На правах рукописи

Тимофеев Андрей Владимирович

Исследование стойкости квантово-криптографических протоколов распространения ключей

01.01.05 — Теория вероятностей и математическая статистика

Автореферат
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2008

Работа выполнена на кафедре квантовой информатики факультета вычислительной математики и кибернетики Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, член-корреспондент Академии криптографии РФ Молотков С. Н.
Официальные оппоненты:	доктор физико-математических наук, академик Академии криптографии РФ, профессор механико-математического факультета МГУ имени М.В.Ломоносова Сидельников Владимир Михайлович
	кандидат физико-математических наук, старший научный сотрудник Академии криптографии РФ Арбеков Игорь Михайлович
Ведущая организация:	Физико-технологическй институт Российской академии наук

Защита диссертации состоится 29 февраля 2008 г. в 11 ч. 00 мин. на заседании диссертационного совета Д 501.001.44 Московского государственного университета имени М. В. Ломоносова по адресу: 119991, ГСП-1, Москва, Ленинские горы, МГУ, 2-й учебный корпус, факультет ВМиК, аудитория 685.

С диссертацией можно ознакомиться в библиотеке факультета ВМиК Московского государственного университета имени М.В.Ломоносова.

С текстом автореферата можно ознакомиться на официальном сайте факультета ВМиК Московского государственного университета имени М.В.Ломоносова http://www.cs.msu.su в разделе “наука” — “работа диссертационных советов” — “Д 501.001.44”

Автореферат разослан 29 января 2008 г.

Учёный секретарь диссертационного совета
профессор Трифонов Н.П.

Общая характеристика работы

Объект исследования и актуальность темы.

Квантовая криптография, или распространение секретных ключей, в принципе позволяет реализовать абсолютно стойкие (не дешифруемые подслушивателем даже теоретически) системы шифрования с одноразовыми ключами. Секретность ключей в квантовой криптографии основана на фундаментальных запретах квантовой механики, а именно, на том обстоятельстве, что пара наблюдаемых, которым отвечают некоммутирующие операторы, не может быть достоверно одновременно различима, что является следствием соотношений неопределенности Гейзенберга. В квантовой криптографии в качестве таких наблюдаемых выступают матрицы плотности информационных состояний, соответствующих классическим битам 0 и 1. Для чистых состояний одновременная ненаблюдаемость (достоверная неразличимость) матриц плотности эквивалентна неортогональности информационных квантовых состояний. Сказанное означает, что не существует измерений, которые с вероятностью единица позволяют различать одно из пары неортогональных состояний и так, чтобы после измерения система оказалась в исходном состоянии, в котором она была до измерения. Таким образом, любое измерение, если оно дает информацию о передаваемых состояниях, неизбежно приводит к их возмущению, что позволяет детектировать любые попытки подслушивания в канале связи. Другими словами, подслушивание (соответственно возмущение состояний) передаваемых состояний должно неизбежно приводить к изменению статистики результатов измерений на приемном конце по сравнению со статистикой результатов измерений на невозмущенных состояниях. Искажение квантовых состояний возникает в неидеальном квантовом канале, что также приводит к изменению статистики результатов измерений. В квантовой криптографии принципиально невозможно отличить изменение статистики результатов по сравнению с идеальным случаем, возникающих за счет шума в канале или от действий подслушивателя, поэтому любые изменения статистики приходится относить на действия подслушивателя.

Если бы законы квантовой механики позволяли обнаруживать только сам факт возмущения передаваемых состояний, то это было бы бесполезно

для целей криптографии, точнее передачи ключей. Квантовая механика позволяет не только обнаруживать возмущение состояний, но и связать изменение статистики результатов измерений с количеством информации, которое может быть получено подслушивателем при наблюдаемом изменении статистики отсчетов по сравнению с идеальным случаем.

В квантовой криптографии кроме квантового канала связи (в реальных условиях это либо оптоволокно, либо открытое пространство), по которому передаются квантовые состояния, необходим также открытый классический канал связи. Классический открытый канал связи необходим для выяснения легитимными пользователями изменений статистики отсчетов и коррекции ошибок в первичном ключе, переданном по квантовому каналу связи. Единственное требование, которое предъявляется к классическому каналу связи состоит в том, что передаваемая открыто и доступная всем, включая подслушивателя, классическая информация не могла быть изменена подслушивателем – сохраняла целостность (так называемый unjammable channel). Такой открытый классический канал является математической идеализацией, поскольку подобных каналов в природе не существует. Для сохранения целостности открыто передаваемых классических данных в реальных условиях необходимо использовать процедуры аутентификации и контроля целостности данных. Для подобных процедур в свою очередь требуется секретный ключ.

Если в качестве открытого классического канала используется, например, интернет, то для целей аутентификации возможна генерация ключей по схеме Хеллмана-Диффи. Если же для открытого классического канала используется та же самая оптоволоконная линия, что и для квантового канала связи, то генерация ключей для аутентификации по схеме Хеллмана-Диффи оказывается принципиально неприемлемой из-за очевидной, так называемой атаки “man in the middle”. В такой ситуации требуется небольшой стартовый ключ один раз при первом сеансе. При последующих сеансах этот ключ выбрасывается, и для аутентификации и сохранения целостности данных, передаваемых по классическому каналу, используется часть ключа, сгенерированного по квантовому каналу в предыдущем сеансе обмена. Оставшаяся бóльшая часть ключа, используется собственно

для шифрования данных. Если для аутентификации и сохранения целостности данных используются процедуры на основе ГОСТа, то длина стартового ключа составляет 256 бит. При этом в результате работы протокола передачи ключа обмена может быть получен новый секретный ключ по квантовому каналу гораздо более длинный, чем исходный.

Разумеется, что стартовый ключ мог бы быть использован для шифрования этим ключом нового ключа и передачи его второму легитимному пользователю. Однако при этом абсолютная секретность нового ключа гарантируется лишь, если его длина не более длины ключа, на котором он шифруется. Т.е. более длинного ключа получить нельзя. В квантовой криптографии стартовый ключ не используется напрямую для передачи нового ключа, который генерируется по квантовому каналу связи. Как будет видно ниже, число бит открытой информации, переданной по открытому классическому каналу на один бит нового секретного ключа меньше единицы, поэтому возможно расширение ключа.

Подход с небольшим стартовым ключом является более предпочтительным, поскольку при этом возможно свести к минимуму число раундов обмена по открытому каналу связи в процессе “чистки” и усиления секретности ключа (privacy amplification).

Основная задача теории сводится к выяснению длины секретного ключа, который может быть получен при наблюдаемых изменениях статистики результатов измерений на приемном конце по сравнению со статистикой на невозмущенных состояниях. Как правило величиной, которая характеризует отклонение статистики измерений от идеальной, является величина вероятности ошибки. Точнее, вероятности того, что переданный бит был 0, а зарегистрирован как 1, и наоборот. Хотя возможны и другие критерии для обнаружения изменения статистики.

Первым этапом любого квантового протокола распределения ключей является передача и детектирование квантовых состояний. После передачи квантовых состояний легитимные пользователи оценивают вероятность ошибки (отклонение статистики отсчетов от идеальной).

Оценка вероятности ошибки получается путем сравнения через открытый канал части переданной последовательности по квантовому кана-

лу, в дальнейшем раскрытая часть отбрасывается.

Следующий этап состоит в коррекции ошибок в нераскрытой части последовательности у легитимных пользователей посредством обмена информацией через открытый канал связи. Обычно легитимных пользователей называют Алиса и Боб, а подслушивателя – Ева (от английского Eavesdropper). В результате коррекции ошибок остается последовательность бит меньшей длины и одинаковая у Алисы и Боба. "Одинаковая" в данном контексте означает, что их последовательности совпадают с вероятностью, сколь угодно близкой к единице (например, $1-2^{-m} \sim 1-10^{-70}$ при $m = 200$, величина параметра m выбирается легитимными пользователями). Напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}).

После "чистки" первичного ключа у подслушивателя имеется строка бит или регистр квантовой памяти с состояниями, или и то и другое вместе. Последний шаг при получении финального секретного ключа состоит в сжатии (фактически в применении случайной функции хэшировании) уже к одинаковой последовательности у Алисы и Боба. Сжатая последовательность бит является общим секретным ключом для легитимных пользователей, про который гарантируется, что подслушиватель имеет о ключе экспоненциально малую информацию по некоторому, заданному Алисой и Бобом, параметру секретности.

Естественным требованием к процедурам коррекции ошибок и усиления секретности ключа является сохранение как можно большего числа бит в финальном ключе. Еще одно требование состоит в минимизации числа обменов по открытому каналу связи в пересчете на один бит в финальном секретном ключе.

При коррекции ошибок в первичном ключе задача легитимных пользователей состоит не только в исправлении ошибок, но также в оценке верхней границы информации, которую может получить об оставшемся ключе подслушиватель из обменов по открытому каналу связи. Для коррекции ошибок возможно использование различных процедур, включая хорошо разработанные классические коды, исправляющие ошибки, либо специальные итерационные процедуры, использующие двусторонние обмены вспо-

могательной информацией между Алисой и Бобом через открытый канал связи. Причем заранее отнюдь не очевидно, какой из методов окажется более эффективным по упомянутым выше критериям.

Цель диссертации.

Целью диссертационной работы является:

1. Исследование криптографической стойкости двух основных протоколов квантового распределения ключей B92 и BB84 с учетом коллективной атаки подслушивателя на передаваемые квантовые состояния;

2. Определение величины критической ошибки Q_c в первичных ключах на приемной стороне, до которой возможно получение общего секретного ключа легитимными пользователями;

3. Оценка длины финального секретного ключа, который можно получить при наблюдаемой вероятности ошибки $Q < Q_c$ в первичных ключах;

4. Исследование различных процедур распределенной коррекции ошибок в первичных ключах, включая процедуры с двухсторонним обменом вспомогательной информацией через открытый канал связи, а также сравнение их эффективности;

5. Разработка компьютерных алгоритмов и программ для распределенной коррекции ошибок.

Научная новизна. В диссертационной работе впервые построена явная атака на передаваемый при помощи квантовых состояний ключ для протокола BB84, достигающая теоретического предела ошибки, до которой возможно распределение ключей. Дана оценка длины секретного ключа, которую можно получить при наблюдаемой вероятности ошибки $Q < Q_c$ в первичных ключах, для двух основных квантовых протоколов распределения ключей BB84 и B92. Предложен новый метод сохранения конфиденциальности для каскадного метода коррекции ошибок в первичных ключах.

Научная и практическая ценность.

Работа имеет теоретическую направленность. Предложенные и реализованные в процессе работы над диссертацией методы и алгоритмы,

позволяют эффективно реализовать распределенную коррекцию ошибок в ключе, и оценивать выданную при этом информацию подслушивателю.

Основные положения, выносимые на защиту:

1. Построена явная атака на передаваемый при помощи квантовых состояний ключ для протокола BB84, достигающая теоретического предела ошибки $Q_c \approx 11\%$, до которой возможно распределение ключей;

2. Дана оценка длины секретного ключа, которую можно получить при наблюдаемой вероятности ошибки $Q < Q_c$ в первичных ключах, для двух основных квантовых протоколов распределения ключей BB84 и B92;

3. Предложен метод сохранения конфиденциальности для каскадного метода коррекции ошибок в первичных ключах;

4. Разработаны алгоритмы и компьютерные программы для распределенной коррекции ошибок.

Публикации и апробирование. Результаты диссертации докладывались на семинаре ВМиК МГУ "Квантовая информатика" (руководители - акад. К. А. Валиев, проф. Ю. И. Ожигов, проф. С. Н. Молотков), на семинаре Физико-технологического института Российской академии наук (ФТИАН) "Квантовые компьютеры" (руководитель - акад. К. А. Валиев), на 10 научно-технической конференции по криптографии (Москва 2006 год), на конференциях Квантовая информатика - 2007 и Квантовая информатика - 2005.

По теме диссертации опубликовано 6 работ.

Структура и объем работы.

Диссертация состоит из введения, шести глав, приложения и списка литературы. Объем работы 125 страниц.

Краткое содержание диссертации

Во введении обоснована актуальность исследуемой проблемы, сформулирована цель и задачи диссертационной работы, перечислены полученные в диссертации новые результаты, их практическая ценность,

представлены положения, выносимые на защиту и описана структура диссертации.

В первой главе приведено описание квантового криптографического протокола B92 и различных стратегий подслушивания.

Во второй главе для протокола B92 определена критическая ошибка, до которой возможно распределение ключей для индивидуальной и коллективной атаках, получена также оценка длины секретного финального ключа в зависимости от наблюдаемой ошибки, если последняя меньше критической.

В третьей главе исследуется криптографическая стойкость основного квантового протокола распределения ключей – BB84. Для данного протокола ранее была найдена (Mayers, Shor, Preskill) точная величина критической ошибки. Однако эти доказательства являются фактически теоремами существования, констатирующими, что при $Q > Q_c \approx 11\%$. Алиса и Боб не могут получить общий секретный ключ. При этом явная стратегия Евы, которая приводит к данной ошибке, *неизвестна*. Точнее говоря, неизвестна оптимальная стратегия подслушивания, которая дает Еве максимум информации о ключе при минимально возможной производимой ей ошибкой у Боба.

Более менее ясно, что при такой стратегии Ева должна использовать квантовую память и коллективные измерения над всей последовательностью квантовых состояний. Это убеждение возникает из того обстоятельства, что для случая индивидуальных измерений над передаваемыми состояниями, оптимальная стратегия известна и построена явно. Но при такой стратегии Евы критическая ошибка оказывается $Q_c \approx 15\%$, что выше точной границы.

Кроме того, оставался открытым вопрос о том, что происходит в области ошибок $11\% < Q_c < 15\%$. Или иначе говоря, какие стратегии Евы будут приводит к критической ошибке в "диапазоне" стратегий (коллективная атака – индивидуальная атака).

В третьей главе стратегия, на которой достигается теоретический предел критической ошибки $Q_c \approx 11\%$, построена явно. Кроме того, прояснен вопрос, что происходит в области ошибок $11\% < Q < 15\%$. Показано,

что существует бесконечный набор стратегий подслушивания Евы, который приводит к ошибкам в интервале $11\% < Q < 15\%$. Установлена связь бесконечного набора стратегий с бесконечным набором *классических пропускных способностей квантового канала связи*. Данное явление не имеет классического аналога. Причем оказывается, что различные атаки внутри бесконечного набора отличаются только на стадии измерений. Если Ева может проводить коллективные измерения сразу над всей последовательностью квантовых состояний, то реализуется оптимальная стратегия, приводящая к критической ошибке в 11%. Если Ева может производить только индивидуальные измерния, то достигается ошибка в 15%. Если Ева может делать измерения не более, чем над k состояниями сразу ($1 < k < \infty$), то критическая ошибка $Q_c(11\%) < Q_c^{(k)} < Q_c(15\%)$.

Критическая ошибка зависит от способа исправления ошибок. Упомянутые критические ошибки достигаются, если легитимные пользователи используют случайные шенноновские коды для исправления ошибок. Однако такая процедура является хоть и конструктивной, но практически нереализуема, поскольку требует экспоненциально большой по длине битовой последовательности таблицы кодовых слов. Шенноновские случайные коды обладают минимальной избыточностью. Поэтому количество вспомогательной классической информации, передаваемой через через канал связи, и которая доступна подслушивателю, является минимально возможным по сравнению с другими процедурами исправления ошибок.

Используемые на практике процедуры исправления ошибок имеют большую избыточность, чем процедуры, основанные на случайных кодах. Поэтому Еве оказывается доступно большее количество информации, что приводит к меньшей допустимой критической ошибке, до которой возможно получение общего секретного ключа для Алимы м Боба.

Одной и важных задач является поиск эффективных процедур распределенной коррекции ошибок.

После исправления ошибок Алисой и Бобом у них возникают одинаковые битовые строки (“очищенный” ключ). Однако информация Евы об “очищенном” ключе все еще является конечной, и заведомо не экспоненциально малой по параметру секретности. Для получения финально-

го секретного ключа необходимо сжатие (хеширование) очищенного ключа при помощи универсальных функций хеширования второго рода (Wegman, Carter), которые сами являются случайными величинами. Причем степень сжатия определяется как величиной ошибки в первичном ключе, так и используемой процедурой коррекции ошибок. Исследованию этих вопросов посвящена **четвертая глава**.

В пятой главе рассмотрена эффективность различных методов коррекции ошибок применительно к задачам квантовой криптографии, основанных на процедуре бисективного поиска, комбинированном каскадном методе, а также на классических кодах Боуза-Чоудхури-Хоквингема и Хэмминга.

Наиболее простая итерационная процедура коррекции ошибок – это бисективный поиск ошибок, который сводится к разбиению первичного ключа на случайные непересекающиеся блоки и вычислению четностей этих блоков. Четности множеств сравниваются, как на приемном, так и на передающем конце через открытый канал. После раскрытия четности какого-либо множества, один из случайно выбранных битов, отбрасывается. При несовпадении четностей размер блока уменьшается вдвое, и процесс повторяется. Поскольку блоки не пересекаются, то выбрасывание битов не представляет труда. Такая процедура сохраняет конфиденциальность – подслушиватель не получает дополнительной информации при "чистке" первичного ключа. Однако, такая процедура крайне неэффективна, поскольку остается достаточно мало битов в "очищенном" ключе (например, при вероятности ошибки в 10% в первичном ключе в "очищенном" ключе остается не более 10% от исходной длины).

Наиболее эффективным, в смысле длины "очищенного" ключа, на сегодняшний день, по-видимому, является каскадный метод коррекции ошибок. В исходном варианте каскадного метода биты четности отдельных, и, в общем случае, *пересекающихся* подмножеств запоминаются и используются на следующих проходах. В процессе работы метода никакие биты не выбрасываются, поэтому метод не сохраняет конфиденциальность. Оценить информацию, которую получает подслушиватель, когда раскрываются биты четности набора пересекающихся множеств, возникающие на

разных проходах, достаточно сложно. До сих пор, насколько нам известно, полный анализ не был выполнен.

Сохранить конфиденциальность и эффективность метода можно, если в конце "чистки" первичного ключа отбрасывать некоторое количество битов. Поскольку, возникающие на каждом проходе множества битов пересекаются, то процедура выбрасывания не является тривиальной.

В данной главе предложен простой регулярный способ сохранения конфиденциальности (отбрасывания раскрытых при "чистке" битов четности пересекающихся множеств).

В шестой главе на основе результатов, полученных в предыдущих главах, приводится описание разработанного программного комплекса и алгоритмов обработки ключей, используемых в экспериментальном образце оптоволоконной системы квантовой криптографии.

В заключении приведены основные выводы по результатам диссертации, формулируются основные результаты.

В приложении приводится часть документации оптоволоконной системы квантовой криптографии, относящаяся к протоколам получения и обработки ключа.

Публикации по теме диссертации

1. С.Н.Молотков, А.В.Тимофеев, *Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки* $\mathbf{Q_c \approx 11\%}$, Письма в Журнал экспериментальной и теоретичесой физики, т.85, вып.10, 634 (2007).

2. А.В.Тимофеев, С.Н.Молотков, *О каскадном методе коррекции ошибок в первичных ключах в квантовой криптографии, сохраняющем конфиденциальность*, Письма в Журнал экспериментальной и теоретичесой физики, т.82, вып.12, 868 (2005).

3. А.В.Тимофеев, Д.И.Помозов, А.П.Маккавеев, С.Н.Молотков, *О структуре открытого классического канала связи в квантовой криптографии: коррекция ошибок, целостность и аутентичность*, Журнал экспериментальной и теоретической физики, т.131, вып.5, 771 (2007).

4. А.П.Маккавеев, С.Н.Молотков, Д.И.Помозов, А.В.Тимофеев, *О практических методах "чистки" ключей в квантовой криптографии*, Журнал экспериментальной и теоретической физики, т.128, вып.2, 263 (2005).

5. A.P. Makkaveyev, S.N. Molotkov, D.I. Pomozov, A.V. Timofeyev, *Practical error-correction procedures in quantum cryptography*, Proc. of SPIE vol. 6264, 62640F, (2006)

6. Молотков С.Н., Тимофеев А.В., *О каскадном методе коррекции ошибок в первичных ключах в квантовой криптографии*, Тезисы докладов 10 научно-технической конференции по криптографии, посвященной 85-летию образования Криптографической Службы России, Москва 2006 год, Академия криптографии Российской Федерации, секция 13, с. 56