном поляризационном объединителе, в результате чего они оказываются разделёнными во времени и по поляризации. Проходя по каналу связи к Бобу, при помощи входного поляризационного делителя импульс, прошедший у Алисы длинное плечо, направляется у Боба в короткое, и наоборот. На выходном объединителе происходит интерференция, в результате которой, если передавался бит "1", сигнал возникает на выходе D1, а если "0", то на D0.
- Классический вариант схемы "plug-n-play", реализованный впервые Женевской группой [11,13], изображён на рис. 2. Принцип работы схемы заключается в интерференции двух слабых импульсов, сдвинутых по фазе относительно друг друга. Фазы импульсов меняются Алисой и Бобом. Конструктивная интерференция вызовет отсчёт в детекторе Боба; таким

образом, независимый выбор фаз пользователями может эффективно транслировать информацию между ними.

Последовательность работы схемы такова:

1. Лазер Боба излучает импульс.
2. На делителе C1 импульс разделяется на два импульса P1 и P2. Первый из них проходит напрямую в канал передачи, а второй - после отражения на фарадеевых зеркалах FM1, FM2.
3. Когда импульс P1достигает PIN-детектора D_A, последний включает фазовый модулятор Алисы PM_A, который вносит фазовый сдвиг в импульс P_2.
4. Оба импульса отражаются на фарадеевском зеркале FM3, и ослабляются аттенюатором A до однофотонного уровня.
5. Когда импульсы вновь достигают делителя C1, часть импульса P1 отражается на зеркале FM2 и проходит через фазовый модулятор Боба PM_B, где приобретает соответствующий фазовый сдвиг.
6. Импульс P2 с фазовым сдвигом от Алисы интерферирует на C1 с импульсом P1, содержащим фазовый сдвиг от Боба.

Интерференция будет конструктивной или деструктивной, если разность фаз между импульсами будет равна 0 или π соответственно. В каждом случае конструктивной интерференции, вызвавшей отсчёт в детекторе Боба, значение сдвига фазы на модуляторе сохраняется как очередной бит данных. Достоинство схемы заключается в простоте её настройки и отсутствии необходимости постоянной подстройки по ходу работы. Так как оба импульса проходят один и тот же путь, интерферометр автоматически оказывается выровненным. Благодаря наличию фарадеевских зеркал, поляризация каждого из этих импульсов подвергается строго определённой и взаимно противоположной эволюции на всём пути прохождения сигнала. Таким образом, видность интерференции всегда остаётся максимальной.

- В статье [12] Женевской группой описан усовершенствованный вариант схемы "plug-n-play" (рис. 3). Он содержит всего одно фарадеевское зеркало,

и по сравнению с классическим вариантом позволяет уменьшить количество ложных отсчётов детектора, вызванных переотражениями излучаемого сигнала. В этой схеме использовался протокол BB84. Отличие схемы состоит в том, что импульсы P1 и P2 разделяются по времени и по поляризации при помощи интерферометра с неравной длиной плеч, образуемого делителем C1 и поляризационным делителем PBS, в то время как в классической схеме разделение по времени осуществляется с помощью двух зеркал Фарадея.

Рис.1. Схема Тауншенда

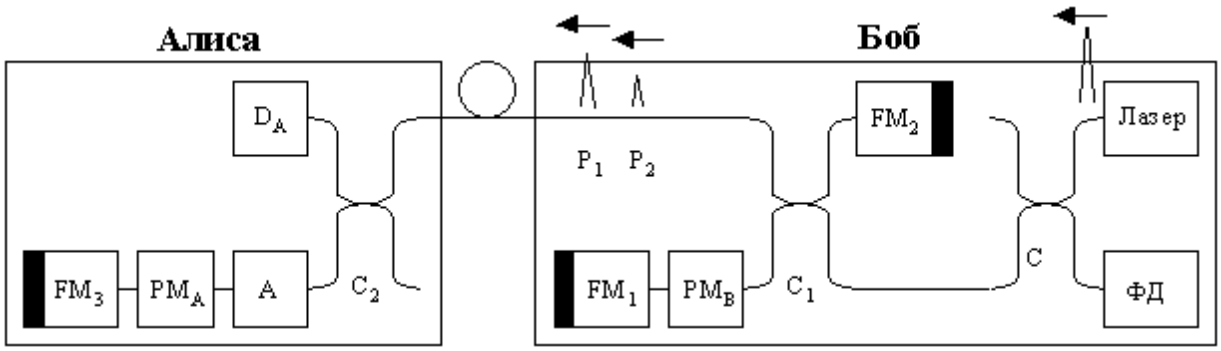

Рис.2. Классическая схема "plug-n-play"

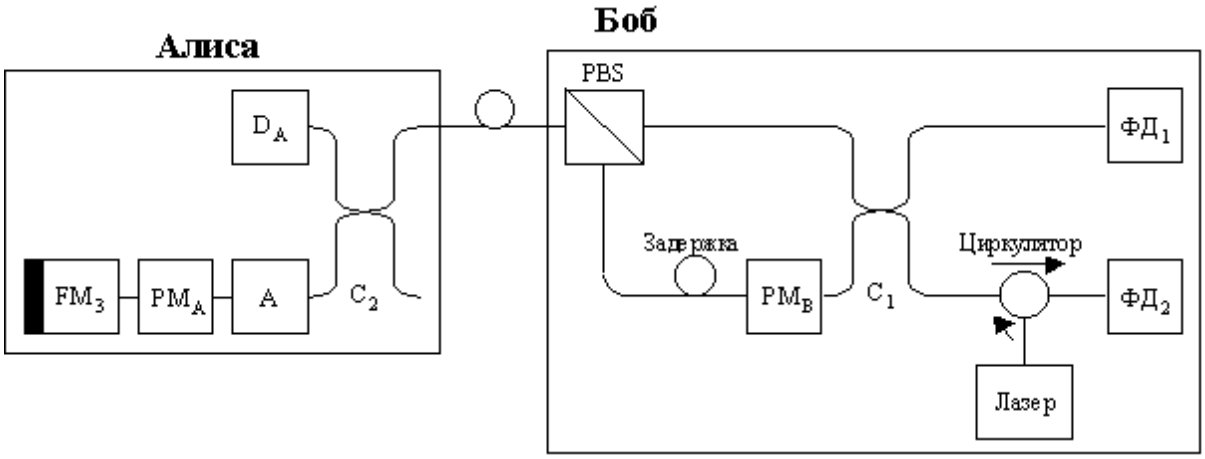

Рис.3. Усовершенствованная схема "plug-n-play"

Способ несанкционированного доступа к абонентам через общий оптический канал связи и возможные меры противодействия

Границы применимости

За последние 10 лет проведено множество исследований по квантовой криптографии [14-20], где доказана её теоретическая устойчивость против многих видов атак, включая такие сложные и нереализуемые на сегодняшний день их разновидности, как, например, когерентные атаки, которые оперируют сразу всеми передаваемыми по квантовому каналу состояниями как единым целым. Обозначены также практические границы этой устойчивости для случая неидеальной среды и аппаратуры [15,17,19,20]. Все эти атаки объединяет то, что для осуществления подслушивания измерительная аппаратура Евы каким-либо образом взаимодействует с передаваемыми квантовыми состояниями. Оказывается, однако, что существует возможность подслушивать эти схемы, и не прибегая к такому взаимодействию, т.е. возможность определить переданную кодовую последовательность либо не имея дела с квантовыми состояниями вообще, либо детектируя их однозначно при помощи некоторой дополнительной информации, почерпнутой во время передачи.
Существует разумная традиция в исследованиях по квантовой криптографии, когда возможности Евы предполагаются ограниченными только лишь законами физики, но не текущим уровнем развития технологии. Мы будем предполагать это в настоящей работе, хотя можно показать, что все актуальные атаки этого вида могут быть реализованы на основе технологий сегодняшнего дня. Мы также даруем Еве исчерпывающее знание структуры передающего и приёмного интерферометров, а также временных диаграмм их работы. Цель данной работы состоит не в подробном описании всех технических деталей

экспериментальной реализации подобной атаки, а лишь в демонстрации её принципиальной возможности и описании главных особенностей.

Все существующие квантово-криптографические системы могут быть разделены на два класса по их подходу к формированию квантовых состояний, составляющих квантовый алфавит. В первом классе формирование квантовых состояний происходит за счёт модуляции какого-либо параметра (например, поляризации или фазы) проходящего света в рамках фиксированного множества значений. Для этого могут использоваться фазовые модуляторы или ячейки Поккельса. Другой класс схем использует различные источники света для формирования различных квантовых состояний; кроме того, здесь можно упомянуть схемы с генерацией запутанных пар без модуляции второго фотона и вероятностным его детектированием.

В реальной квантово-криптографической системе всегда будет присутствовать такое явление, как отражательные потери оптических компонентов. Это составит основу для предлагаемого метода несанкционированного доступа. Представим, что Ева посылает сканирующий импульс относительно большой интенсивности внутрь передающего интерферометра. Часть этого импульса, отражённая от какого-либо из оптических компонентов, возвратится назад. Если внутри передающего интерферометра есть модулятор, тогда сканирующий импульс до и после отражения может пройти через него (и оказаться промодулированным) один или несколько раз. Детектирование отражённого импульса даст Еве некоторую информацию об установках модулятора и, следовательно, о переданных квантовых состояниях. Отсюда следует, что лишь те квантово-криптографические схемы, которые принадлежат к первому классу (т.е. с внутренней модуляцией), подвержены данному виду атаки.

В качестве объекта несанкционированного доступа в настоящей работе будет рассмотрен лишь наиболее распространённый тип квантово-криптографических систем - волоконно-оптические схемы, использующие протоколы обмена BB84 и B92 на фазовых состояниях.

Цикл передачи. Временные параметры схем

Рассматриваемые нами схемы используют фазовые модуляторы, управляемые напряжением, для формирования квантовых состояний. Типичная осциллограмма управляющего напряжения фазового модулятора представлена на рис.4.

Здесь τ_{rf} - максимальное из времён нарастания и спада импульса управляющего напряжения модулятора, τ_{set} - время установления управляющего напряжения с требуемой точностью, τ_{bit} - интервал передачи бита данных, и $\tau_i = \tau_{rf} + \tau_{set} + \tau_{bit}$ - продолжительность цикла передачи одного бита. $\Phi(j)$ и $\Phi(j+1)$ - фазовые сдвиги, кодирующие биты данных в j-том и (j+1)-ом циклах передачи, $V_c(j)$ и $V_c(j+1)$ - управляющие напряжения, соответствующие этим фазовым сдвигам. Обозначим за τ_R время, за которое сканирующий импульс проходит расстояние от фазового модулятора до некоторого отражающего компонента в передающем интерферометре (см. рис.5).

Будем предполагать для удобства, что управляющее напряжение не меняется во время прохождения сканирующего и отражённого импульсов через модулятор, и что сам модулятор работает одинаково в обоих направлениях. Реально всегда присутствуют некоторые (как правило, медленные по сравнению со временем прохождения импульсами модулятора) колебания управляющего напряжения в течение цикла передачи, но они обычно относительно малы по амплитуде и могут привести к фазовой ошибке порядка 10-20 градусов, что терпимо для Евы, поскольку она использует многофотонные сигналы. Для передающей и приёмной стороны, однако, точность установки фазового сдвига в модуляторах должна быть порядка 5-10 градусов для эффективного детектирования.

Одиночный сканирующий импульс, посланный Евой, вызовет множество отражённых сигналов с различными амплитудами, задержками и фазами, и все они в разной степени пригодны для успешного выполнения данной атаки. Амплитуда отдельного отражённого сигнала определит возможность его успешного детектирования, а задержка во времени и фазовый сдвиг определят,

какой информацией будет обладать Ева после детектирования - непосредственно битом данных или базисом передачи. Мы будем рассматривать только сканирующие сигналы, промодулированные дважды во время их прохождения внутри передающего интерферометра, а $2\tau_R$ в этом случае будет обозначать задержку между последовательными актами модуляции.

Доступ к передающей части

Общая схема

Общая схема доступа с передающей стороны показана на рис.6. Импульсы, излучаемые лазером, делятся на разветвителе на сканирующий и опорный импульсы. Сканирующие импульсы проходят к передающему интерферометру через оптический мультиплексор, отражённые сигналы проходят через тот же самый мультиплексор и разветвитель в детектирующую схему. Опорные импульсы, используемые для детектирования фазы, задерживаются во времени так, что они приходят в детектор одновременно с отражёнными сканирующими импульсами. Конкретное содержание схемы детектирования зависит от того, какую информацию хочет иметь Ева: биты данных или базисы передачи. Оптический мультиплексор необходим здесь для того, чтобы данные, посланные легальными пользователями, проходили без искажений от передатчика к приёмнику. Использование мультиплексирования во временной области может быть сопряжено с проблемой рэлеевского рассеяния: если информационный и сканирующий импульсы встречаются где-либо на пути, то некоторое количество рассеянного света от сканирующего импульса может проникнуть в приёмный детектор, что чревато ошибками детектирования, наведения которых Ева должна избегать. Использование сканирования на другой длине волны и, соответственно, мультиплексирования по длине волны

значительно уменьшит влияние этого эффекта.

Косвенное детектирование бит данных

Рассмотрим сканирующий импульс, промодулированный один раз после входа в передающий интерферометр и один раз после отражения внутри него, так что акты модуляции происходят в пределах временных интервалов τ_{set} или τ_{bit} двух соседних циклов передачи (см. рис.7).

Параметр τ_R выбранного отражённого импульса должен удовлетворять условию:

$\tau_{rf} < 2\tau_R < 2\tau_i - \tau_{rf}$

Неравенство выше содержит τ_{rf}, поскольку импульс не должен проходить модулятор во время интервалов нарастания или спада управляющего напряжения. Если это удовлетворено, то полный фазовый сдвиг, полученный сканирующим сигналом, будет равен сумме фазовых сдвигов в двух соседних циклах передачи:

$$\Phi_E = (\Phi(j) + \Phi(j+1)) \bmod 2\pi$$

Заметим, что Φ_E будет равно одному из возможных значений фазового сдвига, кодирующих биты данных в используемом протоколе обмена (для простоты ограничимся рассмотрением случая, когда сканирование производится на той же длине волны, что и передача сигнала в системе; отказ от этого предположения лишь несколько усложнит детектирование). Детектирование этого фазового сдвига не даст Еве однозначного результата, поскольку ей неизвестно значение фазы в первом интервале передачи. Но эта фаза может приобретать лишь фиксированное множество значений, а именно 4 для протокола BB84 и 2 для протокола B92. Это означает, что Ева должна определить правильную кодовую последовательность методом подбора всего из четырёх или даже из двух вариантов, что на практике равносильно знанию Евой кода. Иллюстрация к косвенному детектированию бит данных приведена в табл.1. В случае, если два последовательных акта модуляции отделены друг от друга количеством циклов передачи n, то количество возможных вариантов

кодовой последовательности есть 4^n для протокола BB84 и 2^n для протокола B92.

Детектирование базисов передачи (только для протокола BB84)

Секретность рассматриваемых квантово-криптографических схем определяется тем фактом, что Ева не знает базисов, в которых кодируются биты информации во время передачи. Если же Еве каким-либо образом удаётся узнать значения базисов пока передающиеся квантовые состояния находятся в её распоряжении, то вся секретность схемы исчезает, и оказывается, что Ева способна реализовать идеальную атаку типа “перехват/регенерация”, не будучи обнаруженной легальными пользователями.

Рассмотрим сканирующий импульс, промодулированный один раз после входа в передающий интерферометр и один раз после отражения внутри него, так что оба акта модуляции происходят в интервале времени τ_{set} и/или τ_{bit} одного и того же цикла передачи (рис.8). Параметр τ_R выбранного отражённого импульса должен удовлетворять условию:

$\tau_{rf} < 2\tau_R < \tau_i$

Тогда фазовый сдвиг, приобретённый сканирующим импульсом, будет равен удвоенному значению фазы в данном цикле передачи:

$$\Phi_E = 2\Phi(j) \bmod 2\pi$$

Легко видеть, что результирующее значение фазы будет определяться базисом передачи: $\Phi_E = 0$ если $\Phi(j) = 0$ или π, и $\Phi_E = \pi$, если $\Phi(j) = \pi/2$ или $3\pi/2$.

В реальности атака с детектированием базисов может оказаться значительно сложнее, чем косвенное детектирование бит данных. Откажемся на время от предположения о "всемогущей" Еве. Предположим, что Ева использует для перехвата и дальнейшей пересылки информации (закодированной в известных ей базисах) устройства, идентичные с приёмным и передающим интерферометрами Алисы и Боба (иначе говоря, она не имеет преимущества в технологии). Тогда из-за инерционности фазовых модуляторов, а точнее, невозможности мгновенно выставить правильное управляющее напряжение на

них, Ева ограничена во времени. Поэтому, чтобы корректно продетектировать переданную информацию, Ева должна знать значение базиса как минимум за $\tau_{rf} + \tau_{set}$ до прихода информационного импульса. Более того, Ева должна располагать дополнительно тем же самым интервалом времени $\tau_{rf} + \tau_{set}$, чтобы перехваченная и пересланная далее информация достигла Боба в определённое время (так как передатчик Алисы и приёмник Боба синхронизированы). Имея дело с оптоволоконными квантово-криптографическими системами, Ева может использовать РЧ сигналы, чья групповая скорость в воздухе превышает примерно в полтора раза групповую скорость оптических сигналов в оптоволокне. Детектор базисов помещается где-либо в непосредственной близости от передатчика Алисы, а информационный детектор Евы - на таком расстоянии от детектора базисов, чтобы информация, посланная детектором базисов на радиочастоте, достигала местоположения Евы на $\tau_{rf} + \tau_{set}$ ранее, чем информационные импульсы Алисы. "Регенератор" Евы, в свою очередь, ставится на таком расстоянии от её информационного детектора, что РЧ импульсы, несущие информацию о значениях бит данных и базисов, достигали бы его на $\tau_{rf} + \tau_{set}$ ранее, чем информационные импульсы Алисы.
Обозначим за τ_{out} разницу во времени между отражённым сканирующим импульсом и информационным импульсом (она, разумеется, может принимать и отрицательные значения), v_{RF} и v_L – групповые скорости соответственно РЧ сигналов в воздухе и оптических сигналов в волокне. Тогда необходимое расстояние между детектором базисов и приёмником информации будет равно

$$D_1 = \frac{\tau_{rf} + \tau_{set} - \tau_{out}}{1/v_L - 1/v_{RF}}.$$

Подобным же образом, дистанция между приёмником и передатчиком Евы будет равна

$$D_2 = \frac{\tau_{rf} + \tau_{set}}{1/v_L - 1/v_{RF}}.$$

Схема доступа для этого случая приведена на рис.9.

Доступ к приёмной части

Косвенное детектирование бит данных возможно в рамках протокола B92 таким же образом, как и с передающей стороны. Можно также детектировать базисы передачи в рамках протокола BB84 (поскольку фазовый модулятор Боба обеспечивает 2 возможных значения фазы - 0 и $\pi/2$, которые соответствуют двум различным базисам). Успешная атака типа “перехват/регенерация” возможна здесь в случае, когда отражённый сканирующий импульс покидает приёмный интерферометр перед тем, как переданный носитель информации войдёт внутрь него, иначе информация о базисе станет доступной Еве уже после того, как носитель информации будет уже вне её распоряжения. Таким образом, должно быть удовлетворено следующее условие:

$2(\tau_{PM} + \tau_R) < \tau_i$,

где τ_{PM} -это время требуемое оптическому импульсу для того, чтобы пройти от входа в приёмный интерферометр до фазового модулятора, а остальные символы определены ранее. Временная диаграмма, поясняющая это требование, помещена на рис.10.

Следует отметить, однако, что даже если вышеуказанное неравенство не удовлетворено, Ева может тем не менее почерпнуть некоторую дополнительную информацию, используя детектирование базисов. Представим, что Ева производит обыкновенную атаку типа "расщепление луча". Типичное рассуждение здесь выглядит следующим образом [21]:

«Пускай Ева отделяет часть *f* энергии каждого из импульсов, среднее число фотонов в которых равно μ. Тогда она получит часть $(1-e^{-f\mu})$ от общего числа импульсов, или ~$f\mu$ для малых значений $f\mu$. Таким образом, эта атака даст Еве порцию $f\mu/2$ исправленного ключа, т.к. она вынуждена использовать случайные значения базисов для детектирования. Можно обойти это ограничение, если Ева способна хранить фотоны до фазы открытого обмена,

однако эта фаза всегда может быть задержана на время, достаточное для затухания большинства сохранённых фотонов».

Но если задержки τ_{PM} и τ_R в приёмном интерферометре таковы, что Ева получает информацию о базисах сразу или через короткое время после того, как информационные импульсы достигают её местоположения, она может просто задержать их на это время и затем продетектировать корректно. Таким образом, при учёте возможности детектирования базисов оценка $f\mu/2$ становится неприменимой, и следует предполагать, что Еве, использующей расщепление луча, доступна порция $f\mu$ переданной информации.

Меры защиты

Для защиты от детектирования базисов с приёмной стороны можно предложить увеличение задержки сигнала в приёмном интерферометре, так что

$$2(\tau_{PM} + \tau_R) > \tau_i$$

Кроме этого, возможно применение однонаправленных оптических вентилей на выходе передающей схемы и на входе приёмной, однако *сам по себе* такой вентиль лишь увеличит требуемую мощность сканирующего импульса, не устраняя опасности, т.к. имеет конечное ослабление, причем лишь в одном направлении. Более того, для схем типа “plug-n-play” этот метод не подходит вообще, поскольку принципом их работы основан на двунаправленности.

Существует ещё одна, вообще говоря, полумера для защиты Алисы, заключающаяся в постановке аттенюатора на выходе передающего интерферометра. Дело заключается в следующем. Источник одиночных фотонов для передатчика делается путём ослабления лазерных импульсов до средней интенсивности порядка 0.1 фотона на импульс. Аттенюатор помещается непосредственно после на выходе лазера или же на выходе приёмника, однако нет никаких видимых причин для того, чтобы предпочесть первый способ второму. А для Евы присутствие аттенюатора на выходе

приёмника будет означать значительное увеличение требуемой мощности лазера (а именно, при значении выходного коэффициента ослабления *A* дБ требуемая мощность сканирующего лазера возрастёт на *2A* дБ). Рано или поздно при больших значениях интенсивности сканирующих импульсов станет заметным вредный эффект от рэлеевского рассеяния, упомянутый выше, а также возможно возникновение нелинейных эффектов. По-видимости, применение такого аттенюатора *вкупе* с однонаправленным вентилем может дать приемлемую степень защиты.

Но самой надёжной мерой является измерение входящей оптической мощности в передающем и приёмном интерферометрах для предупреждения легальных пользователей о несанкционированном проникновении в канал. Поскольку для Евы имеется также достаточно широкий выбор длин волн, на которых может осуществляться сканирование (он определяется диапазоном эффективной работы фазового модулятора), то было бы правильно использовать узкополосные чувствительные детекторы вместе с полосовыми фильтрами на выходе передатчика и входе приёмника, вместо широкополосных измерителей оптической мощности.

Замечания по конкретным схемам

Описываемая стратегия подслушивания, в принципе, приложима и ко многим другим схемам квантовой криптографии, не рассматриваемым в настоящей работе. Следует только сделать поправку на способ формирования квантовых состояний, кодирующих биты данных (это могут быть, например, поляризационные состояниях [3,22], или фазовые состояния в боковых полосах фазомодулированного сигнала [23,24]) и соответствующие изменения в приёмной и передающей аппаратуре. Надо отметить, что в схемах, где каналом передачи является открытый воздух [3,22], Ева не может воспользоваться

преимуществом высокой групповой скорости распространения радиочастотных сигналов (см. пункт "Детектирование базисов передачи").
Можно сделать замечание по поводу схем типа "plug-n-play".
Эти схемы потенциально весьма уязвимы по отношению к рассматриваемому виду несанкционированного доступа из-за их исходной "отражательной" природы (Фарадеевские зеркала). По-видимому, из-за этого исследуемая проблема была замечена именно в связи с данными системами. Женевской группой было коротко упомянуто в [12], что детектор в "передающей" схеме должен обеспечивать измерение входящей оптической мощности. Это защищает от косвенного детектирования бит данных, но даже при таком усовершенствовании схема остаётся беззащитной против детектирования базисов с приёмной стороны и, следовательно, успешных атак типа “перехват/регенерация” и "расщепление луча"; более того, при применении протокола B92 становится возможным косвенное детектирование бит данных с приёмной стороны. Bethune и Risk из IBM рассматривали проблему более детально в их недавней работе [21], но также не уделили внимания возможности доступа с приёмной стороны.

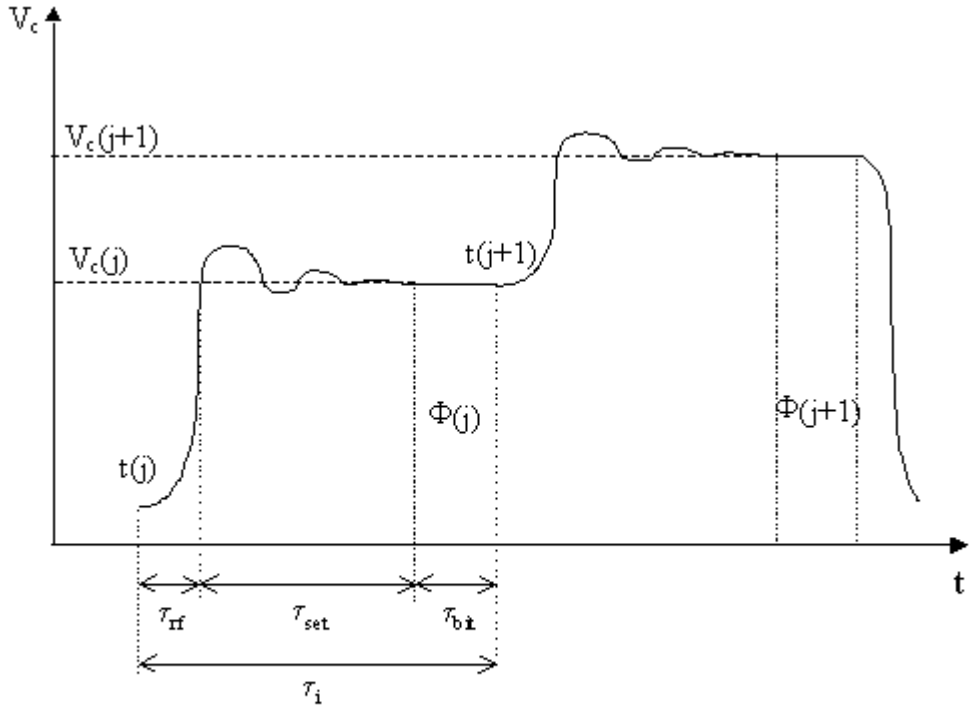

Рис.4. К определению временных параметров

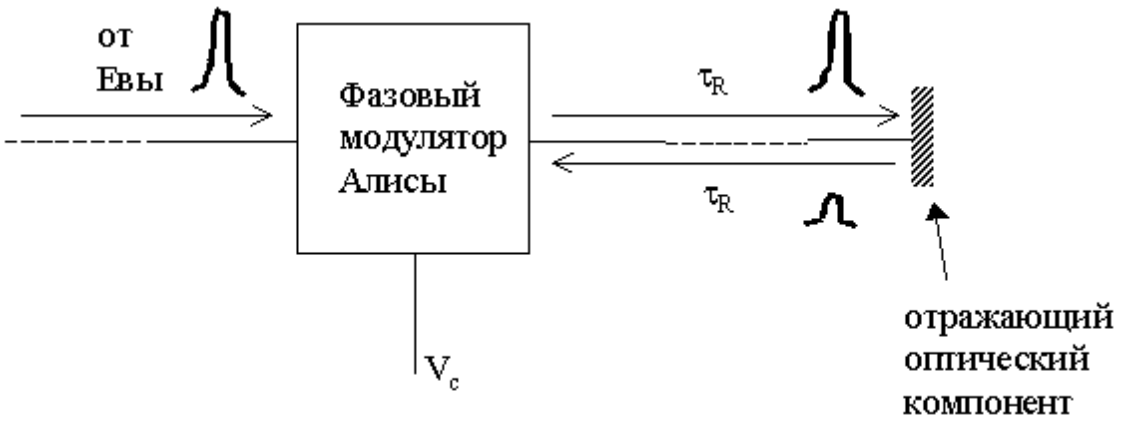

Рис.5. Параметр τ_R

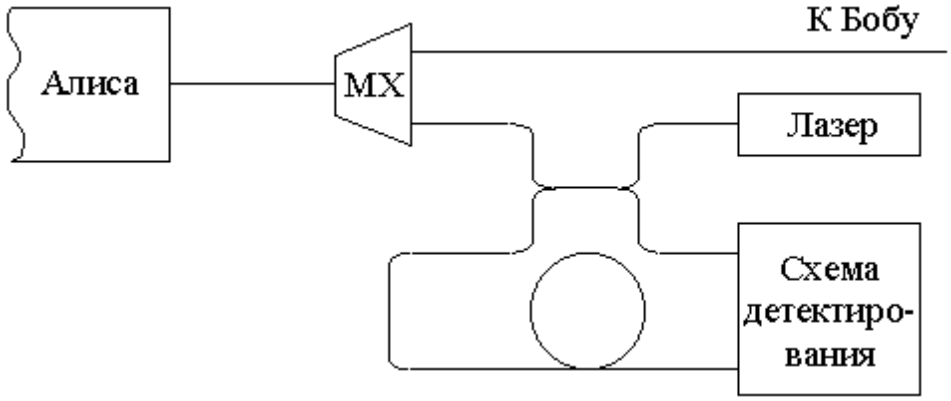

Рис.6. Общая схема доступа к передающей части

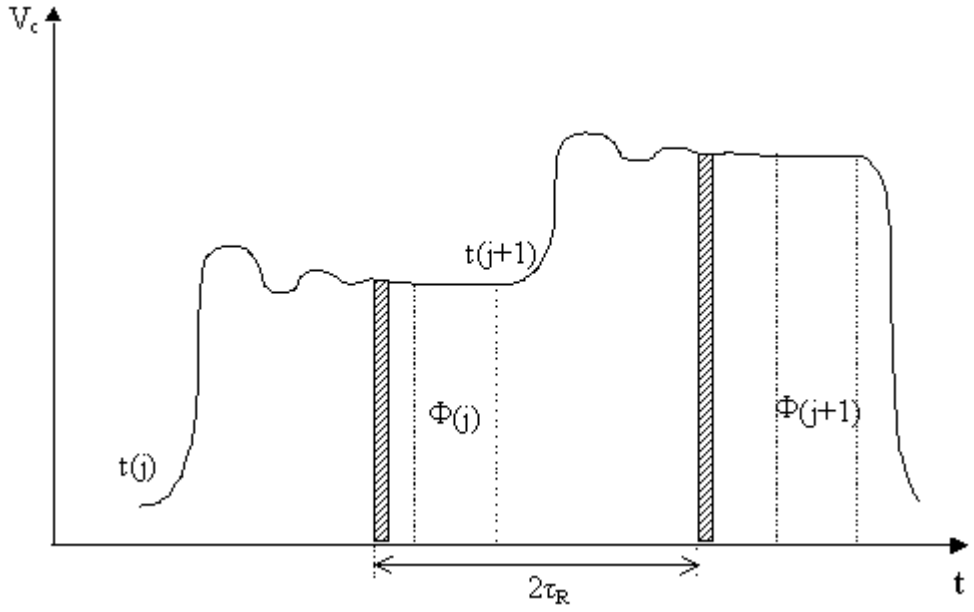

Рис.7. Косвенное детектирование бит данных

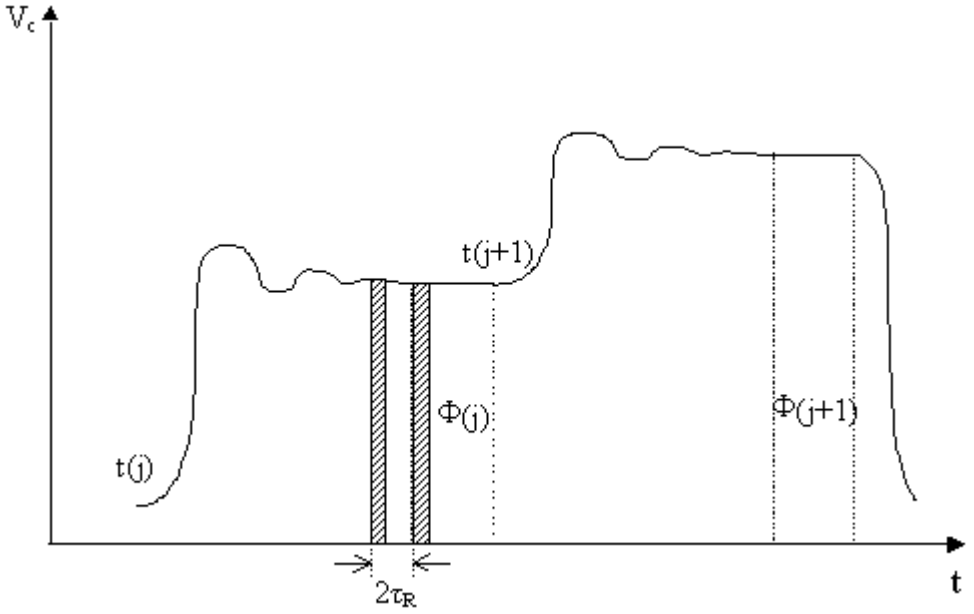

Рис.8. Детектирование базисов передачи

Данные Алисы	1	0^*	0	1	1^*
Фазовые сдвиги Алисы	π	**π/2**	**0**	π	**3π/2**
Фазовые сдвиги, продетектированные Евой	-	3π/2	π/2	π	π/2
Возможные варианты ключа	0?	3π/2	π	0	π/2
	π/2?	π	3π/2	3π/2	π
	3π/2?	0	π	0	π/2
	π?	**π/2**	**0**	π	**3π/2**

Таблица 1. Косвенное детектирование бит данных (доступ с приёмной стороны, протокол BB84)

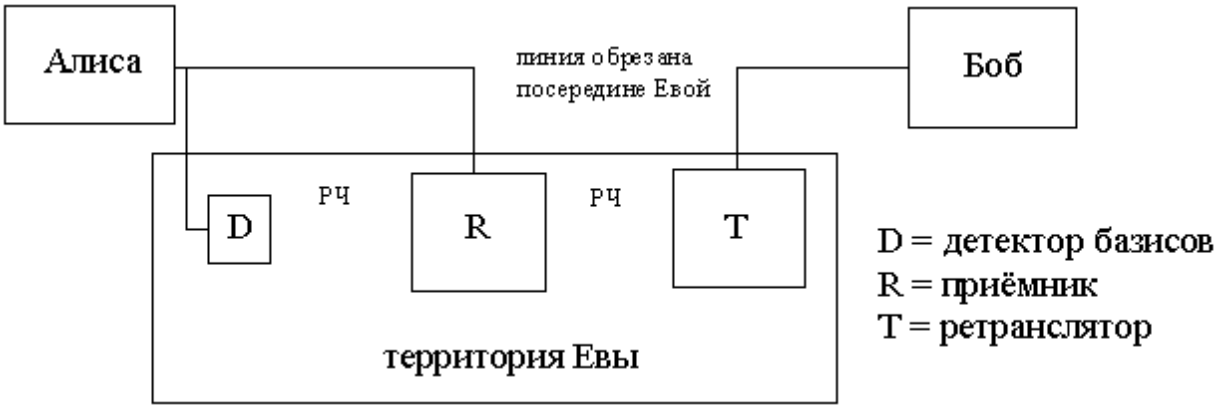

Рис.9. Атака с детектированием базисов в случае Евы, ограниченной технологически.

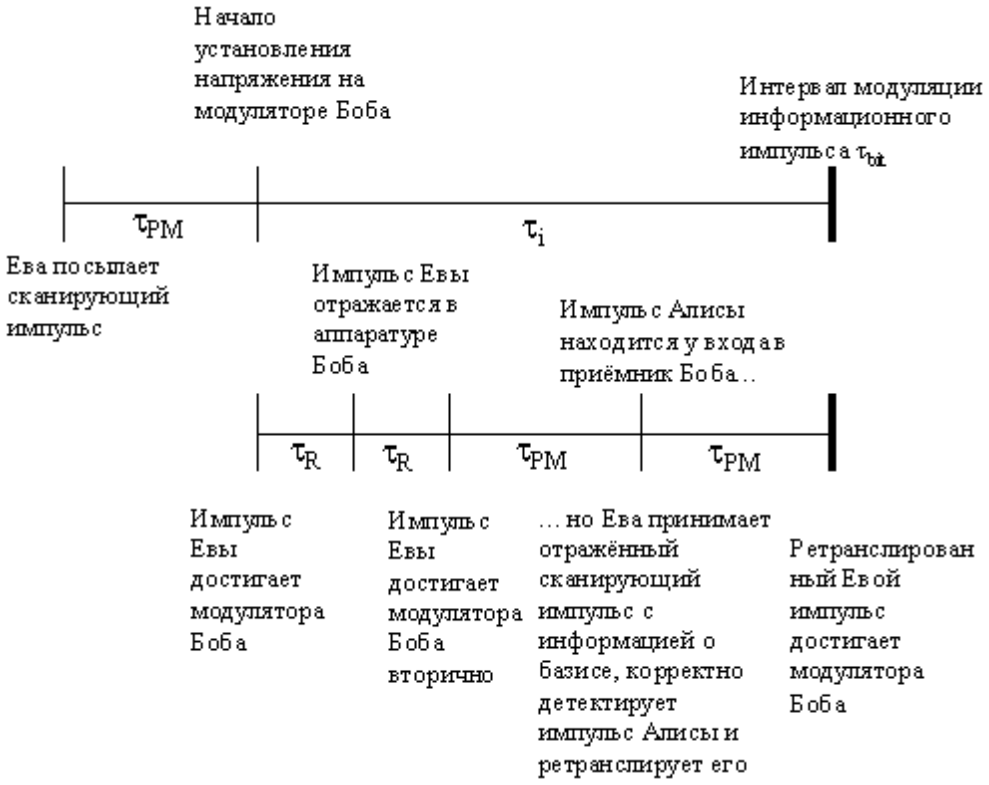

Рис.10. Детектирование базисов на приёмной части (временная диаграмма).

Описание экспериментальной установки и методики измерений

Исходные соображения

Поскольку настоящая стратегия взлома основана на отражательных потерях оптических компонентов, было бы неплохо знать типичные значения этих потерь для различных компонентов. Эти данные приведены в табл. 2 [26]. Легко видеть, что наилучшие результаты могут быть достигнуты на отражениях от лазеров, детекторов, ответвителей, волоконно-оптических (не угловых) коннекторов, свободных концов волокна.

Выбор конкретного отражения для осуществления взлома определяется следующими критериями:

1. Пригодность данного сигнала в смысле временных характеристик (сканирующий импульс должен быть промодулирован в сумме два раза в течение периодов времени, определяемых типом информации, которую хочет получить Ева - базисы передачи или биты данных).
2. Возможность детектирования данного сигнала с заданной вероятностью ошибки. Вероятность ошибки детектирования связана с квантовой эффективностью детектора, скоростью передачи информации, используемой длиной волны и мощностью отражённого сигнала. Конкретный вид этой связи определяется видом принимаемого сигнала, который с точки зрения теории оптической связи можно идентифицировать [25] как синхронный фазоманипулированный сигнал (synchronous PSK signal) для случая детектирования базисов, и как асинхронный дифференциальный фазоманипулированный сигнал (asynchronous DPSK signal) для случая косвенного детектирования бит данных (в обоих случаях применяется гомодинное детектирование). Обращая известные в теории оптических

телекоммуникаций формулы [25] для вероятности ошибки передачи, получим требование на минимальную среднюю интенсивность сигнала:

- для случая детектирования базисов

$$\bar{I} = \frac{h\nu B}{2\eta}\left[erfc^{-1}(2BER)\right]^2;$$

- для случая косвенного детектирования бит данных

$$\bar{I} = -\frac{h\nu B}{2\eta}\ln 2BER,$$

где h - постоянная Планка, ν - несущая частота, B - скорость передачи данных, η - квантовая эффективность детектора Евы, BER - вероятность ошибки передачи.

При осуществлении максимально приближенного к реальным условиям эксперимента по классическому оптическому подслушиванию неизбежно встаёт проблема временного дрейфа поляризации и фазы в канале передачи, в связи с чем необходимо включение в схему петель автоподстройки фазы и поляризации.

Что касается мощности сканирующего лазера, которая определяется величиной потерь на отражение выбранного Евой для работы оптического компонента и потерь на пропускание устройства в целом (приёмника или передатчика), то в данный момент являются коммерчески доступными импульсные волоконно-оптические лазеры мощностью порядка 1-10 кВт в импульсе [28]. Очевидно, вопрос стоит уже в лучевой стойкости используемых оптических компонентов и нелинейных эффектах, наводимых оптическими импульсами такой мощности.

Схема планируемого модельного эксперимента

Исследовательской группой NTNU в рамках проекта "Квантовая криптография" запланировано проведение модельного эксперимента по несанкционированному доступу к абонентам через общий оптический канал

связи с детектированием базисов передачи в рамках протокола BB84 с передающей стороны. Схема модельного эксперимента представлена на рис.11. Воссоздавать полностью реальную ситуацию с подслушиванием в модельном эксперименте признано непрактичным, поскольку конечной целью является не подслушивание, а разработка эффективной защиты, поэтому сделаны следующие упрощения:

1. Из самой криптографической установки используется лишь часть оптического оборудования, относящаяся к Алисе, причём из электроники задействуется только фазовый модулятор. Таким образом, в эксперименте реальная передача информационного сигнала не осуществляется. В связи с этим отпадает надобность в оптическом мультиплексоре.
2. Исключён из схемы аттенюатор, стоящий обычно на выходе передающего интерферометра, по причине отсутствия в нашем распоряжении мощного импульсного лазера для сканирования (используется лазер средней мощности из оптического рефлектометра: Opto-Electronics PPL-30K, 40-пс импульсы с пиковой мощностью порядка 75 мВт).
3. Проблема дрейфа поляризации и фазы решается путём виброизоляции (оптический стол, гасящий вибрации) и теплоизоляции (слои поролона) всей схемы.

Измеряемой величиной является вероятность ошибки детектирования и её экспериментальная зависимость от скорости передачи данных и интенсивности отражённого сигнала. Теоретическое предсказание для этих зависимостей можно сделать по приведенным выше формулам для средней интенсивности сигнала. Идея эксперимента сводится к следующему. Генератор А осуществляет импульсную модуляцию излучения сканирующего лазера и выдаёт синхроимпульсы на компьютер. Через временной интервал, необходимый для прохождения импульсами расстояния от лазера до фазового модулятора, компьютер выдаёт на ЦАП, выход которого соединён через преобразователь $Пр_1$ с управляющим входом фазового модулятора, случайно выбранное число из четырёх возможных вариантов (-1, 0,

1, 2), что соответствует выходным напряжениям (-4В, 0В, +4В, +8В), т.е. фазовым сдвигам на модуляторе ($-\frac{\pi}{2}$, 0, $\frac{\pi}{2}$, π) и значениям базисов передачи (1, 0, 1, 0). Компьютер осуществляет счёт поступающих на него синхроимпульсов. Синхроимпульсы с генератора А поступают также через линию задержки на генератор Б, стробирующий детектор (на основе лавинного фотодиода) в интервалах, определяемых временем прихода на детектор отражённого сигнала. Сигнал с выхода детектора (где нулевое напряжение соответствует базису 0, а положительное - базису 1) через преобразователь напряжений $Пр_2$ поступает на вход компьютера, где программно реализован счётчик совпадений измеренных значений базисов с действительными. Количество совпадений M, зарегистрированных счётчиком, отнесённое к общему количеству синхроимпульсов N, определяет процент ошибок детектирования базисов:

$$BER = \left(1 - \frac{M}{N}\right) \cdot 100\% .$$

Программная часть реализована на компьютере с помощью программы LabView.

К сожалению, из-за задержек с ремонтом экспериментального оборудования первоочередной важности, а именно оптического рефлектометра, на момент завершения работы над данной магистерской диссертацией начать модельный эксперимент не представилось возможным, однако это и не являлось непосредственной целью работы (см. постановку задачи в разделе "Введение"). Схема экспериментальной установки для предварительных измерений представлена на рис. 12. Вверху изображена оптическая часть оборудования Алисы, состоящая из импульсного лазера, поляризатора и интерферометра, реализованного с помощью обычного (на входе) и поляризационного (на выходе) ответвителя. В коротком плече интерферометра сигнал распространяется свободно, в то время как в длинном плече он задерживается во времени при помощи постоянной и переменной (подстроечной) линий

задержки и модулируется по фазе фазовым модулятором. Выходной поляризационный ответвитель разделяет сигналы из разных плеч интерферометра по поляризации (все оптическое волокно внутри интерферометра - с сохранением поляризации). Внизу на рисунке показано оборудование Евы - оптический рефлектометр Opto-Electronics Millimeter Resolution OTDR и интерферометр, состоящий из сигнального и опорного плеч. Сигнальное плечо ведёт к аппаратуре Алисы, а в опорном плече находится переменная линия задержки, реализованная с помощью растяжки оптического волокна на микрометрической подвижке, переменного аттенюатора и отражателя (им служит ровно сколотый свободный конец волокна). Работа схемы состоит в следующем. Световые импульсы с выхода оптического рефлектометра делятся на ответвителе и поступают в сигнальное и опорное плечо. В сигнальном плече импульсы отражаются от какого-либо элемента аппаратуры Алисы и возвращаются обратно. В опорном плече переменная линия задержки настраивается так, чтобы время прихода отражённого сигнала в этом плече совпадало с временем прихода отражённого сигнала от выбранного элемента в сигнальном плече; аттенюатором подбирается ослабление так, чтобы амплитуды отражённых сигналов в сигнальном и опорном плечах совпадали. Таким образом, на делителе Евы наблюдается интерференция сигналов из опорного и сигнального плеча; эта интерференция конструктивна, если разность фаз между сигналами равна 0, и деструктивна, если разность фаз равна π. Разность фаз регулируется изменением статического напряжения на фазовом модуляторе Алисы.

В ходе предварительных измерений было проделано следующее:

1) Выбран конкретный отражённый сигнал для работы. Рабочим отражающим элементом является свободный конец волокна на входе интерферометра Алисы. Однократным отражениям от этого элемента соответствуют четыре сигнала:
   а) Прошедший на прямом и обратном пути короткое плечо интерферометра Алисы. Его параметры: t = 50.00 нс, A = - 27 дБ. Амплитуда сигнала

интерференции менялась от нуля до максимального значения при изменении поляризации в опорном плече путем вращения оптического коннектора. Заведомо не годится для наших целей, поскольку ни разу не проходит фазовый модулятор.

b) Прошедший на прямом пути короткое, а на обратном - длинное плечо интерферометра Алисы. Его параметры: t = 69.40 нс, A = - 44 дБ.
c) Прошедший на прямом пути длинное, а на обратном - короткое плечо интерферометра Алисы. Его параметры идентичны с предыдущим.
d) Прошедший на прямом и обратном пути длинное плечо интерферометра Алисы. Его параметры: t = 88.85 нс, A = - 58 дБ. Амплитуда сигнала интерференции менялась от нуля до максимального значения при изменении поляризации в опорном плече путем вращения оптического коннектора.

Сигналы b) и c) при наблюдении складывались друг с другом, образуя один составной сигнал, так как имели одинаковую задержку. Зависимости амплитуды сигнала интерференции от поляризации в опорном плече для этого сигнала не наблюдалось. По неизвестным причинам при использовании данного составного сигнала не удалось получить сколько-нибудь пригодную для измерений видность интерференции, в связи с чем пришлось использовать сигнал d), обладающий меньшей амплитудой.

2) Сделана теплоизоляция измерительной схемы, увеличившая постоянную ухода фазы Ф в системе с трудно измеримой на опыте малой величины до величины порядка Ф=2 мин/2π, что является уже пригодным для выполнения задуманного модельного эксперимента.
3) Измерена видимость интерференции V для принимаемого сигнала. Наилучшим из достигнутых был результат около 95%. Видится вполне возможным достижение более высокого результата при наличии лучшего согласования поляризации сигналов в опорном и сигнальном плечах измерительного интерферометра. Изначально, кроме измерения видности интерференции, планировалось снять характеристику, где приводилась бы

зависимость амплитуды сигнала интерференции от напряжения на фазовом модуляторе Алисы. Однако из-за неосторожного обращения с источником питания модулятора произошёл пробой между двумя расположенными на поверхности кристалла ниобата лития электродами, расстояние между ними около 8 мкм, с расплавлением участка электродов и повреждением оптического волновода в кристалле. В результате характеристику по точкам снять не удалось.

Осуществление модельного эксперимента планируется исследовательской группой NTNU на осень 2000 г.

Элемент	Максимальный коэф. отражения, дБ	Минимальный коэф. отражения, дБ
Макроизгиб волокна Микроизгиб волокна	69 51	>110 69
Изломы, трещины волокна	14	77
Ответвители	37	71
Оптические переключатели	13	66
Оптические аттенюаторы	9	66
Лазеры и детекторы: - с опт. изолятором - без опт. изолятора	 34 3	 54 21
Неразъёмное соединение - сварка - механич., влажное - механич., сухое	 69 34 19	 104 56 41
Коннекторы: - APC (отполированный под углом 8^0) - PC (обычный) - gap (с зазором)	 47 19 9	 73 51 14
Отпол ированный или ровно сколотый свободный конец волокна	14	15

Таблица 2. Типичные величины коэффициентов отражения для различных волоконно-оптических компонентов [26]

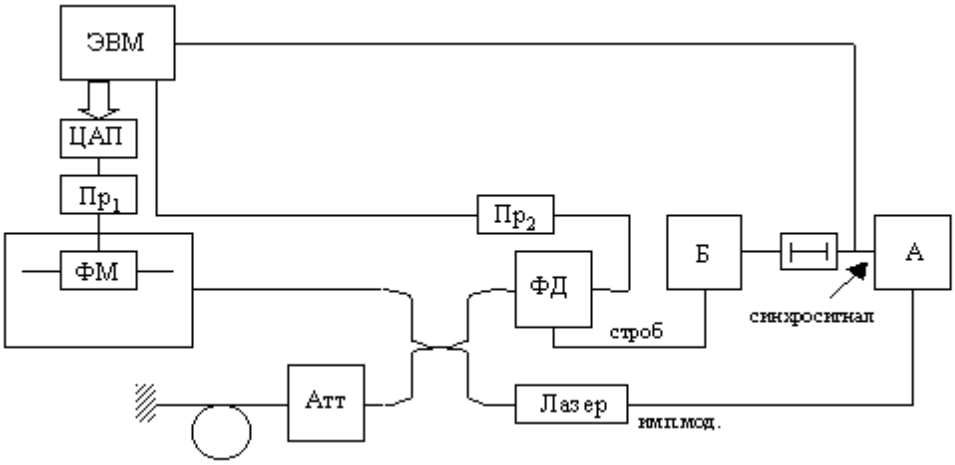

Рис.11. Схема планируемого модельного эксперимента

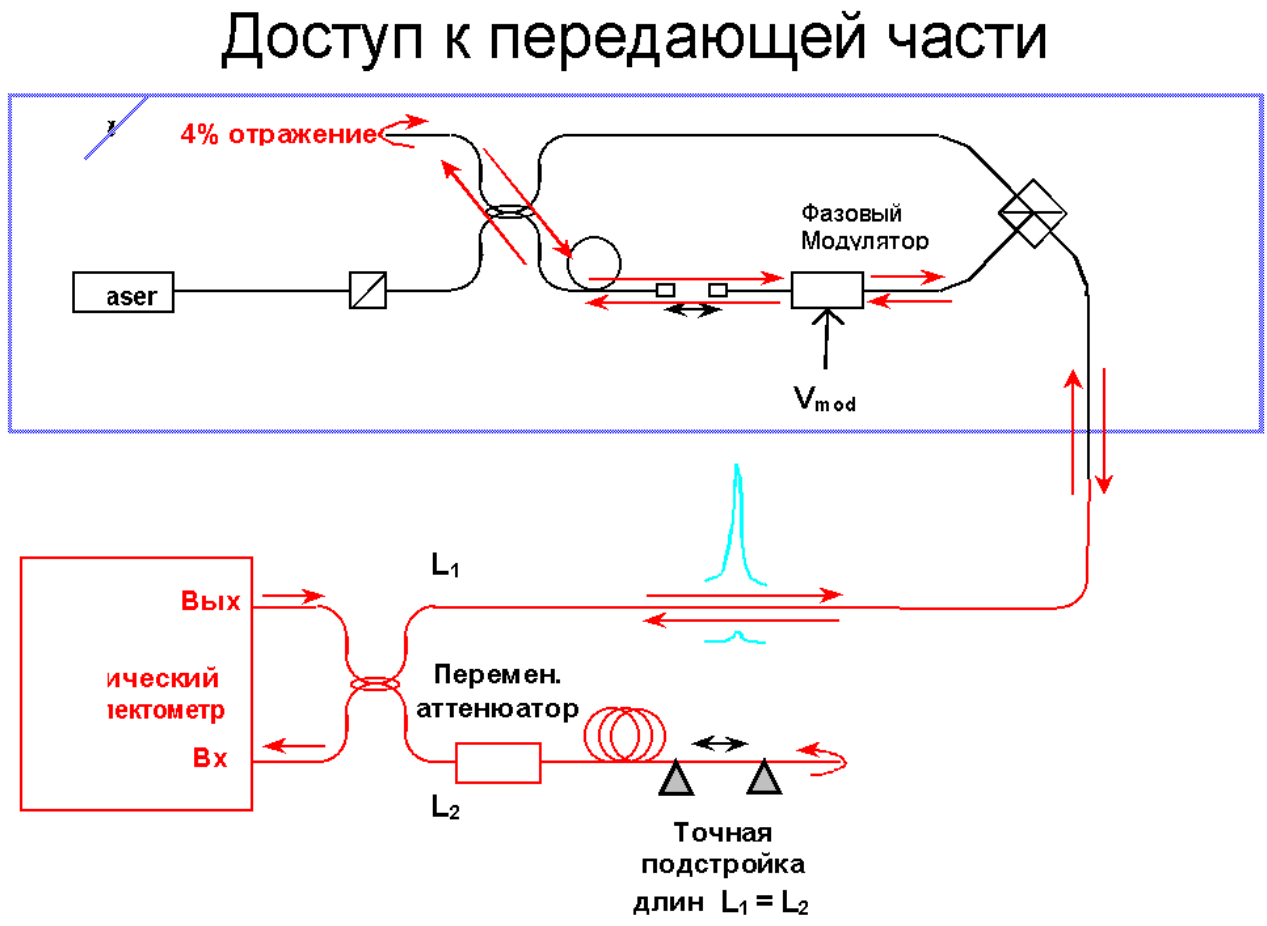

Рис.12. Схема установки для предварительных измерений

Заключение

В результате работы над данной магистерской диссертацией:

1. Осуществлено теоретическое исследование стратегии несанкционированного доступа к абонентам через общий оптический канал связи на примере квантово-криптографических систем на основе волоконно-оптических линий связи с использованием протоколов обмена BB84 и B92 на фазовых состояниях.
2. Предложены меры защиты от данного вида атаки.
3. Разработана структурная схема экспериментальной установки и методика измерений. Осуществлены подготовительные измерения на оптической части квантово-криптографической установки NTNU, в ходе которых экспериментально подтверждён принцип несанкционированного доступа к абонентам через общий оптический канал связи.

Таким образом, задание на дипломное проектирование выполнено полностью.

Список использованной литературы

1. S. Wiesner, "Conjugate Coding", *Sigact News, vol.15, 78 (1983)*.
2. C.H. Bennett, G. Brassard, in *Proceeding of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), 175*
3. C. H. Bennett, F. Bessette, G. Brassard, L. Savail, J. Smolin, "Experimental Quantum Cryptography", *Journal of Cryptology, Vol. 5, 3 (1992)*.
4. D. Bruss, N. Luetkenhaus, "Quantum Key Distribution: From Principles To Practicalities", *arXiv:quant-ph/9901061 v2 (1999)*.
5. C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", *Phys. Rev. Lett., Vol. 68, 3121 (1992)*.
6. B. Huttner, N. Imoto, N. Gisin, T. Mor, "Quantum Cryptography with Coherent States", *Phys. Rev. A, Vol. 51, 1863-1869 (1995)*.
7. A. Ekert, "Quantum Cryptography Based on Bell's Theorem", *Phys. Rev. Lett., Vol. 67, 661 (1991)*.
8. D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States", *Phys. Rev. Lett, Vol. 81, 3018 (1998)*.
9. L. Goldenberg, L. Vaidman, "Quantum Cryptography Based On Orthogonal States", *Phys. Rev. Lett., Vol. 75, 1239 (1995)*.
10. M. Koashi, N. Imoto, "Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps", Phys. Rev. Lett., Vol. 79, 2383 (1997).
11. H. Zbinden, H. Behcmann-Pasquinucci, N. Gisin, G. Ribordy, "Quantum Cryptography", *Appl. Phys. B, Vol. 67, 743 (1998)*.
12. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, "Fast and User-Friendly Quantum Key Distribution", *submitted to the Journal of Modern Optics*.
13. M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, J.P. Ciscar, "Experimental Long Wavelength Quantum Cryptography: From Single Photon

Transmission To Key Extraction Protocols", *J. Modern Optics, Vol. 47, 563 (1998).*

14. N. Luetkenhaus, "Security Against Eavesdropping in Quantum Cryptography", *Phys. Rev. A, Vol. 54, 97 (1996).*
15. D. Mayers, A. Mao, "Quantum Cryptography with Imperfect Apparatus", *arXiv:quant-ph/9809039 (1998).*
16. E. Biham, T. Mor, "Security of Quantum Cryptography Against Collective Attacks", *Phys. Rev. Lett., Vol.78, 2256 (1997).*
17. G. Brassard, N. Luetkenhaus, T. Mor, B.C. Sanders, "Security Aspects of Practical Quantum Cryptography*", quant-ph/9911054 (1999).*
18. M. Dusek, M. Jahma, N. Luetkenhaus, "Unambigious-State-Discrimination Attack with Weak Coherent States", *quant-ph/9910106 (1999).*
19. N. Luetkenhaus, "Estimates for Practical Quantum Cryptography*", arXiv:quant-ph/9806008 v2 (1999).*
20. N. Luetkenhaus, "Security Against Individual Attacks for Realistic Quantum Key Distribution", *arXiv:quant-ph?9910093 v2 (2000).*
21. D.S.Bethune, W.P.Risk, "An Autocompensating Fiber-Optic Quantum Cryptography system based on Polarization Splitting of Light", *IEEE Journal of Quantum Electronics, Vol.36, 340 (2000).*
22. B.C. Jacobs, J.D. Franson, "Quantum Cryptography In Free Space", *Opt. Lett., Vol. 21, 1854 (1996).*
23. P.Ch. Sun, E. Fineman, Yu.T. Mazurenko, "Transmission of Optical Phase Information Using Frequency Separation of Signals as Applied to Quantum Cryptography", *Optics and Spectroscopy, Vol. 78, 887 (1995).*
24. J.-M. Mérolla, Yu. Mazurenko, J.-P. Goedgebuer, W.T. Rhodes, "Single-Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography", *Phys. Rev. Lett., Vol. 82, No. 8, February 1999.*
25. G.P. Agrawal, "Fiber-Optic Communication Systems", *p. 255-260, John Wiley & Sons, 1997.*

26. Reference Manual, Millimeter Resolution OTDR System, *Opto-Electronics, Inc. Oakville, Canada (1994*).
27. S. Lomonaco, "A Quick Glance at Quantum Cryptography", *quant-ph/9811056 (1998)*.
28. См., например, EPLD-1K, http://www.irepolusgroup.com/ErbLasers/EFLGuide.htm
29. C. Marand, P.D. Townsend, "Quantum Key Distribution Over Distances As Long As 30 km", *Opt. Lett., Vol.20, 1695 (1995).*