МОДЕЛИРОВАНИЕ КВАНТОВЫХ ЛИНИЙ СВЯЗИ

***Волосатова Тамара Михайловна**, кандидат технических наук, доцент, г. Москва*
***Чичварин Николай Викторович**, кандидат технических наук, доцент, г. Москва*

Статья содержит:

Анализ результатов обзора доступных публикаций.

Предложения для простого моделирования средств квантовой криптографии с обоснованной степенью адекватности.

В частности, приведено описание предложения, которое, по мнению авторов дополнительно затрудняет несанкционированный доступ к данным, передаваемым по квантовым линиям связи.

Основным источником уязвимости криптографических линий связи является необходимость передачи ключа по окрытым каналам.

Необходимость дополнительных временных потерь для выполнения процедуры:

– анализ случайного участка в передаче ключа.

– многократное повторение процедуры анализа, если процент ошибок велик.

При разработке модификации авторы исходили из следующего:

Как известно, попытка перехватить сообщение приводит к изменению состояния частиц, что позволит обнаружить нарушение секретности передачи. Невозможно получить все сведения о квантовом объекте, и, следовательно, невозможно его незаметно скопировать. Однако возможен доступ с заменой полезного излучения шумом. Предлагаемая модификация позволяет повысить робастность, целостность и криптоустойчивость каналов.

***Ключевые слова**: квант, криптография, волокно, несанкционированный доступ, уравненение, электродинамика, квантовая механика.*

SIMULATION OF QUANTUM COMMUNICATION LINES

***Tamara Volosatova**, Ph.D., Assistant Professor, Moscow*
***Nicolai Chichvarin**, Ph.D., Assistant Professor, Moscow*

This article contains:

• Analysis of the results of the review of available publications.

• Proposals for simple modeling tools of quantum cryptography with a reasonable degree of adequacy.

• In particular, a description of the proposal which, according to the authors further complicates unauthorized access to data transmitted on the quantum communication lines.

• The main source of vulnerability of cryptographic communication lines is the need to transfer the key Opened channels.

• The need for additional time loss for the procedure:

– Analysis of a random site in the keys.

– Repetition of the assay procedure, if the error rate is great.

When designing modifications authors started from the next:

As you know, trying to intercept the message leads to a change in the state of particles that will reveal a violation of the secrecy of transmission. It is impossible to get all the information about a quantum object, and therefore, it is impossible to seamlessly copy. However, access is possible with the replacement of the useful radiation noise. The proposed modification increases the robustness and integrity.

***Keywords**: quantum cryptography, fiber, unauthorized access, equation, electrodynamics, quantum mechanics.*

Импульсный метод кодирования в квантовой криптографии

Перечень сокращений:

ИБ	информационная безопасность	КЛС	квантовая линия связи
КК	квантовая криптография	КПС	канал передачи сообщений
НСД	несанкционированный доступ	НДВ	недокументированные возможности
ОВ	оптическое волокно	ВОЛС	волоконно – оптическая линия связи
ЛФД	лавинный фотодиод	ФЭУ	фотоэлектрический умножит ель

Введение

Статья содержит описание предложения, которое, по мнению авторов дополнительно затрудняет НСД к данным, передаваемым по квантовым линиям связи. При разработке предложения авторы исходили из следующего:

Как известно, попытка перехватить сообщение при НСД приводит к изменению состояния частиц, что позволит обнаружить нарушение секретности передачи. Невозможно получить все сведения о квантовом объекте, и, следовательно, невозможно его незаметно скопировать. Однако возможен НСД путем замены полезного излучения шумом. Предлагаемая модификация позволяет повысить робастность, целостность и криптоустойчивость каналов. Суть предложения заключается в следующем:

• Сообщение разбивается на ряд участков.

• Участки содержат:

- либо ложные данные,

- либо полезные данные,

- смесь сигнала с помехами.

Последовательность участков может быть псевдослучайной, что еще более затрудняет дешифровку.

1. Анализ результатов обзора доступных публикаций

Анализ показывает, что возможны два принципа реализации КЛС:

• Квантовый, когда кодирование осуществляется положением спина фотона. Поскольку, как известно, масса покоя фотона в любой системе отсчета равна нулю, незаметный НСД к КЛС невозможен.

• Импульсный, когда кодирование реализуется положением вектора поляризации. Очевидно, что в этом случае возможен незаметный перехват сообщения.

Поэтому в дальнейшем будем различать поляризационные и квантовые линии связи.

1.1 Источники излучения в квантовых линиях

Анализ статистики фотонов разработанного излучателя [1 - 2] демонстрирует, что вероятность двухфотонного излучения в заданный интервал времени близка к нулю. Использование брэгговского вертикального микрорезонатора позволяет существенно увеличить внешнюю квантовую эффективность излучателя (до уровня ~ 30 %) и значительно уменьшить время спонтанной эмиссии экситона квантовой точки за счет эффекта квантовой электродинамики — эффекта Парселла. Фактор Парселла для разработанного микрорезонатора составляет ~ 2,5, что обеспечивает большее быстродействие излучателя в 2–2,5 раза. Излучатель одиночных фотонов относится к числу первых полупроводниковых оптоэлектронных приборов, принцип работы которых основан на эффектах квантовой электродинамики резонаторов. Уменьшение времени спонтанной эмиссии экситона квантовой точки за счет эффекта Парселла с ~ 1 нс до ~ 0,4 нс позволило поднять быстродействие ИОФ до рекордно высокого уровня 1 ГГц.

Как известно [2], лазеры с вертикальным резонатором (ЛВР) — наиболее миниатюрные, экономичные и быстродействующие лазеры. Они являются рекордсменами по этим параметрам не только среди полупроводниковых лазеров, но и неоспоримо лидируют в области всей лазерной техники: объем резонатора может составлять несколько кубических длин волн, пороговые токи генерации могут быть на уровне ~ 10 мкА, а частота токовой модуляции способна достигать десятков гигагерц.

Вертикальный резонатор, как правило, формируется в едином технологическом процессе выращивания полупроводниковой гетероструктуры, содержащей два полупроводниковых брэгговских зеркала. Ось резонатора ориентирована вертикально по отношению к плоскости полупроводниковой структуры. Вертикальные резонаторы характеризуются малым размером и обеспечивают эффективную локализацию энергии электромагнитной волны, как в аксиальном, так и в латеральном направлениях.

1.2 Приемники излучения в квантовых линиях

Наиболее известные в открытой литературе приемники излучения, работающие в режиме счетчиков квантов. В первую очередь – это лавинные фотодиоды. Как известно, лавинные фотодиоды — высокочувствительные полупроводниковые приборы, преобразующие свет в электрический сигнал за счёт фотоэффекта. Их можно рассматривать в качестве фотоприёмников, обе-

спечивающих внутреннее усиление посредством эффекта лавинного умножения. С функциональной точки зрения они являются твердотельными аналогами фотоумножителей. Лавинные фотодиоды обладают большей чувствительностью по сравнению с другими полупроводниковыми фотоприёмниками, что позволяет использовать их для регистрации малых световых мощностей (□ 1 нВт).

При подаче сильного обратного смещения (близкого к напряжению лавинного пробоя, обычно порядка нескольких сотен вольт для кремниевых приборов), происходит усиление фототока (примерно в 100 раз) за счёт ударной ионизации (лавинного умножения) генерированных светом носителей заряда. Суть процесса в том, что энергия образовавшегося под действием света электрона увеличивается под действием внешнего приложенного поля и может превысить порог ионизации вещества, так что столкновение такого «горячего» электрона с электроном из валентной зоны может привести к возникновению новой электрон-дырочной пары, носители заряда которой также будут ускоряться полем и могут стать причиной образования всё новых и новых носителей заряда.

Существует ряд формул для коэффициента лавинного умножения (M), довольно объективной является следующая:

$$M = \frac{1}{1 - \int_0^L \alpha(x)dx}$$

где L — длина области пространственного заряда, а α — коэффициент ударной ионизации для электронов (и дырок). Этот коэффициент сильно зависит от приложенного напряжения, температуры и профиля легирования. Отсюда возникает требование хорошей стабилизации питающего напряжения и температуры, либо учёт температуры задающей напряжение схемой.

Ещё одна эмпирическая формула показывает сильную зависимость коэффициента лавинного умножения *(M)* от приложенного обратного напряжения:

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

где U_b — напряжение пробоя. Показатель степени n принимает значения от 2 до 6, в зависимости от характеристик материала и структуры p-n-перехода.

Исходя из того, что в общем случае с возрастанием обратного напряжения растёт и коэффициент усиления, существует ряд технологий, позволяющих повысить напряжение пробоя до более чем 1500 вольт, и получить, таким образом, усиление более чем в 1000 раз. Следует иметь в виду, что простое повышение напряженности поля без предпринятия дополнительных мер может привести к увеличению шумов. И это необходимо учесть при проектировании КЛС. Следует учитывать и инженерное противоречие: требование обеспечить максимально возможную дальность связи и максимальное соотношение сигнал/шум.

Если требуются очень высокие коэффициенты усиления (10^5 — 10^6), возможна эксплуатация некоторых типов ЛФД при напряжениях выше пробойных. В этом случае требуется подавать на фотодиод ограниченные по току быстро спадающие импульсы. Для этого могут использоваться активные и пассивные стабилизаторы тока. Приборы, действующие таким образом, работают в режиме Гейгера (Geiger mode). Этот режим применяется для создания однофотонных детекторов (при условии, что шумы достаточно малы).

Типичное применение ЛФД — лазерные дальномеры и волоконные линии связи. Среди новых применений можно назвать позитронно-эмиссионную томографию и физику элементарных частиц. В настоящее время уже появляются коммерческие образцы массивов лавинных фотодиодов.

Сфера применения и эффективность ЛФД зависят от многих факторов. Наиболее важными являются:

• квантовая эффективность, которая показывает, какая доля падающих фотонов приводит к образованию носителей заряда и возникновению тока;

• суммарный ток утечек, который складывается из темнового тока и шумов.

Электронные шумы могут быть двух типов: последовательные и параллельные. Первые являются следствием дробовых флуктуаций и в основном пропорциональны ёмкости ЛФД, тогда как параллельные связаны с механическими колебаниями прибора и поверхностными токами утечки. Другим источником шума является фактор избыточного шума (excess noise factor), *F*. В нём описываются статистические шумы, которые присущи стохастическому процессу лавинного умножения *M* в ЛФД. Обычно он выражается следующим образом:

$$F = kM + (2 - 1/M)(1 - k)$$

где k — соотношение коэффициентов ударной ионизации для дырок и электронов. Таким об-

разом, увеличение асимметрии коэффициентов ионизации приводит к уменьшению этих помех. К этому стремятся на практике, так как $F(M)$ вносит основной вклад в ограничение разрешающей способности приборов по энергии.

Ограничения на скорость работы накладывают ёмкости, времена транзита электронов и дырок и время лавинного умножения. Ёмкость увеличивается с ростом площади переходов и уменьшением толщины. Время транзита электронов и дырок возрастает с увеличением толщины, что заставляет идти на компромисс между емкостью и временем. Задержки, связанные с лавинным умножением определяются структурой диодов, применяемыми материалами, существует зависимость от k. Таким образом, при разработке метода защиты от НСД особое внимание обращено на быстродействие источников излучения и уровень собственных шумов.

Как показал обзор доступных публикаций, для создания малошумящих приборов может быть использован широкий круг полупроводников:

• Кремний используется для работы в ближнем ИК-диапазоне, при этом имеет малые шумы, связанные с умножением носителей.

• Германий принимает инфракрасные волны длиной до 1.7 мкм, но приборы на его основе имеют заметные шумы.

• InGaAs обеспечивает приём волн длиной от 1.6 мкм, при этом имея меньшие, нежели у германия шумы. Обычно этот материал используется для изготовления лавинных фотодиодов на гетероструктурах, также включающих InP в качестве подложки и второго компонента для создания гетероструктуры. Эта система имеет рабочий диапазон в пределах 0,7—0,9 мкм. У InGaAs высокий коэффициент поглощения на длинах волн, используемых в телекоммуникации через волоконно-оптические линии связи, таким образом, достаточно даже микронных слоёв InGaAs для полного поглощения излучения. Эти материалы обеспечивают небольшие задержки и малые шумы, что позволяет получить устройства с полосой частот более 100 ГГц для простой InP / InGaAs системы и до 400 ГГц для InGaAs на кремнии. Это делает возможным передачу данных на скоростях, превышающих 10 Гбит/с.

• Диоды на основе нитрида галлия используются для работы в ультрафиолетовом диапазоне волн.

• HgCdTe применяется для изготовления диодов, работающих в инфракрасной части спектра, обычно максимальная длина волны составляет около 14 мкм. При этом они требуют охлаждения для сокращения темновых токов. Такая система способна обеспечить очень низкий уровень помех.

2. Цель и задачи исследований

При подготовке материалов статьи авторы провели исследования, целью которых была разработка предложений по модификации известного протокола BB84 для повышения криптоустойчивости квантовых линий связи. При этом цитирование известного материала сведено к минимуму. Особое внимание уделяется вопросам выбора более устойчивого кода с опорой на известные протоколы. Для достижения поставленной цели последовательно решены следующие задачи:

• Проведение аналитического литературного обзора методов и протоколов КК.

• Анализ уязвимостей КЛС.

• Анализ проводных и беспроводных линий связи, используемых в КК.

• Разработка собственно предложений.

3. Анализ методов и средств передачи сообщений, шифруемых с применением КК с учетом специфики решаемых задач. Описание принципа возможной модификации

3.1 Иерархические уровни моделирования при проектировании КПС

Анализ проведен в соответствии с блочно-иерархическим подходом к моделированию КК.

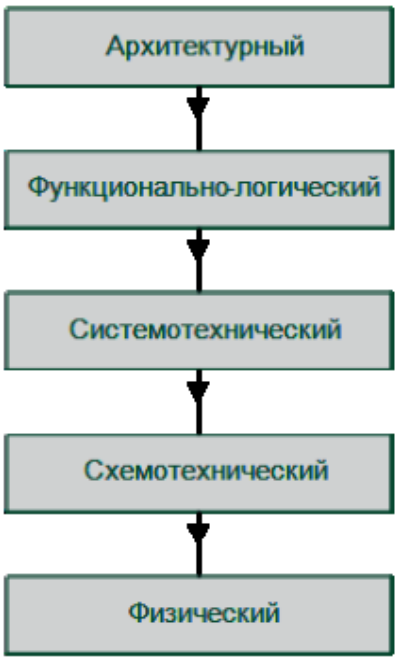

***Рис. 1**. Иерархическая схема структуры КК.*

Принято во внимание описание структуры канала передачи данных, включающее пять уровней (см. Рис.1): архитектурный, функционально-логический, системотехнический, схемотехнический, физический.

Для каждого из данных уровней необходимо рассматривать круг требующих решения задач, определять набор реализуемых на нем функций, производить анализ надежности и полноты обеспечения поставленных целей. Модель архитектурного уровня соответствует степени детализации объекта проектирования, не требующей учета:

• физического носителя сигнала,

• логического носителя сигнала,

• внутренней структуры подсистем передачи сообщений.

На данном уровне иерархической структуры рассматриваются модели топологий каналов, правила и условия их построения. Принятие того или иного протокола осуществляется на архитектурном уровне. Для КК на этом уровне основная проектная задача – выбор метода кодирования. Модели функционально-логического уровня строятся для решения задач согласования подсистем, входящих в состав канала передачи сообщений. В перечень задач, решаемых на данном уровне, входит контроль качества передачи сообщений, а также их защита от внешних помех. К числу подобных помех относят методику криптоанализа с подменой авторизованных участников соединения. Системотехнический уровень соответствует степени детализации в приближении моделей «черный ящик» или «серый ящик». Модель типа «серый ящик» понимается, как объект исследований, о внутреннем устройстве которого либо известно частично, либо существуют некоторые гипотезы. В отличие от черного, модели серого ящика учитывают помимо связей между реакциями и внешними воздействиями и те частичные сведения, которые известны о его внутреннем строении. Подсистемы данного уровня выполняют функции кодирования логических сигналов для их передачи физическим носителем в канале беспроводного соединения. На схемотехническом уровне в модельном представлении объекта проектирования учитывается физическая природа носителей сигнала совместно с характером преобразования в отдельных моделях типа «черный ящик». На физическом уровне иерархической структуры канала передачи защищенных сообщений выполняются работы по проектированию электромагнитной совместимости устройств, входящих в беспроводное соединение. Также на данном уровне рассматриваются аспекты взаимодействия устройств и помех в форме физических сигналов.

В случаях, когда в качестве КПС рассматриваются беспроводные соединения, могут применяться методики проектирования каналов в удовлетворяющих данному требованию стандартах локальной беспроводной связи мобильных устройств (IEEE 802.11, 802.15). Тогда можно сделать выводы о существовании потенциальных проблем в структуре спроектированных каналов:

• на архитектурном уровне (существующие топологии допускают несанкционированное подключение, прослушивание эфира и подмену узлов соединений),

• на функционально-логическом уровне (применяемые методики защиты каналов в ряде случаев являются криптографически слабыми по отношению к методам криптоанализа. В контексте областей применения результатов разработки потенциальную уязвимость могут содержать методики хранения и распространения конфиденциальных данных, например, ключей).

Задача безопасной пересылки ключей может быть решена с помощью квантовой рассылки ключей QKD(Quantum Key Distribution). Надежность метода опирается на нерушимость законов квантовой механики. Злоумышленник не может незаметно отвести часть сигнала с передающей линии, так как нельзя поделить электромагнитный квант на части. Любая попытка злоумышленника вмешаться в процесс передачи вызовет непомерно высокий уровень ошибок. Скорость передачи данных при этой технике не высока, но для передачи ключа она и не нужна. По существу квантовая криптография может заменить алгоритм Диффи-Хелмана, который в настоящее время часто используется для пересылки секретных ключей шифрования по каналам связи.

Первый протокол квантовой криптографии (BB84) был предложен и опубликован в 1984 году Беннетом и Брассардом. Позднее идея была развита Экертом в 1991 году. В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов.

Протокол Беннета:

• Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.

• Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).

• Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга

о полученных результатах. Последний бит каждого блока удаляется.

• Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.

• Чтобы исключить кратные ошибки, которые могут быть не замечены, операции пунктов 1-4 повторяются для большего значения k.

• Для того чтобы определить, остались или нет необнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки:

- Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.
- Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.
- Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.
- Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2^{-m}.

Как известно, дальнейшего улучшения надежности криптосистемы можно достичь, используя эффект EPR (Einstein-Podolsky-Rosen). Эффект EPR возникает, когда сферически симметричный атом излучает два фотона в противоположных направлениях в сторону двух наблюдателей. Фотоны излучаются с неопределенной поляризацией, но в силу симметрии их поляризации всегда противоположны. Важной особенностью этого эффекта является то, что поляризация фотонов становится известной только после измерения. На основе EPR Экерт предложил крипто-схему, которая гарантирует безопасность пересылки и хранения ключа. Отправитель генерирует некоторое количество EPR фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При этом, если эффективность регистрации близка к единице, при получении отправителем значения поляризации 1, его партнер зарегистрирует значение 0 и наоборот. Ясно, что таким образом партнеры всякий раз, когда требуется, могут получить идентичные псевдослучайные кодовые последовательности. Практически реализация данной схемы проблематична из-за низкой эффективности регистрации и измерения спина одиночного фотона.

Однофотонные состояния поляризации более удобны для передачи данных на большие расстояния по оптическим кабелям (алгоритм B92; R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons, «Quantum cryptography over optical fibers», Uni. of California, Physics Division, LANL, Los Alamos, NM 87545, USA).

В алгоритме B92 приемник и передатчик создают систему, базирующуюся на интерферометрах Маха-Цендера. Отправитель определяет углы фазового сдвига, соответствующие логическому нулю и единице ($F_A=p/2$), а приемник задает свои фазовые сдвиги для логического нуля ($F_B=3p/2$) и единицы ($F_B=p$). В данном контексте изменение фазы $2p$ соответствует изменению длины пути на одну длину волны используемого излучения. Хотя фотоны ведут себя при детектировании как частицы, они распространяются как волны. Это учитывалось при формировании модели КЛС.

Вероятность регистрации будет варьироваться от 1 (при нулевой разности фаз) до нуля. Здесь предполагается, что отправитель и получатель используют фазовые сдвиги (F_A, F_B) = (0, 3p/2) для нулевых бит и (F_A, F_B) = (p/2, p) для единичных битов (для алгоритма BB84 используются другие предположения).

3.2 Протокол BB84 [2 с.30]

Далее в качестве примера рассматривается наиболее распространенный протокол – BB84. Как известно, носителями кода по протоколу BB84 являются фотоны, со спинами, ориентированными на 0, 45, 90, 135 градусов. Как известно, с абсолютной достоверностью отличить с вертикальным спином от фотона со спином 45 градусов, принципиально вертикально фотон невозможно. В основу протокола квантового распространения ключа заложено следующие действия Индуктора и Перципиента:

• Индуктор посылает Перципиенту фотон с одним из спинов (0, 45, 90, 135 градусов) и записывает его значение. Отсчет углов ведется от направления «вертикально вверх» по часовой стрелке.

• Перципиент, располагающий двумя анализаторами - вертикально-горизонтальным и диагональным, для каждого фотона случайно выбирает один из анализаторов и записывает тип анализатора и результат измерений.

• По открытому каналу связи Перципиент сообщает Индуктору, какие анализаторы использовались, но не сообщает, какие результаты были получены.

• Индуктор по открытому каналу связи сообщает Перципиенту, какие анализаторы он выбрал правильно. Фотоны, для которых Перципиент неверно выбрал анализатор, отбрасываются.

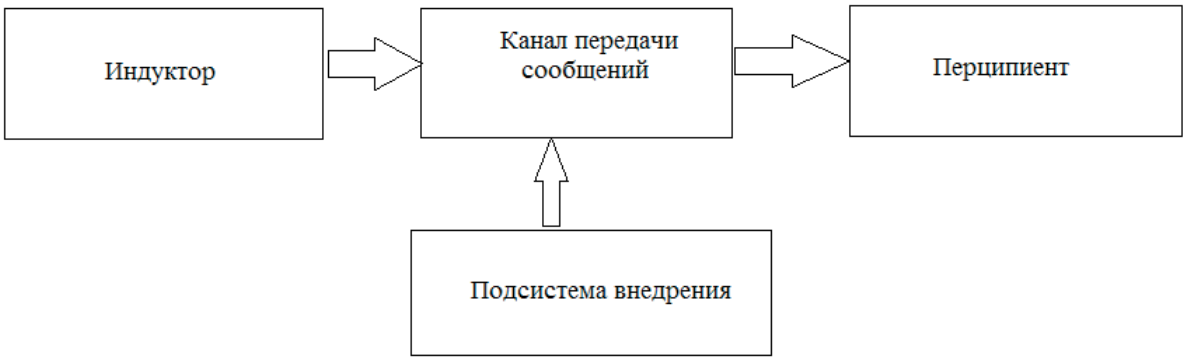

***Рис. 2**. Структура канала передачи сообщений.*

Протокол для обмена ключом представлен на Рис. 3. Следует подчеркнуть, что в цитируемом тексте говорится не о спине, а о положении вектора поляризации.

Обозначения разрядов: в случае вертикально-горизонтальной ориентации спина вертикально-ориентированный фотон означает 0, горизонтально-поляризованный — 1; в случае диагональной ориентации спина под углом 45 градусов - 0, 135 градусов - 1. Правила на Рис. 3 приняты условно, т.к. эти обозначения могут быть заменены на противоположные. Анализ кодов:

1-й столбец — Индуктор послал фотон с вертикальным спином, Перципиент выбрал «прямоугольный» анализатор и, следовательно, смог получить правильный результат — 0. Этот результат вошел в ключ.

2-й столбец — Индуктор посылает фотон, поляризованный под углом 45 градусов, Перципиент выбирает диагональный анализатор и может получить верный результат — 0. Этот результат также входит в ключ.

3-й столбец — Индуктор вновь посылает фотон, спин которого ориентирован под углом 45 градусов, но Перципиент выбирает неверный, прямоугольный анализатор, поэтому с равной вероятностью может получить как 0, так и 1. В случае, показанном на рисунке, его результат равен 1. После сверки анализаторов этот результат будет отброшен и в ключ не войдет.

4-й столбец — Индуктор посылает фотон с горизонтально-поляризованным спином, Перципиент выбирает верный анализатор и получает результат 1, который войдет в ключ.

5-й столбец — Индуктор посылает фотон, спин которого ориентирован под углом 135 градусов, Перципиент выбирает правильный, диагональный анализатор и получает результат 1, который войдет в ключ.

6-й и 7-й столбцы — Индуктор дважды подряд случайно посылает фотон с вертикально-поляризованным спином, но Перципиент оба раза (это тоже случайно) выбирает неверный, диагональный анализатор, в результате чего результаты его

Последовательность фотонов Индуктора	|	/	/	–	\	|	|	–	–
Последовательность анализаторов Перципиента	+	x	+	+	x	x	x	+	x
Результаты измерений Перципиента	0	0	1	1	1	0	1	1	0
Анализаторы выбраны верно	+	+		+	+			+	
Ключ	0	0		1	1			1	

***Рис. 3**. Принцип шифрования по протоколу BB84.*

Условные обозначения:
ориентация спинова фотонов: | - вертикальная, - горизонтальная, / - под углом 45, \ - под углом 135.
Анализаторы: + - прямоугольный, x – диагональный.

измерений — случайны, что и представлено на рисунке: в 6-м столбце Перципиент получил 0, а в 7-м — 1. Оба эти результата при формировании ключа будут отброшены из-за того, что был выбран неверный анализатор.

Если бы производился НСД при помощи оборудования, подобного оборудованию Перципиента, то примерно в 50 процентах случаев будет выбран неверный анализатор и невозможно определить состояние полученного фотона, и отправление фотона Перципиенту произойдет в состоянии, выбранном наугад. При этом в половине случаев будет выбрана неверная поляризация и примерно в 25 процентах случаев результаты измерений Перципиента могут отличаться от результатов Индуктора. Для обнаружения перехвата Индуктор и Перципиент выбирают случайный участок ключа и сравнивают его по общедоступному каналу связи. Если процент ошибок велик, то он может быть отнесен на счет результатов НСД, и процедура повторяется сначала. Анализ результатов обзора показывает, что на практике дополнительно применяются специальные протоколы для коррекции ошибок при передаче, а также протокол усиления секретности (privacy amplification), позволяющий с высокой вероятностью устранить из ключа данные, которые могли быть перехвачены. В статье, посвященной квантовой криптографии авторы предлагают.

Для повышения криптостойкости КЛС, реализующих известные криптографические протоколы предлагается следующее:

• Кодировать единицы и нули цифровой последовательности, составляющей зашифрованное сообщение, либо ключ, либо то и другое в виде двух параллельно передаваемых сигналов.

• Передаваемые сигналы разнести по различным каналам:

- в беспроводных КЛС с применением первой и второй гармоник,
- в ВОЛС применить многомодовые ОВ, по каждой моде передавать указанные сигналы.

• Методы кодирования нулей и единиц менять псевдослучайным способом.

Такой способ разумнее применять в ВОЛС, использующих многомодовые ОВ.

4 Выбор методов модельного представления КЛС

Выбор проведен на основе известности видов кодирования сигналов. Как показывает анализ доступной литературы, возможны два вида физического кодирования:

• С помощью выбора спинов фотонов.

• С помощью выбора векторов поляризации монохроматического когерентного излучения.

Ясно, что для модели второго вида приемлемо решение уравнений Максвелла. Проанализируем их с точки зрения поставленных задач.

4.1 Моделирование КЛС, применяющего способ поляризационного кодирования

В качестве базовой модели электромагнитного излучения приняты основные уравнения Максвелла. Для условий исследований приближения электродинамики обладают должной адекватностью.

$\nabla E = \frac{\rho}{\varepsilon \varepsilon_0}$ - уравнение для свободной среды,

E – вектор электрического поля, ρ - плотность тока смещения, $\varepsilon \varepsilon_0$ - диэлектрические проницаемости.

$\nabla * E = 0$ - *поле при отсутствии источников*

$\nabla * E = \frac{\partial^2 B}{\partial t^2}$. - связь электрического и магнитного полей в свободной среде без источников,

$\nabla * B = j\mu\mu_0 + \frac{\varepsilon\mu}{C^2}\frac{\delta E}{\delta t}$ - магнитное поле в свободной среде без источников.

B - вектор магнитного поля, μ, μ_0 магнитные проницаемости.

Волновое уравнение. При отсутствии зарядов и токов можно перейти к уравнениям второго порядка, каждое из которых зависит только от одного, электрического или магнитного поля:

$$\nabla E = \frac{\varepsilon\mu}{c^2}\frac{\partial^2 E}{\partial t^2} = 0, \quad \nabla E = \frac{\varepsilon\mu}{c^2}\frac{\partial^2 E}{\partial t^2}$$

Численные решения уравнений Максвелла методом конечных разностей показали правильность выбранных моделей. Результаты численных экспериментов приведены на рис. 3.

Один из результатов моделирования прохождения излучения через линзу с учетом расчета вектора поляризации приведен на рис.4.

Один из результатов моделирования утечки излучения через куплер для линии связи с применением ОВ с учетом расчета вектора поляризации приведен на рис.5.

Таким образом, можно убедиться, что предлагаемая методика приемлема и для моделирования утечки из ОВ. Программа, позволяющая решать уравнения Максвелла методом конечных разностей любезно предоставлена сотрудником центра «Фотоника» МГТУ им. Н.Э. Баумана В.Л. Толстогузовым.

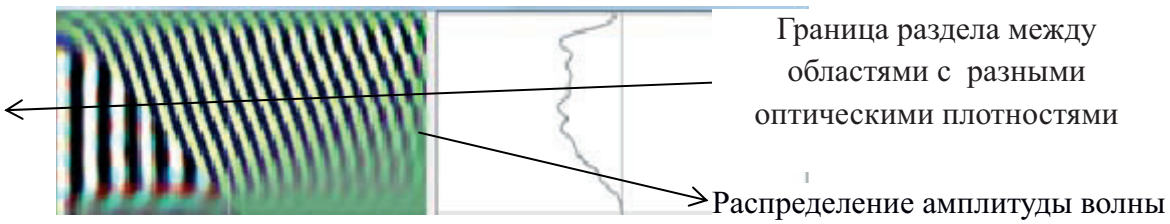

***Рис.3**. Пример прохождения излучения через границу двух диэлектрических сред.*

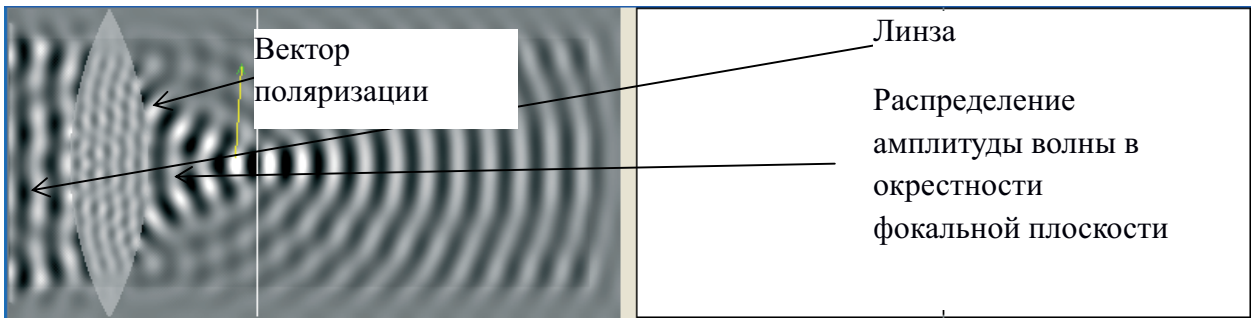

***Рис. 4.** Прохождение излучения через линзу.*

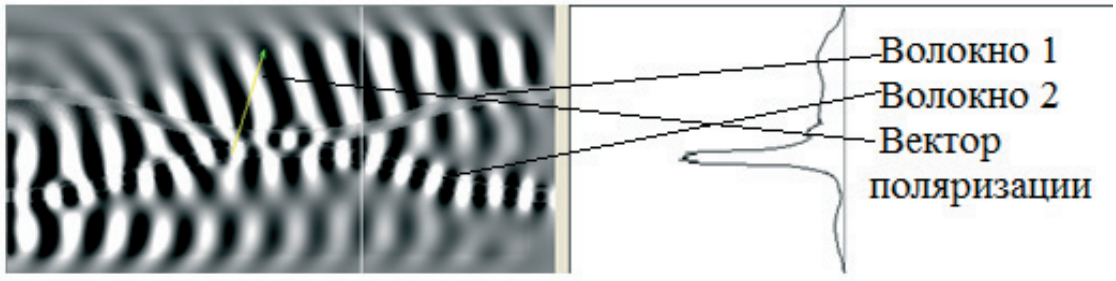

***Рис. 5**. Прохождение излучения через куплер.*

5. Методика моделирования квантового кодирования сообщений

Как показал анализ, проведенный выше, при проектировании квантово-криптографических каналов разумно проводить численные эксперименты. Задачи проектирования и криптоанализа целесообразно решать путем моделирования атак методом статистических испытаний (Монте-Карло). В свою очередь, для решения практических задач требуется решение уравнений Шредингера и Гейзенберга. Они составляют основу моделей, применимых для проектирования методов кодирования и криптоанализа.

Известно [8], уравнение Гейзенберга тесно связано с уравнением Шредингера - линейным обыкновенным дифференциальным уравнением второго порядка вида:

$$\frac{-h^2}{8\pi^2 m}\frac{d^2}{d^2}\{\psi(x)\}+U(x)\psi(x)=E\psi(x) \qquad (3)$$

Где h — постоянная Планка, m — масса частицы, $U(x)$ — потенциальная энергия, E — полная энергия, $\psi(x)$— волновая функция.

В свободном пространстве, где отсутствуют потенциалы уравнение (3) принимает особенно простой вид:

$$\frac{-h^2}{8\pi^2 m}\frac{d^2}{d^2}\{\psi(x)\}+U(x)\psi(x)=E\psi(x),$$

или:

$$\frac{-h^2}{8\pi^2 m}\frac{d^2}{d^2}\{\psi(x)\}=E\psi(x). \qquad (4)$$

Для этого уравнения решением является суперпозиция плоских волн [8] (сравните с решениями волнового уравнения). Итак, общее решение:

$$\psi(x)=¿\ C_1 exp\{j\frac{\sqrt{8\pi}Ex}{h}\}+¿\ C_1 exp\{-j\frac{\sqrt{8\pi}Ex}{h}\}. \qquad (5)$$

Выражение (5) соответствует модели осциллирующего процесса, и, после дополнения значением фазового сдвига, может иллюстрироваться на рис. 6.

1	0	1 1	0	1	0

Рис.6. *График функции (5) с поправкой на фазовый сдвиг.*

Здесь энергия E может принимать все значения выше нуля, поэтому говорят, что собственное значение принадлежит непрерывному спектру. Константы C_1 и C_2 определяются из условия нормировки.

В случае применения для кодирования значения положения вектора поляризации, для моделирования кодирования с достаточной долей адекватности можно принимать следующее. Если пропустить естественный свет через два поляризатора, главные плоскости которых образуют угол, то из первого выйдет плоско-поляризованный свет, интенсивность которого $I_0 = 1/2\ I_{ест}$, из второго выйдет свет интенсивностью $I = I_0 \cos^2 a$.

Откуда $I = I_{max} = 1/2\ I_{ест}$ (если поляризаторы параллельны) и $I = I_{min} = 0$ (если поляризаторы скрещены).

Следует заметить, что при поляризационном кодировании вполне уместно примерять модель, построенную на основе волнового уравнения. Далее приведено уравнение для вектора поляризации, полученного на основе волнового уравнения: $\vec{P} = \chi(\vec{E})\vec{E}$.

Отдельного обсуждения требует задача моделирования криптографических каналов, в которых применяется вторая гармоника излучения. Как известно [7], излучение на второй гармонике используется для перехвата излучения из пассивной аппаратуры.

Как известно, для формирования второй гармоники широко используются нелинейные кристаллы. Для решения задачи о распространении волны в кристалле необходимо решить уравнение:

$$rotrot\ \overline{E} + \frac{1}{c^2}\frac{\partial^2 \overline{E}}{\partial t^2} + \frac{4\pi}{c^2}\frac{\partial^2 \overline{P}_{л}}{\partial t^2} + \frac{4\pi}{c^2}\frac{\partial^2 \overline{P}_{нл}}{\partial t^2} = 0 \qquad (6)$$

Задача (1) распространения света в нелинейной среде не имеет аналитического решения. Поэтому на практике используют косвенный подход, заключающийся в следующем:

Рассматривается падающая гармоническая волна:

$$E_1 = A_1 \cos(\varpi_1 t - \kappa_1 z), \text{ где } \kappa_1 = \frac{\varpi}{c} n(\varpi), \qquad (7)$$

Где $\acute{\omega}$ угловая частота, вызывающая нелинейные колебания диполей по ходу, которые в свою очередь испускают вторичную волну с частотой $2\acute{\omega}$:

$$E_2 = A_2 \cos(2\varpi t - \kappa_2 z), \text{ где } \kappa_2 = \frac{2\varpi}{c} n(2\varpi). \qquad (8)$$

Наиболее эффективным для возбуждения второй гармоники является направление, при котором $\cos\varphi = 1$. При этом , $n(\omega)=n(2\omega)$, что невозможно в изотропных средах. В анизотропных кристаллах имеются направления, в которых $n_o(\omega)=n_e(2\omega)$, это направления пространственного синхронизма. Для получения второй гармоники волны должны распространяться по данному направлению. Формулы Френеля должны быть применимы и для нелинейного случая. Должна появиться и «отраженная» вторая гармоника, т.е. в отраженном свете есть волны ϖ_1 и $2\varpi_1$. Попутным эффектом, положительным для беспроводных КЛС является самофокусировка и самодефокусировка света.

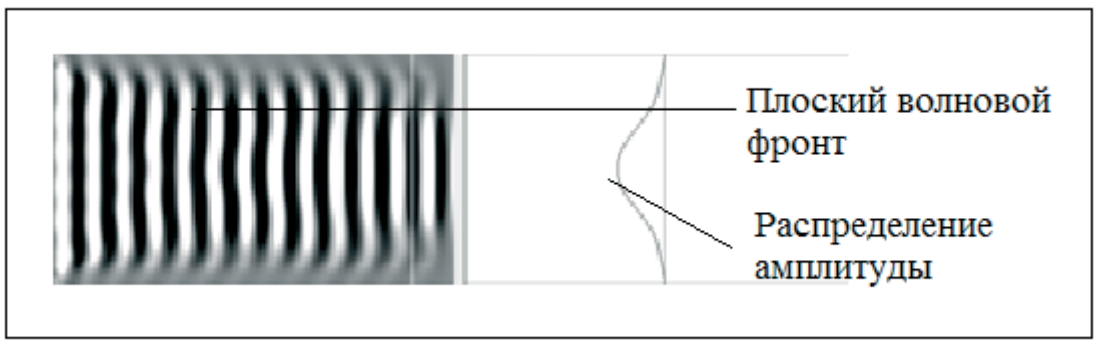

Рис. 7*. Результат численного решения волнового уравнения.*

Если среда линейная, т.е. $n_2=0$ и распространяется пучок диаметром d, то можно считать, что до дальностей $z_g = \frac{d^2}{4\lambda}$ пучок не расходится, в дальнейшем при $z > z_g$ наблюдается расходимость и $2\alpha = \frac{1{,}2}{d}\lambda$. Для лазерных пучков распределение интенсивности по сечению Гауссово. В случае нелинейной среды, $n=n_0+n_2I$ и фазовая скорость по сечению пучка неодинакова.

Если $n_2<0$, то скорость движения центра пучка больше, чем периферии. Фронт волны выгибается, наблюдается явление самодефокусировки или нелинейной рефракции. Если $n_2>0$, то середина волнового фронта отстает от его периферии, лучи стремятся собраться в центр пучка.

Заключение

Проведенные анализ и исследования позволяют заключить следующее:

• Для модельного представления процесса кодирования в поляризационных криптографических линиях связи применимы решения классических уравнений электродинамики.

• Для модельного представления процесса кодирования в квантовых криптографических линиях применимы уравнения гармонического осциллятора.

• Для защиты КЛС, использующей для кодирования положение вектора поляризации предлагается использовать многомодовое волокно и передавать ключ по одной моде, а кодируемое сообщение – по другому. Остальные моды применять для дезинформации.

Литература (References):

1. Килин С. Я. «Квантовая информация / Успехи Физических Наук.» — 1999. — Т. 169. — С. 507—527.
2. В.А. Гайслер, «Наука в Сибири» / № 50 (2785), 23.12.2010 г. Фотоны поштучно.
3. Официальный сайт: http://www.vox.com/2014/4/9/5588236/quantum-computing-explained In 2012, a UC Santa Barbara quantum computer made up of four qubits factored the number 15 (its factors are 3 and 5), последний доступ – 15.02.2015.
4. http://www.ia.ucsb.edu/pa/display.aspx?pkey=2803#description', Nature Communicaion «Perfect eavesdropping on a quantum cryptography system».
5. Nature Communicaion «Full-field implementation of a perfect eavesdropper on a quantum cryptography system, June 2011».
6. Robert Malaney . «Технологии, основанные на принципе ULV (unconditional location verification)», Computerworld Россия , № 37, 2007.
7. Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin, «Experimental Quantum Cryptography», J. of Cryptography 5, 1992.
8. Прокис Дж. Цифровая связь. — Пер. с англ. // Под ред. Д. Д. Кловского. — М.: Радио и связь, 2000. — 800 с. — ISBN 5-256-01434-X.
9. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. — Пер. с англ. — М.: Издательский дом «Вильямс», 2003. — 1104 с. — ISBN 5-8459-0497-8.
10. Феер К. Беспроводная цифровая связь: методы модуляции. — Пер. с англ. // Под. ред. В. И. Журавлёва. — М.: Радио и связь, 2000.
11. Официальный сайт: www.krdu-mvd.ru/_files/kafedra_ib/17.pdf, «Технические средства и методы защиты информации», последний доступ – 10.02.2015.
12. Recent Progress of hotosensor, Kwok K. Ng Complete Guide to Semiconductor Devices. — 2. — Wiley-Interscience, 2002.
13. Tarof, L.E. (1991). «Planar InP/GaAs Avalanche Photodetector with Gain-Bandwidth Product in Excess of 100 GHz». Electronics Letters 27: 34–36. DOI:10.1049/el:19910023.
14. Wu, W.; Hawkins, A.R.; Bowers, J.E. (1997). «Design of InGaAs/Si avalanche photodetectors for 400-GHz gain-bandwidth product». Proceedings of SPIE 3006: 36–47. DOI:10.1117/12.264251.
15. Campbell, J. C. (2007). «Recent advances in Telecommunications Avalanche Photodiodes». IEEE Journal of Lightwave Technology 25: 109–121. DOI:10.1109/JLT.2006.888481.