КВАНТОВАЯ КРИПТОГРАФИЯ

ЧАСТЬ 3*

С. Кулик, д.ф.-м.н. Физический факультет МГУ им. М.В.Ломоносова

В заключительной части обзора рассмотрена работа популярного протокола квантовой криптографии BB84 на примере поляризационных состояний фотонов.

Заметим, что квантовый канал используется для передачи некоторого массива случайных битов квантовой информации (кубитов), реализованных в поляризационных степенях свободы светового поля, а открытый канал – для обсуждения. Этапы, которые включает протокол, описаны в таблице 3 (крестиками обозначены временные слоты, в которых фотоны не были зарегистрированы вообще – либо по причине их отсутствия в исходной передаваемой последовательности, либо из-за конечной квантовой эффективности фотодетекторов, либо из-за потерь в канале связи):

1. Вводится синхронизация между действиями Алисы и Боба, т.е. каждый из них знает наверняка, в какой момент времени посылается состояние;

2. Алиса выбирает случайный массив битов (чередование 0 или 1 в моменты, оговоренные синхронизационным протоколом);

3. Алиса выбирает случайную последовательность (поляризационных) базисов – чередование либо лабораторного, либо диагонального;

4. Алиса посылает Бобу последовательность фотонов, кодируя поляризацию каждого фотона, исходя из массива битов и поляризационного базиса: каждый фотон имеет определенную поляризацию и описывается одним из четырех базисных векторов. Например, единице соответствуют состояния $|\updownarrow\rangle = |V\rangle$, $|\nwarrow\!\searrow\rangle = |-45^0\rangle$, а нулю – состояния $|\leftrightarrow\rangle = |H\rangle$ и $|\swarrow\!\nearrow\rangle = |45^0\rangle$ в лабораторном и диагональном базисах, соответственно.

5. Боб принимает (измеряет) посланные Алисой фотоны в одном из двух базисов. Причем выбор базиса – случаен. Боб интерпретирует результаты своих измерений в бинарном представлении, т.е. пользуясь тем же правилом, что и Алиса: «0» $\rightarrow |\leftrightarrow\rangle, |45^0\rangle$ и «1» $\rightarrow |\updownarrow\rangle, |45^0\rangle$. Заметим, что как следует из теории измерений, Боб полностью теряет информацию о состоянии фотона, поляризованного в лабораторном базисе, измеряя его в диагональном базисе и наоборот. Следовательно, Боб получает достоверную информацию о состоянии фотонов только в половине всех случаев – когда выбранный им базис совпал с базисом Алисы, т.е. когда измерение дает детерминированный результат. Если подслушивания не было, то в оставшейся половине случаев Алиса и Боб имеют некоррелированные результаты. Следовательно, в среднем Боб получает массив битов с 25%-ным содержанием ошибок. Этот массив называется сырым ключом. Кроме того, будем учитывать тот факт, что часть фотонов теряется при передаче. Практически, уровень технических ошибок в квантовых протоколах на сегодняшний день составляет несколько процентов (в отличие от уровня 10^{-9}, достижимого в современных опто-телекоммуникационных линиях связи). Этот уровень называется Quantum Bit Error Rate (QBER).

6. Происходит обсуждение результатов измерений по открытому каналу связи, причем и Алиса, и Боб предполагают, что их могут подслушать, но не перехватить или изменить результаты. Сначала они определяют, какие из фотонов были зарегистрированы Бобом. Затем определяют, в каких случаях Боб угадал базис. Боб сообщает базис, в котором производилось измерение, но не сообщает сам результат. При этом теряется 50% информации – когда Боб неверно угадал базис. Если сообщение не подслушивалось, то Алиса и Боб (по вероятности) делают вывод, что биты, закодированные этими фотонами, переданы правильно. Заметим, что по открытому каналу информация о случайной последовательности битов, посылаемых Алисой, не передается – вывод делается только на основе теории квантовых измерений! Каждый из переданных таким образом фотонов в правильном базисе несет один бит информации, а именно – был ли он поляризован вертикаль-

* Часть 1 и 2 см.: Фотоника, 2010, №2–3.

но или горизонтально в лабораторном базисе или под углами $\pm 45^0$ – в диагональном базисе. В итоге у Боба остается более короткий массив битов, который называется просеянным ключом.

7. Затем Алиса и Боб проверяют, были ли попытки подслушивания во время распределения ключа. Для этого они сравнивают некоторые биты, которые, как они считают, были распределены правильно, по открытому каналу связи. Позиции битов по шкале синхронизационного протокола должны выбираться случайно, но одинаково, скажем, сравнивая каждый третий бит. В этом случае обнаружение подслушивания имеет высокую вероятность и состоит в том, что Алиса и Боб имеют разные биты. После сравнения биты выбрасываются из исходной последовательности, и она сокращается. Если сравнение не обнаруживает разницы, то Алиса и Боб делают вывод, что распределение ключа произошло с высокой степенью надежности (все же, имеется вероятность не обнаружить подслушивания, но при этом у подслушивателя окажется мало информации).

8. Последний шаг протокола квантовой криптографии состоит в том, чтобы, используя классические алгоритмы, исправить ошибки (error correction) и уменьшить информацию, доступную Еве. Последняя процедура называется усилением секретности (privacy amplification). Простейшая *процедура коррекции ошибок* состоит в следующем. Алиса случайно выбирает пары битов и производит над ними операцию XOR. Боб выполняет такую же операцию над соответствующими своими битами. Если результат совпадает, они сохраняют первый из двух битов и уничтожают второй – поскольку сама процедура происходит по открытому каналу и результат доступен Еве. Если результаты отличаются – оба бита выкидываются (на практике используется более сложный алгоритм). После этой процедуры Алиса и Боб имеют одинаковые копии ключа, но у Евы все же может остаться некоторая информация о нем. Возникает необходимость в ее уменьшении – вступает в силу *протоколы усиления секретности*. Эти классические протоколы работают следующим образом. Алиса опять выбирает случайно пары битов и вычисляет их сумму по модулю 2 (XOR). Но в отличие от процедуры коррекции ошибок, она не сообщает это значение. Она лишь оглашает, какие биты были выбраны, например под номерами 103 и 539. Затем Алиса и Боб заменяют два бита на результат операции XOR. Таким образом, Алиса и Боб укорачивают свои ключи. Если Еве доступна лишь часть информации о двух битах, то ее информация о результате выполнения операции XOR будет еще меньше. Рассмотрим, например, случай, когда Еве известен только первый бит и не известен второй. Тогда она вообще ничего не знает про результат операции XOR. Если же Ева знает значения каждого из битов с вероятностью, скажем, 60%, то вероятность того, что она угадает значение операции XOR будет только $0{,}6^2+0{,}4^2=52\%$ (сумма вероятностей того, что оба бита угаданы неправильно и правильно, соответственно). Такую процедуру можно повторить несколько раз. Подчеркнем, что на этих этапах (выполнения протоколов коррекции ошибок и усиления секретности) работают исключительно классические протоколы, использующие открытые каналы связи. Итак, если вероятность ошибок не превосходит некоторой критической величины (в нерелятивистских схемах предел, по-видимому, составляет < 11% [31–33], что определяется потерями в оптическом волокне), то далее возможна коррекция ошибок в нераскрытой части при помощи классических кодов и дальнейшее сжатие ключа для получения результирующего секретного ключа.

9. Включается абсолютно стойкий протокол одноразового блокнота через открытый канал связи.

10. Весь протокол повторяется каждый раз при необходимости посылки очередного сообщения.

Заметим, что на практике для передачи квантовых битов и обмена классическими сообщениями можно использовать один и тот же канал связи. Из последних пунктов протокола видно, что платой за секретность служит существенное укорочение исходной случайной последовательности битов. Такое укорочение даже при идеальных процедурах приготовления, передачи и измерения квантовых состояний происходит за счет отбрасывания исходов, измеренных в несовпадающих базисах, а также в процессе выполнения протоколов коррекции ошибок и сжатия ключа.

В основе другого известного протокола – КК B92 – тоже лежит факт невозможности достоверно различить два неортогональных состояния. В поляризационном варианте этого протокола случайная строка битов кодируется в состояниях "0"→$|\updownarrow\rangle$, "1"→$|\swarrow\nearrow\rangle$. Достоверность различения состояния достигается лишь с конечной вероятностью: если было послано состояние $|\updownarrow\rangle$, то оно никогда не даст отсчета, будучи измеренным в проекции на состояние $|\leftrightarrow\rangle$. В то же время, состояние $|\swarrow\nearrow\rangle$ с вероятностью 50% будет зарегистрировано при этом измерении. Это прямо следует из определения состояния $|\swarrow\nearrow\rangle$ в виде линейной суперпозиции двух ортогональных состояний $|\updownarrow\rangle$ и $|\leftrightarrow\rangle$: $|\swarrow\nearrow\rangle \equiv \frac{1}{\sqrt{2}}\{|\updownarrow\rangle+|\leftrightarrow\rangle\}$, так что получается, что проектор $|\langle\leftrightarrow|\swarrow\nearrow\rangle|^2=\frac{1}{2}$. Таким образом, зарегистрированное событие при измерении проекции $|\leftrightarrow\rangle$ может соответствовать только передаваемому состоянию $|\swarrow\nearrow\rangle$ и никогда – состоянию $|\updownarrow\rangle$. В противном случае, стороны должны сделать вывод о присутствии подслушивателя, искажающего статистику передаваемых состояний.

В настоящее время разрабатываются т.н. детерминистические протоколы КК, в которых вклад в сырой ключ дают все передаваемые квантовые состояния, и нет необходимости отбрасывать исходы измерения, отвечающие несовпадающим базисам [34, 35].

АТАКИ

В КК принято различать способы перехвата квантовых состояний Евой с целью извлечения информации об исходной случайной последовательности битов. При этом Ева пользуется разными стратегиями или атаками. Основное ограничение, накладываемое на действия Евы, – невозможность нарушить законы природы. Вместе с тем, анализ секретности того или иного протокола КК, подвергнутого конкретной атаке, производится исходя из предположения о бесконечных вычислительных или технических возможностях злоумышленника, включая, например, использование квантовых компьютеров. Это требование принципа Керкхгоффа. Среди наиболее известных типов атак в квантовой криптографии выделим:

– *индивидуальные* – при которых Ева оперирует с каждым квантовым состоянием независимо от других;

– *коллективные* – когда Ева производит совместное измерение над группой состояний. Например, она анализирует группы квантовых состояний посредством перепутывания их со вспомогательными состояниями (ancilla) с последующем их хранением в квантовой памяти до этапа публичного сравнения базисов.

Конкретные атаки, которые рассматриваются при анализе секретности КК: перехват-пересылка (intersept-resend); измерения в промежуточном базисе; с человеком посередине (man in the middle); с расщеплением числа фотонов (photon number splitting); троянский конь (Trojan horse); оптимальная атака. Последняя атака, как правило, не имеет реалистичного физического воплощения, однако именно она определяет нижнюю теоретическую границу критической ошибки. Этот уровень определяется из равенства взаимной информации между Алисой-Евой и Алисой-Бобом. Так, для протокола BB84 этот уровень (для оптимальной атаки) составляет примерно 11%. Таким образом, если после статистического анализа случайной выборки переданных/принятых битов в протоколе BB84 легитимные пользователи установили, что ошибка не превышает 11%, они гарантированно могут использовать полученную общую строку битов для формирования ключа (после выполнения процедур коррекции ошибок и усиления секретности). Рассмотрим простейшую атаку «перехват-пересылка» в протоколе BB84. Эта атака сводится к тому, что Ева случайно выбирает один из двух измерительных базисов, производит измерение и переносылает Бобу то состояние, которое она измерила. В половине случаев она правильно угадывает базис, производит адекватное измерение, и перепосылает соответствующее «правильное» состояние Бобу. В этом случае подслушатель остается незамеченным и извлекает всю информацию о состоянии. Однако в другой половине случаев Ева неправильно выбирает базис и, следовательно, посылает «неправильное» состояние, которое, будучи измерено в «правильном» базисе, даст ошибку с вероятностью 0,5×0,5=0,25. Эта ошибка выявляется после процедуры сравнения базисов. Как видно, она превышает критический уровень 0,11.

РЕАЛИЗАЦИЯ И СОВРЕМЕННОЕ СОСТОЯНИЕ

С технической точки зрения различают два основных способа передачи однофотонных состояний – по имеющимся ВОЛС на основе плавленого кварца и через открытое пространство. В случае ВОЛС минимальные потери при распространении электромагнитного излучения (около 0,2 дБ/км) достигаются в диапазоне длин волн 1,3–1,55 мкм. При этом информация кодируется в фазовые степени свободы и используется схема с самокомпенсацией [36] на основе фарадеевского зеркала для устра-

нения флуктуаций поляризации в оптическом волокне. Для открытого пространства минимум потерь достигается в диапазоне 0,8 нм. Используется кодирование в поляризационные степени свободы. Характерные частоты посылок квантовых состояний составляют 100 кГц – 10 МГц. Скорость смены ключей в коммерчески доступных квантовых криптосистемах достигает 100 раз в секунду. Как говорилось выше, статистические ошибки при приеме/передаче квантовых состояний могут быть вызваны не только действием злоумышленника, но и несовершенством аппаратуры, потерями в канале связи, шумами фотодетекторов и др. Перечислим наиболее характерные ошибки, связанные с неидеальностью используемых технологий:

– отличие статистики источника света от однофотонной;

– потери в квантовом канале связи;

– темновые отсчеты фотодетекторов;

На сегодняшний день перечисленные технические трудности являются наиболее серьезным препятствием, ограничивающим длину квантовых каналов связи, при которой гарантируется безусловная секретность передаваемых ключей. Связано это с тем, что при анализе секретности конкретного протокола все ошибки считаются вызванными действиями Евы, независимо от их физической природы. Например, примесь двухфотонной компоненты в распределении фотонов используется при атаке с "расщеплением числа фотонов", когда Ева оставляет один из фотонов пары (тройки, четверки и т.д.) и измеряет его состояние. Шум фотодетектора при наличии потерь в ВОЛС приводит к таким же статистическим исходам, как и действие Евы. Поэтому Ева может заменить реальную ВОЛС, обладающую потерями на идеальную – с меньшими потерями, а "избыточные" фотоны использовать для извлечения информации о передаваемых состояниях. Вообще, регистрация отдельных фотонов в диапазоне 1,3–1,55 мкм представляет отдельную сложную задачу, а сами счетчики фотонов для КК – это уникальные устройства (рис.6). Основные проблемы здесь связаны с уменьшением паразитных (темновых) отсчетов, не сопровождающихся регистрацией фотонов, увеличением квантовой эффективности и частоты запуска детектора. Например, проблема уменьшения вклада шумовых отсчетов частично решается охлаждением фотодиода и его стробированием, т.е. запуском в момент ожидаемого прихода информационного фотона, и задача состоит в формировании короткого (сотни пикосекунд) импульса относительно большой амплитуды (несколько вольт).

Рис.6. **Однофотонный детектор в диапазоне длин волн 1,3–1,55 мкм**

Недавно появились сообщения, что в лабораторных условиях достигнуты скорости регистрации квантовых состояний на уровне 10^{10} бит в секунду, что на несколько порядков превосходит указанные выше значения для коммерческих систем КК [37, 38]. Эти данные вполне сопоставимы со скоростью обмена данных в современных

Таблица 3. Протокол BB84 (нет подслушивания, без усиления секретности)

ПЕРЕДАЧА КВАНТОВЫХ ДАННЫХ																			
АЛИСА																			
Случайная последовательность битов у Алисы	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**
Базис, случайно выбираемый Алисой	**D**	**R**	**D**	**R**	**R**	**R**	**R**	**R**	**D**	**D**	**R**	**D**	**D**	**D**	**R**	**D**	**R**	**R**	**D**
Состояние, которое посылает Алиса	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕	⤡	↔	↕	⤢
БОБ																			
Базис, случайно выбираемый Бобом	**R**	**D**	**D**	**R**	**R**	**D**	**D**	**R**	**D**	**R**	**D**	**D**	**D**	**D**	**R**	**R**	**R**	**D**	**D**
Биты, регистрируемые Бобом (***сырой ключ***)	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**
Учли технические потери	**1**	×	**1**	×	**1**	**1**	**0**	**0**	×	**1**	**1**	**1**	×	**0**	**1**	×	**0**	**0**	**0**
ОТКРЫТОЕ ОБСУЖДЕНИЕ																			
Боб сообщает базис, в котором зарегистрирован бит	**R**		**D**		**R**	**D**	**D**	**R**	×	**R**	**D**	**D**	×	**D**	**R**	×	**R**	**D**	**D**
Алиса сообщает, какой базис совпадает с ее базисом	**-**		**Да**		**Да**	**-**	**-**	**Да**	**-**	**-**	**-**	**Да**	**Да**	**Да**	**Да**		**Да**	**-**	**Да**
Предварительная распределенная информация (подслушивания нет) - ***просеянный ключ***			**1**		**1**			**0**				**1**		**0**	**1**		**0**		**0**
КОРРЕКЦИЯ ОШИБОК																			
Боб сообщает случайно выбранные биты					**1**										**1**		**0**		
Алиса сравнивает их с соответствующими своими					**Да**										**Да**		**Да**		
ИТОГ																			
Распределенный ключ			**1**					**0**				**1**		**0**					**0**

классических телекоммуникациях!

Физические принципы работы разных протоколов КК многократно демонстрировались в лабораториях. Имеются коммерчески доступные системы квантового распределения ключа на основе протокола BB84 с фазовым кодированием [39]. В Лос-Аламосской национальной лаборатории (США) завершена разработка опытной линии связи общей длиной 48 км, в которой на основе квантовой криптографии с фазовым кодированием осуществляется распределение секретных ключей со скоростью несколько кбит в секунду. Последние рекорды по длине квантового канала связи принадлежали исследовательской лаборатории Toshiba Research Europe (Великобритания), компании NEC (Япония) и Basic Research Laboratories NTT (Япония) и составляют 100 км, 120 км и 200 км. В 2004 году была создана первая локальная сеть с квантовой криптографической системой распределения ключей длиной в 10 км в Бостоне, использующей принцип фазового кодирования. Это совместный проект BBN Technologies, MTI, Harvard University, финансируемый правительственным агентством DARPA (Defense Advanced Research Projects Agency). Проект начался в 2001 году, причем продолжительность его первой стадии составила 5 лет. Аналогичный европейский проект недавно реализован в Австрии [40], причем в рамках единой сети были задействованы наиболее популярные протоколы квантового распределения ключа. Крупный шаг в направлении развития систем КК недавно был сделан в Японии. Mitsubishi Electric Corporation, NEC Corporation и Институт промышленных наук успешно произвели соединение различных систем квантового распределения ключей, разработанных Mitsubishi Electric Corporation и NEC. Такое достижение является результатом модифицирования и интеграции различных систем квантового распределения ключей, разработанных независимо NEC и Mitsubishi Electric. Например, был разработан новый интерфейс для выработки общего ключа шифрования, а также подтверждена возможность взаимодействия между различными системами квантового распределения ключей, произведенными Mitsubishi Electric и NEC. Эта ключевая технология в стандартизации систем квантовой криптографии позволит создавать высокозащищенные сети связи в будущем. Достигнуты серьезные успехи по передаче секретных ключей с использованием квантовой криптографии, работающей через открытое пространство. В 2007 году были выполнены эксперименты по передаче

ключей на расстоянии 144 км по открытому пространству между двумя островами La Palma и Tenerife в Атлантическом океане [41]. В 2008 году продемонстрирована принципиальная возможность передачи однофотонных сигналов между наземной станцией и спутником, находящимся на околоземной орбите (1400 км) [42]. Распространение технологии квантовой связи на околоземное пространство является одним из перспективных и в то же время реальных шагов в стратегических планах Европейского сообщества, США и Японии.

ПЕРСПЕКТИВЫ

Основная задача, которую предстоит решить в области КК – увеличение длины квантового канала связи при гарантированной секретности получаемых ключей. В настоящее время для протокола ВВ84 на основе ВОЛС эта длина составляет несколько десятков километров [43]. Технически задача решается путем совершенствования технологий производства ВОЛС, поляризационных и фазовых преобразователей и других элементов. Например, огромное внимание уделяется разработке новых типов однофотонных детекторов, среди которых выделим сверхпроводящие детекторы [44–46] и детекторы с преобразованием частоты вверх [43]. Физически – путем разработки новых протоколов, имеющих более высокую критическую ошибку при имеющемся уровне развития телекоммуникационных технологий:

– на квантовых состояниях более высокой размерности (D>2) [47, 48];

– на состояниях-ловушках (decoy states) [49-51];

– на основе специальной теории относительности [52];

– многопараметрических [53], позволяющих достичь верхней границы критической ошибки в 50% и другие.

Актуальной является разработка новых физических принципов создания электромагнитных полей в однофотонных состояниях, а также элементов квантовой памяти и устройств на их основе [54, 55] – таких как квантовые повторители (quantum repeater) [56]. Специалисты из NEC и Mitsubishi Electric Corporation считают, что использование уже развитой ими технологии позволит создать глобальные квантовые криптографические системы в течение ближайших пяти лет. В связи с возможным ростом использования систем КК, большое значение приобретает стандартизация ее принципов и работы [57] как отдельных узлов, так и систем в целом – в этом направлении работают комиссии Европейского сообщества, США, некоторых стран Юго-Восточной Азии. Отметим, что финансирование работ по квантовой криптографии ведется правительственными организациями всех развитых стран, а также крупнейшими компаниями, специализирующимися в области высоких технологий.

* * *

Нет сомнений, что в будущем системы квантовой криптографии будут обслуживать обмен значительной части информационных потоков. Однако надо отдавать себе отчет в том, что в силу специфики проблемы ее не всегда можно решить закупкой соответствующего оборудования за рубежом. Именно поэтому широкомасштабные исследования в области квантовой связи необходимо развернуть и в России. Подчеркнем, что это движение должно происходить параллельно по нескольким направлениям современной науки и технологии – для этого имеется необходимый теоретический задел и минимальная экспериментальная база. Закончим статью тезисом, который надо воспринимать не как пустой лозунг, а руководство к действию: сильная криптография – это сильное государство! Развитие квантовых технологий в криптографии - это путь, по которому уже двигаются десятки стран, в число которых должна войти и Рос-

сия. Автор выражает глубокую благодарность С.Н.Молоткову за плодотворные обсуждения проблем, затронутых в статье. Работа выполнена при финансовой поддержке Федерального агентства по науке и инновациям (Роснаука), Госконтракт 02.740.11.0223; гранта РФФИ 10-0290036Bel_a; и гранта поддержки Ведущих Российских научных школ 65179.2010.2.

ЛИТЕРАТУРА

31. **Mayers D., Yao A.** Unconditional Security in Quantum Cryptography, quant-ph/9802025.

32. **Biham E., Boyer M., Boykin P. et al.** A Proof of the Security of Quantum Key Distribution, quant-ph/9912053.

33. **Shor P., Preskill J.** Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, quant-ph/0003004.

34. **Beige A., Englert B.-G. et al.** Secure communication with single-photon two-qubit states. J. of Physics A: Mathematical and General, 2002, 35, L407; Secure communication with a publicly known key.– Acta Phys. Pol. A, 2002, 101, 357.

35. **Shaari J., Lucamarini M., Wahiddin M.** Deterministic six states protocol for quantum communication.– Physics Letters A, 2006, 358, 85.

36. **Herzog T., Huttner B., Tittel W. et al.** "Plug and play" systems for quantum cryptography.– Appl. Phys. Lett., 1997, 70 (7), 793.

37. **Yuan L., Dixon R., Dynes F. et al.** Gigahertz quantum key distribution with InGaAs avalanche photodiodes. – Appl. Phys. Lett. 92, 2008, 201104.

38. **Yuan Z., Dixon A., Dynes J. et al.** Practical gigahertz quantum key distribution based on avalanche photodiodes. – New J. Phys. 2009, 11, 045019.

39. http://www.idquantique.com/; http://www.magiqtech.com

40. http://www.secoqc.net/

41. **Ursin R., Tiefenbacher F., Schmitt-Manderbach T. et al.** Free-Space distribution of entanglement and single photons over 144 km .– Nature. Phys., 2007, 3, 481.

42. **Villoresi P., Jennewein T., Tamburini F. et al.** Experimental verification of the feasibility of a quantum channel between space and earth. – New J. Phys. 2008, 10 033038.

43. **Zhang Q., Takesue H., Honjo T. et al.** Megabits secure key rate quantum key distribution.– New J. Phys.2009, 11, 045010.

44. **Goltsman G., Korneev A., Divochiy A. et al.** Ultrafast superconducting single-photon detector.– J. of Modern Optics, 2009, 05.10.

45. **Zhang Q., Takesue H., Honjo T. et al.** Megabits secure key rate quantum key distribution.– New J. of Physics, 2009, 11, 045010.

46. **Ma L., Nam S., Xu H. et al.** 1310nm differential-phase-shift QKD system using superconducting single-photon detectors. – New J. Phys., 2009, 11, 045020.

47. **Bechmann-Pasquinucci H. and. Tittel W.** Quantum cryptography using larger alphabets.– Phys. Rev.A, 2000, 61, 062308.

48. **Bechmann-Pasquinucci H. and Peres A.** Quantum Cryptography with 3-State Systems. – Phys. Rev.Lett., 2000, 85, 3313.

49. **Hwang W.** Quantum Key Distribution with High Loss: Toward Global Secure Communication. – Phys. Rev. Lett., 2003, 91, 057901.

50. **Lo H., Ma X. and K.Chen.** Decoy State Quantum Key Distribution. – Phys. Rev. Lett., 2005, 94 230504.

51. **Wang X.** Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography.– Phys. Rev. Lett, 2005, 94 230503.

52. **Молотков С., Помозов Д.** Что принципиально нового дает специальная теория относительности для квантовой криптографии в открытом пространстве? – ЖЭТФ, 2004, 126.

53. **Кулик С., Молотков С., Маккавеев А.** Комбинированный фазово-временной метод кодирования в квантовой криптографии. – Письма в ЖЭТФ, 2007, 85, 354-359.

54. **Hammerer K., Sorensen A. and Polzik E.** Quantum interface between light and atomic ensembles, quant-ph 807.3358v4.

55. **Lauritzen B., Minar J., H. de Riedmatten et al.** Solid state quantum memory for photons at telecommunication wavelengths. quant-ph 0908.2348v1.

56. **Duan L.-M., Lukin M., Cirac J., Zoller P.** Long-distance quantum communic. with atomic ensembles and linear optics.– Nature, 2001, 414, 413.

57. **Länger T., Lenhart G.** Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD.– New J. Phys., 2009, 11 055051.