Работа представлена на V научную конференцию «Успехи современного естествознания», 27-29 сентября 2004г., РФ ОК «Дагомыс», г. Сочи

МЕТОД СЪЕМА ИНФОРМАЦИИ В КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ

Румянцев К.Е., Хайров И.Е., Новиков В.В.
Таганрогский государственный радиотехнический университет, Таганрог

Классическая криптография основана на использовании секретных ключей. При этом секретность криптограммы полностью зависит от секретности используемого ключа. Как показал Клод Шеннон [1], если ключ является действительно случайным, если он такой же длины, что и само сообщение, и если он никогда не используется повторно, то одноразовая передача сообщения абсолютно защищена. В то же время, эта не взламываемая система имеет один существенный недостаток - распределение ключа. Если решить проблему распределения ключа, то в принципе можно достичь полной секретности. На данный момент существует два очень интересных решения поставленной проблемы: математическое и физическое. Математическое решение называется криптографией с открытым ключом, а физическое известно как квантовая криптография.

Хотя в асимметричных системах нет проблемы распределения ключей, но, к сожалению, их надежность основана на недоказанных предположениях о сложности разложения больших целых чисел на простые множители (факторизации). При этом считается, что всегда возможно найти секретный ключ по открытому ключу, но это трудно сделать за приемлемое время. Это означает, что если и как только будут реализованы быстрые и надежные процедуры для факторизации больших целых чисел, вся секретность и надежность криптосистем с открытым ключом сразу исчезнут. Исследования же по квантовым вычислениям показывают, что квантовые компьютеры способны факторизовать гораздо быстрее, чем классические компьютеры [2]. Это значит, что в некотором смысле криптосистемы с открытым ключом уже незащищены: любое сообщение, зашифрованное, например, с помощью алгоритма RSA, можно будет прочесть после того, как будет внедрен первый квантовый компьютер. Следовательно, с данного момента нельзя использовать RSA для шифрования информации, которая на тот момент должна оставаться секретной.

Квантовая криптография предлагает принципиально новый метод решения проблемы распределения ключа. Как отмечается, например в [3], квантовая криптография обеспечивает абсолютно защищенное распределение ключа. Здесь, в отличие от классической криптографии, защита основана на законах физики, а не на том факте, что для успешного съема информации (подслушивания) потребовались бы огромные вычислительные мощности.

На данный момент существует несколько протоколов квантового распределения ключа, принципы построения которых заключаются в следующем. Квантовое распределение ключа начинается с пересылки одиночных или перепутанных квантов от пользователя А к пользователю Б. Подслушивание (съем информации), с физической точки зрения, основано на серии экспериментов, которые подслушивающий агент (далее агент Е) выполняет на носителях информации, в данном случае на пересылаемых квантах. Согласно принципам квантовой механики, любое измерение, выполняемое агентом Е, неизбежно меняет состояния передаваемых квантов, и пользователи А и Б могут это выяснить в последующей открытой связи [3]. Таким образом, основные составляющие квантового распределения ключа таковы: квантовый канал для обмена квантами и так называемый открытый канал, который используется, чтобы проверить искажено ли сообщение в квантовом канале.

Во время квантовой пересылки ключ либо закодирован с использованием заданного набора неортогональных квантовых состояний одной частицы, либо он получается из заданного набора измерений, выполняемых на перепутанных частицах после пересылки (в этом случае во время пересылки ключ еще даже не существует).

Квантовые протоколы распределения ключа, основанные на передаче одиночных фотонов с неортогональными состояниями поляризации, наиболее привлекательны в свободном пространстве, где сохраняется их поляризация. Однако их труднее осуществить в оптических волноводах из-за деполяризации и случайно флуктуирующего двулучепреломления. Деполяризация не является основной проблемой: ее действие можно подавить посредством достаточно когерентного источника. Временная шкала флуктуаций двулучепреломления при стационарных условиях является довольно медленной (1 час). Электронная система компенсации, осуществляющая непрерывное отслеживание и исправление поляризации, наверняка возможна, но она требует процедуры согласования между пользователями А и Б. Несмотря на эти недостатки ученым из GAP-Optique впервые удалось создать достаточно компактное (две 19-дюймовые коробки) и надежное plug&play QKD-устройство (Quantum Key Distribution — квантовое распространение ключа). С его помощью была установлена двухсторонняя наземная и воздушная оптоволоконная связь между городами Женева и Лузанна, расстояние между которыми составляет 67 км. Источником фотонов служил инфракрасный лазер с длиной волны 1550 нм. Скорость передачи данных была невысока, но для передачи ключа шифра (длина от 27,9 до 117,6 кБит) большая скорость и не требуется. Но что самое важное, система просто подключалась к USB-порту компьютера [4].

Хотя квантовая криптография, основанная на открытых оптических путях, лишена такого недостатка как изменение поляризации, однако здесь возникает проблема прохождения света через турбулентную атмосферу и детектирование единичных фотонов на фоне сильного шума. В то же время, сочетание узкополосной частотной и пространственной фильтрации с наносекундной техникой должно позволить осуществить генерацию ключа с приемлемыми величинами относительной ошибки. В проведенном недавно

группой из Лос-Аламоса эксперименте была достигнута 14 % эффективность связи на расстоянии 950 м в свободном пространстве с ошибкой порядка 1,5 % [5]. В другом эксперименте, проведенном британскими физиками из коммерческого подразделения QinetiQ Британской оборонной исследовательской лаборатории и немецкими физиками из Мюнхенского университета Людвига-Максимиллиана, удалось передать криптографический ключ на расстояние 23,4 км непосредственно через воздушное пространство без использования оптоволоконной техники [6].

В связи со сказанным можно сделать вывод, что наиболее привлекательными на данный момент с точки зрения практической реализации являются протоколы квантовой криптографии, основанные на передаче одиночных несвязанных квантов с кодировкой поляризационных состояний в двух альтернативных базисах, не ортогональных друг другу.

Одним из распространенных протоколов квантовой криптографии, применяемых для передачи секретного ключа от одного пользователя к другому, является одночастичный протокол BB84 [7]. Секретность этого протокола (как и всех квантово-криптографических протоколов) основана на том факте, что в случае осуществления съема информации в квантовом канале третьим неавторизованным лицом (агентом Е), законные пользователи А и Б смогут выявить сам факт съема информации по проценту ошибок, после проведения открытых переговоров, и вынуждены будут повторно возобновить процедуру передачи секретного ключа. При этом предполагается, что пользователь А осуществляет передачу конфиденциальной информации пользователю В.

Необходимо отметить, что при практической реализации квантово-криптографических систем, основанных на кодировании по поляризации и осуществляющего обмен данными между пользователями А и Б, исследуется влияние агента Е. При теоретическом рассмотрении этого процесса, когда передача осуществляется при помощи одиночных фотонов, агент Е не может отвести часть сигнала, так как нельзя поделить электромагнитный квант на части. В реальных же условиях это вызовет сильное затухание сигнала (либо вообще его отсутствие), что поставит под сомнение корректность приема у пользователя Б.

Анализ возможности осуществления несанкционированного доступа в данном случае необходим для разработки и принятия дополнительных мер защиты. Однако в ходе экспериментов рассматривается только непосредственное вмешательство злоумышленника в процесс передачи, т.е подслушивающий агент Е последовательно перехватывает фотоны, генерируемые пользователем А, измеряет их поляризацию и, в соответствии с полученными результатами измерений, пересылает их пользователю Б.

Согласно принципу неопределенности Гейзенберга, попытка произвести измерения в квантовой системе искажает ее состояние, и полученная в результате такого измерения информация не полностью соответствует состоянию системы до начала измерений. Соответственно, попытка съема информации (непосредственного измерения неизвестного поляризационного состояния единичного фотона) агентом Е в квантовом канале связи неизбежно приводит к внесению в него помех, обнаруживаемых легальными пользователями А и Б [3].

Проанализировать присутствие третьего пользователя Е можно, предполагая, что передавался фотон, например, с вертикальным типом поляризации, суперпозиционное состояние которого $|\mathbf{b}\rangle = a_1|/\rangle + b_1|\backslash\rangle$, где a_1, b_1 - амплитуды вероятностей, квадрат модуля которых определяет вероятность перехода суперпозиционного состояния поляризации в одно из базисных состояний.

Рассмотрим четыре возможные ситуации.

1. Использование пользователем Б и агентом Е одинаково ориентированных измерителей (при условии совпадения их базисов с базисом поляризатора пользователя А) позволяет не только извлечь информацию о типе поляризации, но и правильно определить состояние поляризации.

2. При использовании же пользователем Б и агентом Е одинаково ориентированных анализаторов и при их не совпадении с анализатором пользователя А видно, что злоумышленник определит лишь "часть" суперпозиционного состояния, причем состояние фотона на выходе его анализатора будет правильно принято пользователем Б и результат их измерений будет одинаков. Однако он будет неправильным относительно пользователя А и открытые переговоры между отправителем А и получателем Б, предусмотренные квантово-криптографическими протоколами, позволят обнаружить и скорректировать ошибку.

3. Применение же пользователем Б и агентом Е различных анализаторов обусловливает правильность определения поляризационного состояния подслушивающим агентом, а при детектировании информации пользователем Б произойдет ошибка. При коррекции неправильной интерпретации бита информации пользователями А и Б результат измерения все равно будет отброшен.

4. Интерес представляет последний случай, при котором базисы пользователей А и Б совпадают между собой и не совпадают с базисом агента Е. Неправильная ориентация измерителя агента Е вносит ошибку в процесс передачи, хотя при отсутствии злоумышленника результат измерения пользователя Б был бы правильным. В данной ситуации присутствие злоумышленника будет однозначно обнаружено авторизованными пользователями.

Недостатками описанного метода съема являются:

- большой уровень ошибок, вносимых подслушивающим агентом Е в сообщение, передаваемое пользователем А пользователю Б;

- выявление легальными пользователями А и Б факта съема информации в квантово-криптографическом канале;

- минимальное количество информации, которую получает подслушивающий агент Е.

Для снижения уровня ошибок, вносимых агентом Е в перехватываемое сообщение, им должны быть перехвачены не все фотоны, а только незначительная их часть (менее 10 %). При этом, подслушивающий агент Е получит менее 7,5 % полезной информации,

которая будет еще значительно уменьшена легальными пользователями А и Б после проведения процедур усиления секретности.

В работе предложен принципиально новый метод, позволяющий осуществить съем информации. Основной целью метода является уменьшение вероятности обнаружения несанкционированного доступа к информации в квантово-криптографическом канале, используемом пользователем А для передачи секретного ключа пользователю Б. Идея заключается в возможности измерения неизвестного поляризационного состояния путем измерения его известного типа поляризации. Следует отличать тип поляризации, который представляет собой физическую характеристику элементарной частицы, от суперпозиционного состояния поляризации фотона, являющегося неизвестным квантовым состоянием [8]. В основу метода положен эффект вынужденного испускания активного вещества под воздействием первичного фотона, при котором сохраняются все свойства частицы. На выходе будет несколько фотонов с одинаковой поляризацией, а вернее с одинаковым типом поляризации. Эффект вынужденного испускания позволяет получить “копии” фотона, проходящего через активную среду, а измерения, производимые над полученной группой фотонов агентом Е, не повлияют на сеанс связи пользователей А и Б [9]. Окончательный вывод о правильности того или иного измерения принимается после прослушивания диалога по открытому каналу между легальными пользователями.

Применение данного метода не противоречит теореме о невозможности клонирования неизвестного квантового состояния, каким является суперпозиционное состояние поляризации фотона [10]. Метод предполагает копирование только типа поляризации, а измерение суперпозиционного состояния, в конечном итоге, однозначно определяется используемым измерителем. Следует также отметить, что при определенных условиях пользователи А, Б и агент Е будут обладать одной и той же конфиденциальной информацией.

Сравнительный анализ описанных методов позволяет выявить следующие существенные преимущества предложенного метода:

- отсутствие методологических ошибок, вносимых подслушивающим агентом Е при съеме информации в квантово-криптографическом канале;

- невозможность выявление легальными пользователями А и Б самого факта съема информации, даже после проведения открытых переговоров и после применения процедур согласования или коррекции ошибок и квантового усиления секретности;

- подслушивающий агент Е получает достаточно информации, чтобы сформировать секретный ключ, обладая суперкомпьютером или даже квантовым компьютером. В частности, он точно знает, что 50 % из перехваченных им битов правильные, и, что самое важное, знает какие именно правильные. Агент Е точно знает, что в оставшейся второй половине битов еще 50 % могут быть правильными. Таким образом, максимальное количество ошибочных битов в перехваченном ключе составляет около 25 % (если конечно не учитывать искажений при распространении единичных фотонов в канале связи, которые отбрасываются в процессе общения законных пользователей по открытому каналу).

Имея в своем распоряжении секретный ключ и зная, какие именно биты в нем правильные (вернее неправильные с вероятностью 50 %), подслушивающий агент Е с использованием суперкомпьютера сможет, например, методом перебора восстановить правильный секретный ключ.

Таким образом, проведенные исследования позволяют сделать вывод, что предложенный новый метод съема является эффективнее ранее предложенных. Последующие исследования направлены на оценку количественных характеристик, сопутствующих процессу передачи в присутствии подслушивающего агента и определяющих границы применения метода.

СПИСОК ЛИТЕРАТУРЫ

1. C.E. Shannon, Bell Sist. Tech. J, 28, 656 (1949)

2. P. Shor, (1994) Proc. of 35th Annual Symposium on the Foundations of Computer Science, (IEEE Computer Society, Los Alamitos), p.124 (Extended Abstract)

3. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Под ред. Боумейстера Д., Экерта А., Цайлингера А.; Пер. с англ. Кулика С.П., Шапиро Е.А. - М.: Постмаркет, 2002. – 375 с.

4. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard and H. Zbinder Electronics Letters 34, 2116-2117 (1998)

5. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard and H. Zbinder Electronics Letters 34, 2116-2117 (1998)

6. "Nature", Vol, 419, P. 450, 2002

7. Bennett C.H. Phys. Rev. Lett. 68 3121 (1992)

8. Л.В. Тарасов Введение в квантовую оптику: Учеб. пособие для вузов. – М.: Высш. шк., 1987. – 304 с.: ил.

9. К.Е. Румянцев, И.Е. Хайров, В.В. Новиков Доступ к информации, передаваемой по квантово-криптографическому каналу. Материалы электронной конференции “Приоритетные направления развития науки, техники и технологий”. РАЕ, 2004

10. С.Я. Килин Квантовая информация / Успехи физических наук. 1999. Том 169. №5. С. 507-526

Работа представлена на V научную конференцию «Успехи современного естествознания», 27-29 сентября 2004 г., РФ ОК «Дагомыс», г. Сочи