РАДІОТЕХНІКА І ТЕЛЕКОМУНІКАЦІЇ

УДК 003.26:621.39

Василиу Е.В., Воробиенко П.П.
Vasiliu E.V., Vorobiyenko P.P.

ПРОБЛЕМЫ РАЗВИТИЯ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ КВАНТОВО-КРИПТОГРАФИЧЕСКИХ СИСТЕМ

THE DEVELOPMENT PROBLEMS AND USING PROSPECTS OF QUANTUM CRYPTOGRAPHIC SYSTEMS

Аннотация. Рассмотрено современное состояние квантовой криптографии, показан ее вклад в решение проблем современной криптологической науки. Выполнен качественный сравнительный анализ квантовых протоколов распределения ключей и квантовых протоколов защищенной прямой связи в ракурсе их преимуществ над обычными криптографическими схемами, степени эффективности и защищенности, возможности практической реализации. Рассмотрены перспективы использования квантово-криптографических систем в существующей инфраструктуре сетей связи.

Summary. The modern status of quantum cryptography is examined; its contribution to the decision of modern cryptology problems is shown. The qualitative comparative analysis of quantum key distribution protocols and quantum secure direct communication in a foreshortening of their advantages above usual cryptographic schemes, levels of efficiency and security, an opportunity of practical realization is executed. Prospects of use of quantum cryptographic systems in an existing infrastructure of communication networks are considered.

В настоящее время бурное развитие телекоммуникаций, а также автоматизированных средств сбора, хранения и обработки информации требует разработки новых криптографических методов, обеспечивающих защиту при передаче и хранении данных.

В начале 80-х годов прошлого века была выдвинута идея использовать для целей защиты информации природу объектов микромира – квантов электромагнитного поля (фотонов), поведение которых подчиняется законам квантовой физики. Сформировавшаяся в результате развития этой идеи область науки получила название квантовой криптографии. Ее бурное развитие началось в середине 90-х годов, в первую очередь в связи с появлением технических устройств для излучения и детектирования отдельных фотонов, что позволило создать в лабораториях первые квантово-криптографические системы.

В настоящее время квантовая криптография включает несколько направлений: квантовые протоколы распределения ключей (quantum key distribution protocols), квантовые протоколы защищенной прямой связи (quantum secure direct communication), аутентификацию квантовых сообщений (authentication of quantum message) и квантовую цифровую подпись (quantum digital signature).

Отметим, что современная квантовая криптография основана на передаче битов отдельными фотонами, многофотонные импульсы должны быть исключены для обеспечения секретности передачи (см. раздел 5). В результате достигнуть высокой скорости передачи в квантовом канале пока невозможно – в настоящее время максимальная скорость составляет несколько десятков кбит/с. Следовательно, практически квантовую криптографию пока можно применять в основном для распределения ключей, которые затем будут использоваться для шифрования высокоскоростных потоков данных, передаваемых по обычным, в том числе и открытым каналам связи. Этим обусловлен приоритет одного из направлений квантовой криптографии – квантовых протоколов распределения ключей (КПРК). Большинство теоретических и экспериментальных исследований в настоящее время посвящено разработке и совершенствованию КПРК, а также анализу степени их защищенности от возможных атак.

К настоящему времени предложено свыше десятка КПРК, отличающихся как основными принципами, положенными в их основу, так и степенью их надежности, а также методами практической реализации. Следовательно, необходим сравнительный анализ предложенных квантовых протоколов в ракурсе их преимуществ над обычными классическими криптографическими схемами, степени эффективности и защищенности, возможности практической реализации. Такой анализ является целью настоящей работы.

1. Три основные задачи криптографии. Существуют три основные задачи, которые должна решать криптография [1-3]:

1. Обеспечение передачи конфиденциальной информации по открытым каналам связи.

2. Аутентификация сообщений, т.е. установление подлинности отправителя и переданной им информации.
3. Обнаружение прослушивания секретного канала связи, который используется для первоначального распределения ключей.

Решение первой задачи тесно связано с проблемой распределения секретного ключа, который затем используется для шифрования сообщений [1-3]. Как только пользователи получают общий ключ, криптограммы можно пересылать по любому незащищенному от прослушивания каналу, возможно даже по каналу, подверженному полному пассивному прослушиванию (например, публичные объявления через средства массовой информации). Однако, чтобы получить общий ключ, два пользователя, у которых исходно нет никакой общей секретной информации, должны первоначально использовать некий очень надежный и секретный канал. Поскольку перехват представляет собой серию измерений, проводимых подслушивающим агентом, какими бы сложными они не были с технической точки зрения, то любой канал можно в принципе прослушать. Это создает серьезную угрозу безопасности, чем и обуславливается важность обнаружения подслушивающего агента, т.е. решения третьей основной задачи криптографии.

Таким образом, решение первой задачи тесно связано с решением третьей – секретность передаваемой криптограммы может быть гарантирована только при условии, что ключ (или даже некоторая его часть) не попали к подслушивающему агенту. Следует подчеркнуть, что не существует никакого классического криптографического механизма, дающего гарантию, что ключ не был перехвачен во время передачи по обычному (не квантовому) коммуникационному каналу [3].

Что касается второй основной задачи – аутентификации сообщений, то она призвана предотвращать такие нарушения защиты сетевых коммуникаций, как имитация, т.е. внедрение сообщений от ложного источника, модификация содержимого сообщений, а также модификация их последовательности [1]. Задача аутентификации решается в настоящее время с помощью ассиметричных криптосистем (см. раздел 2).

2. Решение трех основных задач в классической криптографии. Классические криптосистемы подразделяются на два класса – симметричные криптосистемы, где для зашифровки и расшифровки используется один и то же ключ, и ассиметричные криптосистемы или системы с открытым ключом [1, 4]. В последних используют два ключа – открытый (публичный) и закрытый (секретный), которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, который общедоступен, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Среди симметричных систем шифрования наиболее совершенным является код Вернама, называемый также схемой с одноразовым блокнотом [1]. Здесь ключ представляет собой случайную последовательность двоичных чисел, а его длина должна быть равна длине шифруемого сообщения. В результате применения такого шифрования получается случайная последовательность, не имеющая статистической связи с самим сообщением (при этом случайный ключ необходимо обновлять с каждым новым сообщением). Поскольку в этом случае шифрованный текст не дает никакой информации о самом сообщении, то нет и способа взломать код. Таким образом, код Вернама обеспечивает полную секретность при условии обеспечения секретности ключа. Поскольку в классической криптографии нет абсолютно надежного способа распределения ключей (хотя бы потому, что не всегда возможно узнать, не прослушивался ли канал связи), а схема Вернама требует постоянной передачи длинных ключей, то на практике код Вернама используется редко, несмотря на его очевидное преимущество перед другими шифрами.

На практике в симметричных криптосистемах используют ключи, которые существенно короче длины сообщения [1-3]. В результате шифр больше не является абсолютно надежным, однако он «практически надежен». Под практической надежностью в криптографии понимают тот факт, что хотя теоретически такой шифр можно взломать, но практически для этого требуются огромные вычислительные (а соответственно и временные) ресурсы. Примером таких практически безопасных систем шифрования являются стандарты DES (Data Encryption Standard) [1] и пришедший ему на смену в 2002 году стандарт AES (Advanced Encryption Standard) [4]. Следует подчеркнуть, что основной причиной замены стандарта DES на более совершенный AES был взлом ключей DES несколькими группами во второй половине 90-х годов с помощью нескольких тысяч персональных компьютеров, объединенных в сеть [5]. Это говорит о том, что шифр, «практически надежный» сегодня, может стать бесполезным в будущем из-за быстрого роста мощности вычислительной техники.

Что касается аутентификации отправителя, то в симметричных криптосистемах эта проблема тесно связана с распределением ключей [1]. Получатель сообщения может быть уверен в том, что отправителем является законный пользователь только в том случае, если он уверен, что ключ не попал в третьи руки – ведь только в этом случае никто, кроме законных пользователей, не владеет ключом, чтобы зашифровать сообщение.

Таким образом, классические симметричные криптосистемы **не решают полностью ни одной** из вышеперечисленных задач криптографии.

Для решения проблемы безопасного распределения ключей в 1970-х гг. были созданы ассиметричные криптосистемы с открытым ключом, предлагающие математическое решение этой проблемы. В таких системах пользователям не нужно пересылать секретный ключ перед тем, как послать сообщение. Каждый пользователь имеет пару ключей – открытый и секретный. При этом, зная открытый ключ, в принципе можно раскрыть и секретный. Однако для этого требуется выполнить значительное число математических операций. Например, безопасность системы Ривеста – Шамира – Адлемана (RSA) основана на том факте, что несложно перемножить два больших простых числа, однако обратная операция – разложение на простые множители полученного произведения – требует значительно больших вычислительных ресурсов.

Таким образом, современные ассиметричные криптосистемы с открытым ключом так же, как и симметричные, «практически надежны». Возможность взлома 425-битных и даже 512-битных RSA-ключей с помощью объединенных в сеть нескольких сотен современных компьютеров была доказана в конце 90-х – начале 2000-х гг. [5]. Отметим, что в 2000 г. 95% коммерческих транзакций в Интернет защищалось 512-битными ключами. В настоящее время уже рекомендуются ключи размером 2048 бит для корпоративного использования и размером 4096 бит для шифрования особо конфиденциальной информации. Однако нет никакой гарантии, что и ключи такой длины не будут взломаны, если не при сегодняшнем уровне быстродействия вычислительной техники, то в ближайшем будущем.

Не останавливаясь на детальном анализе достоинств и недостатков ассиметричных криптосистем, отметим, что в этом случае проблема обнаружения подслушивающего агента снимается, так как ключи не распределяются вообще. Однако, в силу возможности криптоаналитического раскрытия секретного ключа, полной секретности такие системы все же не обеспечивают, тем самым не решая полностью первую задачу криптографии.

Что касается задачи аутентификации сообщения, то ассиметричные криптосистемы решают эту задачу, например, посредством цифровой подписи. Для этого отправитель должен зашифровать свое сообщение дважды – сначала с использованием своего секретного ключа, а затем полученную шифрограмму зашифровать еще раз – с помощью открытого ключа получателя [1]. Существуют и другие методы для создания аутентификатора, например, подход с использованием функций хеширования [1,4].

Резюмируя, контрольный список для ассиметричных криптосистем выглядит следующим образом:

Задача 1 решена?	**НЕ ПОЛНОСТЬЮ**
Задача 2 решена?	**ДА**
Задача 3 решена?	**ПРОБЛЕМА СНИМАЕТСЯ**

Следует также отметить, что существуют методы распределения секретных ключей (которые затем используются для симметричного шифрования) с помощью систем с открытым ключом [1], т.е. используется комбинация методов симметричного и ассиметричного шифрования. Одна из схем такого типа – схема Меркла, в которой секретный ключ передается в зашифрованном виде [1]. В другой известной схеме Диффи-Хеллмана обе стороны генерируют пары своих ключей (открытый/секретный) и обмениваются потом открытыми ключами. При этом пары ключей генерируются по таким правилам, что каждая сторона из комбинации – свой секретный ключ и открытый ключ партнера – может получить единственный ключ, одинаковый у обеих сторон, который они затем используют для шифрования сообщений методами симметричных систем шифрования. Эта схема при той же длине ключей, что и наиболее популярные ассиметричные алгоритмы, обеспечивает значительно более высокую криптостойкость.

Отметим, что изложенный подход к распределению ключей при всех своих преимуществах также является математическим, т.е. основан на том факте, что для успешного раскрытия ключа

требуются огромные вычислительные мощности (например, для алгоритма Диффи-Хеллмана это трудность вычисления дискретных логарифмов).

3. Основные свойства квантовых систем, используемые в квантовой криптографии. Для передачи информации посредством квантовых состояний с технической точки зрения проще всего использовать квантовые системы, которые могут находиться в двух состояниях (перспективы использования в квантовой криптографии систем с большим числом состояний, так называемых кудитов, в настоящей работе не рассматриваются, см., например, [6]). При этом одно из этих состояний считается соответствующим двоичному нулю, а второе – единице. Таким образом, квантовая система, имеющая два состояния, является квантовым аналогом бита. Такую систему называют кубитом (quantum bit), а ее возможные состояния формально обозначают $|0\rangle$ и $|1\rangle$. Отметим, что в квантовой механике состоянием называют полный набор физических величин, определяющих свойства системы. Так как состояние – набор величин, то его можно представить вектором в некотором пространстве комплексных чисел, в котором определены сложение и скалярное умножение векторов. В математике такое пространство называют гильбертовым. Кубит является вектором в двумерном гильбертовом пространстве, канонический ортонормированный базис которого – состояния $|0\rangle$ и $|1\rangle$.

В качестве системы, обладающей двумя состояниями, может выступать фотон, линейно поляризованный в двух взаимоперпендикулярных направлениях, например, вертикально и горизонтально. Тогда состояния, соответствующие «0» и «1», можно обозначить так: $|\updownarrow\rangle$ и $|\leftrightarrow\rangle$.

В квантовой криптографии используют ряд фундаментальных свойств квантовых систем. Перечислим их [7].

1) *Измерение физических характеристик квантовых систем*.

В результате процесса измерения некоторой физической величины состояние квантовой системы *изменяется*. Это обусловлено влиянием на квантовый объект измерительного прибора, которое принципиально невозможно сделать сколь угодно слабым. Чем точнее измерение, тем сильнее оказываемое им воздействие, и лишь при измерениях очень малой точности воздействие на объект измерения может быть достаточно слабым.

Кроме того, возмущение, вносимое взаимодействием квантового объекта с измерительным прибором, предсказуемо только статистически и поэтому не может быть исключено. Этот факт находится в резком противоречии с классической теорией измерения, которая базируется на предположении, что взаимодействие между объектом и прибором, если и не может быть сделано сколь угодно малым, то, по крайней мере, может быть точно учтено и, следовательно, в принципе его можно исключить.

2) *Невозможность точного клонирования неизвестных квантовых состояний*.

Вследствие линейности и унитарности квантовой механики, невозможно создать точную копию неизвестного квантового состояния. Таким образом, подслушивающий агент не может изготовить точную копию передаваемого по коммуникационному каналу кубита, чтобы провести измерение над копией, а оригинал переслать законному пользователю канала, не проводя над ним измерение. Этот факт лежит в основе большинства КПРК, так как вынуждает подслушивающего агента измерять пересылаемые кубиты, что приводит к изменению их состояний и соответственно к ошибкам, которые может обнаружить законный пользователь.

3) *Неортогональные квантовые состояния невозможно различить.*

Квантовая система с двумя состояниями (кубит) может находиться не только в базисных состояниях $|0\rangle$ и $|1\rangle$, но и в состоянии линейной суперпозиции

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

где α и β – комплексные числа, удовлетворяющие условию $|\alpha|^2 + |\beta|^2 = 1$. Измеряя состояние кубита, мы найдем, что кубит с вероятностью $|\alpha^2|$ несет значение «0», а с вероятностью $|\beta^2|$ – значение «1». Отметим, что суперпозиция квантовых состояний не имеет аналога в классической физике.

Вследствие законов квантовой механики невозможно выполнить измерение, которое позволило бы различить состояния

$$\left|\Psi_1\right\rangle = \alpha_1\left|0\right\rangle + \beta_1\left|1\right\rangle \text{ и}$$
$$\left|\Psi_2\right\rangle = \alpha_2\left|0\right\rangle + \beta_2\left|1\right\rangle, \quad (2)$$

кроме случая, когда скалярное произведение $\left\langle\Psi_1\middle|\Psi_2\right\rangle = 0$, т.е. состояния $\left|\Psi_1\right\rangle$ и $\left|\Psi_2\right\rangle$ ортогональны.

4) *Перепутывание (квантовая корреляция).*

Две или более квантовых системы могут быть коррелированны или перепутаны. Пара фотонов в синглетном поляризационном состоянии

$$\left\langle\Psi\right| = \frac{1}{\sqrt{2}}\left(\left|\updownarrow\right\rangle_1\left|\leftrightarrow\right\rangle_2 - \left|\leftrightarrow\right\rangle_1\left|\updownarrow\right\rangle_2\right), \quad (3)$$

где индексы обозначают номера фотонов, – пример максимально перепутанного состояния. Такое состояние называют парой Эйнштейна-Подольского-Розена (ЭПР-парой).

Если измерение выполняется над одной из двух перепутанных квантовых систем (в любом базисе), результат будет «0» или «1» с равной вероятностью. Состояние другой системы *антикоррелировано* с первой, т.е., если первая система в результате измерения перешла в состояние «0», то вторая система перейдет в состояние «1» и наоборот. Без проведения измерения, однако, ни одна из этих двух систем не находится в определенном состоянии. Отметим, что перепутывание, как и суперпозиция состояний, – исключительно квантовые эффекты, не имеющие аналога для объектов классической физики.

Четыре максимально перепутанных состояния в системе двух кубитов образуют базис Белла [2, 7]:

$$\left\langle\Psi^+\right| = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|1\right\rangle\right),$$
$$\left\langle\Psi^-\right| = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|0\right\rangle - \left|1\right\rangle\left|1\right\rangle\right),$$
$$\left\langle\Phi^+\right| = \frac{1}{\sqrt{2}}\left(\left|1\right\rangle\left|0\right\rangle + \left|0\right\rangle\left|1\right\rangle\right),$$
$$\left\langle\Phi^-\right| = \frac{1}{\sqrt{2}}\left(\left|1\right\rangle\left|0\right\rangle - \left|0\right\rangle\left|1\right\rangle\right). \quad (4)$$

Измерения в этом базисе выполняются в некоторых квантовых протоколах защищенной прямой связи (раздел 7).

4. Решение трех основных задач в квантовой криптографии. Квантовая криптография теоретически может обеспечить защищенное от перехвата распределение ключа, поскольку, в отличие от классической криптографии, она основана на законах физики, а не на том факте, что для успешного перехвата потребовались бы огромные вычислительные мощности. Вследствие вышеизложенных свойств квантовых систем, подслушивающий агент вносит в передаваемую отдельными фотонами информацию некоторое количество ошибок, которые могут быть обнаружены получателем.

Однако естественный шум в квантовом канале связи также приводит к ошибкам, и в настоящее время не разработаны методы, позволяющие отличать ошибки, обусловленные несовершенством канала, от ошибок, вносимых подслушиванием. Кроме того, для подслушивающего агента существуют стратегии, позволяющие уменьшить количество вносимых им ошибок [2]. При этом количество попадающей к нему информации также уменьшается, тем самым он получает лишь частичную информацию о ключе. Однако принципиальным является то, что для получения хотя бы этой частичной информации подслушивающий агент должен проводить измерения хотя бы части передаваемых фотонов, и поэтому уровень вносимых им ошибок не может быть сделан сколь угодно малым. Все КПРК требуют, чтобы законные пользователи отказались от распределенного ключа и начали всю процедуру сначала, если уровень ошибок при передаче превышает некоторое пороговое значение. Это значение устанавливается в зависимости от среднего уровня естественных помех в

канале (который должен быть заранее известен пользователям канала), а также зависит от конкретной реализации протокола.

Таким образом, уникальный вклад квантовой криптографии в криптологическую науку состоит в обеспечении возможности обнаружить подслушивающего агента. Таким образом, может быть решена третья проблема криптографии.

Что касается задачи аутентификации отправителя, то квантовая криптография пока практически не обеспечивает ее решения, хотя активные теоретические исследования в этом направлении ведутся [8-11]. Большинство авторов предлагают использовать для квантовой цифровой подписи перепутанные ЭПР-пары (3) или тройки фотонов и разрабатывают соответствующие протоколы. Такие протоколы в принципе могут быть реализованы с современными технологиями. В других работах для создания квантовой цифровой подписи предлагается использовать квантовые вычисления, для чего необходимы квантовые компьютеры, которые пока не созданы. Обзоры современного состояния теоретических и экспериментальных исследований в области квантовых компьютеров можно найти в [2, 12].

Таким образом, первая задача криптографии, т.е. обеспечение передачи конфиденциальной информации по открытым каналам связи, пока не решается полностью методами квантовой криптографии. Перед тем, как пользователи начнут свой протокол квантовой пересылки секретного ключа, они должны будут обменяться аутентификационными ключами, сгенерированными с помощью классических ассиметричных криптосистем.

Следует подчеркнуть, что причины, по которым первая задача не решается полностью ни в классической, ни в квантовой криптографии, различны. Классические криптосистемы не решают первой задачи криптографии по двум основным причинам: отсутствие надежных способов обнаружения подслушивающего агента при передаче ключа (в симметричных криптосистемах) и использование «коротких» ключей, которые в принципе могут быть раскрыты [2,3]. Более высокий уровень безопасности может быть достигнут при использовании кода Вернама, если будет полностью решена задача распределения ключа, т.е. третья задача криптографии. Методы квантовой криптографии позволяют решить именно эту задачу, однако пока не решают второй задачи, т.е. не обеспечивают аутентификации. Таким образом, для квантово-криптографических систем контрольный список задач криптографии в настоящее время выглядит следующим образом:

Задача 1 решена?	**НЕ ПОЛНОСТЬЮ**
Задача 2 решена?	**ПОКА НЕТ**
Задача 3 решена?	**ДА**

В настоящее время возможен синтез классических и квантовых криптографических методов в следующем составе: код Вернама для шифрования сообщения, классические методы аутентификации (например, обычная цифровая подпись) и квантовый протокол для распределения ключа. Такая схема будет обеспечивать более высокий уровень безопасности, чем любая классическая криптографическая схема.

Возможно, вскоре будут созданы и надежные способы аутентификации сообщений с помощью квантовых методов; как отмечено выше, ведутся активные исследования в этом направлении. Тогда квантовая криптография, вероятно, сможет решить все три основные задачи криптографии.

5. Квантовые протоколы распределения ключей с одиночными фотонами и их практическая реализация. Прежде чем перейти к рассмотрению основных принципов КПРК, отметим, что в англоязычной литературе существует традиция называть Алисой и Бобом два лица, которые хотят секретно общаться, а Евой – подслушивающего агента. Общий сценарий КПРК таков: Алиса и Боб хотят установить общий секретный ключ, а Ева хочет получить хотя бы частичную информацию о ключе.

Все предложенные к настоящему времени КПРК на кубитах основаны на пересылке одиночных либо перепутанных фотонов между Алисой и Бобом. Рассмотрим сначала группу протоколов, основанных на пересылке одиночных фотонов. В таких протоколах каждый фотон несет один бит информации.

Первый протокол этого класса был предложен Ч.Х. Беннетом и Г. Брассаром в 1984 г. [2], впоследствии он получил название BB84. В этом протоколе используют два поляризационных

базиса: $\oplus$, соответствующий вертикальной (двоичный 0) либо горизонтальной (двоичная 1) линейной поляризации фотонов и $\otimes$ – соответствующий двум диагональным линейным поляризациям. Алиса случайным образом выбирает базис и поляризацию своих однофотонных импульсов и посылает их Бобу, т.е. Алиса с одинаковой вероятностью посылает одно из четырех квантовых состояний:

$$\begin{aligned} &|0\rangle, \\ &|1\rangle, \\ &|\overline{0}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \\ &|\overline{1}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \end{aligned} \qquad (5)$$

Случайная поляризация выбирается потому, что ключ должен представлять собой случайную последовательность бит, а два базиса нужны для того, чтобы помешать Еве правильно регистрировать поляризацию фотонов. Пример стадий протокола BB84 показан на рис. 1.

Базис А	⊗	⊕	⊕	⊗	⊕	⊗	⊗	⊕	⊗	⊗	⊕
Значенне бита А	0	1	0	1	1	0	1	0	0	0	0
А посылает	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\updownarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$
Базис В	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗	⊕	⊕	⊕
Бит В	0	1	0	0	1	0	1	1	0	1	0
Тот же базис?	да	да	нет	иет	да	да	да	нет	иет	иет	да
У А остается	0	1			1	0	1				0
У В остается	0	1			1	0	1				0
Проверка Евы	да	нет			да	нет	иет				иет
Ключ		1				0	1				0

Рисунок 1 – Пример стадий протокола BB84 [2]

Для каждого фотона Боб случайным образом выбирает базис, и измеряет поляризацию в выбранном базисе. Полученный Бобом набор битов называют сырым ключом. Затем он сообщает Алисе по открытому каналу, какой базис он использовал для каждого измерения (разумеется, не сообщая результаты измерений). Алиса сообщает, какой базис использовала она. Так как Боб угадывает базис, выбранный Алисой, в среднем в половине случаев, то в результате он правильно принимает около половины бит, посланных Алисой. Алиса и Боб отбрасывают все биты, соответствующие случаям, когда они использовали разные базисы и в результате получают просеянный ключ. Эффективность протокола BB84, равная отношению средней длины просеянного ключа к средней длине сырого, в отсутствие помех равна 0,5.

Далее проводится процедура обнаружения перехвата. Так как во время передачи Алиса использует случайный базис, то для Евы нет способа определить, в каком базисе проводить измерение. Она может только также случайно выбрать базис, выполнить измерение и оправить Бобу новый фотон в том состоянии, которое она измерила. Это неизбежно приведет к ошибкам в строке, которую получает Боб. Отметим также, что запрет на клонирование неизвестных квантовых состояний не позволяет Еве клонировать передаваемые Алисой фотоны и хранить их до того момента, пока Алиса не объявит Бобу использованные ею базисы по открытому каналу.

Таким образом, если Ева перехватывает все посылаемые Алисой одиночные фотоны, измеряет их в случайном базисе и отправляет затем новые фотоны Бобу в измеренном ею состоянии, то она вносит в среднем 25% ошибок в просеянный ключ, что легко могут обнаружить Боб и Алиса.

Поясним уровень ошибок, вносимых Евой. Используя для измерений два базиса с одинаковой вероятностью, Ева в среднем в половине случаев правильно угадывает базис, используемый Алисой, и не вносит ошибок. В оставшейся половине случаев Ева выбирает неправильный базис. Согласно законам квантовой механики, измерение поляризации одиночного фотона в $\otimes$-базисе, если он был поляризован в $\oplus$-базисе, с одинаковой вероятностью $p = 1/2$ дает два результата: поляризация фотона повернута на угол 45° и поляризация фотона повернута на угол -45° относительно вертикальной оси [2]. Разумеется, это утверждение справедливо и при перестановке базисов местами.

Пусть, например, для приготовления состояния фотона Алиса использовала $\oplus$-базис, а Ева для его измерения $\otimes$-базис. Тогда независимо от того, что послала Алиса – фотон с вертикальной или горизонтальной поляризацией (состояние $|0\rangle$ или $|1\rangle$), Ева с одинаковой вероятностью $p = 1/2$ измерит поляризацию в направлении, повернутом на 45° (состояние $|\overline{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$), или на -45° (состояние $|\overline{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$) относительно вертикальной оси. Затем Ева отправляет фотон Бобу в измеренном ею состоянии. Однако для битов просеянного ключа Алиса и Боб использовали одинаковые базисы. Это значит, что Боб для измерения отправленного Евой фотона использовал $\oplus$-базис, не совпадающий с базисом Евы. Следовательно, Боб с одинаковой вероятностью $p = 1/2$ измерит состояние фотона как $|0\rangle$ либо $|1\rangle$. Понятно, что в среднем в половине случаев результат измерения Боба, т.е. конкретное значение полученного им бита, совпадет с тем, что отправила Алиса. Таким образом, из половины случаев (в среднем), когда базис Евы не совпадает с базисом Алисы, Боб получит результат, отличающийся от того, который послала Алиса, в среднем в половине случаев, т.е. в итоге биты Алисы и Боба будут отличаться в среднем в 25% случаев.

На практике Алиса и Боб случайным образом выбирают некоторое подмножество битов из просеянного ключа и сравнивают их, пользуясь открытым каналом связи. Если все биты совпадают, то перехвата не было. Отбросив выбранные биты (так как они могут стать известны Еве), они в результате получают окончательный секретный ключ. Отметим, что для приведенного на рис. 1 примера проверочные биты Алисы и Боба совпадают. Это означает, что Евы нет.

Таким образом, протокол BB84 можно считать полностью защищенным против вышеописанной атаки – перехвата всех фотонов, измерения их поляризации в одном из двух случайно выбираемых базисов, и отправки новых фотонов законному пользователю в состояниях с измеренной поляризацией, так как уровень вносимых при этом ошибок – 25% – достаточно велик.

Подчеркнем, что вышесказанное справедливо, только если каждый импульс Алисы несет один фотон. Наличие в импульсе более одного фотона позволяет Еве использовать более изощренные стратегии перехвата [2, 3, 5, 13]. Примером такой стратегии является «атака расщепления числа фотонов» (photon number splitting attack) [13].

При этой атаке Ева измеряет число фотонов в каждом импульсе. Такое измерение не изменяет квантовых состояний самих фотонов. Всякий раз, когда Ева обнаруживает, что импульс содержит два или более фотонов, она изымает один фотон из импульса. Оставшиеся фотоны отправляются Бобу без изменения их состояний. Это значит, что Ева не вносит никаких ошибок в просеянный ключ и, следовательно, не может быть обнаружена.

Затем Ева может отложить измерение состояний перехваченных ею фотонов до того момента, пока она не узнает базис поляризации для каждого фотона по открытому каналу, который используют Алиса и Боб для просеивания ключа. Таким образом, Ева может узнать значение бита для каждого перехваченного ею фотона. Чтобы гарантировать, что Боб не получает слишком много фотонов по сравнению с известным ему средним значением для квантового канала с потерями, Ева может блокировать некоторые сигналы полностью, в первую очередь однофотонные сигналы, которые она не может перехватить, не создавая дополнительных помех в канале. Такая стратегия позволяет Еве получить полный ключ, оставаясь незамеченной, если потери в квантовом канале настолько высоки, что она может блокировать все однофотонные сигналы. Отметим, что хотя

описанная атака допускается квантовой физикой, но ее практическое выполнение находится пока вне возможностей современных технологий.

В 1992 г. Ч.Х. Беннетом был предложен протокол с одиночными фотонами, где вместо поляризации используется фазовое кодирование [14] (детальное описание протокола, получившего название B92, а также его усовершенствований дано в [2,3]). Такая система менее подвержена помехам, возникающим в оптическом волноводе при передаче фотонов, в остальном протокол аналогичен BB84.

Для увеличения эффективности протокола BB84 в [15] была предложена следующая схема. Алиса выбирает один из двух базисов, которые она использует для поляризации фотонов, не с вероятностью $p = 1/2$, а использует $\oplus$-базис с вероятностью $0 < p < 1/2$ и соответственно $\otimes$-базис с вероятностью $(1-p) > 1/2$. Таким образом, один из базисов, в данном случае $\otimes$-базис, является доминантным. Эффективность протокола равна $1-p$ и тем больше, чем меньше величина *p*, т.е. чем чаще используется один из базисов по сравнению с другим.

Однако Ева тоже может выбирать базисы для измерения перехваченных ею фотонов с разной вероятностью. Например с вероятностью p_1 она выполняет измерение в $\oplus$-базисе, с вероятностью p_2 – в $\otimes$-базисе и с вероятностью $1-p_1-p_2$ не проводит измерения вообще, чтобы уменьшить количество вносимых ошибок. В таком случае средний уровень ошибок, вносимых подслушиванием, равен [15]:

$$\bar{e} = \frac{p^2 p_2 + (1-p)^2 p_1}{2\left\{p^2 + (1-p)^2\right\}}. \qquad (6)$$

Если Ева всегда использует доминантный базис, т.е. $p_1 = 0$, $p_2 = 1$, то при $p \to 0$, т.е. когда Алиса использует доминантный базис в подавляющем большинстве случаев, средний уровень ошибок $\bar{e} = \dfrac{p^2}{2\left\{p^2 + (1-p)^2\right\}} \to 0$.

Следовательно, увеличение эффективности протокола BB84 за счет неравновероятного использования базисов приводит к невозможности обнаружить Еву, если определять количество ошибок для всей передачи ключа. Если, однако, определять количество ошибок отдельно для каждого базиса, то ситуация кардинально меняется. Для $\oplus$-базиса Алисы, Ева вносит ошибки, только если проводит измерение в $\otimes$-базисе, причем средний уровень создаваемых ею ошибок $\bar{e}_1 = p_2/2$. Аналогично для $\otimes$-базиса Алисы, Ева вносит ошибки, измеряя в $\oplus$-базисе, т.е. $\bar{e}_2 = p_1/2$. Возвращаясь к рассмотренному случаю $p_1 = 0$, $p_2 = 1$, $p \to 0$ можно видеть, что в то время как $\bar{e} \to 0$, средний уровень ошибок в недоминантном базисе $\bar{e}_1 = 1/2$, т.е. в этом базисе Ева вносит в среднем половину ошибок в строку битов, полученную Бобом. Такой высокий уровень ошибок легко может быть обнаружен. Резюмируя, описанный «смещенный» протокол позволяет увеличить эффективность при передаче ключа, сохраняя при этом секретность, если оценивать ошибки отдельно для каждого базиса.

Для практической реализации протоколов с одиночными фотонами в настоящее время используют слабые когерентные импульсы, излучаемые лазерными светодиодами. Основной их недостаток – наличие в части импульсов нескольких фотонов, что теоретически делает возможным атаку расщепления числа фотонов или другие атаки подобного типа. Для детектирования используются специальные устройства, позволяющие измерить поляризацию одиночного фотона. Эти устройства пока тоже не совершенны и часто вообще не регистрируют одиночный фотон (так называемые «темные отсчеты»).

В качестве передающей среды используют оптоволокно, проводятся также эксперименты по передачи поляризованных одиночных фотонов по воздуху. Основная проблема здесь состоит в том, что в оптоволоконных линиях происходит деполяризация фотонов, а квантовый канал нельзя усилить без потери его квантовых свойств. Поэтому реальная связь с приемлемым уровнем ошибок возможна пока лишь на ограниченных расстояниях – немногим более 100 км. При передаче отдельных фотонов по воздуху мешает солнечный свет, а также турбулентность атмосферы, здесь пока достигнуты расстояния порядка десяти км. Детальное описание выполненных экспериментов по квантовому распределению ключа с использованием протокола BB84 дано, например, в [16] для передачи по

оптоволоконной линии и в [17] для передачи по воздуху. Выполнялись и другие подобные эксперименты, как с одиночными, так и с перепутанными парами фотонов [5].

6. Квантовый протокол распределения ключей с помощью перепутанных состояний. Протокол был предложен А. Экертом в 1991 г. [18]. Обнаружение подслушивания в этом протоколе основано на свойствах перепутанных пар фотонов. Если измерить физические характеристики одного из фотонов перепутанной пары, тем самым изменив его состояние, то изменится состояние и второго фотона, даже если он не взаимодействует с первым после перепутывания.

Распределение ключа производится через квантовый канал, который содержит источник, испускающий ЭПР-пару фотонов в состоянии (3). Фотоны разлетаются в разные стороны (вдоль некоторой оси *z*) по направлению к двум законным пользователям канала, Алисе и Бобу, которые после получения фотонов выполняют измерения и регистрируют результат этих измерений в одном из трех базисов, получаемых вращением $\oplus$-базиса вокруг оси *z* на некоторые заранее определенные углы. При этом значения углов поворота базисов должны быть одинаковыми у Алисы и Боба в двух случаях из трех, например, у Алисы: $\varphi_1^A = 0$, $\varphi_2^A = \pi/4$, $\varphi_3^A = \pi/8$; у Боба: $\varphi_1^B = 0$, $\varphi_2^B = -\pi/8$, $\varphi_3^B = \pi/8$. Конкретный базис для каждого измерения – оба они выбираются случайно и независимо друг от друга.

После того, как произошла передача, Алиса и Боб могут публично объявить, какие ориентации базисов они выбирали в каждом конкретном случае, и разделить проведенные измерения на две различные группы: в первой группе будут измерения, в которых они использовали отличающиеся ориентации базисов, а во второй – те, в которых ориентации базисов совпадали. Они также отбрасывают все случаи, когда один из них или они оба вообще не смогли зарегистрировать ни одного фотона. Таким образом, при отсутствии помех эффективность протокола Экерта равна $2/9$, так как случаи использования разных базисов используются только для контроля подслушивания и отбрасываются при просеивании ключа.

После этого Алиса и Боб могут открыто показать друг другу результаты, которые они получили в рамках одной только первой группы измерений, т.е., когда ориентации их базисов не совпадали. Это позволяет им установить значение некоторой величины *S*, которая составляется из коэффициентов корреляции измерений, в которых они использовали различные базисы. Величину *S* также можно вычислить, используя законы квантовой механики [2, 18]:

$$S = E\left(\varphi_1^A, \varphi_2^B\right) + E\left(\varphi_1^A, \varphi_3^B\right) + E\left(\varphi_2^A, \varphi_3^B\right) - E\left(\varphi_2^A, \varphi_2^B\right), \qquad (7)$$

где $E\left(\varphi_i^A, \varphi_j^B\right) = -\cos\left(2\left(\varphi_i^A - \varphi_j^B\right)\right)$, тогда $S = -2\sqrt{2}$. Если значение *S*, полученное в результате измерений Алисы и Боба при использовании ими различных базисов, равно $-2\sqrt{2}$, то состояния фотонов из перепутанных пар не были изменены на пути от источника к законным пользователям. Следовательно, результаты, полученные во второй группе измерений, т.е. когда Алиса и Боб использовали одинаковые базисы, антикоррелируют и могут быть преобразованы в секретную строку битов – ключ.

Если же полученная величина *S* не равна $-2\sqrt{2}$, то это означает, что состояния фотонов были изменены, либо в результате перехвата, либо в результате помех в канале связи. Далее Алиса и Боб должны оценить уровень ошибок и либо признать его приемлемым и провести так называемую процедуру квантового усиления секретности (детали процедуры описаны, например, в [2]), которая позволит им все-таки установить секретный ключ, либо, если уровень ошибок неприемлем, то независимо от их природы – наличие подслушивающего агента Евы или наличие помех в канале – нужно повторить всю процедуру сначала.

Протокол с перепутанными фотонами, так же, как и протоколы, основанные на пересылке одиночных фотонов, не идеален. Существуют стратегии подслушивания, основанные на использовании Евой заранее приготовленных пробных состояний, которые определенным образом взаимодействуют с перехваченными ею фотонами. Для этого Ева должна выполнить унитарное преобразование, перепутывающее ее пробу с фотоном Алисы или Боба [2,5]. При этом, разумеется, Ева должна выбирать такое преобразование, чтобы подслушивание оставалось осторожным, т.е. чтобы процедура перепутывания проб с фотонами Алисы или Боба не изменяла состояний всех этих фотонов. Затем Ева может сохранять полученные квантовые состояния проб до тех пор, пока Алиса и

Боб не объявят свои базисы измерений, а потом измерить состояния проб так, чтобы извлечь как можно больше информации. Методы извлечения информации из сохраненных Евой проб также, как и методы противодействия подобным атакам, активно исследуются в настоящее время и составляют предмет так называемого квантового криптоанализа [2, 3, 5, 19-21].

7. Квантовые протоколы защищенной прямой связи (КПЗПС). Эти протоколы предназначены для непосредственного обмена секретными сообщениями без первоначального распределения ключа [22-25]. Сообщение пересылается непосредственно через квантовый канал, но для контроля подслушивания необходима передача информации по обычному каналу, аналогично случаю КПРК.

Протоколы основаны на передаче отдельных фотонов из перепутанных ЭПР-пар либо троек. В качестве последних используют так называемые состояния Гринберга-Хорна-Цайлингера (ГХЦ) [2]:

$$\langle\Psi| = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle_1|\updownarrow\rangle_2|\updownarrow\rangle_3 + |\leftrightarrow\rangle_1|\leftrightarrow\rangle_2|\leftrightarrow\rangle_3\right). \qquad (8)$$

Одним из КПЗПС является «пинг-понг протокол», предложенный в [22]. Согласно этому протоколу, Боб готовит два фотона в перепутанном состоянии (3). Он хранит один фотон (домашний фотон) в своей лаборатории и посылает Алисе другой фотон (фотон передачи) через квантовый канал. После получения фотона передачи Алиса случайным образом переключается между режимом контроля подслушивания и режимом сообщения. В режиме контроля Алиса измеряет поляризацию фотона передачи в произвольно выбранном ею базисе и затем объявляет публично результат измерения и использованный базис. После этого Боб также переключается в режим контроля, чтобы измерить домашний фотон в том же самом базисе, который использовала Алиса. Затем он сравнивает оба результата измерения. Согласно законам квантовой механики, результаты должны быть полностью антикоррелированы в отсутствии Евы, т.е. если Алиса получила в результате измерения «0», то Боб должен получить «1», и наоборот. Поэтому, появление идентичных результатов измерений у Алисы и Боба является свидетельством подслушивания, и если это происходит, передача прерывается. В режиме сообщения, Алиса выполняет некоторую перепутывающую унитарную операцию над фотоном передачи, чтобы закодировать информацию и посылает фотон назад Бобу. После получения этого фотона Боб измеряет состояние обоих (домашнего и фотона передачи) в базисе Белла (4), чтобы декодировать посланную Алисой информацию.

Однако в [23] было показано, что пинг-понг протокол подвержен необнаружимым атакам в случае квантового канала с помехами, атака в этом случае может быть замаскирована под естественный шум. Поэтому необходимо разработать способы защиты пинг-понг протокола от таких атак. Некоторые результаты в этом направлении уже получены. Так, например, предложены протоколы с перепутанными трехчастичными ГХЦ-состояниями вида (8), использующие квантовую телепортацию фотонов [24].

Важной задачей совершенствования КПЗПС является их распространение на случай передачи информации не только между парой, а и между множеством пользователей. Некоторые подобные схемы уже предложены [26-28]. Так в [26] три отдельных пользователя посылают сообщения на отдаленный приемник, используя перепутанные состояния четырех фотонов. Эту схему можно рассматривать, как часть коммуникационной сети, где каждая сторона может тайно обмениваться сообщениями с центральной стороной или сервером. Отметим, что практическая важность подобных схем заключается в возможности их использования, например, для защиты транзакций между клиентами и сервером банка. Однако подобные схемы, основанные на перепутанных состояниях нескольких фотонов, достаточны сложны, их стойкость против различных видов атак не доказана, а практическая реализация лежит пока за пределами возможностей существующих технологий.

Недавно был предложен простой протокол непосредственного обмена секретными сообщениями между двумя сторонами [29], основанный на произвольных унитарных преобразованиях кубитов. Единственным условием, налагаемым на выполняемые двумя сторонами преобразования, является их коммутативность.

Схема протокола показана на рис. 2. Протокол состоит из трех стадий пересылки кубитов. Вначале Алиса готовит однокубитное состояние X, которое является одним из двух ортогональных состояний, представляющих собой биты 0 и 1. Например, это состояния $|0\rangle$ и $|1\rangle$, или их линейные

комбинации $\alpha|0\rangle+\beta|1\rangle$ и $\beta|0\rangle-\alpha|1\rangle$. Затем Алиса выполняет унитарное преобразование U_A состояния X и отправляет кубит Бобу (первая стадия). Боб выполняет преобразование U_B над полученным кубитом $U_A(X)$ и отправляет его обратно Алисе (вторая стадия). При этом преобразования U_A и U_B должны быть коммутативны, т.е. $U_A U_B = U_B U_A$. Например, это могут быть операторы независимых поворотов поляризации фотона вокруг двух осей декартовой системы координат:

$$U_A = R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \qquad U_B = R(\varphi) = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}, \tag{9}$$

где θ – угол поворота вокруг оси *OX*, φ – угол поворота вокруг оси *OZ*.

Далее Алиса выполняет сопряженное преобразование U_A^+ над полученным ею кубитом $U_B U_A(X)$ и в результате получает $U_B(X)$, так как $U_A^+ U_B U_A(X) = U_A^+ U_A U_B(X) = U_B(X)$, вследствие коммутативности U_A и U_B и унитарности U_A. Наконец, на третьей стадии Алиса пересылает $U_B(X)$ Бобу и он выполняет преобразование U_B^+, получая в результате исходный кубит *X*, так как $U_B^+ U_B(X) = X$ вследствие унитарности U_B.

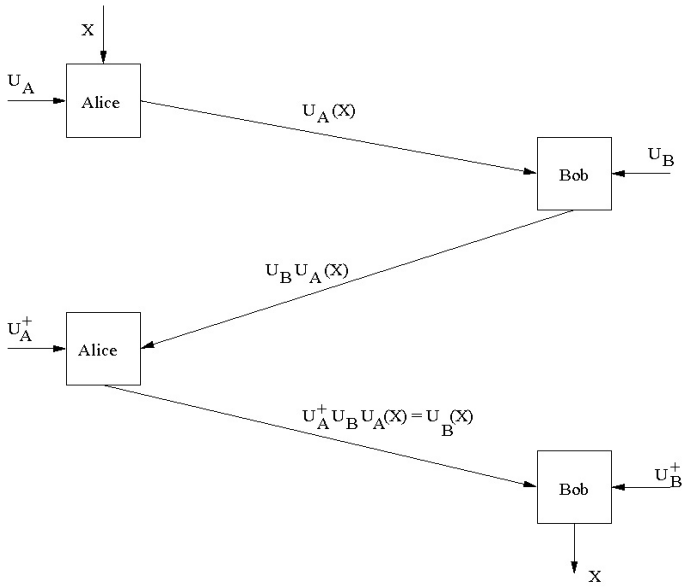

Рисунок 2 – Трехшаговый КПЗПС между двумя пользователями при $U_A U_B = U_B U_A$ [29]

Отметим, что пересылка кубитов может происходить по открытому квантовому каналу связи, поскольку подслушивающий агент Ева, не имея информации о выполняемых преобразованиях над кубитами, не может получить никакой информации о значениях самих кубитов. Однако Боб и Алиса должны предварительно договориться, по крайней мере, о классе допустимых преобразований для обеспечения их коммутативности. При этом точное знание Алисой преобразования Боба, и наоборот, знание Бобом преобразования Алисы, вообще говоря, не требуется.

Отметим также, что этот протокол легко обобщается на случай секретного обмена сообщениями между множеством отдельных пользователей и центром.

8. Перспективы практического использования квантовой криптографии. В настоящее время исследования по безопасной прямой передаче сообщений (без шифрования) с помощью квантовых систем становятся все более активными, однако такая технология еще не достигла степени надежности, необходимой для ее практического применения. Поэтому вопрос о замене существующих сетей передачи данных на защищенные квантовые сети пока не стоит. Так, предложенные квантовые протоколы защищенной прямой связи, с одной стороны, не обладают необходимым уровнем стойкости против некоторых видов атак, а с другой стороны, эти протоколы

либо пока вообще не могут быть реализованы практически, либо реализуются с неприемлемо низкой скоростью передачи кубитов.

Однако технология квантового распределения ключей, в случае, если не требуется высокой скорости их генерации, уже сейчас может быть интегрирована в существующую инфраструктуру сетей передачи данных. Так, большинство виртуальных частных сетей, широко распространенных во всем мире, используют защищенный протокол IPSec, требующий шифрования всего потока обмена данными на уровне IP. Ключи для такого шифрования можно распределять по отдельной квантовой сети.

С 2002 года американской компанией BBN Technologies в сотрудничестве с Гарвардским и Бостонским университетами выполняется пятилетний проект, целью которого является разработка общей архитектуры, соединяющей квантовые сети распределения ключей с IP-сетями [30,31]. Отметим, что этот проект финансируется американским оборонным агентством DARPA (Defense Advanced Research Projects Agency). К настоящему времени уже создана экспериментальная квантовая сеть между указанными выше организациями (максимальное расстояние между которыми 19,6 км), состоящая из десяти узлов квантового распределения ключей [32].

При передаче ключа по протоколам BB84 и B92 между BBN Technologies и Гарвардским университетом (около 10 км) достигнут минимальный уровень ошибок в 3%. Отметим, что это значительно меньше тех 25%, которые внес бы подслушивающий агент при стратегии перехвата всех пересылаемых фотонов в протоколе BB84. Таким образом, защищенный против атаки полного перехвата протокол BB84 уже реализован практически. Однако скорость передачи невысока – около 1000 бит/с, что обусловлено в первую очередь несовершенством излучателей и детекторов фотонов. Тем не менее, технологическое оборудование для КПРК постоянно совершенствуется, поэтому интегрированные сети, архитектура которых предложена в [30-32], видимо, уже близки к внедрению в коммерческую эксплуатацию.

Еще один проект американской фирмы «MagiQ» [33] направлен на создание первого коммерческого варианта квантовой оптоволоконной криптосистемы. Недавно фирма анонсировала такую систему, реализующую протокол BB84 между двумя удаленными пользователями и действующую на расстоянии до 120 км.

9. Выводы. Квантовая криптография представляет собой новое направление в развитии средств конфиденциальной передачи информации и включает в себя несколько разделов, основным из которых является распределение секретных ключей посредством передачи квантовых состояний микрочастиц.

В настоящее время разработаны квантовые криптографические системы, предназначенные для распределения секретных ключей между удаленными легитимными пользователями. Использование таких систем позволяет в принципе построить систему передачи шифрованных сообщений, которые не могут быть дешифрованы третьими лицами (шифрование в режиме одноразового блокнота с помощью ключа, распределенного методами квантовой криптографии). Квантовые криптосистемы также могут использоваться, например, для распределения ключей, с помощью которых шифруется поток обмена данными в виртуальных частных сетях.

Квантовая криптография позволяет обеспечить секретность распределенного ключа, так как подслушивающий агент должен производить измерения состояний передаваемых кубитов, а любое измерение, если оно дает информацию о передаваемых состояниях, неизбежно приводит к их возмущению, что позволяет обнаружить любые попытки подслушивания в канале связи. Отметим, что законы квантовой физики позволяют не только обнаружить возмущение состояний, но и связать уровень ошибок при измерениях у легитимного пользователя с количеством информации, которое может быть получено подслушивающим агентом. Следовательно, легитимные пользователи после передачи ключа могут оценить уровень ошибок и принять решение: производить процедуру усиления секретности, уменьшающую имеющееся у подслушивающего агента небольшое количество информации о ключе, если уровень ошибок мал, или вообще отказаться от распределенного ключа и повторить весь протокол сначала, если уровень ошибок велик, т.е. подслушивающий агент мог получить неприемлемо большое количество информации.

Таким образом, методы одного из направлений квантовой криптографии направлены на решения центральной криптографической проблемы – задачи распределения секретных ключей. В сочетании с кодом Вернама для шифрования сообщений и классическими методами аутентификации, квантовые протоколы распределения ключей способны обеспечить более высокий уровень безопасности, чем любая классическая криптографическая схема.

В настоящее время разрабатываются и квантовые протоколы защищенной прямой связи (протоколы передачи секретных сообщений посредством квантовых состояний без шифрования с помощью предварительно распределенного ключа), а также методы аутентификации квантовых сообщений и квантовой цифровой подписи. В отличие от квантовых криптосистем для распределения ключей, перечисленные направления квантовой криптографии пока находятся на начальном этапе развития. Так, даже экспериментальных систем квантовой защищенной прямой связи, обеспечивающих приемлемую скорость передачи, пока не существует. В связи с этим отметим, что и существующие квантовые системы распределения ключей содержат достаточно сложные оптоволоконные, электронные и программные компоненты, работа с которыми на сегодня представляет собой, скорее, проведение сложного научного эксперимента, чем практическую деятельность с использованием общеупотребительного и стандартного оборудования [34]. Таким образом, для практического использования квантовых криптографических систем в существующей инфраструктуре сетей передачи данных необходимо решить еще ряд задач как практического, так и теоретического характера.

В заключение выделим актуальные на сегодня теоретические задачи квантовой криптографии:

1) Разработка высокоэффективных квантовых протоколов распределения ключей, протоколов прямой связи между парой абонентов и между отдельными абонентами и центром, защищенных не только от атак, реализуемых с современными технологиями, но и от тех, которые существуют пока только «в теории», так как требуют для своей реализации несуществующего оборудования, например, квантовых компьютеров. Такие атаки, невозможные сегодня, вполне могут стать возможными в недалеком будущем, что обуславливает актуальность опережающей разработки протоколов, защищенных от этих атак.
2) Имитационное моделирование сложных квантовых протоколов с учетом различных моделей помех в квантовом канале и различных стратегий атак, что позволит выяснить трудно поддающиеся анализу особенности этих протоколов.
3) Анализ зависимости количества информации, которую может получить подслушивающий агент, от уровня вносимых им ошибок, что позволит сравнить уровни секретности различных протоколов. Отметим, что для нескольких простых КПРК такой анализ уже выполнен, однако для более сложных (например, BB84 с доминантным базисом), а также квантовых протоколов защищенной прямой связи, таких исследований пока не проводилось.
4) Разработка эффективных методов коррекции ошибок, возникающих в квантовом канале с шумом. Эта задача тесно связана с задачей исправления ошибок при квантовых вычислениях.
5) Разработка программного обеспечения, управляющего всеми операциями по передаче ключа через квантовый канал. Сюда входят: первичная генерация и передача фотонов, исправления ошибок в полученной битовой последовательности, оценка утечки информации к подслушивающему агенту, процедура усиления секретности и формирования итогового ключа. Отметим, что для нескольких КПРК такое программное обеспечение уже создано в рамках вышеупомянутых проектов [32,33].
6) Разработка общей архитектуры квантовой сети защищенной передачи данных – архитектуры «квантового Интернета».

Литература

1. *Столлингс В*. Криптография и защита сетей: принципы и практика, – 2-е изд.: Пер. с англ. – М.: ИД «Вильямс», 2001. – 672 с.
2. *Баумейстер Д., Экерт А., Цайлингер А*. Физика квантовой информации. – М.: Постмаркет, 2002.- 376 с.
3. *Lomonaco S. J., Jr*. A Quick Glance at Quantum Cryptography // Cryptologia. – V. 23, №1. – 1999. – P. 1-41. (Preprint: http://www.arxiv.org/abs/quant-ph/9811056).
4. *Баричев С.Г, Серов Р.Е*. Основы современной криптографии: Учебное пособие. – М.: Горячая линия. – Телеком, 2002. – 152 с.
5. *Dusek M., Lutkenhaus N., Hendrych M.* Quantum cryptography. – Preprint: http://www.arxiv.org/abs/quant-ph/0601207. – 2006. – 61 p.
6. *Asin A., Gisin N., Scarani V*. Security bounds in Quantum Cryptography using d-level systems // Quantum Information and Computation. – V. 3, № 6, 2003. – P. 563-581. (Preprint: http://www.arxiv.org/abs/quant-ph/0303009).

7. *Bruss D.*, *Lutkenhaus N.* Quantum Key Distribution: from Principles to Practicalities // Applied Algebra, Algebraic Algorithms, and Error Correcting Codes. – V. 10, 2000. – P. 383-399. (Preprint: http://www.arxiv.org/abs/quant-ph/9901061).
8. *Barnum H., Crepeau C., Gottesman D., Smith A., Tapp A*. Authentication of Quantum Messages // Proc. 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02). – IEEE Press, 2002. – P. 449-458. (Preprint: http://www.arxiv.org/abs/quant-ph/0205128).
9. *Lu X., Feng D.-G.* Quantum Digital Signature Based on Quantum One-way Functions. – Preprint: http://www.arxiv.org/abs/quant-ph/0403046, 2004. – 10 p.
10. *Lee H., Lim J., Yang H*. Quantum Direct Communication with Authentication. – Preprint: http://www.arxiv.org/abs/quant-ph/0512051, 2005. – 9 p.
11. *Hong C., Kim J, Lee H., Yang H*. Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping. – Preprint: http://www.arxiv.org/abs/quant-ph/0601194, 2006. – 6 p.
12. *Берман Г.П., Дулен Г.Д., Майньери Р., Цифринович В.И.* Введение в квантовые компьютеры. – М. – Ижевск: Ин-т комп. иссл.; НИЦ «РХД», 2004,188 с.
13. *Lutkenhaus N., Jahma M*. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack // // New Journal of Physics. – V. 4, 2002. – P. 44.1–44.9.
14. *Bennett C. H*. Quantum cryptography using any two nonorthogonal states // Physical Review Letters. – V. 68, №21. – 1992. – P. 3121-3124.
15. *Lo H*.-K., Chau H.F., Ardehali M. Efficient Quantum Key Distribution Scheme And Proof of Its Unconditional Security // Journal of Cryptology. – V. 18, №2, 2005. – P. 133-165. (Preprint: http://www.arxiv.org/abs/quant-ph/0011056)
16. *Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H.* Quantum key distribution over 67 km with a plug&play system // New Journal of Physics. – V. 4, 2002. – P. 41.1–41.8.
17. *Hughes R. J., Nordholt J. E., Derkacs D., Peterson C. G.* Practical free-space quantum key distribution over 10 km in daylight and at night // New Journal of Physics. – V. 4, 2002. – P. 43.1-43.14.
18. *Ekert A.* Quantum cryptography based on Bell's theorem // Physical Review Letters. – V. 67, №6, 1991. – P. 661-663.
19. *Kofler J., Paterek T., Brukner C*. Experimenter's Freedom in Bell's Theorem and Quantum Cryptography. – Preprint: http://www.arxiv.org/abs/quant-ph/0510167, 2005. – 7 p.
20. Svozil K. Feasibility of the interlock protocol against man-in-the-middle attacks on quantum cryptography. – Preprint: http://www.arxiv.org/abs/quant-ph/0501062, 2005. – 6 p.
21. *Yuen H.P., Nair R., Corndorf E., Kanter G.S., Kumar P.* On the security of $\alpha\eta$: Response to 'Some attacks on quantum-based cryptographic protocols'. – Preprint: http://www.arxiv.org/abs/quant-ph/0509091. – 2005. – 24 p.
22. *Bostroem K., Felbinger T*. Deterministic Secure Direct Communication Using Entanglement // Physical Review Letters. – V. 89. – 2002. – P. 187902.
23. *Wojcik A.* Eavesdropping on the "ping-pong" quantum communication protocol // Physical Review Letters. – V. 90. – 2003. – P. 157901.
24. *Gao T., Yan F.L., Wang Z.X.* Controlled quantum teleportation and secure direct communication. – Preprint: http://www.arxiv.org/abs/quant-ph/0403155, 2004. – 4 p.
25. *Wang C., Deng F.G. Long G.L.* Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. – Preprint: http://www.arxiv.org/abs/quant-ph/0601147, 2006. – 4 p.
26. *Gao T., Yan F.L., Wang Z.X.* A Simultaneous Quantum Secure Direct Communication Scheme between the Central Party and Other *M* Parties. – Preprint: http://www.arxiv.org/abs/quant-ph/0509033, 2005. – 4 p.
27. *Wang J., Zhang Q., Tang C*. Efficient multiparty quantum secret sharing of secure direct communication. – Preprint: http://www.arxiv.org/abs/quant-ph/0510212, 2005. – 6 p.
28. *Zhang Z., Li Y., Man Z.* Multiparty Quantum Secret Sharing. – Preprint: http://www.arxiv.org/abs/quant-ph/0412203, 2004. – 6 p.
29. *Kak S*. A Three-Stage Quantum Cryptography Protocol. – Preprint: http://www.arxiv.org/abs/quant-ph/0503027, 2005. – 5 p.
30. *Elliott C*. Building the Quantum Network // New Journal of Physics. – V. 4, 2002. – P. 46.1-46.12.
31. *Aoun B., Tarifi M*. Quantum Networks. – Preprint: http://www.arxiv.org/abs/quant-ph/0401076, 2004. – 65 p.
32. *Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., Yeh H*. Current status of the DARPA Quantum Network. – Preprint: http://www.arxiv.org/abs/quant-ph/0503058, 2005. – 12 p.
33. http://www.magiqtech.com/
34. *Молотков С.Н.* Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах // Успехи физических наук. – Т. 176. – № 7, 2006. – С. 777-788.