ПО ИТОГАМ ПРОЕКТОВ
РОССИЙСКОГО ФОНДА ФУНДАМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ
Проект РФФИ # 02-02-16289

Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия

Факультет вычислительной математики и кибернетики МГУ им. М. В. Ломоносова
119899 Москва, Россия

Поступила в редакцию 6 апреля 2004 г.

Описан прототип новой системы квантовой криптографии. Подобные криптосистемы естественно называть квантовой криптографией на временных сдвигах. Схема реализует все базовые квантовые криптографические протоколы (BB84, B92, BB84(4+2)) в рамках единой оптоволоконной системы. Схема не использует оптоволоконных интерферометров типа Маха-Цандера, что позволяет естественным образом реализовать мультиплексный режим передачи секретного ключа, а также естественным образом интегрировать данную квантовую криптографическую схему в традиционные оптоволоконные телекоммуникационные системы. Предлагаемый метод временного кодирования в квантовой криптографии позволяет принципиально упростить экспериментальные схемы и вообще избавиться от наиболее тонкой оптоволоконной части – интерферометра. По сути, принципиальное отличие метода временного кодирования от метода фазового кодирования состоит в том, что из метода фазового кодирования выброшена та часть, которая использует фазовые соотношения в суперпозиции между "частями" квантового состояния, и оставлена лишь часть, использующая принцип разделения по времени. Принцип разделения по времени – общий для обоих методов и является минимально необходимым, в отличие от принципа фазового кодирования, который может быть вообще исключен. Проведено краткое сравнение нашей схемы с двумя наиболее развитыми схемами с фазовым кодированием (без самокомпенсации и с пассивной самокомпенсацией).

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

1. Введение. Развитие квантовых технологий и волоконно-оптических линий связи (ВОЛС) привело к появлению квантовых криптографических систем. Данные системы являются предельным случаем абсолютно секретных (защищенных) ВОЛС. Использование фундаментальных законов квантовой механики для защиты информации позволяет получать результаты, недостижимые как техническими методами защиты ВОЛС, так и традиционными методами математической криптографии.

Криптосистемы с одноразовыми секретными ключами дают возможность для создания абсолютно стойких, не взламываемых даже теоретически, систем шифрования [1 – 3]. Квантовая криптография позволяет реализовать распространение ключа между пространственно удаленными легитимными пользователями, секретность которого гарантируется фундаментальными законами природы, а не ограниченными вычислительными или техническими возможностями подслушивателя [4]. Безусловная секретность квантовой криптографии базируется, по сути, на принципе неопределенностей Гейзенберга. Более формально, на невозможности одновременного измерения наблюдаемых, которые описываются некоммутирующими операторами. В терминах пары векторов состояний квантовой системы, в которые кодируется классическая информация о передаваемом ключе, это означает невозможность получения любой информации о передаваемых

[1)] e-mail: molotkov@issp.ac.ru

квантовых состояниях без их возмущения, если последние являются неортогональными [5]. Другим фундаментальным запретом квантовой механики, тесно связанным с предыдущим, является запрет на копирование заранее неизвестного квантового состояния [6] (no cloning-теорема).

Разработки в области квантовой криптографии и реализаций различных квантовых криптосистем ведутся во всех развитых странах и практически во всех ведущих телекоммуникационных компаниях. Исследования в области квантовой криптографии за последние пять лет перешли от чисто фундаментальных к практическим реализациям и первым коммерческим прототипам.

Имеющиеся прототипы квантовых криптосистем используют, в основном, следующие принципы кодирования классической информации в состояния квантовых систем. 1) Информация о ключе кодируется в поляризационные степени свободы [7,8]. 2) Фазовое кодирование, когда используется интерферометр Маха–Цандера, и информация кодируется в разность фаз, которая набирается на приемном и передающем плечах интерферометра [9]. 3) Квантовые криптосистемы с частотной модуляцией несущей частоты [10]. 4) Квантовая криптография на когерентных состояниях с использованием гомодинного детектирования на приемном конце [11]. С данными системами связываются определенные надежды на высокоскоростную квантовую криптографию, однако криптографическая стойкость подобных систем, в отличие от систем 1), 2), исследована еще недостаточно полно. Наибольший прогресс достигнут в криптосистемах с фазовым кодированием и самокомпенсацией [12–17] с использованием фарадеевских отражателей. Первый лабораторный прототип квантовой криптосистемы был создан в 1989 г. в Исследовательском центре компании IBM с длиной квантового канала связи в 1 м. Лабораторный вариант криптосистемы на базе интерферометра Маха–Цандера с разделением времени (time division interferometer) с использованием оптоволоконной линии связи с длиной в 30 км был реализован в исследовательской лаборатории фирмы British Telecom в 1995 г. [18], а также в Лос-Аламосской лаборатории с суммарной длиной оптоволоконной линий в 48 км [9]. В этих схемах использовался принцип фазового кодирования. В 2003 г. достигнута дальность в 100 км в исследовательской лаборатории NEC [19], в 2004 г. уже достигнута дальность в 150 км [20]. Данные схемы являются усложнением и развитием идеи фазового кодирования с самокомпенсацией при помощи фарадеевских отражателей. Упомянутые криптосистемы, особенно схемы с фазовым кодированием и самокомпенсацией, достаточно сложны в реализации. Результатом теоретической разработки группы в Женевском университете стала практическая реализация квантовой криптосистемы с длиной волоконно-оптического кабеля в 23 км, проложенного по дну Женевского озера между городами Нион и Женева. На сегодняшний день длина линии доведена до 67 км и представляет собой сложный оптоволоконный интерферометр с фазовым кодированием и самокомпенсацией с использованием фарадеевских отражателей [16] (так называемая первая Plug&Play система квантовой криптографии). Активные исследования ведутся в исследовательской лаборатории IBM (Almaden) [21,22]. Апробирована первая локальная квантовая криптографическая сеть в Бостоне для распространения секретных ключей между пользователями на расстоянии в 10 км (проект выполняется по заказу DARPA – Defense Advanced Research Projects Agency) [23].

Недавно инновационной фирмой MagiQ был анонсирован первый коммерческий вариант квантовой волоконной криптосистемы, действующей на расстоянии 120 км, использующей принцип фазового кодирования. Схема реализует квантово-криптографический протокол BB84.

Апробирована первая локальная квантовая криптографическая сеть в Бостоне для распространения секретных ключей между пользователями на расстоянии в 10 км (проект выполняется по заказу DARPA – Defense Advanced Research Projects Agency) [23].

По мнению специалистов из QinetiQ и Toshiba Research Europe, UK, широкое применение квантовых криптосистем начнется в ближайшие три года, первыми на очереди стоят правительственные учреждения и банки.

Существуют реализации прототипов квантовых криптосистем, осуществляющих передачу секретного ключа через открытое пространство [24–26]. Рекорд по дальности (из опубликованных данных [26]) составляет 23.4 км как в дневное, так и ночное время. Целью использования квантовых криптосистем является генерация и передача секретных ключей через открытое пространство между наземными объектами и низкоорбитальными спутниками (до высот в 1000 км) или между наземными объектами через спутники. По оценкам руководителя проекта из QinetiQ, уже в марте следующего года начнутся эксперименты по передаче криптографических ключей на низкоорбитальные спутники, а лет через семь с их помощью можно будет посылать секретные ключи в любую точку планеты.

На ближайшее время прогнозируются следующие параметры квантовых криптографических ВОЛС:

1) эффективная скорость передачи информации по оптоволоконному квантовому каналу при количестве ошибок, не превышающем несколько процентов;

2) длина квантового оптоволоконного канала связи $\sim 100-150$ км;

3) количество подканалов при разделении по длинам волн (мультиплексировании) – 8–16.

Несмотря на впечатляющий прогресс в понимании как криптографической стойкости (секретности) квантовых криптосистем, так и в их реализации, данные системы содержат достаточно сложные оптоволоконные, электронные и программные компоненты, работа с которыми на сегодняшний день представляет собой скорее проведение тонкого научного эксперимента и демонстрацию экспериментального искусства, чем работу с общеупотребительным и стандартным научным оборудованием. Следующим важным моментом, который ограничивает пока широкое распространение квантовых криптосистем, использующих принцип фазового кодирования, состоит в том, что квантовые криптосистемы пока плохо встраиваются в стандартные оптоволоконные телекоммуникационные технологии, поскольку содержат специфические компоненты (интерферометры), требующие тонкой юстировки. Наконец, последний принципиальный момент состоит в том, что каждый квантовый криптографический протокол распространения секретного ключа фактически требует создания своей, специфической только для него, передающей и измерительной аппаратуры. Существует три базовых протокола передачи секретного ключа, которые кратко называются BB84 [5], B92 [5] и BB84(4+2) [27]. Протокол BB84 использует 4 квантовых состояния: два ортогональных состояния для 0 и 1 в одном базисе, и два ортогональных для 0 и 1 – в другом. Между базисами состояния попарно неортогональны, что необходимо для обеспечения секретности. В протоколе B92 используется пара любых неортогональных квантовых состояний, отвечающих 0 и 1. Протокол BB84(4+2) является производным от BB84 и отличается от последнего тем, что внутри базисов состояния также делаются неортогональными. Очевидно, что разные протоколы обмена требуют различных физических устройств для формирования квантовых состояний на передающем конце и, соответственно, разных устройств для квантово-механических измерений на приемном конце.

Криптографическая стойкость (секретность) данных протоколов достаточно подробно исследована [27–34]. С учетом реальных параметров – не строгой однофотонности источника, неидеальности лавинных фотодетекторов и затухания в оптоволоконном канале связи – перечисленные протоколы гарантируют секретность распространения ключа до определенной критической длины оптоволоконной линии связи [27]. Протокол B92 является самым минимальным в смысле числа используемых состояний и измерений, однако обеспечивает секретность до длин $\sim 15-20$ км [31]. Наиболее подробно исследованный протокол BB84 использует 4 квантовых состояния, является более сложным в реализации и остается секретным до длин ~ 50 км [27]. Наконец, в протоколе BB84(4+2) применяются 4 попарно неортогональных состояния. Данный протокол еще более сложен в реализации и настройке оптоволоконного интерферометра, однако в смысле секретности протокол выживает до длин ~ 150 км [27].

В зависимости от различных длин каналов связи удобно использовать тот или иной протокол распространения ключа. При этом автоматически придется использовать существенно различные передающие и принимающие физические устройства. В идеальном варианте хотелось бы иметь универсальные физические (hardware) передающие и приемные блоки для различных длин каналов связи и протоколов обмена, в которых различные протоколы реализуются лишь небольшой настройкой компьютерной программы (software).

Принцип фазового кодирования при реализации различных протоколов не позволяет достичь упомянутой универсальности, поэтому требуется разработка новых физических принципов кодирования. Таким принципом, который обладает высокой степенью универсальности, является предлагаемый метод временного кодирования. Ниже будет показано, что метод временного кодирования позволяет решить упомянутые проблемы, кроме того, метод вообще не использует оптоволоконных интерферометров, требующих тонкой настройки и периодической юстировки во время передачи секретного ключа. Описываемая ниже схема естественным образом интегрируется в стандартные оптоволоконные телекоммуникационные системы и позволяет реализовать все базовые протоколы передачи ключа при одних и тех же физических передающих и принимающих измерительных устройствах. Кроме того, метод наиболее простым и естественным способом, в отличие от других методов кодирования, обобщается на мультиплексный режим передачи ключей по одному оптоволоконному каналу связи.

2. Краткое описание базовых протоколов передачи секретного ключа: BB84, B92, BB84(4+2). В этом разделе приведем лишь краткое и минимально необходимое для дальнейшего описание базовых квантовых криптографических протоколов. Поскольку нашей основной целью является обсуждение метода временного кодирования и реализации на его основе оптоволоконных схем квантовой криптографии, то ниже мы не будем подробно касаться математических доказательств секретности различных квантовых криптографических протоколов (подробности см. в [27–34]).

Протокол BB84. Данный протокол был исторически первым протоколом квантового распространения ключа [5]. Подавляющее число экспериментальных реализаций использует именно данный протокол. Основная идея протокола состоит в использовании 4 квантовых состояний, которые ассоциируются с классическими битами 0 и 1. Пара квантовых состояний соответствует 0 ($|0(+)\rangle$) и 1 ($|1(+)\rangle$) и принадлежит одному базису, условно обозначаемому (+). Состояния внутри базиса являются *ортогональными* ($\langle 0(+)|1(+)\rangle = 0$). Вторая пара состояний принадлежит базису, обозначаемому (×), и также отвечает 0 и 1. Внутри второго базиса состояния $|0(\times)\rangle$ и $|1(\times)\rangle$ *ортогональны* ($\langle 0(\times)|1(\times)\rangle = 0$). Однако состояния из разных базисов (+) и (×) попарно *неортогональны*. Неортогональность принципиально необходима для детектирования попыток подслушивания. Базисы повернуты относительно друг друга на 45° ($\langle 1(+)|1,0(\times)\rangle = 1/\sqrt{2}$, $\langle 0(+)|0(\times)\rangle = 1/\sqrt{2}$ и $\langle 0(+)|1(\times)\rangle = -1/\sqrt{2}$). Физическая природа квантовых состояний не важна. Удобно условно изображать данные состояния графически (рис.1a)).

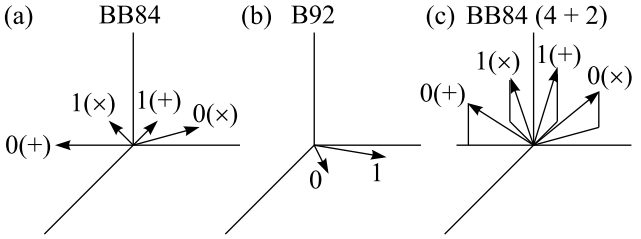

Рис.1

В первых реализациях протокола BB84 0 и 1 кодировались в состояния поляризации фотонов, однако в оптоволоконных системах использование поляризационных состояний не получило дальнейшего развития, поскольку оптоволокно плохо "держит" поляризацию. Для больших расстояний это оказалось неприемлемым. Все последние рекордные достижения по дальности были достигнуты в схемах с фазовым кодированием (см. детали ниже).

Протокол передачи ключа устроен следующим образом. На передающем конце случайно выбирается один из базисов. Затем внутри данного базиса случайно выбирается одно из состояний для 0 или 1. На приемном конце производятся квантовомеханические измерения в одном из базисов, который выбирается случайно и независимо от передающего конца. После достаточно длинной серии измерений через открытый общедоступный классический канал связи раскрывается, какой базис использовался в каждой посылке, но, естественно, не сообщается, какие состояния посылались в каждом из базисов. Для дальнейшего оставляются только те посылки, в которых выбранные базисы совпадали. Число таких посылок будет составлять примерно половину от исходной последовательности. Поскольку внутри базиса состояния ортогональны и, соответственно, достоверно (с вероятностью 1) различимы, то без внешнего вторжения в квантовый канал связи легитимные участники будут иметь одинаковые и случайные последовательности бит. Постселекция базисов принципиально важна для секретности протокола.

Из-за попарной неортогональности состояний в разных базисах они достоверно неразличимы. Поэтому, если в квантовом канале присутствует подслушиватель, который не знает в каком базисе выбраны состояния, то он не сможет достоверно отличать передаваемые состояния, что неизбежно приведет к увеличению потока ошибок на приемном конце.

Для той части оставленной последовательности бит у легитимных пользователей, в которой их базисы совпадали, также через открытый классический канал связи случайным образом раскрываются значения бит и сравниваются их значения. Впоследствии эти раскрытые биты выбрасываются. В идеальном (без шума) квантовом канале связи достаточно несоответствия в одной раскрытой позиции для обнаружения подслушивателя. В реальной ситуации невозможно отличить ошибки, которые произошли от шума в канале и те, которые возникли в результате действий подслушивателя. Строго показано, что если процент ошибок не превышает $\sim 11\%$ [28, 30], то из оставшейся нераскрытой последовательности легитимные пользователи, после коррекции ошибок через открытый канал и процедуры усиления секретности (privacy amplification) могут извлечь секретный ключ, который будет у них одинаков и подслушиватель не будет его знать (точнее, с вероятностью единица будет иметь экспоненциально малую информацию в зависимости от длины ключа).

В реальной экспериментальной ситуации положение несколько хуже. Кроме шума (процессов декогерентности в квантовом канале связи, которые, например, приводят к сбою поляризации), есть еще затухание, приводящее к тому, что не все состояния достигают приемного конца. Кроме того, источник состояний не является строго однофотонным (хотя экспериментальные продвижения в сторону однофотонных источников уже имеются [35]), эффективность лавинных фотодетекторов также не равна единице. Данные обстоятельства приводят к тому, что протокол гарантирует секретность лишь до определенной критической длины. Для реальных параметров затухания в оптоволокне (0.2 Д/км), эффективности фотодетекторов и среднего числа фотонов в ослабленном лазерном излучении (когерентном состоянии) $\mu \approx 0.1$ критическая длина для протокола BB84 составляет ~ 50 км [27].

Поскольку лазерное излучение (когерентное состояние) имеет пуассоновскую статистику по числу фотонов, то с вероятностью $e^{-\mu}$ в канале нет фотонов, с вероятностью $\mu^n e^{-\mu}$ в канале $n = 1..\infty$ фотонов. Формально существуют неразрушающие измерения, которые позволяют выяснить число фотонов, присутствующих в канале в каждой конкретной посылке. Если число фотонов $n = 1$, то канал блокируется подслушивателем, если $n > 1$, то подслушиватель светоделителем отводит часть фотонов для своих измерений, а оставшиеся направляет через свой квантовый канал с меньшим затуханием, причем отведенные для себя фотоны подслушиватель сохраняет в квантовой памяти, не производя измерений до тех пор, пока легитимные пользователи не раскроют, какой базис использовался в каждой посылке. После этого подслушиватель делает измерения в правильном базисе и *достоверно* узнает переданные состояния. Такая процедура подслушивания возможна, если затухание (соответственно длина исходного квантового канала) больше некоторой критической величины. В этом случае подслушиватель имеет полную информацию о передаваемом ключе и остается незамеченным. Правда, на сегодняшний день никто не знает, как технически реализовать такое подслушивание, но поскольку требуется безусловная секретность, которая гарантируется не техническими ограничениями подслушивателя, а лишь фундаментальными запретами квантовой механики, то такую атаку на ключ необходимо учитывать. В этом случае секретность ключа гарантируется до длин ~ 50 км (см. подробности в [27]). Для строго однофотонного источника такая стратегия подслушивания не срабатывает.

Протокол B92. Данный протокол использует любую пару неортогональных квантовых состояний, отвечающих 0 и 1 ($|\varphi_0\rangle$ и $|\varphi_1\rangle$, $\langle\varphi_0|\varphi_1\rangle \neq 0$), которые также удобно для наглядности изображать графически (рис.1b)), причем состояния, вообще говоря, не обязаны быть однофотонными. Например, могут быть использованы когерентные состояния, однако в этом случае процедура измерения должна отличать (пусть не с вероятностью единица) данные состояния как целые, то есть измерения должны реализовывать проекции (или положительные операторнозначные меры) на данные многофотонные состояния. Одной из таких процедур является гомодинное детектирование, реализация которого достаточно сложна и далее не будет обсуждаться. Ниже под состояниями будем понимать однофотонные состояния, в этом случае измерения используют однофотонные фотодетекторы, работающие в режиме счета фотонов.

Протокол работает следующим образом. На передающем конце случайно выбирается одно из состояний. На приемном конце легитимный пользователь производит измерение, которое описывается разложением единицы:

$$\mathcal{P}_0^{\perp} + \mathcal{P}_1^{\perp} + \mathcal{P}_? = I, \quad \mathcal{P}_0^{\perp} = a(I - |\varphi_0\rangle\langle\varphi_0|),$$
$$\mathcal{P}_1^{\perp} = a(I - |\varphi_1\rangle\langle\varphi_1|), \quad \mathcal{P}_? = I - \mathcal{P}_0^{\perp} - \mathcal{P}_1^{\perp},$$
$$a = \frac{1}{1+\cos\zeta}, \quad \cos\zeta = \langle\varphi_1|\mathcal{P}_?|\varphi_1\rangle = \langle\varphi_0|\mathcal{P}_?|\varphi_0\rangle. \tag{1}$$

Пространство результатов (различных исходов) состоит из трех элементов $\{0, 1, ?\}$, которые возникают случайно. Измерение устроено таким образом, что если было послано состояние $|\varphi_0\rangle$, то возможен исход $\{1\}$ или $\{?\}$ и никогда $\{0\}$, поскольку вероятность исхода $\{0\}$ (операторно-значная мера $\mathcal{P}_0^{\perp}$) на входном состоянии $|\varphi_0\rangle$ тождественно равна нулю. Аналогично, если было послано состояние $|\varphi_1\rangle$. Далее через открытый классический канал участник на приемном конце сообщает номера тех посылок, когда у него был исход с определенным результатом, либо $\{0\}$, либо $\{1\}$ (сами исходы, естественно, не сообщаются). Посылки, где были исходы $\{?\}$, отбрасываются. Исходы $\{?\}$ могут возникать как от состояния 0, так и 1. В оставленной последовательности исходов $\{0\}$ и $\{1\}$ легитимным пользователям известно, что если было послано состояние $|\varphi_0\rangle$, то оно дало исход $\{1\}$, и наоборот. В итоге, если нет шума в канале и вторжения подслушивателя, то легитимные пользователи имеют одинаковую последовательность бит. Шум в канале и присутствие подслушивателя

приводит к увеличению потока ошибок. Исследование секретности протокола показывает (см. детали в [31]), что при учете затухания и неидеальности фотодетекторов протокол гарантирует секретность ключа до длин оптоволоконной линии связи ~ 20 км.

На качественном уровне понять, почему с некоторой критической величины затухания (длины канала связи) протокол не может обеспечить секретную передачу ключа, можно при помощи следующих рассуждений (см. детали, например, в [27]). Если имеется затухание, то подслушиватель может использовать измерения (1) такие же, как и легитимный пользователь. При этом, если получен исход $\{0\}$ или $\{1\}$ (conclusive results), то подслушиватель перепосылает на приемный конец состояния для 0 или 1, в зависимости от полученного результата, через свой канал с меньшим затуханием. Если же получен неопределенный исход $\{?\}$ (inconclusive result), то подслушиватель ничего не посылает на приемный конец. При достаточно большом затухании в исходном канале такое подслушивание не детектируется (исчезновение состояний в канале приписывается затуханию), а подслушиватель имеет полную информацию о передаваемом ключе и остается незамеченным.

Протокол BB84(4+2). Данный протокол в определенном смысле является промежуточным между двумя предыдущими квантовыми протокола распространения секретного ключа [27]. В протоколе используются 4 квантовых состояния для 0 и 1 в двух базисах, аналогично протоколу BB84. Единственная разница состоит в том, что состояния выбираются в каждом базисе неортогональными. Состояния остаются также попарно неортогональными в разных базисах. Удобно для наглядности представлять их графически при помощи векторов (рис.1c)). Протокол выглядит следующим образом. На передающем конце легитимный участник случайно выбирает один из базисов. Далее случайно внутри базиса выбираются состояния 0 или 1 и направляются в квантовый канал связи. На приемном конце второй легитимный участник независимо выбирает измерения двух типов (в разных базисах[2)]). Разные типы измерений описываются разными разложениями единицы: в базисе $(+)$

$$\mathcal{P}^{\perp}_{0(+)} + \mathcal{P}^{\perp}_{1(+)} + \mathcal{P}_{?(+)} = I,$$
$$\mathcal{P}^{\perp}_{0(+)} = a(+)(I - |0(+)\rangle\langle 0(+)|),$$
$$\mathcal{P}^{\perp}_{1(+)} = a(+)(I - |1(+)\rangle\langle 1(+)|),$$
$$\mathcal{P}_{?(+)} = I - \mathcal{P}^{\perp}_{0(+)} - \mathcal{P}^{\perp}_{1(+)}, \qquad (2)$$
$$a(+) = \frac{1}{1+\cos\zeta(+)},$$

$$\cos\zeta(+) = \langle 1(+)|\mathcal{P}_{?(+)}|1(+)\rangle = \langle 0(+)|\mathcal{P}_{?(+)}|0(+)\rangle,$$

в базисе $(\times)$

$$\mathcal{P}^{\perp}_{0(\times)} + \mathcal{P}^{\perp}_{1(\times)} + \mathcal{P}_{?(\times)} = I,$$
$$\mathcal{P}^{\perp}_{0(\times)} = a(\times)(I - |0(\times)\rangle\langle 0(\times)|),$$
$$\mathcal{P}^{\perp}_{1(\times)} = a(\times)(I - |1(\times)\rangle\langle 1(\times)|),$$
$$\mathcal{P}_{?(\times)} = I - \mathcal{P}^{\perp}_{0(\times)} - \mathcal{P}^{\perp}_{1(\times)}, \qquad (3)$$
$$a(\times) = \frac{1}{1+\cos\zeta(\times)},$$

$$\cos\zeta(\times) = \langle 1(\times)|\mathcal{P}_{?(\times)}|1(\times)\rangle = \langle 0(\times)|\mathcal{P}_{?(\times)}|0(\times)\rangle.$$

Здесь все состояния попарно неортогональны. Возможны и другие измерения, однако измерения (3), (4) проще реализовать экспериментально.

Далее, после передачи достаточно длинной последовательности участники через открытый канал сообщают, какой базис был использован в каждой посылке. Те посылки, где базисы не совпадали, отбрасываются. Для оставшихся посылок участник на приемном конце публично открывает номера тех посылок, где у него были неопределенные исходы ($\mathcal{P}^{\perp}_{?(+,\times)}$). Такие посылки тоже отбрасываются. Из оставшихся посылок, где имел место определенный исход, извлекается секретный ключ путем процедуры коррекции ошибок через открытый канал и усиления секретности. Данный протокол менее подробно изучен, чем два предыдущих. Однако имеющийся анализ его секретности показывает, что данный протокол является самым "живучим" в смысле дальности, и остается секретным до длин квантового оптоволоконного канала связи ~ 150 км [27].

3. Универсальная реализация базовых протоколов квантовой криптографии в оптоволоконной схеме без интерферометров (метод временного кодирования). Необходимым условием для достижения секретности и детектирования попыток подслушивания при передаче секретного ключа является неортогональность состояний. Идея временного кодирования также использует свойство достоверной неразличимости неортогональных состояний. Фактически для кодирования 0 и 1 ис-

[2)] Из-за неортогональности состояний слово "базис" возможно не слишком удачно, но в данном контексте не приводит к двусмысленности.

пользуется состояние лишь с одной пространственно-временной формой (волновой функцией), но сдвинутой на различные временные интервалы в каждой посылке, за счет чего и достигается неортогональность. Данная идея позволяет радикально упростить оптоволоконную часть схемы квантовой криптографии и полностью отказаться от интерферометра Маха-Цандера, который является наиболее деликатной, в смысле настройки, частью систем, использующих фазовое кодирование. Отказ от интерферометра позволяет реализовать все базовые квантовые криптографические протоколы в рамках единой оптоволоконной системы, без ее изменения и настройки, а также без изменения управляющей электроники под конкретный протокол обмена. Кроме того, данная схема естественно обобщается в рамках имеющихся оптоволоконных технологий на многоканальный (мультиплексный) случай, когда несколько секретных ключей передаются по одной оптоволоконной линии связи.

Опишем сначала временные диаграммы различных протоколов, а затем их реализацию.

Протокол BB84. Основная идея исходного протокола BB84 состоит в использовании двух базисов. В каждом базисе состояния 0 и 1 ортогональны, а между базисами попарно неортогональны.

Состояния на передающем конце. В качестве однофотонного состояния используется одно и то же состояние, но сдвинутое относительно синхроимпульса в каждой посылке на определенную величину (рис.2). Синхроимпульс представляет собой короткое (длительностью ~ 1 нс) многофотонное (классическое) состояние с несущей длиной волны 1310 нм. На рис.2 синхроимпульс изображен темным фоном. Используются два базиса: $\{+(1), \times(1)\}$ и $\{+(2), \times(2)\}$. Внутри первого базиса (индекс 1) в каждом подбазисе $\{+(1)$ и $\times(1)\}$, состояния для 0 – $|0_1(+)\rangle$ и 1 – $|1_1(+)\rangle$, соответственно, в подбазисе $|0_1(\times)\rangle$ и 1 – $|1_1(\times)\rangle$, ортогональны. Между подбазисами $+(1)$ и $\times(1)\}$ состояния попарно неортогональны, что достигается соответствующими временными сдвигами.

Аналогично для базиса 2 ($\{+(2), \times(2)\}$). Состояния в каждом базисе и подбазисах показаны на рис.2.

Введение двух базисов с двумя подбазисами внутри каждого из них, по сравнению с исходным BB84 протоколом, необходимо, чтобы не использовать интерферометр. По существу, данная реализация эквивалентна исходному протоколу BB84.

Протокол выглядит следующим образом. Выбирается случайно один из двух базисов $\{+(1), \times(1)\}$ или $\{+(2), \times(2)\}$. Далее внутри выбранного базиса случайно выбирается один из подбазисов $+$ или $\times$.

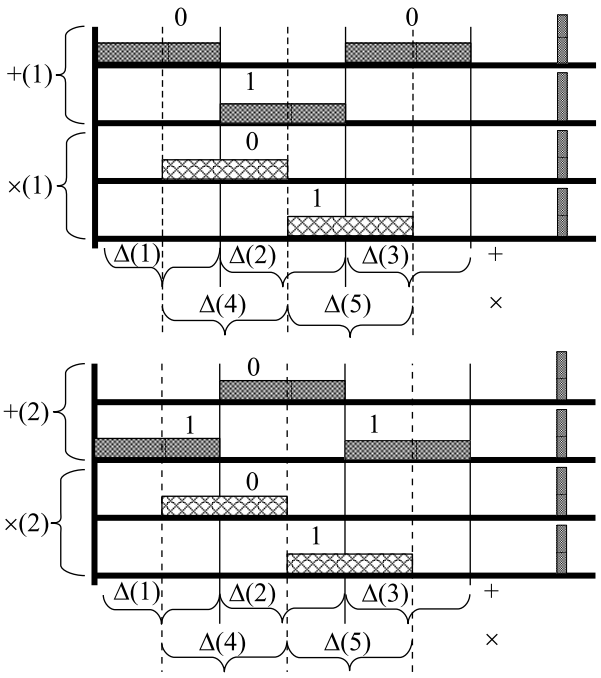

Рис.2

Затем случайно в подбазисе выбирается 0 или 1. Например, как видно из рис.2, если выбран базис 1 и далее подбазис, например, $+(1)$, то при выборе 0 возможны два варианта. Один из возможных вариантов для 0 выбирается случайно.

Для второго базиса в подбазисе $2(+)$ имеются два варианта для 1, что устраняет асимметрию.

В канал связи всегда посылается лишь одно из состояний (изображенных в виде "полочек" на рис.2). Форма состояния всегда одинакова. Разница в сдвигах относительно синхроимпульса регулируется на программном уровне (см. ниже).

Измерение состояний на приемном конце. На приемном конце относительно синхроимпульса в каждой посылке во временном окне $\Delta(1), \ldots, \Delta(5)$, которое выбирается случайно независимо от выбора на передающем конце, производится детектирование состояний (см. детали ниже).

После длинной серии измерений пользователь на приемном конце сообщает через открытый канал номера посылок, где имел факт срабатывания фотодетектора. Пользователь на передающем конце также через открытый канал для этих посылок сообщает, какой базис, $\{+(1), \times(1)\}$ или $\{+(2), \times(2)\}$, а также какой подбазис использовался в каждой из них, но, естественно, не сообщает, что было выбрано, 0 или 1, в подбазисе.

Поскольку пользователь A знает, что он посылал, а пользователь B знает, в каком временном окне у

него был отсчет, то после анонсирования базиса и подбазиса пользователю B становится однозначно известно, что было послано пользователем – A, 0 или 1 (см.рис.2).

Например, если участник A послал 0 в базисе $+(1)$ (левая "полочка" в верхней строке рис.2), и отсчет у B возник в окне $\Delta(1)$ (информация об окне не сообщается), то после сообщения базиса 1 или 2 и подбазиса $+$ или $\times$ оба пользователя будут знать, что было передано.

Если же участник B производил измерения, например, в окне $\Delta(4)$, то такая посылка будет отброшена.

В отличие от стандартного протокола BB84, в нашем протоколе для согласования базиса требуется два бита классической информации вместо одного, как в BB84.

Протокол B92. В протоколе B92 используется состояние с той же формой амплитуды (волновой функцией). Состояния, отвечающие 0 и 1, являются неортогональными за счет временного сдвига относительно синхроимпульса в каждой посылке.

Пользователь A случайно выбирает одно из состояний и направляет участнику B. Второй легитимный участник B на приемном конце случайно и независимо от A выбирает временное окно регистрации, $\Delta(0)$ или $\Delta(1)$. После длинной серии измерений участник B сообщает через открытый классический канал, в каких посылках у него было срабатывание. После этого оба участника знают переданный бит (см. рис.3).

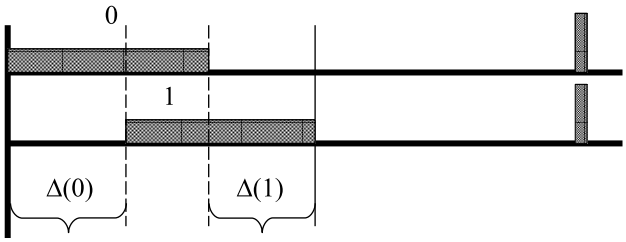

Рис.3

Протокол BB84(4+2). Данный протокол аналогичен BB84, единственная разница состоит в том, что состояния в различных подбазисах становятся неортогональными (см. рис.4). Степень неортогональности (перекрытие) может регулироваться. Выбор состояний осуществляется аналогично протоколу BB84. Имеется небольшая разница при выборе временных окон для измерений на приемном конце. Временные окна выбираются случайно и независимо от передающего конца. После серии

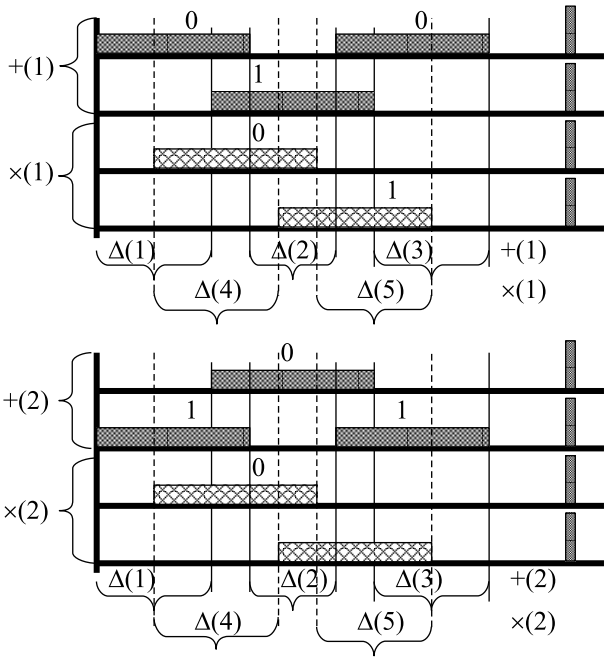

Рис.4

измерений участник A сообщает, какой базис и подбазис были использованы в каждой конкретной посылке. Участник B, зная анонсированный базис, подбазис, а также выбранное им для измерения временное окно, сообщает через открытый канал номера тех посылок, где выбор временного окна был согласован с базисом (аналогично протоколу BB84, см. рис.4).

Измерение в конечных временных окнах, по сути, реализует измерения (1)–(3), в которых получается результат с определенным или неопределенным исходами. Измерения в конечном временном окне формально описываются разложением единицы, когда каждой временной области приписывается положительная операторно-значная мера (см., например, [36]).

Описание работы блок-схемы. Блок-схема прототипа представлена на рис.5. Перед сеансом передачи ключа запускается генератор случайных чисел, который создает случайную последовательность 0 и 1, которая записывается во временную память. Далее случайная последовательность из памяти используется, в зависимости от используемого протокола, как внутренний код для выбора базиса и информационных состояний 0 или 1. Тактовый генератор запускает схему формирования синхроимпульса для лазера с несущей длиной волны 1310 нм и схему формирования информационных состояний (CW DFB лазер с несущей длиной волны 1550 нм). В нашем случае,

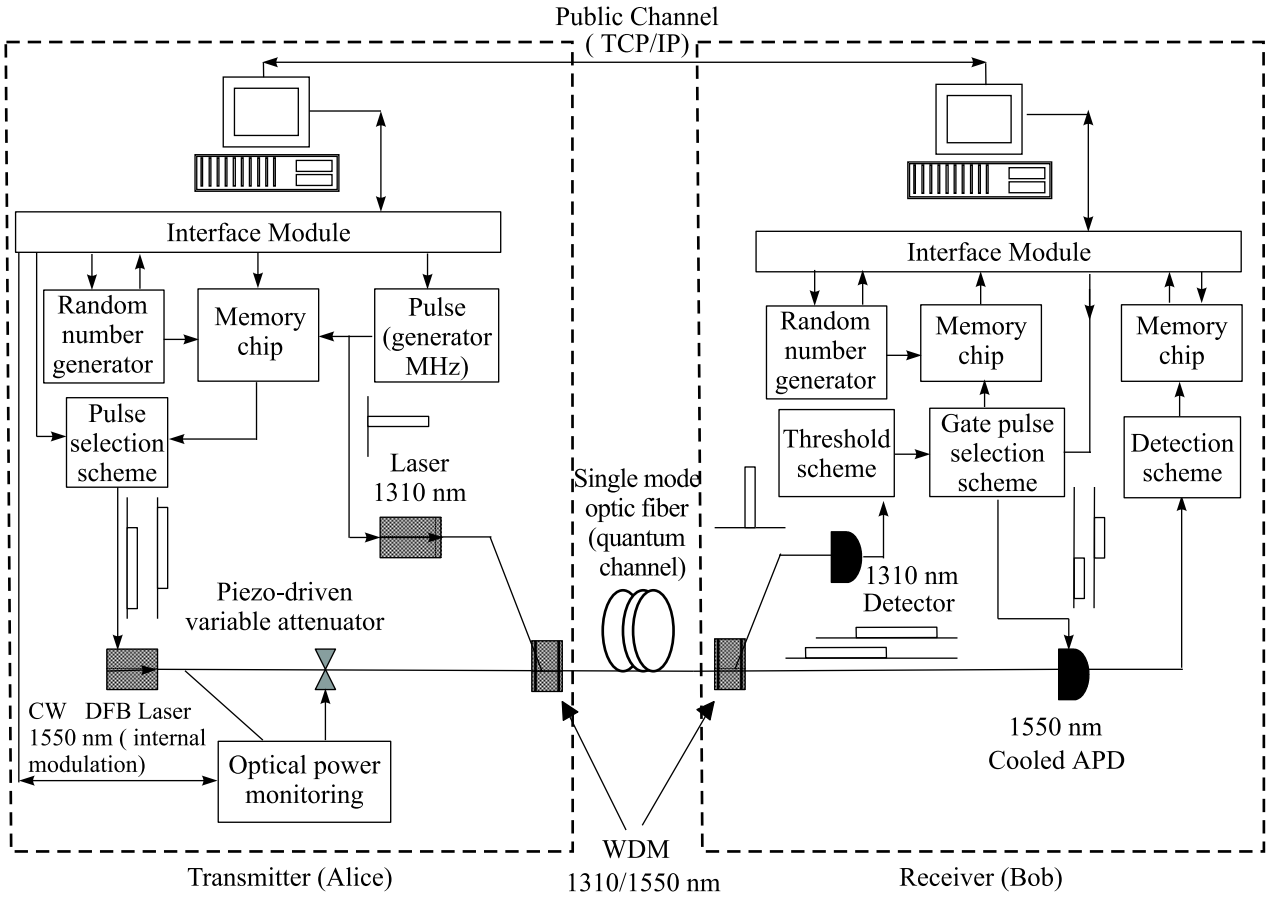

Рис.5

CW DFB-лазер – это источник, который постоянно почти включен. При непосредственной модуляции приложение "ступеньки" дополнительного импульса тока к CW DFB-лазеру приводит к появлению сигнала в оптоволоконной линии связи. Возможно также использование внешнего модулятора (затвора в оптоволоконном исполнении), в этом случае лазер включен и находится в режиме генерации. В хороших CW DFB-лазерах с множественными квантовыми ямами (MQW) ширина линии может достигать сотен кГц. Для наших целей достаточно длительности информационного состояния, например, в 20 нс (соответственно, достаточно ширины линии излучения CW DFB-лазера при работе в непрерывном режиме в $\sim 10^7$ Гц). Не имеет смысла выбирать длительность информационных состояний слишком большой, поскольку требуется в течение этого времени держать APD обратно смещенным, что увеличивает вероятность паразитных темновых отсчетов.

На приемном конце также имеется независимый генератор случайной последовательности, который перед сеансом создает эту последовательность и записывает ее во временную память. В дальнейшем данная последовательность используется при выборе временных окон для наложения импульсов обратного смещения на лавинный фотодетектор (условно запускает APD). Запуск APD инициируется приходом синхроимпульса от лазера с длиной волны 1310 нм. При срабатывании APD схема детектирования выдает сигнал в другую временную память для накопления первичного ключа, из которого после окончания передачи по квантовому каналу, затем обмена через классический открытый канал (по протоколу TCP/IP с аутентификацией) коррекции ошибок и усиления секретности (privacy amplification) получается секретный ключ.

Мультиплексный случай. Данная схема допускает естественное обобщение на мультиплексный случай с разделением каналов по длинам волн. На рис.6 приведена блок-схема мультиплексной криптосистемы, принцип работы которой аналогичен предыдущей схеме. Единственное изменение связано с введением в схему маршрутизатора (дифракционной решетки на массиве волноводов), изготовленного по

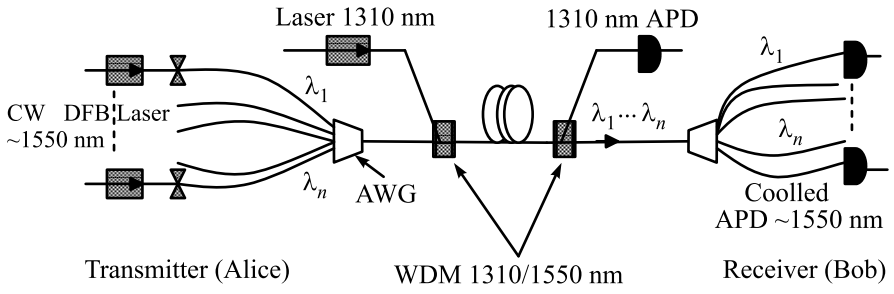

Рис.6

AWG технологии, которая позволяет "свести" на передающем конце в один оптоволоконный кабель, а на приемном "развести" по разным каналам состояния с различными длинами волн. Схема оптоволоконной части показана на рис.6.

4. Краткое сравнение со схемами квантовой криптографии, использующими метод фазового кодирования (без самокомпенсации и с самокомпенсацией).

Сделаем краткий сравнительный анализ нашей схемы с наиболее развитыми схемами, основанными на методе фазового кодирования.

Схема с фазовым кодированием без самокомпенсации. Данная оптоволоконная схема используется в первой локальной квантовой криптографической сети в Бостоне [23] (проект выполняется по заказу DARPA)[3)].

На рис.7 представлена блок-схема прототипа схемы квантовой криптографии с фазовым кодированием, реализующая протокол BB84 и не использующая пассивную самокомпенсацию. Схема представляет собой разбалансированный интерферометр Маха–Цандера с разделением времени (time division). Внутри малых плеч – между длинным и коротким плечом – интерференции нет. Интерференция имеет место между плечами на передающем и приемном концах.

Схема реализует квантовый протокол передачи ключа BB84. Кодирование происходит следующим образом. На передающем конце выбирается один из двух базисов, + или ×, причем для посылки 0 или 1 в +–базисе устанавливается фазовая задержка $(0,1) \to \varphi_A = (0,\pi)$. В случае выбора ×–базиса имеет место соответствие $(0,1) \to \varphi_A = (\pi/2, 3\pi/2)$. Выбор 0 или 1 в каждом из базисов происходит случайно путем введения соответствующей фазовой задержки. На приемном конце, независимо от передающего узла, случайно выбирается один из базисов. Устанавливается задержка φ_B, в зависимости от выбранного базиса. Посланный бит 0 или 1 различается по тому, какой из детекторов (верхний или нижний) сработал. В зависимости от варьируемой разности фазовых задержек на передающем и приемном концах на выходе имеет место конструктивная или деструктивная интерференция в том смысле, что вероятность срабатывания верхнего фотодетектора (см. рис.7) $\propto \cos^2(\varphi_A - \varphi_B) = \cos^2(2\pi(\Delta l_A - \Delta l_B)/\lambda)$, а нижнего фотодетектора – $\propto \sin^2(\varphi_A - \varphi_B) = \sin^2(2\pi(\Delta l_A - \Delta l_B)/\lambda)$.

После длинной серии Alice раскрывает, какой из базисов был выбран в каждой посылке, но не сообщается, что было выбрано внутри базиса, 0 или 1. Те посылки, где не было совпадения базисов отбрасываются. В оставшихся по тому, какой из детекторов сработал, оба участника будут знать переданный бит. Например, если оба выбрали базис + и Alice посылала 1 ($\varphi_A = \pi$), Bob, соответственно, выбрал базис + ($\varphi_B = 0$), то вероятность срабатывания верхнего фотодетектора $\propto \cos^2(\varphi_A - \varphi_B) = \cos(\pi) = 1$, а вероятность нижнего, соответственно, $\propto \sin^2(\varphi_A - \varphi_B) = \sin(\pi) = 0$. Если же Alice в том же базисе выбрала 0 ($\varphi_A = 0$), то сработает нижний фотодетектор, $\propto \sin^2(\varphi_A - \varphi_B) = \sin(0) = 1$.

На выходе передающего плеча интерферометра состояние в канале связи представляет собой суперпозицию двух "половинок", между которыми имеется фазовый сдвиг (разность хода) $\exp ik(\Delta L + \Delta l_A)$ ($k = 2\pi/\lambda$, $\lambda = 1550$ нм). Здесь ΔL – постоянная разность хода за счет разной длины верхнего и нижнего плечей в малом интерферометре на передающем конце, $2\pi\Delta l_A/\lambda = \varphi_A$ – варьируемая величина разности хода в верхнем и нижнем плечах. Величина ΔL обеспечивает раздвижку "половинок" в суперпозиции по времени (принцип разделения по времени – time division).

На приемном конце на выходе перед фотодетекторами состояние представляет собой суперпозицию трех раздвинутых по времени на величину $\Delta L/c$

[3)] Рис.7 воспроизводится из работы [23] с любезного разрешения авторов.

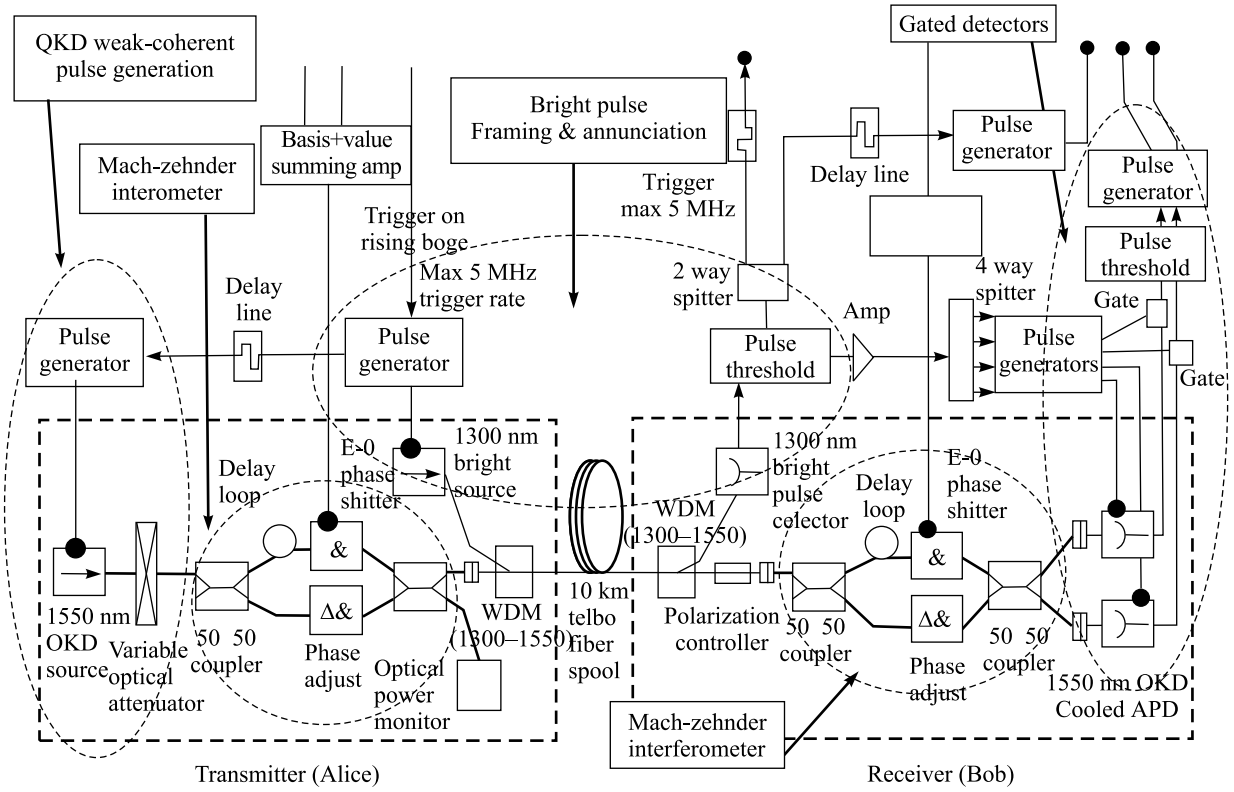

Рис.7

"пичков", причем амплитуда центрального "пичка" в два раза больше боковых. Суперпозиция трех "пичков" возникает из-за того, что каждая из "половинок" состояния, пришедших из канала связи, проходит как по длинному, так и по короткому плечу интерферометра на приемном конце. Состояние детектируется посредством наложения отрицательного смещения на лавинные фотодетекторы к моменту прихода центрального "пичка".

Для работы схемы принципиально важно выдерживать разность между разностью длин коротких и длинных путей, $\Delta l_A - \Delta l_B \sim$ доли $\lambda \sim$ доли микрон на передающем и приемном концах интерферометра. Передающее и приемное плечи интерферометра разнесены на десятки километров. Любой уход от идеальных значений приводит к ошибкам вида: был послан 0, но из-за ухода разности фаз результат детектирования может стать 1, и наоборот. Поэтому для устойчивой работы неизбежно требуется термостабилизация плеч и периодическая юстировка плеч. На это время передача ключа, естественно, прерывается. Для точной периодической юстировки существуют специальные пьезоуправляемые модуляторы в коротких плечах интерферометра. Подобная юстировка требует дополнительной управляющей электроники и программного обеспечения и сильно усложняет всю схему. Фактически работа с таким устройством является большим экспериментальным искусством.

Принцип фазового кодирования, кроме разделения по времени, использует для кодирования фазовые соотношения между отдельными "частями" состояний, которые сдвинуты по времени. Использование для кодирования фазовых соотношений неизбежно приводит к тому, что приходится использовать интерферометрические схемы, которые требуют высокой точности.

Наша схема, основанная на принципе временного кодирования, фактически исключает из схемы наиболее тонкие и сложные фазовые соотношения и оставляет лишь разделение по времени.

Отметим, что схемы с фазовым кодированием не допускают естественного и простого обобщения на мультиплексный случай, поскольку набег разности фаз будет различным для разных длин волн.

Схемы с фазовым кодированием и пассивной самокомпенсацией. Сделаем краткий сравнительный анализ со схемой квантовой криптографии с фазовым кодированием и пассивной самокомпенсацией. Дан-

ная схема подробно изучалась в исследовательской лаборатории фирмы IBM (Almaden, Californnia)[4)].

Фазовые сдвиги чувствительны к двояколучепреломлению, которое неизбежно имеет место в оптоволоконных линиях связи. Двояколучепреломление приводит к тому, что различные компоненты поляризации в состояниях приобретают разный фазовый сдвиг. Для устранения подобных паразитных фазовых сдвигов используется метод пассивной самокомпенсации, который приводит к тому, что оптоволоконная часть системы квантовой криптографии еще больше усложняется. Кроме того, схема становится двухпроходной, что эффективно вдвое удлиняет оптоволоконную линию связи. Идея самокомпенсации состоит в следующем. При прямом проходе две ортогональные компоненты поляризации – горизонтальная и вертикальная – набирают различный фазовый сдвиг. При обратном проходе за счет отражения на фарадеевском зеркале происходит переключение горизонтальной компоненты в вертикальную и наоборот. При обратном проходе приобретенный различными компонентами поляризаций разный набег фазы компенсируется.

Системы квантовой криптографии интенсивно развивались в ряде групп. Создание и настройка таких систем также является тонким экспериментальным искусством. Разберем работу такой схемы на двух примерах [21].

На рис.8 приведен прототип такой системы [21]. Излучение лазера формирует сигнальные состояния, которые после ослабления проходят через систему поляризационных светоделителей (рис.8). На выходе PBS3-фильтра возникает состояние с двумя компонентами поляризации (вертикальной и горизонтальной). Горизонтальная компонента поступает в канал связи, а вертикальная – следом за ней с некоторой временной задержкой, которая обеспечивается петлей оптоволокна, поддерживающего состояние поляризации. Здесь также используется принцип разделения по времени "частей" квантового состояния. К моменту прихода на приемный конец (рис.8, Alice) горизонтальная составляющая за счет неконтролируемого вращения в оптоволокне имеет произвольное направление. Поляризационный светоделитель (PBS4) выделяет из состояния две ортогональные составляющие, которые через оптоволокно, сохраняющее поляризацию, поступают в петлю задержки, в которой они распространяются навстречу друг другу. В середине петли имеется фазовый модулятор, при помощи которого Alice устанавливает фазовую задержку (аналогично кодированию в предыдущей схеме без самокомпенсации). Из-за того, что модулятор находится посередине петли, распространяющиеся навстречу друг другу разные компоненты поляризации приобретают к моменту встречи посередине одинаковый набег фазы. После прохождения модулятора возникает одинаковый дополнительный набег фазы, который отвечает выбору 0 или 1 в ключе. После отражения на фарадеевском зеркале происходит переключение между ортогональными компонентами поляризации (ортогональные компоненты поляризации меняются местами друг с другом). После прохождения петли обе компоненты направляются назад к передающему концу (Bob). На обратном проходе происходит пассивная компенсация разного набега фаз для ортогональных компонент поляризации, которая возникла при прямом проходе, за счет их переброса компонент между собой на фарадеевском зеркале. Аналогичные трансформации происходят с компонентой с исходно вертикальной поляризацией и сдвинутой (задержанной) по времени.

К моменту возвращения "частей" состояния (задержанной и не задержанной) на передающий конец Alice выставляет модулятором свою фазовую задержку в нижнем плече интерферометра, аналогично тому, как это имеет место в ранее описанной схеме. В зависимости от разности фаз на стороне Alice и Bob имеет место конструктивная или деструктивная интерференция между не задержанной и задержанной "частями" состояния. При совпадении базисов (выборе фазовых задержек) срабатывает детектор в канале 0 или 1 (см. рис.8).

На рис.8 (нижняя часть) приведен усовершенствованный вариант предыдущей схемы. Принцип работы аналогичен предыдущей. Уменьшение числа поляризационных светоделителей в той части схемы, которая чувствительна к фазовым изменениям, достигнуто за счет использования всюду поляризационно-поддерживающего оптоволокна.

Даже из беглого описания работы схем видно, что системы с фазовым кодированием являются очень деликатными оптическими схемами, их использование и работа с ними является скорее высоким экспериментальным искусством, чем работой со стандартной физической измерительной аппаратурой.

5. Заключение. Метод временного кодирования в квантовой криптографии позволяет принципиально упростить экспериментальные схемы и вообще избавиться от наиболее тонкой оптоволоконной части – интерферометра.

[4)] Рис.8 воспроизводится из работы [21] с любезного разрешения авторов.

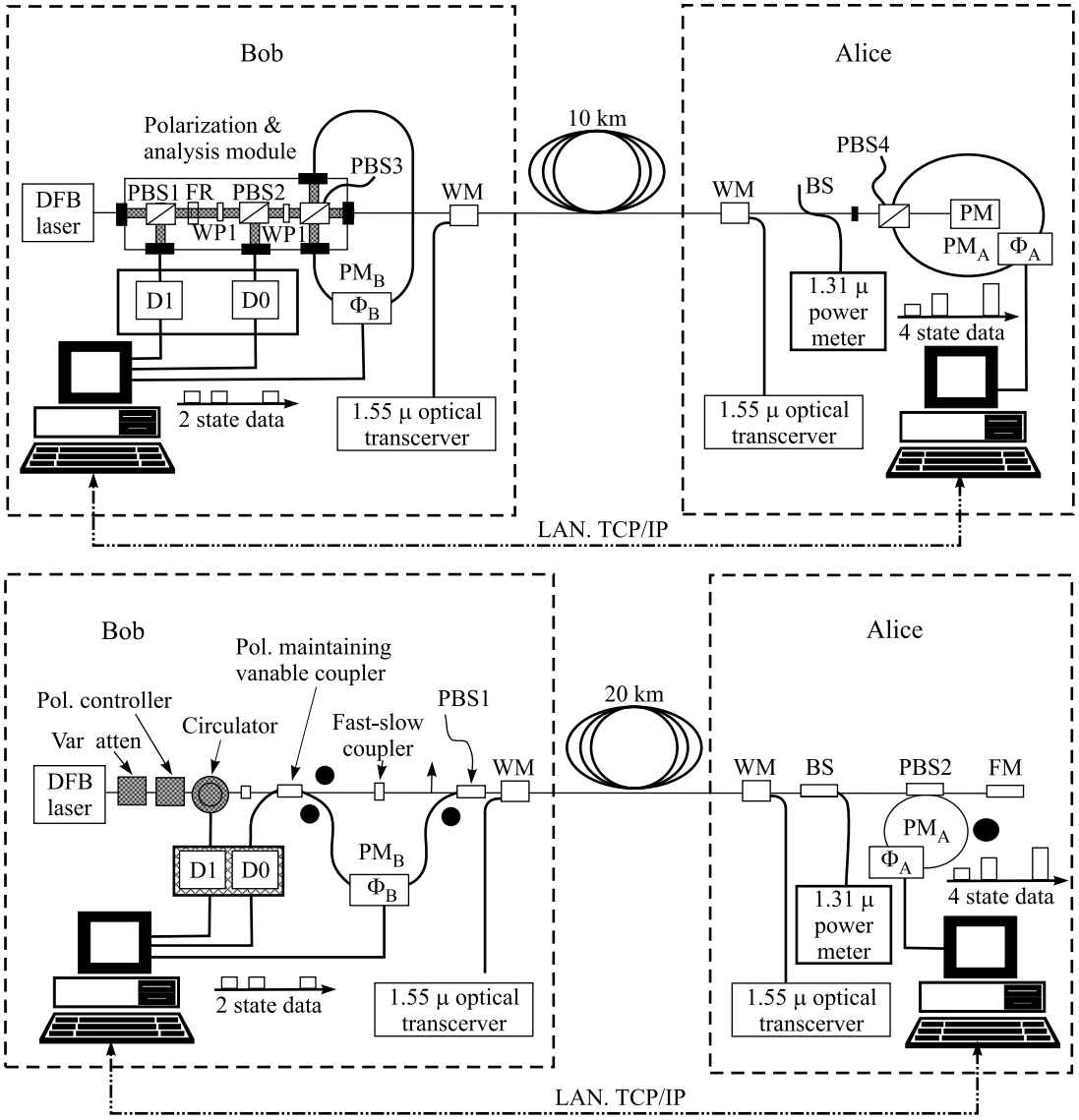

Рис.8

По сути принципиальное отличие метода временного кодирования от метода фазового кодирования состоит в том, что из метода фазового кодирования выброшена та часть, которая использует фазовые соотношения в суперпозиции между "частями" квантового состояния, и оставлена лишь часть, использующая принцип разделения по времени. Принцип разделения по времени является общим для обоих методов и является минимально необходимым в отличие от принципа фазового кодирования, который может быть вообще исключен.

Таким образом, обсуждаемые выше схемы прототипов квантовой криптографии, использующие метод временного кодирования по сравнению с существующими схемами на методе фазового кодирования, на наш взгляд, обладают рядом принципиальных преимуществ:

Не требуется оптоволоконный интерферометр, что избавляет от точной (до долей микрона) балансировки плеч и их постоянной юстировки во время работы. Не требуется электроники для управления оптическими фазовыми модуляторами в плечах интерферометра. Не требуется использование поляризационно-чувствительных оптоволоконных компонентов.

Схема позволяет реализовать все базовые квантовые криптографические протоколы.

Схемы с временным кодированием допускают естественное расширение на мультиплексный режим, что позволяет увеличить скорость передачи ключа

за счет увеличения частотных каналов и использовать криптосистему в локальных сетях, когда каждому получателю отвечает своя длина волны.

Схема является однопроходной, содержит минимальное число оптоволоконных компонентов и соединителей, что позволяет, из-за меньших потерь в оптоволокне, увеличить длину оптоволоконного канала связи.

Наконец, идеология метода временного кодирования естественно вписывается в структуру стандартных телекоммуникационных систем по структуре передаваемых сигналов (см. временные диаграммы работы), и, по сути, является почти классической, с той лишь разницей, что уровень сигнала понижен до однофотонного уровня.

Выражаю благодарность А. Н. Климову, К. Н. Ельцову, М. И. Беловолову, С. С. Назину, А. В. Королькову, А. Н. Пенину, С. П. Кулику. Работа поддержана Академией Криптографии Российской Федерации, а также проектом Российского фонда фундаментальных исследований (# 02-02-16289).

1. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).
2. В. А. Котельников, Отчет (1941).
3. C. E. Shannon, Bell Syst. Tech. Jour. **28**, 658 (1949).
4. S. Wiesner, SIGACT News **15**, 78 (1983).
5. C. H. Bennett, G. Brassard, *Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India, December, 1984, p. 175; C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
6. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
7. C. H. Bennett, F. Bessette, G. Brassard et al., J. Cryptology **5**, 3 (1992).
8. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).
9. R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Optics **47**, 533 (1998).
10. P. C. Sun, Y. Mazurenko, and Y. Fainman, Opt. Lett. **20**, 1062 (1995); Y. Mazurenko, R. Giust, and J. P. Goedgebuer, Optics Commun. **133**, 87 (1997).
11. F. Grosshans, G. Van Assche, J. Wenger et al., Nature **421**, 238 (2003).
12. H. Zbinden, H. B. Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. (Germany) **B67**, 743 (1998).
13. A. Muller, T. Herzog, B. Huttner et al., Appl. Phys. Lett. **70**, 793 (1997).
14. H. Zbinden, J. D. Gautier, N. Gisin et al., Electron. Lett. **33**, 586 (1998).
15. D. S. Bethune and W. P. Risk, IEEE J. Quantum Electr. **36**, 340 (2000).
16. G. Ribordy, J. D. Gautier, N. Gisin et al., Electron. Lett. **34**, 2116 (1998); D. Stucki, N. Gisin, O. Guinnard et al., quant-ph/0203118.
17. M. Bourennane, F. Gibson, A. Karlsson et al., Opt. Express **4**, 10 May (1999).
18. C. Marand and P. D. Townsend, Optics Lett. **20**, 1695 (1995).
19. H. Kosaka, A. Tomita, Y. Nambu et al., quant-ph/0306066.
20. T. Kimura, Y. Nambu, T. Hatanaka et al., preprint (2004).
21. D. S. Bethune and W. P. Risk, New J. of Phys. **4**, 42.1 (2002).
22. D. S. Bethune, M. Navarro, and W. P. Risk, quant-ph/0104089.
23. C. Elliot, D. Pearson, and G. Troxel, quant-ph/0307049.
24. J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82.1 (2002).
25. R. J. Huges, J. E. Nordholt, D. Derkas, and C. G. Peterson, quant-ph/0206092.
26. C. Kurtsiefera, P. Zarda, M. Halder et al., preprint (2002).
27. A. Acin, N. Gisin, and V. Scarani, quant-ph/0302037.
28. D. Mayers and A. Yao, quant-ph/9802025.
29. E. Biham, M. Boyer, P. O. Boykin et al., quant-ph/9912053.
30. P. W. Shor and J. Preskill, quant-ph/0003004.
31. K. Tamaki, M. Koashi, and N. Imoto, quant-ph 0212161 (2002).
32. N. Lutkenhaus, Phys. Rev. **A61**, 052304 (2000).
33. G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
34. G. Gilbert and M. Hamrick, *Practical Quantum Cryptography: A Comprehensive Analysis (Part I)*, Mitre Technical Report, MTR00W0000052, Mitre Corporation, 7515 Colshire Drive, McLean, VA 22102-7508 USA (2000).
35. A. Beveratos, R. Brouri, T. Gacoin et al., quant-ph 0206136.
36. С. Н. Молотков, Письма в ЖЭТФ **78**, 1156 (2003).