КВАНТОВОЕ ФОРМИРОВАНИЕ КЛЮЧА С ВЕРОЯТНОСТНЫМ КОНТРОЛЕМ ПРОСЛУШИВАНИЯ

В.Ф. Голиков, С.Г. Скобля***

*Белорусский национальный технический университет,
кафедра информационные технологии в управлении;
ул. Ф. Скорины, 25, г. Минск, Республика Беларусь
телефон: + (37529) 266-26-58; e-mail: vgolikov@bntu.by

**Барановичский государственный университет,
кафедра информационных систем и технологий
ул. Королика 8, Барановичи, Республика Беларусь
телефон: + (37529) 790-17-23; e-mail: skoblia@tut.by

Предлагается модификация известного алгоритма вычисления общего криптографического ключа с использованием квантового канала Ч. Беннета и Г. Брассара, обеспечивающая меньшие потери ключевой информации при формировании «сырого» ключа. Приведены расчетные соотношения, подтверждающие эффективность модификации.

Ключевые слова - криптографический ключ, квантовый канал.

Современные системы квантового распределения ключей в основном используют алгоритм, предложенный в протоколе [1]. Протокол удобен в реализации как в системах, использующих поляризационное кодирование, так и в системах, основанных на фазовом кодировании. Однако в данном протоколе при формировании общего первичного ключа теряется в среднем около половины ключевых бит, что наряду с другими проблемами физико-технического характера снижает эффективность систем квантового распределения ключа.

В основе модификации протокола лежит предположение, что «прослушивание» квантового канала криптоаналитиком может быть обнаружено не обязательно по всей ключевой последовательности, как это делается в базовом протоколе, а по гораздо меньшему количеству ключевых бит, специально сформированных для этого и названных индикаторными. При отсутствии прослушивания в модифицированном протоколе в сырой ключ входят все биты ключевой последовательности за исключением индикаторных, в то время как в базовом – только половина. При обнаружении прослушивания сеанс формирования ключа отменяется как в базовом протоколе, так и в модифицированном.

Рассмотрим принцип работы модифицированного протокола на примере системы, использующей двухбазисное поляризационное кодирование. На передающей станции *A* устройством управления формируют порождающую случайную последовательность битов R_i, где i=1, 2,..., n; n – размер последовательности. Эту последовательность по открытому каналу связи передают на устройство управления принимающей станции *B*. Устройство управления *A* 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 управления *B* 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 *A* устройством управления формируют ключевую последовательность битов K_i, где i=1, 2,..., n. Каждый бит ключевой последовательности кодируют в однофотонном квантовом импульсе, генерируемым источником *A*. Базис, используемый для кодирования бита кодирующим модулем, задают устройством управления в соответствии с R_i^A, либо прямоугольным (+), либо диагональным (x).

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

Далее с передающей станции сообщают по открытому каналу связи на принимающую станцию номера I_s^A и значения бит 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 криптоаналитик E подключился к каналу открытой связи и квантовому каналу, то ему известна порождающая последовательность битов R_i, и он использует ее при прослушивании квантового канала. При этом все биты ключевой последовательности K_i принимаются им в согласованных базисах, кроме битов, соответствующих номерам I_s^A. Принимая одиночные фотоны в согласованных базисах, криптоаналитик правильно определяет ключевые биты и возвращает фотоны обратно в квантовый канал в тех же поляризационных базисах, что и при приеме. Поэтому факт прослушивания канала не обнаруживается. Поскольку прием фотонов с номерами I_s^A криптоаналитиком происходит в рассогласованных базисах, то с вероятностью 0,5 каждый из этих фотонов возвращается в канал в противоположном базисе, что приводит к несовпадению ключевых бит с этими номерами на приемной станции B с переданными A.

Возникает вопрос при каком числе индикаторных бит можно обеспечить требуемую вероятность обнаружения прослушивания.

Обозначим через j случайную величину - число индикаторных бит. Можно показать, что вероятность того, что при выбранных значениях n и r образуется m индикаторных бит, равна

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

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

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

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

Минимальное количество индикаторных бит, необходимых для надежного обнаружения прослушивания, можно найти, задавшись вероятностью не обнаружения прослушивания $P_{необн}=1/2^m$. Откуда $m=-\log_2 P_{необн}$. Например, для $P_{необн}=1/256\approx 0{,}004$ получаем $m=8$. Зная m, несложно найти r для заданного n, задав достаточно большое значение вероятности $P(j\geq m)$

$$\sum_{j=m}^{r}\frac{\binom{r}{j}\binom{n-r}{r-j}}{\binom{n}{r}}\geq\alpha,$$

где α – вероятность, близкая к 1. Расчеты показывают, что для получения m=8 при n=500 с вероятностью α=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 бит равно r (полное совпадение последовательностей I_s^A и I_s^B), а максимальное $2r$ (полное несовпадение за вычетом m совпавших), т.е.

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

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

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

Расчеты показывают, что выигрыш возрастает с ростом величины n. Так при n=1000 выигрыш составляет $k=3{,}54\div 3{,}11$. Пример формирования ключа приведен в таблице 1. В этой таблице введены дополнительные обозначения: $Б_A$ – базис передающей станции A; $Б_B$ – базис приемной станции B; $Б_E$ – базис приемной и передающей станций криптоаналитика E; K_i^B –сырой ключ, сформированный $Б$; K_i^{AB} – общий ключ A и B после удаления индикаторных бит; $И_n$ – индикаторные биты при наличии прослушивания; $И_{бп}$ – индикаторные биты при отсутствии прослушивания; «+» – прямоугольный базис; «х» – диагональный базис; «1» и «0» – значения битов; «0/1» – бит принимает значение либо «1», либо «0» с равной вероятностью.

Таблица 1

№ бита	R_i	I_s^A	I_s^B	R_i^A	$Б_A$	R_i^B	$Б_B$	$K_i^И$	$Б_E$	K_i^B	K_i^{AB}	$И_n$	$И_{бп}$
1	1			1	+	1	+	0	+	0	0		
2	0		2	0	x	1	+	0	x	0/1			
3	0			0	x	0	x	1	x	1	1		
4	1	4	4	0	x	0	x	0	+	0/1		0/1	0
5	1			1	+	1	+	0	+	0	0		
6	1			1	+	1	+	1	+	1	1		
7	0			0	x	0	x	1	x	1	1		
8	0			0	x	0	x	1	x	1	1		
9	1	9		0	x	1	+	0	+	0/1			
10	0			0	x	0	x	1	x	1	1		
11	1		11	1	+	0	x	0	+	0/1			
12	1			1	+	1	+	1	+	1	1		
13	0			0	x	0	x	1	x	1	1		
14	0			0	x	0	x	0	x	0	0		
15	0	15	15	1	+	1	+	0	x	0/1		0/1	0
16	1			1	+	1	+	1	+	1	1		
17	1			1	+	1	+	1	+	1	1		
18	0	18		1	+	0	x	1	x	0/1			
19	0			0	x	0	x	0	x	0	0		
20	1		20	1	+	0	x	0	+	0/1			
21	0			0	x	0	x	1	x	1	1		
22	0	22		1	+	0	x	0	x	0/1			

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

ЛИТЕРАТУРА

[1] Quantum cryptography. Public key distribution and coin tossing / C.H. Bennett, G. Brassard// Proceedings of the International Conference on Computers, Systems and Signal Processing, – Bangalore, India, 1984, – С. 175 -179.