МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА
ФИЛИАЛ МГУ В ГОРОДЕ СЕВАСТОПОЛЕ

ФАКУЛЬТЕТ КОМПЬЮТЕРНОЙ МАТЕМАТИКИ

Направление подготовки:
01.03.02 «Прикладная математика и информатика»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

МОДЕЛИРОВАНИЕ ОПТИМАЛЬНОЙ АТАКИ НА ПРОТОКОЛ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ БЕННЕТА-БРАССАРА 84

Выполнила:
Шадрина Анастасия Владимировна
студентка учебной группы ПМ-401

Научный руководитель:
профессор, д.ф.-м.н.
Молотков Сергей Николаевич

Севастополь – 2018

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, УСЛОВНЫХ ОБОЗНАЧЕНИЙ

Алиса – сторона, передающая секретный ключ

Боб – сторона, принимающая секретный ключ от Алисы

Ева – потенциальный аналитик, злоумышленник с подслушивающим оборудованием

QKD – квантовое распределение ключа

BB84 – протокол Беннета и Брассара 1984 года

B92 – протокол Беннета 1992 года для двух состояний

Sarg04 – протокол предложенный Сакрани, Эйсеном, Рэйборди и Гизином в 2004 году

SSP – протокол с шестью состояниями

ВВЕДЕНИЕ

Важным аспектом в современном мире является безопасность. Безопасная передача информации - это главное требование любой организации или физического лица. Криптография представляет собой такой способ передачи данных от одной стороны к другой, где данные сначала шифруются с помощью некоторого ключа на стороне отправителя, а затем зашифрованные данные передаются на принимающую сторону и расшифровываются там с помощью ключа в соответствии с принятым между двумя сторонами протоколами. И чем лучше и эффективнее такой ключ, тем труднее перехватчику взломать передаваемые зашифрованные данные. Но если ключ расшифровки украден третьей стороной в ходе обмена, то может быть разрушен весь фундамент надежности передачи.

Квантовая криптография является методом защиты коммуникации, соединяющим в себе понятие квантовой механики с классической концепцией криптографии. Квантовые сети состоят из пространственно разнесенных узлов с помещенными в них управляемыми кубитами и квантовых коммуникационных каналов, соединяющих эти узлы. Обмен информацией внутри такой сети выполняется посредством пересылки кубитов по каналам. Для быстрой и надежной передачи данных на большие расстояния лучшими носителями кубитов служат фотоны.

В начале 20 века Вернер Гейзенберг сформулировал принципы, согласно которым при измерении одного параметра квантового объекта происходит воздействие на измеряемую систему, внося в нее непредсказуемые изменения. Можно измерять все параметры по отдельности, но важный момент заключается в том, что чем более точными являются показания одного параметра, тем меньше наблюдателю будет известно о другом. И наоборот. Это называется принципом неопределенности Гейзенберга, который лег в основу квантовой криптографии. В рамках исследуемой области это означает, что попытка подслушивания вносит нарушения в квантовую систему, а по уровню шума в канале легитимные пользователи могут распознать активность перехватчика.

Основу революционной концепции заложили Чарльз Беннет и Жиль Брассар в 1984 году [1][2], когда описали первый протокол для реализации квантового распределения ключа (Quantum key distribution). Позднее были предложены протоколы с использованием пары запутанных фотонов, а также расширенная версия протокола BB84 с использованием только двух квантовых состояний.

В последние годы в рамках международной конференции и проекта SECOQC, направленного на развитие квантовой криптографии, состоялась первая живая демонстрация безопасной передачи данных по действующей сети QKD [3].

Позднее, в 1992 году Чарльзом Беннетом на основе протокола BB84 был предложен новый протокол квантового распределения ключа, который обеспечивал дополнительный уровень безопасности [4]. Доказательство безопасности этого притокола было описано К.Тамаки в 2003 году [5]. Исчерпывающий алгоритм для последовательности действий был описан в статье журнала International Journal of Universal Computer Sciences [6].

Вскоре были описаны новые протоколы, позволяющие создать теоретически гораздо более совершенные алгоритмы для передачи данных - SSP [7], SARG04 [8], протокол Экерта [9], BBBSS [10].

Особое место в литературе занимает теорема Шеннона, которая является основополагающей для квантовых протоколов [11].

Но с течением времени обнаруживаются различные лазейки в концепции квантовой криптографии, что требует дальнейших исследований и надлежащих мер. Выполняются различные эффективные атаки по сетям QKD, классификация которых в исчерпывающем виде описана в отечественной литературе [12].

В статье профессора, доктора физико-математических наук, С.Н. Молоткова приведено теоретическое обоснование оптимальности атаки с коллективными измерениями на протол квантового распределения ключа BB84 [13].

Поскольку в наши дни квантовая криптография стремительно развивается, а исследования в этой области создания квантовых компьютеров

начались в 2007 году гигантами технической отрасли, то можно уверенно говорить о реальной возможности их создания. Но для достижения безусловной безопасности предстоит изучить еще множество аспектов. В данном случае актуальной проблемой является теоретическое изучение стратегий несанкционированного доступа и разработка мер защиты.

Таким образом, объект исследования определен как безопасность протокола квантового распределения ключей BB84. Предметом исследования в настоящей дипломной работе является анализ областей секретности протокола квантового распределения ключей BB84, в том числе предполагается теоретическое исследование различных стретегий перехватчика. Целью является разработка модели, направленной на реализацию выбранной стратегии атаки злоумышленника на рассматриваемый протокол.

Теореретическая значимость работы состоит в том, что в ней не только рассматриваются различные стратегии атак, но и разрабатывается подход существенно другого метода, а именно решается задача создания программного обеспечения с графическим интерфейсом, позволяющая пользователю моделировать атаку на протокол.

Практическая значимость определяется тем, что полученный результат может быть полезен при дальнейшем исследовании безопасности как протокола BB84, так и других протоколов квантового распределения ключей, что предоставляет теоретическую возможность их совершенствования.

1 ПОСТАНОВКА ЗАДАЧИ

Основной задачей настоящей дипломной работы является создание компьютерной программы, или приложения, моделирующей оптимальную атаку на протокол квантового распределения ключа BB84.

Разработанное приложение должно выполнять следующие требования:

1. Выполнение обмена между легитимными пользователями битовыми строками, сгенерированными случайным образом, до этапа получения секретного ключа с возможностью атаки во время выполнения алгоритма передачи.

2. Пользовательский интерфейс, который подразумевает наличие полей для ввода и/или редактирования данных (или инструмент для автоматической генерации данных), необходимые кнопки управления, а также поле, в котором содержится информация о событиях, происходящих во время работы программы.

3. Все поля и кнопки управления обладают интуитивно понятным пользователю интерфейсом.

4. Исходный код программы носит открытый характер и возможно внесение изменений и дополнений, расширяющих функционал.

Таким образом, на выходе имеется пользовательское приложение, моделирующее атаку на протокол квантового распределения ключа BB84.

2 ОБЗОР СУЩЕСТВУЮЩИХ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В традиционной криптографии с открытым ключом для обеспечения секретности сообщений между двумя пользователями используется односторонняя функция с потайным входом (функция, которую легко вычислить в одном направлении, но трудно вычислить в противоположном (найти ее обратную) без специальной информации, называемой «потайным входом»), несмотря на отсутствие какой-либо первоначальной общей секретной информации между двумя пользователями. В квантовой криптографии широко распространены публичные ключи, квантовый канал не используется для того, чтобы напрямую отправлять сообщения, а скорее служит для передачи случайных битов между пользователями, что позволит с большой вероятностью обнаружить в канале подслушивающее устройство, если в ходе обмена этими битами будут нарушения. Если передача не была нарушена, они соглашаются использовать эти общие секретные биты известным им способом в качестве одноразовой площадки для сокрытия смысла последующих значимых сообщений, требующих гарантии отсутствия утечки информации. Если передача была нарушена, они отбрасывают ее и пытаются снова, пока им не удастся передать достаточное количество случайных битов через квантовый канал. Здесь играет роль параметр для квантового протокола Q_c, который называется критическая ошибка - величина, до которой будет гарантироваться секретность распределения ключей.

В общих чертах, ключевыми компонентами сети QKD являются квантовый канал, классический канал связи, а также отправитель и приемник, которые оснащены соответствующим детектором и устройствами.

В 1984 году Чарльз Беннетт и Жиль Брассар опубликовали первый протокол квантового распределения ключа. Он был основан на принципе неопределенности Гейзенберга и был известен как протокол BB84, название образовано как первые буквы фамилий авторов и год, в ко-

тором он был опубликован. Это по-прежнему один из самых известных протоколов, и можно утверждать, что все другие протоколы, основанные на принципе неопределенности Гейзенберга, по существу являются вариантами идеи BB84. Основная идея для всех этих протоколов заключается в том, что Алиса может передать случайный секретный ключ Бобу, отправив строку фотонов, где биты секретного ключа кодируются в поляризации фотонов. Принцип неопределенности Гейзенберга может быть использован, чтобы гарантировать, что злоумышленник не может измерить эти фотоны и передать их Бобу, не нарушая состояние фотона обнаруживаемым способом, раскрывая таким образом наличие подслушивающего устройства.

2.1 ПРОТОКОЛ BB84

Рассмотрим более подробно протокол BB84. Здесь используются два базиса - прямолинейный (+) и диагональный (×). В прямолинейном базисе двумя возможными поляризациями являются 0° и 90°, то есть горизонтальная и вертикальная, которые являются 0 и 1 бит соответственно. Аналогично, в диагональном базисе две поляризации - 45° и 135°, 0 и 1 бит соответственно. Наглядное представление битовых значений показано ниже:

Таблица 1: Поляризация базисов

Поляризация	**Значение бита**	
	0	1
Прямолинейный базис	0°, →	90°, ↑
Диагональный базис	45°, ↗	135°, ↖

Отправитель (будем его условно называть «Алиса») случайным образом выбирает битовую строку и последовательность поляризаций (прямолинейную или диагональную). Затем он отправляет другому пользователю («Боб») последовательность фотонов, каждый из которых представляет один бит, в горизонтальной или 45-градусной поляризации, если

значение бита равно нулю, и вертикальной или 135-градусной поляризации для значения, равного единице. По мере того, как Боб получает фотоны, для каждого из них случайным и независимым от Алисы образом он выбирает поляризацию, в которой будет измерять - прямолинейную или диагональную, и интерпретирует результат как двоичный ноль или единицу. Если фотон, отправленный, например, в прямоугольной поляризации, Боб измерит в диагональной, то получит случайный ответ, а информация будет потеряна. Таким образом, получатель, приняв все фотоны, имеет некоторую строку, состоящую из случайных битов, но значимые данные представляет только та часть, где правильно был угадан базис поляризации. Но в реальности ситуация еще может усугубляться тем, что часть фотонов может быть потеряна при передаче или неверно интерпретирована неэффективными детекторами на приемной стороне.

Последующий обмен информацией осуществляется по классическому каналу связи, который можно подслушать, но невозможно внести изменения или полностью подменять сообщения. Боб и Алиса сначала определяют путем публичного обмена сообщениями, какие фотоны были успешно получены и для каких из них был выбран верный базис, сохраняя в секрете результаты измерений. Если квантовая передача не нарушена, Алиса и Боб в итоге получают секретный ключ. Другими словами, каждый из этих фотонов предположительно несет один бит случайной информации (например, был ли прямолинейный фотон вертикальным или горизонтальным), известный только Алисе и Бобу.

Из-за случайного смешения прямолинейных и диагональных фотонов в квантовой передаче любое подслушивание влечет риск изменения информации таким образом, что возникают разногласия между Бобом и Алисой по некоторым битам, на которые, по их мнению, они должны согласиться. Поэтому они могут проверить канал на возможное прослушивание, публично сравнив некоторые из бит, которые, по их мнению, должны были совпасть, хотя, конечно, это приносит в жертву секретность этих бит. Битовые позиции, используемые в этом сравнении, должны быть случайным подмножеством правильно полученных битов, так

что при прослушивании большого количества фотонов вряд ли удастся избежать обнаружения. Если в ходе сравнения все позиции совпали, Алиса и Боб могут заключить, что квантовая передача была свободна от значительного подслушивания, а оставшиеся биты, которые были отправлены и получены в этом сеансе, могут быть безопасно использованы для последующей безопасной связи по общественному каналу. Следующий пример иллюстрирует работу протокола:

Таблица 2: Пример

КВАНТОВАЯ ПЕРЕДАЧА ДАННЫХ																
Случайные биты Алисы	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1	0
Поляризация Алисы	×	+	×	+	+	+	+	+	×	×	+	×	×	×	+	+
Отправленные фотоны	↗	↑	↖	→	↑	↑	→	→	↖	↗	↑	↖	↗	↗	↑	→
Поляризация Боба	+	×	×	+	+	×	×	+	×	+	×	×	×	×	+	+
Полученные фотоны	1		1		1	0	0	0		1	1	1		0	1	0
КЛАССИЧЕСКИЙ КАНАЛ СВЯЗИ																
Боб открывает свои базисы	+		×		+	×	×	+		+	×	×		×	+	+
Согласование базисов с Алисой			OK		OK			OK				OK		OK	OK	OK
Полученная информация			1		1			0				1		0	1	0
Согласование части ключа					1									0		
Корректность					OK									OK		
ИТОГ																
Секретный ключ			1					0				1			1	0

2.2 ПРОТОКОЛ B92

В 1992 году Беннетт предлагает протокол для квантового распределения ключа, основанный на двух неортогональных состояниях и известный под названием B92, или протокол двух состояний [4]. Он аналогичен протоколу BB84, но использует только два состояния вместо четырех. Протокол B92 также основан на принципе неопределенности Гейзенберга. Протокол B92 доказал свою безусловную безопасность. Замечатель-

ным доказательством безусловной безопасности B92 является доказательство К.Тамаки [5]. Это доказательство гарантировало безопасность B92 в присутствии любого врага, который может выполнить любую операцию,допускаемую квантовой физикой.

Использование квантового канала, который Ева не может контролировать без обнаружения, позволяет создать секретный ключ с безусловной безопасностью, основанной на законах квантовой физики. Присутствие злоумышленника проявляется для пользователей таких каналов через необычно высокую частоту ошибок. B92 – это протокол квантового распределения ключей, который использует поляризованные фотоны в качестве носителей информации. Онпредполагает, что два законных пользователя, Алиса и Боб, общаются по двум определенным каналам, к которым враг также имеет доступ:

- Классический канал, который может быть публичным; Ева может слушать без обнаружения;
- Квантовый канал, который (по своей природе) Ева не может слушать пассивно.

Первая фаза B92 включает в себя передачи по квантовому каналу, в то время как вторая фаза происходит по классическому каналу. Кодирование данных происходит согласно 1.

При выполнении протокола B92 выполняются следующие шаги[6]:

1. Квантовая передача данных

   1.1. Алиса случаным образом выбирает вектор бит A, состоящий из 0 и 1, длины n. Если некоторое состояние в векторе является нулевым, то она посылает Бобу состояние $|\uparrow\rangle$, а если значение равно единице, то она отправляет $|\nearrow\rangle$.

   1.2. Боб в свою очередь также генерирует двоичную вектор-строку B длины n. Если позиция в строке равна нулю, то Боб выбирает +-базис, в случае, если значение единичное, Боб получает $\times$-базис.

1.3. Боб измеряет соответственно каждое состояние, посланное ему Алисой($|\uparrow\rangle$ или $|\nearrow\rangle$) в выбранном базисе($+$ или $\times$).

1.4. Боб имеет вектор T длины n, полученный по следующим правилам: если измеренное Бобом состояние является $|\uparrow\rangle$ или $|\nearrow\rangle$, то значение в данной позиции вектора равно нулю, иначе оно принимает значение, равное единице.

2. Классический канал связи

2.1. По общедоступному каналу связи Боб отправляет Алисе свой вектор B.

2.2. Алиса и Боб сохраняют биты векторов A и B для $T_i = 1$. В случае, если Ева отсутствует, мы имеем $A_i = 1 - B_i$ и общий ключ формируется как A_i.

2.3. Алиса выбирает некоторые i-позиции ключа и раскрывает их Бобу. Если значение Боба в этой позиции не соответствует A_i, то считается, что в канале детектирована Ева, и сеанс считается оконченным.

2.4. Общий ключ K длины N (n $<$ N) формируется из сырого ключа путем исключения из него элементов из шага 2.3.

В Таб. 3 показано, как работает протокол B92.

Таблица 3: Пример работы протокола B92

Шаги алгоритма	1	2	3	4	5	6	7	8	9	10
1.1	1	0	1	1	0	0	1	0	1	1
	$\nearrow$	$\uparrow$	$\nearrow$	$\nearrow$	$\uparrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\nearrow$
1.2	1	0	0	1	1	0	1	0	1	1
	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$\times$
1.3	$\nearrow$	$\uparrow$	$\rightarrow$	$\nearrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\uparrow$	$\nearrow$	$\nearrow$
1.4	0	0	1	0	1	0	0	0	0	0
2.2	0	0	1	0	1	0	0	0	0	0
2.3	0			0			0			
	OK			OK			OK			
2.4			1			0			0	0

Здесь важно отметить 3 момента. Во-первых, если значение полученного Бобом вектора оказалось равным нулю при измерении, то Боб еще не знает, что ему прислала Алиса. Таким образом, если Боб выбирает базис +(соответственно, ×), он может получить в результате своего измерения $|\uparrow\rangle$ (соответственно, $|\nearrow\rangle$) для любого квантового состояния, отправленного Алисой ($|\uparrow\rangle$ или $|\nearrow\rangle$).

Во-вторых, если значение полученного Бобом вектора оказалось равным единице, то Боб точно знает, что прислала ему Алиса, например, если Боб выбирает базис × (соответственно, +), он получит после измерения состояние $|\nwarrow\rangle$ (соответственно, $|\rightarrow\rangle$) и Алиса точно послала ему $|\uparrow\rangle$ (соответственно, $|\nearrow\rangle$).

В-третьих, в шаге 2.2 Алиса и Боб проверяют наличие Евы; идея состоит в том, что если для i-го значения $T_i = 1$, то $A_i = 1 - B_i$, иначе выдвигается предположение о том, что либо в квантовом канале есть шум, либо ошибки вызваны присутствием в канале злоумышленника.

2.3 ПРОЧИЕ ПРОТОКОЛЫ, ОСНОВАННЫЕ НА НЕОПРЕДЕЛЕННОСТИ ГЕЙЗЕНБЕРГА

Другой вариант BB84 – это протокол с шестью состояниями (Six-State Protocol, SSP), предложенный Паскуинуччи и Гизином в 1999 году [7]. SSP идентичен BB84 за исключением того, что, как следует из его названия, вместо использования двух или четырех состояний SSP использует шесть состояний на трех ортогональных базисах, с помощью которых кодируются отправленные биты. Это означает, что злоумышленнику придется угадать один из 3 возможных базисов. Это означает, что подслушиватель с большей вероятностью допустит ошибку, что приведет к его раскрытию. Брюс и Миккьявелло доказали в 2002 году, что такие многомерные системы обеспечивают повышенную безопасность [14].

В то время как есть ряд других вариантов протокола BB84, одним из последних был предложен в 2004 году Сакрани, Эйсен, Рэйборди и Гизином [8]. В SARG04 протоколе первый этап такой же, как и в BB84. На втором этапе, когда Алиса и Боб определяют, для каких битов их базисы

совпадают, Алиса напрямую не объявляет свои базисы, а объявляет пару неортогональных состояний, одно из которых она использовала для кодирования своего бита. Если Боб верно выбрал базис для измерения, то он будет измерять полученное состояние. Если он выбрал неправильно, он не измеряет состояние, посланное ему Алисой, и не сможет определить бит. Этот протокол имеет особое преимущество при использовании в практическом оборудовании.

2.4 ПРОТОКОЛ ЭКЕРТА

Артур Экерт внес свой вклад в новый подход к распределению квантовых ключей, где ключ распределяется с помощью квантовой телепортации [9]. Этот раздел описывает протокол и его применение к протоколам на основе принципа неопределенности Гейзенберга, описанных ранее.

Экерт описывает канал, где есть один источник, который испускает пары запутанных частиц, которые могут быть поляризованными фотонами [9]. Частицы разделены, и Алиса и Боб получают по одной частице от каждой пары, как показано на рис. 1.

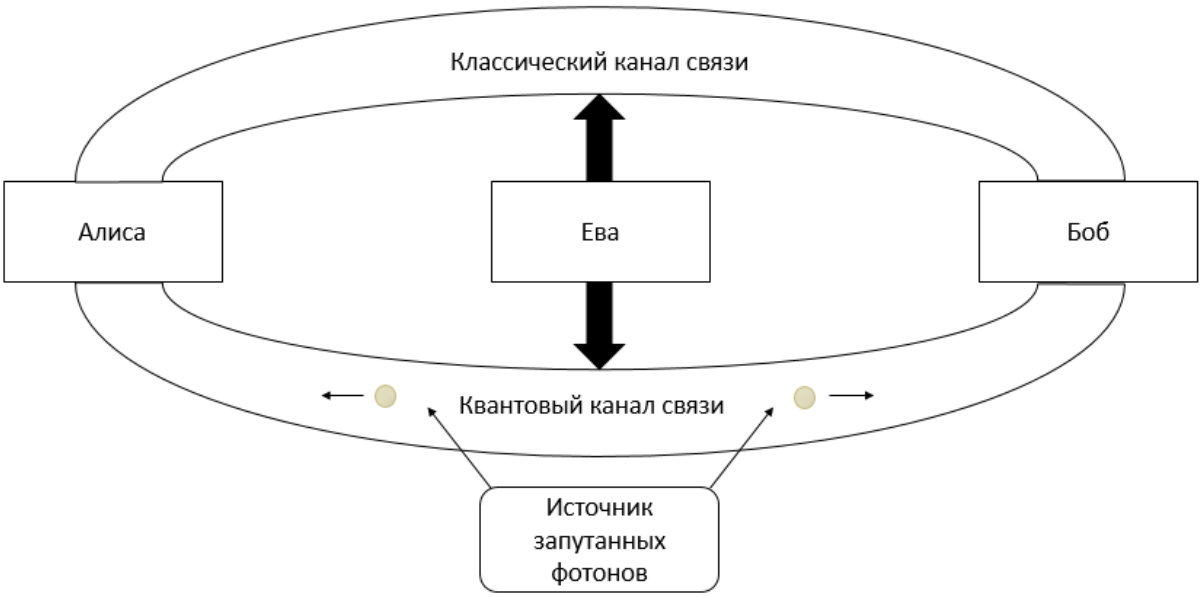

Рис. 1: Иллюстрация к протоколу Экерта

По [15],Алиса и Боб будут выбирать случайные базы для измерения полученных частиц. Как и в BB84, они обсудят в общедоступном канале

связи, какие базисы они использовали для своих измерений. Для каждого измерения, где Алиса и Боб использовали одни и те же основания, они должны ожидать противоположных результатов из-за принципа квантовой запутанности. Это означает, что если Алиса и Боб интерпретируют свои измерения как биты, как и раньше, то каждый из них будет иметь битовую строку, которая является двоичным дополнением битовой строки другого. Любая из сторон может перевернуть свою окончательную битовую строку, и они, таким образом, получают секретный ключ.

Наличие подслушивающего устройства можно обнаружить изучив фотоны, для которых Алиса и Боб выбрали разные базы для измерения. Алиса и Боб могут измерить эти фотоны в третьем базисе и обсудить их результаты. С этой информацией они могут проверить неравенство Белла [16]. Если неравенство сохраняется, это будет означать, что фотоны не были действительно запутаны и, таким образом, может присутствовать подслушивающий.

Важно отметить сходство между протоколом Экерта и BB84. Если Алиса была источником, и Алиса и Боб не выполняли проверку запутанности Экерта, то по существу реализован протокол BB84. Беннет и Брассар [17] отметили, что любой вариант BB84 может быть адаптирован для использования запутанного источника фотонов вместо источника Алисы. В частности, в 2002 году [18] была описана запутанная версия протокола SSP с дополнительной безопасностью. Была также проделана работа, которая показывает, что протокол SARG04 может допускать меньше ошибок с двухфотонным источником (запутанным), чем с однофотонным источником (Алиса) [19].

В этом разделе описан подход к квантовому распределению ключей, который использовал принцип квантовой запутанности. Артур Экерт был первым, кто предложил эту идею в своем документе 1991 года, но Беннетт и Брассар указали, что его идеи могут быть включены в протокол BB84. В ряде их последующих работ исследовалось использование квантовых запутанных фотонов в вариантах протоколов BB84.

2.5 ВЫВОД

Две стороны, имеющие доступ к небезопасному квантовому и классическому каналам, могут надежно установить секретный ключ, не делая никаких предположений о возможностях подслушивающего устройства, которое может присутствовать. Это связано с тем, что принципы квантовой механики гарантируют, что ни одно подслушивающее устройство не может успешно измерить квантовое состояние, не внося помех в канал связи. В этом разделе был дан краткий обзор наиболее известных протоколов квантового распределения ключей, представленных в литературе. К ним относятся протокол BB84 и его варианты, безопасность которых следует из принципа неопределенности Гейзенберга, а также подход Экерта с использованием квантовой запутанности.

3 ВТОРИЧНАЯ ОБРАБОТКА КЛЮЧА

3.1 АЛГОРИТМ КОНТРОЛЯ И КОРРЕКЦИИ ОШИБОК

По завершению этапа, в котором Алиса и Боб просеяли ключ, необходимо избавиться от различий в данных, которые возникли при пересылке, проще говоря, исправить ошибки. Для этого легитимные пользователи открыто обмениваются сообщениями по классическому каналу связи, но данное действие должно раскрывать минимальное количество информации, если в канале присутствует злоумышленник. Поставленная задача аналогична проблеме передачи информации через канал с шумом, который вносит шум в последовательность передаваемых битов, создавая тем самым иную последовательность. Для определения верхнего предела уровня ошибок, при котором еще возможно квантовое распределение ключа, воспользуемся теоремой Шеннона [11].

Согласно этой теореме, минимально необходимое количество битов r для исправления данных на приемной стороне при постоянной Q (вероятность ошибки), задано выражением

$$r = N(-Q\log_2 Q - (1-Q)\log_2(1-Q)), \tag{5.1}$$

где в качестве параметра N выступает длина просеянного ключа. Из этого соотношения возможно найти допустимый уровень ошибок, если учитывать тот факт, что в вышеописанном протоколе при одном измерении Ева может получить не более, чем $\frac{1}{2}$ информации о бите, поскольку это обусловлено исключительно случайным распределением базисов пересылаемых битов. Отсюда по закону аддитивности информации следует, что оставшаяся $\frac{1}{2}$ информации находится у Алисы и Боба, при раскрытии которой у них не останется битов для формирования ключа. Подставим эту предельную величину в соотношение (1):

$$1/2 = -Q_c\log_2 Q_c - (1-Q_c)\log_2(1-Q_c) \tag{5.2}$$

Вычисляя это выражение, получим $Q_c \approx 11\%$. Это говорит о том, что при $Q < Q_c$ еще возможно извлечение секретного ключа, а при $Q = Q_c$

его получить не удастся, так как формально длина ключа обратится в нуль. Но как было показано в работе [2], при проведении индивидуальных измерений во время атаки, предельное значение возрастает до 15%, которое больше $Q_c = 11\%$, что отражает не самый оптимальный характер действий злоумышленника. Поэтому в дальнейшем стратегия злоумышленника будет рассматриваться с позиции коллективных измерений, что обеспечит достижения минимального уровня ошибки в 11%.

3.2 КАСКАДНЫЙ ПРОТОКОЛ ИСПРАВЛЕНИЯ ОШИБОК БРАССАРА И СЭЛВЕЙЛА

Каскадный протокол исправления ошибок был впервые предложен Жилем Брассаром и Луи Салвейлом [20]. Он представляет собой уточнение немного более раннего протокола, известного как BBBSS [10], созданного в 1991 году.

Выполнение алгоритма протокола BBBSS происходит после квантовой передачи, просеивания ключа и оценки ошибок. Первый шаг, заключающийся в том, чтобы договориться о случайной перестановке, происходит публично, по классическому каналу. Алиса и Боб выполняют эту перестановку на своих соответствующих просеянных битах, чтобы попытаться равномерно распределить любые ошибки. Затем Алиса и Боб делят свой просеянный ключ на блоки размера k, где k определяется таким образом, что каждый блок, вероятно, будет иметь не более одной ошибки, на основе частоты ошибок, полученной при оценке. Авторы каскадного протокола эмпирически определили, что идеальный размер блока будет приблизительно равен $\frac{0.73}{p}$, где p представляет собой расчетную частоту ошибок. После этого шага для каждого блока рассчитывается бит четности и согласовывается по общедоступному каналу. Если у Алисы и Боба значения совпали, то они предполагают, что в этом блоке нет ошибок, и они двигаются дальше. С другой стороны, если четность блока не согласуется между Алисой и Бобом, то они выполняют двоичный поиск по этому блоку, чтобы определить ошибку одного бита, которую они затем исправляют.

Таким образом, максимум $1 + \lfloor \log_2 k \rfloor$ битов четности заменятся для каждого блока с ошибкой и на 1 бит четности изменится значение для блоков без ошибок. Для того, чтобы выявить эти просочившиеся биты по публичному каналу и минимизировать информацию, которую любым возможным способом может заполучить Ева, отбрасывается последний бит каждого блока и подблоков, для которых был изменен бит четности.

После того, как этот процесс завершен, а Алиса и Боб находятся в согласии с четностью для всех своих блоков, они могут быть уверены, что каждый блок либо не будет иметь ошибок вовсе, либо будет иметь четное их количество. Это связано с тем, что одна проверка не может определить четное количество ошибок в блоке. Поэтому Алиса и Боб должны снова переставить свой новый ключ до повторения вышеописанных действий. Кроме того, после каждого прохода размер блока увеличивается с учетом того, что остается меньше ошибок. Когда Алиса и Боб уверены, что все ошибки были исправлены, они применяют новый подход для исправления ошибок. Причина этого состоит в том, что утечка информации при проверке четности слишком велика, когда процент ошибок мал, так как большинство блоков не будет содержать ошибок и четность этих блоков будет совпадать. Новая стратегия состоит в случайном выборе подмножества битов из исправленной ключевой строки для формирования нового блока для сравнения четности и выполнения той же процедуры двоичного поиска, если биты четности окажутся не согласованы.

Таким образом, Алиса и Боб не отбросят столько битов четности, как если бы они должны были выполнить полный проход, как описано ранее, хотя они все еще отбрасывают последний бит от каждого блока и подблока, для которого был изменен бит четности. В какой-то момент Алиса и Боб обнаружат, что все их сравнения четности согласуются. Когда это происходит для нескольких проходов, Алиса и Боб заключают, что их согласованные ключи идентичны, и они переходят к усилению секретности.

Различия между BBBSS и каскадным протоколом исправления ошибок минимальны, но значительны. Как и в BBBSS, в каскаде первый

проход выполнен путем разделения просеянного ключа в блоки длины k, основанной на частоте повторения ошибок, и происходит смена битов четности для каждого блока. Двоичный поиск выполняется для того, чтобы определить ошибки одного бита на блоках, которые не имеют согласованности. Однако в отличие от BBBSS, бит не отбрасывается во время первого прохода. Вместо этого исправляются ошибки блока, применяется перестановка, размер блока увеличивается до $2k$ и выполняется другой проход, идентичный первому. Именно в этот момент каскадный протокол больше всего отклоняется от BBBSS. На каждую ошибку, исправленную на втором проходе, должна быть по крайней мере одна ошибка, которая находилась в том же блоке на предыдущем проходе, так как ни одна ошибка не была найдена или исправлена в тот раз. По этой причине для каждого исправления, сделанного в любом проходе после первого, двоичный поиск перезапускается на блоке, содержащем этот исправленный бит во всех предыдущих проходах, чтобы определить любые потенциальные ошибки. Каждый раз, когда выявляется новая ошибка, она раскрывает потенциальные ошибки в предыдущем проходе, поэтому процесс повторяется, а обнаружение и исправление ошибок выполняется рекурсивно для всех предыдущих проходов. Этот процесс проиллюстрирован ниже.

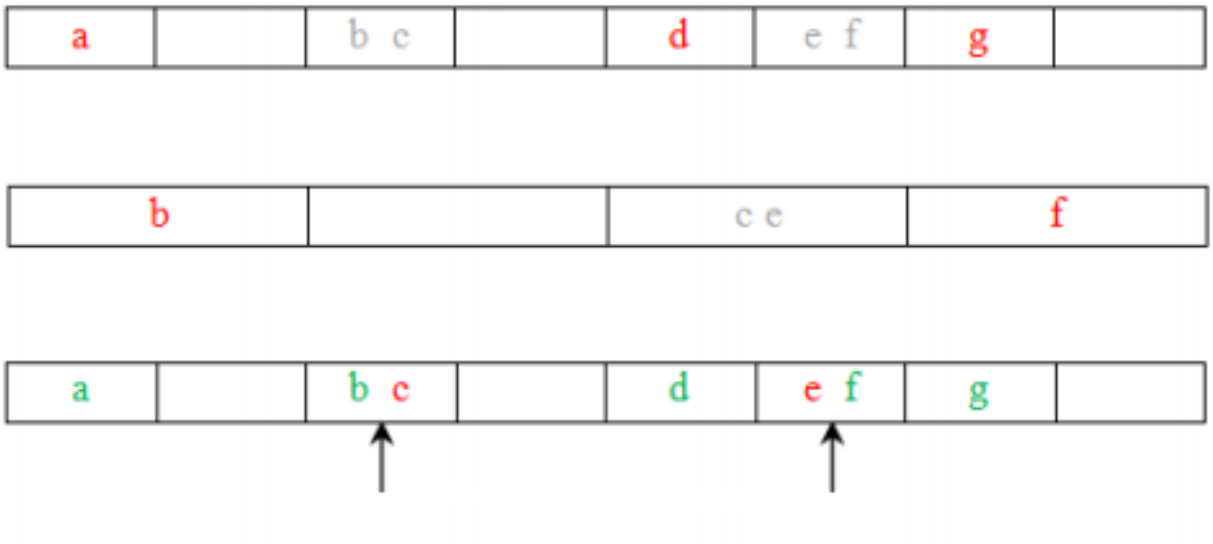

Рис. 2: Коррекция ошибок

1. Красные буквы обозначают выявленные и исправленные ошибки

(a, d, g). Ошибки b, c, e, f пока не были обнаружены.

2. Красные буквы обозначают выявленные ошибки (b, f). Ошибки c, e пока не были обнаружены.

3. Для каждой выявленной ошибки возвращаемся к блокам первого прохода и определяем соответствующие ошибки. Так как ошибки b и f были выявлены во втором проходе, ошибки c и e теперь идентифицируются при повторном поиске.

В каждом проходе после первого для каждого обнаруженного бита будут исправлены в среднем две ошибки, поэтому количество ошибок, присутствующих в согласованном ключе, уменьшается экспоненциально для каждого прохода. Эмпирическим путем было установлено, что четыре прохода, как правило, считается достаточным для исправления всех ошибок.

В каскадном протоколе максимальное количество уязвимых битов равно $B + n \cdot \lceil \log_2 k \rceil$ за проход, где B - количество блоков, n - количество ошибок, выявленных в ходе согласования, а k - размер блока для данного прохода. На самом деле, для каждого бинарного поиска происходит утечка битов в зависимости от местоположения ошибки в блоке.

3.3 УСИЛЕНИЕ СЕКРЕТНОСТИ

Последним этапом в исправлении ошибок в передаваемом ключе является усиление секретности. Цель этого шага состоит в том, чтобы учесть любую информацию, полученную во время фазы согласования ошибок, и гарантировать, что любые присутствующие подслушивающие устройства не получат достаточной информации, чтобы восстановить значительную часть ключа.

Усиление секретности – это искусство выделения очень секретной информации для использования, например, в качестве криптографического ключа, из большего объема общей информации, которая является лишь частично секретной.

Пусть Алиса и Боб будут имеют случайную величину W в виде случайной битовой строки длины n, в то время как подслушивающая Ева обладает информацией, заключенной в V - это битовая строка длины t, причем $t < n$ бит информации о W, т. е. $H(W|V) \geq n - t$. Подробные сведения о распределении P_{VW}, как правило, неизвестны для Алисы и Боба, за исключением того, что оно выполняет ограничение. Они могут как знать, так и не знать значение P_W. Алиса и Боб публично выбрают функцию сжатия $g : \{0.1\}^n \to \{0,1\}^r$ так, что частичная информация Евы о W и ее полная информация о g дают ей незначительную информацию о $K = g(W)$, за исключением малейшей вероятности. Полученное K практически равномерно распределяется с учетом всей доступной Еве информации, следовательно, его можно безопасно использовать в качестве криптографического ключа.

Длина r секретного ключа, который Алиса и Боб могут получить, зависит от вида, а также от количества информации, доступной Еве. Предполагая, что W - это случайная битовая строка длины n, рассмотрим возможные сценарии, в которых Ева получает информацию:

1. t произвольных бит из W;
2. t произвольных проверок W на четность;
3. результат преобразования произвольной функции из n-битовой строки в t-битовую строку;
4. строку W, передаваемую через бинарный симметричный канал с вероятностью ошибки ε, удовлетворяющей $h(\varepsilon) = 1 - \frac{t}{n}$, где $h(\cdot)$ обозначает функцию двоичной энтропии.

Опишем решение для общего сценария, включающего все вышеперечисленные случаи. В этом сценарии Еве разрешено указывать произвольное распределение P_{VW} (неизвестное Алисе и Бобу) при условии, что накладывается единственное ограничение $R(W|V = v) \geq n - t$, где $R(W|V = v)$ обозначает условную энтропию Реньи для W с учетом $V = v$. Для любого $s < n - t$ Алиса и Боб могут выделить $r = n - t - s$

битов секретного ключа $K = G(W)$ пока информация Евы о K незначительна, публично выбирая функцию сжатия G (которая теперь является случайной величиной) случайным образом из соответствующего класса $\{0,1\}^{n-t-s}$.

3.3.1 УНИВЕРСАЛЬНОЕ ХЭШИРОВАНИЕ И ЭНТРОПИЯ РЕНЬИ

Для усиления секретности принято использовать универсальное хэширование, эта концепция была введена Картером и Вегманом [21]. Класс функций $\mathcal{G} : \mathcal{A} \to \mathcal{B}$ называется универсальным, если для некоторых x_1, x_2 из $\mathcal{A}$ вероятность того, что $g(x_1) = g(x_2)$ составляет не более, чем $\frac{1}{|\mathcal{B}|}$, где g выбрано случайным образом из $\mathcal{G}$.

Когда $\mathcal{A} = \mathcal{B}$, то класс состоит из тождественных функций и называется универсальным. В любом случае, класс всех функций от $\mathcal{A}$ до $\mathcal{B}$ будет универсальным, но это не используется ввиду того, что функций будет слишком много. Наиболее универсальным классом является класс линейных функций такой, что $\{0,1\}^n \to \{0,1\}^r$.

[22] Пусть X - случайная переменная из $\mathcal{X}$ с распределением P_X. Вероятность столкновения (*collision probability*) $P_c(X)$ определяется как вероятность того, что X примет одинаковое значение дважды в двух независимых экспериментах:

$$P_c(X) = \sum_{x \in \mathcal{X}} P_X(x)^2. \tag{5.2}$$

Энтропия Реньи определяется как отрицательный логарифм от вероятности столкновения:

$$R(X) = -\log_2 P_c(X) \tag{5.3}$$

Для события ε вероятность столкновения и энтропия Реньи при условии, что выполнилось X, определяются, соответственно, как $P_c(X|\varepsilon)$ и $R(X|\varepsilon)$, то есть учитывается условное распределение $P_{X|\varepsilon}$.

Энтропия Реньи, обусловленная случайной величиной $R(X|Y)$ это математическое ожидание данной величины:

$$R(X|Y) = \sum_y P_Y(y) R(X|Y = y). \tag{5.4}$$

Энтропия Реньи, как и энтропия Шеннона, всегда положительна и может быть выражена как

$$R(X) = -\log 2E[P_X(X)] \tag{5.5},$$

где $E[\cdot]$ означает ожидаемое значение. Энтропия Шеннона может быть записана как

$$H(X) = -E[\log_2 P_X(X)]. \tag{5.6}$$

Для любого дискретного распределения вероятности $P_X : R(X) \leq H(X)$, причем равенство достигается тогда и только тогда, когда P_X имеет равномерное распределение по $\mathcal{X}$ или подмножеству $\mathcal{X}$. Более того, для каждого распределения P_{XY} выполняется

$$R(X|Y) \leq H(X|Y). \tag{5.7}$$

На первый взгляд кажется возможным провести аналогию между энтропией Реньи и Шеннона, другими словами, определить взаимную информацию Реньи между X и Y как $I_R(X;Y) = R(X) - R(X|Y)$. Однако в общем случае выражения $R(X) - R(X|Y)$ и $R(Y) - R(Y|X)$ различны, более того значение $R(X) - R(X|Y)$ может быть отрицательным.

Алиса и Боб имеют случайную n-битовую строку W и Ева получает строку V, когда W передается через бинарный симметричный канал связи с вероятностью ошибки ε. Тогда имеем

$$P_{W|V=v}(w) = (1-\varepsilon)^{n-d(v,w)}\varepsilon^{d(v,w)}, \tag{5.8}$$

где $d(w,v)$ - расстояние Хэмминга между v и w. Поскольку энтропия Реньи, как и энтропия Шеннона, аддитивна для независимых случайных величин, следует, что

$$H(W|V=v) = nh(\varepsilon) = -n(\varepsilon\log_2\varepsilon + (1-\varepsilon)\log_2(1-\varepsilon)) \tag{5.9}$$

и

$$R(W|V=v) = -n\log_2((1-\varepsilon)^2 + \varepsilon^2) \tag{5.10}$$

для всех v.

[22] Пусть W - случайная n-битновая строка с равномерным распределением над $\{0,1\}^n$, и пусть $V = e(W)$ для любой функции подслушивания $e : \{0,1\}^n \to \{0,1\}^t$ для некоторого $t < n$. Пусть $s < n - t$ - положительный параметр безопасности, и пусть $r = n - t - s$. Если Алиса и Боб выбирают $K = G(W)$ в качестве своего секретного ключа, где G выбирается случайным образом из универсального класса хэш-функций от $\{0,1\}^n$ до $\{0,1\}^r$, тогда ожидаемая информация Евы о секретном ключе K с учетом G, V выражается как

$$I(K; GV) \leq \frac{2^{-s}}{\ln 2}. \tag{5.11}$$

Этот результат указан как среднее по значениям V. Также важным замечанием будет, что стратегия Алисы и Боба не зависит от e и, следовательно, усиление конфиденциальности работает, даже если у них нет информации о e, если они знают верхнюю границу t. Доказательство приведено в [22].

Подводя итог, перечислим основные шаги в ходе выполнения этапа усиления секретности [22]:

1. Согласованный ключ x является случайной N-битовой строкой с равномерным распределением по бинарному алфавиту $\{0,1\}^n$.

2. $V = e(x)$ является случайной функцией злоумышленника, причем $e : \{0,1\}^n \to \{0,1\}^t$, где $t < n$.

3. Вероятность ошибки рассчитывается по формуле $\Omega(e) = e \log 1/e + \overline{e} \log 1/\overline{e}$, где $\overline{e} = 1 - e$ для вычисления t в рамках частоты ошибок e.

4. Пропускная способность канала определяется как $I_{max}(x, y) = 1 - \Omega(e)$.

5. V - это случайная t-битовая строка, полученная Евой.

6. Параметр s является положительной величиной и определяет параметр безопасности, удовлетворяющий $s < n - t$ и $N \geq s > 0$, который используется для минимазиции количества битов, которые будут получены Евой.

7. $K = g(x)$ - случайный произвольный ключ, выбранный Алисой и Бобом, который станет секретным ключом из универсального класса хэш-функций: $g : \{0,1\}^n \to \{0,1\}^r$.

8. Секретный ключ K является строкой длины R, который был создан Алисой и Бобом, где $r \leq n$ и вычисляется по формуле $r = n - t - s$.

9. Секретный ключ K - это r-битовая строка, сгенерированная Алисой и Бобом, где $0 \leq r \leq n$.

10. Ожидаемая информаця Евы о секретном ключе K с учетом G, V выражается как $I(K; GV) \leq \frac{2^{-s}}{\ln 2}$.

11. Мера информации I(K;GV) определена как среднее по значениям V.

12. Тактика Алисы и Боба не рассчитывается для e, поскольку модель усиления конфиденциальности работает, когда Алиса и Боб не имеют никакой информации о e, но учитывается, что есть верхняя граница t битов, которые заполучила Ева.

Таким образом, Алиса и Боб могут иметь секретный ключ, который используется в гибридных методах шифрования для использования в качестве криптографического ключа во время обмена сообщениями. Таким

образом, использование усиления конфиденциальности путем публичного обсуждения позволяет легитимным пользователям отбирать секретный ключ, о котором Ева имеет ничтожно малую информацию.

После согласования ошибок и усиления секретности Алиса и Боб могут быть уверены, что у них одинаковая версия ключа и что общее количество битов, которые могла заполучить Ева, было сведено к минимуму. В качестве одной из последних мер безопасности Алиса и Боб обсуждают по классическому каналу выбор случайной хэш-функции. Эта хэш-функция, которая еще сильнее уменьшает размер конечного ключа, затем применяется к согласованному ключу.

Следовательно, даже если Ева обладает очень эффективным подслушивающим устройством и имеет существенную часть ключа, выполнение этого действия увеличивает любые ошибки в полученной Евой информации, так как небольшие изменения во входе хорошей хэш-функции приводят к большим изменениям на выходе. Поэтому, даже если бы у Евы было всего несколько ошибок в ее версии ключа, после усиления конфиденциальности ее ошибки возрастают до предела.

4 ОПИСАНИЕ АТАК НА ПРОТОКОЛ BB84

Хотя сети QKD с теоретической точки зрения обеспечивают нам безусловную безопасность, но есть различные стратегии атаки, которые были предложены, что требует серьезного внимания. Некоторые из этих атак возможны в идеальной среде, в то время как другие атаки получают свои корни от реализации в реальном времени. В каждой стратегии главная цель состоит в том, чтобы получить большое содержание информации без обнаружения или отслеживания. Чем больше прирост информации, тем умнее атака.

Перехватывая информацию в квантовом канале, злоумышленнику необходимо совершить квантовое измерение. Оно может быть двух типов [12]:

1. прямое;
2. косвенное.

В первом случае квантовая система будет взаимодействовать непоседственно с измерительным аппаратом подслушивателя. Во втором – использует вспомогательное состояние, или анциллу, которая по завершению подвергается уже прямому измерению.

Все атаки на протоколы квантового распределения ключа можно условно разделить на следующие классы [12]:

- Некогерентные атаки;
- Когерентные атаки;
- Коллективные атаки.

Особенности их реализации и структура будет рассмотрена в далее.

4.1 НЕКОГЕРЕНТНЫЕ АТАКИ

Некогерентные атаки иначе ещё называют индивидуальными. При совершении данного типа атак, злоумышленник Ева будет обрабатывать

каждый пойманный фотон отдельно. Самая простая атака такого типа называется «перехват-посылка», где Ева перехватывает фотон, посылаемый Алисой, совершает измерение его состояния и отправляет измеренный (и, соответственно, изменённый) фотон Бобу. Такая стратегия является непрозрачной, поскольку Ева излучает новые фотоны вместо пересылки по каналу фотонов Алисы.

Другой некогерентной атакой является перепутывание вспомогательного состояния Евы с пересылаемыми фотонами. Здесь Ева использует отдельную пробу для каждого посылаемого Алисой фотона. Фотон оказывается в запутанном состоянии, после чего Ева сохраняет в своей квантовой памяти пробу, а возбужденный фотон отправляется далее по каналу к Бобу. Когда завершается процесс открытого обмена сообщениями между легитимными пользователями, Ева проводит измерения над полученными ею пробами. Ожидание конца обмена обусловлено тем, что Ева из классического канала узнает базисы, используемые Алисой, что позволяет ей выбрать оптимальные измерения для своих проб. Данный вид атак называется полупрозрачным.

Поскольку Ева должна оставаться незамеченной, то необходимо уменьшать уровень вносимых ею ошибок. Она может достичь этого посредством уменьшения информации, которую она получает, другими словами – перехватывать только часть фотонов, пересылаемых по квантовому каналу связи Алисой.

4.2 КОГЕРЕНТНЫЕ АТАКИ

При выборе этой стратегии Еве необходимо воспользоваться своим вспомогательным состоянием, но в отличие от описанной выше атаки проба может иметь любую размерность и взаимодействовать не с каждым отдельным фотоном, а сразу с группой. В предельном варианте Евы перепутывает анциллу со всеми передаваемыми фотонами. Далее, как и в случае с некогерентной атакой, Ева сохраняет полученную пробу в своей квантовой памяти и дожидается окончания открытого обмена сообщениями, после чего измеряет все полученные состояния.

4.3 КОЛЛЕКТИВНЫЕ АТАКИ

Некоторым промежуточным вариантом является класс коллективных атак. Суть этой атаки заключается в том, что Ева, как и в случае с некогерентной атакой, запутывает каждый фотон со своей пробой, а получив из классического канала связи всю необходимую информацию, измерение проводит сразу на всех пробах, которые рассматриваются как целая квантовая система.

Классификация атак Евы также может быть представлена как на рис. 3 [23].

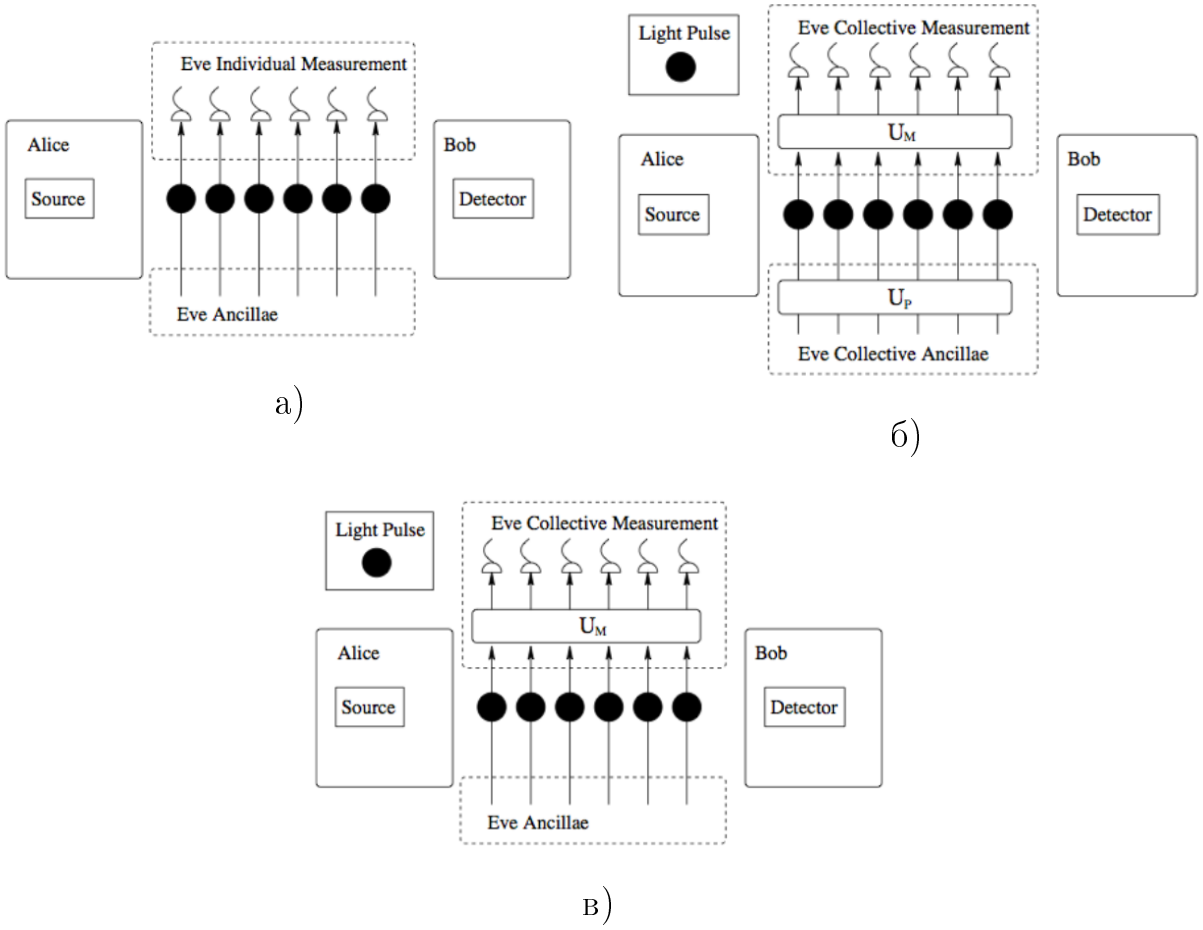

Рис. 3: Различные атаки Евы: а) индивидуальная атака; б) когерентная атака; в) коллективная атака

4.4 ВЫВОД

Следует сказать, что индивидуальные атаки пока единственные, которые возможны с использованием современных технологий. Для выполнения коллективных и когерентных атак Еве потребуются долгоживущая квантовая память и способность выполнять когерентные квантовые операции с высокой точностью, т. е. что-то вроде квантового компьютера. QKD, как правило, не считается безопасным с теоретико-информационной точки зрения, пока не будет доказана устойчивость от когерентных атак. Протокол BB84 является одним из протоколов, который, как было доказано, защищен от этого самого общего класса атак.

QKD – это теоретически безопасный способ распределения ключей в идеальном случае. То есть, если реализация BB84 точно такая же, какой она описана в теории, то Алиса и Боб имеют теоретико-информационную безопасность на их общем ключе. Однако на самом деле всегда есть практические недостатки и возможные лазейки. Например, если выбор базиса Алисы связан с громким шумом, то Ева может просто слушать, чтобы получить информацию о базисах и, следовательно, заполучить ключ путем измерения в правильном базисе каждый раз без ведома Алисы и Боба.

Необходимо быть очень осторожным при реализации QKD, чтобы избежать таких ошибок или побочных каналов, через которые может быть скомпрометирована безопасность. Еще одним классом практических трудностей при внедрении BB84 являются технологические проблемы, связанные с созданием и обнаружением одиночных фотонов. Обе эти задачи являются сложными, однако существует много исследований в области разработки источников одиночных фотонов и детекторов одиночных фотонов для того, чтобы удовлетворить эту потребность.

Отсутствие реальных одиночных детекторов фотона не компрометирует безопасность QKD, но может уменьшить коэффициент безопасности ключа. Отсутствие истинных одиночных источников фотона влияет на безопасность QKD, потому что если Алиса на самом деле отправляет два фотона в одном и том же состоянии вместо одного, Ева может

поймать один из них (это называется атакой расщепления числа фотонов). К счастью, это легко исправить (за счет снижения эффективности), что называется протоколом с состояниями «приманки». В соответствии с этой модификацией BB84, Алиса случайным образом заменяет один из своих фотонов данных на мультифотонное состояние «приманки». Боб измеряет это состояние как обычно, и после измерения Бобом (возможно, на стадии просеивания) Алиса показывает, какие из ее импульсов были состояниями приманки. Если Ева попытается атаковать расщепление числа фотонов на любой из импульсов приманки, Алиса и Боб могут детектировать это, посмотрев на результаты измерений Боба для импульсов приманки. И Ева не может избежать только этих импульсов, потому что их наличие обнаруживается только после квантовой фазы, когда все квантовые сигналы были переданы и обнаружены.

5 ИССЛЕДОВАНИЕ И ПОСТРОЕНИЕ РЕШЕНИЯ ЗАДАЧИ

Как было показано в работе [13] для известной для протокола BB84 величины критической ошибки, равной $Q_c \approx 11\%$, оптимальной в терминах того, что злоумышленник получит максимальное количество информации, внеся при этом минимум ошибок, будет являться такая стратегия Евы, при которой она совершает явную атаку на данный протокол и производит коллективные измерения в конце работы протокола. Рассмотрим более подробно этот алгоритм с позиции криптоаналитика Евы.

5.1 КОЛЛЕКТИВНАЯ АТАКА НА BB84

В протоколе BB84 вводится два базиса, которые кодируют биты следующим образом:

$$\{0,1\} \mapsto \{|x\rangle, |y\rangle\}$$
$$\{0,1\} \mapsto \{|u\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle), |v\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle)\} \tag{7.1}$$

Без ограничения общности, положим, что Ева инициализирует свою анциллу в состоянии $|A\rangle$. Для каждого бита $|b\rangle$, посылаемого Алисой, Ева выполняет унитарную операцию $\mathcal{U}$ на $|A\rangle \otimes |b\rangle$. Действие оператора $\mathcal{U}$ можно определить как[13]:

$$\mathcal{U}(|x\rangle \otimes |A\rangle) = |X\rangle = \sqrt{1-Q}|x\rangle \otimes |\phi_x\rangle + \sqrt{Q}|y\rangle \otimes |\theta_x\rangle \tag{7.2}$$

$$\mathcal{U}(|y\rangle \otimes |A\rangle) = |Y\rangle = \sqrt{1-Q}|y\rangle \otimes |\phi_y\rangle + \sqrt{Q}|x\rangle \otimes |\theta_y\rangle \tag{7.3}$$

$$\mathcal{U}(|u\rangle \otimes |A\rangle) = |U\rangle = \frac{1}{\sqrt{2}}(|X\rangle + |Y\rangle) = \sqrt{1-Q}|u\rangle \otimes |\phi_u\rangle + \sqrt{Q}|v\rangle \otimes |\theta_v\rangle \tag{7.4}$$

$$\mathcal{U}(|v\rangle \otimes |A\rangle) = |V\rangle = \frac{1}{\sqrt{2}}(|X\rangle - |Y\rangle) = \sqrt{1-Q}|v\rangle \otimes |\phi_v\rangle + \sqrt{Q}|u\rangle \otimes |\theta_v\rangle, \tag{7.5}$$

где $|\phi\rangle$ и $|\theta\rangle$ - состояния Евы.

Эти состояния должны выполнять требование по нормировке и сохранять унитарность, то есть:

$$\langle X|Y\rangle = \langle x|y\rangle, \langle U|V\rangle = \langle u|v\rangle \tag{7.6}$$

Основная часть анализа касается пространства Евы и Боба, в котором был передан i-ый кубит, которое является Гильбертовым пространством $\mathcal{H}^{A_i} \otimes \mathcal{H}^{b_i}$, содержащее пробу Евы и кубит Боба. Оператор плотности на этом пространстве обозначется как ρ. Если Алиса посылает $|0\rangle_z$, тогда состояние Евы и Боба это $|\varphi_0^z\rangle$ и $\rho_0 = |\varphi_0^z\rangle\langle\varphi_0^z|$, где z - это некоторое направление в базисе. Если она посылает $|1\rangle_z$, мы получим $\rho_1 = |\varphi_1^z\rangle\langle\varphi_1^z|$. Однако ни Ева, ни Боб не знают, послала Алиса $|0\rangle_z$ или $|1\rangle_z$, поэтому у них смешанное состояние: $\rho = \sqrt{1-Q}\rho_0 + \sqrt{Q}\rho_1$.

Состояния Евы - это след по состояниям Боба:

$$|x\rangle \mapsto \rho_x^{Eve} = (1-Q)|\phi_x\rangle\langle\phi_x| + Q|\theta_x\rangle\langle\theta_x| \tag{7.7}$$

$$|u\rangle \mapsto \rho_u^{Eve} = (1-Q)|\phi_u\rangle\langle\phi_u| + Q|\theta_u\rangle\langle\theta_u|, \tag{7.8}$$

когда Алиса послала $|0\rangle_z$, и

$$|x\rangle \mapsto \rho_y^{Eve} = (1-Q)|\phi_y\rangle\langle\phi_y| + Q|\theta_y\rangle\langle\theta_y| \tag{7.9}$$

$$|x\rangle \mapsto \rho_v^{Eve} = (1-Q)|\phi_v\rangle\langle\phi_v| + Q|\theta_v\rangle\langle\theta_v|, \tag{7.10}$$

когда Алиса послала $|1\rangle_z$. Состояния Боба получаются аналогично взятием следа по пространству состояний Евы

После этого происходит этап измерения у Боба и согласование им базисов с Алисой, а Ева пока сохраняет свои состояния в квантовой памяти. Следующим шагом будет оценка ошибки Q, где раскроется некоторая часть ключа, которая будет впоследствии отброшена. После завершения основных этапов, между Алисой и Бобом будет производиться вторичная обработка ключа, алгоритм которой описан в разделе «Вторичная обработка ключа в протоколе BB84». Здесь введем понятия пропускной способности классического канала связи и функции энтропии Шеннона.

Согласно [24], если канал связи с шумом описывается как $p(y|x)$ - вероятность того, что на принимающей стороне (выход) состояние принято как y, когда посылалось (вход) x, то уменьшение информации можно описать с помощью формулы Шеннона:

$$I(X;Y) = H(X) - H(X|Y), \tag{7.11}$$

где $H(X) = -\sum_x p_x \log p_x$ - это энтропия источника, а

$$H(X|Y) = \sum_y p_y H(X|Y=y) = -\sum_y p_y \sum_x \frac{p_{x,y}}{p_y} \log \frac{p_{x,y}}{p_y} = \tag{7.12}$$

$$= -\sum_{x,y} p_{x,y} \log p_{x,y} + \sum_y p_y \log p_y = H(X,Y) - H(Y)$$

- условная энтропия входа относительно выхода Y. $H(X,Y)$ - совместная энтропия случайных величин.

Если подставить эти формулы в формулу (1), то получим вазимную информацию в виде:

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = H(Y) - H(Y|X). \tag{7.13}$$

Важно заметить, что эта величина является неотрицательной.

Пропускная способность каналя связи определяется Шенноновской пропускной способностью:

$$C = max_{\{p_x\}} I(X;Y), \tag{7.14}$$

где $\{p_x\}$ - все возможные распределения на входе.

Введем энтропию случайного бита, или энтропийную функцию Шеннона, как:

$$h(Q) = -Q \log Q - (1-Q) \log(1-Q). \tag{7.15}$$

Для бинарного симметричного канала связи, который используют в протоколе легитимные пользователи Алиса и Боб, двочиная энтропия будет записана в том же виде. Тогда взаимная информация примет вид $I(X;Y) = H(X) - h(p)$, а ее максимум будет равен $C = 1 - h(Q)$

По [13][24], верным будет утверждение о том, что при использование случайного кодирования даст нам примерно $2^{nH(X)}$ (или $2^{nH(Y)}$) битов на входе и $2^{nH(Y|X)}$ битоы на выходе. И для того, чтобы ошибка в различении этих слов была минимальной, т.е. стремилась к нулю, размер кода не должен превышать следующего значения:

$$N \approx \frac{2^{nH(Y)}}{2^{nH(Y|X)}} = 2^{n(H(Y)-H(Y|X))} = 2^{nI(X;Y)} \Rightarrow N \approx 2^{nC} \tag{7.16}$$

Введем величину классической пропускной способности для квантового канала связи $\overline{C}(\varepsilon(Q))$ [13]:

$$\overline{C}(\varepsilon(Q)) = S(\sum_{i=x,y,u,v} \frac{1}{4}\rho_i^{Eve}) - \sum_{i=x,y,u,v} \frac{1}{4}S(\rho_i^{Eve}) \tag{7.17}$$

$$S(\rho) = -Tr\{\rho \log \rho\}$$

Для вычисления этого значения понадобятся собственные числа матрицы плотности ρ_i^{Eve}, которые равны $1-Q$ и Q [13].

Поскольку

$$\overline{C}(\varepsilon(Q)) = -Q\log Q - (1-Q)\log(1-Q) \tag{7.18}$$

$$\varepsilon(Q) = 1 - 2Q$$

Объединяя полученные значения для нахождения величины критической ошибки при коллективных измерениях Евы, мы получим:

$$C(Q_c) = \overline{C}(\varepsilon(Q_c)) \tag{7.19}$$

$$\Rightarrow 1 - h(Q_c) = h(Q_c) \tag{7.20}$$

С учетом (7.15) и (7.20), величина критической ошибки $Q_c \approx 11\%$, что полностью совпадает с её точным значением для рассматриваемого протокола.

6 ОПИСАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ

Результатом данной выпускной квалификационной работы является программный продукт, или приложение, которое позволяет пользователю не только понять основные принципы функционирования протокола квантового распределения ключа BB84, но и смоделировать возможную атаку на него, в качестве которой при реализации была выбрана самая оптимальная из возможных. Кроме того, для удобства пользования можно регулировать длину последовательности, которая будет генерироваться автоматически.

Компьютерная программа разработана на языке $C++$ в среде Visual Studio 2015 на основе интерфейса программирования приложений Windows Forms.

Разрабатываемый продукт может использоваться в различных операционных системах Windows, начиная с Windows NT 5.0 и заканчивая самыми последними. Приложение должно стабильно работать на всех версиях упомянутых операционных систем, не снижая своей надежности и эффективности от различных системных настроек.

Представленный программный продукт направлен на массовое использование, не требуя при этом особых предметных знаний в области квантовой криптографии. Другими словами, использовать приложение может любой пользователь, владеющий базовыми знаниями и навыками работы с компьютером, оснащенным операционной системой семейства Windows.

6.1 АЛГОРИТМ АТАКИ

Схематично алгоритм работы протокола с совершенной на него атакой можно представить в следующем виде:

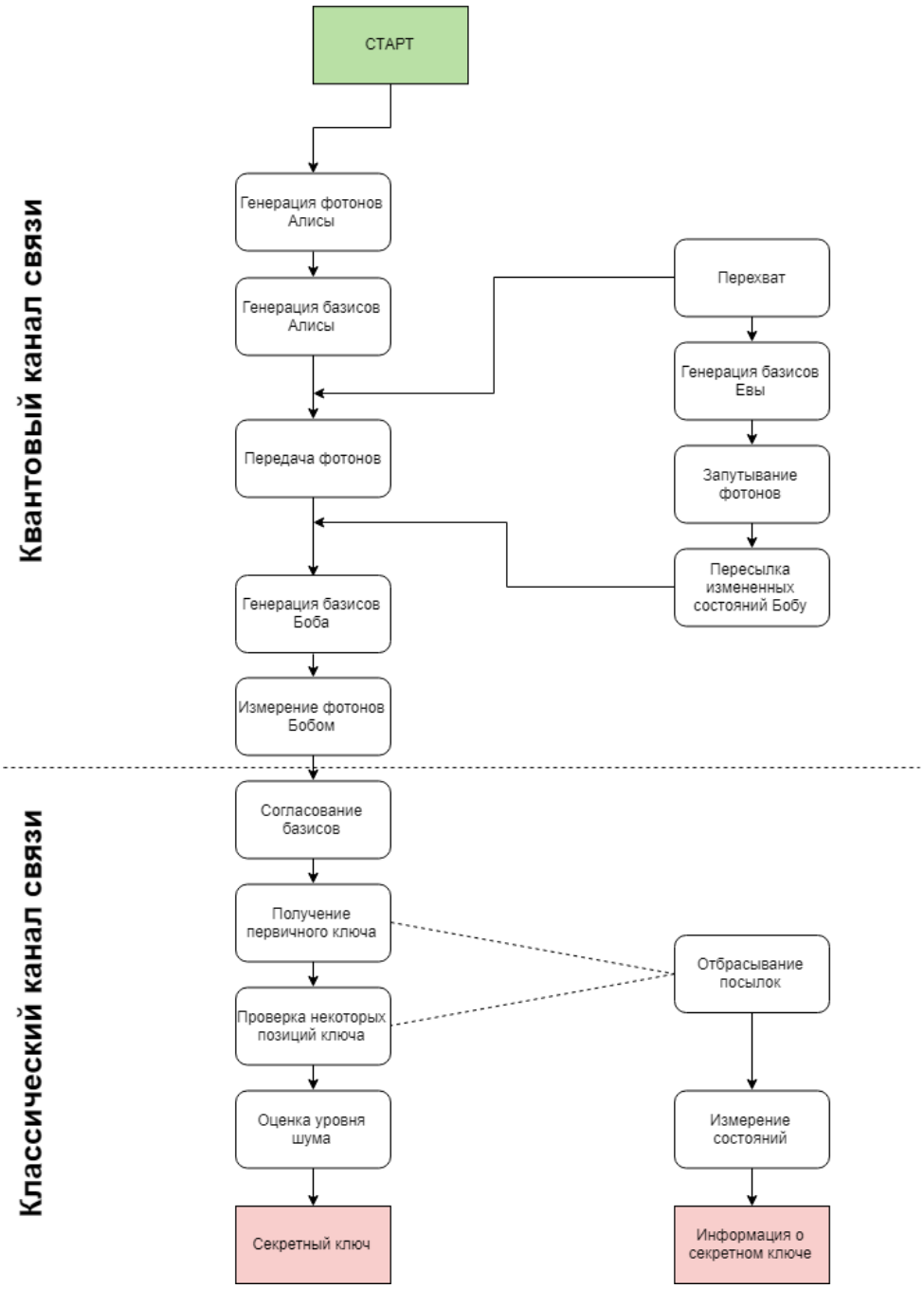

Рис. 4: Блок-схема выполнения коллективной атаки на протокол BB84

6.2 ИНСТРУКЦИИ ПО РАБОТЕ С ПРОГРАММОЙ

Описанная ниже инструкция к компьютерной программе, написание которой выполнено в рамках настоящей дипломной работы, предполагает возможность моделирования атаки для любого пользователя, возможно даже незнакомого с основными принципами квантовой криптографии и математики.

После запуска программы перед пользователем появляется интер-

фейс, содержащий следующие возможности:

1. Поле для указания длины строки посылаемой битовой последовательности
2. Две кнопки:
   2.1. Старт. После выбора длины (или используя установленную по умолчанию) пользователь может начать выполнение алгоритма работы протокола.
   2.2. Начать заново. Если на каком-то из этапов выполнения алгоритма работы протокола пользователь прервать и начать выполнение заново, то данная кнопка очистит все поля и вернет окно в исходный вид.
3. После нажатия кнопки «Старт» активируются поля и кнопки, содержащие необходимую информацию для начала передачи битовой строки:
   3.1. Генерация строки
   3.2. Генерация базисов (Алиса, Ева, Боб)
4. Когда необходимые для ввода поля заполнены, активизируется кнопка «Передача» и «Вмешаться» (для выполнения перехвата злоумышленником Ева)
5. Далее происходит активация кнопки «Сообщить о базисах», которая выполняет шаг алгоритма по согласованию базисов Алисой и Бобом.
6. Для этапа соглсования далее становится активной кнопка «Сообщить о корректности», после которой в поле «Оставшаяся строка» пользователь видит те биты, в которых согласование оказалось успешным.
7. На последнем этапе работы основного протокола активна кнопка «Сравнение и вычисление ошибки», которая заполняется полученными значениями оставшиеся поля.

8. Когда Алиса и Боб получили секретный ключ, Ева может измерить свои состояния, для этого пользователю необходимо нажать «Отбросить посылки» и «Измерение».

Кроме того, реализованы поля, которые отражают по какому каналу происходит общение между пользователями. В дополнение в правой части реализовано окно, отражающее ход выполнения и историю действий пользователя.

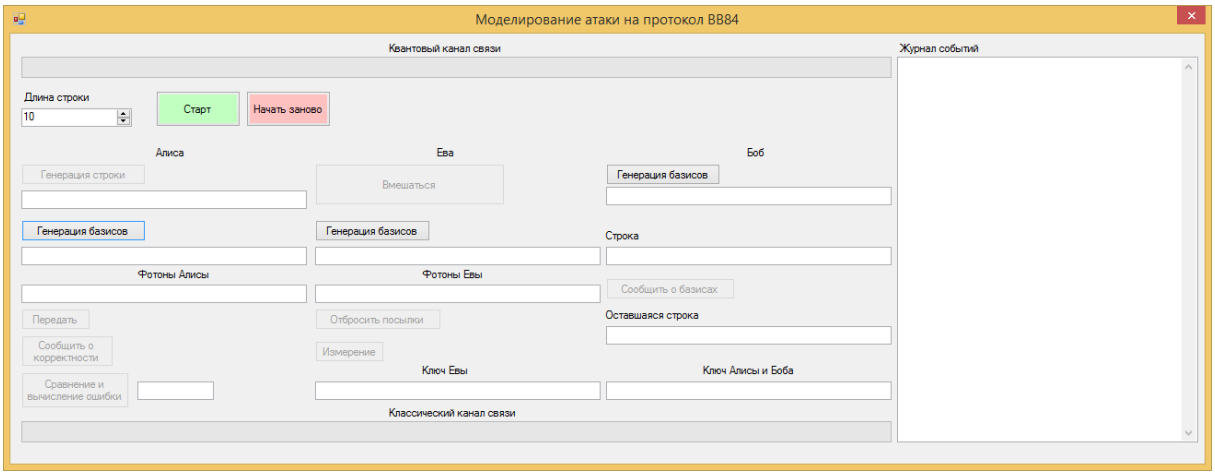

Рис. 5: Интерфейс программы

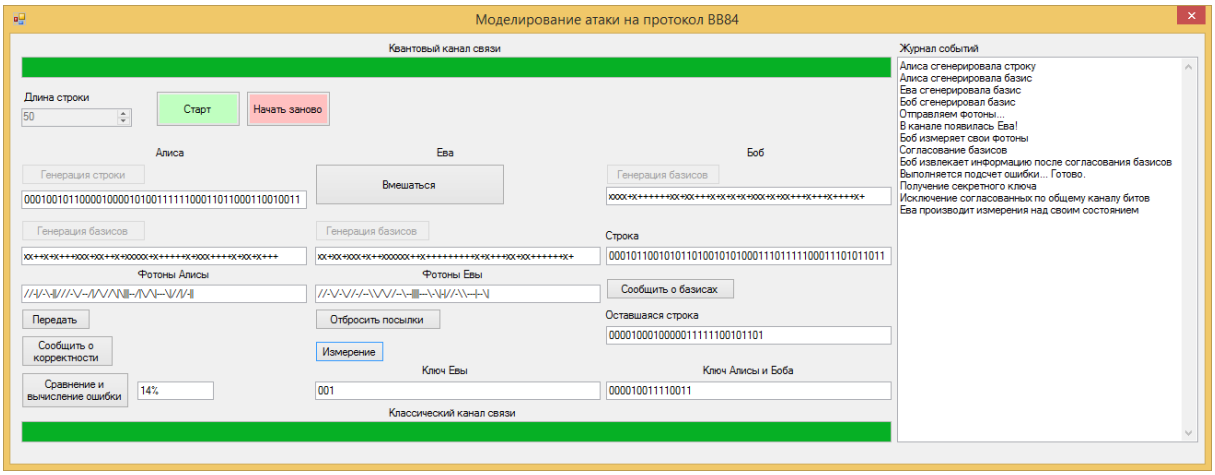

Рис. 6: Окно приложения после выполнения всех этапов протокола

Активизация кнопок по ходу выполнения выполнена для удобства пользователя, не знакомого ранее с интерфейсом программы или алгоритмом работы протокола. Кроме того, реализованы поля, которые отражают по какому каналу происходит общение между пользователями.

Для нескольких итераций запуска программы с различными числовыми значениями для длины битовой строки мы видим (Рис. 7), что выбор длины меньше ≈ 40 в целом нецелесообразен, поскольку ошибка может достигать довольно высоких значений ($> 20\%$), а при остальных значениях разброс в полученной ошибке минимальный, в том числе, в среднем, не превышает величины, при которой сеанс связи между легитимными пользователями не прерывался бы из-за помех, внесенных присутсвием в канале подслушивателя.

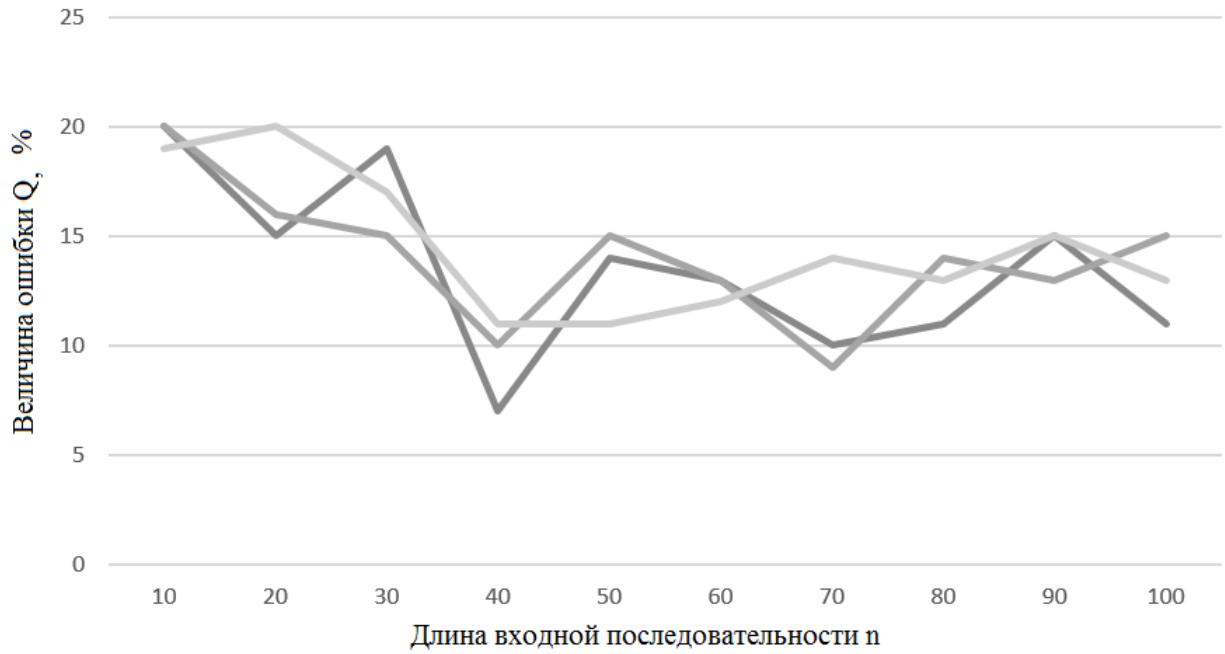

Рис. 7: Ошибка для различной длины строки

ЗАКЛЮЧЕНИЕ

В рамках данной выпускной квалификационной работы было разработано программное обеспечение, позволяющее моделировать атаку на протокол квантового распределения ключа BB84 с различными входными данными.

Данная компьютерная программа обладает не только особой уникальностью в своей сфере, но и предполагает возможность расширения для других видов атак и других протоколов, что определяет ее практическую ценность как для исследования квантовой криптографии, так и для компьютерной области в целом, поскольку она может быть рассчитана на массовое использование, в том числе с целью ознакомления.

Кроме того, исходный код программы позволяет использовать ее полностью или частично как компонент другой компьютерной системы.

Разработанное приложение полностью удовлетворяет поставленной задаче, а именно:

1. Она полностью реализует алгоритм работы протокола BB84
2. Обеспечен графический интерфейс для взаимодействия с пользователем
3. Исходный код построен таким образом, что его полностью или частично можно использовать для реализации других возможных задач, связанных с моделированием в квантовой криптографии

Поскольку квантовая криптография является актуальной наукой, то разработка моделей для реализации таких ее аспектов, как, например, протоколы квантового распределения ключа или алгоритмы устранения различного рода ошибок, является перспективной задачей.

Список литературы

[1] C.H. Bennet, G. Brassard. Quantum cryptography: public key distribution and coin tossing // Proceedings of IEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984. С. 175 – 179.

[2] Fuchs C.A., Gisin N., Griffiths R. [и др.] // Physical Review A. 1997. с. 1163.

[3] A. Poppe, M. Peev, O. Maurhart. Outline of the SECOQC quantum-key-distribution network in Vienna // International Journal of Quantum Information. 2008. С. 209 – 218.

[4] C.H. Bennet. Quantum Cryptography Using Any Two Nonorthogonal States // Physical Review Letters. 1992. С. 1 – 4.

[5] K. Tamaki, M. Koashi, N. Imoto. Unconditionally secure key distribution based on two nonorthogonal states // Physical Review Letters. 2003. с. 167904.

[6] M. Elboukhari, M. Azizi, A. Aziz. Quantum Key Distribution Protocols: A Survey // International Journal of Universal Computer Sciences. 2010. С. 59–67.

[7] H. Bechmann-Pasquinucci, N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography // Physical Review A. 1999. С. 4238 – 4248.

[8] Quantum cryptography protocols robust against photon number splitting attacks / Scarani A., Acin A., Ribordy G. [и др.] // Physical Review Letters. 2004. С. 1 – 4.

[9] A.K. Ekert. Quantum cryptography based on Bell's theorem // Physical Review Letters. 1991. С. 661 – 663.

[10] Experimental quantum cryptography / Bennett C.H., Bessette F., Brassard G. [и др.] // J. Cryptol. 1992. С. 3 – 28.

[11] C.E. Shannon. Communication in the Presence of Noise // Proc. IRE. 1944. С. 10 – 21.

[12] С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. Квантовая криптография: идеи и практика. 2007. С. 180 – 181.

[13] С.Н. Молотков, А.В. Тимофеев. Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки // Письма в ЖЭТФ. 2007. С. 632 – 637.

[14] D. Bruss, C. Macchiavello. Optimal eavesdropping in cryptography with three-dimensional quantum states // Physical Review Letters. 2002. С. 1 – 4.

[15] M. Haitjema. A Survey of the Prominent Quantum Key Distribution Protocols [Электронный ресурс]. 2007. URL: cse.wustl.edu/~jain/cse571-07/ftp/quantum/hup_protocols (09.05.2018).

[16] Quantum Cryptography / Gisin N., Ribordy G., Tittel W. [и др.] // Reviews of Modern Physics. 2002. С. 146 – 195.

[17] C.H. Bennet, G. Brassard, N.D. Mermin. Quantum cryptography without Bell's theorem // Physical Review Letters. 1992. С. 557 – 559.

[18] Entangled-photon six-state quantum cryptography / Enzer D., Hadley P., Gughes R. [и др.] // New Journal of Physics. 2002. С. 1 – 8.

[19] C. Fung, K. Tamaki, H. Lo. On the performance of two protocols: SARG04 and BB84 // Physical Review A. 2006. С. 1 – 4.

[20] G. Brassard, L. Salvail. Secret key reconciliation by public discussion // Secret key reconciliation by public discussion, Advances in Cryptology, Eurocrypt' 93 Proceedings. 1993. С. 410 – 423.

[21] J.L. Carter, M.N. Wegman. Universal classes of hash functions // Journal of Computer and System Sciences. 1979. С. 143 – 154.

[22] Generalized Privacy Amplification / Bennet C.H., Brassard G., Crepeau C. [и др.] // IEEE International Symposium on Information Theory. 1995. С. 1919 – 1920.

[23] M. Sarovar. Lectures 12-13: Introduction to quantum key distribution [Электронный ресурс]. 2014. URL: pdfs.semanticscholar.org (09.05.2018).

[24] А.С. Холево. Математическое основы квантовой информатики. 2015. С. 85 – 89.