ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **BY** (11) **14139**

(13) **C1**

(46) **2011.02.28**

(51) МПК (2009)
H 04L 9/08

(54) СПОСОБ ПЕРЕДАЧИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА

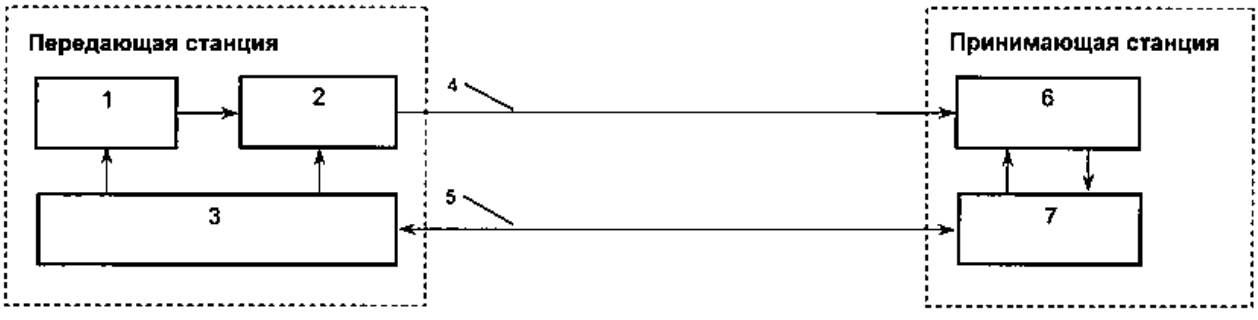
(21) Номер заявки: a 20090400
(22) 2009.03.18
(43) 2010.10.30

(71) Заявитель: Белорусский национальный технический университет (BY)
(72) Авторы: Голиков Владимир Федорович; Скобля Сергей Геннадьевич (BY)
(73) Патентообладатель: Белорусский национальный технический университет (BY)

(56) БРАССАР Ж. Современная криптология. - М.: Полимед, 1999. - С. 132-137.
RU 2302085 C1, 2007.
WO 2008/153774 A2.
US 2009/0003591 A1.
US 2006/0056630 A1.

(57)

Способ передачи криптографического ключа, при котором формируют на передающей станции последовательность битов, образующую исходный ключ, генерируют передающей станцией однофотонные импульсы, кодируют биты ключевой последовательности поляризационными состояниями упомянутых импульсов в двух альтернативных базисах, не ортогональных друг другу, со случайным выбором базиса для каждого упомянутого импульса, передают кодированные однофотонные импульсы по оптоволоконному или атмосферному каналу принимающей станции, на которой осуществляют декодирование принятых однофотонных импульсов в двух альтернативных базисах, не ортогональных друг другу, со случайным выбором базиса для каждого принятого однофотонного импульса, **отличающийся** тем, что при кодировании и декодировании соответственно на передающей и приемной станциях осуществляют случайный выбор базисов в соответствии с заранее согласованной одинаковой последовательностью, за исключением базисов, случайно выбираемых в упомянутой последовательности передающей и принимающей станциями независимо друг от друга, количество которых достаточно для обнаружения факта прослушивания с требуемой точностью, причем номера этих базисов и значения битов ключевой последовательности, переданных и полученных в этих базисах, стороны оглашают после декодирования всей ключевой последовательности.



BY 14139 C1 2011.02.28

Изобретение относится к области квантовой криптографии, а более конкретно к способам и устройствам кодирования и передачи криптографических ключей по квантовому каналу, и может быть использовано для защиты информации в телекоммуникациях.

Известен способ кодирования и передачи случайных двоичных последовательностей [1] на основе их кодирования поляризационными либо фазовыми состояниями единичных фотонов в двух альтернативных базисах, не ортогональных друг другу, с последующей передачей кодированных фотонов по оптоволоконному или атмосферному каналу и декодированием их на принимающей станции. Недостатком известного способа является использование только половины переданной двоичной последовательности.

Наиболее близким к предлагаемому способу является способ кодирования и передачи криптографических ключей [2], включающий формирование на передающей станции последовательности битов, образующей исходный ключ, генерацию передающей станцией однофотонных импульсов, кодирование битов ключа поляризационными либо фазовыми состояниями этих импульсов в двух альтернативных базисах, не ортогональных друг другу, со случайным выбором базиса для каждого фотона, передачу кодированных фотонов по оптоволоконному или атмосферному каналу принимающей станции, на которой производится декодирование принятых импульсов в двух альтернативных базисах, не ортогональных друг другу, со случайным выбором базиса для каждого фотона, причем выбор базисов передающей и принимающей станций независим друг от друга.

Одним из существенных недостатков указанного способа является потеря примерно пятидесяти процентов битов исходной ключевой последовательности из-за того, что на принимающей станции базис, в котором принимается очередной квантовый импульс, выбирается случайным образом и, в общем случае, совпадает с базисом, в котором был передан данный импульс, только в 50 % случаев, что, наряду с другими причинами, ограничивает скорость формирования секретной ключевой последовательности. Независимый порядок переключений базисов передающей и принимающей станций используется для обнаружения факта "прослушивания" канала связи третьей стороной и принципиально необходим в данном способе для обеспечения конфиденциальности передаваемого ключа.

Задача, решаемая изобретением, заключается в повышении количества правильно декодируемых принимающей станцией битов ключевой последовательности, кодируемых передающей станцией при сохранении требуемого уровня конфиденциальности формируемого ключа.

Решение поставленной задачи достигается тем, что в способе передачи криптографического ключа, при котором формируют на передающей станции последовательность битов, образующую исходный ключ, генерируют передающей станцией однофотонные импульсы, кодируют биты ключевой последовательности поляризационными состояниями упомянутых импульсов в двух альтернативных базисах, не ортогональных друг другу, со случайным выбором базиса для каждого упомянутого импульса, передают кодированные однофотонные импульсы по оптоволоконному или атмосферному каналу принимающей станции, на которой осуществляют декодирование принятых однофотонных импульсов в двух альтернативных базисах, не ортогональных друг другу, со случайным выбором базиса для каждого принятого однофотонного импульса, при кодировании и декодировании соответственно на передающей и приемной станциях осуществляют случайный выбор базисов в соответствии с заранее согласованной одинаковой последовательностью, за исключением базисов, случайно выбираемых в упомянутой последовательности передающей и принимающей станциями независимо друг от друга, количество которых достаточно для обнаружения факта прослушивания с требуемой точностью, причем номера этих базисов и значения битов ключевой последовательности, переданных и полученных в этих базисах, стороны оглашают после декодирования всей ключевой последовательности.

Эти биты, названные индикаторными, в дальнейшем используют только для обнаружения прослушивания и исключают из общего ключа. Таким образом, за счет согласования передающих и приемных базисов для подавляющего числа битов порождающей последовательности формируется общий ключ с нулевым количеством ошибок (кроме шумовых ошибок), а факт прослушивания устанавливается по относительно небольшому количеству индикаторных битов. Если прослушивание обнаруживается, то текущий сеанс формирования общего ключа отменяется.

При осуществлении заявляемого способа увеличивается количество правильно декодируемых принимающей станцией битов ключевой последовательности в 1,5-4 раза при сохранении требуемого уровня конфиденциальности формируемого ключа.

Сущность изобретения поясняется чертежом, где приведена блок-схема для осуществления способа, которая содержит: источник единичных фотонов 1, кодирующий модуль 2, осуществляющий кодирование последовательности битов будущего ключа (например, задавая поляризацию фотонов) в одном из возможных базисов, устройство 3 управления, осуществляющее управление источниками фотонов, кодирующими модулями, выполняющее функции связи по каналу обсуждения, функции коррекции ошибок в ключевой последовательности и пр., которое может быть реализовано в виде ЭВМ, квантовый канал 4, канал 5 для обсуждения, который может быть реализован в виде любого канала связи в зависимости от конкретной реализации установки, декодирующий модуль 6 приемной станции, служащий для регистрации фотонов и декодирования ключевой последовательности, устройство 7 управления принимающей станции.

При использовании двухбазисного поляризационного кодирования формирование секретного квантового ключа заявленным способом может осуществляться следующим образом. На передающей станции устройством 3 управления формируют порождающую последовательность битов R_i, где i = 1, 2, …, n. Эту последовательность по каналу 5 передают на устройство 7 управления принимающей станции. Устройство 3 управления формирует случайную последовательность чисел $I_s^A \in \overline{\{1, n\}}$, где s = 1, 2, …, r; $r \le n/2$. Все биты последовательности R_i, номера которых $i = I_s^A$, заменяют на противоположные. В дальнейшем эту последовательность обозначают R_i^A.

Устройство 7 управления формирует случайную последовательность чисел $I_s^B \in \overline{\{1, n\}}$, где s = 1, 2, …, r; $r \le n/2$. Все биты последовательности R_i, номера которых $i = I_s^B$, заменяют на противоположные. В дальнейшем эту последовательность обозначают R_i^B.

На передающей станции устройством 3 управления формируют ключевую последовательность битов K_i, где i = 1,2,…,n. Каждый бит ключевой последовательности кодируют в однофотонном квантовом импульсе, генерируемом источником 1. Базис, используемый для кодирования бита кодирующим модулем 1, задают устройством управления в соответствии с R_i^A либо прямоугольным (+), либо диагональным (x).

Квантовые импульсы регистрируют и декодируют на принимающей станции. Базисы, используемые декодирующим модулем 6 принимающей станции, выбирают устройством 7 управления принимающей станции в соответствии с R_i^B.

Далее с передающей станции сообщают через канал обсуждения 5 на принимающую станцию номера I_s^A и значения битов K_i, для которых $i = I_s^A$. На принимающей станции производят сравнение I_s^A с I_s^B. Для всех совпадающих номеров базис передающей станции совпадает с базисом приемной стороны, поэтому биты K_i, принятые в согласованных

базисах, должны совпадать с переданными. Это совпадение свидетельствует об отсутствии прослушивания, поэтому эти биты названы индикаторными $K_i^{И}$. Далее из принятой последовательности K_i исключают биты с номерами, равными I_s^A и I_s^B, поскольку они были оглашены.

В случае если злоумышленник подключился к каналам 4, 5, то ему известна порождающая последовательность битов R_i, поэтому он использует ее для прослушивания канала 4. При этом все биты ключевой последовательности K_i принимают в согласованных базисах, кроме базисов, соответствующих номерам I_s^A. Поскольку прием битов с этими номерами злоумышленником происходит в рассогласованных базисах, то с вероятностью 0,5 каждый индикаторный бит на приемной станции не совпадает с переданным. При некотором числе индикаторных битов можно обеспечить требуемую вероятность обнаружения прослушивания.

Ниже приведены расчетные соотношения, подтверждающие реализуемость метода. Обозначим через j случайную величину - число индикаторных битов. Вероятность того, что при выбранных значениях n и r образуется m индикаторных битов, равна

$$P(j=m)=\frac{\binom{r}{m}}{\binom{n}{r}}\cdot\binom{n-r}{r-m},$$

где $\binom{n}{k}$ - число сочетаний из n по k.

Вероятность того, что количество индикаторных битов j окажется не менее m, равна

$$P(j\geq m)=\sum_{j=m}^{r}\frac{\binom{r}{j}}{\binom{n}{r}}\cdot\binom{n-r}{r-j}. \qquad (1)$$

Минимальное количество индикаторных битов, необходимых для надежного обнаружения прослушивания, можно найти, задавшись вероятностью необнаружения прослушивания $P_{необн}=\frac{1}{2^m}$. Откуда $m = -\log_2 P_{необн}$. Например, для $P_{необн}=\frac{1}{256}\approx 0{,}004$ получаем m = 8. Зная m, из (1) можно найти r для некоторого n, задав достаточно большое значение этой вероятности $\sum_{j=m}^{r}\frac{\binom{r}{j}}{\binom{n}{r}}\cdot\binom{n-r}{r-j}\geq\alpha$. Расчеты показывают, что для получения m = 8 при n = 500 с вероятностью $\alpha = 0{,}97$ необходимо $r \geq 80$. С учетом того, что все биты K_i, используемые для обнаружения прослушивания, удаляются из ключевой последовательности, окончательная длина сформированного ключа n_0 окажется несколько меньше, чем n, так как минимальное количество удаляемых битов равно r (полное совпадение последовательностей I_s^A и I_s^B), а максимальное 2r (полное несовпадение за вычетом m совпавших)

$$n\text{-}r \geq n_0 \geq n\text{-}(2r\text{-}m).$$

В рассматриваемом примере $420 > n_0 > 348$. Способ, предложенный в [1], дает $n_0^1 = 250$. Выигрыш в длине ключа составляет

$$k=\frac{n_0}{n_0^1}=1{,}7\div 1{,}4\ .$$

Расчеты показывают, что выигрыш возрастает с ростом величины n. Так, при n = 1000

$$k = 3{,}54\div 3{,}11.$$

В таблице приведен пример формирования общего ключа в соответствии с заявляемым способом.

Номер бита	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
R_i	1	0	0	1	1	1	0	0	1	0	1	1	0	0	0	1	1	0	0	1	0	0
I_s^A				4					9						15			18				22
I_s^B		2		4							11				15					20		
R_i^A	1	0	0	0	1	1	0	0	0	0	1	1	0	0	1	1	1	1	0	1	0	1
Передающий базис А	+	x	x	x	+	+	x	x	x	x	+	+	x	x	+	+	+	+	x	+	x	+
R_i^B	1	1	0	0	1	1	0	0	1	0	0	1	0	0	1	1	1	0	0	0	0	0
Приемный базис В	+	+	x	x	+	+	x	x	+	x	x	+	x	x	+	+	+	x	x	x	x	x
K_i^A	0	0	1	0	0	1	1	1	0	1	0	1	1	0	0	1	1	1	0	0	1	0
Приемн. и перед. базис Е	+	x	x	+	+	+	x	x	+	x	+	+	x	x	x	+	+	x	x	+	x	x
K_i^B	0	$\frac{0}{1}$	1	$\frac{0}{1}$	0	1	1	1	$\frac{0}{1}$	1	$\frac{0}{1}$	1	1	0	$\frac{0}{1}$	1	1	$\frac{0}{1}$	0	$\frac{0}{1}$	1	$\frac{0}{1}$
K_i^{AB}	0		1		o	1	1	1		1		1	1	0		1	1		0		1	
Индикаторн. биты при наличии прослуш.				$\frac{0}{1}$											$\frac{0}{1}$							
Индикаторн. биты при отсутствии прослуш.				0											0							

Примечание: "+" - прямоугольный базис; "x" - диагональный базис; "1" и "0" - значения битов; "$\frac{0}{1}$" - бит принимает значение либо "1", либо "0" с равной вероятностью; K_i^{AB} - итоговый ключ, сформированный у А и В.

В приведенном примере выбрано r = 5. Передающая сторона А рассогласовала базисы с номерами 4, 9, 15, 18, 22. Приемная сторона В рассогласовала базисы с номерами 2, 4, 11, 15, 20. Индикаторные биты образовались в базисах с номерами 4, 15. Длина сформированного ключа равна 14 бит.

Источники информации:

1. Bennet C.H. and Brassard G., in "Proc. IEEE Int. Conference on Computers, Systems and Signal Processing", IEEE. - New York, 1984.

2. Брассар Ж. Современная криптология. - М.: Полимед, 1999. - С. 132-137.

Национальный центр интеллектуальной собственности.
220034, г. Минск, ул. Козлова, 20.