Квантовая криптография

Материал из Википедии — свободной энциклопедии

Квантовая криптография — метод защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике информации, так как рассматривает случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приема информации всегда выполняется физическими средствами, например при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определенных параметров физических объектов — в нашем случае, переносчиков информации.

Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы — невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой. Это фундаментальное свойство природы в физике известно как принцип неопределенности Гейзенберга, сформулированный в 1927 г.

Используя квантовые явления, можно спроектировать и создать такую систему связи, которая всегда может обнаруживать подслушивание. Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в нее нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

Содержание

Простейший алгоритм генерации секретного ключа

(На примере реализации метода поляризации фотонов)

Для объяснения алгоритма воспользуемся широко распространенной схемой персонажей (Алиса и Боб обмениваются секретной информацией). Алиса посылает Бобу последовательность фотонных импульсов. Каждый из импульсов случайным образом поляризован в одном из четырех направлений: | — \ /. Например, Алиса посылает: — / \ | \ — |.

Боб настраивает свой детектор произвольным образом на измерение серии либо диагонально, либо ортогонально поляризованных импульсов (мерить одновременно и те и другие нельзя): X X + X X + +.

В тех случаях, где Боб угадал поляризацию, он получит правильный результат (такую же поляризацию, какую посылала Алиса). В остальных случаях результат будет случайным.

Боб и Алиса по открытому каналу сообщают друг другу использованные типы поляризаций (диагональная или ортогональная). Оставляют только правильно измеренные.

В нашем примере Боб угадал поляризацию 2-го, 5-го, 6-го и 7-го импульсов. Таким образом, остаются: \ \ — |.

По заранее оговоренным условиям эти результаты превращаются в последовательность битов (например, 0° и 45° принимаются за единицу, 90° и −45° — за ноль, в приведённом выше примере получится 0010).

Перехват сообщения-ключа Боб и Алиса могут обнаружить посредством контроля ошибок, сверив случайно выбранные из сообщения биты. Несовпадения указывают на перехват сообщения, тогда ключ изменяется, то есть передается повторно.

Если расхождений нет, то биты, использованные для сравнения, отбрасываются, ключ принимается. С вероятностью $1 - 2^{-k}$ (где k — число сравненных битов) канал не прослушивался.

Впрочем, если недоброжелатель может не только прослушивать основной канал Алиса->Боб, но и может фальсифицировать работу открытого канала Боб->Алиса, то вся схема рушится. (Man-In-The-Middle)

Описанный алгоритм носит название протокола квантового распределения ключа BB84. В нем информация кодируется в ортогональные квантовые состояния. Помимо использования ортогональных состояний для кодирования информации, можно использовать и неортогональные состояния (например протокол B92).

К вопросу о стойкости квантовой криптографии

Известен ряд протоколов квантовой криптографии (в т.ч. квантовой рассылки ключей).

Итак, два способа компрометации квантовых криптографических протоколов указаны выше. Это

- метод посредника в основном канале,
- метод посредника во вспомогательном канале.

Ещё очевидный (даже студентам) способ компрометации:

- неприцельная "порча" (случайные подмены квантов) в канале, приводящие при достаточно интенсивной порче с удельной энтропией, близкой к 1, к необходимости высокой избыточности квантовых посылок Алисы, подрывая тем самым всю идею квантовой криптографии (т.к. при высокой избыточности посылок возможность репликации посланий Алисы криптоаналитиком очевидна). Этот способ компрометации вынуждает Алису и Боба отказываться от канала квантовой криптографии (ККК). Поскольку декларируемые свойства протоколов квантовой криптографии прямо противоречат теореме Simmons (80-е гг. 20-го в.), из которой следует, что одновременно совершенную секретность и совершенную

достоверность обеспечить каким бы то ни было математически формализуемым алгоритмом невозможно, квантовая криптография привлекла к себе повышенное внимание математиков и физиков.

- Например, А.В. Горшков (ЮУрГУ, г.Челябинск) в 2003 г. указал ряд физически осуществимых способов скрытной репликации посланий Алисы по ККК (см. список литер.) с помощью как многопроходного, так и однопроходного квантового усилителя и быстродействующего рассекателя фотонного цуга. Этим методом (во всяком случае, на расстояниях ККК, превосходящих "естественную длину фотона" (см. Квантовая механика)) при существующем уровне техники возможно создавать (в принципе, сколько угодно) копий посылок Алисы, в которых (во всяком случае, в 1-й копии) физическое различие между оригиналом в состоянии, отправленным в ККК Алисой, оригиналом в состоянии, принятым из ККК Бобом, и репликой (а оно всегда ненулевое - см. Квантовая механика - Соотношение неопределённостей Гайзенберга; его частное следствие - теорема о "невозможности клонирования", см. выше) будет находиться в пределах собственной "решающей области" посланного Алисой значения. Таким образом, ККК принципиально не способен гарантировать отсутствие корреляции между оригиналом (у Алисы, у Боба) и репликой (у криптоаналитика).

Ещё более очевидно, что оптоволоконные линии связи ничуть не более защищены от такого копирования фотонов, чем воздушные. Так, тот же А.В. Горшков там же предложил для этой цели использовать явление нарушенного полного внутреннего отражения (высоковероятное туннелирование фотонов через барьер) на границе сердцевины световода и зонда. Так же можно ввести фотоны в ККК без физического нарушения целостности сердцевины его световода. Использование зонда с показателем преломления большем, чем у сердцевины световода ККК, позволяет придать этому процессу вероятность, сколь угодно близкую к единице.

На тех же конференциях по защите информации докладчиком было отмечено, что по вышеуказанным причинам воздушная (вакуумная) линия связи, парадоксально, более криптостойка, чем твердотельная (световодная), вследствие необходимости нулевого сдвига фазы возврата фотона криптоаналитиком в ККК, если Алиса и Боб используют контроль фазы (например, интерферометрические версии протоколов квантовой криптографии). Однако использование криптоаналитиком однопроходного газового квантового усилителя компрометирует и эти протоколы ККК.

Таким образом, секция сделала вывод, что ККК в нынешнем её состоянии нельзя рекомендовать к использованию в РФ и при контактах с зарубежными партнёрами.

Вскоре работы, по существу тождественные методу Горшкова, были осуществлены в зарубежных учреждениях — как теоретические, так и экспериментальные, и опубликованы, но без указания на российский источник.

Может показаться, что остаётся "экологическая ниша" ККК — работа на относительно малых расстояниях (менее естественной длины фотона и "длины сцеплённого состояния"). Но использование высокоэнергичных фотонов (лазерный и инфракрасный цуг) делает взлом ККК элементарной задачей. Использование низкоэнергичных фотонов (СБММ, СВЧ, радиочастотных) делает сомнительной возможность самой генерации отдельного фотона в техническом устройстве небольших (лабораторных) размеров.

Сообщения же экспериментаторов об осуществлении ККК на расстояниях, близких к характерным размерам атома, интересны теоретически, но пока далеки от практики. Более того, упомянутый теоретический интерес состоит в основном в том, что известный двухфотонный протокол генерации посылок Алисы в ККК, основанный на известном явлении Эйнштейна-Подольского-Розена (когерентная двухфотонная генерация), использует физически неточную до степени ошибочности трактовку упомянутого эффекта, приводящую к отрицанию принципа причинности и в микромире. В физике до сих пор неизвестны сколько-нибудь достоверные явления, нарушающие принцип (точнее, гипотезу) причинности.

Итак, корреляция во времени публичного доклада А.В. Горшкова, последующее его теоретическое и экспериментальное подтверждение за рубежом, соответствующих публикаций в СМИ, резкое уменьшение интенсивности публикаций по исследованию КК объясняют известную осторожность пользователей России и зарубежных в приобретении систем КК. Нам неизвестны факты их коммерческого приобретения и использования где-либо в мире.

Итак, мы присоединяемся к вышеуказанному отзыву всероссийской конференции о КК.

Таким образом, известная проблема Simmons о совершенно криптостойком и одновременно совершенном достоверном распространения первичных ключей остаётся актуальной. При этом собственно теорема Simmons 80-х гг. (и ряд других известных 30-х - 50-х гг.) является частным случаем более общей "универсальной теоремы кодирования", доказанной и обнародованной в 2007 г. (в России), не использующей никаких предположений о физических свойствах канала связи.

В заключение целесообразно уточнить приведённое в начале этой Вики-статьи утверждение о соотношении неопределённостей Вернера Гайзенберга. Оно не является фундаментальным принципом ни природы, ни физической теории. Он является следствием свойств преобразования , например, Фурье (а также его можно вывести через ряд других - преобразования Хартли, Уолша, Радемахера, Котельникова и др.), применённого к нестационарному уравнению Э.Шрёдингера для волновой функции (введённого интуитивно с целью обобщения экспериментальных фактов) и критерия разрешения Рэлея (введённого интуитивно). Известны N-мерные обобщения этого соотношения. Известна, наконец, доказанная в 80-е гг. и тогда же опубликованная в специальной рецензируемой литературе (в т.ч. на английском языке) теорема В.Е. Косарева (д.ф.-м.н., ин-т физических проблем им. П.Л. Капицы, г.Москва), в которой через разложение как по функциям Котельникова, так и через любую другую систему ортогональных функций выведены, во-первых, соотношение, более общее, чем N-мерное соотношение Гайзенберга, во-вторых, показано, что существует не противоречащая принципам физики возможность "сверхразрешения" волновой функции (а следовательно, и плотности вероятности существования физического объекта) "до предела сверхразрешения", который является третьим результатом указанной работы В.Е. Косарева. Четвёртым результатом является вывод известной формулы пропускной способности информационного канала с помехой (впервые выведенной - В.Котельниковым, К.Шенноном) как одного из частных случаев теоремы Косарева. Заметим, что из вышеупомянутой теоремы кодирования, обнародованной А.В. Горшковым в 2007 г., следует формула пропускной способности канала с помехой (известная в открытой печати как формула Шеннона) тоже как частный случай.

Уже осуществлённые практические применения теоремы Косарева (80-е гг.) и теоремы, обнародованной Горшковым (2000-е гг.), относятся не только к области защиты

информации, но и, в частности, к сверхразрешению сигналов и изображений (устранение последствий зашумления, искажений, размытий, смазов, ненулевого размера апертуры, ненулевой длины волны физического посредника, переносящего информацию, различной физической природы) для фундаментальных научно-исследовательских задач в области физики низких температур, квантовой и ядерной физики (зарегистрированный пакет программ Recovery - соавторы Косарев, Гельфгат, Подоляк - ИФП РАН им. П.Л. Капицы, МГУ, ОИЯИ - 80-е - 90-е гг.), а также научно-исследовательских и прикладных задач в области дистанционного зондирования (в т.ч. субатмосферных объектов), физики элементарных частиц и ядерной физики, физики пучков зараженных частиц и плазмы (зарегистрированные пакеты программ Respectr и Reimage автор Горшков — МФТИ в сотрудничестве с НИИ тепловых процессов им. М.В. Келдыша, ИКИ, ИХП, ЦНИИМаш, ОИЯИ, НПО ЭЛАС — 90-е гг. — и ЮУрГУ в сотрудничестве с определёнными государственными учреждениями - 2000-е гг.).

Математический аппарат, использованный для доказательства вышеупомянутых теорем и создания вышеупомянутых программ, в значительной мере базируется на известных теоремах Радона, Банаха, Качмажа, Тихонова, Вайнштейна, Бочека, Танабе, Тананы, на известных алгоритмах Качмажа, Тихонова, Бочека, Танабе, Тараско, Фридена и др.

Анаграмма для указания на автора настоящей заметки (о нестойкости протоколов КК) по состоянию на 10.09.2009: АКГвактонисщлвапенжийооереетотим.

Автор заметки убедительно просит оппонентов его вышеизложенного мнения излагать своё мнение (в т.ч. возражения) ниже сей строки.

Реализации алгоритма

- 1989 г. Беннет и Брассар в Исследовательском центре IBM построили первую работающую квантово-криптографическую систему. Она состояла из квантового канала, содержащего передатчик Алисы на одном конце и приёмник Боба на другом, размещённые на оптической скамье длиной около метра в светонепроницаемом полутораметровом кожухе размером 0,5x0,5 м. Собственно квантовый канал представлял собой свободный воздушный канал длиной около 32 см. Макет управлялся от персонального компьютера, который содержал программное представление пользователей Алисы и Боба, а также злоумышленника.

- 1989 г. передача сообщения посредством потока фотонов через воздушную среду на расстояние 32 см с компьютера на компьютер завершилась успешно. Основная проблема при увеличении расстояния между приемником и передатчиком — сохранение поляризации фотонов. На этом основана достоверность способа.

- Активные исследования в области квантовой криптографии ведут IBM, GAP-Optique, Mitsubishi, Toshiba, Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт, молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны.

- Созданная при участии Женевского университета компания GAP-Optique под руководством Николаса Гисина совмещает теоретические исследования с практической деятельностью. Специалистам этой фирмы удалось передать ключ на расстояние 67 км из Женевы в Лозанну с помощью почти промышленного образца

аппаратуры. Этот рекорд был побит корпорацией Mitsubishi Electric, передавшей квантовый ключ на расстояние 87 км, правда, на скорости в один байт в секунду.

- 2001 г. доктор Эндрю Шилдс и его коллеги из TREL и Кембриджского университета создали диод, способный испускать единичные фотоны. В основе нового светодиода лежит «квантовая точка» — миниатюрный кусочек полупроводникового материала диаметром 15 нм и толщиной 5 нм, который может при подаче на него тока захватывать лишь по одной паре электронов и дырок. Это дало возможность передавать поляризованные фотоны на большее расстояние. В ходе экспериментальной демонстрации удалось передать зашифрованные данные со скоростью 75 Кбит/с — при том, что более половины фотонов терялось.

- Министерством обороны Великобритании поддерживается исследовательская корпорация QinetiQ, активно совершенствующая технологию квантовой шифрации. Эта компания появилась на свет в результате деления британского агентства DERA (Defence Evaluation and Research Agency) в 2001 г., вобрав в себя все неядерные оборонные исследования. О своих достижениях она широкой публике пока не сообщает.

- Исследованиями в области квантовой криптографии занимается также группа молодых компаний, в том числе швейцарская Id Quantique (http://www.idquantique.com/), представившая коммерческую систему квантовой криптографии, и Magiq Technologies (http://www.magiqtech.com/) из Нью-Йорка, выпустившая прототип коммерческой квантовой криптотехнологии собственной разработки. MagiQ Technologies была создана в 1999 г. на средства крупных финансовых институтов. Помимо собственных сотрудников с ней взаимодействуют научные работники из целого ряда университетов США, Канады, Великобритании и Германии. Вице-президентом MagiQ является Алексей Трифонов, в 2000 г. защитивший докторскую диссертацию в Петербургском университете. Год назад Magiq получила 7 млн. долл. от нескольких инвесторов, включая основателя Amazon.com Джеффа Безоса.

В продукте Magiq средство для распределения ключей (quantum key distribution, QKD) названо Navajo — по имени индейцев Навахо, язык которых во время Второй мировой войны американцы использовали для передачи секретных сообщений, поскольку за пределами США его никто не знал. Navajo способен в реальном времени генерировать и распространять ключи средствами квантовых технологий и предназначен для обеспечения защиты от внутренних и внешних злоумышленников. Продукт Navajo находится в состоянии бета-тестирования и станет коммерчески доступным в конце 2003 года. Несколько коммуникационных компаний тестируют Navajo в своих сетях.

Интерес к квантовой криптографии со стороны коммерческих и военных организаций растет, так как эта технология гарантирует абсолютную защиту. Создатели технологий квантовой криптографии вплотную приблизились к тому, чтобы выпустить их из лабораторий на рынок. Осталось немного подождать, и уже очень скоро квантовая криптография обеспечит еще один слой безопасности для нуждающихся в этом организаций.

Литература

- Квантовая криптография: идеи и практика / под ред. С.Я.Килина, Д.Б.Хорошко, А.П.Низовцева. – Мн., 2008. – 392 с.

- *Kilin S.Ya.* Quanta and information / Progress in optics. – 2001. – Vol. 42. – P. 1–90.
- *Килин С. Я.* Квантовая информация / Успехи Физических Наук. – 1999. – Т. 169. – С. 507-527. [1]
- *Васильев М.Н., Горшков А.В.* Разработка и создание аппаратно-программного комплекса для автоматизированного томографического анализа пучков заряженных частиц с высоким пространственным разрешением. / Аннотированный НТО по программе "Управляемый термоядерный синтез и плазменные процессы." - Долгопрудный: МФТИ, 01.12.1992. - 30 с.
- *Горшков А.В.* О нестойкости квантовой криптографии. http://www.fml31.ru/newsite2/pages/gorshkov/kriptokw.doc . // Труды 4-й международной конференции молодых учёных и студентов "Актуальные проблемы современной науки", секция "Радиотехника и связь". - Самара, 10-12.09.2003. - Части 12-16. С.39-42. http://povman.sstu.edu.ru // Республиканская научная конференция "Проблемы экономического роста национальной экономики". - Челябинск: ЮУрГУ, 15-17.12.2003. - Секция "Информационные технологии в экономике, управлении, бизнесе и образовании".
- *Горшков А.В.* О нестойкости квантовой криптографии. // 1-я Всероссийская научно-практическая конференция «Информационная безопасность региона». - Челябинск, ЮУрГУ, 5-7 октября 2004. С.207-211. - секция «Технические проблемы защиты информации». http://www.fml31.ru/newsite2/pages/gorshkov/04infbez.rar

См. также

- Квантовая информация
- Квантовая запутанность

Категория: Квантовый компьютер