УДК 003.26:621.39+530.145

Василиу Е.В.
Vasiliu E.V.

БЕЗОПАСНОСТЬ ПИНГ-ПОНГ-ПРОТОКОЛА КВАНТОВОЙ СВЯЗИ ДЛЯ ПЕРЕДАЧИ ТЕКСТОВЫХ СООБЩЕНИЙ

THE PING-PONG QUANTUM COMMUNICATION PROTOCOL'S SECURITY FOR TRANSMISSION OF TEXT MESSAGES

Аннотация. Проведен анализ безопасности пинг-понг-протокола для передачи секретных текстовых сообщений, закодированных с помощью кодовых таблиц CP-1251 и Unicode, с учетом частот употребления букв в осмысленных английских и русских текстах. Показано, что использование кодировки Unicode вместо CP-1251 делает пинг-понг протокол более безопасным. Показано, что для пинг-понг протокола с квантовым плотным кодированием и с использованием в режиме контроля подслушивания одного измерительного базиса существует невидимый режим подслушивания, при котором противник может получить почти 50 % информации при использовании легитимными пользователями кодировки CP-1251 и ~36 % при использовании ими кодировки Unicode. Следовательно, пинг-понг протокол с квантовым плотным кодированием и с использованием в режиме контроля подслушивания одного измерительного базиса нельзя применять для передачи секретных текстовых сообщений без дополнительных мер по усилению секретности. Предложен метод усиления секретности, состоящий в обратимом хешировании блоков сообщения посредством умножения на случайную обратимую двоичную матрицу.

Summary. The security analysis of ping-pong protocol for transmission of secret text messages coded by tables CP-1251 and Unicode is carried out, taking into account frequencies of using the letters in sensible English and Russian texts. It is shown, that use of coding by Unicode instead of CP-1251 makes the ping-pong protocol more secure. It is shown, that for ping-pong protocol using quantum dense coding and one measurement basis in control mode there is an invisible mode of eavesdropping, at which the opponent can gain almost 50 % of the information using by legitimate users of CP-1251 and ~ 36 % using Unicode by them. Hence, the ping-pong protocol using quantum dense coding and one measurement basis in control mode cannot be applied for transmission of secret text messages without additional arrangements on privacy amplification. The method of the privacy amplification is proposed, that consists in invertible hashing the message blocks using multiplication by a random invertible binary matrix.

В настоящее время, в связи с быстрым развитием и все более широким распространением телекоммуникационных систем, остро стоит проблема защиты информации в таких системах от несанкционированного доступа. Одним из перспективных подходов к решению этой проблемы является квантовая криптография – бурно развивающийся в последние два десятилетия раздел квантовой теории информации [1].

Квантовые протоколы безопасной связи (КПБС) – одно из направлений квантовой криптографии – предназначены для непосредственной передачи секретных сообщений через квантовый канал без их предварительного шифрования. В схемах квантовой безопасной связи секретный ключ вообще не используется, а его роль играет квантовомеханический ресурс – совместно используемые абонентами пары перепутанных квантовых частиц, например, пары Эйнштейна-Подольского-Розена [2…4]. Такая технология защиты коммуникаций является значительным прогрессом в криптографии, так как в значительной степени снимает сложную проблему распределения секретных ключей – для КПБС ключи не нужны, а общий секретный ключ может понадобиться абонентам только для взаимной аутентификации перед началом протокола.

К настоящему времени предложено несколько КПБС, которые отличаются как базовыми принципами, положенными в их основу, так и степенью их стойкости против различных атак противника. Проведены исследования стойкости таких протоколов против некоторых видов атак, предложены соответствующие усовершенствования протоколов [2…9]. При этом исследования стойкости, как правило, ограничиваются лишь вычислением максимального количества информации, которое может быть получено противником при определенных условиях, а важный вопрос о том, каким образом противник может использовать полученную им частичную информацию и какие криптоаналитические методы для этого необходимы, остается за рамками выполненных исследований. Вероятно, такое положение вещей обусловлено тем, что в рамках классической криптографии подобные задачи вообще не возникают – предполагается, что противник может

перехватить передаваемое сообщение полностью и, если оно не зашифровано, то, следовательно, может быть полностью прочитано.

В [9] проведен общий анализ безопасности пинг-понг протокола с квантовым плотным кодированием и с использованием в режиме контроля подслушивания одного измерительного базиса, получено выражение для максимальной информации, доступной противнику, как функции от вероятности обнаружения противника легитимными пользователями. Показано, что безопасное использование такого протокола возможно для передачи битовых строк специального вида. Однако вопросы о безопасности протокола для передачи текстовых сообщений и трудоемкости раскрытия такого сообщения противником с использованием полученной им частичной информации рассмотрены не были. Целью настоящей работы является анализ безопасности пинг-понг протокола с квантовым плотным кодированием и с использованием в режиме контроля подслушивания одного измерительного базиса для передачи текстовых сообщений, закодированных с помощью общеупотребительных кодовых таблиц, а также качественный анализ трудоемкости раскрытия такого сообщения противником.

1. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием для передачи текстовых сообщений. В пинг-понг протоколе с квантовым плотным кодированием Боб (принимающая сторона) приготавливает пару полностью перепутанных фотонов в одном из белловских состояний – $\left|\psi^{+}\right\rangle$ и посылает один из фотонов Алисе (передающая сторона), которая выполняет одну из четырех возможных кодирующих операций на этом фотоне и отсылает его назад Бобу. Затем Боб выполняет измерение над обоими фотонами в базисе Белла и тем самым декодирует посланную Алисой двухбитовую комбинацию (двоичную биграмму, в дальнейшем просто “биграмма”) [2, 4, 9]. Пусть Алиса выполняет операции, соответствующие биграммам «00», «01», «10» и «11» с частотами p_1, p_2, p_3, и p_4 соответственно.

Таким образом, в пинг-понг протоколе с квантовым плотным кодированием одна пара перепутанных фотонов служит для передачи двух бит информации. Отметим, что в первоначальной версии пинг-понг протокола, где плотное кодирование не используется, каждая пара перепутанных фотонов служит для передачи только одного бита [3].

Кроме описанного выше режима передачи сообщения, в пинг-понг протоколе предусмотрен также режим контроля подслушивания в квантовом канале [2…4, 9]. Алиса переключается в этот режим случайным образом с некоторой вероятностью q. Как только подслушивание обнаружено – передача прерывается. При этом в протоколе без плотного кодирования достаточно использовать в режиме контроля подслушивания один измерительный базис – $B_z = \{|0\rangle, |1\rangle\}$ [3]. Для протокола с плотным кодированием можно использовать два измерительных базиса – B_z и $B_x = \{|+\rangle, |-\rangle\}$, что в принципе позволяет усилить безопасность протокола [2, 4]. В настоящей работе анализ безопасности пинг-понг протокола с квантовым плотным кодированием для передачи текстовых сообщений выполнен только для случая, когда Алиса и Боб используют в режиме контроля подслушивания один измерительный базис B_z.

Атака подслушивающего агента (Евы) на пинг-понг протокол с квантовым плотным кодированием (при использовании легитимными пользователями одного измерительного базиса в режиме контроля подслушивания) проанализирована в [9]. Получено выражение для максимального количества информации $I_{\max}$ Евы, как функции от вероятности d обнаружения атаки в режиме контроля подслушивания и от частот p_1, p_2, p_3, и p_4 кодирующих операций Алисы:

$$I_{\max} = -\sum_{i=1}^{4} \lambda_i \log_2 \lambda_i \,, \tag{1}$$

где

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 (d - d^2)},$$
$$\lambda_{3,4} = \frac{1}{2}(p_3 + p_4) \pm \frac{1}{2}\sqrt{(p_3 + p_4)^2 - 16 p_3 p_4 (d - d^2)}. \tag{2}$$

Как показано в [9], если Алиса использует четыре кодирующие операции с равными или близкими значениями частот, то Ева может получить значительное количество информации при малой вероятности ее обнаружения, а при $p_1 = p_2 = p_3 = p_4 = 0{,}25$ и $I_{\max} \le 1$ бита вероятность обнаружения Евы $d \equiv 0$. Однако если Алиса передает битовые строки специального вида, например, «00010001…», то Ева получит небольшое количество информации и при этом $d > 0$. Поскольку в осмысленных текстах любого естественного языка различные буквы встречаются с разной частотой, а сами тексты передаются в какой-либо двоичной кодировке, где четыре биграммы также будут иметь разные частоты, то представляет интерес проанализировать безопасность пинг-понг протокола при определенных значениях p_1, p_2, p_3, и p_4, соответствующих передаче осмысленного текста на каком-либо языке в одной из общеупотребительных кодировок.

Будем считать, что Алиса передает текстовое сообщение по идеальному квантовому каналу, т. е. без использования кодов, корректирующих ошибки. Будем считать также, что сообщение не сжимается перед передачей. Вычислим частоты p_1, p_2, p_3, и p_4 при передаче текстового сообщения на английском и русском языках с использованием восьмибитовой кодовой страницы CP-1251 и шестнадцатибитовой Unicode. Для простоты будем считать, что в сообщении есть только строчные буквы и пробелы, поскольку в большинстве обычных текстов частоты заглавных букв и знаков препинания малы. В табл. 1 и 2 приведены относительные частоты строчных букв в английском и русском текстах, полученные на основе подсчетов частот на больших объемах текста [10].

Таблица 1 – Относительные частоты букв в английских текстах

Буква	Частота, %	Буква	Частота, %	Буква	Частота, %	Буква	Частота, %
a	6,37	h	4,31	o	5,30	v	0,92
b	1,28	i	6,22	p	1,45	w	1,44
c	2,27	j	0,13	q	0,14	x	0,14
d	3,21	k	0,33	r	5,46	y	1,22
e	10,29	l	2,81	s	5,30	z	0,04
f	2,10	m	1,94	t	7,78	пробел	19,97
g	1,59	n	6,01	u	1,98		

Таблица 2 – Относительные частоты букв в русских текстах

Буква	Частота, %	Буква	Частота, %	Буква	Частота, %	Буква	Частота, %
а	6,2	и	6,2	р	4,0	ш	0,6
б	1,4	й	1,0	с	4,5	щ	0,3
в	3,8	к	2,8	т	5,3	ы	1,6
г	1,3	л	3,5	у	2,1	ъ, ь	1,4
д	2,5	м	2,6	ф	0,2	э	0,3
е, ё	7,2	н	5,3	х	0,9	ю	0,6
ж	0,7	о	9,0	ц	0,4	я	1,8
з	1,6	п	2,3	ч	1,2	пробел	17,5

В табл. 3 приведены двоичные коды CP-1251 для строчных букв английского и русского алфавитов. Шестнадцатибитовые коды Unicode букв английского алфавита (а также пробела) отличаются от соответствующих кодов CP-1251 только дополнительным первым байтом, состоящим из 8 нулей, и поэтому здесь отдельно не приводятся. Для букв русского алфавита кодовая страница Unicode приведена в табл. 4.

С использованием табл. 1…4 получены значения частот биграмм для английского и русского текстов (с пробелами между словами и без них), передаваемых по пинг-понг протоколу с плотным кодированием (табл. 5), а также значения частот «0» и «1» при передаче по пинг-понг протоколу без плотного кодирования (табл. 6). В последней строке табл. 5 приведена энтропия двоичного кода, вычисленная по формуле:

$$H = -\sum_{i=1}^{4} p_i \log_2 p_i \,. \qquad (3)$$

Таблица 3 – Кодовая таблица CP-1251 для строчных букв английского и русского алфавитов

Английский				Русский			
Буква	Код	Буква	Код	Буква	Код	Буква	Код
a	01100001	o	01101111	а	11100000	р	11110000
b	01100010	p	01110000	б	11100001	с	11110001
c	01100011	q	01110001	в	11100010	т	11110010
d	01100100	r	01110010	г	11100011	у	11110011
e	01100101	s	01110011	д	11100100	ф	11110100
f	01100110	t	01110100	е	11100101	х	11110101
g	01100111	u	01110101	ж	11100110	ц	11110110
h	01101000	v	01110110	з	11100111	ч	11110111
i	01101001	w	01110111	и	11101000	ш	11111000
j	01101010	x	01111000	й	11101001	щ	11111001
k	01101011	y	01111001	к	11101010	ъ	11111010
l	01101100	z	01111010	л	11101011	ы	11111011
m	01101101	пробел	00100000	м	11101100	ь	11111100
n	01101110			н	11101101	э	11111101
				о	11101110	ю	11111101
				п	11101111	я	11111111

Таблица 4 – Кодовая таблица Unicode для строчных букв русского алфавита

Буква	Код	Буква	Код	Буква	Код
а	0000010000110000	л	0000010000111011	ц	0000010001000110
б	0000010000110001	м	0000010000111100	ч	0000010001000111
в	0000010000110010	н	0000010000111101	ш	0000010001001000
г	0000010000110011	о	0000010000111110	щ	0000010001001001
д	0000010000110100	п	0000010000111111	ъ	0000010001001010
е	0000010000110101	р	0000010001000000	ы	0000010001001011
ж	0000010000110110	с	0000010001000001	ь	0000010001001100
з	0000010000110111	т	0000010001000010	э	0000010001001101
и	0000010000111000	у	0000010001000011	ю	0000010001001110
й	0000010000111001	ф	0000010001000100	я	0000010001001111
к	0000010000111010	х	0000010001000101	пробел	0000000000100000

Для пинг-протокола без плотного кодирования энтропия двоичного кода

$$H = -\sum_{i=1}^{2} p_i \log_2 p_i \qquad (4)$$

приведена в последней строке табл. 6.

Таблица 5 – Частоты биграмм p_1, p_2, p_3, p_4 и энтропия H (бит/биграмму) двоичного кода при передаче сообщения по пинг-понг протоколу с плотным кодированием

	Английский				Русский			
	CP-1251		Unicode		CP-1251		Unicode	
	с проб.	без проб.	с проб.	без проб.	с проб.	без проб.	с проб.	без проб.
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
p_1	0,2549	0,1311	0,6274	0,5760	0,2600	0,1562	0,6245	0,5720
p_2	0,3436	0,4295	0,1718	0,2188	0,0889	0,1077	0,1775	0,2147
p_3	0,2561	0,2577	0,1281	0,1312	0,2870	0,2948	0,0799	0,0704
p_4	0,1454	0,1817	0,0727	0,0740	0,3641	0,4413	0,1181	0,1429
H	1,940	1,859	1,513	1,601	1,863	1,805	1,522	1,608

Таблица 6 – Частоты «0» (p_1) и «1» (p_2), а также энтропия H (бит/двоичный символ) двоичного кода при передаче сообщения (с пробелами между словами) по пинг-понг протоколу без плотного кодирования

	Английский		Русский	
	CP-1251	Unicode	CP-1251	Unicode
	1	**2**	**3**	**4**
p_1	0,5548	0,7774	0,4479	0,7554
p_2	0,4452	0,2226	0,5521	0,2446
H	0,991	0,765	0,992	0,803

На рис. 1, 2 приведены зависимости максимальной информации $I_{\max}$ Евы от вероятности d того, что атака будет обнаружена в режиме контроля подслушивания. Кривые 1…5 на этих рисунках построены для пинг-понг протокола с квантовым плотным кодированием и с использованием в режиме контроля подслушивания одного измерительного базиса B_z. Максимальная информация $I_{\max}$ Евы для этого случая определена в (1). Кривая 1 на рис. 1, 2 соответствует одинаковым значениям частот биграмм ($p_1 = p_2 = p_3 = p_4 = 0{,}25$), т. е. случайной последовательности строчных букв, закодированных, например, с использованием равномерного пятибитового кода Бодо. Как видно, в этом случае Ева может получить больше всего информации по сравнению с любым другим распределением частот биграмм. Кривые 2…5 на рис. 1 соответствуют частотам, приведенным в столбцах 1…4 табл. 5. Те же кривые на рис. 2 соответствуют частотам, приведенным в столбцах 5…8 табл. 5.

Максимальная информация Евы для пинг-понг протокола без плотного кодирования определяется выражением [3]:

$$I_{\max} = -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2 , \tag{5}$$

где

$$\lambda_{1,2} = \frac{1}{2} \pm \frac{1}{2} \sqrt{1 - \left(4d - 4d^2\right)\left(1 - \left(p_1 - p_2\right)^2\right)} . \tag{6}$$

Кривые 6, 7 на рис. 1, 2 построены для пинг-понг протокола без плотного кодирования и соответствуют частотам, приведенным в столбцах 1, 2 табл. 6 (рис. 1) и столбцах 3, 4 табл. 6 (рис. 2).

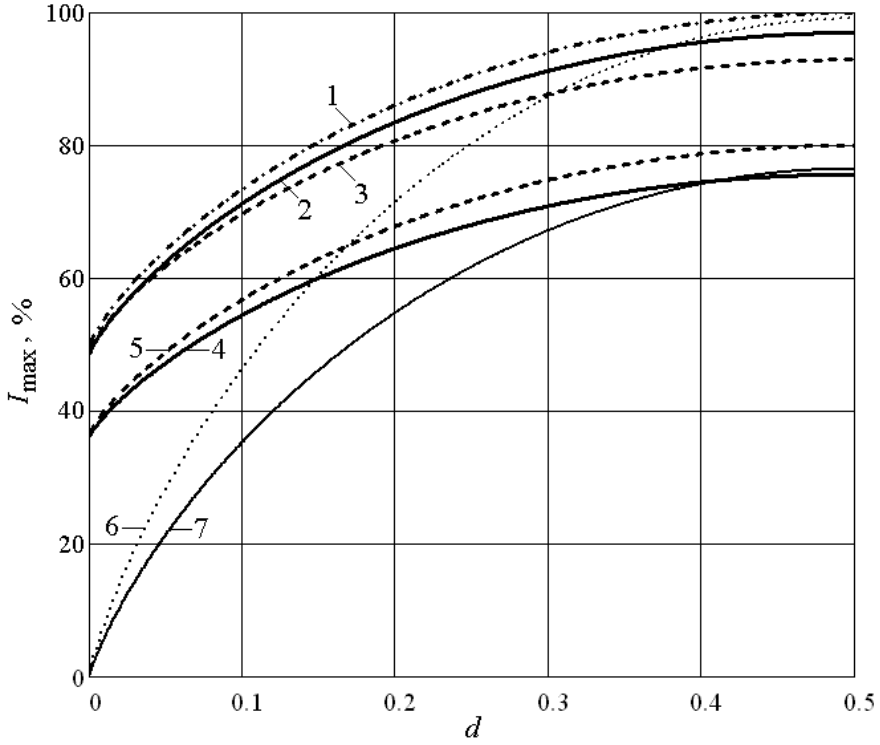

Рисунок 1 – Максимальная информация $I_{\max}$ Евы при передаче сообщения на английском языке (см. текст)

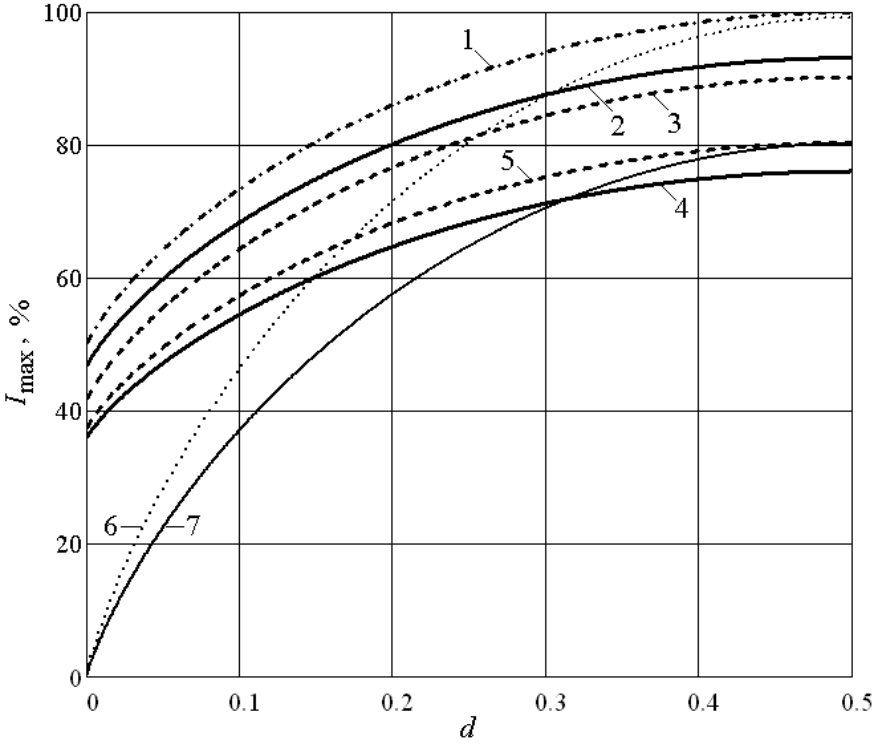

Рисунок 2 – Максимальная информация $I_{\max}$ Евы при передаче сообщения на русском языке (см. текст)

Как видно из табл. 5 и 6, при использовании кодовой таблицы Unicode энтропия двоичного кода существенно меньше, чем при использовании таблицы CP-1251 (что обусловлено преобладанием нулей в кодах как английских, так и русских строчных букв в таблице Unicode). Соответственно и количество информации, которую может получить Ева, существенно меньше при передаче сообщения в кодировке Unicode, чем в кодировке CP-1251 (см. рис. 1, 2).

Удаление из текста сообщения пробелов ненамного меняет количество доступной Еве информации, при этом для кодировки CP-1251 информация Евы уменьшается (сравнить кривые 2 и 3 на рис. 1, 2), а для кодировки Unicode – увеличивается (сравнить кривые 4 и 5 на рис. 1, 2). Это объясняется тем, что энтропия двоичного кода при использовании CP-1251 несколько выше при наличии в исходном тексте пробелов, а для кодировки Unicode ситуация обратная, как для английского, так и для русского текстов (см. табл. 5).

Таким образом, для пинг-понг протокола с квантовым плотным кодированием можно сделать вывод, что чем меньше энтропия двоичного кода, тем меньше информации доступно подслушивающему агенту при фиксированной вероятности его обнаружения *d*. Следовательно, чем меньше будет энтропия двоичного кода, т. е. чем сильнее будут отличаться частоты биграмм при кодировании сообщения, тем быстрее подслушивающий агент будет обнаружен. Аналогичный вывод можно сделать и для пинг-понг протокола без квантового плотного кодирования – из сравнения кривых 6 и 7 на рис. 1, 2 видно, что при использовании кодировки Unicode Ева получит значительно меньше информации, чем при использовании кодировки CP-1251 (в первом случае энтропия двоичного кода значительно меньше, см. табл. 6).

Однако главный недостаток пинг-понг протокола с квантовым плотным кодированием, при использовании в режиме контроля подслушивания только одного измерительного базиса, состоит в том, что Ева может получить достаточно большое количество информации при нулевой вероятности ее обнаружения (см. рис. 1, 2). При $p_1 = p_2 = p_3 = p_4 = 0{,}25$ и $d = 0$ максимальная информация Евы составляет 50%, т. е. каждый первый бит в биграмме будет ей известен. Физически это связано с тем, что если Ева выбрала параметры своей пробы так, чтобы *d* равнялось нулю, то ее последующее измерение не дает возможности отличить состояние $\left|\psi^+\right\rangle$ от состояния $\left|\psi^-\right\rangle$, а также $\left|\varphi^+\right\rangle$ от $\left|\varphi^-\right\rangle$, однако Ева может отличить состояния $\left|\psi^\pm\right\rangle$ от состояний $\left|\varphi^\pm\right\rangle$ [2].

Значения максимальной информации $I_{\max}$ Евы при $d = 0$ для рассмотренных в работе вариантов кодирования сообщений приведены в табл. 7.

Таблица 7 – Максимальная информация $I_{\max}$ Евы при $d = 0$, %

Английский				Русский			
CP-1251		Unicode		CP-1251		Unicode	
с проб.	без проб.	с проб.	без проб.	с проб.	без проб.	с проб.	без проб.
48,6	49,5	36,2	36,6	46,6	41,6	35,9	37,4

Рассмотрим теперь важный вопрос о том, насколько трудным будет для Евы раскрыть передаваемое сообщение, если она выберет стратегию, при которой ее подслушивание не будет обнаружено ($d = 0$).

Как видно из табл. 7, при использовании кодировки CP-1251 максимальная информация Евы близка к 50% для английского текста и немного меньше для русского. Для упрощения анализа будем считать, что $I_{\max} = 50\ \%$, т. е. Ева точно знает значение первого бита в каждой биграмме. Из табл. 3 видно, что второй бит в первой биграмме равен «1» для всех строчных букв английского и русского алфавитов, т. е. этот бит также известен Еве заранее. Следовательно, остается три неизвестных бита – вторые биты во второй, третьей и четвертой биграммах. Таким образом, Ева имеет всего $2^3 = 8$ возможных вариантов расположения бит для каждой буквы. Если в тексте присутствуют пробелы, то Ева достаточно легко сможет отличить их от букв (учитывая, что частота пробела почти в 2 раза больше частоты са́мой употребительной буквы, а код пробела содержит 7 нулей) и, следовательно, будет точно знать длину каждого слова. Для слова из четырех букв нужно будет просмотреть всего $8^4 = 4096$ возможных вариантов расположения бит, а для слова из десяти букв – чуть больше 1 млрд. вариантов. Поскольку средняя длина слова в английском языке составляет 5 букв, а в русском – 5,7 буквы [10], то в среднем для каждого слова Ева будет иметь всего порядка 33000 и 140500 вариантов соответственно. Автоматизированный перебор этих вариантов с использованием словаря, а также известных критериев на осмысленный текст [10] можно выполнить достаточно быстро на современной вычислительной технике. Для этого можно применить алгоритмы, аналогичные алгоритмам раскрытия шифров простой замены [10, 11].

Удаление из текста пробелов несколько затруднит такой криптоанализ, поскольку при неизвестных длинах слов для получения осмысленного текста в среднем потребуется перебрать больше вариантов. Количество вариантов будет также несколько больше вышеприведенного в случае передачи сообщения на русском языке, так как здесь при отсутствии в тексте пробелов $I_{\max} = 41{,}6\ \%$ (см. табл. 7), а не 50 %, как предполагалось при нашем анализе. Однако и в этом случае криптоанализ останется достаточно легким.

Что касается использования кодировки Unicode, то здесь Ева может получить ~ 36 % информации (см. табл. 7), т. е. из 16 бит, кодирующих букву, неизвестными для нее останутся в среднем 10,2 бита. Однако из 16 бит, кодирующих строчную букву, для английского алфавита совпадают первые 11, а для русского – первые 9. Предположим, что Ева знает 1-ый, 4-ый, 7-ый, 10-ый и 13-ый биты (31,3 % информации). Тогда для буквы английского алфавита ей нужно подобрать только 12-ый, 14-ый, 15-ый и 16-ый биты, а для буквы русского – 11-ый, 12-ый, 14-ый, 15-ый и 16-ый биты. Таким образом, Ева будет иметь $2^4 = 16$ вариантов расположения бит для каждой буквы английского и $2^5 = 32$ варианта для каждой буквы русского алфавита, а в среднем для каждого слова $16^5 \approx 10^6$ и $32^{5,7} \approx 3{,}8 \cdot 10^8$ вариантов соответственно. Это существенно больше того количества вариантов, которые нужно проверить для раскрытия текста, передаваемого в кодировке CP-1251. Отметим однако, что, например, в кодовой таблице Unicode для букв русского алфавита (табл. 4) 10-ый и 11-ый биты встречаются только в комбинации «01» или «10», т. е., зная 10-ый бит, Ева сразу может определить 11-ый. Имеются и другие подобные закономерности в кодовых таблицах для отдельных групп букв. При тщательном анализе таких закономерностей и соответствующем их учете при раскрытии сообщения, количество возможных вариантов будет значительно меньше вышеуказанных.

Подытоживая, можно сделать общий вывод, что чем меньше энтропия передаваемого по пинг-понг протоколу двоичного кода, тем меньше информации будет доступно противнику и тем

сложнее будет для него задача раскрытия исходного текста. В частности, использование кодировки Unicode вместо CP-1251 уменьшает энтропию двоичного кода и соответственно делает оба варианта пинг-понг протокола – с квантовым плотным кодированием и без него – более безопасными.

Однако для протокола с квантовым плотным кодированием при использовании в режиме контроля подслушивания одного измерительного базиса, ввиду существования невидимой стратегии подслушивания, использование кодировки Unicode вместо CP-1251 хотя и затрудняет криптоанализ, но отнюдь не делает его невозможным – даже перебор в среднем 380 млн. вариантов расположения бит для каждого слова русского текста не представляет существенной проблемы при использовании в соответствующей программе закономерностей кодовых таблиц, а также словаря и критериев на осмысленный текст.

Следовательно, пинг-понг протокол с квантовым плотным кодированием при использовании в режиме контроля подслушивания одного измерительного базиса нельзя применять для передачи секретных текстов без дополнительных мер по усилению секретности, поскольку подслушивающий агент всегда может выбрать стратегию, при которой подслушивание не будет обнаружено, а раскрытие текста не будет составлять для него большого труда.

2. Метод усиления секретности пинг-понг протокола с квантовым плотным кодированием. Рассмотрим процедуру усиления секретности, применяемую в квантовых протоколах распределения ключа [1, 12]. В этих протоколах Алиса сначала передает Бобу битовую последовательность через квантовый канал. В результате они получают сырой ключ некоторой длины n, а затем согласовывают его, исправляя ошибки. Далее, зная уровень ошибок при передаче сырого ключа, Алиса и Боб определяют величину τ – число битов, на которое надо сократить согласованный ключ, чтобы сделать информацию Евы о ключе ниже заданного малого значения. Затем Алиса генерирует случайную двоичную матрицу K размера $(n-\tau)\times n$ и открыто передает ее Бобу. Конечный секретный ключ (длины $n-\tau$) тогда получается умножением (по модулю 2) матрицы K на согласованный ключ длины n (процедура хеширования). При этом можно строго доказать, что при данном τ информация Евы о ключе будет ниже некоторого определенного значения [12]. Последнее можно выбрать сколь угодно малым (естественно, чем меньше информации должно быть у Евы, тем больше будет τ и, соответственно, тем короче будет конечный секретный ключ).

Описанный выше метод может быть применен и для усиления секретности пинг-понг протокола с квантовым плотным кодированием. Перед передачей Алиса разбивает сообщение на блоки некоторой фиксированной длины n, а затем генерирует случайную двоичную матрицу K (обратимую) размера $n\times n$, умножает эту матрицу на блок сообщения и передает полученную битовую последовательность Бобу по квантовому каналу. Матрица K передается Бобу по обычному открытому каналу, Боб обращает ее и, умножив обратную матрицу на полученную последовательность битов, восстанавливает исходный блок сообщения.

Описанная процедура может быть названа обратимым хешированием или хешированием с использованием двухсторонней хеш-функции, роль которой играет случайная обратимая матрица двоичных чисел. При этом, в отличие от протоколов распределения ключа, блок сообщения нельзя просто сократить, и, соответственно, информацию Евы невозможно сделать сколь угодно малой. Однако поскольку Ева имеет лишь частичную информацию (максимум 50 % в невидимом режиме подслушивания), а умножение на случайную двоичную матрицу сильно увеличит энтропию передаваемого блока сообщения, то восстановление исходного блока будет представлять для Евы достаточно сложную задачу. Отметим, что умножение на случайную матрицу обладает свойством лавинного эффекта – изменение даже одного бита исходного блока сообщения влечет за собой изменение каждого из битов результата умножения с вероятностью, близкой к 0,5.

Вопрос о том, какой длины должны быть блоки сообщения, чтобы в достаточной степени затруднить Еве криптоанализ, требует дополнительных исследований и соответствующего моделирования. Отметим, что такая квантовая криптосистема, использующая пинг-понг протокол с квантовым плотным кодированием и с одним измерительным базисом в режиме контроля подслушивания, а также предложенный метод усиления секретности, будет, в отличие от квантовых протоколов распределения ключа, обладать только вычислительной стойкостью.

В заключение отметим следующее. В работе проведен анализ безопасности пинг-понг протокола для передачи секретных текстовых сообщений, закодированных с помощью таблиц CP-1251 и Unicode, с учетом частот употребления букв в осмысленных английских и русских текстах. Показано, что чем меньше энтропия двоичного кода, тем меньше информации доступно противнику

и тем сложнее для него задача раскрытия исходного текста. В частности, использование кодировки Unicode вместо CP-1251 уменьшает энтропию двоичного кода и, соответственно, делает пинг-понг протокол более безопасным.

Показано, что для пинг-понг протокола с квантовым плотным кодированием и с использованием в режиме контроля подслушивания одного измерительного базиса существует невидимый режим подслушивания, при котором противник может получить почти 50 % информации при использовании легитимными пользователями кодировки CP-1251 и ~36 % при использовании ими Unicode. При этом раскрытие сообщения может быть достаточно легко выполнено противником. Следовательно, пинг-понг протокол с плотным кодированием при использовании в режиме контроля подслушивания одного измерительного базиса нельзя применять для передачи текстовых сообщений без дополнительных мер по усилению секретности. Предложен метод усиления секретности, состоящий в обратимом хешировании блоков сообщения посредством умножения на случайную обратимую двоичную матрицу.

Литература

1. *Баумейстер Д., Экерт А., Цайлингер А*. Физика квантовой информации. – М.: Постмаркет, 2002. – 376 с.
2. *Deng F.-G., Long G.L., Liu X.-S.* Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block // Physical Review A.– 2003.– V. 68. – № 4. – Art. 042317.
3. *Boström K., Felbinger T*. Deterministic Secure Direct Communication Using Entanglement // Physical Review Letters. – 2002. – V. 89, № 18.– Art. 187902.
4. *Cai Q*.-Y., Li B.-W. Improving the capacity of the Boström-Felbinger protocol // Physical Review A.– 2004.– V. 69. – № 5. – Art. 054301.
5. *Wojcik A*. Eavesdropping on the “ping-pong” quantum communication protocol // Physical Review Letters. – 2003. – V. 90. – № 15. – Art. 157901.
6. *Cai Q.-Yu, Li B.-W*. Deterministic Secure Communication Without Using Entanglement // Chinese Physics Letters. – 2004.– V. 21. – № 4. – P. 601–603.
7. *Cai Q*.-Yu. Eavesdropping on the two-way quantum communication protocols with invisible photons // Physics Letters A. – 2006.– V. 351. – № 1–2.– P. 23–25.
8. *Li X.-H., Deng F.-G., Zhou H.-Yu.* Improving the security of secure direct communication based on the secret transmitting order of particles // Physical Review A. – 2006. – V. 74. – № 5.– Art. 054302.
9. *Василиу Е.В.* Анализ безопасности пинг-понг протокола с квантовым плотным кодированием // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.
10. *Бабаш А.В., Шанкин Г.П*. Криптография. – М.: СОЛОН–Р, 2002. – 512 с.
11. *Аграновский А.В., Хади Р.А.* Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН–Пресс, 2002. – 256 с.
12. *Bennett C.H., Brassard G., Crepeau C., Maurer U.M.* Generalized privacy amplification // IEEE Trans. Inform. Theory. – 1995. – V. 41. – № 6. – P. 1915–1923.