УДК 004.056.53+530.145

УСИЛЕНИЕ БЕЗОПАСНОСТИ МЕТОДОМ ГАММИРОВАНИЯ ПРОТОКОЛА КВАНТОВОЙ ПРЯМОЙ БЕЗОПАСНОЙ СВЯЗИ

С.В. НИКОЛАЕНКО

В статье рассматривается классический (не квантовый) способ усиления безопасности пинг-понг протокола с парами перепутанных кубитов. Этот способ заключается в шифровании методом гаммирования блоков сообщений и позволяет обеспечить достаточно высокий уровень безопасности протокола. При этом сами гаммы не являются секретной информацией и передаются открытым каналом только после того, как легитимные пользователи убедились в отсутствии атаки в квантовом канале. Разработана имитационная модель пинг-понг протокола с парами перепутанных кубитов в квантовом канале с использованием шифрования методом гаммирования. Выполнен расчет необходимых для обеспечения заданного уровня безопасности длин блоков сообщения в зависимости от параметров протокола и параметров атакующей операции злоумышленника, а также соответствующий расчет необходимых размеров случайных гамм. Выполнены оценки вычислительной сложности генерации гамм для данного метода усиления безопасности. Показано, что время генерации является приемлемым для гамм размером около 2000 бит при использовании вычислительной техники с невысоким быстродействием.

Ключевые слова: квантовая криптография, пинг-понг протокол, метод усиления безопасности протокола, шифрования методом гаммирования, имитационное моделирование, временные оценки.

ВВЕДЕНИЕ

В современном мире передача конфиденциальных данных между несколькими абонентами в сетях связи может привести не только к потере передаваемой информации, но и к ее компрометации, т.е. разглашению информации, которая становится известной кому-либо, кто не имеет права доступа к ней. В последнее десятилетие активно развивается новое направление защиты информации – квантовая криптография. В отличие от криптографических методов, безопасность которых основывается на недоказанных математических утверждениях, безопасность квантовой криптографии основана на законах квантовой физики, а для переноса информации используются объекты квантовой механики. Такими объектами могут быть фотоны в линиях волоконно-оптической связи. Квантовые явления, используемые в целях криптографической защиты информации, позволяют создать такую систему защиты, при которой любое подслушивания обнаруживается с высокой степенью достоверности. Попытка подслушивания приводит к возмущению исходного состояния квантовой системы, поскольку невозможно измерить хотя бы одну характеристику фотона, не нарушив и не исказив другие.

Одним из направлений квантовой криптографии являются протоколы квантовой прямой безопасной связи (КПБС), которые позволяют передавать конфиденциальные сообщения непосредственно по квантовому каналу, т.е. без использования шифрования. В настоящее время предложено большое количество различных по назначению протоколов КПБС [1-7]. Одним из таких протоколов, который не нуждается в квантовой памяти большого объема, является пинг-понг протокол с парами перепутанных кубитов и без использования квантового сверхплотного кодирования, который позволяет передать один бит классической информации за один цикл протокола [1].

Пинг-понг протокол является одним из простых протоколов КПБС, который может быть реализован с использованием современных технологий квантовой информатики [8]. В настоящее время существуют различные варианты этого протокола [1, 2, 6, 7], но не до конца исследована их стойкость к различным атакам злоумышленника. Поскольку пинг-понг протокол предназначен для безопасной передачи классической информации квантовыми каналами связи, то существует возможность использования классических методов защиты информации для усиления безопасности пинг-понг протокола и других КПБС.

В настоящее время существует большое количество классических методов усиления безопасности протоколов передачи данных [9–12], которые надежно защищают данные от вмешательства и могут быть применены для защиты от злоумышленников информации, передаваемой с помощью квантовых пинг-понг протоколов. Одним из таких актуальных и криптографически гарантированных методов защиты информации является метод гаммирования. Однако, если оценки надежности и скорости метода гаммирования для пинг-понг протокола с парами перепутанными кутритов частично выполнялись ранее [13], то для пинг-понг протоколов с группами перепутанных кубитов таких оценок раньше вообще не проводилось.

Целью настоящей работы является усиление безопасности пинг-понг протокола с парами перепутанных кубитов с помощью метода гаммирования.

1. МЕТОД УСИЛЕНИЯ БЕЗОПАСНОСТИ ПИНГ-ПОНГ ПРОТОКОЛА С ПАРАМИ ПЕРЕПУТАННЫХ КУБИТОВ С ПОМОЩЬЮ ГАММИРОВАНИЯ

Пинг-понг протокол является двусторонним протоколом квантовой безопасной связи – для передачи сообщения от одного абонента (Алисы) к другому абоненту (Бобу) кубит пересылается сначала от Боба к Алисе, а затем обратно от Алисы к Бобу. В пинг-понг протоколе применяются два режима – режим передачи самого сообщения и режим контроля подслушивания, необходимый для обнаружения атаки пассивного перехвата. Алиса и Боб чередуют эти режимы случайным образом. Атака обнаруживается с некоторой вероятностью в режиме контроля подслушивания.

Для усиления безопасности пинг-понг протоколов можно применять метод гаммирования [9]. Идея этого метода состоит в следующем.

Перед передачей Алиса разбивает свое двоичное сообщение на l блоков некоторой фиксированной длины r, обозначим эти блоки через a_i ($i = 1,...l$), затем генерирует для каждого блока отдельно случайную двоичную гамму γ_i размером r и складывает полученные гаммы с соответствующими блоками сообщения: $b_i = a_i + \gamma_i$.

Полученные в результате блоки b_i передаются по квантовому каналу с использованием пинг-понг протокола. Даже если подслушивающему агенту (Еве) удастся перехватить один (или несколько) из этих блоков, оставшись не обнаруженной, то, не зная использованных гамм γ_i, Ева не может восстановить исходные блоки a_i. Для обеспечения достаточного уровня безопасности длина блока r и соответственно размер гамм γ_i должны выбираться так, чтобы вероятность необнаружения Евы после передачи одного блока была пренебрежимо малой величиной.

Гаммы γ_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 складывает их с соответствующими блоками b_i и восстанавливает исходное сообщение: $a_i = b_i + \gamma_i$.

В соответствии с вышеизложенным методом усиления безопасности пинг-понг протоколов, для имитационного моделирования протокола с парами перепутанных кубитов разработан алгоритм последовательности действий, который состоит в следующем.

Шаг 1. Сообщение разбивается на l блоков a_i заданной длины r. Длина блока определяется из условия того, что вероятность необнаружения атаки после передачи одного блока не превышает заданную величину 10^{-k} [7]:

$$r \geq I = \frac{-kI_0}{\lg((1-q)/(1-q\cdot(1-d)))}, \qquad (1)$$

где I – количество информации, которое получает Ева при передаче одного блока; I_0 – количество информации, которое получает Ева за один раунд протокола; q – вероятность перехода в режим контроля подслушивания; d – уровень ошибок, вносимый атакой Евы.

Шаг 2. Генерация случайной двоичной гаммы γ_i размером r и сложение гаммы с соответствующим блоком $b_i = a_i + \gamma_i$ (т.е. выполнение *операции XOR* или исключающее ИЛИ).

Шаг 3. Выполнение режима передачи сообщения пинг-понг протокола с парами перепутанных кубитов. Режим контроля подслушивания протокола не моделировался.

Шаг 4. В случае, когда легитимные пользователи убедились в отсутствии подслушивания, моделируется передача гамм обычным открытым каналом связи.

Шаг 5. Восстановление исходного блока данных a_i, т.е. сложение полученного блока b_i с соответствующей гаммой γ_i: $a_i = b_i + \gamma_i$ (т.е. выполнение *операции XOR* или исключающее ИЛИ).

Для моделирования работы режима передачи сообщения пинг-понг протокола с парами перепутанных кубитов с использованием метода гаммирования, согласно вышеизложенному алгоритму, в среде программирования C++ Builder разработано программное обеспечение. Так, например, для передачи сообщения длинной 340 бит его нужно разбить на 5 блоков по 68 бит согласно (1) и для каждого сгенерировать свою гамму (ключ шифрования). Затем нужно передать это закодированное сообщение по квантовому каналу, убедиться в отсутствии прослушивания и передать по открытому каналу соответствующие гаммы для каждого блока зашифрованного сообщения, согласно выше описанному алгоритму. На принимающей стороне нужно сделать расшифровку полученного сообщения.

2. ОЦЕНКИ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ГЕНЕРАЦИИ ДВОИЧНЫХ ГАММ ОПРЕДЕЛЕННОГО РАЗМЕРА

Для алгоритма, который был описан выше, были рассчитаны средние оценки вычислительной сложности генерации случайных двоичных гамм определенного размера r, приведенные в табл. 1. Вычисления проводились на двухъядерном процессоре Intel Pentium Dual-CoreT3200 со следующими параметрами: тактовая частота (MHz): 2000, частота шины (MHz): 667, кэш 2-го уровня (Kb): 1024, поддерживается набор команд MMX, SSE, SSE2, SSE3, SSSE3, EM64T. Соответствующее программное обеспечение для генерации случайных двоичных гамм определенного размера было разработано в среде программирования C++ Builder. С использованием генератора случайных чисел выполнялась генерация 1000 случайных двоичных гамм заданного размера r и вычислялось время, которое требуется для генерации одной такой гаммы. Описанная процедура выполнялась 1000 раз для каждого размера гамм, а затем были вычислены средние значения, которые и приведены в табл. 1.

Для сравнительного анализа данного метода повышения безопасности пинг-понг протокола с методом повышения безопасности, предложенным в [7] и основанном на использовании обратимого хеширования (с использованием обратимых матриц), разработано программное обеспечение для обращения случайных двоичных матриц в среде программирования C++ Builder, в котором используется алгоритм LUP-разложения [14]. С помощью этого программного обеспечения генерировалось по 1000 псевдослучайных двоичных матриц заданного размера r с использованием генератора случайных чисел, с проверкой их на обратимость и расчетом времени, необходимого для генерации одной обратимой матрицы. Для каждого размера матриц описанная процедура выполнялась 1000 раз с вычислением среднего значения, результаты приведены в табл. 1. Согласно результатам работы [15], доля обратимых в двоичном поле Галуа GF (2) матриц составляет 0,289 от полного количества таких матриц (при $r \geq 16$).

Таблица 1

Оценки вычислительной сложности генерации двоичных гамм размера r и генерации случайных обратимых двоичных матриц размера $r \times r$

r	Среднее время генерации одной случайной обратимой двоичной матрицы, с	Среднее время генерации одной случайной двоичной гаммы, с
50	0,0122	0,0009
100	0,0728	0,0046
150	0,2094	0,0095
200	0,4429	0,0169
250	0,9184	0,0254
300	1,6102	0,0371
350	2,5682	0,0502
400	3,8923	0,0671
450	5,3113	0,0836
500	6,6605	0,1057
550	8,5056	0,1314
600	11,395	0,1578
650	14,610	0,1856
700	18,214	0,2145
750	22,385	0,2460
800	28,452	0,2788
850	31,597	0,3113
900	36,741	0,3557
950	44,027	0,3955
1000	55,075	0,4381
1250	99,148	0,6911
1500	186,75	0,9972
1750	323,18	1,3517
20000	438,23	1,7635

Согласно данным в табл. 1, время генерации одной случайной двоичной гаммы незначительно для небольших гамм даже на таком сравнительно слабом процессоре. Так, для двоичных гамм размером 500 бит на генерацию одной гаммы нужно примерно 0,106 секунд, а для гамм размером 2000 бит – 1,763 секунд. Генерация же одной случайной обратимой двоичной матрицы размером 500×500 происходит примерно за 6,6 секунд, а матрицы 1000×1000 – примерно за минуту. Однако это время быстро растет с увеличением размера матриц.

Таким образом, новый предложенный способ усиления безопасности пинг-понг протокола требует значительно меньше времени на подготовительную операцию – генерацию случайных гамм (ключа шифрования) в поле GF (2) заданного размера, чем способ, который использует обратимое хеширование [7]. На приемной стороне процедура восстановления исходных блоков сообщения вообще практически не влияет на эффективность протокола.

Следует подчеркнуть, что предложенный метод усиления безопасности пинг-понг протокола, хотя и использует гаммы для шифрования блоков сообщения, но (как и предложенный ранее метод с использованием обратимого хеширования) не является традиционным шифрованием. Нет необходимости сохранять гаммы в секрете, они передаются по открытому каналу связи после того, как легитимные пользователи пинг-понг протокола убедились, что во время квантовой передачи не было атаки пассивного перехвата, что обеспечивается режимом контроля подслушивания самого протокола. Таким образом, при использовании предложенного метода усиления безопасности пинг-понг протоколов не существует проблемы хранения и передачи секретной информации, и основное преимущество квантовых протоколов безопасной связи, т.е. отсутствие традиционного шифрования, сохраняется при использовании этого метода.

При использовании метода усиления безопасности, который основан на обратимом хешировании [7], выполняются сложные криптографические операции с использованием случайных двоичных обратимых матриц (перемежевание), а при гаммировании выполняется только простая операция XOR. Однако метод гаммирования имеет несколько меньшую безопасность, т.к. для восстановления исходного блока данных при обратимом хешировании злоумышленнику нужно перехватить как весь блок данных при его передаче в квантовом канале, так и всю соответствующую хеш-матрицу, а при гаммировании он имеет возможность сразу восстановить ту часть блока данных, которую он перехватил в квантовом канале, если перехватит также соответствующую часть гаммы. Однако возможность этого может быть сделана как угодно малой, если легитимные пользователи выберут достаточную длину блока для гаммирования так, чтобы вероятность обнаружения атаки в квантовом канале была сколь угодно малой. Если же легитимные пользователи обнаружат атаку, то они не будут передавать гамму по открытому каналу, и злоумышленник не получит никакой информации.

ВЫВОДЫ

Методы симметричного шифрования являются одними из актуальных и криптографически гарантированных методов защиты информации, которые с соответствующей модификацией могут применяться и для усиления безопасности протоколов квантовой прямой безопасной связи, в частности, для пинг-понг протокола с парами перепутанных кубитов. Предложенный в данной статье метод усиления безопасности такого протокола с помощью гаммирования блоков сообщения имеет значительно большую скорость, чем метод усиления безопасности, основанный на использовании случайных обратимых матриц [7]. При этом новый метод также сохраняет основное преимущество пинг-понг протокола – отсутствие необходимости шифрования сообщений с распределением секретных ключей, – гаммы не являются секретными ключами и передаются открыто в случае, если не было подслушивания при передаче сообщения в квантовом канале. Таким образом, предложенный в данной статье метод усиления безопасности пинг-понг протокола предпочтительнее известного ранее и является вполне приемлемым для практического применения.

Литература

[1] Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.

[2] Deng F.-G. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block / F.-G. Deng, G.L. Long, X.-S. Liu // Physical Review A. – 2003. – V. 68, № 4. –042317.

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

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

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

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

[7] Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83–91.

[8] Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, issue 17. – P. 4540–4544.

[9] АграновскийА.В. Практическая криптография (серия «Аспекты защиты») / А.В. Аграновский, Р.А. Хади. – М.: Солон-Пресс, 2002.– 254 с.

[10] Диффи У. Новые направления в криптографии / У. Диффи, М.Э. Хеллман. – М.: ИЛ, 1976. –654 с.

[11] Шеннон К. Э. Работы по теории информации и кибернетике / К. Э. Шеннон. – М.: ИЛ, 1963. –832 с.

[12] Партыка Т.Л. Информационная безопасность/ Т.Л. Партыка, И.И. Попов. – М.: Форум - Инфра, 2007. –368 с.

[13] Кінзерявий В.М. Новий метод підсилення секретності пінг-понг протоколу з парами переплутаних кутритів / В.М. Кінзерявий, Є.В. Василіу, С.О. Гнатюк, Т.О. Жмурко// Захист інформації. – 2012, №2 (55). – С. 5–13.

[14] Кормен Т. Алгоритмы: построение и анализ = Introduction to Algorithms /Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн.– М.:Вильямс, 2005. – 1296 с. – ISBN 5-8459-0857-4.

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

Поступила в редколлегию 16.04.2013

Николаенко Сергей Валентинович, ассистент кафедры информационных технологий Одесской национальной академии связи им. А.С. Попова. Научные интересы: криптография, квантовая криптография, Web-программирование, базы данных.

УДК 004.056.53+530.145

Підсилення безпеки методом гамування протоколу квантового прямого безпечного зв'язку/ С.В. Ніколаєнко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 347–350.

У статті розглянуто класичний (не квантовий) спосіб підсилення безпеки пінг-понг протоколу з парами переплутаних кубітів. Цей спосіб використовує шифрування методом гамування блоків повідомлень. При цьому самі гами не є секретною інформацією і передаються відкритим каналом зв'язку тільки після того, як легітимні користувачі переконалися у відсутності атаки у квантовому каналі. Крім того, запропонований спосіб не потребує квантової пам'яті.

Ключові слова: квантова криптографія, пінг-понг протокол, метод підсилення безпеки протоколу, шифрування методом гамування, імітаційне моделювання, часові оцінки.

Табл.: 1. Бібліогр.: 15 найм.

UDC004.056.53+530.145

Improving security of quantum direct secure communication protocol by XOR encryption / S.V. Nikolaenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 347–350.

The paper considers the classical (not quantum) method of improving security of the ping-pong protocol with pairs of entangled qubits. This method uses XOR encryption of message blocks. Keys are not secret information and are transmitted via an open channel only after legitimate users convince in the absence of an attack in the quantum channel. In addition, the suggested method of security improving does not require a quantum memory.

Keywords: quantum cryptography, ping-pong protocol, method of improving protocol security, XOR encryption, simulation, time estimations.

Tab.: 01. Ref.: 15 items.