Квантовая криптография

Учебное пособие

Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский
МГУ имени М.В.Ломоносова, факультет ВМК

Пособие посвящено квантовой криптографии — разделу квантовой информатики, в котором исследуется возможность генерации ключей, секретность которых гарантируется фундаментальными законами квантовой механики. В пособии рассматриваются основные однофотонные протоколы квантовой криптографии: BB84, B92, SARG04. Показывается, каким образом ограничения, накладываемые квантовомеханической природой сигналов, позволяют оценить количество информации, доступной перехватчику после выполнения протокола, и при каких условиях возможна генерация полностью секретного ключа. Также рассматриваются основные атаки перехватчика и демонстрируются методы оценки их эффективности.

Пособие предназначено для студентов, изучающих квантовую информатику, а также для всех интересующихся проблемой обеспечения секретной передачи информации и квантовомеханическому подходу к решению этой проблемы.

Оглавление

Введение **5**

1 О задаче секретной передачи данных **8**
1.1 Исторические сведения 9
1.2 Симметричные шифры 13
1.3 Криптографические системы с открытым ключом 18

2 Основные понятия квантовой теории информации **24**
2.1 Квантовые состояния 25
2.2 Измерения 30
2.3 Составные квантовые системы 35
2.4 Передача информации по квантовым каналам 43
2.5 Квантовые коды коррекции ошибок 54

3 Протокол квантового распределения ключей BB84 **61**
3.1 Общая схема протокола 62
3.2 Стойкость протокола 68
3.3 Стратегии подслушивателя 77

4 Другие протоколы квантовой криптографии **92**
4.1 Протокол B92 93

4.2 PNS-атака 94
4.3 Протокол 4+2 99
4.4 Протокол SARG04 101

Задачи **107**

Литература **110**

Введение

Квантовая криптография как наука зародилась в 1984 году, когда был разработан первый протокол квантового распределения ключей, названный BB84 [3]. Главным преимуществом квантовых криптографических протоколов перед классическими является строгое теоретическое обоснование их стойкости: если в классической криптографии стойкость сводится, как правило, к предположениям о вычислительных возможностях подслушивателя, то в квантовой криптографии перехватчик может предпринимать все допустимые законами природы действия, и всё равно у него не будет возможности узнать секретный ключ, оставшись при этом незамеченным.

Важным для квантовой криптографии свойством квантовой механики является свойство коллапса волновой функции, которое означает, что при измерении любой квантовомеханической системы её исходное состояния, вообще говоря, меняется. Это ведёт к важному следствию о том, что невозможно достоверно различить квантовые состояния из их неортогонального набора. Именно это свойство используется в обосновании секретности квантовой криптографии: при попытке подслушать передаваемые состояния из их неортогонального набора перехватчик неизбежно вносит в них ошибку, в результате

чего он может быть обнаружен по дополнительным помехам на приёмной стороне. Поэтому решение о возможности секретного распространения ключей достигается легитимными пользователями на основе величины наблюдаемой ошибки на приёмной стороне: при приближении значения этой ошибки к критической величине (зависящей от используемого протокола) длина секретного ключа в битах стремится к нулю, и передача ключей становится невозможной.

Это означает, что важнейшей характеристикой протоколов квантовой криптографии является допустимая критическая ошибка на приёмной стороне, до которой возможно секретное распространение ключей: чем она больше, тем более устойчивой является система квантовой криптографии по отношению к собственным шумам и попыткам подслушивания. Важным результатом является нахождение точной величины критической ошибки для протокола BB84, которая оказывается равной приблизительно 11%[15].

Экспериментальная реализация квантовой криптографии натолкнулась на ряд технологических трудностей, наиболее важной из которых является сложность генерации строго однофотонных квантовых состояний. На практике обычно используются ослабленные лазерные импульсы, которые описываются когерентными квантовыми состояниями. Лазерное излучение имеет пуассоновское распределение по числу фотонов, поэтому с определённой вероятностью, зависящей от среднего числа фотонов, в когерентных состояниях могут встречаться посылки, в которых присутствуют два, три и более фотонов с убывающими вероятностями. Это оказывается важным допущением, так как использование многофотонных состояний в

сочетании с неизбежным затуханием в реальных каналах связи даёт перехватчику теоретическую возможность задержать часть фотонов у себя, а после получения некоторых сведений от легитимных пользователей, передаваемых по открытому каналу, извлечь из них всю необходимую информацию, в результате чего схемы квантовой криптографии теряют свою секретность. Подобные действия перехватчика получили название атаки с разделением по числу фотонов, или PNS-атаки (Photon number splitting attack)[1].

Разработки в области противодействия PNS-атаке привели к появлению протокола с изменённой (по сравнению с BB84) конфигурацией состояний, используемых легитимными пользователями. Подобная конфигурация хотя и обеспечивает меньшую скорость генерации ключа, уже не позволяет перехватчику получить всю необходимую информацию о ключе даже при успешной задержке части передаваемых фотонов в своей квантовой памяти. Наиболее известным протоколом, устойчивым к PNS-атаке, является протокол SARG04[1, 11], предложенный в 2004 году. Как показал анализ, он перестаёт быть секретным только в том случае, когда перехватчик имеет возможность блокировать все одно-, двух- и трёхфотонные посылки. А это значит, что квантовое распространение ключей возможно на большей дистанции, чем при использовании протокола BB84, так как возможная длина линии связи зависит от среднего числа фотонов в посылке. Таким образом, можно говорить о понятии критической дистанции секретного распределения ключей, на которой доля доля импульсов с большим числом фотонов достаточно мала, и устойчивость протокола против PNS-атаки определяется именно этой критической дистанцией.

Глава 1

О задаче секретной передачи данных

Задача передачи секретной информации известна человечеству с самых ранних времён. Из основных типов сведений, для которых может быть важна их секретная передача, можно выделить следующие:

- важная государственная информация
- информация, содержащая военные секреты
- коммерческие данные
- личная конфиденциальная информация

Исход большого количества военных кампаний и финансовый успех многих корпораций всегда был напрямую связан в том числе с умением передавать информацию без её утечки к третьим лицам, что говорит о существенной ценности развития технологий секретной передачи данных.

В этой главе будет дано краткое описание исторических сведений о секретной пересылке

информации, а также будут рассмотрены несколько типов криптографических систем, используемых в настоящее время.

1.1 Исторические сведения

Можно выделить три основных технологии передачи конфиденциальной информации:

1. Конструирование полностью секретного канала связи — этот метод оказывается наиболее сложным, и его сложность лишь увеличивается с развитием технологий подслушивания.

2. Сокрытие самого факта передачи информации — этот метод получил название *стеганографии*, и с тем или иным успехом использовался во все времена. С расширением технологического арсенала применение этого метода становится всё проще, однако с другой стороны у него есть существенные недостатки: так, трудно обеспечить гарантии непопадания информации третьим лицам, и при использовании одного и того же способа стеганографии в течение долгого времени велика вероятность того, что предполагаемый перехватчик также читает сообщения, не выдавая себя.

3. Открытая передача сообщения по открытому каналу, но лишь после специального преобразования — *зашифрования*, подразумеващего невозможность получения полезной информации о сообщении без знания определённых данных — *секретного ключа*. Криптография изучает именно этот способ передачи секретной информации.

Исторические способы шифрования данных

Применение шифров началось ещё несколько тысячелетий назад, и за прошедшее время было изобретено огромное количество технологий шифрования той или иной степени надёжности. Рассмотрим некоторые наиболее известные из самых ранних способов защиты информации.

Шифр «Сцитала». Этот метод шифрования известен ещё со времен войны между Афинами и Спартой в V в. до н.э. В нем использовалась специальная дощечка круглой формы и определенного радиуса, называемая сциталой. На сциталу наматывалась лента, на которой (вдоль оси сциталы) писался текст. Затем лента разматывалась и отправлялась получателю. Он, имея в распоряжении сциталу того же радиуса, наматывал на неё ленту и читал сообщение. Всем же остальным сообщение представлялось лишь бессвязным набором символов, записанных в столбик.

Шифр Цезаря. Этот способ шифрования заключается в том, что каждая буква исходного сообщения заменяется третьей по счету буквой алфавита, следующей за ней. Алфавит в этом случае считается циклическим, то есть за последней его буквой снова следует первая. Получатель сообщения может безошибочно восстановить его исходный текст, заменив каждую букву третьей по счёту до него. Сам Цезарь использовал сдвиг на 3 позиции, в то время как более общая версия подобного шифра, называемого *шифром сдвига*, может использовать любую величину сдвига: важно лишь, чтобы её знали как отправитель сообщения, так и его получатель.

Шифр замены. Этот способ шифрования является дальнейшим обобщением шифра Цезаря: в нём каждая буква заменяется не следующей за ней в алфавите на

некотором интервале, а буквой (или другим символом), получающейся из исходной с использованием специальной таблицы, известной только передающей и принимающей стороне. Такая таблица имеет вид

$$\begin{array}{cccccc} a & b & c & d & e & \ldots \\ g & r & e & x & o & \ldots, \end{array}$$

то есть каждой букве в ней поставлена в соответствие новая буква. Очевидно, что по сравнению с шифром сдвига такой шифр взломать значительно сложнее: уже недостаточно перебрать 26 (число букв в латинском алфавите) вариантов, так как подобных таблиц намного больше — 26!. Также вместо букв сообщение может шифроваться другими известными обеим сторонам символами. Подобный шифр можно встретить, к примеру, в рассказе А. Конан Дойла «Пляшущие человечки».

Отметим, что по современным меркам все приведённые методы шифрования нельзя назвать сколь-либо удовлетворительными: при знании самих методов шифрования (а узнать их можно, например, подкупив кого-нибудь из лиц, приближённых к обменивающимся информацией) их очень легко взломать. Для первых двух шифров элементарно подобрать соответственно диаметр сциталы и величину сдвига, а в случае общего шифра замены может помочь знание статистики упоминания разных букв языка, на котором происходит общение [21].

Криптографические протоколы

Задача передачи секретного сообщения между двумя абонентами — главная, но не единственная задача криптографии. Существует ещё ряд важных задач, близких по технологиям их решения. Согласованные

действия пользователей, приводящие к решению подобной задачи, называются *криптографическим протоколом*. Приведём здесь несколько примеров подобных задач.

Протокол распределения ключей ставит своей целью генерацию общего случайного ключа между двумя пользователями с условием того, чтобы он был известен только им и никому другому. Как будет показано в дальнейшем, наличие подобного ключа нужной длины практически означает возможность гарантированно секретной передачи данных. Таким образом, задачу генерации ключа можно считать эквивалентной задаче передачи секретного сообщения.

Протокол подписания контракта решает задачу, возникающую при подписании соглашений удалёнными абонентами: два не доверяющих друг другу человека при подписании контракта не хотят допустить ситуацию, при которой один из абонентов получил подпись другого, а сам не подписался.

Протокол аутентификации работает со следующей задачей: при взаимодействии двух человек у каждого из них могут возникнуть опасения, что их собеседник — не тот, за кого себя выдаёт. Задача аутентификации состоит в том, чтобы убедить собеседника в собственной личности.

Наиболее распространённой криптографической задачей является пересылка секретных данных. Основных действующих лиц, участвующих в обмене информацией, принято называть по именам: обычно в книгах и статьях по криптографии передающую сторону называют Алисой, принимающую сторону — Бобом, а подслушивателя, стремящегося перехватить сообщение и получить секретную информацию — Евой. В итоге задача Алисы состоит в передаче сообщения Бобу таким образом, чтобы Ева (предпринимающая определённый набор отведённых

ей действий) не могла получить достаточно информации об исходном тексте сообщения. В каждом конкретном случае могут допускаться разные наборы возможных действий Евы, так как возможности преполагаемых перехватчиков различны: это могут быть как хулиганы, так и мощные государственные структуры.

1.2 Симметричные шифры

Все рассмотренные в первом разделе способы шифрования использовали некоторый ключ, который (при знании алгоритма) нужно было также знать для расшифровки сообщения: это диаметр сциталы в первом случае, величина сдвига при применении шифра Цезаря и таблица значений при использовании общего шифра замены. Легко видеть, что в каждом из этих случаев для зашифрования и расшифрования данных использовался один и тот же ключ. Методы, обладающие этим важным свойством, носят название *симметричных шифров*. В этом разделе будут рассмотрены теоретические основы симметричных криптографических систем, а также будет дана схема обоснования полной секретности одноразового блокнота — единственного полностью секретного шифра, важным частным случаем которого является шифр Вернама [16].

Стойкость симметричного шифрования

Итак, главным свойством симметричных шифров является то, что в них используется один и тот же ключ k для зашифрования и расшифрования сообщения. Это можно обозначить как

$$C = E_k(m), \quad m = D_k(C),$$

где E и D — соответственно шифрующая и расшифровывающая функции, m — исходный текст сообщения, а C — шифротекст.

Дадим теоретическое обоснование стойкости одной из наиболее важным систем симметричного шифрования — одноразового ключа-блокнота. Введём обозначения:

$\mathbb{P}$ — множество всевозможных открытых текстов P,

$\mathbb{C}$ — множество шифротекстов C,

$\mathbb{K}$ — множество ключей K.

На каждом из приведённых множеств введена вероятность выбора соответствующего элемента. Очевидно, что для возможности однозначного расшифрования сообщения P требуется инъективность шифрующей функции, а из этого следует, что множество $\mathbb{C}$ должно содержать не меньше элементов, чем $\mathbb{P}$. Будем обозначать это как $|\mathbb{C}| \geq |\mathbb{P}|$. Также целесообразно считать, что $p(P = m, K = k) = p(P = m)p(K = k)$: выбор ключа не должен зависеть от передаваемого сообщения.

При вскрытии шифра Ева стоит перед задачей нахождения исходного текста сообщения m по его шифротексту c. Её вероятность узнать его равна

$$p(P = m|C = c) = \frac{p(P = m)p(C = c|P = m)}{p(C = c)}. \qquad (1.1)$$

Цель легитимных пользователей состоит в том, чтобы шифротекст давал как можно меньше информации об исходном сообщении, то есть подобная условная вероятность должна быть как можно ближе к вероятности $p(P = m)$. Таким образом, мы приходим к определению *абсолютной стойкости криптосистемы*:

Определение 1 *Криптосистема называется абсолютно стойкой, если для всех открытых текстов $m \in \mathbb{P}$ и для всех шифрограмм $c \in \mathbb{C}$ выполняется*

$$p(P = m|C = c) = p(P = m). \tag{1.2}$$

Из формулы (1.1) очевидно, что (1.2) в определении эквивалентно

$$p(C = c|P = m) = p(C = c).$$

Наиболее важный результат, относящийся к симметричным криптосистемам — это теорема Шеннона (1949 г.), дающая критерии абсолютно стойкой системы [21]:

Теорема 1 *Симметричная система, заданная набором*

$$(\mathbb{P}, \mathbb{C}, \mathbb{K}, E_k(\cdot), D_k(\cdot)),$$

где $|\mathbb{P}| = |\mathbb{C}| = |\mathbb{K}|$, является абсолютно стойкой тогда и только тогда, когда выполнены два условия:

1. *Вероятности использования всех ключей равны: $p(K = k) = 1/|\mathbb{K}|, \forall k \in \mathbb{K}$*

2. *Для каждой пары сообщения $m \in \mathbb{P}$ и шифротекста $c \in \mathbb{C}$ существует только один ключ k такой, что $E_K(m) = c$.*

Одноразовый шифр-блокнот

Теорема Шеннона даёт требования к шифру, которые более неформальным образом можно записать так: для абсолютной стойкости шифра необходимо и достаточно, чтобы ключ полностью случайно выбирался

из множества, мощность которого равна мощности множества открытых текстов, и использовался лишь однократно для пересылки каждого сообщения. Подробнее эти принципы можно проиллюстрировать на примере *шифра Вернама*[16], который был предложен в 1917 г. (то есть до формулировки теоремы Шеннона).

Шифр Вернама работает так: передаваемое сообщение записывается в двоичном формате, а затем берется полностью случайный ключ такой же длины, и Алиса производит операцию побитового сложения сообщения и ключа. Боб, зная ключ, производит на своей стороне побитовое сложение ещё раз, получая в точности исходное сообщение. После выполнения этих операций ключ перестаёт использоваться, что объясняет другое называние шифра Вернама — *одноразовый шифр-блокнот*.

Следствием абсолютной стойкости шифра Вернама является то, что ранее рассмотренная задача генерации ключей может использоваться для секретной пересылки данных, так как обладая достаточным запасом случайных ключей Алиса и Боб могут воспользоваться этим шифром для распространения информации. Таким образом, одной из важнейших криптографических задач становится генерация секретных ключей у легитимных пользователей, и как показывает опыт, эта задача оказывается весьма непростой.

Использование псевдослучайных генераторов

Развитие технологий послушивания делает задачу распредления ключей сложной и дорогостоящей, поэтому встаёт вопрос о том, насколько секретной

может считаться криптографическая система, более «экономно» использующая секретные ключи. Поскольку подобные системы не соответствуют требованиям теоремы Шеннона, их нельзя назвать абсолютно стойкими, и требуются новые методы для оценки степени их защищённости.

Не вдаваясь в подробности, дадим описание этих методов. Заметим, что при атаке на шифр Вернама у Евы есть два основных типа действий: попытка угадать ключ (не требует большого времени, но имеет мало шансов дать успешный результат) и перебор всех его возможных вариатов (всегда даёт верный ответ, но может требовать очень большого времени). Оценка стойкости криптографических протоколов подразумевает получение соотношения на шансы Евы подобрать ключ в зависимости от доступного ей времени: хорош тот протокол, при котором Ева, даже потратив значительное время на подбор ключа, имеет мало шансов узнать его.

Один из способов передачи секретной информации с помощью секретного ключа меньшего размера подразумевает использование *псевдослучайных генераторов* — алгоритмов, которые по заданному ключу k длины l строят последовательность символов большей длины $p(l)$, по которой «сложно» вычислить исходный ключ k. В этом случае полученная последовательность оказывается близка к случайной, отсюда и название. «Сложность» задачи означает то, что время её гарантированного выполнения экспоненциально зависит от длины входных параметров, в то время как для «простых» задач эта зависимость полиномиальна. Если Алиса и Боб используют один и тот же псевдослучайный генератор, то они могут из исходного ключа построить ключ большей длины, практически не нарушив его

секретность, так как Еве требуется много времени, чтобы узнать исходный ключ.

Вопрос о существовании псевдослучайных генераторов до сих пор остаётся открытым, и было показано, что он тесно связан с нерешённой проблемой равенства классов сложности P и NP[25], а именно: если $P = NP$, то псевдослучайных генераторов не существует (то есть найдутся «быстрые» алгоритмы получения исходного ключа по сгенерированной последовательности), в противном же случае ничего об их существовании сказать нельзя, то есть возможно, что при $P \neq NP$ псевдослучайных генераторов нет. Это значит, что существование псевдослучайных генераторов является более сильным утверждением, чем $P \neq NP$. Таким образом, стойкость симметричных криптографических протоколов, использующих псевдослучайные генераторы, основывается на недоказанном утверждении, которое оказывается неверным в случае $P = NP$, что означает немалую угрозу их надёжности. Отметим, однако, что по мнению большинства современных математиков классы сложности P и NP не совпадают.

1.3 Криптографические системы с открытым ключом

Большим неудобством, связанным с использованием симметричных криптографических протоколов, оказывается необходимость наличия секретного ключа между каждой парой обменивающихся информацией абонентов. Так, если имеется группа из n человек, внутри которой требуется обеспечить возможность пересылки секретных сообщений (защищённых в том

числе и от других абонентов группы), то для решения подобной задачи требуется $(n-1)!$ ключей — число, слишком большое для практического применения. В то же время описанная ситуация встречается очень часто, особенно с появлением Интернета, в котором число взаимодействующих друг с другом пользователей очень велико. Долгое время считалось, что подобная задача не может быть эффективно решена, однако в 1976 году вышла статья «Новые направления в криптографии» Диффи и Хеллмана [5], в которой была описана технология шифрования, прекрасно подходящая именно для ситуаций, подобных описанной выше.

Односторонние функции

Основным понятием статьи Диффи и Хеллмана стали *односторонние функции*, которые неформально можно описать так: для каждой односторонней функции $F(x)$ существует полиномиальный алгоритм её вычисления, но в то же время не существует полиномиального алгоритма её инвертирования, то есть решения уравнения $F(x) = y$ при известном y. С односторонними функциями также тесно связано понятие *функции с секретом* $F_K(x)$: такой функции, которую легко вычислить при любых значениях K и x, но возможности инвертирования которой существенно зависят от знания K: при известном K функцию можно инвертировать за полиномиальное вермя, в то время как если K неизвестно, то полиномиального алгоритма инвертирования $F_K(x)$ не существует.

Опишем, как происходит пересылка сообщения с использованием функций с секретом. Алиса, чтобы дать другим возможность отправлять ей шифрованные сообщения, выбирает функцию с секретом $F_K(x)$ и открыто объявляет её, оставляя в тайне секрет K.

Боб, чтобы послать Алисе сообщение x, вычисляет за полиномиальное время $F_K(x)$ и открыто передаёт результат Алисе. Так как Алиса, зная K, может легко инвертировать результат, она без труда сможет прочитать исходное сообщение. В то же время если результат попадёт Еве, она при достаточной его длине не сможет инвертировать функцию $F_K(x)$ за разумное время, поэтому не получит никакой полезной информации. Таким образом, для пересылки секретной информации уже нет надобности генерировать специальный секретный ключ непосредственно между Алисой и Бобом, поэтому схема с открытым ключом прекрасно подходит для обмена информацией между большим количеством пользователей: каждому из них теперь достаточно иметь два ключа: открытый, который объявляется всем для возможности шифровать информацию, и секретный, который держится в секрете и используется для расшифровки приходящих сообщений.

Как и в случае использования псевдослучайных генераторов в симметричных криптосистемах, до сих пор открытым остаётся вопрос о существовании односторонних функций и функций с секретом. Более того, оказывается, что эти два вопроса эквивалентны: односторонние функции (а вместе с ними и функции с секретом) существут в том и только том случае, когда существуют псевдослучайные генераторы[25], поэтому криптосистемы с открытым ключом также нельзя считать гарантированно надёжными.

Алгоритм RSA

Наиболее известной функцией с секретом является произведение двух простых чисел: действительно, легко перемножить два даже очень больших числа «в столбик»

и несложно разделить число на один из его сомножителей, чтобы получить другой. В то же время до сих пор не было найдено алгоритма, достаточно быстро раскладывающего произвольное составное число на два сомножителя, хотя ввиду большой важности этой задачи над ней десятилетиями работает большое количество исследователей.

Алгоритм RSA[10], самый распространённый алгоритм шифрования с открытым ключом, основан на так называемой «задаче RSA», которая эквивалентна задаче факторизации в том смысле, что при решении одной из этих задач можно быстро (за полиномиальное время) решить вторую. Поскольку задача факторизации выглядит более наглядной, принято считать, что алгоритм RSA сводится именно к ней.

Опишем схему алгоритма RSA. Сначала Алиса выбирает два больших простых числа p и q и вычисляет их произведение N. Затем она выбирает число E, удовлетворяющее соотношению

$$(E, (p-1)(q-1)) = 1.$$

Алиса объявляет всем желающим пару (N, E), которая и является открытым ключом. Далее Алиса вычисляет число d, называемое секретной экспонентой и удовлетворяющее условию

$$E \cdot d = 1 (\mathrm{mod} (p-1)(q-1)). \tag{1.3}$$

Секретным ключом Алисы является тройка (p, q, d).

Если Боб хочет послать зашифрованное сообщение Алисе, то он должен представить его в виде числа m, меньшего объявленного Алисой N. Далее Боб получает шифротект по формуле

$$C = m^E (\mathrm{mod} N). \tag{1.4}$$

Алиса после получения шифрограммы может легко её расшифровать, воспользовавшись числом d:

$$m = C^d (\mathrm{mod} N). \tag{1.5}$$

Действительно, из простоты p и q следует, что функция Эйлера $\varphi(N) = (p-1)(q-1)$ и по теореме Эйлера

$$x^{(p-1)(q-1)} = 1 (\mathrm{mod} N).$$

Далее, из (1.3) следует, что для некоторого s

$$Ed = 1 + s(p-1)(q-1),$$

откуда окончательно получаем, что

$$C^d = m^{Ed} = m^{1+s(p-1)(q-1)} = m \cdot m^{s(p-1)(q-1)} = m (\mathrm{mod} N).$$

Задача, используемая в этом алгоритме, носит название задачи RSA: по заданным числам C и E, последнее из которых удовлетворяет

$$(E, (p-1)(q-1)) = 1$$

для некоторых простых p и q, требуется найти число m, удовлетворяющее соотношению

$$m^E = C (\mathrm{mod} pq).$$

Как уже было сказано, эта задача эквивалентна задаче разложения числа $N = pq$ на простые сомножители.

Возможность создания квантового компьютера

Из-за чрезвычайно широкой распространённости алгоритма RSA одним из важнейших предположений

криптографии является сложность задачи факторизации больших чисел. И действительно, до настоящего времени не было найдено алгоритма, достаточно быстро решающего эту задачу. Однако в 1994 г. Шором[14] был предложен алгоритм, с полиномиальной сложностью решающий эту задачу на квантовом компьютере. Главная причина подобного феноменального ускорения — в возможности использования так называемого «квантового параллелизма» для проведения быстрого преобразования Фурье, на котором основаны наиболее эффективные из известных алгоритмов факторизации. Нахождение этого алгоритма позволяет свести задачу факторизации к технологической задаче построения квантового компьютера: если его удастся построить, схема шифрования RSA окажется ненадёжной. Это ставит возможности шифрования с открытым ключом под большую угрозу. Стоит, однако, отметить, что за последнее десятилетие не было достигнуто существенного прогресса в построении квантового компьютера.

Далее в этой работе будет показано, как использование свойств квантовой информации может не только нарушить секретность алгоритма RSA, но и предоставить новые возможности для секретной передачи данных. Как будет ясно из дальнейшего изложения, протоколы квантового распределения ключей позволяют на приемлемой скорости генерировать полностью секретные ключи между удалёнными абонентами.

Глава 2

Основные понятия квантовой теории информации

Квантовая теория информации лежит на стыке двух наиболее значительных теорий XX века: квантовой механики и теории информации. Она имеет дело с кванновомеханическими состояниями и рассматривает их способность участвовать в переносе и обработке информации. Эта наука появилась в 60-е гг. XX в., во времена бурного развития вычислительной техники, как следствие того, что при постоянном уменьшении размеров вычислительных устройств со временем неизбежно возникнет необходимость использовать одиночные квантовые состояния в качестве информационного ресурса. В то время подобная перспектива означала новые сложности, в перую очередь сильное влияние квантового шума, который считался однозначно разрушающим фактором. Однако при более подробном изучении этого явления выяснилось, что квантовый шум может и оказывать существенную помощь при

передаче и обработке информации: так, явление квантового «размазывания» частицы по нескольним точкам пространства обладает свойством интерференции, способном в ряде случаев принести большую пользу. Квантовая теория информации как новая наука работает с квантовыми явлениями, устанавливает их свойства и изучает применяющие их технологии. Оказывается, что в частности применение квантовых состояний способно вывести скорость вычислений на новый уровень благодаря идее квантового компьютера, а также гарантировать абсолютную секретность распространения ключей в квантовой криптографии.

В этой главе будут рассмотрены основные понятия и факты квантовой теории информации, которые будут использоваться при изложении свойств протоколов квантовой криптографии в дальнейшем.

2.1 Квантовые состояния

При проведении первых опытов над элементарыми частицами было обнаружено, что их поведение очень сложно увязать с имевшимися на тот момент представлениями о физических явлениях. Это привело к тому, что после формулировки новых законов, описывающих поведение элементарных частиц, эту часть физики стали называть квантовой теорией, а сложившуюся на тот момент физическую картину мира — классической.

Волновая функция и чистые состояния

Существенных отличий квантовой теории от классической несколько, и одно из главных таких отличий проявляется

уже в самом определении квантовой частицы и её состояния. Представление о такой частице как о некотором теле, имеющем определенные координаты, размеры и массу, оказалось в корне неверным, так как для некоторых таких частиц не удавалось даже в принципе понять, в какой точке пространства они находятся. Зато оказалось возможным предсказывать поведение таких частиц. Однако трудность заключалась в том, что объяснить это поведение удалось лишь после окончательного отказа от попыток вычислить в точности все «традиционные» физические характеристики системы. Это привело к тому, что состояние всякой элементарной частицы (или системы частиц, если их несколько) стало представляться с помощью так называемой «волновой функции» — принципиально нового объекта квантовой картины мира.

Введем сначала понятие *чистого квантового состояния*. Таким состоянием будем называть вектор в гильбертовом пространстве $\mathcal{H}$ с единичной нормой. Под нормой вектора понимается корень из его скалярного квадрата:

$$\|\psi\| = \sqrt{(\psi, \psi)}, \quad \psi \in \mathcal{H}$$

В рамках данной работы будут рассматриваться только конечномерные гильбертовы пространства, и из их свойств наиболее важным будет наличие скалярного произведения. Так, для вектора ψ свойство единичной нормы можно аналогично записать как $\psi^*\psi = 1$.

Легко связать приведенное определение с традиционным формализмом волновых функций: каждой волновой функции соответствует вектор ψ, i-я координата которого ψ_i равна амплитуде вероятности обнаружения частицы в i-й точке пространства. Таким образом, становится важной задача нахождения пространства, наилучшим образом соответствующего условиям задачи.

Требование нормировки состояния говорит о том, что полная вероятность обнаружения частицы равна единице.

В квантовой теории информации для состояний и операторов принято использовать обозначения, введенные Дираком. Состояние ψ будем обозначать как $|\psi\rangle$, а сопряженное состояние ψ^*, используемое в скалярном произведении, как $\langle\psi|$. Тогда скалярное произведение векторов φ и ψ записывается как $\langle\varphi|\psi\rangle$.

Для каждого чистого квантового состояния $|\psi\rangle$ можно определить соответствующий ему оператор $\rho_\psi = |\psi\rangle\langle\psi|$, называемый оператором плотности. Этот оператор имеет ранг 1, его след равен единице и он действует как проектор на чистое состояние $|\psi\rangle$.

Смешанные состояния

С помощью операторов плотности вводится общее понятие квантового состояния. *Смешанным квантовым состоянием* называется статистическая смесь нескольких чистых состояний (то есть набор чистых состояний с соответствующими вероятностями):

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad p_i \geq 0 \quad \forall i, \quad \sum_i p_i = 1.$$

Очевидно, что след смешанного состояния равен единице. Его положительную определенность также несложно показать:

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i |\langle\varphi|\psi\rangle|^2 \geq 0 \quad \forall |\varphi\rangle \in \mathcal{H}.$$

Далее, любой эрмитов оператор A, как известно, имеет спекральное разложение

$$A = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|,$$

где собственные значения λ_i вещественны, а собственные векторы $|\lambda_i\rangle$ нормированы и ортогональны. Это означает, что любой положительный эрмитов оператор с единичным следом можно назвать оператором плотности некоторого квантового состояния: из положительной определенности следует положительность всех собственных значений (которые трактуются как вероятностные веса), а из условия единичного следа — то, что сумма собственных значений равна единице, а значит, подобная их комбинация может трактоваться как статистическая смесь. Это приводит к общему определению квантового состояния:

Определение 2 *Квантовое состояние — положительный эрмитов оператор в гильбертом пространстве $\mathcal{H}$ с единичным следом.*

Квантовые состояния образуют выпуклое множество в пространстве операторов над $\mathcal{H}$. Множество квантовых состояний принято обозначать $\mathcal{S}(\mathcal{H})$. Крайними точками этого множества являются чистые квантовые состояния, описывающиеся операторами ранга 1.

Изменение состояний во времени

Одним из ключевых законов квантовой механики является уравнение Шрёдингера, которое описывает изменение квантовых состояний во времени. В традиционных курсах квантовой механики это уравнение записывается как

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle, \tag{2.1}$$

где $\hbar$ — постоянная Планка, определяемая из эксперимента и равная приблизительно $1,054 \times 10^{-34}$ Дж·с.

Эрмитов оператор H называется гамильтонианом системы и именно он оказывает влияние на её эволюцию.

В силу соответствия между эрмитовыми и унитарными операторами[20]

$$U = e^{iH}$$

уравнение Шрёдингера может быть переписано в виде

$$|\psi'\rangle = U|\psi\rangle. \tag{2.2}$$

Для дальнейших выкладок именно такой вид уравнения Шрёдингера оказывается наиболее удобным, так как он означает, что любая эволюция квантовой системы может быть представлена как действие некоторого унитарного преобразования. Напомним, что унитарным оператором называется оператор, удовлетворяющий условию

$$UU^\dagger = U^*U = I.$$

Кубиты

Простейшим примером нетривиального квантового объекта является система с двумя базисными состояниями. Физическими примерами подобных систем могут быть фотоны с соответствующими направлениями поляризации (вертикальной $|\updownarrow\rangle$ и горизонтальной $|\leftrightarrow\rangle$) или направления спина электрона (вверх $|\uparrow\rangle$ и вниз $|\downarrow\rangle$). В этом случае соответствующее гильбертово пространство будет двумерным, и его принято обозначать $\mathcal{H}^2$. Обычно, если не важна конкретная физическая природа двухуровневой системы, её состояния обозначают как $|0\rangle$ и $|1\rangle$. По аналогии с классическим битом такую систему называют *кубитом*, что означает «квантовй бит».

Произвольное чистое состояние кубита можно записать как

$$|\psi\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle,$$

ранг же оператора плотности ρ может быть равен 1 (для чистого состояния $|\psi\rangle\langle\psi|$) или 2 — для смешанного состояния, которое в случае $\mathcal{H}^2$ всегда может быть представлено как статистическая смесь двух ортогональных чистых состояний:

$$\rho = p|\psi\rangle\langle\psi| + (1-p)|\psi^\perp\rangle\langle\psi^\perp|.$$

2.2 Измерения

Именно процедура измерений квантовых состояний отличает квантовый случай проведения опытов от классического и дает возможность применения квантовой криптографии. Важнейшим отличием квантовой механики от классической является то, что в общем случае *измерение квантовой системы меняет её исходное состояние.*

Квантовые наблюдаемые

Рассмотрим сначала общие принципы проведения экспериментов над некоторой физической системой. В любом эксперименте можно выделить две его стадии: приготовление состояния ρ и его измерение M. Измерение не обязано давать точно предсказуемый результат, в общем случае результат измерения — это статистический набор исходов $\{x\}$ с соответствующими вероятностями $\mu_\rho(x)$. Естественно требовать, чтобы для статистических ансамблей нескольких квантовых состояний результаты их наблюдения также были статистическими смесями

результатов наблюдения соответствующих отдельных состояний ансамбля. Такое требование называется требованием аффинности:

$$\mu_S(x) = \sum_i p_i \mu_{\rho_i}(x), \qquad \rho = \sum_i p_i \rho_i. \tag{2.3}$$

Этого требования оказывается достаточно для следующего утверждения [23]:

Теорема 2 *Пусть $\rho \to \mu_\rho$ — аффинное отображение множества квантовых состояний $\mathcal{S}(\mathcal{H})$ в вероятностные распределения на конечном множестве X. Тогда существует семейство эрмитовых операторов $\{M_x\}$ в $\mathcal{H}$, такое, что*

$$\begin{gathered} M_x \geq 0, \quad \sum_{x \in X} M_x = I, \\ \mu_\rho(x) = Tr \rho M_x \end{gathered} \tag{2.4}$$

Эта теорема утверждает, что измерение квантовой системы можно связать с набором положительных эрмитовых операторов, сумма которых равна единичному оператору. В этом случае вероятность каждого из исходов равна следу произведения состояния и оператора, соответствующего данному исходу. Это приводит к следующему определению:

Определение 3 *Квантовая наблюдаемая со значениями из множества X — набор эрмитовых операторов $\{M_x\}_{x \in X}$, таких, что*

$$M_x \geq 0, \quad \sum_{x \in X} M_x = I. \tag{2.5}$$

Такой набор операторов называют также *разложением единицы*.

Из приведенной теоремы следует, что при измерении состояния ρ, описываемом разложением единицы $\{M_x\}$, вероятность получить каждый из исходов x равна

$$Pr(x|\rho) = \mathrm{Tr} M_x \rho, \tag{2.6}$$

а для чистого состояния $|\psi\rangle$ в силу свойств следа эта вероятность даётся более простым выражением

$$Pr(x|\rho_\psi) = \langle\psi|M_x|\psi\rangle. \tag{2.7}$$

Коллапс волновой функции

Важным законом квантовой механики является *редукция,* или *коллапс волновой функции*. Это свойство называется также *редукцией фон Неймана* и означает переход состояния после измерения в одно из собственных состояний оператора измерения. Так, при измерении $\{M_i\}$ и получении результата i исходное состояние будет преобразовано в

$$\rho_i' = \frac{\sqrt{M_i}\rho\sqrt{M_i}}{\mathrm{Tr} M_i \rho}. \tag{2.8}$$

Это одно из важнейших для квантовой криптографии свойств. Поскольку оно говорит о том, что попытки измерить систему влекут к помехам, из этого следует, что попытки перехвата информации всегда можно детектировать по дополнительным ошибкам на приёмной стороне. В дальнейшем будет показано, как именно происходит обнаружение попыток подслушивания и по их количеству даются оценки возможной утечки информации к перехватчику.

Невозможность достоверного различения неортогональных состояний

Невозможность достоверного различения неортогональных квантовых состояний [20] — важный частный результат, на котором также во многом основывается секретность протоколов квантовой криптографии.

Этот результат можно сформулировать так: для чистых состояний $|\psi_0\rangle$ и $|\psi_1\rangle$, таких, что $\langle\psi_0|\psi_1\rangle = \cos\alpha \neq 0$, не существует измерения $\{M_0, M_1\}$, дававшего точный результат, то есть соответствовавшего условиям

$$\begin{aligned} &\langle\psi_0|M_0|\psi_0\rangle = 1, \quad \langle\psi_1|M_0|\psi_1\rangle = 0, \\ &\langle\psi_0|M_1|\psi_0\rangle = 0, \quad \langle\psi_1|M_1|\psi_1\rangle = 1. \end{aligned} \tag{2.9}$$

Докажем это утверждение. Рассмотрим представление $|\psi_1\rangle$ как линейной комбинации состояния $|\psi_0\rangle$ и его нормированного ортогонального дополнения $|\psi_0^\perp\rangle$:

$$|\psi_1\rangle = a|\psi_0\rangle + b|\psi_0^\perp\rangle, \quad |a|^2 + |b|^2 = 1.$$

Поскольку $|\psi_0\rangle$ и $|\psi_1\rangle$ неортогональны, то $0 < |a|, |b| < 1$. Из условий на операторы измерения (2.9) очевидно следует, что $\sqrt{M_1}|\psi_0\rangle = 0$, а значит,

$$\sqrt{M_1}|\psi_1\rangle = \sqrt{M_1}a|\psi_0\rangle + \sqrt{M_1}b|\psi_0^\perp\rangle = \sqrt{M_1}b|\psi_0^\perp\rangle,$$

из чего следует, что равенство в (2.9) можно записать в виде

$$\langle\psi_1|M_1|\psi_1\rangle = |b|^2\langle\psi_0^\perp|M_1|\psi_0^\perp\rangle \leq |b|^2,$$

а это в силу $|b| < 1$ противоречит (2.9). Полученное противоречие доказывает невозможность различения неортогональных состояний — важнейший факт в квантовой теории информации.

Четкие и нечеткие наблюдаемые

В традционных курсах по квантовой механике под наблюдаемой обычно подразумевают лишь ортогональное разложение единице, при котором операторы $\{M_i\}$ удовлетворяют соотношению

$$M_i M_j = \delta_{ij} M_i. \tag{2.10}$$

Такие наблюдаемые в дальнейшем будем называть *чёткими наблюдаемыми* [23]. В то же время требование взаимной ортогональности всех операторов не является обязательным, и более того, в некоторых случаях с точки зрения получения максимального количества информации выгоднее пользоваться наблюдаемыми, в которых не все операторы ортогональны друг другу. Такие наблюдаемые называются *нечёткими*.

На первый взгляд нечёткие наблюдаемые лишь смешивают вероятности разных исходов, а значит, не могут принести дополнительной пользы. Однако это не так. Рассмотрим пример того, как нечёткая наблюдаемая может помочь различить неортогональные состояния $|\varphi\rangle$ и $|\psi\rangle$:

$$\langle\varphi|\psi\rangle = \cos\eta.$$

Одно из возможных измерений для такой пары состояний принято называть «измерение с тремя исходами», и оно, как видно из названия, использует три результата: $\{0, 1, ?\}$. Соответствующие эрмитовы операторы равны

$$\begin{aligned} M_0 &= \frac{|\psi^\perp\rangle\langle\psi^\perp|}{1+\cos\eta} = \frac{I - |\psi\rangle\langle\psi|}{1+\cos\eta}, \\ M_1 &= \frac{|\varphi^\perp\rangle\langle\varphi^\perp|}{1+\cos\eta} = \frac{I - |\varphi\rangle\langle\varphi|}{1+\cos\eta}, \\ M_? &= I - M_0 - M_1. \end{aligned} \tag{2.11}$$

Нетрудно видеть, что

$$\mathrm{Tr}M_0|\psi\rangle\langle\psi| = \langle\psi|M_0|\psi\rangle = \frac{\langle\psi|\psi^\perp\rangle\langle\psi^\perp|\psi\rangle}{1+\cos\eta} = 0,$$

и аналогично $\mathrm{Tr}M_1|\varphi\rangle\langle\varphi| = 0$. Это значит, что при применении такого измерения нет шансов получить исход 0 при измерении состояния $|\psi\rangle$, а при измерении состояния $|\varphi\rangle$ аналогичным образом не может получиться исход 1. Это означает, что подобное измерение позволяет безошибочно различать неортогональные состояния. Цена этого — некоторая вероятность (равная $\cos\eta$) получить несовместный исход «?», который отвечает уклонению от принятия решения.

Связь между четкими и нечеткими наблюдаемыми становится ясной из теоремы Наймарка[23]:

Теорема 3 *Пусть* $\{M_i\}_{i=1}^n$ — *разложение единицы в пространстве* $\mathcal{H}$ *размерности* d. *Тогда существует пространство* $\mathcal{H}'$ *размерности не более* nd *и ортогональное разложение единицы в нём* $\{M_i'\}$, *а также изометрический оператор* V, *такой, что выполняется*

$$M_i = VM_i'V^\dagger$$

Таким образом, как утверждает приведенная теорема, всякой нечеткой наблюдаемой можно поставить в соответствие чёткую наблюдаемую в расширенном пространстве.

2.3 Составные квантовые системы

Рассмотрение квантовых систем, состоящих из нескольких частиц (их называют *составными системами*),

может порой привести к интересным свойствам, не встречающимся в классическом случае. Ещё в 1935 году в переписке Эйнштейна, Подольского и Розена [6] были отмечены очень необычные свойства составных квантовых систем, противоречащие локальности: выходило, что действия над одной из подсистем могут мгновенно оказать влияние на другую подсистему, каково бы ни было расстояние между ними. Описание этого свойства привело к возникновению формализма составных квантовых систем и свойств совершаемых над ними действий.

Тензорное произведение

Определим для начала то, в каком пространстве обитают составные квантовые системы.

Рассмотрим сначала наиболее элементарный случай двух кубитов. На интуитивном уровне очевидно, что возможны 4 варианта их совместного состояния:

- оба кубита в состоянии $|0\rangle$
- первый кубит в состоянии $|0\rangle$, второй — в состоянии $|1\rangle$
- первый кубит в состоянии $|1\rangle$, второй — в состоянии $|0\rangle$
- оба кубита в состоянии $|1\rangle$

Именно эти 4 вектора будут являться базисными в пространстве двух указанных кубитов.

Более формально это звучит так. Если есть пространства $\mathcal{H}_1$ и $\mathcal{H}_2$ с размерностями d_1 и d_2 и ортонормированными базисами $\{e_i\}$ и $\{f_i\}$, то можно

определить пространство с базисом $\{e_i \otimes f_j\}$, где i принимает значения от 1 до d_1, а j — от 1 до d_2. Если ввести на новом пространстве скалярное произведение по закону

$$\langle e_i \otimes f_j | e_m \otimes f_n \rangle = \langle e_i | e_m \rangle \cdot \langle f_j | f_n \rangle \tag{2.12}$$

и продолжить его по линейности на остальные векторы, то в результате получится гильбертово пространство, которое называется *тензорным произведением* $\mathcal{H}_1$ и $\mathcal{H}_2$ и обозначается $\mathcal{H}_1 \otimes \mathcal{H}_2$. Очевидно, что его размерность равна $d_1 d_2$.

Тенорное произведение операторов $A_1 \in \mathcal{S}(\mathcal{H}_1)$ и $A_2 \in \mathcal{S}(\mathcal{H}_2)$ — оператор $A_1 \otimes A_2$ в пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$, действующий по закону

$$(A_1 \otimes A_2)|e_1 \otimes e_2\rangle = (A_1|e_1\rangle) \otimes (A_2|e_2\rangle).$$

Встает вопрос о том, всякое ли состояние в пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$ можно задать как тензорное произведение состояний, принадлежащих частичным пространствам $\mathcal{H}_1$ и $\mathcal{H}_2$. Ответ на этот вопрос отрицателен, и классическим контрпримером является состояние в пространстве двух кубитов $\mathcal{H}^2 \otimes \mathcal{H}^2$, называемое ЭПР по первым буквам фамилий первооткрывателей[6]:

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right).$$

Легко видеть, что это состояние нельзя представить в виде тензорного произведения одночастичных состояний:

$$|\psi_{EPR}\rangle \neq (a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle).$$

Частичный оператор плотности и частичные измерения

После определения тензорного произведения операторов плотности возникает потребность определить и обратную операцию, с помощью которой можно было бы по состоянию $\rho_1 \otimes \rho_2 \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ получить исходные операторы $\rho_1 \in \mathcal{S}(\mathcal{H}_1)$ и $\rho_2 \in \mathcal{S}(\mathcal{H}_2)$. Такая операция есть, она называется взятием *частичного следа* и определяется для состояния $\rho_{12} \in \mathcal{S}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ следующим образом:

$$\mathrm{Tr}_{\mathcal{H}_2}\rho_{12} = \sum_{i,j,k} |e_i\rangle\langle e_j|\langle e_i \otimes f_k|\rho_{12}|e_j \otimes f_k\rangle, \tag{2.13}$$

Аналогично для частичного следа по первому подпространству:

$$\mathrm{Tr}_{\mathcal{H}_1}\rho_{12} = \sum_{i,j,k} |f_i\rangle\langle f_j|\langle e_k \otimes f_i|\rho_{12}|e_k \otimes f_j\rangle,$$

где $\{e_i\}$ и $\{f_i\}$ — элементы ортонормированных базисов пространств $\mathcal{H}_1$ и $\mathcal{H}_2$ соответственно.

Нетрудно видеть, что указанная операция действительно является в некотором роде обратной к операции тензорного произведения, так как

$$\mathrm{Tr}_{\mathcal{H}_2}\rho_1 \otimes \rho_2 = \rho_1,$$

$$\mathrm{Tr}_{\mathcal{H}_1}\rho_1 \otimes \rho_2 = \rho_2.$$

Рассмотрим также важный пример применения законов квантовых измерений и составных квантовых систем. Это ситуация, когда квантовое состояние распределено между двумя участниками (или участником и окружением), один из которых производит измерение над своей подсистемой. Такое действие называют *частичным измерением*.

При измерении одной лишь подсистемы над второй подсистемой не производится активных действий, поэтому в разложении единицы, описывающем общее измерение, все операторы, соответствующие второй подсистеме, будут тождественными. Так, если первый участник применяет измерение $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, то в составной системе это измерение будет выглядеть так:

$$M_0 = |0\rangle\langle 0|_1 \otimes I_2, \quad M_1 = |1\rangle\langle 1|_1 \otimes I_2. \tag{2.14}$$

Замечательно, однако, что несмотря на тождественные операторы в правой части, измерение первой подсистемы в общем случае *влияет на состояние второй подсистемы.* Это важное слествие из свойства редукции волновой функции будет прояснено в следующем разделе.

Парадокс измерений ЭПР и явление сцепленности

Рассмотрим уже встречавшееся выше состояние ЭПР в пространстве двух кубитов

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

и посмотрим, что произойдет, если провести измерение (2.14) над первой подсистемой. При выпадении исхода 0 начальное состояние перейдет в

$$\frac{\sqrt{M_0}|\psi_{EPR}\rangle\langle\psi_{EPR}|\sqrt{M_0}}{\langle\psi_{EPR}|M_0|\psi_{EPR}\rangle} = |00\rangle\langle 00|,$$

что соответствует чистому состоянию $|00\rangle$. Аналогично при получении результата 1 исходное состояние преобразуется в $|11\rangle$. Это говорит об удивительном

факте: измерение одной лишь части квантового состояния может фиксировать всё состояние в целом.

Указанное свойство имеет место не для произвольных квантовых состояний, а лишь для их важного класса, называемого *сцеленными состояниями* (entangled states, другой перевод этого термина — «запутанные состояния»). Они определяются как состояния в составном пространстве, которые нельзя представить в виде тензорного произведения состояний в каждом из частичных пространств:

$$\rho_{12} \neq \rho_1 \otimes \rho_2. \tag{2.15}$$

Для состояний, не являющихся сцепленными (их называют *разделимыми*), подобное свойство не имеет места: измерение над одной подсистемой никак не влияет на состояние второй.

Очищение состояний и теорема Шмидта

Очищение смешанных квантовых состояний — важный результат, дающий связь смешанных состояний со сцепленными состояниями в пространствах большей размерности.

Теорема 4 *Для любого смешанного состояния $\rho \in \mathcal{S}(\mathcal{H})$ существует (в общем случае не единственное) чистое состояние $|\psi_\rho\rangle \in \mathcal{H} \otimes \mathcal{H}_E$, такое, что*

$$\rho = Tr_{\mathcal{H}_E} |\psi_\rho\rangle\langle\psi_\rho|. \tag{2.16}$$

Для доказательства рассмотрим спектральное разложение состояния ρ:

$$\rho = \sum_{i=1}^{N} s_i |e_i\rangle\langle e_i|$$

и возьмем пространство $\mathcal{H}_E$ не меньшей размерности, чем число N ненулевых членов в приведенном спектральном разложении. Тогла в $\mathcal{H}_E$ найдётся N ортонормированных векторов $|f_i\rangle$, и можно рассмотреть в качестве $|\psi_\rho\rangle$ состояние

$$|\psi_\rho\rangle = \sum_{i=1}^{N} \sqrt{s_i}|e_i\rangle \otimes |f_i\rangle,$$

которое, очевидно, будет удовлетворять требуемому условию (2.16).$\diamond$

Таким образом, смешанные квантовые состояния можно рассматривать как находящиеся в сцепленном состоянии с некоторой вспомогательной системой в дополнительном пространстве.

Теорема Шмидта[23] даёт другой важный результат, касающийся свойств частичных операторов плотности чистых сцепленных состояний:

Теорема 5 *Для любого чистого состояния* $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ *его частичные состояния* $\rho_1 = Tr_{\mathcal{H}_2}|\psi\rangle\langle\psi|$ *и* $\rho_2 = Tr_{\mathcal{H}_1}|\psi\rangle\langle\psi|$ *имеют одинаковый набор ненулевых собственных значений.*

Отметим, что случай разделимого состояния $|\psi_1\rangle \otimes |\psi_2\rangle$ тривиален, так как его частичные операторы плотности соотвествуют чистым состояниям $|\psi_1\rangle$ и $|\psi_2\rangle$, а значит единственное ненулевое собственное значение каждого из них равно единице. Для сцепленных же состояний этот результат очень примечателен: поскольку собственные значения оператора плотности связаны с вероятностями получения определённых результатов при измерении его в ортогональном базисе, то эта теорема в частности утверждает, что статистики измерений двух подсистем общего сцепленного состояния совпадают.

Невозможность клонирования

Покажем ещё один частичный результат из теории составных квантовых систем, важный для квантовой криптографии. Выше было показано, что неортогональные квантовые состояния нельзя достоверно различить, здесь же будет показано, что такие состояние нельзя и клонировать — например, для того, чтобы собрать более полную статистику результатов измерений.

Преобразование U, клонирующее произвольное чистое квантовое состояние $|\psi\rangle$, можно описать так:

$$U|\psi\rangle \otimes |A\rangle = |\psi\rangle \otimes |\psi\rangle, \tag{2.17}$$

где $|A\rangle$ — исходное состояние вспомогательной системы.

Для того, чтобы показать невозможность такого преобразования, достаточно рассмотреть его действие на базисные состояния $|0\rangle$ и $|1\rangle$

$$\begin{aligned} U|0\rangle \otimes |A\rangle &= |0\rangle \otimes |0\rangle, \\ U|1\rangle \otimes |A\rangle &= |1\rangle \otimes |1\rangle, \end{aligned} \tag{2.18}$$

а также на состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. В силу линейности оператора U и приведённых выше соотношений (2.18) должно выполняться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes |A\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$$

с другой стороны, по определению U, должно получаться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \otimes |A\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle).$$

Полученное противоречие доказывает невозможность клонирования произвольных квантовых состояний.

Отметим, что клонировать состояния из ортогонального набора можно: для этого достаточно, например, измерить их и приготовить состояние, соответствующее результату измерения — в этом случае он будет безошибочным.

2.4 Передача информации по квантовым каналам

При исследовании передачи информации с помощью квантовых состояний возникает ряд вопросов, связанных с характеристиками использующих квантовые объекты каналов. Основной из этих вопросов связан с пропускной способностью таких каналов, то есть с максимальной скоростью безошибочной передачи данных.

Общий случай передачи квантовых состояний

Самый общий случай квантового канала — это отображение квантовых состояний во множество квантовых состояний. Такое отображение можно расширить на случай произвольных операторов в гильбертовом пространстве [23]:

$$\Phi : \mathfrak{T}(\mathcal{H}) \to \mathfrak{T}(\mathcal{H}). \tag{2.19}$$

Под $\mathfrak{T}(\mathcal{H})$ понимается пространство операторов со следовой нормой:

$$\| T \|_1 = \mathrm{Tr}|T|, \qquad |T| = \sqrt{T^* T}, T \in \mathfrak{T}(\mathcal{H}).$$

Подобный подход автоматически даёт два требования, связанных с тем, что оператор плотности должен переходить в оператор плотности:

- положительные операторы должны переходить в положительные;
- должен сохраняться след оператора.

Также естественно требовать аффинность отображения Φ: статистические ансамбли состояний должны переходить также в статистические ансамбли их образов, то есть для набора вероятностей $\{p_i\}$

$$\Phi[\sum_i p_i\rho_i] = \sum_i p_i\Phi[\rho_i], \quad p_i \geq 0, \quad \sum_i p_i = 1. \tag{2.20}$$

Более формально, требования к отображению Φ на пространстве $\mathfrak{T}(\mathcal{H})$ операторов в гильбертовом пространстве таковы:

- линейность: $\Phi[\sum_i c_i\rho_i] = \sum_i p_i\Phi[\rho_i], \quad c_i \in \mathbb{C}$;
- положительность: $\rho \geq 0 \Rightarrow \Phi[\rho] \geq 0$;
- сохранение следа: $\mathrm{Tr}\Phi[\rho] = \mathrm{Tr}\rho$.

Для каждого отображения Φ, действующего на множестве квантовых состояний и соответствующего картине Шрёдингера, определяется сопряженное отображение Φ^*, соответствующее картине Гейзенберга, и действующее на множестве $\mathcal{M}$ квантовых наблюдаемых. Эти отображения связаны соотношением

$$\mathrm{Tr}\Phi[\rho]M = \mathrm{Tr}\rho\Phi^*[M]. \tag{2.21}$$

Сопряженное отображение действует на пространстве $\mathfrak{B}(\mathcal{H})$ операторов с операторной нормой

$$\| B \| = \| B \|_\infty = \max_{\psi:\|\psi\|=1} \| B\psi \| .$$

При подобном определении сопряженное отображение Φ^* должно обладать следущими свойствами:

- линейность;
- положительность: $M \geq 0 \Rightarrow \Phi^*[M] \geq 0$;
- сохранение единицы (унитальность): $\Phi^*[I] = I$.

Определение квантового канала

Помимо перечисленных выше требований к прямому и сопряженному отображениям добавляется ещё одно важное требование [23]:

Определение 4 *Отображение* Φ *называется вполне положительным, если* $\Phi \otimes I_m \geq 0$, *где* I_m — *тождественный оператор в* m*-мерном гильбертовом пространстве.*

Это требование оказывается важным для канала с физической точки зрения, и его смысл станет ясен в дальнейшем.

Свойство вполне положительности позволяет сформулировать важный частный случай более общей теоремы Стайнспринга[23]:

Теорема 6 *Для любого вполне положительного унитального отображения* $\Phi^* : \mathfrak{B}(\mathcal{H}_2) \to \mathfrak{B}(\mathcal{H}_1)$ *существует гильбертово пространство* $\mathcal{H}_0$ *и изометрический оператор* $V : \mathcal{H}_1 \to \mathcal{H}_2 \otimes \mathcal{H}_0$, *такие что*

$$\Phi^*[M] = V^*(M \otimes I_0)V, \quad M \in \mathfrak{B}(\mathcal{H}_2), \tag{2.22}$$

и двойственным образом для отображения Φ*:*

$$\Phi[\rho] = Tr_{\mathcal{H}_0} V \rho V^*, \quad \rho \in \mathfrak{T}(\mathcal{H}_1). \tag{2.23}$$

В дальнейшем нас будет интересовать не столько сама теорема Стайнспринга, сколько два её важных следствия. Первое из них, представление Крауса[23], даёт формулы для записи всякого вполне положительного отображения:

Теорема 7 *Унитальное отображение* Φ^* *вполне положительно тогда и только тогда, когда оно может быть представлено в виде*

$$\Phi^*[M] = \sum_i V_i^* M V_i, \quad M \in \mathfrak{B}(\mathcal{H}_2), \tag{2.24}$$

и двойственным образом

$$\Phi[\rho] = \sum_i V_i \rho V_i^*, \quad \rho \in \mathfrak{T}(\mathcal{H}_1), \tag{2.25}$$

где

$$\sum_i V_i^* V_i = I.$$

Второе следствие утверждает, что свойство вполне положительности позволяет рассматривать квантовый канал как совместную обратимую эволюцию исходной системы и окружения[23]:

Теорема 8 *Всякое вполне положительное сохраняющее след отображение* Φ*, действующее на пространстве* $\mathcal{H}$*, может быть расширено до унитарной эволюции системы, взаимодействующей с окружением* $\mathcal{H}_0$*:*

$$\Phi[\rho] = Tr_{\mathcal{H}_0} U(\rho \otimes \rho_0)U^* \tag{2.26}$$

Таким образом, с учётом указанной физической интерпретации общее определение квантового канала в пространстве состояний таково:

Определение 5 *Каналом в пространстве состояний называется линейное вполне положительное сохраняющее след отображение* Φ.

Схожим образом даётся определение квантового канала в пространстве наблюдаемых, соотвествующее картине Гейзенберга:

Определение 6 *Каналом в пространстве наблюдаемых называется линейное вполне положительное унитальное отображение* Φ^*.

Примеры каналов

Рассмотрим несколько примеров квантовых каналов, которые прояснят введённые ранее определения.

Определение 7 *Канал* Φ *называется классически-квантовым (c-q), если*

$$\Phi[\rho] = \sum_i \rho_i \langle e_i|\rho|e_i\rangle, \tag{2.27}$$

где $\{\rho_i\}$ — *состояния в* $\mathcal{H}_2$, *а* $\{|e_i\rangle\}$ — *ортонормированный базис в* $\mathcal{H}_1$.

Этот канал можно интерпретировать как преобразование классических распределений вероятностей $p_i = \langle e_i|\rho|e_i\rangle$ во множество квантовых состояний $\Phi[\rho] = \sum_i p_i\rho_i$, либо в случае $p_i^k = \delta_{ki}$ — как преобразование входного алфавита p_i^k в квантовые состояния ρ_k.

Чтобы построить представление Крауса для такого канала, рассмотрим сначала отображение $|e_i\rangle\langle e_i| \to |\psi_i\rangle\langle\psi_i|$ элементов ортонормированного базиса

во множество чистых квантовых состояний. Легко видеть, что в представлении Крауса этому отображению соответствует набор операторов $V_i = |\psi_i\rangle\langle e_i|$, для которого выполняется требование

$$\sum_i V_i^* V_i = \sum_i |e_i\rangle\langle\psi_i|\psi_i\rangle\langle e_i| = \sum_i |e_i\rangle\langle e_i| = I.$$

Если же теперь рассмотреть отображение $|e_i\rangle\langle e_i| \to \rho_i$ во множество произвольных операторов плотности, то для каждого из них можно записать спектральное разложение

$$\rho_i = \sum_j s_{ij} |\psi_{ij}\rangle\langle\psi_{ij}|$$

и построить аналогичным образом набор операторов $V_{ij} = \sqrt{s_{ij}}|\psi_{ij}\rangle\langle e_i|$. Нетрудно проверить действие такого набора на базисных векторах

$$\sum_{ij} V_{ij}|e_i\rangle\langle e_i|V_{ij}^* = \sum_j V_{ij}|e_i\rangle\langle e_i|V_{ij}^* =$$

$$= \sum_j s_{ij}|\psi_{ij}\rangle\langle e_i|e_i\rangle\langle e_i|e_i\rangle\langle\psi_{ij}| = \rho_i$$

и условие суммирования в единицу

$$\sum_{ij} V_{ij}^* V_{ij} = \sum_{ij} s_{ij}|e_i\rangle\langle e_i| = \sum_i |e_i\rangle\langle e_i| = I,$$

из чего следует соответствие $\{V_{ij}\}$ операторам представления Крауса для указанного c-q-канала $|e_i\rangle\langle e_i| \to \rho_i$.

Определение 8 *Канал* Φ *называется квантово-классическим (q-c), если*

$$\Phi[\rho] = \sum_i |e_i\rangle\langle e_i| \, Tr\rho M_i, \tag{2.28}$$

где $\{M_i\}$ — *наблюдаемая в* $\mathcal{H}_1$, *а* $\{|e_i\rangle\}$ — *ортонормированный базис в* $\mathcal{H}_2$.

Квантово-классические каналы играют роль, обратную роли c-q-каналов: они переводят квантовое состояние ρ в классическое распределение вероятностей, которое можно представить в виде диагонального оператора плотности $\rho' = \sum_i s_i |e_i\rangle\langle e_i|$, соответствующего измерению наблюдаемой $\{M_i\}$, так как $s_i = \mathrm{Tr}\rho M_i$.

Для построения представления Крауса такого канала запишем спектральное разложение каждого оператора в $\{M_i\}$:

$$M_i = \sum_j m_{ij} |\mu_{ij}\rangle\langle\mu_{ij}|,$$

и по аналогии с предыдущим примером возьмём набор операторов $V_{ij} = \sqrt{m_{ij}} |e_i\rangle\langle\mu_{ij}|$. Тогда, так как $\mathrm{Tr}\rho M_i = \sum_j m_{ij}\langle\mu_{ij}|\rho|\mu_{ij}\rangle$, то

$$\sum_{ij} V_{ij}|\rho V_{ij}^* = \sum_{ij} m_{ij}|e_i\rangle\langle\mu_{ij}|\rho|mu_{ij}\rangle\langle e_i| =$$

$$= \sum_i |e_i\rangle\langle e_i|\mathrm{Tr}\rho M_i = \Phi[\rho],$$

и по свойству суммирования в единицу наблюдаемых также выполняется

$$\sum_{ij} V_{ij}^* V_{ij} = \sum_{ij} m_{ij}|\mu_{ij}\rangle\langle\mu_{ij}| = I.$$

Определение 9 *Канал* $\Phi : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ *называется деполяризующим, если*

$$\Phi[\rho] = (1-p)\rho + \frac{p}{\dim \mathcal{H}} I. \tag{2.29}$$

Такой канал с вероятностью $1-p$ оставляет состояние без изменения, а с вероятностью p стирает всю информацию в нём, превращая исходное состояние в хаотическое. При $p = 1$ такой канал называется *полностью деполяризующим*.

Полностью деполяризующий канал соответстует c-q-каналу, на выходе которого все состояния ρ_i равны $\frac{I}{\dim \mathcal{H}}$, а для такого канала представление Крауса уже было получено. В то же время тождественный канал соответствует тривиальному случаю с единственным оператором $V_0 = I$ в представлении Крауса. Пользуясь этим, легко построить представление Крауса для деполяризующего канала.

Пропускная способность классически-квантового канала

Простейшая модель квантового канала, которая и будет далее рассматриваться в этой работе — это классически-квантовый (c-q) канал. Он, напомним, состоит из входного алфавита $\{x\}$ и его отображения $x \to \rho_x$ во множество квантовых состояний. Важен вопрос о скорости передачи классической информации с использованием подобного канала. Для её исследования следует сначала формализовать процедуру передачи данных.

В случае канала без памяти каждое передаваемое слово исходного алфавита преобразуется в состояние, являющееся тензорным произведением соответствующих состояний на выходе [23]:

$$w = \{x_1, ..., x_n\} \to \rho_w = \rho_{x_1} \otimes ... \otimes \rho_{x_n} \in \mathcal{S}(\mathcal{H}^{\otimes n}).$$

Приёмник на выходе канала производит измерение наблюдаемой $M = \{M_i^{(n)}\}$ в пространстве $\mathcal{H}^{\otimes n}$. Произведя

измерение, приёмник сообщает о принятом решении. Отметим, что в классическом случае место квантовой наблюдаемой занимает классический приемник и процедура принятия решения на основании результатов измерения. Таким образом, должным образом выбранная квантовая наблюдаемая соотвествтует сразу двум элементам классической схемы. Подобная схема передачи информации приводит к следующему определению:

Определение 10 *Кодом* (W, M) *размера* N *для c-q-канала называется набор* N *кодовых слов* $W = \{w^{(i)}\}, \quad i = 1, ..., N$ *длины* n *и правило декодирования, задаваемое наблюдаемой* $M = \{M_i, i = 0, 1, ..., N\}$ *в* $\mathcal{H}^{\otimes n}$

В этом определении исход 0 означает уклонение от принятия решения. Вероятность ошибки на каждом кодовом слове — это вероятность получить исход j при посланном сигнале $i \neq j$. Она равна

$$p_{WM}(j|i) = \mathrm{Tr}\rho_{w^{(i)}} M_j. \tag{2.30}$$

Так как вероятность принятия верного решения при посланном сигнале i равна $p_{WM}(i|i)$, можно определить среднюю ошибку кода

$$P_e(W, M) = \frac{1}{N} \sum_{i=1}^{N} [1 - p_{WM}(i|i)], \tag{2.31}$$

а также среднюю ошибку, минимизированную по всем кодам размера N с длиной кодовых слов n:

$$p_e(n, N) = \min_{W,M} P_e(W, M). \tag{2.32}$$

Далее, пропускная способность канала определяется как точная верхняя грань скоростей, при которых возможна асимптотически безошибочная передача данных [23]:

Определение 11 *Величина C называется классической пропускной способностью c-q-канала $x \to \rho_x$, если выполнены следующие условия:*

- $\lim_{n\to\infty} p_e(n, 2^{nR}) = 0$, *если* $R \leq C$,
- $\lim_{n\to\infty} p_e(n, 2^{nR}) \neq 0$, *если* $R > C$.

При рассмотрении пропускной способности c-q-каналов потребуется ввести понятие энтропии фон Неймана, которая является квантовым аналогом энтропии Шеннона, введённой для классических распределений вероятностей. Для оператора плотности ρ со спектральным разложением $\sum_i s_i |e_i\rangle\langle e_i|$ эта величина определяется как

$$H(\rho) = -\sum_i s_i \log s_i.$$

(значение $0 \log 0$ для нулевых собственных значений принимается в этом определении равным нулю.)

Введённое понятие энтропии фон Неймана позволяет сформулировать квантовую теорему кодирования[23]:

Теорема 9 *Пропускная способность c-q-канала $x \to \rho_x$ равна*

$$C = \max_{\pi} \chi(\pi, \{\rho_x\}),$$

где $\pi = \{\pi_x\}$ — априорное распределение квантовых состояний, а

$$\chi(\pi, \{\rho_x\}) = H\left(\sum_x \pi_x \rho_x\right) - \sum_x \pi_x H(\rho_x). \qquad (2.33)$$

Величина $\chi(\pi, \{\rho_x\})$, введённая А.С. Холево в 1973 г.[24], очень важна для оценок информации, которую

можно получить из набора квантовых состояний. Её называют величиной Холево, или χ-энтропией.

Важной особенностью передачи информации по квантовым каналам является свойство супераддитивности, которое заключается в следующем. Рассмотрим код размера N с длиной кодового слова n. Как уже было отмечено, на его вход могут быть поданы N различных сигналов, которые могут быть декодированы $N+1$ различными способами, N из которых соответствуют принятию определённого решения. Это даёт возможность рассматривать классический канал с набором переходных вероятностей $p_n(j|i), \quad i,j = 1,...,N$. Пропускную способность такого канала будем обозначать как C_n. Явление супераддитивности заключается в выполнении неравенства

$$C_n > nC_1.$$

Это свойство может выполняться уже в случае кодирования, состоящего из кодовых слов длины 2: $C_2 > 2C_1$. Можно определить величину

$$C_\infty = \lim_{n\to\infty} \frac{C_n}{n}. \tag{2.34}$$

Квантовая теорема кодирования, таким образом, утверждает, что $C = C_\infty$.

Важным частным случаем применения квантовой теоремы кодирования является c-q-канал, на выходе которого имеются два состояния ρ_0 и ρ_1. В этом случае максимум пропускной способности достигается при их равномерном распределении $\pi_0 = \pi_1 = 1/2$ и равен

$$C = H\left(\frac{1}{2}(\rho_0 + \rho_1)\right) - \frac{1}{2}(H(\rho_0) + H(\rho_1)). \tag{2.35}$$

2.5 Квантовые коды коррекции ошибок

Классические коды коррекции ошибок используются для безошибочной передачи данных по каналам с помехами. Так, если в канале допустима помеха в одном произвольном бите, то простейшим кодом для безошибочной передачи данных будет код с повторением: вместо сигнала 0 будем посылать 000, а вместо 1 — 111. На приемной стороне для принятия решения о переданном сигнале принимается решение по близости в метрике Хемминга: сигнал, содержащий два или три нуля (000, 001, 010, 100) трактуется как 0, сигнал же с двумя или тремя единицами — как единица.

Указанный подход невозможен для применения в квантовом случае. Первое же препятствие этому — запрет на клонирование квантовых состояний, из которого следует невозможность преобразования $U : |\psi\rangle \to |\psi \otimes \psi \otimes \psi\rangle$, необходимого для использования кода с повторением. К счастью, подобный запрет можно обойти благодаря использованию специфических квантовых эффектов.

Коды, исправляющие ошибку в одном кубите

Отличия квантового случая восстановления информации от классического видны уже при описании ошибки: если в классическом случае единственным вариантом ошибки является смена бита $0 \leftrightarrow 1$, то в квантовом случае возможные ошибки образуют непрерывное множество. Простейшим примером чисто квантовой ошибки является фазовая ошибка:

$$|0\rangle \to |0\rangle,$$

$$|1\rangle \to -|1\rangle.$$

Обратим внимание, что если битовая ошибка меняет местами состояния из множества $\{|0\rangle, \quad |1\rangle\}$, то фазовая ошибка оставляет такие состояния нетронутыми (за исключением несущественной общей фазы), но меняет местами состояния в наборе $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, устойчивом к битовым ошибкам.

Заметим, что произвольное кубитовое состояние $\psi = \alpha|0\rangle + \beta|1\rangle$ можно обезопасить от битовой ошибки с помощью следующего кода (запрета на клонирование *ортогональных* состояний нет):

$$|0\rangle \to |000\rangle,$$

$$|1\rangle \to |111\rangle.$$

Покажем, как это происходит. На выходе канала можно произвести измерение

$$\begin{aligned} M_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ M_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ M_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|, \\ M_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned} \tag{2.36}$$

Нетрудно видеть, что такое измерение не меняет исходного состояния, и что при отсутствии ошибки выпадет результат M_0, а при ошибке в i-й позиции — результат M_i. Результат такого измерения называют *синдромом ошибки*. Тогда, зная, в какой позиции произошла ошибка, можно произвести корректирующее преобразование K_i, заключающееся в инверсии i-го кубита. В результате на выходе окажется исходное состояние.

Также несложно показать, что исправить произвольную фазовую ошибку можно применением

указанного выше кода к состоянию $H|\psi\rangle$, где H — оператор Адамара:

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{2.37}$$

Опишем теперь принцип действия кода Шора[13], способного исправить *любую* квантовую ошибку в одном кубите. При таком кодировании каждый кубит кодируется кодом, исправляющим битовую ошибку, а затем каждый получившийся кубит — кодом исправления фазовой ошибки. В результате получается девятикубитовый код с кодовыми словами

$$|0_S\rangle = \frac{1}{2\sqrt{2}}\left[(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\right],$$

$$|1_S\rangle = \frac{1}{2\sqrt{2}}\left[(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\right].$$

Покажем, что этот код способен исправлять не только битовую и фазовую ошибки, но и вообще произвольную квантовую ошибку при условии того, что она произошла лишь в одном кубите. Напомним, что произвольная ошибка квантового канала описывается, согласно представлению Крауса, набором операторов $\{V_i\}$. Если состояние кубита до возникновения ошибки обозначить как $|\psi\rangle$, то после воздействия шума это состояние преобразуется в

$$\Phi[|\psi\rangle\langle\psi|] = \sum_i V_i|\psi\rangle\langle\psi|V_i^*.$$

Каждый из операторов V_i в этой сумме можно представить как комбинацию тождественного оператора, битовой

ошибки X, фазовой ошибки Z и их сочетания:

$$V_i = a_i I + b_i X + c_i Z + d_i XZ.$$

В таком случае $V_i|\psi\rangle$ является суперпозицией набора состояний $\{|\psi\rangle,\ X|\psi\rangle,\ Z|\psi\rangle,\ XZ|\psi\rangle\}$, и после измерения синдрома ошибки общее состояние отобразится на одно из состояний указанного набора, каждое из которых может быть исправлено благодаря процедуре, аналогичной описанной выше.

Это нетривиальное свойство квантовых кодов коррекции: произвольное множество ошибок, описываемое в квантовом случае набором *непрерывных* параметров, может быть скорретировано благодаря процедуре, исправляющей *дискретное* подмножество ошибок.

Линейные коды

Определим важное подмножество классических кодов, которое удобно тем, что его можно задать с помощью матриц сравнительно небольшого размера. Такие коды называются *линейными кодами*. Исходное сообщение длины n преобразуется в кодовое слово длины k с помощью умножения на *порождающую матрицу*: матрицу размера $n \times k$, состоящих из нулей и единиц. Так, уже встречавшийся код с повторением для входных слов длины 2 описывается с помощью матрицы размера 2×6:

$$G = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Легко видеть, что действие этой матрицы на входные слова соответствует коду с повторением:

$$G(0,0) = (0,0,0,0,0,0), \quad G(0,1) = (0,0,0,1,1,1),$$
$$G(1,0) = (1,1,1,0,0,0), \quad G(1,1) = (1,1,1,1,1,1).$$

Существеное преимущество линейных кодов в том, что вся информация, необходимая для кодирования 2^n кодовых слов, содержится всего лишь в kn элементах порождающей матрицы, что позволяет сильно экономить компьютерную память.

Процесс обнаружения и исправления ошибок описывается в этом случае другой матрицей, которая называется *проверочной матрицей*. По определению это матрица H, ядром которой являются кодовые слова и только они, то есть $Hx = 0$ выполняется тогда и только тогда, когда x — кодовое слово. В этом случае проверочная матрица будет иметь размеры $(k-n) \times n$. Очевидно, что если исходное кодовое слово x при передаче по каналу преобразовалось в ошибочное слово $y = x + e$, то $Hy = Hx + He = He$. Это даёт возможность, имея значения He_j для набора $\{e_j\}$ всевозможных n-мерных векторов с единицей на одной лишь j-й позиции, определить, в какой именно позиции произошла ошибка и исправить её.

Линейный код, где каждое из сообщений длины n кодируется с помощью k битов информации, называется $[n,k]$-кодом. Основное из свойств линейных кодов заключается в том, что существует $[n,k]$-код, способный при больших n исправить q ошибок в n битах исходного сообщения, если

$$\frac{n}{k} \geq 1 - h(\frac{2q}{n}). \tag{2.38}$$

Этот важный результат называется *границей Варшамова-Гильберта*.

Также в дальнейшем будет полезно наблюдение, что для всякого линейного кода C его проверочную матрицу H после транспонирования можно использовать как порождающую матрицу другого кода, который в этом случае называется *двойственным* к коду C и обозначается как $C^{\perp}$. Его порождающая матрица — H^T, а проверочная — G^T. Из определения проверочной матрицы очевидно, что его кодовые слова будут ортогональны кодовым словам исходного кода C.

Коды Кальдербанка-Шора-Стина (CSS-коды)

Подобно тому, как код Шора использует комбинацию двух кодов с повторением для исправления произвольной битовой или фазовой ошибки, коды Кальдербанка-Шора-Стина (CSS-коды) используют для исправления q произвольных квантовых ошибок комбинацию двух линейных кодов, каждый из которых способен исправлять q ошибок. Точнее, используется $[n, k_1]$-код C_1, исправляющий q ошибок, и $[n, k_2]$-код $C_2 \subset {}_1$, такой, что $C_2^{\perp}$ способен исправить q ошибок.

Для каждого кодового слова $x \in C_1$ вводится состояние

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x \oplus y\rangle,$$

где $\oplus$ обозначает сложение по модулю 2. Очевидно, что при $x - x' \in C_2$ элементы $|x + C_2\rangle$ и $|x' + C_2\rangle$ совпадают, а это значит, что состояние $|x + C_2\rangle$ определяется лишь классом смежности C_1/C_2. Далее, так как при $x - x' \notin C_2$ и $\{y, y'\} \in C_2$ не может выполняться $x + y = x' + y'$, то состояния $|x + C_2\rangle$ и $|x' + C_2\rangle$ взаимно ортогональны при x и x' из разных классов смежности C_1/C_2.

В [20] было показано, каким именно образом подобная комбинация двух классических линейных кодов способна исправлять q произвольных квантовых ошибок. В рамках данной работы наибольший интерес представляют ограничения относительно того, какое максимальное количество ошибок в строке длины n может быть исправлено с помощью CSS-кодов. Квантовый аналог границы Варшамова-Гильберта даёт эту величину: существуют CSS-коды длины k, исправляющие q ошибок в n кубитах, если

$$\frac{n}{k} \geq 1 - 2h(\frac{2q}{n}).$$

Таким образом, CSS-коды способны решать задачу безошибочной передачи квантовых состояний через каналы с некоторым уровнем квантового шума. В дальнейшем это свойство исправления квантовых ошибок будет использоваться в работе при доказательстве возможности двум пользователям сгенерировать полностью секретный ключ.

Глава 3

Протокол квантового распределения ключей BB84

К 1984 году основная часть описанных выше результатов уже была известна, и их оказалось достаточно для того, чтобы сформулировать принципы квантовой криптографии и предоставить хоть на тот момент и не строгие, но достаточно интуитивно понятные доводы в пользу секретности подобного способа распределения ключей. Затем пришло время для развития собственно формализма квантовой криптографии: были описаны требуемые действия легитимных пользователей, формализованы действия перехватчика, а также была доказана секретность первого протокола квантового распределения ключей, названного BB84[3].

Основные факты квантовой теории информации, на которых основывается квантовая криптография — это связанные между собой утверждения о невозможности копирования произвольных квантовых состояний и о невозможности достоверного различения

неортогональных состояний. В сочетании эти факты дают то, что *попыти различения квантовых состояний из неортогонального набора ведут к помехам*, а значит, действия перехватчика могут быть детектированы по величине ошибки на приёмной стороне.

Важно отметить, что квантовая криптография не делает никаких предположений о характере действий подслушивателя и объеме доступных ему ресурсов: полагается, что *перехватчик может обладать любыми ресурсами и делать все возможные действия в рамках известных на сегодняшний день законов природы*. Это существенным образом отличает квантовую криптографию от классической, которая опирается на ограничения в вычислительной мощности подслушивателя.

В этой главе будет рассмотрен протокол квантового распределения ключей BB84 и дана схема доказательство его секретности, а затем будут рассмотрены различные классы атак перехватчика.

3.1 Общая схема протокола

Неформально принцип действия всех протоколов квантовой криптографии можно описать так: передающая сторона (Алиса) на каждом шаге посылает одно из состояний из их неортогонального набора, а принимающая сторона (Боб) производит такое измерение, что после дополнительного обмена классической информацией между сторонами они должны иметь битовые строки, полностью совпадающие случае идеального канала и отсутствия перехватчика. Ошибки же в этих строках могут говорить как о неидеальности канала, так и о действиях подслушивателя. При величине ошибки,

превышающей некоторый предел, действие протокола прерывается, иначе легитимные пользователи могут извлечь полностью секретный ключ из их (частично совпадающих) битовых строк.

В этом разделе будет дано описание протокола BB84, а также общая схема действий легитимных пользователей при квантовом распределении ключей.

Передача сигнальных состояний

Протокол BB84 использует два базиса:

$$\begin{aligned} + &: |x\rangle = |0\rangle, \quad |y\rangle = |1\rangle, \\ \times &: |u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{3.1}$$

Легко проверить, что эти базисы удовлетворяют *условию несмещённости*

$$\begin{aligned} |\langle x|u\rangle|^2 = |\langle x|v\rangle|^2 = \tfrac{1}{2}, \\ |\langle y|u\rangle|^2 = |\langle y|v\rangle|^2 = \tfrac{1}{2}, \end{aligned} \tag{3.2}$$

которое неформально сводится к тому, что с точки зрения одного базиса состояния в другом расположены симметрично.

На этапе приготовления состояний Алиса случайным образом выбирает один из указанных базисов (3.1), а затем случайно выбирает значение бита: 0 или 1, и в соответствии с этим выбором посылает один из четырех сигналов:

- $|x\rangle$, если это базис «+» и значение бита равно 0,
- $|y\rangle$ при том же базисе и значении бита 1,
- $|u\rangle$ при выпадении базиса «×» и бита 0,

- $|v\rangle$, если в базисе «×» выпал бит 1

При посылке каждого из этих сигналов Алиса запоминает свой выбор базиса и выбор бита, что приводит к появлению двух случайных битовых строк на её стороне.

Боб, получая каждый из присланных Алисой сигналов, производит над ним случайным образом одно из двух измерений, каждое из которых способно дать достоверный результат из-за ортогональности состояний внутри каждого базиса Алисы:

$$\begin{aligned} M_0^+ &= |x\rangle\langle x|, \quad M_1^+ = |y\rangle\langle y|, \\ M_0^\times &= |u\rangle\langle u|, \quad M_1^\times = |v\rangle\langle v|. \end{aligned} \tag{3.3}$$

В результате у него оказывается две строки: с тем, какие из базисов были выбраны для измерения, и с исходами этих измерений.

Итак, после передачи всех состояний и проведения измерений Алиса и Боб имеют по две строки. Здесь происходит согласование базисов: по открытому каналу Алиса и Боб объявляют друг другу свои строки с выбором базисов, и они выбрасывают посылки, в которых их базисы не совпали. Следует обратить внимание, что если базис, используемый для посылки состояния Алисой, совпал с базисом измерения Боба, то в случае отутствия помех в канале связи результаты в их битовых строках на соответствующей позиции будут совпадать, поэтому после этапа согласования базисов в случае идеального канала и отсутствия действий со стороны перехватчика Алиса и Боб должны обладать одними и теми же битовыми строками.

Однако, если в канале были ошибки или перехватчик пытался подслушать информацию, битовые строки Алисы и Боба могут не совпадать, поэтому для проверки они должны согласованно раскрыть примерно половину своих битовых строк. Согласно центральной предельной

теореме, ошибка в раскрытой битовой последовательности даёт достаточно точную оценку ошибки во всей последовательности, и по ней можно достаточно точно оценить вероятность ошибки в оставшихся позициях. Если величина ошибки оказывается больше некоторой величины (параметра протокола), передача данных прекращается: это означает, что перехватчик обладает слишком большой информацией о ключе. В противном же случае перед Алисой и Бобом стоит задача получения общего секретного ключа. Эту задачу можо разбить на два этапа: сначала производится *коррекция ошибок*, в результате которой в распоряжении Алисы и Боб оказываются совпадающие битовые строки. Второй этап, называемый *усилением секретности*, ставит своей целью исключить информацию о ключе, которая могла попасть к перехватчику в результате действий над использовавшимися квантовыми состояниями или в ходе коррекции ошибок. В результате этого шага у перехватчика не должно оставаться информации об общей битовой строке Алисы и Боба.

Коррекция ошибок

Итак, целью процедуры коррекции ошибок является получение из частично совпадающих битовых строк Алисы и Боба полностью идентичных. Это классическая процедура, так как она имеет дело лишь с классическими битами и открытыми каналами связи.

Наиболее эффективная процедура коррекции ошибок сводится к использованию случайных кодов. Пропускная способность классического канала с вероятностью ошибки Q равна [12]

$$C_{clas}(Q) = 1 - h(Q),$$

где $h(Q)$ — бинарная энтропия Шеннона. Зная вероятность ошибки в канале и имея последовательность длины n, Алиса генерирует $2^{n(C_{clas}-\delta)}$ случайных кодовых слов. Параметр δ можно сделать малым при больших значениях n. К этому списку Алиса присоединяет и свою последовательность битов, после чего открыто сообщает набор кодовых слов Бобу (а значит, они становятся известны и Еве). Из полученного списка кодовых слов Боб выбирает ближайшее к своей последовательности в метрике Хемминга. Согласно теореме кодирования для канала с шумом, при таком выборе кодовых слов Боб с вероятностью единица выберет битовую строку Алисы.

Отметим, однако, что полностью случайные коды трудно реализовать на практике, так как при их использовании необходимо хранить в памяти экспоненциально большое (в зависимости от длины битовой строки n) число кодовых слов. Обычно в реальных схемах используются другие, конструктивные, коды, эффективность которых ниже.

Усиление секретности

На этом этапе Алиса и Боб имеют совпадающие битовые строки и оценку информации, которая доступна Еве. Эта оценка даётся из числа ошибок в «сыром» ключе (напомним, что это число ошибок связано с помехами в канале связи, а по предположению они все вызваны деятельностью Евы. Как именно можно оценить её информацию по количеству ошибок, будет показано в дальнейшем) и из процедуры коррекции ошибок, в ходе которой часть информации, как было отмечено, также уходит к перехватчику.

Задача этапа усиления секретности состоит в том, чтобы получить из частично секретных общих битовых

строк Алисы и Боба полностью неизвестного Еве секретного ключа. Обычно в ходе подобной процедуры длина ключа существенно уменьшается.

Основным методом, позволяющим проводить усиление секретности, является использование класса *универсальных хеш-функций* $\mathcal{G}$ [4]. Это функции, отображающие набор n-битовых строк A в набор m-битовых строк B таким образом, что для случайно выбранной хеш-функции $g \in \mathcal{G}$ и любых несовпадающих элементов $a_1, a_2 \in A$ вероятность совпадения их образов $g(a_1) = g(a_2)$ не превосходит $1/|B|$. То есть задача нахождения прообразов двух различных элементов в B не может решиться более эффективно, чем с помощью перебора или угадывания.

Существует теорема [20], оценивающая информацию Евы о финальном ключе через её исходную информацию о частично секретном ключе и длину финального ключа m:

Теорема 10 *Пусть X — случайная величина с распределением $p(x)$, а G — случайная величина, соответствующая равновероятному случайному выбору хеш-функций из универсального класса хеш-функций, отображающих алфавит X в $\{0,1\}^m$. Тогда*

$$H(G(X)|G) \geq H_c(G(X)|G) \geq m - 2^{m-H_c(X)}, \qquad (3.4)$$

где

$$H_c(X) = -\log\left[\sum_x p(x)^2\right]$$

называется коллизионной энтропией.

Её применение сводится к тому, что легитимные пользователи, имея оценку информации Евы (которая

задаётся величиной $H_c(X)$), всегда могут выбрать длину финального ключа m настолько малой, что неопределённость Евы относительно финального ключа (задаваемая левой частью (3.4)) будет сколь угодно близка к неопределённости простого угадывания, что соответствует его полной секретности.

Таким образом, в ситуации, когда взаимная информация Алисы и Боба превосходит взаимную информацию Алисы и Евы, всегда можно из исходного частично секретного ключа получить полностью секретный ключ, сжав его с помощью универсальной хеш-функции.

3.2 Стойкость протокола

При предложении протокола BB84 его стойкость была показана лишь на интуитивном уровне: попытка Евы измерить передаваемые состояния влечёт к их разрушению, что приводит к дополнительным ошибкам на приёмной стороне. Однако одними лишь измерениями посылаемых сигналов действия Евы не ограничиваются. Более того, непросто рассчитать информацию, способную попасть к Еве при *всех возможных* действиях с её стороны. Однако оказывается, что стойкость протокола BB84 можно доказать, и не прибегая к оценкам информационных величин для всех возможных атак Евы. Так, в 2000 году было показано [15], что секретность квантовой криптографии можно свести к свойствам квантовых кодов коррекции ошибок: если ошибки, возникающие в квантовом канале связи, можно достоверно исправить, то можно добиться и секретной передачи данных. Это даёт критическую величину ошибки, до которой возможно секретное распределение

ключей.

Доказательство стойкости протокола проще всего провести, введя несколько дополнительных протоколов: так, стойкость введённого первым ЭПР-протокола легко вытекает из теории квантовых измерений, а благодаря последовательному изменению некоторых действий легитимных пользователей он может быть сведён к более строго описанному протоколу BB84 без нарушения исходной секретности.

Вспомогательный протокол ЭПР

Ранее уже было введено состояние ЭПР

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

важнейшим свойством которого является то, что при измерении его в любом базисе состояния, получающиеся в результате в обоих подсистемах, оказываются одинаковыми. Так, для уже встречавшихся измерений Боба в базисах «+» и «×» имеем

$$\frac{\sqrt{M_0^+}|\psi_{EPR}\rangle}{\langle\psi_{EPR}|\sqrt{M_0^+}|\psi_{EPR}\rangle} = |00\rangle = |xx\rangle,$$

$$\frac{\sqrt{M_1^+}|\psi_{EPR}\rangle}{\langle\psi_{EPR}|\sqrt{M_1^+}|\psi_{EPR}\rangle} = |11\rangle = |yy\rangle,$$

$$\frac{\sqrt{M_0^\times}|\psi_{EPR}\rangle}{\langle\psi_{EPR}|\sqrt{M_0^\times}|\psi_{EPR}\rangle} = \frac{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)}{2} = |uu\rangle,$$

$$\frac{\sqrt{M_1^\times}|\psi_{EPR}\rangle}{\langle\psi_{EPR}|\sqrt{M_1^\times}|\psi_{EPR}\rangle} = \frac{(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle)}{2} = |vv\rangle.$$

На этом свойстве основан принцип действия протокола ЭПР: раз результаты двух участников измерения ЭПР-состояния совпадают, можно использовать это для генерации случайного секретного ключа. Для этого Алисе и Бобу требуется просто договориться об использовании согласованных базисов для измерения: их исходы в случае идеальных ЭПР-пар будут совпадать, и у перехватчика не будет какой-либо информации о ключе (это гарантируется чистотой идеальной ЭПР-пары).

Тем не менее, если между Алисой и Бобом нет чистых ЭПР-состояний, то по степени совпадения своих состояний с идеальным случаем они всегда способны оценить информацию, которая может быть доступна Еве: в [20] была доказана следующая

Теорема 11 *Пусть* $^{\otimes n}\langle\psi_{EPR}|\rho|\psi_{EPR}\rangle^{\otimes n} > 1 - 2^{-s}$, *тогда энтропия* ρ *ограничена сверху величиной*

$$H(\rho) < (2n + s + \frac{1}{\ln 2})2^{-s} + O(2^{-2s}). \qquad (3.5)$$

По теореме Шмидта собственные значения частичных операторов плотности системы и окружения совпадают, а значит, энтропия системы Евы также будет ограничена сверху той же величиной (3.5). Поскольку величина Холево в свою очередь оценивается сверху энтропией $H(\rho)$, приведённую теорему можно успешно использовать для оценки информации, доступной перехватчику. Это означает, что Алиса и Боб всегда могут быть уверены в том, что Ева не обладает большей информацией о ключе, чем они: в противном случае (при низкой степени совпадения общего состояния Алисы и Боба ρ с идеальным случаем $|\psi_{EPR}\rangle\langle\psi_{EPR}|$) выполнение протокола прерывается. Если же утечка информации к Еве невелика, то с помощью классических процедур коррекции ошибок

и усиления секретности получение полностью секретного ключа возможно.

Протокол Ло-Чу

Протокол Ло-Чу был разработан как своего рода промежуточное звено между протоколами ЭПР и BB84. Подобно ЭПР-протоколу, он использует ЭПР-пары в качестве исходных состояний, но теперь уже эти состояния явно генерируются на стороне Алисы и посылаются Бобу по квантовому каналу с использованием произвольного кодирования, подобно тому, как это происходит в протоколе BB84.

Как было показано выше, информация Евы может быть оценена сверху с помощью степени совпадения исходных состояний между Алисой и Бобом с идеальным случаем чистых ЭПР-состояний $|\psi_{EPR}\rangle$. Благодаря этой оценке Алиса и Боб могут понять, какие параметры коррекции ошибок и усиления секретности им следует применять. Идея протокола Ло-Чу заключается в том, что вместо этих двух классических процедур Алиса и Боб могут применить очищение сцепленности, которое даст им точные ЭПР-пары, из которых они смогут получить полностью эквивалентные секретные ключи. Таким образом, процедуру очищения сцепленности можно считать квантовым аналогом классических процедур коррекции ошибок и усиления секретности.

Поскольку очищение сцепленности можно провести с помощью соответствующего квантового кода коррекции ошибок, требуется оценить количество фазовых и битовых ошибок в передаваемой последовательности состояний. Если ошибки произошли не более чем в q кубитах, то из исходных n кубитов можно получить k ЭПР-пар с помощью $[n, k]$-кода, исправляющего q ошибок.

Более строго, протокол Ло-Чу выглядит так:

1. Алиса создаёт $2n$ ЭПР-пар в состоянии $|\psi_{EPR}\rangle^{\otimes 2n}$.

2. Алиса случайно выбирает n из $2n$ ЭПР-пар, чтобы использовать их в дальнейшем как контрольные для проверки степени совпадения состояний у себя и у Боба.

3. Алиса генерирует случайную битовую строку s_A длины $2n$ и применяет преобразование Адамара ко второму кубиту каждой пары, для которой в соответствующей позиции $s_A = 1$.

4. Алиса по квантовому каналу посылает второй кубит каждой пары Бобу.

5. Боб получает кубиты и публично объявляет об этом.

6. Алиса публично объявляет позиции n контрольных кубитов и строку s_A.

7. Боб применяет преобразование Адамара к тем кубитам, для которых $s_A = 1$.

8. Алиса и Боб измеряют n контрольных кубитов в базисе «+» и публично объявляют результаты. Если более чем q битов не совпали, выполнение протокола прерывается.

9. Алиса и Боб измеряют оставшиеся n кубитов в соответствии с проверочной матрицей $[n, k]$-кода, исправляющего до q ошибок. После обмена результатами и вычисления синдрома ошибок они могут получить k ЭПР-пар

10. Алиса и Боб измеряют k ЭПР-пар в базисе «+» для получения общего секретного ключа.

Преобразование Адамара над случайным набором кубитов на этапах 3 и 7 нужно здесь для того, чтобы убедиться, что какую бы атаку ни предприняла Ева, вероятности фазовых и битовых ошибок будут максимально близки друг к другу, а это создаёт наиболее благоприятные условия для применения квантовых кодов коррекции ошибок.

Протокол CSS-кодов

Протокол Ло-Чу, основанный на протоколе ЭПР, использует квантовый код коррекции ошибок для получения ЭПР-пар. В то же время исправление квантовых ошибок — сложная техническая задача, требующая в общем случае квантового компьютера для своей реализации. Протокол CSS-кодов избавляется от этой необходимости, используя только классические коды коррекции ошибок. Это можно сделать, не нарушая надёжности всей процедуры.

Так как измерения, проводимые Алисой на шаге 8, разрушают сцепленность исходных состояний, нет необходимости посылать именно части ЭПР-пар: можно просто приготовить известное квантовое состояние $|0\rangle$ или $|1\rangle$ и послать его Бобу, произведя предварительно преобразование Адамара над произвольным подмножеством состояний.

Аналогично измерения пользователей на этапах 9 и 10 разрушают исходные ЭПР-пары, превращая их в случайные кубиты, закодированные некоторым случайным квантовым кодом коррекции ошибок. Поэтому вместо использования кода для получения ЭПР-пар

Алиса может просто закодировать случайный ключ из k битов с помощью кода $\mathrm{CSS}_{x,z}(C_1, C_2)$ со случайными параметрами x и z, отослав Бобу закодированные n кубитов. Затем Алиса на этапе 6 публично объявляет не только строку s_A и позиции контрольных битов, но ещё и параметры кода x и z, чтобы Боб мог безошибочно декодировать секретный ключ длины k.

Итак, с учётом приведённых изменений протокол CSS-кодов выглядит так:

1. Алиса создаёт n случайных контрольных битов, случайный ключ длины k, а также две случайных битовых строки x и z. Она применяет код $\mathrm{CSS}_{x,z}(C_1, C_2)$ для кодирования ключа и приготавливает n контрольных кубитов в состоянии $|0\rangle$ или $|1\rangle$ в соответствии с контрольными битами.

2. Алиса случайно выбирает n из $2n$ позиций, помещая туда контрольные кубиты. В оставшихся позициях располагаются кубиты закодированного сообщения.

3. Алиса генерирует случайную битовую строку s_A длины $2n$ и применяет преобразование Адамара ко второму кубиту каждой пары, для которой в соответствующей позиции $s_A = 1$.

4. Алиса по квантовому каналу посылает Бобу полученные в результате кубиты.

5. Боб получает кубиты и публично объявляет об этом.

6. Алиса публично объявляет позиции n контрольных кубитов и строки s_A, x и z.

7. Боб применяет преобразование Адамара к тем кубитам, для которых $s_A = 1$.

8. Боб измеряет n контрольных кубитов в базисе «+» и публично объявляют результаты. Если более чем q битов не совпали, выполнение протокола прерывается.

9. Боб декодирует оставшиеся n кубитов в соответствии с кодом $\mathrm{CSS}_{x,z}(C_1, C_2)$.

10. Боб измеряет свои кубиты для получения общего с Алисой секретного ключа.

Сведение к протоколу BB84

Протокол CSS-кодов, хотя и проще протокола Ло-Чу с технической точки зрения, до сих пор всё равно достаточно сложен, так как требует квантовых вычислений для проведения кодирования и декодирования квантовых состояний, так же как и хранения их в квантовой памяти до получения сообщения от Алисы. Надёжная версия протокола BB84, к которой этот протокол будет сведён в этом разделе, не накладывает подобных технологических требований.

В силу того, что CSS-код использует два *классических* кода C_1 и C_2, процедуру квантового декодирования можно заменить на измерение состояния с дальнейшим классическим декодированием (см. точное обоснование в [20]). Суть этого перехода в том, что теперь выбирается лишь два класса смежности, один из которых соответствует коду C_1 и процедуре исправления ошибок, а второй — классу в коде C_2 и связан с усилением секретности. Это упрощает этапы протокола, на которых производится кодирование и декодирование сигнала, так как теперь достаточно просто объявить кодовое слово из C_1, а затем, при усилении секретности — класс смежности

в C_2/C_1.

Наконец, чтобы избавиться от необходимости хранения посылаемых Алисой кубитов в квантовой памяти до согласования кодовых слов с Бобом, можно пойти на то, что Боб будет измерять каждый сигнал сразу же после его получения, используя случайно выбранный базис «+» или «×», а Алиса в свою очередь будет посылать сигнал в одном из этих базисов. Так как примерно в половине посылок базисы Алисы и Боба не совпадут и им придётся отбросить значение их измерений, общую длину строки следует увеличить с $2n$ до $4n(1+\delta)$.

Таким образом, окончательная надёжная версия протокола BB84 такова:

1. Алиса выбирает $4n(1+\delta)$ случайных битов.

2. Для каждого из битов Алиса посылает сигнал Бобу, выбирая базис «+» или «×» в соответствии со случайной строкой s_A.

3. Алиса выбирает случайное кодовое слово $v_k \in C_1$.

4. Боб получает кубиты и измеряет каждый из них в базисе «+» или «×» в соответствии со случайной строкой s_B.

5. Алиса и Боб раскрывают строки s_A и s_B, оставляя только те позиции полученных в результате пересылки кубитов строк, в которых соответствующие значения их битов совпали. С большой вероятностью остаётся $2n$ битов, иначе выполнение протокола прекращается.

6. Алиса произвольно выбирает из оставшихся $2n$ битов n контрольных.

7. Алиса и Боб открыто сравнивают значения своих контрольных битов. Если количество различающихся битов больше критической величины q, выполнение протокола прекращается.

8. Алиса объявляет $x - v_k$. Боб, вычитая эту строку из своего результата, с помощью кода C_1 исправляет ошибку, получая v_k — безошибочную строку, которая однако может быть частично известная Еве.

9. Алиса и Боб вычисляют класс смежности $v_k + C_2$ в C_1, чтобы получить общий секретный ключ k.

Эта схема протокола, незначительно отличающаяся от рассмотренной до этого, использует для коррекци ошибок и усиления секретности свойства CSS-кодов, которые не являются оптимальными. Теоретическая оценка на величину ошибки q, которую можно исправить в квантовом канале, даётся границей Шеннона: $1 - 2h(q) > 0$, которая лучше границы Варшамова-Гильберта, гарантирующей существование соответствующих CSS-кодов. При использовании границы Шеннона (достижение которой сводится к использованию случайных классических кодов) получается теоретический предел ошибки, до которой возможно секретное распределение информации. Он равен приблизительно 11%, а именно корню уравнения $1 - 2h(q) = 0$.

3.3 Стратегии подслушивателя

Приведённое выше доказательство секретности протокола BB84 утверждает, что при величине ошибки на приёмной стороне менее 11% возможна секретная передача данных. В то же время не говорится о том, каким образом протокол

теряет секретность при большей величине ошибки. В этом разделе явным образом строится схема атаки, при которой достигается теоретический предел ошибки на приёмной стороне в 11%.

Также будут рассмотрены другие стратегии подслушивателя и будут найдены критические величины ошибки для каждой из них. Важным результатом является то, что наиболее общим случаем подслушивания можно считать коллективную атаку: при незначительном изменении схемы протокола более общая когерентная атака не даёт дополнительной выгоды перехватчику.

Прием-перепосыл

Наиболее простым сценарием действий Евы является измерение передаваемого по квантовому каналу состояния с дальнейшим пересылом полчившегося результата дальше. Именно таким образом могут прослушаться классические каналы. Покажем, что в квантовом случае подобная стратегия не срабатывает. Этот раздел даёт оценки информации Евы на менее формальном языке, чем это будет делаться в дальнейшем, однако в нем наиболее простым образом видны идеи, лежащие в основе анализа стойкости протоколов квантовой криптографии.

Если Ева стремится произвести те же действия, что производит на своей стороне Боб, то, не зная исходного состояния, она неизбежно сталкивается с нерешаемой проблемой различения состояний из неортогонального набора. Так, применяя случайным образом одно из измерений

$$\begin{aligned} +: &\quad M_x = |x\rangle\langle x| \quad M_y = |y\rangle\langle y|, \\ \times: &\quad M_u = |u\rangle\langle u| \quad M_v = |v\rangle\langle v| \end{aligned} \tag{3.6}$$

к посланному состоянию, примерно в половине случаев

Ева будет неверно угадывать базис: применять измерение «×» при посланном состоянии $|x\rangle$ или $|y\rangle$ или применять измерение «+» над состоянием из набора $\{|u\rangle, |v\rangle\}$. Легко видеть, что в силу свойства несмещённости (3.2) базисных состояний при неверно угаданном базисе вероятность ошибки Евы составляет 50%, то есть Ева не получает полезной информации о сигнале.

Однако это ещё не все проблемы Евы. Неверно угадав базис при проведении измерения, Ева вследствие свойства редукции волновой функции неизбежно пошлёт ошибочное состояние Бобу. Так, при применении измерения «+» вне зависимости от исходного состояния дальше будет послано одно из состояний набора $\{|x\rangle, |y\rangle\}$, а при измерении«×» — одно из состояний $\{|u\rangle, |v\rangle\}$. Измеряя эти состояния в «верном» для них базисе, Боб получит ошибку, по которой могут быть детектированы действия Евы.

Величину ошибки на приёмной стороне можно вычислить так: допустим, Ева подвергала атаке не все состояния, а некоторую их часть, атакуя каждый сигнал с вероятностью p. Тогда доля в $1 - p$ сигналов приходит к Бобу без какой-либо ошибки (Еве же приходится просто угадывать значение бита в каждой такой посылке, а значит, в её ошибку это даст вклад, равный $(1 - p)/2$). В то же время для сигналов, атакованных Евой, существует два равновероятных поворота событий:

- Ева верно угадала базис измерения, а значит, с одной стороны, точно получила информацию о передаваемом сигнале, а с другой стороны, не внесла какого-либо возмущения.

- Ева ошиблась в выборе базиса измерений. Тогда с вероятностью $1/2$ она получила ошибочный

результат, и совершенно точно она передала ошибочное состояние Бобу, что приводит к появлению ошибки на его стороне, вероятность которой равна также $1/2$.

Вероятность каждого из подобных сценариев равна $p/2$, и несложно видеть, что при такой стратегии доля ошибок на приёмной стороне будет равна $p/4$, а доля ошибок у Евы составит

$$\frac{1-p}{2} + \frac{p}{4} = \frac{1}{2} - \frac{p}{4}.$$

Это значит, что при всех значениях параметра p, меньших единицы, Ева имеет больше ошибок, чем Боб, а значит, её информация о передаваемом ключе строго меньше. В то же время при $p = 1$ доля ошибок у Боба и у Евы совпадают и равны 25%. Так как ошибка Боба однозначно связана с параметром p, можно считать, что 25% — пороговая величина ошибки при такой атаке, до которой возможно секретное распространение ключей.

Важно отметить, что ошибка на применой стороне может быть вызвана не только действиями Евы, но и причинами вроде неидеальности канала или детекторов. Однако при оценке стойкости протокола предполагается, что все ошибки были вызваны перехватчиком: очевидно, это лучший для него вариант развития событий.

Таким образом, критическая ошибка на приёмной стороне, до которой возможно секретное распространение ключей — основная характеристика протоколов квантовой криптографии. В общем случае она зависит лишь от самого протокола, однако в ряде частных случаев конкретных классов атак можно вычислить критическую ошибку для кадого из них. Протокол квантовой криптографии тем лучше, чем больше его критическая

ошибка: в этом случае он лучше противостоит помехам в канале связи и способен генерировать секретный ключ с большей скоростью и на бóльших расстояниях.

Прозрачное индивидуальное подслушивание

Очевидно, что стратегия приема-перепосыла не является оптимальной с точки зрения Евы — хотя бы потому, что её критическая величина ошибки значительно больше теоретического предела в 11%. Предложенная в этом разделе *прозрачная атака* способна добиться лучших результатов.

Суть прозрачного подслушивания заключается в том, что Ева не обязана мерить состояние в каждой посылке непосредственно в момент его пересылки по каналу, поскольку в этот момент ещё неизвестен используемый базис. Еве оказывается выгоднее подвергнуть каждый передаваемый сигнал совместной эволюции со своим состоянием, чтобы в итоге оставить у себя часть общего, сцепленного, состояния, а остаток переслать Бобу. Напомним, что в случае сцепленного общего состояния измерение Боба фиксирует частичное состояние Евы, и зная базис (информация о котором передаётся по открытому каналу), она может провести измерение над своей подсистемой. В итоге Ева сможет получить больше информации о передаваемых состояниях, и критическая величина ошибки будет меньше, чем в случае применения стратегии приёма-перепосыла.

Схема исследования стойкости протокола BB84 против прозрачного подслушивания такая же, как и при исследвании подслушивания методом приёма-перепосыла: сначала параметризуются действия Евы, затем находится

зависимость информации Боба и Евы от используемых параметров, и затем считается критическая величина ошибки.

Общий случай преобразования, производимого над состоянием $|\psi\rangle \in \mathcal{H}_{AB}$ в квантовом канале между Алисой и Бобом, даётся выражением

$$\Phi[|\psi\rangle\langle\psi|] = \rho_\psi,$$

где ρ_ψ — в общем случае смешанное состояние, получаемое на выходе канала. Такое состояние всегда можно очистить:

$$\rho_\psi = \mathrm{Tr}_{\mathcal{H}_E}|\Psi\rangle\langle\Psi|, \quad |\Psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_E,$$

$\mathcal{H}_E$ здесь — пространство окружения, имеющее достаточную размерность, чтобы итоговое состояние $|\Psi\rangle$ было чистым.

Рассмотрим посылку состояния $|x\rangle$. Заметим, что Ева производит свои действия после измерения Боба, которое фиксирует ρ_x. Так как базис его измерения совпадает с базисом посланного сигнала (остальные посылки отбрасываются при согласовании базисов), то можно считать, что оператор ρ_x после измерения оказывается диагональным в базисе $\{|x\rangle, |y\rangle\}$:

$$\rho_x = (1 - Q)|x\rangle\langle x| + Q|y\rangle\langle y|. \tag{3.7}$$

В этом выражении Q — вероятность ошибки на стороне Боба. Такое представление оператора ρ_x даёт возможность записать его очищение $|X\rangle$ в виде

$$|X\rangle = \sqrt{1-Q}|x\rangle|\psi_x\rangle + \sqrt{Q}|y\rangle|\theta_x\rangle, \tag{3.8}$$

где состояния $|\psi_x\rangle$ и $|\theta_x\rangle$ ортогональны. Так как Ева при такой атаке производит одинаковые действия над

каждым сигнальным состоянием, можно считать, что её исходное вспомогательное состояние (анцилла) всегда равна $|A\rangle$. Также предполагается, что Еве доступно всё окружение, то есть её пространство совпадает с $\mathcal{H}_E$. Это даёт возможность представить преобразование на общем пространстве легитимных пользователей и Евы U_{AE} : $\mathcal{H}_{AB} \otimes \mathcal{H}_E \to \mathcal{H}_{AB} \otimes \mathcal{H}_E$ в виде

$$U_{AE}(|x\rangle \otimes |A\rangle) = |X\rangle = \sqrt{1-Q}|x\rangle|\psi_x\rangle + \sqrt{Q}|y\rangle|\theta_x\rangle.$$

Аналогично получаются и другие соотношения, характеризующие преобразование Евы. Было показано [19], что при таком подслушивании оптимальной оказывается симметричная стратегия, при которой ошибка на стороне Боба Q не зависит от базиса. Имеем

$$\begin{aligned}
U_{AE}(|x\rangle \otimes |A\rangle) &= |X\rangle = \sqrt{1-Q}|x\rangle|\psi_x\rangle + \sqrt{Q}|y\rangle|\theta_x\rangle, \\
U_{AE}(|y\rangle \otimes |A\rangle) &= |Y\rangle = \sqrt{1-Q}|y\rangle|\psi_y\rangle + \sqrt{Q}|x\rangle|\theta_y\rangle, \\
U_{AE}(|u\rangle \otimes |A\rangle) &= |U\rangle = \sqrt{1-Q}|u\rangle|\psi_u\rangle + \sqrt{Q}|v\rangle|\theta_u\rangle, \\
U_{AE}(|v\rangle \otimes |A\rangle) &= |V\rangle = \sqrt{1-Q}|v\rangle|\psi_v\rangle + \sqrt{Q}|u\rangle|\theta_v\rangle,
\end{aligned} \tag{3.9}$$

где $\langle\psi_i|\theta_j\rangle = 0, \quad i,j \in \{x,y,u,v\}$. Более того, максимум достигается при симметрии состояний в пространстве Евы $\langle\psi_x|\psi_y\rangle = \langle\theta_x|\theta_y\rangle = \cos\alpha$. Требования унитарности и линейности U_{AE} влекут за собой, что

$$\begin{gathered}
\langle X|Y\rangle = \langle x|y\rangle, \quad \langle U|V\rangle = \langle u|v\rangle, \\
|U\rangle = \frac{1}{\sqrt{2}}(|X\rangle + |Y\rangle), \quad |V\rangle = \frac{1}{\sqrt{2}}(|X\rangle - |Y\rangle),
\end{gathered} \tag{3.10}$$

а из этого следует связь между векторами в пространстве

Евы

$$\begin{aligned}
2\sqrt{1-Q}|\psi_u\rangle &= \sqrt{1-Q}(|\psi_x\rangle + |\psi_y\rangle) + \sqrt{Q}(|\theta_x\rangle + |\theta_y\rangle),\\
2\sqrt{Q}|\theta_u\rangle &= \sqrt{1-Q}(|\psi_x\rangle - |\psi_y\rangle) - \sqrt{Q}(|\theta_x\rangle - |\theta_y\rangle),\\
2\sqrt{1-Q}|\psi_v\rangle &= \sqrt{1-Q}(|\psi_x\rangle + |\psi_y\rangle) - \sqrt{Q}(|\theta_x\rangle + |\theta_y\rangle),\\
2\sqrt{Q}|\theta_v\rangle &= \sqrt{1-Q}(|\psi_x\rangle - |\psi_y\rangle) + \sqrt{Q}(|\theta_x\rangle - |\theta_y\rangle).
\end{aligned} \tag{3.11}$$

Таким образом, в дальнейшем можно рассматривать только состояния из базиса «+», так как остальные состояния Евы однозначно выражаются через них.

Далее, ребование нормировки $\langle\psi_u|\psi_u\rangle = \langle\theta_u|\theta_u\rangle = 1$ приводит к тому, что

$$\cos\alpha = 1 - 2Q, \tag{3.12}$$

а это значит, что в распоряжении Евы имеется один параметр Q.

После преобразования Евы состояние, доступное для измерения Бобу, даётся частичным следом по пространству $\mathcal{H}_E$, а значит, его частичные операторы плотности соответственно равны

$$\begin{aligned}
\rho_x^B &= (1-Q)|x\rangle\langle x| + Q|y\rangle\langle y|,\\
\rho_y^E &= (1-Q)|y\rangle\langle y| + Q|x\rangle\langle x|
\end{aligned} \tag{3.13}$$

и дают ошибку на приёмной стороне, очевидно равную Q. Аналогично состояния Евы равны

$$\begin{aligned}
\rho_x^E &= (1-Q)|\psi_x\rangle\langle\psi_x| + Q|\theta_x\rangle\langle\theta_x|,\\
\rho_y^E &= (1-Q)|\psi_y\rangle\langle\psi_y| + Q|\theta_y\rangle\langle\theta_y|.
\end{aligned} \tag{3.14}$$

В случае индивидуальной атаки Ева производит измерение над каждым своим состоянием в отдельности,

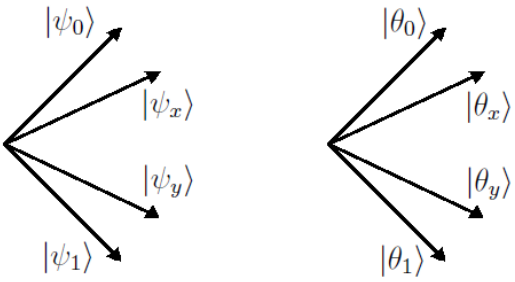

Рис. 3.1: Симметричное расположение базисных векторов $|\psi_0\rangle, |\psi_1\rangle, |\theta_0\rangle, |\theta_1\rangle$ относительно состояний в пространстве Евы.

то есть она стоит перед задачей различения квантовых состояний ρ_x^E и ρ_y^E. Оптимальное решение этой задачи известно [23]. Запишем матрицы операторов плотности

Евы (3.14) в базисе

$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{2}\left[\left(\frac{1}{\sqrt{1+\cos\alpha}}+\frac{1}{\sqrt{1-\cos\alpha}}\right)|\psi_x\rangle+\right.\\
&\left.+\left(\frac{1}{\sqrt{1+\cos\alpha}}-\frac{1}{\sqrt{1-\cos\alpha}}\right)|\psi_y\rangle\right],\\
|\psi_1\rangle &= \frac{1}{2}\left[\left(\frac{1}{\sqrt{1+\cos\alpha}}-\frac{1}{\sqrt{1-\cos\alpha}}\right)|\psi_x\rangle+\right.\\
&\left.+\left(\frac{1}{\sqrt{1+\cos\alpha}}+\frac{1}{\sqrt{1-\cos\alpha}}\right)|\psi_y\rangle\right],\\
|\theta_0\rangle &= \frac{1}{2}\left[\left(\frac{1}{\sqrt{1+\cos\alpha}}+\frac{1}{\sqrt{1-\cos\alpha}}\right)|\theta_x\rangle+\right.\\
&\left.+\left(\frac{1}{\sqrt{1+\cos\alpha}}-\frac{1}{\sqrt{1-\cos\alpha}}\right)|\theta_y\rangle\right],\\
|\theta_1\rangle &= \frac{1}{2}\left[\left(\frac{1}{\sqrt{1+\cos\alpha}}-\frac{1}{\sqrt{1-\cos\alpha}}\right)|\theta_x\rangle+\right.\\
&\left.+\left(\frac{1}{\sqrt{1+\cos\alpha}}+\frac{1}{\sqrt{1-\cos\alpha}}\right)|\theta_y\rangle\right],
\end{aligned}
\tag{3.15}
$$

элементы которого симметрично расположены относительно векторов $|\psi_x\rangle, |\psi_y\rangle$ и $|\theta_x\rangle, |\theta_y\rangle$ соответственно (см. рис. 3.1). Произведения базисных векторов на $|\psi_i\rangle, |\theta_i\rangle$ равны

$$\langle\psi_0|\psi_x\rangle = \langle\theta_1|\theta_x\rangle = \cos a, \quad \langle\psi_0|\psi_y\rangle = \langle\theta_0|\theta_y\rangle = \sin a,$$

$$\langle\psi_1|\psi_x\rangle = \langle\theta_1|\theta_x\rangle = \sin a, \quad \langle\psi_1|\psi_y\rangle = \langle\theta_1|\theta_y\rangle = \cos a,$$

где для краткости введено обозначение $a = \frac{\pi}{4} - \frac{\alpha}{2}$. Матрицы операторов плотности Евы будут равны

$$\rho_x^E = \frac{1}{2}\begin{pmatrix} (1-Q)\cos^2 a & (1-Q)\cos a\sin a & 0 & 0 \\ (1-Q)\cos a\sin a & (1-Q)\sin^2 a & 0 & 0 \\ 0 & 0 & Q\cos^2 a & Q\cos a\sin a \\ 0 & 0 & Q\cos a\sin a & Q\sin^2 a \end{pmatrix},$$

$$\rho_y^E = \frac{1}{2}\begin{pmatrix} (1-Q)\sin^2 a & (1-Q)\cos a \sin a & 0 & 0 \\ (1-Q)\cos a \sin a & (1-Q)\cos^2 a & 0 & 0 \\ 0 & 0 & Q\sin^2 a & Q\cos a \sin a \\ 0 & 0 & Q\cos a \sin a & Q\cos^2 a \end{pmatrix}.$$

В [23] было показано, что оптимальным набором различающих операторов измерения будет набор $\{M_x = M, M_y = I - M\}$, где M — проектор на собственное подпространство оператора $\frac{1}{2}(\rho_x^E - \rho_y^E)$, отвечающее положительным собственным значениям. Легко вычислить, что

$$M_x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad M_y = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

и вероятность получения ошибки равна

$$\mathrm{Tr} M_y \rho_x^E = \mathrm{Tr} M_x \rho_y^E = (1-Q)\sin^2 a + Q\sin^2 a = \sin^2 a = \\ = \frac{1-\sin\alpha}{2} = \frac{1-\sqrt{1-\cos^2\alpha}}{2} = \frac{1-2\sqrt{Q(1-Q)}}{2}.$$

Итак, построена зависимость ошибки на стороне Боба и на стороне Евы от единственного её параметра — Q. При малых значениях Q ошибка легитимных пользователей мала, а ошибка Евы близка к $\frac{1}{2}$, а значит, распространение секретной информации возможно. Критическая величина Q, до которой возможно секретное распространение ключа, даётся равенством

$$Q_c = \frac{1-2\sqrt{Q_c(1-Q_c)}}{2} \tag{3.16}$$

и равна $\frac{2-\sqrt{2}}{4} \approx 14,64\%$. Таким образом, критическая ошибка при прозрачном индивидуальном подслушивании Евы оказывается меньше, чем при подслушивании с помощью приёма-перепосыла, а значит, такая стратегия

лучше. Это улучшение вызвано тем, что Ева в своих действиях учитывает информацию, поступающую к ней от легитимных пользователей при согласовании базисов, производимого по открытому каналу.

Коллективная атака

Критическая величина прозрачного индивидуального подслушивания, равная приблизительно $14,6\%$, всё равно превосходит теоретический порог в 11%. Возникает вопрос: как Еве нужно изменить схему атаки, чтобы добиться ещё лучших результатов? Оказывается, что слабая сторона индивидуальной атаки — в проведении измерений над каждым передаваемым состоянием по отдельности. Из-за свойства супераддитивности информации в классически-квантовом (c-q) канале оказывается, что со стороны Евы выгоднее проводить измерение над всей последовательностью полученных состояний сразу.

После проведения измерений и согласования базисов Алиса и Боб находятся в состоянии классического бинарного канала связи с вероятностью ошибки Q. Пропускная способность такого канала известна [12] и даётся величиной $C_{AB} = 1 - h(Q)$, где $h(Q)$ — бинарная энтропия Шеннона

$$h(Q) = (1-Q)\log(1-Q) + Q\log Q. \qquad (3.17)$$

В то же время Алиса с Евой оказываются в ситуации c-q-канала с состояниями на выходе, равными ρ_x^E и ρ_y^E. Фундаментальное ограничение на информацию, которую можно извлечь из такого канала, даётся формулой Холево

$$C_{AE} = \chi = H(\frac{1}{2}(\rho_x^E + \rho_y^E)) - \frac{1}{2}(H(\rho_x^E) + H(\rho_y^E)). \qquad (3.18)$$

Распространение секретного ключа возможно, когда $C_{AE} < C_{AB}$.

Для подсчёта величины χ нужно найти собственные значения оператора $\rho^E = \frac{1}{2}(\rho_x^E + \rho_y^E)$. Выпишем его матрицу в базисе $\{|\psi_0\rangle, |\psi_1\rangle, |\theta_0\rangle, |\theta_1\rangle\}$:

$$\rho^E = \frac{1}{2}\begin{pmatrix} (1-Q) & (1-Q)\cos\alpha & 0 & 0 \\ (1-Q)\cos\alpha & (1-Q) & 0 & 0 \\ 0 & 0 & Q & Q\cos\alpha \\ 0 & 0 & Q\cos\alpha & Q \end{pmatrix}. \tag{3.19}$$

Собственные значения этой матрицы равны

$$\lambda_{1,2} = (1-Q)\frac{1 \pm \cos\alpha}{2}, \quad \lambda_{3,4} = Q\frac{1 \pm \cos\alpha}{2}, \tag{3.20}$$

а собственные значения частичных матриц плотности ρ_x^E и ρ_y^E равны $1-Q$ и Q. В итоге, с учётом (3.12), находим

$$C_{AE} = (1-Q)\log(1-Q) + Q\log Q = h(Q). \tag{3.21}$$

Из этого следует, что критическая ошибка Q_c для коллективной атаки равна корню уравнения $1 - h(Q_c) = h(Q_c)$, а это совпадает с полученным выше теоретическим пределом и приблизительно равно 11%.

Величина критической ошибки в 11%, однако, достигается лишь при условии использования Евой коллективных измерений сразу над всей последовательностью символов. Также допустима ситуация, когда Ева производит измерения не над всей последовательностью состояний, а над каждым из её блоков длины n в отдельности. Вообще говоря, существует бесконечное множество пропускных способностей C_n, соответствующих именно таким блочным измерениям, и последовательность $\{C_n\}$ возрастает.

Возрастание пропускной способности c-q-канала при использовании блоков большей длины даёт ответ на вопрос о том, что происходит при ошибке между 11% (предельное значение при коллективной атаке) и $14,6\%$ (для индивидуального подслушивания): такие случаи соответствуют критическим ошибкам при использовании Евой измерения над n блоками одновременно. Однако до тех пор, пока не создана квантовая память, критической ошибкой протокола BB84 можно считать величину в $14,6\%$.

Когерентная атака

Главным ограничением коллективной атаки является то, что Ева должна использовать одно и то же преобразование для каждого сигнала. Возможно, однако, что более общий случай атаки, при котором Ева производит унитарное преобразование сразу над всей последовательностью передаваемых состояний, или учитывает на каждом шаге какие-либо результаты предыдущих шагов (например, результаты частичных измерений её подсистем), может дать Еве больше информации о передаваемом ключе по сравнению с «ограниченным» случаем коллективной атаки. Но оказывается, что это не так, и коллективная атака является наиболее эффективной.

Причина, по которой когерентная атака не способна принести дополнительной пользы Еве, состоит в следующем. После достаточно большого числа посылок N общее состояние всех участников протокола можно описать оператором плотности $\rho_{A^N B^N E^N}$. В [9] была доказана теорема, которая утверждает, что если Алиса и Боб дополнительно совершат случайную согласованную перестановку состояний своих подсистем в разных посылках, то частичный оператор плотности Алисы и

Боба $\rho_{A^N B^N}$ может быть сколь угодно точно представлен в виде тензорного произведения операторов плотности, относящихся к отдельным посылкам:

$$\rho_{A^N B^N} \approx \sigma_{AB}^{\otimes N}. \tag{3.22}$$

Таким образом, получается, что простой случайной перестановкой битов Алиса и Боб могут свести на нет всю дополнительную выгоду Евы от использования когерентной атаки. Это важный результат для квантовой криптографии, так как он позволяет использовать коллективное подслушивание в качестве наиболее эффективного метода атаки, а его исследование значительно проще, чем анализ когерентного случая.

Глава 4

Другие протоколы квантовой криптографии

Протокол BB84 является первым и наиболее изученным протоколом квантового распределения ключей. Тем не менее попытки его технической реализации натолкнулись на ряд технологических трудностей, в результате чего у Евы появляется возможность провести новый тип перехвата информации, невозможный при «строгой» реализации всех принципов протокола BB84. Так как квантовая криптография ставит своей целью обеспечение секретности при *всех возможных* действиях Евы, появилась необходимость разработки протоколов, способных противостоять Еве и на современном уровне развития технологий.

В начале этой главы будет рассказано о близком к BB84, но более гибком протоколе B92, идеи которого будут использованы в дальнейшем. Затем будет описан новый тип атаки, возможный в практических схемах квантовой криптографии — атака с расщеплением по числу фотонов (PNS — photon number splitting attack). Далее описываются технологии противодействия этой

атаке, которые находят своё наиболее важное применение в протоколе SARG04.

4.1 Протокол B92

Изложим сначала основные сведения о протоколе B92[2], который использует два неортогональных состояния. Этот протокол важен, так как идеи использования неортогональной пары состояний будут использованы в протоколах SARG04 и неортогональной версии протокола с фазово-временным кодированием.

Обратим внимание, что в протоколе BB84 при отсутствии действий перехватчика и помех в канале вероятность ошибки на приемной стороне до согласования базисов составляет 25%. Это вызвано использованием «жёсткой» конфигураци двух пар базисных векторов. Цель протокола B92 состоит в возможности гибкого изменения этого параметра в зависимости от дополнительных условий — таких, например, как длина канала или его качество. Это может в ряде случаев помочь добиться большей скорости передачи данных.

На каждом шаге протокола B92 Алиса посылает Бобу одно из двух неортогональных состояний $|\psi_0\rangle$, $|\psi_1\rangle$, где $\langle\psi_0|\psi_1\rangle = \cos\eta$ — основной параметр протокола. Боб на своей строне производит уже описанное выше «измерение с тремя исходами» (2.11)

$$M_0 = \frac{|\psi_1^\perp\rangle\langle\psi_1^\perp|}{1+\cos\eta} = \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta},$$

$$M_1 = \frac{|\psi_0^\perp\rangle\langle\psi_0^\perp|}{1+\cos\eta} = \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta},$$

$$M_? = I - M_0 - M_1.$$

Напомним, что при применении подобного измерения над указанными состояниями первые два исхода будут при отсутствии ошибок отвечать точным результатам, в то время как несовместный (inconclusive) исход «?» не даёт полезных сведений о передаваемом состоянии. Посылки с такими исходами отбрасываются.

После передачи всех сообщений Алиса и Боб, подобно тому, как это происходило в протоколе BB84, согласованно раскрывают часть своих битовых последовательностей и оценивают число ошибок. Если их оказалось больше некоторой пороговой величины, выполнение протокола прерывается, иначе из оставшейся части битовых строк извлекается полностью секретный ключ. Стойкость протокола против наиболее эффективной (коллективной) атаки Евы была исследована в [18].

Важнейшим свойством протокола B92 является наличие у него параметра — угла η между сигнальными состояниями. Чем ближе этот угол к $\pi/2$, тем ближе оказывается протокол к простой пересылке сигналов с помощью ортогональных состояний. При этом скорость передачи данных возрастает, однако их стойкость против перехвата снижается. При использовании же небольших значений η велика вероятность получения несовместных исходов, что снижает скорость передачи данных, но существенно осложняет ситуацию для подслушивателя.

4.2 PNS-атака

Главной особенностью практических схем квантовой криптографии с точки зрения перехватчика оказывается использование ослабленных лазерных импульсов вместо строго однофотонного источника. Покажем, каким образом подобное техническое ограничение вместе с

неизбежным затуханием в реальных каналах связи может привести к потере секретности протоколов из-за возможности использования PNS-атаки[1].

Операция разделения фотонов

При использовании ослабленных лазерных импульсов вместо состояний $|0\rangle$ и $|1\rangle$ по квантовому каналу пересылаются состояния вида $|0\rangle^{\otimes n}$ и $|1\rangle^{\otimes n}$, где $n \geq 1$ — число фотонов в импульсе. Нетрудно видеть, что если Ева произведёт измерение, описывающееся разложением единицы

$$\begin{aligned} M_1 &= |0\rangle\langle 0| + |1\rangle\langle 1|, \\ M_2 &= |00\rangle\langle 00| + |11\rangle\langle 11|, \\ &\ldots \\ M_n &= |0\rangle^{\otimes n}\langle 0|^{\otimes n} + |1\rangle^{\otimes n}\langle 1|^{\otimes n}, \\ &\ldots \end{aligned} \tag{4.1}$$

то она, во-первых, получит всю информацию о числе фотонов в импульсе, а во-вторых, не внесёт в канал никаких помех. Таким образом, законы квантовой механики не налагают ограничений на получение точной информации о числе фотонов в импульсе.

Зная, какие импульсы содержат несколько фотонов, Ева может заблокировать те из них, которые содержат лишь один фотон, а для многофотонных импульсов переслать Бобу один из фотонов, произведя некоторые действия над остальными. Блокировка одночастичных импульсов может быть компенсирована использованием более совершенного канала для транспортировки оставшихся импульсов на сторону Боба. По предположению легитимные пользователи не имеют полного контроля над квантовым каналом связи,

и Ева может заменить его на свой канал, затухание в котором меньше, чем в канале между Алисой и Бобом. В идеале Ева может использовать для пересылки оставшихся фотонов Бобу канал, не дающий никаких потерь. Поэтому при достаточной доле многофотоннных импульсов на стороне источника и потерях в канале связи действия Евы не могут быть детектированы.

Атака на протокол BB84

Покажем, каким образом операция разделения фотонов может быть приненена для взлома протокола BB84. Итак, Ева может без каких-либо последствий узнать число фотонов в каждом из импульсов. Атака строится следующим образом: если импульс содержит лишь один фотон, Ева его блокирует, в противном случае она оставляет в своей квантовой памяти (для её реализации достаточно иметь обычную линию задержки) один из фотонов, пересылая остальные Бобу по своему более совершенному каналу (в идеале по каналу вообще без потерь). После операции согласования базисов, проводящейся по открытому каналу, Ева получает всю необходимую информацию для достоверного различения имеющихся у неё фотонов, а значит, способна узнать весь ключ, не будучи обнаруженной. Это делает протокол BB84 полностью незащищённым перед PNS-атакой.

Атака на протокол B92

Атака на протокол B92 оказывается ещё более простой. Она возможна даже в случае строго однофотонного источника, и для её проведения достаточно лишь затухания в канале связи между Алисой и Бобом. Ева может провести то же измерение, которое на своей

стороне производит Боб. В случае совместного исхода Ева получает всю информацию о передаваемом сигнале, и может переслать его Бобу без ошибок (снова используя более совершенный канал для компенсации потерь). Если же измерение дало несовместный исход, то Ева попросту блокирует импульс. При такой атаке Ева получает всю информацию, не будучи обнаруженной.

Следует отметить, что формально описанная атака даже не попадает под определение PNS-атаки, так как не использует операцию разделения фотонов. Эта атака возможна не в случае передачи многофотонных лазерных испульсов, а при использовании неидеального канала связи с потерями больше некоторого критического уровня. Таким образом, протокол B92 оказывается значительно более уязвимым для подобного подслушивания.

Критическая длина линии связи

Важным фактором в ообоих описанных схемах атаки является компенсация дополнительного затухания, вызванного блокировкой части импульсов Евой: при отсутствии подобной компенсации Ева может быть обнаружена по дополнительным показателям затухания. Так как исходные потери в канале зависят от его длины, то Ева может компенсировать блокировку всех однофотонных импульсов только при использовании достаточно длинного канала между Алисой и Бобом. Покажем, как именно оценивается критическая длина канала при PNS-атаке на протокол BB84.

Число фотонов в лазерном импульсе распределено по закону Пуассона

$$p(n) = \frac{e^{-\mu}\mu^n}{n!}, \tag{4.2}$$

где μ — среднее число фотонов, обычно приблизительно

равное 0.1. Вероятность испускания состояния с одним фотоном равна

$$p_1 = \mu e^{-\mu}, \tag{4.3}$$

а вероятность генерации импульса с несколькими ($n \geq 2$) фотонами равна

$$p_{\geq 2} = 1 - e^{-\mu} - \mu e^{-\mu}. \tag{4.4}$$

В этих выражениях $e^{-\mu}$ — вероятность вакуумной компоненты, то есть состояния без фотонов. Доля фотонов, которые достигнут приёмной стороны в канале длины L с коэффициентом поглощения α равна

$$(p_1 + p_{\geq 2})10^{-\alpha L/10}. \tag{4.5}$$

Для стандартных современных одномодовых волокон типа SMF-28 значение коэффициента поглощения составляет $\alpha = 0.18 - 0.2$ дБ/км. В приведённой формуле была использована консервативная в пользу Евы оценка, так как вероятности достижения приёмной стороны отличаются для состояний с разным количеством фотонов, а чем меньше вероятность достижения приёмника, тем больше возможности Евы по перехвату.

Действия Евы при проведении PNS-атаки сводятся к следующему. Не меняя общей доли достигающих Боба посылок, Ева должна блокировать как можно больше однофотонных сигналов, оставляя у себя один из фотонов в случае обнаружения многофотонного импульса. В идеальной для неё ситуации Ева должна блокировать все однофотонные компоненты, таким образом получая всю информацию о передаваемом ключе. Она может это сделать в том случае, когда количество испускаемых многофотонных испульсов (4.4) оказывается не меньше количества достигающий приёмной стороны сигналов

(4.5). Так как величина (4.5) является константой протокола и зависит от длины линии связи L, можно говорить о критической величине расстояния между Алисой и Бобом, до которого PNS-атака оказывается неприменимой. Таким образом, целью противодействия PNS-атаке является увеличение критической длины линии связи: чем она больше, тем более устойчивым является протокол.

4.3 Протокол 4+2

Протокол, названный «4+2»[8], был первой попыткой противостояния PNS-атаке. Его идея такова: раз PNS-уязвимость протокола BB84 вызвана тем, что после согласования базисов Ева может получить точную информацию о передаваемом состоянии, то можно сделать состояния внутри каждого базиса неортогональными, тем самым сделав для Евы невозможным точное определение передаваемого состояния даже при известном базисе. В то же время если Ева решит провести то же измерение, что производит на своей стороне Боб, то это приведет к ситуации, похожей на явное просушивание протокола BB84: Ева внесет в канал ошибку, провизводя измерение в наугад выбранном базисе, и её вмешательство будет обнаружено. Так как на неортогональных состояниях основан протокол B92, то можно считать, что в протоколе 4+2 используется своеобразная комбинация протоколов BB84 и B92, отсюда и его название.

Сигнальные состояния протокола

В качестве примера такой конфигурации состояний удобно взять набор из четырех состояний, которые лежат в двух

перпендикулярных плоскостях на сфере Пуанкаре, но не являются ортогональными, например (различные базисы обозначены как X и Y):

$$|0_x\rangle = \cos\frac{\eta}{2}|0\rangle + \sin\frac{\eta}{2}|1\rangle, \quad |1_x\rangle = \cos\frac{\eta}{2}|0\rangle - \sin\frac{\eta}{2}|1\rangle,$$
$$|0_y\rangle = \cos\frac{\eta}{2}|0\rangle + i\sin\frac{\eta}{2}|1\rangle, \quad |1_y\rangle = \cos\frac{\eta}{2}|0\rangle - i\sin\frac{\eta}{2}|1\rangle. \tag{4.6}$$

Здесь наложение векторов каждого базиса равно

$$\langle 0_x|1_x\rangle = \langle 0_y|1_y\rangle = \cos^2\frac{\eta}{2} - \sin^2\frac{\eta}{2} = \cos\eta.$$

Возможность взлома 4+2

На первых взгляд такой подход способен защитить от PNS-атаки. Однако при более подробном рассмотрении оказывается, что этот протокол не способен дать существенной защиты: авторы [1] показали, что Ева может провести следующее измерение, которое они назвали фильтрацией (filtering):

$$A_{ok} = \frac{1}{\sqrt{1+\cos\eta}}(|+x\rangle\langle 1_x^{\perp}|+|-x\rangle\langle 0_x^{\perp}|), \quad A_? = \sqrt{I - A_{ok}A_{ok}^{\dagger}}. \tag{4.7}$$

Суть его в том, что оно в случае успеха делает состояния из базиса X оротогальными, проецируя их на $|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, а с некоторой вероятностью неудачи даёт несовместный исход.

Проблема протокола 4+2 в том, что это же измерение может сделать ортогональными и состояния в базисе Y. Покажем это. Оператор плотности состояния ρ после измерения A_i переходит в одно из соостояний ρ_i:

$$\rho_i = \frac{A_i\rho A_i^{\dagger}}{\mathrm{Tr}(A_i\rho A_i^{*})}. \tag{4.8}$$

В нашем случае имеем

$$A_{ok}|0_y\rangle\langle 0_y|A_{ok}^* =$$
$$= \frac{1}{1+\cos\eta}(|+x\rangle\langle 1_x^\perp| + |-x\rangle\langle 0_x^\perp|)|0_y\rangle\langle 0_y|(|1_x^\perp\rangle\langle +x| +$$
$$+|0_x^\perp\rangle\langle -x|) = \frac{2\cos^2\frac{\eta}{2}\sin^2\frac{\eta}{2}}{1+\cos\eta}(|+x\rangle\langle +x| +$$
$$+|-x\rangle\langle -x| + i|+x\rangle\langle -x| - i|-x\rangle\langle +x|) =$$
$$= (1-\cos\eta)|+y\rangle\langle +y|,$$

аналогично

$$A_{ok}|1_y\rangle\langle 1_y|A_{ok}^* = (1-\cos\eta)|-y\rangle\langle -y|,$$

где $|\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$

Таким образом, указанное измерение фильтрации способно свести посылаемые состояния к парам ортогональных состояний, то есть фактически атака на протокол 4+2 сводится к атаке на протокол BB84. Действия Евы таковы: при получении совместного исхода фильтрации она оставляет у себя одну из частиц и после процедуры согласования базисов получает из неё полную информацию. В случае же несовместного исхода Ева блокирует импульс. В итоге при указанных действиях Евы протокол 4+2 также оказывается незащищённым против PNS-атаки.

4.4 Протокол SARG04

Авторы [1], наряду с демонстрацией уязвимости протокола 4+2, предложили также способ противостояния подобным действиям перехватчика. Проблема протокола 4+2, как

видно, в том, что возможно проведение измерения, которое бы делало (с некоторой ненулевой вероятностью) ортогональными состояния в каждой паре базисов. Была придумана схожая конфигурация векторов, при которой проведение подобного измерения становится невозможным.

Невозможность различающего измерения

В общем случае требование к конфигурации векторов таково: пары векторов из разных базисов не должны быть связаны унитарным преобразованием. Если это требование выполняется, то возможность проведения фильтрации со стороны Евы исключается. Поясним, почему это происходит. Пусть есть две пары базисов — «a» и «b»:

$$a : \{|0_a\rangle, |1_a\rangle\}$$
$$b : \{|0_b\rangle, |1_b\rangle\},$$

и векторы из разных базисов связаны унитарным преобразованием U:

$$\begin{pmatrix} |0_b\rangle \\ |1_b\rangle \end{pmatrix} = U \begin{pmatrix} |0_a\rangle \\ |1_a\rangle \end{pmatrix}, \tag{4.9}$$

или, иначе:

$$\begin{aligned} |0_b\rangle &= u_{11}|0_a\rangle + u_{12}|1_a\rangle \\ |1_b\rangle &= u_{21}|0_a\rangle + u_{22}|1_a\rangle. \end{aligned} \tag{4.10}$$

Если Ева теперь проводит фильтрацию, проектируя исходные состояния из базиса «a» на ортогональные состояния $\{|0'_a\rangle, |1'_a\rangle\}$, то это измерение можно описать так:

$$M|i_a\rangle = \frac{1}{\sqrt{p_a}}|i'_a\rangle, \quad i = 0, 1, \tag{4.11}$$

векторы же из базиса «b» будут, по линейности, отображаться следующим образом:

$$M|0_b\rangle = M(u_{11}|0_a\rangle + u_{12}|1_a\rangle) = \frac{1}{\sqrt{p_a}}(u_{11}|0'_a\rangle + u_{12}|1'_a\rangle)$$
$$M|1_b\rangle = M(u_{21}|0_a\rangle + u_{22}|1_a\rangle) = \frac{1}{\sqrt{p_a}}(u_{21}|0'_a\rangle + u_{22}|1'_a\rangle). \tag{4.12}$$

Тогда наложение векторов в базисе «b» после такого преобразования будет равно

$$|\langle 0'_b|1'_b\rangle| = |u_{11}u_{21} + u_{12}u_{22}|, \tag{4.13}$$

а из определения унитарного преобразования ($UU^* = U^*U = I$) следует свойство $u_{11}u_{21} + u_{12}u_{22} = 0$, и это значит, что для всякого унитарного преобразования, связывающего состояния из разных базисов, Ева сможет подобрать измерение, проектирущее векторы каждого базиса на ортогональные состояния. И напротив, если векторы связаны преобразованием, отличным от унитарного, то выполнение неравенства

$$|u_{11}u_{21} + u_{12}u_{22}| > |\langle 0_a|1_a\rangle| \tag{4.14}$$

гарантирует, что любое измерение, делающее ортогональным состояния одной пары базисов, будет неминуемо уменьшать угол между состояниями другой пары, делая их менее различимыми. А именно это и нужно протоколу для противостояния PNS-атаке.

Описание протокола

Протокол SARG04 основывается на показанном выше свойстве: при определенной конфигурации состояний

Ева уже не сможет провести процедуру фильтрации, которая бы делала ортогональными состояния в каждой паре базисов. Конфигурация, предложенная его авторами ([11]), выглядит так:

$$\begin{aligned} |0_a\rangle &= \begin{pmatrix} \cos\frac{\eta}{2} \\ \sin\frac{\eta}{2} \end{pmatrix}, \quad |1_a\rangle = \begin{pmatrix} \cos\frac{\eta}{2} \\ -\sin\frac{\eta}{2} \end{pmatrix}, \\ |0_b\rangle &= \begin{pmatrix} \sin\frac{\eta}{2} \\ -\cos\frac{\eta}{2} \end{pmatrix}, \quad |1_b\rangle = \begin{pmatrix} \sin\frac{\eta}{2} \\ \cos\frac{\eta}{2} \end{pmatrix}. \end{aligned} \tag{4.15}$$

Это две пары базисов: $\{|0_a\rangle, |1_a\rangle\}$ и $\{|0_b\rangle, |1_b\rangle\}$. В каждом из базисов угол между векторами равен η:

$$\langle 0_a|1_a\rangle = \cos\eta, \quad \langle 0_b|1_b\rangle = -\cos\eta,$$

состояния же из разных базисов связаны соотношениями

$$\langle 0_a|0_b\rangle = \langle 1_a|1_b\rangle = 0,$$

$$\langle 0_a|1_b\rangle = \langle 1_a|0_b\rangle = \sin\eta.$$

Рассмотрим теперь, способна ли такая конфигурация векторов препятствовать проедению PNS-атаки. Связь между векторами разных базисов даётся соотношением

$$|0_b\rangle = c|0_a\rangle + c'|1_a\rangle$$

$$|1_b\rangle = c'|0_a\rangle + c|1_a\rangle,$$

где

$$c = -\frac{\cos\eta}{\sin\eta}, \quad c' = \frac{1}{\sin\eta}.$$

Конфигурация состояний протокола показана на рис. 4.1.

Как нетрудно видеть, значение величины перекрытия (4.14) тут равно

$$2cc' = \frac{2\cos\eta}{\sin^2\eta} \geq \cos\eta,$$

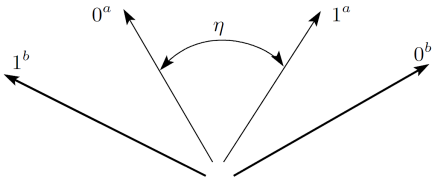

Рис. 4.1: Геометрия состояний в протоколе SARG04: обычными векторами показаны состояния, относящиеся к базису «a», жирными — к базису «b». Состояния 0 и 1 из разных базисов взаимно ортогональны.

а значит, как было показано ранее, этот протокол способен эффективно противостоять PNS-атаке.

Стойкость протокола против PNS-атаки может быть нарушена только в том случае, когда перехватчик обладает способностью блокировать все посылки, содержащие один и два фотона, а для посылок, содержащих три фотона, измерять два из них в разных базисах, блокируя импульс при получении хотя бы одного несовместного исхода. Так как при угле η между состояниями, меньшем $\pi/4$, вероятность получения несовместного исхода хотя бы при одном измерении оказывается больше $\cos^2 \frac{\pi}{4} = 1/2$, то можно считать, что для эффективного прослушивания протокола SARG04 Ева должна обладать возможностью блокировать и трёхфотонные посылки. Таким образом, протокол теряет секретность в случае, когда Ева может блокировать все одно-, двух- и трёхфотонные посылки, что означает существенно бóльшую защищённость против PNS-атаки, чем при использовании протокола BB84.

В работе [11] был также показан важный частный случай этого протокола, который использует те же

сигальные состояния, что и протокол BB84, но с другой техникой кодирования информации, благодаря чему ценой скорости передачи данных улучшается стойкость против PNS-атаки. Этот частный случай рассматривает угол η, равный $\frac{\pi}{4}$, тогда сигнальными состояниями можно считать (после поворота) $|\pm x\rangle$ и $|\pm z\rangle$, как и в случае BB84. Использование тех же сигнальных состояний предпочтительно с точки зрения простоты технической реализации. Боб теперь также случайно меряет компоненту σ_x или σ_z, но при публичном согласовании вместо базиса Алиса называет одну из четырех пар состояний $A_{m,n}$, где $m, n \in \{\pm 1\}$. Считается, что сигнал 0 кодируется состояниями $|\pm x\rangle$, а 1 — состояниями $|\pm z\rangle$. Например, если Алиса хочет послать сигнал 1, она может послать состояние $|-z\rangle$ и публично объявить пару $A_{+,-}$. Тогда Боб сможет достоверно распознать этот результат лишь в случае, если он мерил σ_x и получил -1. При получении результата $+1$ он не сможет понять, хотела ли Алиса послать ему 0 в базисе σ_x или что-либо в базисе σ_z, а измерив σ_z, Боб обязательно получит -1, но не будет знать, из какого базиса посылалось состояние, так как Алиса могла бы использовать и базис σ_x. Таким образом, после согласования базисов у Алисы и Боба совпадет четверть посланных сигналов, и скорость передачи в таком протоколе будет вдвое меньше, чем в протоколах BB84 и B92.

Задачи

1. Было приготовлено одно из состояний: $\{|0\rangle, |1\rangle\}$. Посчитать вероятности каждого из исходов при измерении его наблюдаемой:

$$a) M_+ : M_+^0 = |0\rangle\langle 0|, M_+^1 = |1\rangle\langle 1|, \tag{4.16}$$

$$\begin{aligned} b) M_\times : M_\times^0 &= \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|), \\ M_\times^1 &= \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|). \end{aligned} \tag{4.17}$$

   В каком состоянии окажется система после измерения в обоих случаях?

2. Было приготовлено состояние: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Затем оно было измерено а) наблюдаемой (4.16) б) наблюдаемой (4.17). Результат наблюдения неизвестен. В каком состоянии будет система после измерения?

3. Над состоянием $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ было произведено измерение наблюдаемой (4.16), а затем наблюдаемой (4.17). Какова вероятность каждой возможной пары исходов? Каковы будут эти вероятности, если указанные измерения провести в обратном порядке?

4. В протоколе B92, использующем два неортогональных состояния $|\varphi\rangle$ и $|\psi\rangle$, применяется «измерение с тремя исходами» (2.11). Какова вероятность получения каждого из исходов этого измерения? Как преобразуется состояние $|\varphi\rangle$ после этого измерения? В чем смысл множителя $1/(1+\langle\varphi|\psi\rangle)$ перед операторами M_0 и M_1?

5. * Как будет выглядеть расширение Наймарка для «измерения с тремя исходами» (2.11)?

6. Ева атакует протокол BB84 методом приема-перепосыла с параметром p — вероятностью измерения данного сигнала. Если сигнал не измеряется, соответствующее значение битовой строки угадывается. Посчитать вероятность ошибки на стороне Боба и на стороне Евы при такой атаке. При каком критическом значении ошибки на приемной стороне вероятность ошибки Боба перестанет быть меньше вероятности ошибки Евы?

7. Ева атакует протокол B92 методом приема-перепосыла. Параметр протокола — угол между сигнальными состояниями, — равен $\cos\alpha$. Параметр атаки — вероятность измерения каждого сигнала, — равен p. Найти величину ошибки на приемной стороне, до которой ошибка Евы при такой атаке оказывается больше.

8. Алиса передает Бобу по квантовому каналу одно из состояний $\{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\}$. Ева добавляет к нему анциллу в состоянии $|0\rangle$ и производит над получившейся парой кубитов преобразование CNOT. Какие состояния окажутся после этого в распоряжении Боба и Евы?

9. Написать представление Крауса для канала, в котором Ева применяет атаку «прием-перепосыл» с параметром p — вероятностью измерения кубита а) для протокола BB84 б) для протокола B92.

10. * Написать представление Крауса для «прозрачного» подслушивания с параметром Q — вероятностью ошибки на приемной стороне а) для протокола BB84 б) для протокола B92.

11. * Написать представление Стайнспринга для атаки методом «прием-перепосыл» с параметром p — вероятностью измерения кубита а) для протокола BB84 б) для протокола B92.

12. * Написать представление Стайнспринга для «прозрачного» подслушивания с параметром Q — вероятностью ошибки на приемной стороне а) для протокола BB84 б) для протокола B92.

13. Сформулировать протокол ЭПР-состояний (протокол Экерта) и обосновать его стойкость.

14. Вычислить критическую длину линии связи для протокола B92 как функцию значения угла между сигнальными состояниями, интенсивности лазерного излучения и затухания в канале связи.

15. Вычислить критическую длину линии связи для протоколов «4+2» и SARG04 как функцию значения угла между состояниями внутри базисов, интенсивности лазерного излучения и затухания в канале связи.

Литература

[1] *Acin A., Gisin N., and Scarani V.* Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Phys. Rev. A — 2004. — Vol. 69, 012309.

[2] *Bennett C.H.* Quantum Cryptography using any Two Nonortogonal States // Phys. Rev. Lett. — 1992. —Vol. 68, 3121.

[3] *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, — 1984. — Pp. 175 –179.

[4] *Carter J.L., Wegman M.N.* Universal classes of hash functions // Journal of Computer and System Sciences — 1979. — Vol. 18, 143.

[5] *Diffie W., Hellman M.E.* New Directions in Cryptography // IEEE Transactions on Information Theory — 1976. — Vol. 22, 644.

[6] *Einstein A., Podolsky B., Rosen N.* Can quantum-mechanical description of physical reality be considered complete? // Phys. Rev. A — 1935. — Vol. 47, 777.

[7] *Helstrom C.W.* Quantum Detection and Estimation Theory // Academic Press, 1976.

[8] *Huttner B., Imoto N., Gisin N., Mor T.* Quantum cryptography with coherent states // Phys. Rev. A — 1995. — Vol. 51, 1863.

[9] *Renner R.* Security of Quantum Key Distribution // arXiv: quant-ph/0512258.

[10] *Rivest R.L., Shamir A., Adleman L.* A method for obtaining digital signature and public key cryptosystems // Commun. ACM — 1978. — Vol. 21, 120.

[11] *Scarani V., Acin A., Ribordy G., Gisin N.* Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations // Phys. Rev. Lett. — 2004. — Vol. 92, 057901.

[12] *Shannon C.E.* Mathematical Theory of Communication // Bell Syst. Tech. Jour., 1948.

[13] *Shor P.W.* Scheme for reducing decoherence in quantum computer memory // Phys. Rev. A — 1995. — Vol. 52, 2493.

[14] *Shor P.W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J.Sci.Statist.Comput. — 1997. — Vol. 26, 1484.

[15] *Shor P.W., Preskill J.* Simple proof of security of the BB84 quantum key distribution protocol // Phys. Rev. Lett. — 2000. — Vol. 85, 441.

[16] *Vernam G.S.* Cipher printing telegraph systems for secret wire and radio telegraphic communications // Journal of the IEEE — 1926. —Vol. 55, 109.

[17] *Галлагер Р.* Теория информации и надежная связь. — М.: Сов. Радио, 1974.

[18] *Молотков С.Н.* О коллективной атаке на ключ в квантовой криптографии на двух неортогональных состояниях // Письма в ЖЭТФ — 2004. — Т. 80, 639.

[19] *Молотков С.Н., Тимофеев А.В.* Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки $Q_c \approx 11\%$ // Письма в ЖЭТФ, 2007, Т. 85, С. 632 –637.

[20] *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация — М.: Мир, 2006.

[21] *Смарт Н.* Криптография — М.: Техносфера, 2006.

[22] *Холево А.С.* Введение в квантовую теорию информации. — М.: МЦНМО, 2002.

[23] *Холево А.С.* Квантовые системы, каналы, информация. — М.: МЦНМО, 2010.

[24] *Холево А.С.* Некоторые оценки для количества информации, передаваемого квантовым каналом связи // Проблемы передачи информации — 1973. — Т. 9 Вып.3, С. 3–11

[25] *Под ред. В.В.Ященко* Введение в криптографию. — М.: МЦНМО, 2000.