УДК 621.396

05.00.00 Технические науки

КВАНТОВЫЕ СИСТЕМЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ: ФИЗИЧЕСКИЕ ОСНОВЫ, ПРОТОКОЛЫ, ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ[1]

Лойко Валерий Иванович
Заслуженный деятель науки РФ, доктор технических наук, профессор
Кубанский государственный аграрный университет, Краснодар, Россия

Хисамов Франгиз Гильфанетдинович
Доктор технических наук, профессор
Кубанский институт информзащиты, Краснодар, Россия

Бобылев Михаил Владимирович
Оператор научной роты
Краснодарское высшее военное училище, Краснодар, Россия

Власов Константин Евгеньевич
Оператор научной роты
Краснодарское высшее военное училище, Краснодар, Россия

Целью данной работы является анализ разработанных систем квантового распределения ключей, возможности применения этих систем, анализ физических основ поведения квантовых объектов используемых в системах квантовой криптографии и протоколов распределения квантовых ключей

Ключевые слова: КРИПТОГРАФИЯ, КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА

UDC 621.396

Technical sciences

QUANTUM DISTRIBUTION SYSTEMS: PHYSICAL BASES, PROTOCOLS, OPPORTUNITIES OF THEIR IMPLEMENTATION

Loyko Valeriy Ivanovich
Honored science worker of the Russian Federation, Dr.Sci.Tech., professor
Kuban state agrarian university, Krasnodar, Russia

Khisamov Frangiz Gilfanetdinovich
Dr.Sci.Tech., professor
Kuban Institute of Informprotection, Krasnodar, Russia

Bobilev Mihail Vladimirovich
Operator of the Scientific department
Krasnodar high military academy, Krasnodar, Russia

Vlasov Konstantin Evgenievich
Operator of the Scientific department
Krasnodar high military academy, Krasnodar, Russia

The aim of the article is to analyze existing quantum distribution systems, their facilities, physical bases of quantum objects behavior used in quantum distribution systems and protocols of quantum keys distribution

Keywords: CRYPTOGRAPHY, QUANTUM KEY DISTRIBUTION

Введение

За границей активно ведутся работы в области создания компьютерных систем, систем связи и защиты информации на основе использования квантовых технологий. Данные системы по своим параметрам количественно и качественно превосходят существующие классические системы настолько, что дальнейшее расширение их практического применения приведет к существенному изменению форм,

[1] Работа выполнена при финансовой поддержке РФФИ, проект № 16-06-00114А

методов и способов проведения атак на инфокоммуникационные системы и сети и противодействия им.

При применении квантовых методов распределения ключа потенциально возможна мгновенная, скрытная, бескомпроматная, помехозащищенная передача информации на любое расстояние между предварительно разнесенными запутанными квантовыми системами, вне зависимости от разделяющей их физической среды;

Использование квантовых криптографических систем (ККС) выработки и распределения ключей в волоконно-оптических и атмосферно-оптических системах передачи специальной информации обеспечит возможность быстрой, полностью автоматической (без привлечения и участия персонала) смены ключей в распределенных системах высокоскоростного шифрования, характеризующуюся высокой скрытностью ключевого обмена и отсутствием записанных на физические носители ключевой информации, а также гарантированной способностью к обнаружению попыток перехвата.

Появление квантового компьютера у противника представляет реальную угрозу всем действующим системам защищенной связи, использующих криптографические системы с фиксированной длинной ключа, в силу качественного и количественного превосходства квантовых компьютеров над классическими, для защиты от атак, с использованием которых рассчитаны существующие системы.

Уже наблюдаются определенные тенденции в этом направлении, в частности, в США ККС применяются для защиты каналов связи и передачи данных между Пентагоном и Белым домом, а квантовые компьютеры активно закупаются для решения специальных задач АНБ, а также военно-промышленного комплекса. Агентство DARPA ежегодно увеличивает финансирование исследований в области разработки квантовых технологий в интересах вооруженных сил США.

Образцы ККС доступны в открытой продаже и уже ввезены на территорию России. Однако, современные ККС представляют собой сложные программно-аппаратные комплексы, что позволяет иностранным производителям реализовать в них широкий спектр недокументированных возможностей.

Этим обуславливается необходимость разработки и внедрения ККС отечественного производства в сети связи специального назначения Минобороны России и других ведомств, обеспечивающих национальную безопасность. Теоретические исследования в этом направлении проводятся несколькими гражданскими и военными научными коллективами.

К настоящему времени создан и находится в опытной эксплуатации опытный образец ККС выработки и распределения ключей. Существенным ограничивающим фактором изготовленного образца является возможность его применения только внутри контролируемой зоны (для внутриобъектового использования).

Физические основы систем квантовой криптографии

Под квантовыми системами (или квантовыми объектами) обычно подразумевают объекты микромира, например, электроны, атомы, молекулы и их совокупности, световые пучки, одиночные фотоны и т.д. Принципиальной особенностью квантовых систем является их статистический характер в отношении результатов всевозможных измерений. Приготовленные тождественным образом квантовые системы демонстрируют в общем случае, различающиеся результаты измерений. Для описания этого факта в квантовой теории вводят понятие состояния квантовой системы.

Состояние квантовой системы - это список возможных результатов измерений над этой системой [1, с. 35-50].

В квантовой теории рассматривают два типа состояний квантовых систем - чистые и смешанные.

Чистые состояния описывают квантовые системы, которые независимы от всех остальных окружающих их квантовых объектов.

Смешанное состояние отдельной квантовой системы возникает, когда такая независимость отсутствует. (Смешанные состояния в данной работе не будут рассматриваться.)

Более строго, если состояние квантовой системы описывается некоторым нормированным вектором $|\psi\rangle$ конечномерного гильбертова пространства над полем комплексных чисел C, то говорят, что квантовая система находится в чистом состоянии [1, с. 35-50].

Таким образом, с математической точки зрения, чистое состояние квантовой системы задается вектором состояния (по-другому называемого волновой функцией), который принято записывать в обозначениях Дирака как кет-вектор $|\psi\rangle$. Этот вектор имеет норму 1 и является элементом многомерного комплексного евклидова пространства, который именуется гильбертовым пространством. Размерность D гильбертова пространства задает важный параметр - число независимых состояний (уровней) квантовой системы.

Далее чистые состояния квантовых систем будем называть просто состояниями.

В принципе любой вектор $|\psi\rangle$ гильбертова пространства с нормой, равной единице, представляет собой возможное состояние квантовой системы. Используя произвольный ортонормированный базис $\{|k\rangle|k = 1,2,\dots,D\}$ гильбертова пространства можно представить любой вектор $|\psi\rangle$ в виде суперпозиции (линейной комбинации) базисных векторов:

$$|\psi\rangle = \sum_{k=1}^{D} c_k|k\rangle, c_k \in C, k = 1,2,\dots,D.$$

Существует бесконечное число ортонормированных базисов и, следовательно, бесконечное число различных представлений любого вектора состояний. Смысл выбора того или иного ортонормированного базиса $\{|k\rangle | k = 1,2,\ldots,D\}$ и коэффициентов $\{c_k | k = 1,2,\ldots,D\}$ разложения состояния $|\psi\rangle$, а вместе с тем и суть квантовой теории, определяется в процедуре квантового эксперимента и его неотъемлемой части - измерении.

Обратим теперь внимание на очень важное понятие квантовой информатики (раздела квантовой теории) - кубит (quantum bit = qubit) [2, с. 353 - 356].

Кубит - это фундаментальное понятие в области квантовых вычислений и квантовой информации, имеющее смысл единицы квантовой информации. Кубит реализуется на основе двухуровневых квантовых систем, то есть квантовых систем имеющих два независимых состояния Естественными двухуровневыми квантовыми системами являются, например, отдельные электроны в атомах, ядра атомов, протоны с абсолютным значением спина, равным S. Состояния всех этих систем описываются двухкомпонентными спиновыми волновыми функциями, представляющими собой векторы состояния в двухмерном гильбертовом пространстве C^2.

Кубиты в квантовой области являются «аналогами» таких классических единиц, как биты. Напомним, что бит - это фундаментальное понятие в области классических вычислений и классической информации, имеющее смысл единицы классической информации. Аналогично классическому биту, который может находиться в состоянии 0 или 1, кубит также имеет состояния. Двумя возможными состояниями кубита являются $|0\rangle$ и $|1\rangle$, соответствующие состояниям 0 и 1 классического бита. Однако главным различием между битами и кубитами является то, что кубит может

находиться в состоянии, отличном от $|0\rangle$ или $|1\rangle$. И таких состояний бесконечно много. Состояниями кубита являются векторы двухмерного гильбертова пространства C^2 над полем комплексных чисел C вида $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где α, $\beta \in C$, $|\alpha|^2 + |\beta|^2 = 1$, $|\alpha|$ и $|\beta|$ - модули комплексных чисел α и β ;и $\{|0\rangle,\} |1\rangle$ - ортонормированный базис пространства C^2. Векторы $|0\rangle$ и $|1\rangle$ называются состояниями вычислительного базиса в случае одного кубита, и при этом вектор $|\psi\rangle$ является суперпозицией (линейной комбинацией) векторов $|0\rangle$и$|1\rangle$.

Обратим внимание на еще одно очень существенное отличие кубита от бита, связанное с выявлением их состояний путем измерения.

Мы можем измерить бит, чтобы определить, находится ли он в состоянии 0 или 1. Например, компьютеры делают это каждый раз, когда считывают содержимое своей памяти [4, с 264 – 273].

В случае измерения кубита в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ситуация совершенно иная.

Из квантовой механики следует, что само состояние $|\psi\rangle$ кубита не наблюдаемо, то есть путем измерения невозможно определить состояние $|\psi\rangle$. Путем измерения можно получить гораздо более ограниченную информацию: при измерении кубита, находящегося в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ мы получаем либо результат $|0\rangle$ с вероятностью, либо $|1\rangle$ с вероятностью $|\beta|^2$. Этот разрыв между ненаблюдаемым состоянием кубита и доступными нам наблюдениями, то есть отсутствие между ними привычного прямого соответствия, затрудняет интуитивное понимание поведения квантовых систем. Однако существует непрямое соответствие: состояния кубита можно менять тем или иным способом, в результате чего данные измерений будут существенно зависеть от различных свойств исходного состояния. Можно сказать, что в состоянии кубита природа

прячет массу скрытой информации. Но, несмотря на это, измерение кубита всегда дает только $|0\rangle$ или $|1\rangle$ с некоторой вероятностью [2, с. 353 - 356].

Под квантовой криптографией, в широком смысле, понимается научно- практическое направление, предметом которого является решение задач криптографической защиты информации с привлечением ресурсов квантовой физики.

Под квантовой связью понимается научно-практическое направление, предметом которого является решение задач хранения, обработки и передачи информации с привлечением ресурсов квантовой физики.

Примерами ресурсов квантовой физики, используемых в квантовой криптографии и квантовой связи служат:

1. Квантовый ресурс несепарабельных состояний;
2. Квантовый ресурс, основанный на невозможности клонирования неизвестного состояния квантового объекта. [1, с. 35-50]

Квантовый ресурс невозможности клонирования неизвестного состояния квантового объекта

Одним из основных направлений разработки и исследований свойств квантовых криптографических систем является направление, в котором защита передаваемой информации обеспечивается фундаментальной теоремой о невозможности копирования (клонирования) неизвестного состояния квантового объекта [2, с. 353 - 356].

Как известно, эволюция состояния физической системы в квантовой механике описывается линейным унитарным преобразованием. Оказывается, свойство унитарности не позволяет по неизвестному исходному квантовому состоянию создать его точную копию. Доказательство невозможности копирования впервые было получено Вуттерсом и Зуреком [3, с. 3229 – 3239]. Приведем формулировку этой теоремы

Теорема. Не существует унитарной матрицы U, такой, что справедливо равенство

$$U(x \otimes |0\rangle) = x \otimes x$$

Для произвольного нормированного вектора $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ из гильбертова пространства C^2 размерности 2, где C - поле комплексных чисел, $x_1, x_2 \in C, x_1\overline{x_1} + x_2\overline{x_2} = 1$, $\otimes$- знак операции тензорного умножения.

Принцип невозможности различения двух не ортогональных квантовых состояний физических носителей информации реализован в ряде протоколах, описания основных из которых представлены ниже.

Квантовые криптографические протоколы генерации и распределения ключей.

Протокол BB84

В 1984 году Беннет (фирма IBM) и Брассард (Монреальский университет) предположили, что квантовые состояния фотонов могут быть использованы в криптографии для получения надежно защищенного канала. Они предложили простую схему квантового распределения ключей, названную ими BB84. Эта схема использует квантовый канал, по которому пользователи (отправитель и получатель) обмениваются сообщениями, передавая их в виде поляризованных фотонов. Квантовый канал может представлять собой, например, просто оптоволокно в совокупности с оконечными устройствами, которые дают возможность генерировать и передавать отдельные фотоны, а также производить некоторые измерения их состояний.

Противник в случае перехвата может попытаться производить измерение этих фотонов, но, как сказано выше, он не может сделать это, не внося в них искажений. Отправитель и получатель используют открытый классический канал для обсуждения и сравнения сигналов, передаваемых по

квантовому каналу, проверяя их на возможность перехвата. Если не выявлено деструктивное воздействие на квантовый канал, пользователи могут извлечь из полученных данных информацию, которая надежно распределена, случайна и секретна, несмотря на преднамеренные технические ухищрения и вычислительные возможности, которыми располагает противник [3, с. 3229 – 3239].

Основные шаги протокола BB84 можно описать следующим образом.

Отправитель с помощью генератора случайных чисел ГСЧ1 формирует случайную последовательность двоичных битов. В процессе передачи секретного ключа, отправитель посылает получателю данную последовательность, кодируя каждый бит в квантовом состоянии фотона. При этом у него есть возможность закодировать каждый двоичный бит одним из двух возможных способов, в одном из двух различных ортонормированных базисах: нормальном базисе - где двоичный ноль кодируется горизонтальной поляризацией фотона $0 \rightarrow |\backslash\rangle$, а двоичная единица - вертикальной $1 \rightarrow |/\rangle$,или в диагональном - где двоичный ноль кодируется леводиагональной поляризацией фотона $0 \rightarrow |\backslash\rangle$, а двоичная единица – право диагональной$1 \rightarrow |/\rangle$. Конкретный вид базиса выбирается для каждого элемента последовательности с помощью ГСЧ2, при этом двоичному нулю соответствует нормальный базис, а единице - диагональный. Таким образом, получается последовательность фотонов с произвольной (0^0, 90^0 или 45^0 ,135^0) поляризацией, которую отправитель посылает получателю по оптическому каналу связи:

|	/	-	\	-	-	/	\	|

Получатель измеряет состояния фотонов, выбирая на каждом шаге один из возможных базисов с помощью ГСЧ3 при этом двоичному нулю соответствует нормальный базис «+», а единице - диагональный «х». [4, с 264 – 273]

+	+	x	x	+	x	x	x	+

Измерение состояния фотона получателем приводит к тому, что если для определения вида поляризации фотона был выбран тот же базис что и при его кодировании, то получатель с вероятностью 1 определит правильное значение поляризации, если же базис был выбран неверно, то в качестве результата измерения будет выступать один из векторов выбранного базиса с вероятностью S. В результате получатель получает следующую последовательность β:

|	-	/	\	-	/	/	/	|

После того, как все биты переданы, получатель сообщает отправителю по открытому каналу, какие базисы он использовал для раскодирования фотонов при приеме. Отправитель сообщает получателю по тому же открытому каналу, какие базисы он выбрал правильно:

∨			∨	∨		∨		∨

Биты, полученные при совпавших измерениях, стороны будут использовать в качестве ключа, все остальные будут отброшены:

1			\	-		/		|
1			1	0		0		1

В среднем отправитель и получатель будут иметь примерно 50% совпадений базисов, т.е. для ключа будет использована примерно половина передаваемых битов. Примерно в половине случаев он будет использовать ложные базисы [1, с. 35-50].

Всякое подслушивание в квантовом канале увеличивает число ошибок передачи, что легко может быть обнаружено легальными пользователями, если они сравнят по открытому каналу некоторое количество контрольных битов ключа. В этом случае легальные пользователи прекращают сеанс закрытой связи, и ключ объявляется недействительным [4, с 264 – 273].

Протокол B92

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

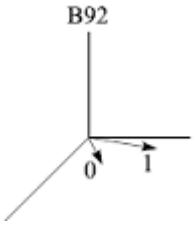

Рисунок 1 – Поляризационные состояния, используемые в протоколе B92

Станция Алиса посылает фотоны, поляризованные в направлениях 0 и $+45^0$, представляющие нули и единицы. Причем последовательность фотонов, посылаемая станцией Алиса, случайно ориентирована. Станция Боб принимает фотоны через фильтры ориентированные под углом 90^0 и 135^0 (-45^0). При этом если фотон, переданный станцией Алиса, будет анализирован станцией Боб при помощи фильтра ориентированного под углом 90^0 по отношению к передаваемому фотону, то фотон не пройдет через фильтр. Если же этот угол составит 45^0, то фотон пройдет через фильтр с вероятностью 0,5 [1, с. 35-50].

Для определения поляризации станция Боб анализирует принимаемые ей фотоны, используя выбранный случайным образом один из двух неортогональных базисов «+» или «×». Если станция Боб анализирует посланный фотон фильтром с ортогональным направлением поляризации, то он не может точно определить, какое значение данный фотон представляет: 1, соответствующее фотону, который не проходит, или 0, соответствующее фотону, который не проходит с вероятностью 0,5. Если же

направления поляризации между посланным фотоном и фильтром, неортогональны, то станция Боб может определить, что принят фотон соответствующий 0. Если фотон был принят удачно, то очередной бит ключа кодируется 0 (если фотон был принят фильтром, ориентированным под углом 135^0), либо 1 (если фотон был принят фильтром, ориентированным по направлению H) (таблица 1)

Таблица 1 – Формирование квантового ключа по протоколу B92

Двоичный сигнал станции Алиса	1	0	1	0
Поляризационный код станции Алиса	↗	↕	↗	↕
Поляризационный код станции Боб	↘	↘	↔	↔
Двоичный код станции Боб	0	0	1	1
Результат, полученный станцией Боб	–	–	+	–

В первой и четвертой колонке поляризации при передаче и приеме ортогональны и результат детектирования будет отсутствовать. В колонках 2 и 3 коды двоичных разрядов совпадают и поляризации не ортогональны. По этой причине с вероятностью 50% может быть положительный результат в любом из этих случаев (и даже в обоих). В таблице предполагается, что успешное детектирование фотона происходит для случая, представленного в колонке 3. Именно этот бит становится первым битом общего секретного ключа передатчика и приемника. Отсюда минимальное количество фотонов, которое может быть принято станцией Боб

$$n = \frac{1}{\cdot}.$$

То есть в результате передачи такого ключа, около 25% фотонов будут правильно детектированы станцией Боб.

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

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

Протокол E91

Протокол E91 отличается от протокола BB84 тем, что биты ключа получаются из фундаментально случайного процесса, основанного на свойствах запутанных квантовых состояний.

Основные шаги протокола E91 можно описать следующим образом.

Центр (допускается, что он может совпадать с одним из абонентов) генерирует N пар фотонов в состоянии Белла $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ (которое может быть записано и в другом виде $\frac{|s_1 s_1\rangle+|s_2 s_2\rangle}{\sqrt{2}}$, где $s_1 = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $s_2 = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ и посылает их абонентам A и B, которые независимо измеряют полученные ими фотоны в случайно выбранных каждым из абонентов базисах (нормальном или диагональном). При этом, если в результате измерения были получены состояния $|-\rangle$ или $|\backslash\rangle$, то принимается решение что значение двоичного бита в соответствующем

такте равно 0, если же в результате измерения были получены состояния $|1\rangle$ или $|/\rangle$, то принимается решение что значение двоичного бита в соответствующем такте равно 1. После этого абоненты обмениваются друг с другом информацией об использованных ими для измерения базисах по открытому каналу. При этом в качестве элементов общего ключа принимаются биты, выработанные в тех тактах, в которых абоненты А и В использовали для измерения одинаковые базисы, т.к. при совпадении измерительных базисов абоненты гарантированно получают одинаковые значения измеряемых параметров, вследствие того, что измеряемые ими пары фотонов находятся в вышеуказанном несепарабельном состоянии Белла.

Состояние работ

Активные исследования в области квантовой криптографии ведут IBM, GAP-Optique, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт, молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны.

Квантовая криптография как сегмент рынка только начинает формироваться, и здесь пока на равных могут играть и мировые компьютерные корпорации, и небольшие начинающие компании.

В IBM продолжаются фундаментальные исследования в области квантовых вычислений, начатые группой Чарльза Беннетта. Ими занимается принадлежащая корпорации лаборатория Almaden Research Center. О практических достижениях IBM в квантовой криптографии известно немногое - эти работы мало рекламируются.

Исследователям из Лос-Аламоса удалось передать фотонный ключ по оптоволокну на расстояние 48 км со скоростью в несколько десятков

килобитов в секунду. Этого достаточно, чтобы соединить между собой отделения банка или правительственные учреждения.

Созданная при участии Женевского университета компания GAP Optique под руководством Николаса Гисина совмещает теоретические исследования с практической деятельностью. Специалистам этой фирмы удалось передать ключ на расстояние 67 км из Женевы в Лозанну с помощью почти промышленного образца аппаратуры. Этот рекорд был побит корпорацией Mitsubishi Electric, передавшей квантовый ключ на расстояние 87 км, правда, на скорости в 1 байт/с.

Исследования в области квантовой криптографии ведутся и в европейском исследовательском центре Toshiba Research Europe Limited (TREL), расположенном в Кембридже (Великобритания). Отчасти они спонсируются английским правительством; в них участвуют сотрудники Кембриджского университета и Империал-колледжа в Лондоне. Сейчас они могут передавать фотоны на расстояние до 100 км. Таким образом, технология может использоваться только в пределах одного города. Есть надежда, что вскоре будут выпущены коммерческие продукты.

Два года назад доктор Эндрю Шилдс и его коллеги из TREL и Кембриджского университета создали диод, способный испускать единичные фотоны. В основе нового светодиода лежит "квантовая точка" - миниатюрный кусочек полупроводникового материала диаметром 15 нм и толщиной 5 нм, который может при подаче на него тока захватывать лишь по одной паре электронов и дырок. Рекомбинация одного электрона с одной дыркой приводит к испусканию фотона. При этом ток, подаваемый на "квантовую точку" подбирается так, чтобы в рекомбинации участвовала только одна пара электрон - дырка. Но даже если новый светодиод испустит два фотона, они будут характеризоваться разной длиной волны, что позволяет отсечь лишнюю частицу при помощи фильтра. Обычные светодиоды и лазеры испускают фотоны группами, что теоретически дает

возможность доступа к определению характеристик отдельных фотонов, в то время как другие фотоны продолжат свой путь в неизменном виде [2, с. 353 - 356].

Чтобы обойти трудность, связанную с созданием источников отдельных фотонов, Фредерик Гроссан из Института оптики в Орсэ (Франция) разработал методику, позволяющую шифровать сообщения с помощью импульсов, состоящих из нескольких сот фотонов. На ее безопасность не влияет даже ослабление сигнала на больших расстояниях. Гроссан отказался от отдельных квантов света и предложил усреднять значения амплитуды и фазы электрического поля группы фотонов. Как и поляризация отдельного фотона, эти переменные связаны друг с другом принципом неопределенности. Однако в отличие от поляризации фотона, принимающей одно из двух значений вдоль каждого ортогонального направления, эти переменные могут принимать непрерывный ряд значений.

Подобные исследования в квантовой криптографии ведутся одновременно несколькими группами. Но только группе Гроссана удалось продемонстрировать практические перспективы, а также создать аппаратуру и ПО для работы с квантовым ключом. При измерении непрерывного ряда значений уже не обязательно регистрировать каждый фотон. В ходе экспериментальной демонстрации удалось передать зашифрованные данные со скоростью 75 кбит/с - при том, что более половины фотонов терялось.

Такая схема потенциально обладает намного большим быстродействием, чем схемы со счетом единичных фотонов. Это делает ее, по мнению разработчиков, весьма привлекательной для быстрой передачи секретных данных на расстояния менее 15 км. Перспективы ее использования на больших дистанциях требуют дополнительного изучения.

В исследования высокоскоростной квантовой криптографии углубилась и корпорация NEC в лице своего института NEC Research

Institute. Над прототипами коммерческих систем квантовой криптографии, действующих по оптоволоконным линиям связи, работает подразделение телекоммуникационного гиганта Verizon Communications - BBN Technologies.

Команда Северо-Западного университета (США) сотрудничает с Telcordia Technologies и BBN Technologies, стараясь довести технологию до коммерческого применения. Им удалось передать зашифрованные данные по оптоволокну со скоростью 250 Мбит/с. Теперь стоит задача доказать, что схема позволяет сигналам проходить сквозь оптические усилители. В этом случае метод можно будет использовать не только в специальных оптоволоконных линиях связи между двумя точками, но и в более широких сетях. Еще эта команда работает над тем, чтобы достичь скоростей порядка 2,5 Гбит/с. Исследования Северо-Западного университета в области квантовой криптографии финансируются DARPA - оборонным ведомством США.

Министерством обороны Великобритании поддерживается исследовательская корпорация QinetiQ, активно совершенствующая технологию квантовой шифрации. Эта компания появилась на свет в результате деления британского агентства DERA (Defence Evaluation and Research Agency) в 2001 г., вобрав в себя все неядерные оборонные исследования. О своих достижениях она широкой публике пока не сообщает.

К исследованиям присоединилось и несколько молодых компаний, в том числе швейцарская Id Quantique (www.idquantique.com), представившая коммерческую систему квантовой криптографии, и MagiQ Technologies (www.magiqtech.com) из Нью-Йорка, выпустившая прототип коммерческой квантовой криптотехнологии собственной разработки. MagiQ Technologies была создана в 1999 г. на средства крупных финансовых институтов. Помимо собственных сотрудников с ней

взаимодействуют научные работники из целого ряда университетов США, Канады, Великобритании и Германии. Вице-президентом MagiQ является Алексей Трифонов, в 2000 г. защитивший докторскую диссертацию в Петербургском университете. Год назад MagiQ получила 7 млн. долл. от нескольких инвесторов, включая основателя Amazon.com Джеффа Безоса.

В продукте MagiQ средство для распределения ключей (quantum key distribution, QKD) названо Navajo - по имени индейцев Навахо, язык которых во время Второй мировой войны американцы использовали для передачи секретных сообщений, поскольку за пределами США его никто не знал. Navajo способен в реальном времени генерировать и распространять ключи средствами квантовых технологий и предназначен для обеспечения защиты от внутренних и внешних злоумышленников. Продукт Navajo находится в состоянии бета-тестирования и станет коммерчески доступным в конце года. Несколько коммуникационных компаний тестируют Navajo в своих сетях.

Заключение

Дальнейшее развитие систем квантового распределения ключа приведет к созданию сетей связи с более высоким уровнем защиты информации. Данные сети найдут применение как в гражданском секторе экономики, так и в тех организациях, деятельность которых связана с обеспечением государственной безопасности. Исходя из этого отечественные разработки в этой сфере позволят повысит уровень обороноспособности страны. Системы квантового распределения ключей – это сложные программно-аппаратные комплексы, в которые могут быть заложены недокументированные возможности, что недопустимо для систем оборонного назначения. Этим обусловлен интерес разработчиков к данной теме и актуальность работ по созданию собственных систем генерации и распределения квантового ключа.

Список литературы

1. Бауместер Д., Экерт А., Цайлингер А. Физика квантовой информации. – М.: Постмаркет, 2003. – 253 с.
2. Bennett C., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // J. of Cryptology, 1992. – № 5 – P. 356-353.
3. Tittel W., Brendel J., Gisin B., Herzog T., Zbinden H., Gisin N. Experimental demonstration of quantum correlations over more than 10 km // Phys. Rev. A., 1998. – V.57 – P. 3229-3232.
4. Курочкин В.Л., Зверев А.В., Курочкин Ю.В., Рябцев И.И., Неизвестный И.Г. Экспериментальные исследования в области квантовой криптографии. Микроэлектроника 2011, том 40, №4, с 264 – 273.

References

1. Baumester D., Jekert A., Cajlinger A. Fizika kvantovoj informacii. – M.: Postmarket, 2003. – 253 s.
2. Bennett S., Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // J. of Cryptology, 1992. – № 5 – P. 356-353.
3. Tittel W., Brendel J., Gisin B., Herzog T., Zbinden H., Gisin N. Experimental demonstration of quantum correlations over more than 10 km // Phys. Rev. A., 1998. – V.57 – P. 3229-3232.
4. Kurochkin V.L., Zverev A.V., Kurochkin Ju.V., Rjabcev I.I., Neizvestnyj I.G. Jeksperimental'nye issledovanija v oblasti kvantovoj kriptografii. Mikrojelektronika 2011, tom 40, №4, s 264 – 273.