ключей. Ситуация не совсем гипотетическая.

Предположим теперь, что получатель информации располагает некоторым программно-аппаратным средством, позволяющим ему временно закрыть канал связи цифровым шумом и компенсировать его при приеме. Он извещает владельца информации о своей готовности и зашумляет канал связи.

Владелец информации осуществляет передачу ключей по зашумленному каналу. По завершении передачи ключей шум выключается и осуществляется передача информации обычным способом по схеме закрытого ключа.

При наличии подобных устройств с обоих концов обмен ключевой информацией может осуществляться двусторонне, причем автоматически.

Реализуется, таким образом, идея криптографической защиты информации с одноразовыми закрытыми ключами. Это – новая и вполне реальная технология.

Список литературы

1.Баранов В.М., Вальков Г.В., Еремеев М.А. и др. Защита информации в системах и средствах связи. Учебное пособие.– Санкт- Петербург: ВИККА имени А.Ф. Можайского. 2007.

2.Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонных каналах.– М.: Энергоатомиздат. 2008.

3.Устройство защиты телефонных линий и помещений от прослушивания 2008.

Поступила 07.01.2009

УДК 003.26:621.39+530.145 **Василиу Е.В., Николаенко С.В.**

БЕЗОПАСНАЯ СИСТЕМА ПРЯМОЙ ПЕРЕДАЧИ СООБЩЕНИЙ НА ОСНОВЕ ПИНГ – ПОНГ ПРОТОКОЛА КВАНТОВОЙ БЕЗОПАСНОЙ СВЯЗИ

Введение

В информационном обществе все большее количество людей испытывают необходимость в конфиденциальной связи. Квантовые коммуникации, основанные на передаче информации, закодированной в отдельных квантовых состояниях, предлагают ряд новых способов для безопасного обмена сообщениями. Например, квантовые протоколы распределения ключей служат для создания секретного ключа, используя который две авторизованные стороны, Алиса и Боб, могут затем обмениваться секретными сообщениями с использованием алгоритмов классической криптографии [1]. Другое направление квантовых коммуникаций – квантовые протоколы безопасной связи (КПБС), в которых секретный ключ вообще не используется, а его роль в некотором смысле играет информационный ресурс квантовой механики – совместно используемые авторизованными пользователями группы перепутанных квантовых частиц [2 – 9]. Секретное сообщение, закодированное с помощью квантовых состояний таких групп кубитов, передается непосредственно через квантовый канал связи (в качестве таких каналов можно использовать существующие оптические каналы). При этом законы квантовой механики гарантируют обнаружение подслушивание в канале, для чего легитимные стороны должны выполнить определенную последовательность квантовых измерений над некоторой частью переданных кубитов. Обнаружив подслушивающего агента, Еву, Алиса и Боб прекращают передачу сообщения.

Большинство предложенных к настоящему времени КПБС требуют передачи кубитов блоками [4 – 8]. Это позволяет обнаружить прослушивание квантового канала до начала передачи самого сообщения и таким способом гарантировать безопасность передачи – если прослушивание обнаружено до передачи сообщения, то Алиса и Боб прерывают передачу и никакая информация не попадает к Еве. Однако, для хранения таких блоков кубитов необходима квантовая память большого объема. Технология квантовой памяти активно разрабатывается в настоящее время, также и в связи с проблемой создания квантовых компьютеров, однако эта технология пока еще далека от массового применения в стандартном телекоммуникационном оборудовании. Поэтому определенным преимуществом обладают протоколы, в которых передача осуществляется одиночными кубитами или небольшими их группами. Таких протоколов предложено немного, главным образом в связи с тем, что они обладают только асимптотической безопасностью, т.е. подслушивающий агент будет обнаружен с высокой вероятностью, однако прежде он сможет получить некоторую часть сообщения. Однако безопасность таких протоколов может быть усилена с применением определенных методов классической (не квантовой) криптографии [10].

Одним из протоколов квантовой безопасной связи, не требующим наличия квантовой памяти большого объема, является пинг – понг протокол [2]. В его первоначальном варианте протокол использует перепутанные пары кубитов (белловские пары) и позволяет передать один бит классической информации за один цикл протокола. Использование квантового сверхплотного кодирования [1] позволяет передать два бита за цикл [3]. Дальнейшее увеличение информационной емкости возможно путем использования вместо перепутанных пар кубитов их троек, четверок и т.д. [9], так как информационная емкость пинг – понг протокола равна n бит на цикл, где n – количество перепутанных кубитов.

Атаки с использованием вспомогательных квантовых систем (проб) на пинг – понг протокол с белловскими парами и сверхплотным кодированием и на пинг – понг протокол с триплетами Гринбергера – Хорна – Цайлингера (ГХЦ) были проанализированы в [4, 11, 12]. Показано, что эти протоколы асимптотически безопасны, как и оригинальный протокол [2]. В [13] получена количественная оценка информации, попадающей к Еве, при различных параметрах вышеназванных протоколов. Основываясь на этих результатах, можно обобщить полученные выражения на пинг –понг протокол с произвольным числом перепутанных кубитов, а затем синтезировать безопасную систему прямой передачи сообщений, основанную на таком протоколе и определенных средствах классической криптографии, как для идеального, так и для шумного квантового канала связи. Это и является целью настоящей работы.

1. Информация Евы при атаке на пинг – понг протокол с n-кубитными ГХЦ – состояниями и вероятность необнаружения атаки

Информация Евы при атаке с использованием квантовой пробы на пинг-понг протокол с перепутанными n-кубитными ГХЦ – состояниями определяется энтропией фон Неймана [2, 11, 12]:

$$I_0 = S(\rho) \equiv -Tr\{\rho \log_2 \rho\} = -\sum_i \lambda_i \log_2 \lambda_i , \qquad (1)$$

где λ_i – собственные значения матрицы плотности ρ системы "передаваемые кубиты – проба".

Для протокола с белловскими парами ($n = 2$) и сверхплотным кодированием матрица плотности имеет размер 4×4 и четыре ненулевых собственных значения [11]:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16 p_1 p_2 d(1-d)};$$

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

где d – вероятность обнаружения атаки легитимными пользователями при однократном переключении в режим контроля подслушивания; p_i – частоты биграмм "00", "01", "10" и "11" в передаваемом сообщении.

Для протокола с ГХЦ – триплетами ($n = 3$) размер матрицы плотности равен 16×16, а ненулевых собственных значений – восемь [12]:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16p_1p_2 \cdot \frac{2}{3}d\left(1 - \frac{2}{3}d\right)};$$

$$\lambda_{7,8} = \frac{1}{2}(p_7 + p_8) \pm \frac{1}{2}\sqrt{(p_7 + p_8)^2 - 16p_7p_8 \cdot \frac{2}{3}d\left(1 - \frac{2}{3}d\right)}, \qquad (3)$$

где p_i – частоты триграмм "000", "001", … в передаваемом сообщении.

Для протокола с ГХЦ – четверками размер матрицы плотности будет уже 64×64, а в общем случае он равен $\left(2^{n-1}\right)^2 \times \left(2^{n-1}\right)^2$, где n – количество перепутанных кубитов в ГХЦ – состоянии. Таким образом, даже вывод матрицы плотности, начиная с $n = 4$, не говоря уже о непосредственном нахождении ее собственных значений, представляет собой очень трудную задачу.

Основываясь на подобии структуры выражений (2) и (3), а также на некоторых аналогиях в процедуре их вывода [11, 12], можно сделать предположения о структуре собственных значений матрицы плотности в общем случае n-кубитных ГХЦ – состояний, используемых в пинг – понг протоколе. А именно, количество ненулевых собственных значений равно 2^n, а их вид:

$$\lambda_{1,2} = \frac{1}{2}(p_1 + p_2) \pm \frac{1}{2}\sqrt{(p_1 + p_2)^2 - 16p_1p_2 \cdot \frac{2^{n-2}}{2^{n-1} - 1}d\left(1 - \frac{2^{n-2}}{2^{n-1} - 1}d\right)};$$

$$\lambda_{2^n-1,\,2^n} = \frac{1}{2}\left(p_{2^n-1} + p_{2^n}\right) \pm \frac{1}{2}\sqrt{\left(p_{2^n-1} + p_{2^n}\right)^2 - 16p_{2^n-1}p_{2^n} \cdot \frac{2^{n-2}}{2^{n-1} - 1}d\left(1 - \frac{2^{n-2}}{2^{n-1} - 1}d\right)}. \qquad (4)$$

Проверка правильности выражений (4) может быть выполнена следующим образом. Полную информацию Ева получает при максимальной вероятности обнаружения атаки $d_{\max}$. Основываясь на результатах работ [11, 12], для $d_{\max}$ получена следующая формула:

$$d_{\max} = 1 - \frac{1}{2^{n-1}}. \qquad (5)$$

Полная информация Евы I_0 (1), с подстановкой в это выражение собственных значений (4) при $d = d_{\max}$ и некоторых значениях p_i, должна равняться энтропии источника сообщения при тех же p_i, где энтропия определяется формулой:

$$H = -\sum_{i=1}^{2^n} p_i \log_2 p_i. \qquad (6)$$

Проведена проверка равенства выражений (1) и (6) для $n = 4$, $n = 5$ и десяти различных наборов p_i для каждого n, которая показала, что при $d = d_{\max}$ эти выражения равны при всех взятых для проверки наборах p_i. Таким образом, выражения для собственных значений (4), выведенные не путем прямого расчета, а путем анализа структуры соответствующих выражений для $n = 2$ и $n = 3$, являются правильными.

При одинаковых значениях частот n-грамм $p_1 = \ldots = p_{2^n} = 2^{-n}$ выражения (4) принимают следующий вид:

$$\lambda_{1,2} = \ldots = \lambda_{2^n-1,2^n} = \frac{1}{2^n} \pm \frac{1}{2}\sqrt{\frac{1}{2^{2n-2}} - \frac{1}{2^{2n-4}} \cdot \frac{2^{n-2}}{2^{n-1}-1} d\left(1 - \frac{2^{n-2}}{2^{n-1}-1} d\right)}. \qquad (7)$$

Вероятность того, что Ева не будет обнаружена после m успешных атак и получит информацию $I = m I_0$, определяется выражением [2]:

$$s(I, c, d) = \left(\frac{1-c}{1-c(1-d)}\right)^{\frac{I}{I_0}}, \qquad (8)$$

где c – вероятность переключения в режим контроля подслушивания, I_0 определено в (1).

На рис. 1 показаны зависимости $s(I, c, d)$ для различных n, одинаковых частот $p_i = 2^{-n}$, $c = 0.5$ и $d = d_{\max}$ (5). Видно, что информационная емкость и безопасность различных вариантов пинг – понг протокола находятся в обратно пропорциональной зависимости, если говорить о количестве информации I, которую может получить Ева при определенной полной вероятности s необнаружения перехвата. Такой результат закономерен, так как чем больше n, тем больше информации передается за один цикл протокола и тем больше информации дает Еве каждая атакующая операция. Однако вероятность необнаружения убывает экспоненциально с ростом перехваченной информации при любом n. Таким образом, пинг – понг протокол с многокубитными ГХЦ – состояниями является асимптотически безопасным при любом количестве кубитов n, образующих перепутанное ГХЦ – состояние.

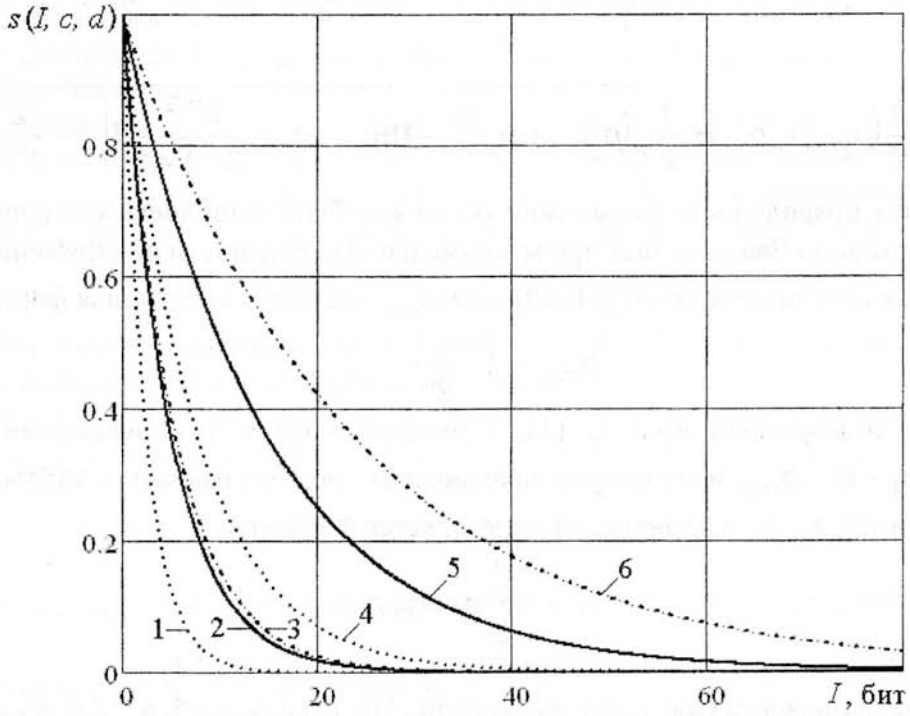

Рис. 1. Полная вероятность необнаружения подслушивания s для пинг – понг протокола с многокубитными ГХЦ – состояниями: $n = 2$, оригинальный протокол (1); $n = 2$, с плотным кодированием (2); $n = 3$ (3); $n = 5$ (4); $n = 10$ (5); $n = 16$ (6).

2. Способ усиления безопасности пинг – понг протокола

Как следует из результатов предыдущего раздела, Ева может получить некоторую информацию, прежде чем будет обнаружена, причем количество этой информации растет с увеличением количества используемых в протоколе перепутанных кубитов. Следовательно, для практического использования протокола необходим способ, который сделает полученную Евой информацию бесполезной для нее. Такой способ может быть разработан на основе метода усиления секретности, применяемого в квантовых протоколах распределения ключей [1, 10]. В данном случае этот способ будет представлять собой некоторую аналогию шифра Хилла.

Перед передачей Алиса разбивает свое двоичное сообщение на q блоков некоторой фиксированной длины r, обозначим эти блоки через a_i $(i = 1,\ldots q)$, затем генерирует для каждого блока *отдельно* случайную *обратимую* двоичную матрицу K_i размера $r \times r$ и умножает полученные матрицы на соответствующие блоки сообщения (умножение выполняется по модулю 2):

$$b_i = K_i a_i . \qquad (9)$$

Полученные в результате блоки b_i, передаются по квантовому каналу с использованием пинг – понг протокола. Даже если Еве удастся перехватить один (или несколько) из этих блоков, оставшись не обнаруженной, то, не зная использованных матриц K_i, Ева не может восстановить исходные блоки a_i. Для обеспечения достаточного уровня безопасности длина блока r и соответственно размер матриц K_i должны выбираться так, чтобы вероятность необнаружения Евы s (8) после передачи *одного* блока была пренебрежимо малой величиной. Матрицы K_i передаются Бобу по обычному открытому каналу после завершения квантовой передачи, но только в том случае, если Алиса и Боб убедились в отсутствии подслушивания. Затем Боб обращает полученные матрицы и, умножив их на соответствующие блоки b_i, восстанавливает исходное сообщение:

$$a_i = K_i^{-1} b_i . \qquad (10)$$

Отметим, что описанная процедура не является шифрованием сообщения, а может быть названа обратимым хешированием или хешированием с использованием двухсторонней хеш – функции, роль которой играет случайная обратимая матрица двоичных чисел.

Для каждого блока должна использоваться своя матрица K_i, что позволит предотвратить криптоаналитические атаки, подобные атакам на шифр Хилла, которые возможны там при многократном использовании одной матрицы для шифрования разных блоков (подобную атаку Ева могла бы провести, если бы ей удалось до обнаружения ее операций в квантовом канале перехватить несколько блоков, хешированных с одной и той же матрицей). Поскольку матрицы в данном случае не являются ключом и их можно передавать по открытому классическому каналу, передача нужного количества матриц не представляет проблемы.

Рассмотрим теперь вопрос о выборе необходимой длины блока r. Как видно из рис. 1 эта величина будет зависеть от количества n используемых в протоколе перепутанных кубитов – чем больше n, тем больше должна быть длина r блока для обеспечения того же уровня безопасности. Конкретное значение r может быть вычислено с использованием (8) при заданном n и заданной вероятности необнаружения Евы s. Однако сама величина s зависит от параметров c и d.

Величину c – вероятность переключения в режим контроля подслушивания – выбирают легитимные пользователи. Чем больше c, тем быстрее атака Евы будет обнаружена, однако тем меньше будет общая эффективность протокола, так как чем чаще Алиса и Боб переключаются в

режим контроля подслушивания, тем реже они передают сами биты сообщения. На наш взгляд, вполне разумным выбором будет $c = 0.5$.

Величину d – вероятность обнаружения атаки при однократном выполнении контроля подслушивания – может регулировать Ева, выбирая соответствующим образом параметры своих квантовых проб, используемых для атаки. Однако чем меньше d, тем меньше информация Евы в любом варианте пинг – понг протокола [2, 11, 12]. Таким образом, уменьшив d, Ева сможет определить правильно только некоторые передаваемые биты, причем она не будет даже точно знать, какие именно биты определены правильно. Это значительно затруднит Еве определение исходных блоков сообщения a_i, даже если она останется необнаруженной и узнает соответствующие им матрицы K_i. Таким образом, при определении длины r блока будем полагать, что Ева стремится получить полную информацию, это соответствует максимальной вероятности ее обнаружения $d_{\max}$ (5). Вопрос о том, насколько сделанное предположение может повлиять на безопасность и повлияет ли оно вообще, требует дополнительного исследования, такое исследование будет выполнено в отдельной работе.

Остановимся теперь кратко на вопросе выбора двоичных матриц K_i. Эти матрицы должны быть случайными и обратимыми. Следовательно, Алиса должна генерировать случайную матрицу, проверять ее на обратимость в двоичном поле Галуа GF(2) и, в случае успеха, принимать матрицу. Поэтому возникает вопрос о вероятности того, что сгенерированная случайным образом двоичная матрица является обратимой. Эта вероятность была вычислена в [14] и для матриц в GF(2) при $r \geq 16$ становится константой, равной 0.289. Таким образом, в среднем почти каждая третья из случайно сгенерированных двоичных матриц при $r \geq 16$ будет обратимой, что вполне приемлемо.

Доля же инволютивных двоичных матриц, т.е. матриц, равных своей обратной, по отношению ко всем двоичным матрицам размера $r \times r$ при $r = 16$ составляет $\sim 4.9 \cdot 10^{-39}$, а при $r = 32$ составляет $\sim 1.3 \cdot 10^{-154}$ и продолжает уменьшаться с ростом r [14]. Следовательно, генерация случайных матриц с проверкой их на инволютивность смысла не имеет. Псевдослучайные инволютивные матрицы в принципе можно конструировать [15], однако вопрос о том, какая операция быстрее – генерация случайной матрицы и ее проверка на обратимость или конструирование псевдослучайной инволютивной матрицы, требует дополнительных исследований, и мы пока оставим этот вопрос в стороне. Будем считать, что легитимные пользователи используют для усиления безопасности пинг – понг протокола случайные обратимые матрицы.

Следует сделать также следующее замечание. Предложенный метод усиления безопасности пинг – понг протокола не требует наличия у легитимных пользователей никаких предустановленных ключей – в отличие от шифра Хилла матрицы здесь не являются ключом и передаются открыто, если Алиса и Боб убедились в отсутствие подслушивания в квантовом канале, а последнее обеспечивается методами квантовой механики. Таким образом, основное преимущество квантовых протоколов безопасной связи, а именно отсутствие необходимости распределять ключи (за исключением небольшого ключа для аутентификации, см. след. раздел), сохраняется при использовании предложенного метода.

3. Безопасная система прямой передачи сообщений в идеальном квантовом канале на основе пинг – понг протокола с ГХЦ – триплетами

Синтезируем теперь безопасную систему передачи сообщений от Алисы к Бобу, основанную на пинг – понг протоколе и использующую предложенный выше метод усиления безопасности. В качестве базового протокола выберем пинг – понг протокол с ГХЦ – триплетами.

Существует восемь полностью перепутанных ортонормированных ГХЦ –состояний триплета кубитов $|\Psi_1\rangle \ldots |\Psi_8\rangle$ (табл. 1), которые образуют базис в гильбертовом пространстве трех кубитов и соответственно могут быть точно различены соответствующим измерением. Таким образом, выполнив измерение, Боб получит один из восьми возможных вариантов, что соответствует трем битам информации.

Состояния $|\Psi_1\rangle \ldots |\Psi_8\rangle$ могут быть трансформированы одно в другое применением однокубитных унитарных операторов к любым двум из трех кубитов. Считая, что начальным состоянием является $|\Psi_1\rangle$, можно построить набор унитарных операторов, которые преобразуют $|\Psi_1\rangle$ в $|\Psi_1\rangle \ldots |\Psi_8\rangle$ соответственно и действуют на первые два кубита (на третий кубит всегда будет действовать тождественный оператор). Эти операторы, а также трехбитовые строки, соответствующие каждому из состояний $|\Psi_1\rangle \ldots |\Psi_8\rangle$, приведены в табл. 1 [9].

Таблица 1

Унитарные операторы преобразования состояния $|\Psi_1\rangle$ в состояния $|\Psi_1\rangle \ldots |\Psi_8\rangle$

k	Состояние	Оператор $\|\Psi_1\rangle \to \|\Psi_k\rangle$	Строка
1	$\|\Psi_1\rangle = (\|000\rangle + \|111\rangle)/\sqrt{2}$	$T \otimes T \otimes T$	000
2	$\|\Psi_2\rangle = (\|000\rangle - \|111\rangle)/\sqrt{2}$	$T \otimes \sigma_z \otimes T$	001
3	$\|\Psi_3\rangle = (\|100\rangle + \|011\rangle)/\sqrt{2}$	$\sigma_x \otimes T \otimes T$	010
4	$\|\Psi_4\rangle = (\|100\rangle - \|011\rangle)/\sqrt{2}$	$i\sigma_y \otimes T \otimes T$	011
5	$\|\Psi_5\rangle = (\|010\rangle + \|101\rangle)/\sqrt{2}$	$T \otimes \sigma_x \otimes T$	100
6	$\|\Psi_6\rangle = (\|010\rangle - \|101\rangle)/\sqrt{2}$	$T \otimes i\sigma_y \otimes T$	101
7	$\|\Psi_7\rangle = (\|110\rangle + \|001\rangle)/\sqrt{2}$	$\sigma_x \otimes \sigma_x \otimes T$	110
8	$\|\Psi_8\rangle = (\|110\rangle - \|001\rangle)/\sqrt{2}$	$i\sigma_y \otimes \sigma_x \otimes T$	111

В табл. 1 $T = |0\rangle\langle 0| + |1\rangle\langle 1|$ – тождественный оператор; $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ и $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ – операторы Паули.

Пинг – понг протокол требует наличия, кроме квантового канала для передачи кубитов, также и классического канала для обмена сообщениями в режиме контроля подслушивания [2, 9 – 12]. Этот классический канал может быть открытым для пассивного прослушивания и нет необходимости шифровать передаваемые по этому каналу сообщения. Однако Ева не должна иметь возможность изменять передаваемые в классическом канале сообщения, иначе, контролируя также и квантовый канал, она может провести атаку "человек в середине". В случае же, если Ева может лишь пассивно прослушивать классический канал, ее операции над передаваемыми кубитами в квантовом канале будут обязательно обнаружены.

Таким образом, легитимные пользователи нуждаются в аутентификации сообщений, передаваемых по классическому каналу в режиме контроля подслушивания. Высокий уровень безопасности обеспечивает аутентификация сообщений по алгоритму *HMAC* с функцией хеширования *SHA*, выдающей строку длиной 256 бит (*SHA*–256), когда код аутентичности сообщения вычисляется по формуле [16]:

$$HMAC = SHA((K \oplus a) \| SHA((K \oplus b) \| m)), \quad (11)$$

где K – общий секретный ключ, который Алиса и Боба должны иметь до начала протокола; a и b – некоторые константы, также известные Алисе и Бобу; m – сообщение; $\|$ – операция конкатенации строк.

Само сообщение, передаваемое по квантовому каналу, также может быть снабжено кодом аутентичности, вычисленным по (11).

Опишем теперь детально безопасную систему прямой передачи сообщений от Алисы к Бобу в идеальном квантовом канале.

Предварительная подготовка. Алиса подготавливает свое сообщение M в виде битовой строки, вычисляет его код аутентичности по (11) и формирует строку $M \| HMAC$. Затем Алиса вычисляет необходимую длину r блока, используя (8) и задавшись желаемой вероятностью необнаружения Евы. Например, пусть $s = 10^{-6}$. Согласно (8), для протокола с ГХЦ – триплетами при $c = 0.5$ и $d = d_{\max} = 0.75$ количество полученной Евой информации будет $I \approx 74$ бита. Тогда r можно выбрать как ближайшее сверху кратное трем число, т.е. 75 бит. Затем Алиса разбивает сообщение $M \| HMAC$ на блоки по 75 бит (если последний блок меньше 75 бит, то он дополняется случайными числами), генерирует необходимое количество обратимых двоичных матриц и умножает их на блоки сообщения согласно (9). После этого Алиса разбивает полученные блоки b_i на триграммы – строки по три бита.

Шаг 1. Боб приготавливает три кубита в состоянии $|\Psi_1\rangle$.

Шаг 2. Он оставляет у себя третий кубит и посылает Алисе первые два по квантовому каналу связи.

Шаг 3. Алиса получает два кубита от Боба. С вероятностью $c = 0.5$ она переключается в режим контроля подслушивания и выполняет шаг 4, иначе Алиса переключается в режим передачи сообщения и выполняются шаги, начиная с 5-го.

Шаг 4. Алиса посылает сообщение Бобу по классическому каналу о переключении в режим контроля подслушивания (к сообщению добавляется код аутентичности). Получив сообщение и проверив его аутентичность, Боб случайным образом выбирает один из двух измерительных базисов – $B_z = \{|0\rangle\langle 0|; |1\rangle\langle 1|\}$ или $B_x = \{|+\rangle\langle +|; |-\rangle\langle -|\}$, где $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, а затем выполняет измерение состояния своего кубита в выбранном базисе.

В результате измерения в базисе B_z Боб получит $|0\rangle$ с вероятностью $1/2$, а состояние триплета после измерения будет $|000\rangle$. Тогда Боб сообщает Алисе по классическому каналу, что он выбрал базис B_z, а также сообщает результат своего измерения. Алиса выполняет измерения состояний своих двух кубитов также в базисе B_z, при этом ее результат должен быть $|0\rangle$, $|0\rangle$. С вероятностью $1/2$ Боб получит результат $|1\rangle$ и состояние триплета будет $|111\rangle$. Тогда Алиса, выполнив измерения в том же базисе, должна получить $|1\rangle$, $|1\rangle$. Если же результаты Алисы отличаются от приведенных, то в идеальном квантовом канале это свидетельствует о вмешательстве Евы. Тогда Алиса и Боб делают вывод о наличии подслушивания и прерывают передачу. Если же результаты измерений Алисы правильные, то переход к шагу 1.

Аналогично, если Боб выбирает базис B_x, то он с вероятностью $1/2$ получит $|+\rangle$ и состояние триплета будет $|\Psi^+\rangle \otimes |+\rangle$, или Боб получит $|-\rangle$ и состояние триплета будет $|\Psi^-\rangle \otimes |-\rangle$, где $|\Psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ и $|\Psi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ – два из состояний Белла.

Тогда после получения сообщения от Боба о выбранном базисе и результате измерения Алиса измеряет два своих кубита в базисе Белла и в первом случае должна получить $|\Psi^+\rangle$, а во втором $|\Psi^-\rangle$. Если это не так, то протокол прерывается, иначе переход к шагу 1. Подчеркнем еще раз, что все сообщения, которыми обмениваются Алиса и Боб в режиме контроля подслушивания, должны снабжаться кодами аутентичности, что позволит предотвратить атаку "человек в середине".

Отметим также, что использование двух базисов для контроля подслушивания необходимо по причине того, что в противном случае, т.е. при использовании только одного измерительного базиса, Ева имеет возможность провести не обнаруживаемую атаку на пинг – понг протокол [11, 12].

Шаг 5. В соответствие со своей текущей триграммой, Алиса выбирает одну из восьми кодирующих операций (см. табл. 1), выполняет эту операцию над двумя своими кубитами, а затем отправляет эти кубиты обратно Бобу по квантовому каналу.

Шаг 6. Получив кубиты от Алисы, Боб выполняет измерение над всеми тремя кубитами в ГХЦ – базисе, что позволяет ему достоверно определить состояние, созданное кодирующей операцией Алисы, и тем самым определить трехбитовую строку, которую она послала. ГХЦ – базис представляет собой набор из восьми операторов: $GHZ = \{|\Psi_k\rangle\langle\Psi_k|\}$, где $k = 1\ldots8$.

Шаг 7. Если сообщение передано полностью, то переход к шагу 8, иначе переход к шагу 1.

Шаг 8. Алиса передает Бобу по открытому каналу матрицы K_i, поскольку подслушивания нет, иначе протокол был бы прерван на шаге 4.

Шаг 9. Боб обращает матрицы и восстанавливает исходное сообщение M согласно (10), затем проверяет его код аутентичности и при правильном результате протокол успешно закончен, иначе сообщение отвергается, и протокол должен быть выполнен снова.

При использовании в протоколе вместо триплетов перепутанных кубитов большего их количества, описанный порядок действий меняется только в тех шагах, которые от этого зависят. Так, длина r блока должна быть кратна количеству кубитов n в группе. На шаге 1 один вместо трехкубитного ГХЦ – состояния $|\Psi_1\rangle$ Боб готовит соответствующее n – кубитное ГХЦ – состояние:

$$|\Psi_1\rangle = \left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)/\sqrt{2}. \qquad (12)$$

Естественно, меняются также кодирующие операции Алисы, представленные в табл. 1 для протокола с триплетами. Еще одно изменение – операции, выполняемые при контроле подслушивания (шаг 4). В работе [9] представлены все эти составляющие для пинг – понг протокола с четырехкубитными ГХЦ – состояниями. Аналогичным образом они могут быть получены для протокола с любым количеством кубитов. Отметим, что в настоящее время в эксперименте достигнуто перепутывание группы из 10 кубитов [17], так что реализация пинг – понг протокола с группой до 10 перепутанных кубитов находится в пределах возможностей современных технологий.

4. Модификация системы безопасной передачи сообщений для шумного квантового канала связи

В случае шумного канала, очевидно, Алиса и Боб не могут прервать протокол сразу же после возникновения первой ошибки в режиме контроля подслушивания, поскольку такая ошибка может быть вызвана естественным шумом в канале, а не подслушиванием. В шумном канале Алиса должна сначала передать некоторое количество хешированных

блоков, достаточное для того, чтобы можно было сделать статистически значимую оценку уровня ошибок, которые регистрируются в режиме контроля подслушивания. Затем эта оценка сравнивается с известным заранее граничным значением естественного уровня помех в данном квантовом канале. Если сделанная оценка уровня ошибок превышает допустимое граничное значение, то протокол прерывается, так как это превышение приписывается подслушиванию Евы, иначе передается следующая последовательность блоков и снова выполняется оценка уровня ошибок. Матрицы K_i передаются все сразу только после успешного завершения квантовой передачи.

Отметим также, что в квантовом канале с шумом ошибки будут возникать, конечно, не только в режиме контроля подслушивания, но и при передаче самих блоков сообщения. Поэтому здесь необходимо применение помехоустойчивых кодов. Это могут быть квантовые коды исправления ошибок [1]. Однако пинг – понг протокол предназначен для передачи *классической информации по квантовому каналу*, поэтому в данном случае могут применяться и классические помехоустойчивые коды, что в настоящее время, на наш взгляд, является более простым и эффективным решением.

Заключение

В работе получено общее выражения для информации подслушивающего агента при атаке на пинг – понг протокол с многокубитными перепутанными ГХЦ – состояниями. Вычислена полная вероятность необнаружения подслушивания. Синтезирована безопасная система передачи сообщений, основанная на протоколе с ГХЦ – триплетами и использующая усиление безопасности протокола путем обратимого хеширования блоков сообщения. Рассмотрены необходимые модификации системы безопасной передачи сообщений для шумного квантового канала.

В дальнейшем необходимо рассмотреть еще ряд вопросов, касающихся предложенной системы безопасной передачи сообщений. Так необходимо выяснить, как может повлиять на безопасность стратегия атаки, при которой Ева уменьшает вероятность обнаружения атаки за счет уменьшения доступной ей в квантовом канале информации. Также необходимо построить эффективные коды исправления ошибок, учитывающие специфику пинг – понг протокола, а именно то, что при передаче в шумном квантовом канале будут возникать пакеты ошибок, длина которых будет равна количеству используемых в протоколе перепутанных кубитов.

Список литературы

1. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. – Москва: Мир, 2006.

2. *Bostrom K., Felbinger T.* Deterministic secure direct communication using entanglement // Physical Review Letters. – 2002. – V. 89, № 18. – Art. 187902.

3. *Cai Q.-Y., Li B.-W.* Improving the capacity of the Bostrom – Felbinger protocol // Physical Review A. – 2004. – V. 69, № 5. – Art. 054301.

4. *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.

5. *Wang Ch., Deng F.G., Long G.L.* Multi – step quantum secure direct communication using multi – particle Greenberger – Horne – Zeilinger state // Optics Communications.– 2005. – V. 253, № 1. – P. 15 – 20.

6. *Wang J., Zhang Q., Tang C.J.* Multiparty controlled quantum secure direct communication using Greenberger – Horne – Zeilinger state // Optics Communications. – 2006. – V. 266, № 2. – P. 732 – 737.

7. *Multiparty* Quantum Remote Secret Conference / Li X.-H., Li C.-Y., Deng F.-G. et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23 – 26.

8. *Three-party* quantum secure direct communication based on GHZ states / Jin X.-R., Ji X., Zhang Y.-Q. et al // Physics Letters A. – 2006. – V. 354, № 1-2. – P. 67 – 70.

9. *Василиу Е.В., Василиу Л.Н.* Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171 – 176.

10. *Василиу Е.В.* Безопасность пинг – понг протокола квантовой связи для передачи текстовых сообщений // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 2. – С. 36 – 44.

11. *Василиу Е.В.* Анализ безопасности пинг – понг протокола с квантовым плотным кодированием // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32 – 38.

12. *Василиу Е.В.* Анализ атаки на пинг – понг протокол с триплетами Гринбергера – Хорна - Цайлингера // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 15 – 24.

13. *Василиу Е.В., Василиу Л.Н.* Оценка количества информации, попадающей к злоумышленнику, для трех вариантов пинг-понг протокола квантовой безопасной связи // Материали за IV международна научна практична конференция «Научно пространство на Европа – 2008», 15 – 30 апреля 2008 г. – София, «Бял ГРАД-БГ» ООД. – Т. 29. – С. 34 – 40.

14. *Overbey, J., Traves, W., Wojdylo, J.* On the keyspace of the Hill cipher // Cryptologia.– 2005. – V. 29, № 1. – P. 59 – 72.

15. *Levine J., Nahikian H.M.* On the Construction of Involutory Matrices // American Mathematical Monthly. – 1962. – V. 69, № 4. – P. 267 – 272.

16. *Фергюсон Н., Шнайер Б.* Практическая криптография: Пер. с англ. – М.: Изд. дом "Вильямс", 2005. – 424 с.

17. *Experimental* demonstration of a hyper – entangled ten – qubit Schrodinger cat state / Gao W.-B, Lu C.-Y., Yao X.-C. et al // [Электронный ресурс] http://arxiv.org/abs/0809.4277.

Поступила 22.12.2008

УДК 519.676:681.51 **Блавацкая Н.Н.**

ОПТИМИЗАЦИЯ АДАПТИВНОСТИ МЕТОДОВ СЖАТИЯ ИНФОРМАЦИИ

Наилучших на сегодняшний день результатов по степени сжатия информации позволяют достичь методы вероятностного моделирования информационного источника. Преимущество методов данной группы особенно заметно при сжатии текстов, где они являются признанными лидерами.

Однако в последние несколько лет лидирующее положение методов группы моделирования источника с учетом контекстуальных зависимостей (ММКЗ) несколько пошатнулось по причине изобретения блочно-сортирующих преобразований BW94 и ST [1,2,3], которые тоже фактически используют контекстуальные зависимости, но без построения вероятностной модели источника, а также появления новых разновидностей словарных методов сжатия (таких как LZP, оптимальное LZ –кодирование). Упомянутые методы позволяют достичь сравнимой с контекстуальными методами степени сжатия при заметно лучшем быстродействии.

Рассмотрим процесс сжатия информации методом группы ММКЗ. Он разбивается на 2 этапа – моделирования и кодирование. Структурная схема таких методов приведена на рис.1.

Моделировщик строит статистическую модель входного потока. Модель источника в схеме ММКЗ строится следующим образом.