УДК 003.26 + 004.056.55 + 004.22 Вестник УрФО № 4(26) / 2017, с. 31–35

Филиппов М. А., Кротова Е. Л.

КВАНТОВАЯ КРИПТОГРАФИЯ. ПРОТОКОЛЫ КВАНТОВОЙ КРИПТОГРАФИИ

В этой статье представлен обзор распределения квантовых ключей, ориентированного на сферу информационных технологий. В частности, в этой статье описывается протокол BB84 и его многочисленные варианты, а также произведён их сравнительный анализ. Привлекательность идеи квантовой криптографии состоит в разработке *новейшего способа генерирования полностью случайных скрытых ключей между пользователями квантовой линии связи, которые раньше никогда не встречались и не имеют общей скрытой информации. Секретность способа и невозможность незаметного съема информации с линии связи основаны на законах квантовой физики — в противоположность используемым в настоящее время способам криптографии, которые основаны на математических закономерностях и поддаются расшифровке.*

Ключевые слова: *Криптография, квантовая криптография, протокол, BB84, B92, BB84 (4+2), E91, шифрование.*

Filippov M. A., Krotova E. L.

QUANTUM CRYPTOGRAPHY. PROTOCOLS OF QUANTUM CRYPTOGRAPHY

This article presents an overview of the distribution of quantum keys oriented to the sphere of information technologies. In particular, this article describes the BB84 protocol and its numerous variants, as well as their comparative analysis. The attraction of the idea of quantum cryptography is the development of the newest way to generate completely random hidden keys between users of the quantum communication line, which previously never met and do not have common hidden information. The secrecy of the method and the impossibility of unnoticeable retrieval of information from the communication line are based on the laws of quantum physics - in contrast to the currently used cryptography methods, which are based on mathematical laws and can be deciphered.

Keywords: *Cryptography, quantum cryptography, protocol, BB84, B92, BB84 (4 + 2), E91, encryption.*

Что такое протокол BB и принцип работы

Существует множество протоколов квантовой криптографии основанных на передаче информации посредством кодирования в состояниях одиночных фотонов, например: BB84, B92, BB84 (4+2) и их модификации. Кроме того, существует протокол, разработанный для кодирования информации в спутанных состояниях – E91.

BB84 — первый протокол квантового рас-

пределения ключа, который был предложен в 1984 году Чарльзом Беннетом и Жилем Брассаром. Он основан на идеях поляризации фотонов. Ключ состоит из битов, которые передаются как фотоны.

При рассмотрении протокола будем называть отправителя Алисой, а получателя Бобом. Сегодня у них есть по сути два варианта: встретиться и сообща сгенерировать криптографический ключ (надеясь, что никто его не подсмотрит) или использовать протоколы с открытым ключом, такой как RSA.

Первый вариант не особо удобен - ключ надо постоянно обновлять (чем дольше используем один и тот же ключ, тем больше шансов, что его кто-то узнает).

Второй вариант используется повсеместно, но, если будет создан квантовый компьютер с адекватным набором элементов, протокол RSA станет уязвим.

Тут в дело и вступает протокол BB84. Что же нужно для того, чтобы он заработал? У Алисы и Боба есть два канала связи: открытый и закрытый. Закрытый канал используется для генерации ключа, открытый - для передачи зашифрованной информации. Открытый канал должен быть устроен так, что, хотя прослушивать его могут все и вся, изменений в передаваемую информацию не может вносить никто. Что касается закрытого канала - необходимо следить, чтобы его никто не прослушивал (и протокол BB84 с этим справляется). Разберём более подробно прокол BB84, позволяющим двум пользователям создать общий криптографический ключ[1].

В протоколе BB84 используются 4 квантовых состояния фотонов, как представлено на рисунке 1, например направление вектора поляризации одно из которых Алиса выбирает в зависимости от передаваемого бита: 90° или 135° для «1», 45° или 0° для «0».

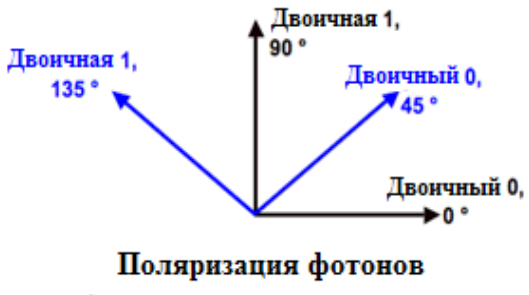

Рисунок 1 – Поляризация состояний в протоколе BB84

Одна пара квантовых состояний принадлежит базису «+». Другая пара квантовых состояний принадлежит базису «×» (рисунок 2). Внутри обоих базисов состояния ортогональны, но состояния из разных базисов являются попарно неортогональными (неортогональность необходима для попыток съёма информации)[4].

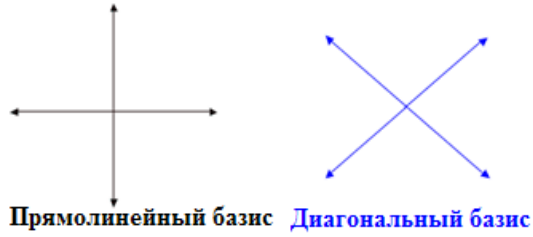

Рисунок 2 – Базисы квантовых состояний

Этапы генерации общего ключа:

Для генерации ключа отправитель пропускает фотоны через четыре традиционных однонаправленных фильтра (линейных поляризатора). Получатель для определения посылаемых бит (поляризации фотонов) применяет две поляризационные разделительные призмы, работающие в прямолинейном и диагональном базисах.

Рассмотрим ситуацию, когда Алиса и Боб передают информацию без прослушивания на примере таблицы 1:

1. Алиса генерирует случайную последовательность бит и для каждого из них случайным образом выбирает один из двух базисов. Полученные фотоны посылает Бобу

2. Боб получает фотоны и считывает их случайным образом, чередуя базисы, т.к. он не знает какую последовательность базисов выбрала Алиса. Некоторые базисы будут правильно отгаданы.

3. Боб открыто сообщает Алисе порядок использования им базисов.

4. Алиса открыто сообщает Бобу, какие базисы были выбраны Бобом правильно, те базисы, которые совпали, формируют ключ.

5. Биты для правильно выбранных базисов используются для проверки целостности переданных данных и формирования ключа. В оригинальном протоколе BB84 из этих «правильных» битов выбирается определенная часть и открыто сравнивается. В случае совпадения (канал не прослушивается и данные дошли без искажений), биты, которые открыто сравнивались, удаляются из ключа и оставшаяся часть используется для формирования ключа требуемой длины[3].

Рассмотрим другую ситуацию, когда пе-

Таблица 1

Пример обмена ключами по протоколу BB84

Этапы									
	1	Случайным образом сгенерированные биты	1	0	0	1	1	1	0
		Базис, выбранный Алисой	×	×	+	×	+	+	+
		Фотоны	\	/	–	\	|	|	–
	2	Базис, выбранный Бобом	+	×	×	+	+	+	×
		Биты, определенные Бобом	0	0	1	0	1	1	1
	3,4	Проверка правильности применения базисов Бобом		V			V	V	
	5	Биты для контроля целостности и формирования ключа		0			1	1	

редаваемую информацию между Алисой и Бобом хочет подслушать злоумышленник (будем именовать Евой):

Как раньше было сказано, в среднем половина посланных Алисой фотонов отбрасывается за счёт того, что Боб выбрал не тот базис. Дальше рассматриваются «правильные» фотоны. Ева перехватывает «правильный» фотон, выбирает базис и посылает этот фотон Бобу. С вероятностью 50% она выберет правильный базис, тем самым получая правильный ответ и пересылает дальше правильный фотон. Но с той же самой вероятностью она выбирает неправильный базис, получает случайный ответ и посылает дальше заведомо ложный фотон. Боб же, выбирая для этого фотона базис, с вероятностью 50% получит правильный ответ, который послала Алиса.

Получается, что при вмешательстве, Ева с вероятностью 50% не меняет ничего, а в половине случаев из оставшихся 50% Боб всё равно получает правильный ответ. Таким образом, Ева вносит изменения в четверть битов ключа. Алиса и Боб подозревают, что их общение подслушивается, и жертвуют частью ключа и сверяют по открытому каналу. Если обнаружено несовпадение в 25% случаев, то их общение становится небезопасным.

Модификации протокола BB и их сравнительный анализ

Протокол B92

В 1992 году Чарльз Беннетт предложил, по сути, упрощенный вариант BB84. Основное различие в B92 заключается в том, что необходимы только два состояния, а не возможные 4 поляризационных состояния в BB84. Как показано на рисунке 3, «0» может быть закодирован, как 0 градусов в прямолинейной основе и «1» может быть закодирована на 45 градусов по диагонали. Как и BB84, Алиса передает Бобу строку фотонов, закодированную со случайно выбранными битами, но на этот раз Алиса диктует, какие базисы она должна использовать. Боб все еще случайно выбирает базисы, но если он выбирает неправильный базис, он ничего не будет менять. Боб может говорить Алисе после каждого бита, который она отправляет, правильно ли он выбрал базис.

Рисунок 3 – Поляризация состояний в протоколе B92

Протокол BB84 (4+2)

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

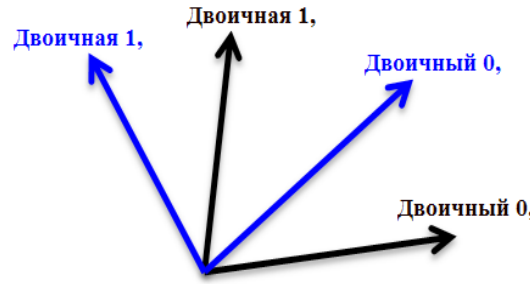

Рисунок 4 – Поляризация состояний в протоколе BB84 (4+2)

Процесс генерации ключа точно такой же как и в протоколе BB84, который описан выше[4].

Протокол E91

В протоколе используются пары фотонов, рождающиеся в антисимметричных поляризационных состояниях.

Отправитель генерирует некоторое количество фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При получении отправителем значения поляризации «1», его партнер зарегистрирует значение «0» и наоборот. Ясно, что таким образом партнеры всякий раз, могут получить идентичные псевдослучайные кодовые последовательности.

Предположим, что изначально создастся некоторое количество пар фотонов максимально запутанных, затем один фотон из каждой пары посылается Алисе, а другой Бобу. Тогда образуется три возможных квантовых состояния для этих пар. Каждое из этих трёх состояний кодирует биты «0» и «1» в уникальном базисе. Затем Алиса и Боб осуществляют измерения на своих частях разделённых пар фотонов, применяя соответствующие приборы. Алиса записывает измеренные биты, а Боб записывает их дополнения до 1. Результаты измерений, в которых пользователи выбрали одинаковые базисы, формируют «сырой» ключ. Для остальных результатов Алиса и Боб проводят проверку на присутствие Евы[5].

Заключение

В заключении хотелось бы сказать, что квантовая криптография - очень перспективная часть криптографии, ведь технологии, используемые там, позволяют вывести безопасность информации на высочайший уровень. Интерес к квантовой криптографии со стороны коммерческих и военных организаций растет, так как эта технология гарантирует абсолютную защиту. Создатели технологий квантовой криптографии вплотную приблизились к тому, чтобы выпустить их из лабораторий на рынок. Осталось немного подождать, и уже очень скоро квантовая криптография обеспечит еще один слой безопасности для нуждающихся в этом организаций.

Литература

1. Квантовая криптография. // TRENDCLUB. URL: http://trendclub.ru/365 (дата обращения 16.06.2017)

2. A Survey of the Prominent Quantum Key Distribution Protocols // QKD. URL: http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#b92 (дата обращения 13.06.2017)

3. BB84 // Википедия. URL: https://ru.wikipedia.org/wiki/BB84 (дата обращения 15.06.2017)

4. Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография учебное пособие / под ред. МАКС Пресс – 2011. – С. 112.

5. О квантовой криптографии. Проктоколы E91 & Lo05 // Хабрахабр. URL: https://habrahabr.ru/post/316252/ (дата обращения 15.06.2017)

References

1. Kvantovaya kriptografiya. // TRENDCLUB. URL: http://trendclub.ru/365 (data obrashcheniya 16.06.2017).

2. A Survey of the Prominent Quantum Key Distribution Protocols // QKD. URL: http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#b92 (data obrashcheniya 13.06.2017.

3. VV84 // Vikipediya. URL: https://ru.wikipedia.org/wiki/BB84 (data obrashcheniya 15.06.2017).

4. Kronberg D.A., Ozhigov YU.I., Chernyavskiy A.YU. Kvantovaya kriptografiya uchebnoye posobiye / pod red. MAKS Press – 2011. – S. 112.

5. O kvantovoy kriptografii. Proktokoly E91 & Lo05 // Khabrakhabr. URL: https://habrahabr.ru/post/316252/ (data obrashcheniya 15.06.2017).

ФИЛИППОВ Михаил Александрович, студент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: Misha-Fill@mail.ru

КРОТОВА Елена Львовна, кандидат физико-математических наук, кафедра «Высшей математики» Пермского национального исследовательского политехнического университета. 614990, Пермский край, г. Пермь, Комсомольский проспект, д. 29. E-mail: lenkakrotova@yandex.ru

FILIPPOV Mikhail, student of the Department of Automation and Telemechanics of the Perm National Research Polytechnic University. 614990, Permsky Kray, Perm, Komsomolsky Prospekt, 29. E-mail: Misha-Fill@mail.ru

KROTOVA Elena, candidate of physico-mathematical sciences, Department of Higher mathematics, Perm National Research Polytechnic University, docent. 614990, Permsky Kray, Perm, Komsomolsky Prospekt, 29. E-mail: lenkakrotova@yandex.ru