КВАНТОВАЯ КРИПТОГРАФИЯ: ПРИНЦИПЫ, ПРОТОКОЛЫ, СИСТЕМЫ

Д.М. Голубчиков, К.Е. Румянцев

Таганрогский технологический институт Южного федерального университета
347928, Ростовская область, г. Таганрог, пер. Некрасовский, д. 44

Аннотация. Изложены этапы развития формирования теории квантовой криптографии. Освещены два основных направления развития систем квантового распределения ключей. Дан сравнительный анализ существующих протоколов распределения ключей: BB84, B92, 4+2, с шестью состояниями, Гольденберга-Вайдмана, Коаши-Имото и ЭПР. Приведены типовые структуры систем квантового распределения ключей на основе кодирования информации в поляризационных, фазовых и временных состояниях фотонов. Сформулированы перспективы развития систем квантового распределения ключей.

Annotation. The stages of development of quantum cryptography's theory are expounded. Two main directions of developing of quantum key distribution system are elucidated. Comparative analysis of present distribution key protocols (BB84, B92, 4+2, with 6 states, Goldenberg-Vaidman, Koashi-Imoto, EPR) is given. Standard structures of quantum key distribution systems based on coding of information in polarized, phase and time states of photons are given. Prospects of development of quantum key distribution systems are formulated.

1. История квантовой криптографии

Стивен Визнер (Stephen Wiesner), являясь студентом Колумбийского университета, в 1970 подал статью по теории кодирования в журнал IEEE Information Theory, но она не была опубликована, так как изложенные в ней предположения казались фантастическими, а не научными. Именно в [1] была описана идея возможности использования квантовых состояний для защиты денежных банкнот. Визнер предложил в каждую банкноту вмонтировать 20 так называемых световых ловушек, и помещать в каждую из них по одному фотону, поляризованному в строго определенном состоянии. Каждая банкнота маркировалась специальным серийным номером, который заключал информацию о положении поляризационного фотонного фильтра. В результате этого при применении отличного от заданного фильтра комбинация поляризованных фотонов стиралась. Но на тот момент технологическое развитие не позволяло даже рассуждать о таких возможностях. Однако в 1983 году его работа «Сопряженное кодирование» была опубликована в SIGACT News и получила высокую оценку в научных кругах.

В последствии на основе принципов работы Визнера С. ученые Чарльз Беннет (Charles Bennett) из фирмы IBM и Жиль Брассард (Gilles Brassard) из Монреальского университета разработали способ кодирования и передачи сообщений. Ими был сделан доклад на тему «Квантовая криптография: Распределение ключа и подбрасывание монет» на конференции IEEE International Conference on Computers, Systems, and Signal Processing. Описанный в работе [2] протокол впоследствии признан первым и базовым протоколом квантовой криптографии и был назван в честь его создателей BB84. Для кодирования информации протокол использует четыре квантовых состояния микросистемы, формируя два сопряжённых базиса.

В это время Артур Экерт работал над протоколом квантовой криптографии, основанном на спутанных состояниях [3]. Опубликование результатов его работ состоялось в 1991 году. В основу положены принципы парадокса Эйнштейна–Подольсого-Розенберга, в частности принцип нелокальности спутанных квантовых объектов.

На протяжении двадцати пяти лет, квантовая криптография прошла путь от теоретических исследований и доказательства основных теорий до коммерческих систем, использующих оптическое волокно для передачи на расстояние десятков километров.

В первой экспериментальной демонстрации установки квантового распределения ключей проведенной в 1989 в лабораторных условиях [4], передача осуществлялась через открытое пространство на расстояние тридцати сантиметров. Далее эти эксперименты были проведены с использованием оптического волокна в качестве среды распространения. После первых экспериментов Мюллера и др. в Женеве, с использованием оптоволокна длиной 1,1 км [5, 6], в 1995 расстояние передачи было увеличено до 23 км через оптическое волокно, проложенное под водой [7, 8]. Приблизительно в то же время, Таунсендом из British Telecom была продемонстрирована передача на 30 км [9]. Позднее он, продолжив тестирование систем с использованием различных конфигураций оптических сетей [10, 11], увеличил дальность до 50 км [12]. Эксперименты по передаче на это же расстояние были позднее повторены Хьюзом и др. в Лос-Аламосе [13]. В 2001г., Хискетом и др. в Соединенном Королевстве была осуществлена передача на расстояние 80 км [14]. В 2004-2005гг., две группы в Японии и одна в Соединенном Королевстве сообщили об осуществлении экспериментов по квантовому распределению ключей и интерференции одиночных фотонов на расстояние свыше 100 км [15, 16, 17]. Первые эксперименты по передаче на расстояние 122 км проводились учеными из Toshiba в Кембридже с использованием детекторов на основе лавинных фотодиодов (ЛФД) [16]. Рекорд по дальности передачи информации принадлежит объединению ученых Лос-Аламоса и Национального института стандартов и технологий, и составляет 184 км [18]. В нем использовались однофотонные приемники охлаждаемые до температур близких к нулевым по Кельвину.

Первая презентация коммерческой системы квантовой криптографии произошла на выставке CeBIT-2002. Там, швейцарские инженеры компании GAP-Optique (www.gap-optique.unige.ch) из Женевского университета представили первую систему квантового распределения ключей (QKD – Quantum Key Distribution). Ученым удалось создать достаточно компактное и надежное устройство. Система располагалась в двух

19-дюймовых блоках и могла работать без настройки сразу после подключения к персональному компьютеру. С его помощью была установлена двухсторонняя наземная и воздушная волоконно-оптическая связь между городами Женева и Лузанна, расстояние между которыми составляет 67 км [19]. Источником фотонов служил инфракрасный лазер с длиной волны 1550 нм. Скорость передачи данных была невысока, но для передачи ключа шифра (длина от 27,9 до 117,6 кбит) большая скорость и не требуется.

В последующие годы к проектированию и изготовлению систем квантовой криптографии подключились такие коммерческие монстры как Toshiba, NEC, IBM, Hewlett Packard, Mitsubishi, NTT . Но наряду с ними стали появляться на рынке и маленькие, но высокотехнологичные компании: MagiQ (www.magiqtech.com), Id Quantique (www.idquantique.com), Smart Quantum (www.smartquantum.com). В июле 2005 в гонке за увеличение расстояния передачи ключа вперед вышли инженеры Toshiba, представив на рынке системы способную передать ключ на 122 км. Однако, как и у конкурентов, скорость генерации ключа в 1,9 кбит/с оставляла желать лучшего (http://www.toshiba-europe.com/research/crl/QIG/quantumkeyserver.html). Производители в настоящие время стремятся к разработке интегрированных систем – новинкой от Id Quantique, является система Vectis, использующая квантовое распределение ключей для создания VPN туннелей, шифрующая данные на канальном уровне с помощью шифра AES. Ключ может быть 128, 196 или 256-битной длины и меняется с частотой до 100 Гц. Максимальная дистанция для данной системы составляет 100 км. Все вышеперечисленные компании производят системы кодирующие информацию о битах ключа в фазовых состояниях фотонов. Со времен первых реализаций, схемы построения систем квантового распределения ключей значительно усложнились.

Британские физики из коммерческого подразделения QinetiQ Британской оборонной исследовательской лаборатории и немецкие физики из Мюнхенского университета Людвига-Максимиллиана впервые осуществили передачу ключа на расстояние 23,4 км непосредственно через воздушное пространство без использования оптического волокна [20]. В эксперименте для кодирования криптографической информации использовались поляризации фотонов — одна для передачи двоичного символа «0» и противоположная для символа «1». Эксперимент проводился в горах

Южной Германии. Слабый импульсный сигнал посылался ночью с одной горной вершины (2 950 м) на другую (2 244 м), где находился счетчик фотонов.

Руководитель проекта Джон Рэрити (John Rarity) из QinetiQ полагал [21], что уже в 2005 году будет проведен эксперимент с посылкой криптографического ключа на низкоорбитальный спутник, а к 2009 году с их помощью можно будет посылать секретные данные в любую точку планеты. Отмечалось, что для этого придется преодолеть ряд технических препятствий. Во-первых, необходимо улучшить устойчивость системы к неизбежной потере фотонов при их посылке на расстояния в тысячи километров. Во-вторых, существующие спутники не оснащены соответствующим оборудованием для пересылки криптографических данных по квантовому протоколу, так что потребуется конструирование и запуск совершенно новых спутников [22].

Исследователи из Северо-западного университета (Эванстон, штат Иллинойс) продемонстрировали технологию, позволяющую передавать на небольшое расстояние шифрованное сообщение со скоростью 250 Мбит/с [23]. Ученые предложили метод квантового кодирования самих данных, а не только одного ключа. В этой модели учитывается угол поляризации каждого переданного фотона, Поэтому любая попытка декодировать сообщение приводит к такой зашумленности канала, что всякая расшифровка становится невозможной. Исследователи обещают, что уже модель следующего поколения сможет работать практически на магистральной скорости Интернета порядка 2,5 Гбит/с. По словам одного из разработчиков, профессора Према Кумара (Prem Kumar), "еще никому не удавалось выполнять квантовое шифрование на таких скоростях". Ученые уже получили несколько патентов на свои разработки и сейчас работают вместе со своими промышленными партнерами Telcordia Technologies и BBN Technologies над дальнейшим усовершенствованием системы. Первоначально рассчитанный на пять лет проект был поддержан грантом DARPA (the Defense Advanced Research Projects Agency) в 4,7 миллиона долларов. Результатом данного проекта стала система квантового кодирования AlphaEta [24].

Группа Ричарда Хьюгса (Richard Hughes) из Лос-Аламоса занимается разработками спутниковых оптических линий связи (ОЛС). Для реализации преимуществ квантовой криптографии фотоны должны проходить через атмосферу без

поглощения и изменения поляризации. Для предотвращения поглощения исследователи выбирают длину волны в 770 нм, соответствующую минимальному поглощению излучения молекулами атмосферы. Сигнал с большей длиной волны также слабо поглощается, но более подвержен турбулентности, которая вызывает изменение локального показателя преломления воздушной среды и, ввиду этого, изменение поляризации фотонов. Ученым приходится решать и побочные задачи. Спутник, наряду с фотонами, несущими сообщение, может принять и фотоны фонового излучения, исходящего как от Солнца, так и отраженного Землей или Луной. Поэтому применяются сверхузконаправленный приемник, а также фильтр для отбора фотонов определенной длины волны. Кроме того, фотоприемник чувствителен к приему фотонов в течение 5 нс периодически с интервалом в 1 мкс. Это должно быть согласовано с параметрами передатчика. Такие ухищрения вновь обуславливают влияние турбулентности. Даже при сохранении поляризации, вследствие турбулентности может измениться скорость передачи фотонов, приводя к фазовому дрожанию. С целью компенсации фазового дрожания впереди каждого фотона высылается световой импульс. Этот синхронизирующий импульс, подвергается такому же, как следующий за ним фотон, влиянию атмосферы. Поэтому независимо от момента получения импульса приемник спутника знает, что через 100 нс нужно открыться для приема информационного фотона. Изменение показателя преломления вследствие турбулентности вызывает уход луча от антенны. Поэтому для направления потока фотонов передающая система отслеживает слабое отражение от синхроимпульсов. Группой Хьюгса осуществлена передача сообщения по квантовому криптографическому каналу через воздушную среду на расстояние в 500 м на телескоп диаметром 3.5 дюйма [25]. Принимаемый фотон попадал на распределитель, который направлял его на тот или иной фильтр. После этого ключ контролировался на наличие ошибок. Реально, даже при отсутствии перехвата, уровень ошибок достигал 1,6% из-за наличия шума, фоновых фотонов и рассогласования. Это несущественно, поскольку при перехвате уровень ошибок обычно более 25%.

Позднее группой Хьюгса было передано сообщения по квантовому каналу через воздушную среду на расстояние 2 км [26, 27]. При испытаниях сигналы передавались горизонтально, вблизи поверхности Земли, где плотность воздуха и флуктуации

интенсивности максимальны. Поэтому расстояние в 2 км вблизи поверхности Земли эквивалентны 300 км, отделяющим низкоорбитальный искусственный спутник от Земли.

Таким образом, менее чем за 50 лет квантовая криптография прошла путь от идеи до воплощения в коммерческую систему квантового распределения ключей. Действующая аппаратура позволяет распределять ключи через квантовый канал на расстояние превышающие 100 км (рекорд 184 км), со скоростями достаточными для передачи ключей шифрования, но не достаточными для поточного шифрования магистральных каналов с помощью шифра Вернама. Основными потребителями систем квантовой криптографии в первую очередь выступают министерства обороны, министерства иностранных дел и крупные коммерческие объединения. На настоящий момент высокая стоимость квантовых систем распределения ключей ограничивает их массовое применение для организации конфиденциальной связи между небольшими и средними фирмами и частными лицами.

2. Основные направления развития квантовой криптографии

В квантовой криптографии выделились два основных направления развития систем распределения ключей.

Первое направление основано на кодировании квантового состояния одиночной частицы и базируется на принципе *невозможности различить абсолютно надёжно два неортогональных квантовых состояния.*

Произвольное состояние любой двухуровневой квантово-механической системы можно представить в виде линейной суперпозиции

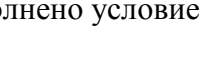
$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

её собственных состояний $|0\rangle$ и $|1\rangle$ с комплексными коэффициентами α и β, причем

$$|\alpha|^2 + |\beta|^2 = 1.$$

Законы квантовой механики не позволяют абсолютно надёжно различить два квантовых состояния

и

если не выполнено условие  , т.е. если состояния ортогональны.

Защищенность первого направления основывается на *теореме о запрете клонирования неизвестного квантового состояния*. Благодаря унитарности и линейности квантовой механики, невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние. Пусть, например, отправитель (назовём его Алиса) и получатель (Боб) используют для передачи информации двухуровневые квантовые системы, кодируя состояния этих систем. Если злоумышленник (Ева) перехватывает носитель информации, посланный Алисой, измеряет его состояние и пересылает далее Бобу, то состояние этого носителя будет иным, чем до измерения. Таким образом, подслушивание квантового канала приводит к ошибкам передачи, которые могут быть обнаружены легальными пользователями.

Основным протоколом квантовой криптографии на одночастичных состояниях

является протокол BB84 [2].

Второе направление развития основано на эффекте *квантового перепутывания (запутывания)***.** Две квантово-механические системы (в том числе и разделённые пространственно) могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое над одной из систем, определит результат измерения этой величины на другой. Ни одна из запутанных систем не находится в определённом состоянии. Поэтому запутанное состояние не может быть записано как прямое произведение состояний систем. Состояние двух частиц со спином 1/2 может служить примером запутанного состояния:

$$|\Psi_0\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Измерение, проведённое на одной из двух подсистем, дает с равной вероятностью состояния $|0\rangle$ или $|1\rangle$. Состояние же другой подсистемы будет противоположным, т.е. $|0\rangle$, если результат измерения на первой системе был $|1\rangle$, и наоборот.

Базовым протоколом квантового распределения ключей на основе эффекта квантового запутывания является протокол EPR (Einstein-Podolsky-Rosen), второе его название E91[3].

Базовые принципы этих двух направлений легли в основу разработки всех протоколов квантового распределения ключей.

3. Протоколы квантовой криптографии

Существует множество протоколов квантовой криптографии основанных на передаче информации посредством кодирования в состояниях одиночных фотонов, например: BB84, B92 [28], BB84(4+2) [29], с шестью состояниями [30], Гольденберга-Вайдмана [31], Коаши-Имото [32] и их модификации. Единственный протокол, разработанный для кодирования информации в спутанных состояниях – E91. Рассмотрим более подробно существующие протоколы квантового распределения ключей.

Квантовый протокол BB84

В протоколе BB84 используются 4 квантовых состояния фотонов, например, направление вектора поляризации, одно из которых Алиса выбирает в зависимости от передаваемого бита: 90° или 135° для «1», 45° или 0° для «0». Одна пара квантовых состояний соответствует $0\left(\left|0(+)\right\rangle\right)$ и $1\left(\left|1(+)\right\rangle\right)$ и принадлежит базису «+». Другая пара квантовых состояний соответствует $0\left(\left|0(\times)\right\rangle\right)$ и $1\left(\left|1(\times)\right\rangle\right)$ и принадлежит базису «×». Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно неортогональными (неортогональность необходима для детектирования попыток съёма информации).

Квантовые состояния системы можно описать следующим образом:

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

Здесь состояния $\left|0_{+}\right\rangle$ и $\left|1_{+}\right\rangle$ кодируют значения «0» и «1» в базисе «+», а $\left|0_{\times}\right\rangle$ и $\left|1_{\times}\right\rangle$ кодируют те же значения в базисе «×». Базисы повернуты друг относительно друга на 45° (рисунок 1).

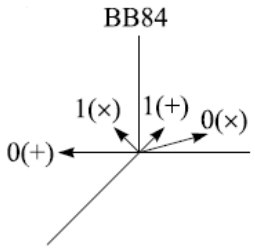


Рисунок 1 – Состояния поляризации фотонов, используемые в протоколе BB84

Этапы формирования ключей:

1) Алиса случайным образом выбирает один из базисов. Затем внутри базиса случайно выбирает одно из состояний, соответствующее 0 или 1 и посылает фотоны (рисунок 2):

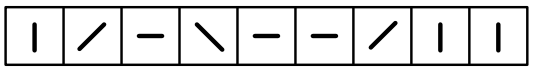


Рисунок 2 - Фотоны с различной поляризацией

2) Боб случайно и независимо от Алисы выбирает для каждого поступающего фотона: прямолинейный (+) или диагональный (×) базис (рисунок 3):

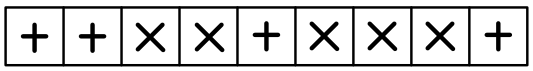


Рисунок 3 - Выбранный тип измерений

Затем Боб сохраняет результаты измерений:

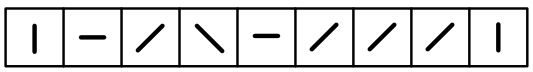


Рисунок 4 - Результаты измерений

3) Боб по открытому общедоступному каналу связи сообщает, какой тип измерений был использован для каждого фотона, то есть какой был выбран базис, но результаты измерений остаются в секрете;

4) Алиса сообщает Бобу по открытому общедоступному каналу связи, какие измерения были выбраны в соответствии с исходным базисом Алисы (рисунок 5):

Рисунок 5 - Случаи правильных замеров

5) далее пользователи оставляют только те случаи, в которых выбранные базисы совпали. Эти случаи переводят в биты (0 и 1), и получают, таким образом, ключ (рисунок 6):

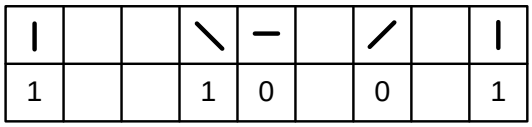


Рисунок 6 - Получение ключевой последовательности по результатам правильных замеров

Число случаев, в которых выбранные базисы совпали, будет составлять в среднем половину длины исходной последовательности, т.е. $n = \frac{1}{2}$ (пример определения количества фотонов, принятых Бобом, показан в таблице 1).

Таблица 1 - Формирование квантового ключа по протоколу BB84

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

Таким образом, в результате передачи ключа Бобом в случае отсутствия помех и искажений будут правильно зарегистрированы в среднем 50% фотонов.

Однако идеальных каналов связи не существует и для формирования секретного ключа необходимо провести дополнительные процедуры поиска ошибок и усиления секретности. При этом для части последовательности бит пользователей, в которых базисы совпали, через открытый общедоступный канал связи случайным образом раскрываются и сравниваются значения бит. Далее раскрытые биты отбрасываются. В идеальном квантовом канале (без шума) достаточно выявить несоответствие в одной раскрытой позиции для обнаружения злоумышленника. В реальной ситуации невозможно различить ошибки, произошедшие из-за шума и из-за воздействия злоумышленника. Известно, что если процент ошибок QBER ≤ 11%, то пользователи из нераскрытой последовательности, после коррекции ошибок через открытый общедоступный канал связи и усиления секретности, могут извлечь секретный ключ, который будет у них одинаковым и не будет известен Еве. Ключ, полученный до дополнительных операций с последовательностью, называется "сырым" ключом.

При коррекции ошибок эффективным способом для согласования последовательностей Алисы и Боба является их «перемешивание» для более равномерного распределения ошибок и разбиение на блоки размером k, при котором вероятность появления блоков с более чем одной ошибкой пренебрежимо мала. Для каждого такого блока стороны производят проверку чётности. Блоки с совпадающей чётностью признаются правильными, а оставшиеся делятся на несколько более мелких блоков, и проверка чётности производится над каждым таким блоком, до тех пор, пока ошибка не будет найдена и исправлена. Процедура может быть повторена с блоками более подходящего размера. Наиболее мелкие блоки отбрасываются при наличии в них ошибки.

Когда в каком-либо блоке количество ошибок окажется чётным, то даже с оптимальным размером блока некоторые из них могут быть не выявлены. Для их исключения производят перемешивание последовательности бит, разбиение её на блоки и сравнение их чётности производится ещё несколько раз, каждый раз с уменьшением размера блоков, до тех пор, пока Алиса и Боб не придут к выводу, что вероятность ошибки в полученной последовательности пренебрежимо мала.

В результате всех этих действий Алиса и Боб получают идентичные последовательности бит. Эти биты и являются ключом, с помощью которого

пользователи получают возможность кодировать и декодировать секретную информацию и обмениваться ей по незащищённому от съема информации каналу связи.

Квантовый протокол B92

В протоколе используются фотоны, поляризованные в двух различных направлениях для представления нулей и единиц ($|\varphi_0\rangle$ и $|\varphi_1\rangle$, $\langle\varphi_0|\varphi_1\rangle \neq 0$). Фотоны, поляризованные вдоль направления $+45^0$, несут информацию о единичном бите, фотоны, поляризованные вдоль направления 0^o(V) – о нулевом бите. Эти состояния удобно для наглядности изображать графически (рисунок 7).

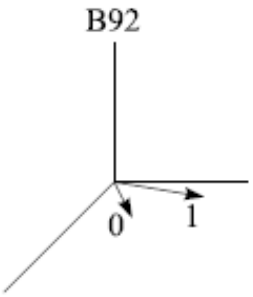


Рисунок 7 - Поляризационные состояния, используемые в протоколе B92

Алгоритм работы протокола B92:

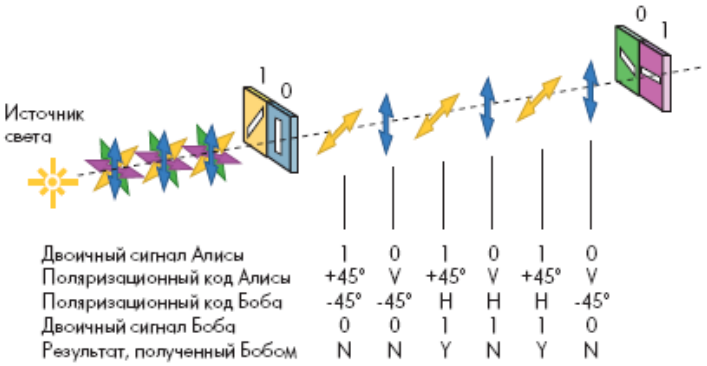


Рисунок 8 - Формирование квантового ключа по протоколу B92

Станция Алиса посылает фотоны, поляризованные в направлениях *0* и $+45^0$, представляющие нули и единицы. Причем последовательность фотонов, посылаемая станцией Алиса, случайно ориентирована. Станция Боб принимает фотоны через фильтры ориентированные под углом 90^0 и $135^0(-45^0)$. При этом если фотон, переданный станцией Алиса, будет анализирован станцией Боб при помощи фильтра ориентированного под углом 90^0 по отношению к передаваемому фотону, то фотон не пройдет через фильтр. Если же этот угол составит 45^0, то фотон пройдет через фильтр с вероятностью *0,5*.

Для определения поляризации станция Боб анализирует принимаемые ей фотоны, используя выбранный случайным образом один из двух неортогональных базисов «+» или «×». Если станция Боб анализирует посланный фотон фильтром с ортогональным направлением поляризации, то он не может точно определить, какое значение данный фотон представляет: *1*, соответствующее фотону, который не проходит, или *0*, соответствующее фотону, который не проходит с вероятностью *0,5*. Если же направления поляризации между посланным фотоном и фильтром, неортогональны, то станция Боб может определить, что принят фотон соответствующий *0*. Если фотон был принят удачно, то очередной бит ключа кодируется *0* (если фотон был принят фильтром, ориентированным под углом 135^0), либо *1* (если фотон был принят фильтром, ориентированным по направлению *H*) (таблица 2)

Таблица 2 - Формирование квантового ключа по протоколу B92

Двоичный сигнал станции Алиса	1	0	1	0
Поляризационный код станции Алиса	⬀	⇕	⬀	⇕
Поляризационный код станции Боб	⬂	⬂	↔	↔
Двоичный сигнал станции Боб	0	0	1	1
Результат, полученный станцией Боб	-	-	+	-

В первой и четвертой колонке поляризации при передаче и приеме ортогональны и результат детектирования будет отсутствовать. В колонках 2 и 3 коды

двоичных разрядов совпадают и поляризации не ортогональны. По этой причине с вероятностью *50%* может быть положительный результат в любом из этих случаев (и даже в обоих). В таблице предполагается, что успешное детектирование фотона происходит для случая, представленного в колонке 3. Именно этот бит становится первым битом общего секретного ключа передатчика и приемника. Отсюда минимальное количество фотонов, которое может быть принято станцией Боб $n = \frac{1}{4}$. То есть в результате передачи такого ключа, около *25%* фотонов будут правильно детектированы станцией Боб.

После этого по открытому каналу связи станция Боб может передать станции Алиса, какие *25* фотонов из каждых *100* были ей получены. Данная информация и будет служить ключом к новому сообщению. При этом чтобы злоумышленник не узнал информацию о ключе, по открытому каналу связи можно передать информацию только о том, какие по порядку фотоны были приняты, не называя состояния фильтров и полученные значения поляризации. После этого станция Алиса может передавать сообщения Бобу зашифрованные этим ключом.

Для обнаружения факта съема информации в данном протоколе используют контроль ошибок, аналогичный контролю ошибок в протоколе BB84. То есть, станции Алиса и Боб сверяют случайно выбранные биты ключа. Если обнаруживаются несовпадения, то можно говорить о несанкционированном съеме информации.

Рассмотренные выше протоколы являются основными. Однако существует ряд производных протоколов. Приведем некоторые из них.

Протокол с шестью состояниями

Исходно представляет протокол BB84, но ещё с одним базисом, а именно:

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

В соответствии с этим, существует ещё два возможных направления поляризации для переданного фотона: правоциркулярное и левоциркулярное.

Таким образом, можно посчитать количество фотонов, которые будут приняты станцией Боб.

Таблица 3 - Формирование квантового ключа по протоколу с шестью состояниями

Двоичный сигнал станции Алиса	1	0	1	0	1	0
Поляризационный код станции Алиса	⇗	⇕	↔	⇘	↺	↻
Детектирование станции Боб	✥	✥	✥	✥	✥	✥
Двоичный сигнал станции Боб	?	0	1	?	?	?

Из таблицы 3 видно, что минимальное количество фотонов, которое будет принято станцией Боб при детектировании $n = \frac{2}{6} = \frac{1}{3}$. То есть при использовании протокола с шестью состояниями будет принято около *33%* фотонов посылаемых станцией Алиса.

Квантовый протокол BB84(4+2)

Данный протокол является промежуточным между протоколами BB84 и B92. В протоколе используются 4 квантовых состояния для кодирования «0» и «1» в двух базисах. Состояния в каждом базисе выбираются неортогональными, состояния в разных базисах также попарно неортогональны. Это удобно представить графически (рисунок 9):

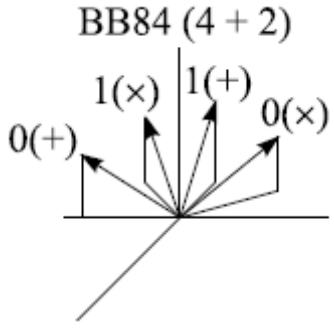


Рисунок 9 - Поляризованные состояния, используемые в протоколе BB84(4+2)

Протокол реализуется следующим образом.

Станция Алиса случайным образом выбирает один из базисов. Внутри базиса также случайным образом выбираются состояния *0* или *1*, затем они направляются в квантовый канал связи. Станция Боб независимо выбирает измерения двух типов (в разных базисах). Затем, после передачи достаточно длинной последовательности пользователи через открытый общедоступный канал связи сообщают, какой базис был использован в каждой посылке. Посылки, в которых базисы не совпадали, отбрасываются. Для оставшихся посылок станция Боб публично открывает номера тех посылок, где у него были неопределенные исходы (такие посылки тоже отбрасываются). Из оставшихся посылок (с определенным исходом) извлекается секретный ключ путем процедуры коррекции ошибок через открытый канал и усиления секретности. Подсчет количества фотонов, принятых станцией Боб, представлен в таблице 4.

Таблица 4 - Формирование квантового ключа по протоколу BB84(4+2)

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

Таким образом, в результате передачи ключа станцией Боб будут получены *50%* фотонов, то есть $n = \frac{1}{2}$.

Протокол Гольденберга-Вайдмана

В протоколе Гольденберга-Вайдмана Алиса и Боб используют для сообщения два ортогональных состояния:

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

кодирующие соответственно биты «0» и «1».

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 этого волновые пакеты 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 пакетом $|a\rangle$, 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

Данный 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

$$|\psi_0\rangle = -i\sqrt{R}|a\rangle + \sqrt{T}|b\rangle \qquad \text{и} \qquad |\psi_1\rangle = \sqrt{R}|a\rangle - i\sqrt{T}|b\rangle,$$

кодирующие биты «0» и «1», определяются отражательной R и пропускательной T способностями входного разделителя лучей.

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. Поэтому при применении Евой вышеописанной тактики существует ненулевая вероятность ошибки детектирования.

Проведя сравнительный анализ приведенных выше протоколов, из расчета количества принятых фотонов, можно судить о том, что наиболее эффективным является BB84. Более поздние его модификации направлены на уменьшение процента ошибок и количества полезной информации, которую теоретически может получить злоумышленник. Альтернативой в развитии протокола BB84 является протокол B92. Преимуществом протокола B92 перед BB84 является использование фотонов с двумя типами поляризации (вместо четырех), что позволяет упростить схему реализации, однако обеспечивает меньшую эффективность (уменьшается количество принятых фотонов), и гарантированную секретность ключа только на расстоянии до 20 км, тогда как BB84 – на расстоянии до 50 км. В настоящее время в коммерческих системах распределения ключа применяется протокол BB84.

Протокол E91(EPR)

Протокол E91 был предложен А. Экертом в 1991 году. Второе название протокола – EPR. так как он основан на парадоксе Эйнштейна-Подольски-Розенберга. В протоколе предлагается использовать, например, пары фотонов, рождающихся в антисимметричных поляризационных состояниях. Перехват одного из фотонов пары не приносит Еве никакой информации, но является для Алисы и Боба сигналом о том, что их разговор подслушивается.

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 и предложил протокол, который 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.

Пусть вначале создаётся N максимально запутанных EPR-пар фотонов, затем один фотон из каждой пары посылается Алисе, а другой - Бобу. Три возможных квантовых состояния для этих EPR-пар есть:

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

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

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

Это 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 EPR-пар, применяя соответствующие проекторы

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

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.

Эксперименты по реализации данного протокола начались недавно. Их проведение стало возможным после получения источников спутанных пар с высокой степенью корреляции и продолжительным временем жизни.

4. Типовые структуры квантовых систем распределения ключей

В системах квантовой криптографии в настоящее время применяют три вида кодирования квантовых состояний: поляризационное, фазовое и кодирование временными сдвигами. Ниже более подробно рассмотрим типовые структуры квантовых систем распределения ключей, реализующие каждый из видов кодирования.

Структура системы с поляризационным кодированием

Исторически первой реализацией системы квантового распределения ключей была поляризационная схема кодирования, работающая по протоколу BB84.

Схема квантовой криптографической установки с поляризационным кодированием по протоколу BB84 с четырьмя состояниями показана на рисунке 10.

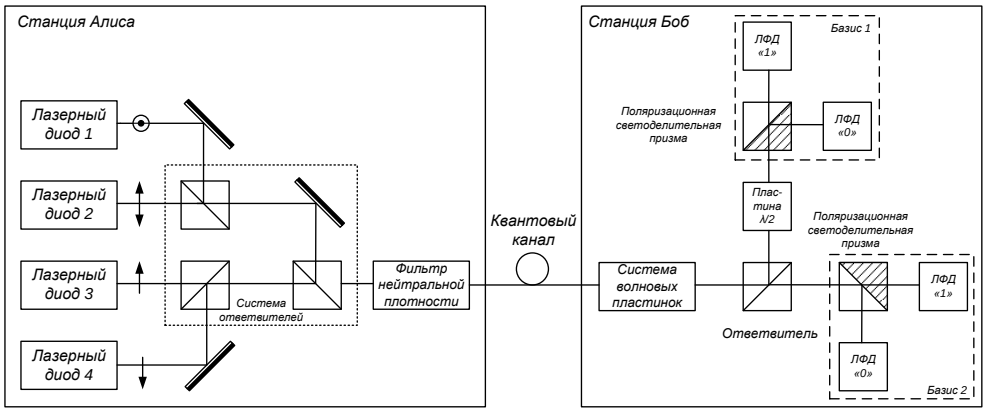


Рисунок 10 - Схема квантовой криптографической установки с поляризационным кодированием

Станция Алиса, состоит из четырёх лазерных диодов, которые излучают короткие импульсы света длительностью 1 нс. Поляризации фотонов составляет -45^{o}, 0^{o}, $+45^{o}$ и 90^{o}. Для передачи одного бита активизируется один из лазерных диодов. Затем импульсы ослабляются набором фильтров для обеспечения условия однофотонности, т. е. среднее количество фотонов в импульсе выбирается менее

одного $n<1$. После этого фотон излучается по направлению к станции Боб. Важным условием правильного детектирования информации станцией Боб является сохранение поляризации фотонов в волокне.

Импульсы, достигая станции Боб, проходят через набор волновых пластинок, используемых для восстановления исходных поляризационных состояний путём компенсации изменений, внесённых волокном. Затем импульсы достигают светоделителя, осуществляющего направление фотона к линейному или диагональному анализатору. Переданные фотоны анализируются в ортогональном базисе при помощи поляризационной светоделительной призмы и двух лавинных фотодиодов (ЛФД). Поляризация фотонов, прошедших через волновые пластинки поворачивается на 45^o (с -45^o до 0^o). В то же время, остальные фотоны анализируются второй системой «поляризационная светоделительная призма - ЛФД» в диагональном базисе.

Пусть имеется фотон, поляризованный под углом $+45^o$. После того, как он покидает станцию Алиса, его поляризация случайным образом преобразуется в оптическом волокне. В станции Боб система из волновых пластинок должна быть установлена таким образом, чтобы компенсировать изменение поляризации. Если фотон пройдет на выход светоделителя, соответствующий линейному базису поляризации, у него будут равные вероятности попасть в один из фотодетекторов, что приведёт к случайному результату. С другой стороны, если будет выбран диагональный базис, его поляризация будет повёрнута на 45^o. Тогда светоделитель отразит его с единичной вероятностью, что приведёт к определённому результату.

Вместо использования четырёх лазеров станцией Алиса и двух поляризационных светоделительных призм станцией Боб, возможно также применение активных поляризационных модуляторов, таких как ячейки Поккельса. Для каждого импульса света модулятор активируется по случайному закону, приводя поляризацию в одно из четырёх состояний, в то время как принимающая сторона в случайном порядке вращает поляризацию половины принимаемых импульсов на 45^o.

Заметим, что поляризационная модовая дисперсия (ПМД) может привести к изменению поляризации фотонов, при условии, что время задержки между поляризационными модами больше времени когерентности. Это вносит ограничение на типы лазеров, используемых станцией Алиса.

Антон Мюллер и его коллеги из Женевского университета использовали подобную систему для проведения экспериментов в области квантовой криптографии [5]. Они передавали ключ на расстояние 1100 м, используя фотоны с длиной волны 800 нм. Для увеличения максимальной дистанции передачи они повторили эксперимент с фотонами на длине волны излучения 1300 нм [6] и передавали ключ на 23 км. Особенностью данного эксперимента было использование в качестве квантового канала, связывающего станции Алиса с Боб, стандартного телекоммуникационного оптического кабеля, который использовался компанией Swisscom для проведения телефонных переговоров.

Результаты этих экспериментов показали, что изменения поляризации, вносимые оптическим волокном, были нестабильны во времени. Несмотря на то, что они стабилизировались на некоторое время (порядка нескольких минут), в случайный момент поляризация резко менялась. Это означает, что реальная квантовая криптографическая система требует создания механизма активной компенсации поляризационных изменений. Несмотря на наличие принципиальной возможности создания такого механизма, очевидно, что его практическая реализация весьма затруднена.

Джеймс Френсон разработал систему автоматической подстройки поляризации, но не стал заниматься её дальнейшим совершенствованием [33]. Существуют и другие способы автоматического контроля поляризации, разработанные для когерентных волоконно-оптических систем связи. Интересно то, что замена стандартного волокна на волокно, сохраняющее поляризацию, не решает проблему, так как такие волокна сохраняют только два ортогональных состояния поляризации, а в системах квантовой криптографии используются четыре попарно неортогональных состояния.

По этим причинам, поляризационное кодирование не является оптимальным методом кодирования при построении волоконно-оптических систем квантовой криптографии.

Структура системы с фазовым кодированием

Нестабильность поляризации в системах с поляризационным кодированием сильно затрудняет (хотя и не делает невозможным) их создание. В связи с этим был разработан другой тип квантовых криптографических систем. Идея кодирования бит фазой фотонов была впервые упомянута Беннеттом, когда он описывал протокол с использованием двух состояний [28]. Получение квантовых состояний и последующий их анализ производятся интерферометрами, которые могут быть реализованы одномодовыми компонентами волоконной оптики. На рисунке 11 показана волоконно-оптическая реализация интерферометра Маха-Цендера.

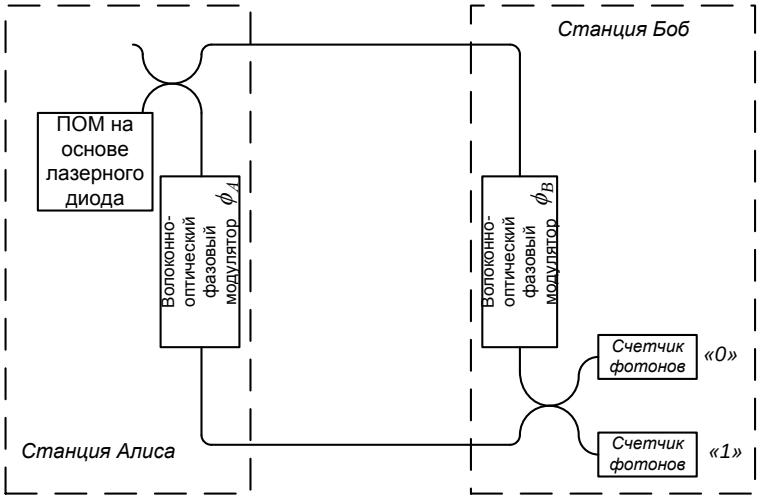


Рисунок 11 - Интерферометр Маха-Цендера

Интерферометр выполнен из двух волоконно-оптических разветвителей, соединённых между собой, и двух фазовых модуляторов – по одному в каждом плече. В такую систему можно ввести оптическое излучение, используя классический непрерывный источник, и наблюдать мощность оптического излучения на выходах. В случае если длина когерентности света лазера больше разности длин плеч интерферометра, можно получить интерференционную картину. Принимая во внимание фазовый сдвиг $\pi/2$, происходящий на разветвителе, действия фазовых

модуляторов (φ_A и φ_B) и разность длин плеч (ΔL), мощность оптического излучения на выходе *"0"* определяется следующей формулой:

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

где k – волновое число, а P – мощность источника.

Если разность фаз составляет $\pi/2 + \nu\pi$, где n – целое число, то на выходе *"0"* образуется деструктивная интерференция. Поэтому мощность оптического излучения, регистрируемого на выходе *"0"*, достигает минимума и всё оптическое излучение регистрируется на выходе *"1"*. Когда разность фаз составляет $\nu\pi$, ситуация обратная – на выходе *"0"* наблюдается конструктивная интерференция, в то время как мощность на выходе *"1"* достигает минимума. В случае появления ошибки оптическое излучение может быть зарегистрирован на обоих выходах. Данное устройство работает как оптический переключатель. Необходимо отметить, что крайне важным является сохранение постоянной и малой разности длин плеч для получения устойчивой интерференции.

Описанное выше поведение интерферометра справедливо для классического оптического излучения. Тем не менее, интерферометр работает аналогично для случая одиночных фотонов. Вероятность зарегистрировать фотон на одном из выходов будет изменяться с изменением фазы. Несмотря на то, что фотон ведёт себя как частица при регистрации, он распространяется через интерферометр как волна. Интерферометр Маха-Цендера – это волоконно-оптический вариант эксперимента Юнга со щелями, в котором плечи интерферометра аналогичны апертурам. Такой интерферометр вместе с однофотонным источником и с ЛФД может быть использован в квантовой криптографии. Станция Алиса в таком случае будет содержать источник, первый разветвитель и первый фазовый модулятор, а станция Боб будет состоять из второго модулятора, разветвителя и ЛФД.

Рассмотрим применение к такой схеме протокола BB84 с четырьмя состояниями. Алиса может осуществлять один из четырёх фазовых сдвигов ($0, \pi/2, \pi, 3\pi/2$). Она сопоставляет значению бита «*0*» – 0^o и $\pi/2$, а значению бита «*1*» - π и $3\pi/2$. В свою очередь, станция Боб производит выбор базиса, в случайном порядке сдвигая фазу на 0 или $\pi/2$, и присваивает биту, пришедшему на фотодетектор,

подсоединённый к выходу *"0"* значение «*0»*, а биту, пришедшему на фотодетектор, подсоединённый к выходу *"1"* значение бита «*1»*. Когда разности фаз равны *0* или *π*, то в станциях Алиса и Боб используются совместимые базисы и получаются вполне определённые результаты. В таких случаях станция Алиса может определить, в какой из фотодетекторов станции Боб попадёт фотон, и, следовательно, она может определить значение бита. Со своей стороны, станция Боб может определить, какая фаза была выбрана станцией Алиса при передаче каждого фотона. В случае, когда разность фаз принимает значения *π/2* или *3π/2*, стороны используют несовместимые базисы, и фотон случайным образом попадает на один из фотодетекторов станции Боб. Все возможные комбинации фазовых состояний приведены в таблице 5.

Таблица 5 - Иллюстрация протокола BB84 с четырьмя состояниями для фазового кодирования.

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

Заметим, что для системы крайне важно сохранять стабильной разность длин плеч интерферометра в течение сеанса передачи ключа. Эта разность не должна изменяться более чем на долю длины волны фотонов. Изменения длины одного из плеч приведёт к дрейфу фазы и выразится в ошибках в передаваемом ключе. Несмотря на то, что данная схема прекрасно работает в лабораторных условиях, на практике не

представляется возможным сохранение длин плеч в случае, когда пользователи отделены друг от друга более чем на несколько метров. Беннетт показал, как обойти эту проблему [28]. Он предложил использовать два несбалансированных интерферометра Маха-Цендера, соединённых последовательно оптическим волокном.

Однако в коммерческих реализациях систем квантового распределения ключей применяется еще более сложная и совершенная схема кодирования фазовых состояний. Данная схема представляет собой распределенный интерферометр с автоматической компенсацией поляризационных искажений [34, 35]. Типовая структура реализации коммерческих систем представлена на рисунках 14-15.

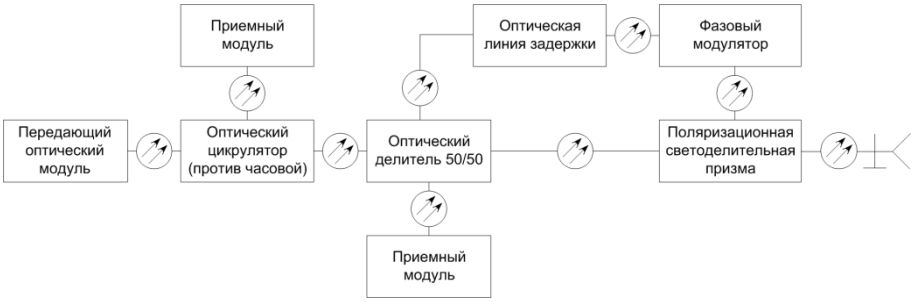


Рисунок 14 – Схема приемо-передающего модуля системы Id 3000 Clavis

Рисунок 15 – Схема кодирующего модуля системы Id 3000 Clavis

Как можно заметить, в одном блоке совмещены функции передатчика и приемника. Однако функция кодирования квантового состояния фазы фотона возложена на фазовый модулятор во втором блоке. Таким образом, схема изображенная на рисунке 15 является схемой устройства Алиса в классической интерпретации протокола BB84. По аналогичной схеме построено оборудование MagiQ QPN, производимое компанией MagiQ Technologies. Различие составляет только реализация подсистемы синхронизации.

Структура системы с временным кодированием

Принципы построения систем квантовой криптографии использующих неортогональность временных интервалов предложил Сергей Молотков из института физики твердого тела РАН [36]. Для кодирования «0» и «1» используется состояние лишь с одной пространственно временной формой, но сдвинутой на различные временные интервалы в каждой посылке. За счет этого и достигается неортогональность.

Данная идея позволяет упростить волоконно-оптическую часть системы квантовой криптографии и полностью отказаться от применения интерферометров. Предложенная схема позволяет реализовать большинство известных протоколов квантовой криптографии [37].

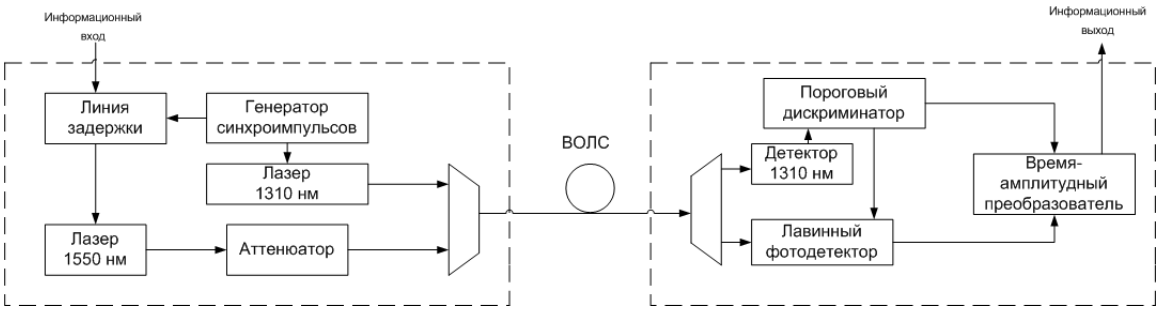


Рисунок 12 – Схема оптоволоконной системы квантовой криптографии на временных сдвигах без интерферометров

В качестве однофотонного состояния используется состояние, сдвинутое относительно синхроимпульса, в каждой посылке на определенную величину. Синхроимпульсом является короткий оптический импульс, излучаемый лазером с длиной волны 1310 нм. В реализации используются два базиса {+(1), ×(1)} и {+(2), ×(2)}. Внутри первого базиса в каждом подбазисе {+(1) и ×(1)}, состояния для 0 - $|0_1(+)\rangle$ и 1 - $|1_1(+)\rangle$, соответственно, в подбазисе 0 - $|0_1(\times)\rangle$ и 1 - $|1_1(\times)\rangle$ - ортогональны. Между подбазисами +(1) и ×(1) состояния попарно неортогональны, что достигается соответствующими временными сдвигами. Аналогично и для базиса {+(2), ×(2)}.

Состояния в базисах отражены на рисунке 13. Данная реализация эквивалентна протоколу BB84.

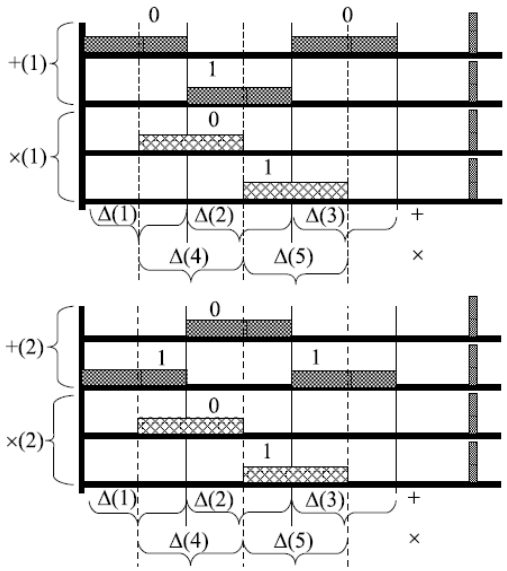


Рисунок 13 – Квантовый состояния в базисах и подбазисах для схемы на временных сдвигах при реализации протокола BB84

При работе по протоколу BB84 сначала случайно выбирается один из двух базисов – 1 или 2, затем также случайно внутри выбранного базиса выбирается один из подбазисов – + или ×. На следующем шаге выбирается непосредственно значение бита «1» или «0». Соответственно для передачи бита «0» в первом базисе существует три варианта последовательности временных сдвигов. Во втором базисе аналогичная картина при передаче бита «1». На приемном конце производится измерение состояний в случайно выбранные интервалы времени Δ1… Δ5. Интервалы отсчитываются от момента прибытия синхроимпульса. После серии измерений получатель сообщает через открытый канал номера посылок, где были зарегистрированы факты срабатывания фотодетектора, пользователь на передающем конце сообщает какой базис и подбазис были выбраны.

В отличие от стандартного протокола BB84 для согласования базиса требуется пересылка двух бит классической информации вместо одного.

Система с временным кодированием позволяет реализовать обмен ключами по протоколу B92 без изменения структурной схемы оборудования. Изменения коснутся только управляющей подсистемы, выполненной в виде программного обеспечения.

Элементная база систем квантовой криптографии

Элементная база, применяемая в системах квантового распределения ключей, представляет собой набор высокотехнологичных оптоэлектронных модулей. К применяемым лазерам предъявляются высокие требования по точности установки мощности, чистоте спектральных составляющих и длительности генерируемых импульсов. Для систем квантовой криптографии разрабатываются специальные однофотонные источники излучения на квантовых точках [38]. Мощность излучения на длине волны 1550 нм при частоте следования импульсов 5 МГц и единичном среднем количестве фотонов на импульс составляет –101 дБм. Для регистрации столь слабого излучения фотодетекторы должны обладать сверхвысокой чувствительностью. На сегодняшний день для регистрации одиночных фотонов применяют лавинные фотодиоды. Однако их квантовая эффективность в инфракрасной области невелика и составляет порядка 10%. У лучших моделей квантовая эффективность достигает 30-70%, но они требуют азотного охлаждения, что не позволяет применять их вне лабораторий.

Для кодирования поляризационных состояний применяют ячейки Поккельса и Керра, работающие на основе одноименных электрооптических эффектов. Для кодирования фазовых состояний используют оптические фазовые модуляторы на основе ниобата лития. К оборудованию, управляющему электрооптическими устройствами, предъявляются высокие требования по скорости воздействия. Высокая инерционность оптических аттенюаторов не позволяет достаточно точно контролировать уровень среднего количества фотонов в каждом импульсе.

Несовершенство технологического процесса изготовления электрооптических компонентов на сегодняшний день не позволяет вывести скоростные показатели квантово-криптографических систем на качественно новый уровень.

5. Тенденции развития квантовой криптографии

Проведенный анализ показал, что квантовая криптография уже заняла достойное место среди систем обеспечивающих конфиденциальную передачу информации. От обсуждения достоинств и недостатков различных протоколов распределения ключей научный мир перешел к поиску наиболее удачных структурных и схемотехнических решений, обеспечивающих увеличение дальности связи, повышение скорости формирования ключей и снижение влияния дестабилизирующих факторов. Одной из тенденций развития является совершенствование элементной базы систем квантовой криптографии, предусматривающее преодоление технологических сложностей изготовления компонентов.

В литературе отсутствует описание влияния параметров функциональных узлов на характеристики эффективности систем квантовой криптографии[39]. Тесным образом с этой проблемой связано отсутствие общепризнанных методик исследования (измерения) параметров систем квантового распределения ключей в целом, а так же всех функциональных узлов, входящих в состав систем [40]. Слабо изучено влияние неидеальности характеристик компонентов на условия несанкционированного съёма информации [41, 42]. Для исключения возможности несанкционированного доступа в системах [43], работающих на одночастичных состояниях, требуется разработать промышленные образцы однофотонных источников излучения. Для реализации систем, работающих на спутанных состояния, необходимо создание источников оптического излучения нового класса, позволяющих формировать спутанные фотонные пары. Известно, что к однофотонным детекторам могут быть отнесены только приборы с коэффициентом усиления больше 10^4. Это указывает на необходимость разработки однофотонных лавинных фотодиодов с большими коэффициентами умножения и меньшим уровнем собственных шумов. При кодировании информации в фазовых состояниях фотонов должна быть решена проблема сохранения идентичности плеч интерферометров в условии изменения температур, вибрации и других внешних воздействующих факторов. Необходимо повысить стабильность модуляционных характеристик фазовых и поляризационных модуляторов наряду со снижением их инерционности.

Отдельной задачей является исследование влияния параметров подсистемы синхронизации на качественные характеристики систем квантового распределения ключей.

Список литературы

1. S. Wiesner, "Conjugate coding", Sigact News 15, 78-88 (1983).
2. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175-179.
3. A. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. 67, 661-663 (1991).
4. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography", J. Cryptology 5, 3-28 (1992).
5. A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km", Europhysics Lett. 23, 383-388 (1993).
6. J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibers: experimental and practical limits", J. Mod. Opt. 41, 2405-2412 (1994).
7. A. Muller, H. Zbinden, and N. Gisin, "Underwater quantum coding", Nature **378,** 449-449 (1995).
8. A. Muller, H. Zbinden, and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fiber", Europhysics Lett. 33, 335-339 (1996).
9. C. Marand and P. Townsend, "Quantum key distribution over distances as long as 30 km", Opt. Lett., 20, 1695-1697 (1995).
10. P.D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fiber using wavelength-division multiplexing", Electronics Lett. **33,** 188-190 (1997).
11. P.D. Townsend, "Quantum cryptography on multiuser optical fibre networks", Nature 385, 47-49 (1997).
12. P.D. Townsend, "Quantum cryptography on optical fiber networks", Opt. Fiber Tech. 4, 345-370 (1998).

13. R. Hughes, G. Morgan, and C. Peterson, "Practical quantum key distribution over a 48-km optical fiber network", J. Mod. Opt. 47, 533-547 (2000).
14. P.A. Hiskett, G. Bonfrate, G.S. Buller, and P.D. Townsend, "Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 ^m," J. Mod. Opt. 48, 1957-1966 (2001).
15. T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150km transmission using silica-based integrated optic interferometers for quantum cryptography", Jpn. J. Appl. Phys. 43, L1217-L1219 (2004).
16. C. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber", Appl. Phys. Lett. 84, 3762-3764 (2004).
17. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M.M. Fejer, K. Inoue, and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105km fiber", New J. Phys. 7, 232 (2005).
18. P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller, and J.E. Nordholt, "Long-distance quantum key distribution in optical fiber", New J. Phys. 8, 193 (2006).
19. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system", *New Journal of Physics* 4 (2002) 41.1–41.8
20. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity "Quantum cryptography: A step towards global key distribution" , Nature. 2002. V.419. P.450.
21. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, "A step towards global key distribution", Nature **419,** 450-450 (2002).
22. J.G. Rarity, P.R. Tapster, P.M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography", New J. Phys. 4, 82 (2002).
23. G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, "Secure communication using mesoscopic coherent states", Physical Review Letters, Vol. 90, No. 22, 227901 (2003).

24. E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, "Quantum-noise randomized data-encryption for WDM fiber-optic networks", Physical Review A. 2005.
25. W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, "Practical free-space quantum key distribution over 1 km", Phys. Rev. Lett. 81, 3283-3286 (1998).
26. W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, "Daylight quantum key distribution over 1.6 km", Phys. Rev. Lett. 84, 5652-5655 (2000).
27. R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, "Free-space quantum key distribution in day light", J. Mod. Opt. **47,** 549-562 (2000).
28. C.H. Bennett, "Quantum cryptography using any two non-orthogonal states", Phys. Rev. Lett. 68, 3121-3124 (1992).
29. B. Huttner, N. Imoto, N. Gisin, T. Mor, "Quantum Cryptography with Coherent States", *Phys. Rev. A, Vol. 51, 1863—1869 (1995).*
30. D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States", *Phys. Rev. Lett, Vol. 81, 3018 (1998).*
31. L. Goldenberg, L. Vaidman, "Quantum Cryptography Based On Orthogonal States", *Phys. Rev. Lett., Vol. 75, 1239 (1995).*
32. M. Koashi, N. Imoto, "Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps", Phys. Rev. Lett., Vol. 79, 2383 (1997).
33. B.C. Jakobs and J.D. Franson, "Quantum cryptography in free space", Opt. Lett. 21, 1854-1856 (1996).
34. M. Martinelli, "A universal compensator for polarization changes induced by birefringence on a retracting beam", Opt. Commun. 72, 341-344 (1989).
35. M. Martinelli, "Time reversal for the polarization state in optical systems", J. Mod. Opt. 39, 451-455 (1992).

36. С.Н. Молотков. “Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы”, Письма в ЖЭТФ, Том 79, Выпуск 11.
37. С.Н. Молотков. “Мультиплексная квантовая криптография с временным кодированием без интерферометров”, Письма в ЖЭТФ, Том 79, Выпуск 9.
38. K.Alchalabi, D.Zimin, G.Kostorz, and H.Zogg. “Self-assembled semiconductor quantum dots with nearly uniform sizes” Phys. Rev. Lett. 90 (2003)
39. К.Е. Румянцев, И.Е. Хайров, “Эффективность волоконно-оптической системы передачи информации”, Научно-практический журнал «Информационное противодействие угрозам терроризма», 2004, №2, с.50-52
40. Д.М. Голубчиков. “Применение квантовых усилителей для съема информации с квантовых каналов распределения ключа”, Известия ТТИ ЮФУ. 2008. №1(78) С.119.
41. Д.М. Голубчиков. “Анализ способов съема информации с квантового канала распределения ключа и методы их обнаружения”, Современные информационные технологии – 2007: материалы докладов Всероссийской НТК с международным участием. 2007.
42. Д.М. Голубчиков. “Анализ возможности использования квантового усилителя для съема информации с квантового канала распределения ключа и методы его обнаружения”, Информационные системы и технологии 2007: материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых специалистов. Обнинск. 2007.
43. К.Е. Румянцев, И.Е. Хайров, В.В. Новиков, “Анализ возможности несанкционированного доступа в квантово-криптографическом канале”, Материалы международной научной конференции «Анализ и синтез как методы научного познания», 2004, Часть 3, с.55-57.