ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **BY** (11) **14813**

(13) **C1**

(46) **2011.10.30**

(51) МПК

H 04L 9/08 (2006.01)

(54) СПОСОБ ПЕРЕДАЧИ КРИПТОГРАФИЧЕСКОГО КЛЮЧА

(21) Номер заявки: a 20080283
(22) 2008.03.12
(43) 2009.10.30

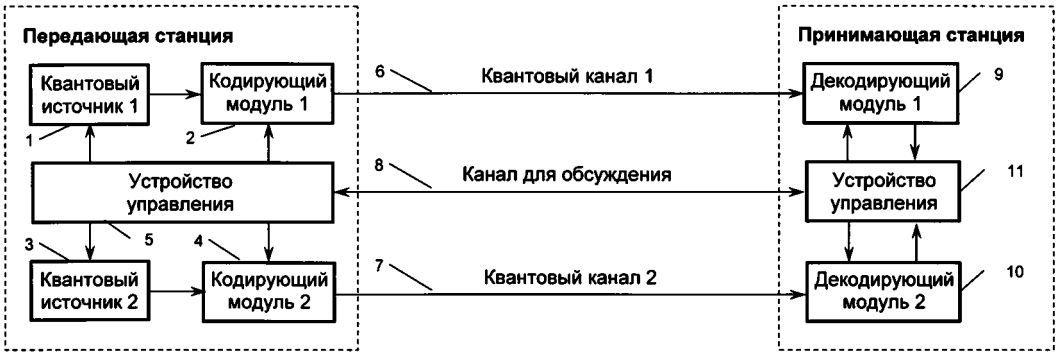
(71) Заявитель: Учреждение образования "Белорусский государственный университет информатики и радиоэлектроники" (BY)
(72) Авторы: Голиков Владимир Федорович; Скобля Сергей Геннадьевич (BY)

(73) Патентообладатель: Учреждение образования "Белорусский государственный университет информатики и радиоэлектроники" (BY)

(56) BENNET C.H. et al. Quantum cryptography: Public key distribution and coin tossing. International Conference on Computers, Systems and Signal Processing. India, 1984.
RU 2302085 C1, 2007.
WO 96/06491 A1.
US 2006/0056630 A1.

(57)

Способ передачи криптографического ключа, при котором формируют на передающей станции исходную последовательность битов, образующую ключ, кодируют биты посредством однофотонной последовательности, передают их и детектируют на принимающей станции, **отличающийся** тем, что биты последовательности передают одновременно по двум квантовым каналам, причем значение одного и того же бита передают одиночными фотонами по каждому каналу в противоположных базисах, а для детектирования принятых битов используют два декодирующих устройства, соответственно первого и второго каналов, базисы которых выбирают одинаковыми и синхронно изменяющимися по случайному закону.



Изобретение относится к области квантовой криптографии, а более конкретно к способам и устройствам передачи криптографических ключей.

Из уровня развития техники известны способы формирования квантовых криптографических ключей с помощью одиночных фотонов, включающие: формирование на пере-

BY 14813 C1 2011.10.30

дающей станции последовательности битов, образующих исходный ключ; генерацию передающей станцией квантовых импульсов, с использованием последовательности ключевых битов и последовательности шифрующих битов, применяемой для кодирования импульсов; регистрацию импульсов на принимающей станции и их декодирование. При этом для непосредственно кодирования одиночных фотонов используется либо поляризационное кодирование, либо фазовое. Первый вариант предложен Ч.Х. Беннетом и Г. Брассаром [1], второй - Ч.Х. Беннетом [2].

Установки, в основу которых положены указанные способы, используют для формирования квантового ключа два канала: квантовый (оптоволоконный или атмосферный), который используется для передачи квантовых импульсов, и любой незащищенный канал, используемый для обсуждения базисов и коррекции ошибок.

Одним из существенных недостатков указанных способов 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.

Технический результат, на достижение которого направлено изобретение, заключается в повышении количества правильно регистрируемых принимающей станцией битов ключевой последовательности, кодируемой передающей станцией.

Технический результат 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 отношении к базису первого канала. Соответственно при регистрации и детектировании каждого импульса на принимающей станции базис приемника первого канала выбирается случайным образом, а второго канала - одинаковым по отношению к базису первого канала.

Предложенный способ изображен на фиг. 1. Приняты следующие обозначения:

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. Канал 8 может быть, также 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.

При использовании двухбазисного поляризационного кодирования формирование секретного квантового ключа заявленным способом может осуществляться следующим образом. На передающей станции устройством управления формируется исходная после-

довательность битов, которая и будет использоваться в качестве будущего ключа. 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 (x). Базис, используемый для кодирования бита кодирующим модулем 2, задается устройством управления противоположным, по отношению к базису, используемому кодирующим модулем 2. То есть, если для кодирования некоторого бита кодирующим модулем 1 используется базис (+), то для кодирования этого же бита кодирующим модулем 2 используется базис (x) 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 (x). 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.

Далее с передающей станции сообщают через канал обсуждения на принимающую станцию 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 известных алгоритмов, например, как в протоколе BB84.

Ниже приведен пример кодирования и декодирования последовательности битов ключа.

№ бита	Передача			Прием				Сырой ключ
	Значение бита	Базис канала 1	Базис канала 2	Базис канала 1	Базис канала 2	Рез-тат канала 1	Рез-тат канала 2	
1	2	3	4	5	6	7	8	9
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 ис-

пользовании 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 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 25 % случаев (от всего количества битов ключа) базисы будут выбраны неправильно, что приведет к тому, что 12,5 % битов сырого ключа на принимающей станции будут получены одинаковые значения битов из разных каналов, но базисы, использованные для декодирования, не будут совпадать с базисами, использованными для кодирования передающей станцией, что и будет свидетельствовать о наличии злоумышленника. Кроме того, 6,25 % битов принятого сырого ключа окажутся инвертированными, по отношению к битам переданной последовательности.

Источники информации:

1. BENNET C.H. et al. Quantum cryptography: Public key distribution and coin tossing. International Conference on Computers, Systems and Signal Processing. India, 1984.

2. BENNET C.H., Phys. Rev. Lett. 68, 3121, 1992.

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