ЭЛЕКТРОНИКА

УДК 621.391.25 (075.8)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КВАНТОВОЙ ДВУХКАНАЛЬНОЙ СИСТЕМЫ ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКОГО КЛЮЧА

В.Ф. ГОЛИКОВ, С.Г. СКОБЛЯ

Белорусский государственный университет информатики и радиоэлектроники, П.Бровки,6, Минск, 220013, Беларусь

Барановичский государственный университет, Королика, 8, Барановичи, 220030, Беларусь

Поступила в редакцию 23 июня 2009

Дано описание квантовой двухканальной системы распределения криптографического ключа. Построена математическая модель двухканальной системы и определены ее основные параметры.

Ключевые слова: криптографический ключ, квантовое распределение ключа, двухканальная система квантового распределения ключа.

Введение

В системах квантового распределения ключей существуют проблемы физико-технического характера, связанные с генерацией однофотонных импульсов и их дальнейшей обработкой. Однако помимо этой существует еще и другая проблема, решение которой позволит сделать квантовую передачу криптоключей более эффективной.

Обзор публикаций и патентов в данной области показывает, что уже имеющиеся практические реализации систем, предназначенных для квантового распределения криптографических ключей, не основанные на использовании перепутанных фотонов, используют протокол взаимодействия отправителя и получателя ключа BB84, который предложен в [1]. Данный протокол удобен в реализации как в системах, использующих поляризационное кодирование, так и в системах, основанных на фазовом кодировании, но его очевидный недостаток — потеря 50% битов сырого ключа, что, наряду с другими факторами, существенно снижает эффективность систем квантового распределения ключа.

Как показывают расчеты, при использовании данного протокола во всех ситуациях (кроме ситуации согласованных Алисой и Бобом базисов и отсутствия злоумышленника) формируемая последовательность битов содержит ошибки от 25 % при отсутствии злоумышленника до 37,5% при его наличии. Причем местонахождение ошибочных бит в полученной последовательности неизвестно, поэтому использовать такой ключ целиком невозможно. Для исключения ошибочных бит при квантовой передаче ключа стороны Алиса и Боб по ее окончании обмениваются информацией о порядке использованных базисов при передаче и приеме. После чего оставляют только те биты, которые были получены при согласованных базисах. Естественно, что вероятность получения правильного бита в пределах всей передаваемой информации уменьшается и при отсутствии злоумышленника составит 0,5, а при наличии злоумышленника — 0,375 общей длины ключа соответственно.

Наличие дополнительных ошибочных бит в ключе, состоящем только из бит, принятых сторонами в одинаковых базисах, и свидетельствует о наличии злоумышленника (Евы).

Имея вероятности правильной передачи ключевого бита, несложно рассчитать производные характеристики системы, например, длину сформированного ключа, вероятность обнаружения злоумышленника и т.д.

При полном согласовании передающих и приемных базисов Алисы и Боба все биты передаваемой последовательности определяются принимающей стороной правильно. Поэтому одним из возможных подходов к решению задачи повышения эффективности квантового распределения ключа является использование алгоритмов, в основе которых лежит согласование базисов Алисы и Боба. Наиболее общее описание подобного подхода дано в [2]. Однако этот вариант плох тем, что для его реализации требуется предварительное секретное распределение между Алисой и Бобом некоторой информации, на основании которой будет формироваться последовательность переключения базисов приемника и передатчика, которое создает массу новых проблем с ее распределением и безопасным хранением.

Второе направление – разработка новых алгоритмов либо модификация уже имеющихся таким образом, чтобы без использования согласования последовательности переключения базисов количество бит, которые можно было бы использовать для формирования чистого ключа, в сыром ключе увеличилось.

Двухканальный протокол квантовой передачи криптоключей

Одной из очевидных модификаций классического протокола, позволяющих существенно увеличить длину сформированного ключа, является двухканальный протокол. Повышение эффективности квантового распределения криптоключей достигается тем, что для передачи битов секретного ключа используется не один квантовый канал, а два (при использовании двухбазисного кодирования). При передаче каждого бита по одному каналу базис выбирается случайным образом, а по второму — базис выбирается противоположным по отношению к базису первого канала образом. Соответственно, при регистрации и детектировании каждого импульса на принимающей станции базис приемника первого канала выбирается случайным образом, а второго канала — противоположным по отношению к базису первого канала.

Техническая система для реализации такого протокола впервые предложена в [3] и изображена на рис. 1.

При использовании двухбазисного поляризационного кодирования формирование секретного квантового ключа в данном случае может осуществляться следующим образом. На передающей станции устройством управления формируется исходная последовательность битов, которая и будет использоваться в качестве будущего ключа.

Опишем один из возможных вариантов использования такой системы. Каждый бит последовательности кодируется в двух однофотонных квантовых импульсах, генерируемых источниками *1* и *3*. Базис, используемый для кодирования бита кодирующим модулем *1*, задается устройством управления случайным образом и устанавливается либо прямоугольным (+), либо диагональным (х). Базис, используемый для кодирования бита кодирующим модулем *2*, задается устройством управления противоположным, по отношению к базису, используемому кодирующим модулем *2*. Т.е., если для кодирования некоторого бита кодирующим модулем *1* используется базис (+), то для кодирования этого же бита кодирующим модулем *2* используется базис (х) и наоборот.

Квантовые импульсы регистрируются и декодируются на принимающей станции. Базисы, используемые декодирующими модулями *9* и *10* принимающей станции, выбираются устройством управления принимающей станции *11* одинаковыми, но случайными, т.е. либо (+) для двух модулей, либо (х). При этом если базис, выбранный для декодирования некоторого бита первым декодирующим модулем *9* принимающей станции, совпадает с базисом, использованным для кодирования этого бита первым кодирующим модулем *2* передающей станции, то бит с исключительно высокой вероятностью декодируется первым декодирующим модулем правильно, в то время как значение этого бита, полученное вторым декодирующим модулем *10* с равной вероятностью будет либо «1», либо «0». И наоборот, если базис первого декодирующего модуля не совпал с базисом, использованным первым кодирующим модулем для кодирования, то результатом декодирования первым модулем будут с равной вероятностью либо «1»,

либо «0», а результат декодирования, полученный вторым декодирующим модулем *10*, будет правильным.

Рис. 1. Структурная схема двухканальной системы: 1 – первый квантовый источник — источник единичных фотонов; 2 – первый кодирующий модуль, осуществляющий кодирование последовательности битов будущего квантового ключа (например, задавая поляризацию фотонов) в одном из возможных базисов; 3 – второй квантовый источник; 4 – второй кодирующий модуль, осуществляющий кодирование последовательности битов будущего квантового ключа в базисах, противоположных по отношению к базисам, используемым для кодирования каждого бита кодирующим модулем *1*; 5 – устройство управления, осуществляющее управление источниками фотонов, кодирующими модулями, выполняющее функции связи по каналу обсуждения, функции коррекции ошибок в ключевой последовательности и пр. (может быть реализовано в виде ЭВМ); 6, 7 – первый и второй квантовые каналы; 8 – канал для обсуждения (может быть реализован в виде любого канала связи, в зависимости от конкретной реализации установки: в том числе, например, для целей обсуждения могут использоваться и квантовые каналы *6*, *7*, а канал *8* может быть, в зависимости от конкретной реализации установки, как открытым, так и секретным); 9, 10 – декодирующие модули приемной станции, служащие для регистрации фотонов и декодирования ключевой последовательности; 11 – устройство управления принимающей станции.

Далее с передающей станции на принимающую станцию через канал обсуждения сообщают последовательность базисов, которая использовалась для кодирования первым кодирующим модулем *2*. На принимающей станции из последовательности, полученной первым декодирующим модулем *9*, выбираются биты, при декодировании которых базисы, использованные первым кодирующим модулем *2* и первым декодирующим модулем *9* совпали, а остальные биты выбираются из последовательности, полученной вторым декодирующим модулем *10*. После формирования сырого ключа осуществляется поиск и коррекция ошибок одним из известным алгоритмов, например, как в протоколе BB84.

В таблице приведен пример кодирования и декодирования последовательности битов ключа.

Пример кодирования и декодирования последовательности битов ключа

№ бита	Передача			Прием				Сырой ключ
	Значение бита	Базис канала 1	Базис канала 2	Базис канала1	Базис канала 2	Рез-тат канала 1	Рез-тат канала2	
1	1	+	x	+	+	1	1/0	1
2	0	x	+	x	x	0	1/0	0
3	1	x	+	+	+	1/0	1	1
4	1	x	+	x	x	1	1/0	1
5	0	+	x	+	+	0	1/0	0
6	1	x	+	+	+	1/0	1	1
7	0	+	x	x	x	1/0	0	0
8	0	+	x	+	+	0	1/0	0
9	1	x	+	x	x	1	1/0	1
10	0	x	+	x	x	0	1/0	0

Здесь: «+» — прямоугольный базис, «x» — диагональный базис, «1» и «0» — значения битов, «1/0» — бит принимает значение либо «1», либо «0» с равной вероятностью. Таким образом, потери битов ключа из-за неправильного выбора базиса декодирования, как, например, при использовании протокола BB84 в чистом виде, не происходит, и количество принятых битов сырого ключа возрастает практически на 50%.

Использование данного способа формирования квантового ключа, равно как и формирование ключа с помощью любых других квантовокриптографических систем, подразумевает, что стороны, участвующие в формировании ключа, прошли процедуру идентификации.

В случае перехвата фотонов, передаваемых по квантовым каналам, злоумышленником, присутствие злоумышленника, так же как и в протоколе BB84, обнаруживается по существенному увеличению количества ошибок в сыром ключе. Предположим, что злоумышленник перехватывает фотоны с помощью установки, подобной принимающей станции и генерирует ключевую последовательность для принимающей станции с помощью установки, подобной передающей станции. Тогда при декодировании в 50% случаев злоумышленник получит одинаковые значения битов из обоих каналов — оба нуля или обе единицы (см. столбцы *7, 8* таблицы). Однако в каких базисах передавались эти биты, неизвестно. Поэтому злоумышленник вынужден случайным образом выбирать базисы для кодирования этих битов при передаче принимающей станции. В 50% случаев, когда полученные злоумышленником из разных каналов значения бита не совпадают, он вынужден отсылать объекту *B* случайное значение в случайном базисе.

Математическая модель двухканальной системы распределения квантового ключа

Для исследования параметров двухканальной системы квантового распределения ключа ограничимся случаем, когда у злоумышленника нет квантовой памяти. Для одноканальной системы с протоколом BB84 такой случай рассмотрен в [4].

В отличие от него предположим, что Алиса и Боб для каждого из каналов используют базисы *x* и *y*, описываемые выражениями:

$$|x+\rangle = |0\rangle,\ |x-\rangle = |1\rangle,\ |y+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |y-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Будем считать, что Ева выполняет измерения в плоскости *xy* и что ее первый базис повернут на угол ϕ относительно базиса *x* Алисы и Боба (рис.2), а второй базис на угол $\varphi' = \frac{\pi}{4} - \varphi$ (что не изменяет среднего значения информации Евы).

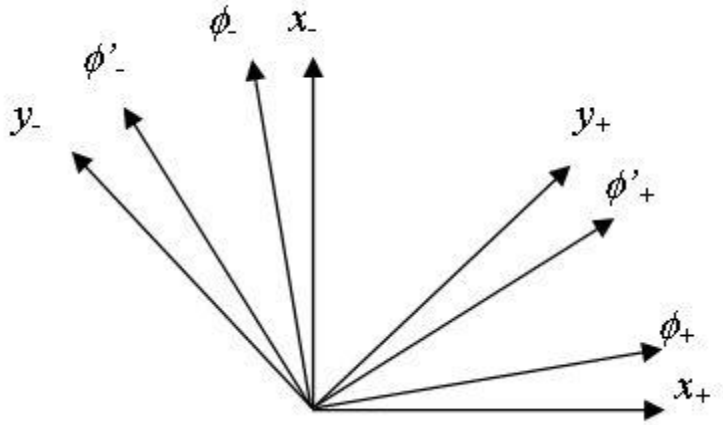

Рис. 2. Базисы Алисы и Евы

Тогда, например, первый базис Евы можно описать выражениями:

$$|\phi+\rangle = \sqrt{\cos\phi}\cdot|0\rangle + \sqrt{\sin\phi}\cdot|1\rangle, \quad |\phi-\rangle = \sqrt{\cos\phi}\cdot|1\rangle - \sqrt{\sin\phi}\cdot|0\rangle.$$

Предполагая, что по каждому из каналов Алиса посылает независимые последовательности битов в выбираемых с равной вероятностью базисах (*x* или *y*), получим, что в принятых обозначениях среднее значение информации Евы для каждого из каналов описывается выражением:

$$I_E = \frac{1}{4}\left(I^x_{E,\phi} + I^y_{E,\phi} + I^x_{E,\phi'} + I^y_{E,\phi'}\right), \tag{1}$$

где $I^x_{E,\varphi}$ — шенноновская информация в случае, когда Алиса передала бит в базисе *x*, а Ева регистрировала его в базисе ϕ. Аналогичным образом определяются и другие слагаемые в правой части (1). Их значения рассчитываются по формулам:

$$\begin{aligned} I^x_{E,\phi} &= I^y_{E,\phi'} = 1 + F^x_{E,\phi}\log F^x_{E,\phi} + D^x_{E,\phi}\log D^x_{E,\phi} \\ I^y_{E,\phi} &= I^x_{E,\phi'} = 1 + F^y_{E,\phi}\log F^y_{E,\phi} + D^y_{E,\phi}\log D^y_{E,\phi} \end{aligned}. \tag{2}$$

В (2) символами *F* и *D* обозначены вероятности правильной и неправильной регистрации состояния Евой. Их значения рассчитываются по формулам:

$$\begin{aligned} F^x_{E,\phi} &= F^y_{E,\phi'} = \cos^2\phi, \quad D^x_{E,\phi} = D^y_{E,\phi'} = \sin^2\phi \\ F^y_{E,\phi} &= F^x_{E,\phi'} = \cos^2\left(\frac{\pi}{4}-\phi\right), \quad D^y_{E,\phi} = D^x_{E,\phi'} = 1-\cos^2\left(\frac{\pi}{4}-\phi\right) \end{aligned}. \tag{3}$$

Для Боба вероятности правильной регистрации состояния при наличии Евы имеют вид:

$$\begin{aligned} F^x_{B,\phi} &= F^y_{B,\phi'} = F^{x\,2}_{E,\phi} + D^{x\,2}_{E,\phi} \\ F^y_{B,\phi} &= F^x_{B,\phi'} = F^{y\,2}_{E,\phi} + D^{y\,2}_{E,\phi} \end{aligned}.$$

Средняя вероятность правильной регистрации бита из одного канала Бобом и среднее значение вероятности ошибки равны соответственно:

$$\begin{aligned} F_{B,\phi} &= \frac{1}{2}\left(F^{x\,2}_{E,\phi} + F^{y\,2}_{E,\phi}\right) \\ D_{B,\phi} &= 1 - F_{B,\phi} \end{aligned}.$$

Вычисления показывают, что при использовании протокола BB84 в частном случае, когда $\phi = 0$ и $\phi' = \frac{\pi}{4}$ (а при отсутствии квантовой памяти это оптимальный вариант «подслушивания» для Евы), ошибка Боба в сыром ключе составит $\frac{1}{4}$, если Ева будет «прослушивать» всю последовательность. Как показано в [4], информация Евы, как функция информации Боба для протокола BB84, может быть выражена соотношением:

$$I_E(D_B) = 2D_B.$$

Анализируя формулы (3), легко заметить, что при использовании двухканальной системы в случае отсутствия квантовой памяти наиболее удачной стратегией Евы будет стандартная стратегия перехват-пересылка фотонов в базисах с $\phi = 0$ или $\phi' = \frac{\pi}{4}$, выбираемых случайным образом одинаковыми для обоих каналов. Действительно, когда Алиса по первому каналу посылает фотон в базисе *x,* а по второму — фотон, кодирующий вторую случайную последовательность битов, в базисе *y*, при использовании Евой базиса ϕ вероятность корректного определения состояния в первом канале $F^{x}_{E,\phi} = 1$, а в случае, когда Ева использует для первого канала базис ϕ', то базисы Алисы и Евы (*y* и ϕ') совпадут во втором канале и вероятность правильного определения состояния во втором канале будет равна 1.

Если Ева перехватывает лишь часть последовательности, ее информация как функция ошибок Боба (рис. 3) в случае двухканальной системы может быть выражена соотношением:

$$I_E(D_B) = 4D_B \text{, где } D_B \in \left[0, \frac{1}{4}\right].$$

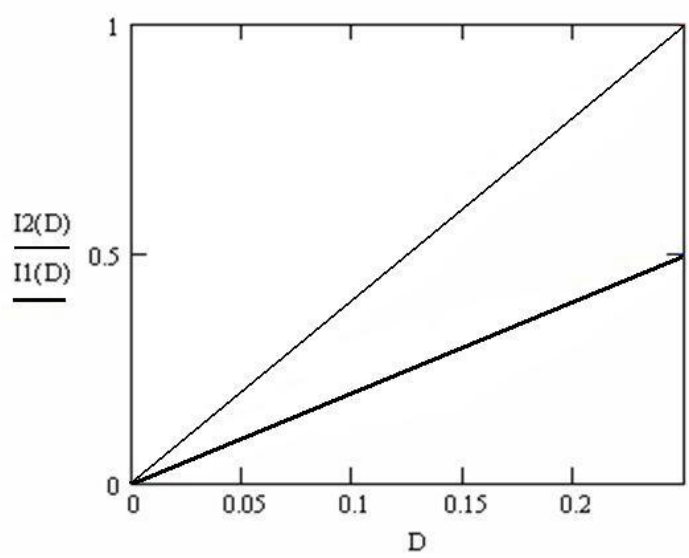

Рис. 3. Зависимость информации Евы от количества ошибок в ключе Боба. *I*1(*D*) — для одноканальной системы, *I*2(*D*) — для двухканальной системы

Заключение

1. Полученные результаты говорят о том, что двухканальная система дает возможность получения сырого ключа, в среднем, в 2 раза большей длины по сравнению с одноканальной, за примерно одинаковые промежутки времени, отведенные на передачу.

2. При наличии, в среднем, 25% ошибок в сыром ключе Боба, сформированного с помощью двухканальной системы, от использования ключа необходимо отказаться, т.к. Еве будут известны значения всех его битов.

3. При малых значениях ошибки в ключе Боба возможно использование ключа, сформированного с помощью двухканальной системы после процедуры коррекции ошибок и усиления секретности.

4. Из-за особенностей процедуры перехвата Евой в двухканальной системе следует, что Еве нет необходимости использовать квантовую память [5] при «прослушивании» всей передаваемой последовательности, т.к. количество получаемой ей информации максимально при классической стратегии «перехват-пересылка».

5. Стоимость двухканальной системы меньше стоимости двух одноканальных из-за упрощения системы передачи ввиду связанности двух каналов.

MATHEMATICAL MODEL OF TWO-CHANNEL QUANTUM KEY DISTRIBUTION SYSTEM

V.F. GOLIKOV, S.G. SKOBLIA

Abstract

Description of two-channel quantum key distribution system is presented. Mathematical model of two-channel quantum key distribution system is created and its main parameters are calculated.

Литература

1. *Bennet C. H. Brassard. G. //* Quantum cryptography: quantum key distribution and coin tossing. Int. conf. on computers systems ans signal processing. Bangalore, 1984. P.175-179.
2. Патент WO 2007/036012 A1.
3. *Голиков В.Ф., Скобля С.Г.*. Способ кодирования и передачи квантового ключа. Заявка на получение патента. Номер 20080283 от 12.03.2008.
4. *H. Bechmann-Pasquinucci.* // Eavesdropping without quantum memory. Quant-ph. 050403. 2005. Vol.1.
5. *Fuchs C.A., Gisin N., Griffiths R.B. et al* // Optimal eavesdropping in quantum cryptography. Phys. Rev. 9701039. 1997. Vol. 1. P.163-172.