Инженерный вестник Дона, №5 (2023)
ivdon.ru/ru/magazine/archive/n5y2023/8414

Разработка обучающей системы моделирования и демонстрации криптографических протоколов квантового распределения ключа

В.В. Баранов, В.В. Ромащенко, И.Н. Цыгулев

Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Аннотация: Проведён анализ основ современных криптографических систем. Рассмотрены проблемы классической криптографии, возникающие при развитии квантовых компьютеров. Рассмотрены криптографические протоколы квантового распределения ключа их преимущества и недостатки. Проведён анализ доступных на рынке стендов моделирования квантового распределения ключей. Сделано обоснование необходимости разработки обучающей системы. Авторами разработана система моделирования и демонстрации квантовых криптографических протоколов BB84, B92 и BB84(4+2), предназначенная для детального изучения принципов квантовых криптографических протоколов в динамике. Система обеспечивает процесс работы, как в текстовом, так и графическом виде. Разработанная система полностью отвечает потребностям обучения студентов современным квантовым технологиям защиты информации.

Ключевые слова: информационная безопасность, шифрование, квантовая обработка информации, квантовая криптография, моделирование, система обучения.

Обоснование необходимости системы

Кафедра «Информационная безопасность» Южно-Российского государственного политехнического университета (НПИ) имени М.И. Платова ведёт обучение по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» (специализация — «Защита информации в системах связи и управления») и по программе магистерской подготовки 10.04.01 «Информационная безопасность» [1]. Для подготовки квалифицированных специалистов имеет важное значение формирование компетенций в области криптографической защиты информации.

В настоящее время безопасность наиболее популярных коммуникационных протоколов основана на сложности определённых числовых задач, таких, как факторизация целых чисел или проблема дискретного журнала для разных групп [2].

В скором времени начнут появляться всё более мощные и доступные квантовые компьютеры, новые технологии, использующие физические

свойства материи и энергии для выполнения расчётов, которые смогут эффективно решать каждую из указанных выше числовых задач, тем самым делая все криптосистемы с открытым ключом на основе применяемых в настоящее время коммуникационных протоколов бесполезными для защиты данных [3-6]. Достаточно мощный квантовый компьютер будет представлять угрозу безопасности многим формам современной коммуникации - от обмена ключами до шифрования и цифровой аутентификации [7-9].

Для решения данной проблемы в 1984 году Чарльзом Беннетом и Жилем Брассаром был предложен первый протокол квантового распределения ключа (КРК) BB84, основанный на принципе неопределённости Гейзенберга. Протокол использует для кодирования информации четыре квантовых состояния двухуровневой системы, формирующие два сопряжённых базиса. Носителями информации являются двухуровневые системы, называемые кубитами (квантовыми битами).

Протокол использует четыре квантовых состояния, образующих два базиса, например, поляризационные состояния света. Состояния внутри одного базиса ортогональны, но состояния из разных базисов — попарно неортогональны. Эта особенность протокола позволяет определить возможные попытки нелегитимного съёма информации [10-11].

В настоящее время применение квантовых криптографических протоколов в телекоммуникационных системах не получило широкое распространение, но внедрение осуществляется всё более высокими темпами. В связи с этим выпускаемые специалисты должны быть подготовлены к применению квантовых криптографических технологий, знать их преимущества и слабые стороны.

Стоимость доступных на рынке лабораторных установок КРК в минимальной комплектации начинается с 8 млн. руб., а с возможностью эмуляции присутствия нарушителя стоимость может достигать 22 млн. руб. и

выше. В связи с высокой стоимостью установок трудно обеспечить всю учебную группу стендами, на которых можно провести работы с КРК в режиме без деструктивных воздействий и в режиме воздействия нарушителя. Это обстоятельство обусловило необходимость создания обучающей системы моделирования и демонстрации криптографических протоколов КРК.

Требования к системе

Необходимо разработать программное обеспечение моделирующей системы, выполняющей следующие функции и возможности:

- обеспечивает моделирование и демонстрацию работы современных криптографических протоколов, таких как BB84, B92 и BB84 (вариант 4+2);
- позволяет работать как в режиме без деструктивных воздействий, так и при воздействии нарушителя, который может действовать по различным сценариям;
- представляет процесс коммуникации в текстовом и в графическом виде с подробными комментариями для повышения наглядности;
- должна эксплуатироваться, в соответствии с современными требованиями, в среде операционных систем, входящих в реестр Российского программного обеспечения;
- должна обеспечивать работу в сетевом варианте, при котором система запускается на различных компьютерах (рабочих местах студентов) с применением протоколов коммуникации.

III. Принципы работы квантовых протоколов.

КРК - это новый инструмент в наборе инструментов криптографа, который обеспечивает безопасное согласование ключей по ненадёжному каналу. При передачи выходной ключ полностью независим от любого

входного значения, что невозможно при использовании классической криптографии. КРК не устраняет необходимость в других криптографических элементах, таких, как аутентификация, но его можно использовать для построения систем с новыми свойствами безопасности.

Работу КРК рассмотрим на примере протокола ВВ84. Чтобы преодолеть ошибки, вносимые шумом и прослушиванием передаваемой информации в квантовом канале, было разработано гарантированно безопасное согласование секретного ключа по общедоступному каналу. Первое общее, хотя и довольно сложное, доказательство гарантированной безопасности ВВ84 было приведено Майерсом [12], за которым последовал ряд других доказательств. В доказательстве Майерса схема ВВ84, предложенная Беннеттом и Брассардом, оказалась безоговорочно безопасной. Основываясь на идее квантовой генерации ключей для усиления конфиденциальности защищаемой информации, проф. университета Торонто Хой-Квонг Ло и проф. Гонконга Хой Фонг Чау предложили концептуально более простое доказательство безопасности КРК [13].

В КРК две стороны, Анна и Борис, получают некоторые квантовые состояния кубитов и измеряют их параметры. Затем они общаются по классическим каналам, чтобы определить, какие из результатов их измерений могут привести к битам секретного ключа. Некоторые биты отбрасываются в процессе, называемом просеиванием, потому что настройки измерения были несовместимы. Анна и Борис выполняют исправление ошибок и, затем, оценивают параметр безопасности, который описывает, сколько информации смогла получить криптоаналитик (Ева) о ключевых данных. Если объем скомпрометированной информации превышает определённый порог, передача сообщений прерывается, поскольку не может гарантироваться их секретность. Если объем скомпрометированной информации ниже порогового значения, они могут применить усиление конфиденциальности,

чтобы исключить любую оставшуюся информацию, которую может перехватить злоумышленник и получить общий секретный ключ. Передаваемые по классическому каналу сообщения должны быть аутентифицированы, чтобы избежать атак «человек посередине». Пример сети для КРК приведён на Рис. 1.

Протокол BB84 состоит из трёх фаз: «фаза общения по квантовому протоколу», «фаза совместного сравнения ключей» и «фаза проверки».

Рассмотрим фазу общения по квантовому протоколу. В BB84 Анна посылает Борису последовательность фотонов через незащищенный квантовый канал. Для каждого фотона независимо выбирается одна из четырёх поляризаций: вертикальная, горизонтальная, 45 градусов или 135 градусов. Принцип кодирования информации показан на Рис. 2.

Для каждого фотона Борис для выполнения измерения выбирает случайным образом один из двух базисов измерения прямолинейный или диагональный. Борис записывает свои базисы и результаты измерений. Борис по открытому каналу подтверждает получение сигналов.

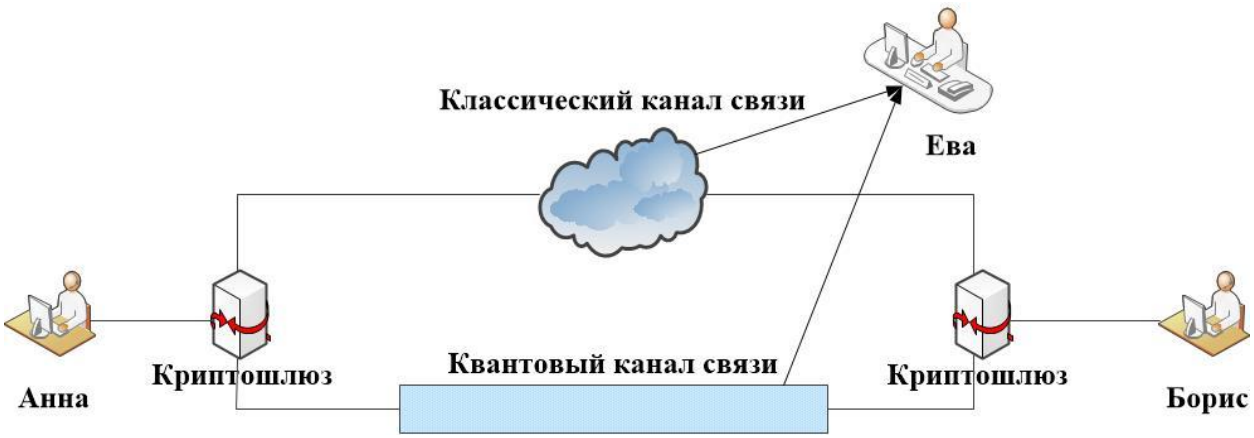

Рис. 1. Сеть для квантового распределения ключей.

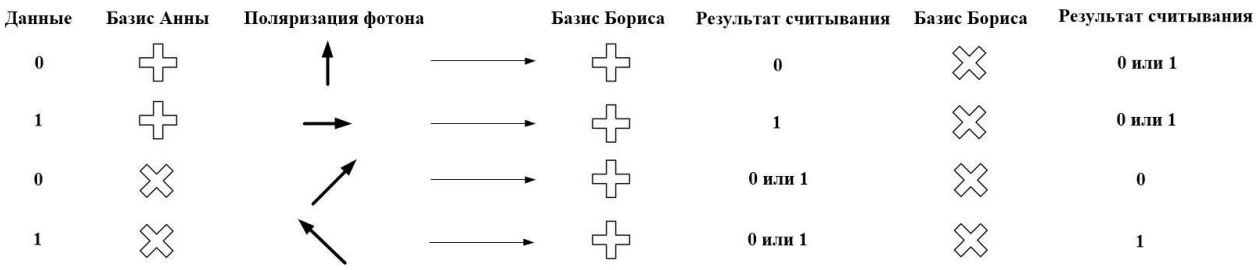

Рис. 2. Принцип кодирования и декодирования в протоколе BB84.

Анна и Борис преобразуют выбранные поляризации и результаты замеров в двоичную строку, называемую необработанным ключом, путём сопоставления фотона с поляризацией 45 или 90 градусов в «0» и фотона с поляризацией 0 или 135 градусов в «1».

Далее следует фаза совместного сравнения. Борис передаёт базисы своих измерений. Анна сообщает о случаях совпадения базисов измерения. Анна и Борис отбрасывают все случаи, в которых они используют разные базисы для сигнала. Оставшиеся биты называются просеянным ключом.

Завершающей является фаза проверки. Чтобы проверить информацию на предмет фальсификации, Анна случайным образом выбирает долю всех оставшихся событий в качестве тестовых событий. Для этих событий она публично транслирует свои выбранные позиции в ключе и результаты замеров.

Борис сообщает о количестве совпадений со своей версией ключа. Анна и Борис вычисляют частоту ошибок тестовых событий, то есть часть данных, для которых их значения не совпадают. Если вычисленная частота ошибок превышает какое-либо установленное пороговое значение (для BB84 — 11%) то передача сообщений прерывается. Если ключ не скомпрометирован, то начинается передача защищаемой информации по каналу.

Стороны могут производить классическую постобработку, такую, как исправление ошибок и усиление конфиденциальности, для генерации окончательного ключа.

IV. Разработка системы

Разработка программной системы эмуляции квантовых криптографических протоколов, названная «Велес», выполнена на языке программирования Java с применением библиотеки Swing. Это позволило разработать программный комплекс как мультиплатформенное приложение, которое может работать в среде множества операционных систем, в том числе входящих в реестр Российского программного обеспечения.

Для коммуникации системы «Велес» в сетевом варианте выбран протокол UDP, так как в этом случае соединение не устанавливается что позволило моделировать потерю пакетов в канале и достигать более высокой скорости связи между компьютерами.

Пример типовой схемы запуска системы приведён на Рис. 3.

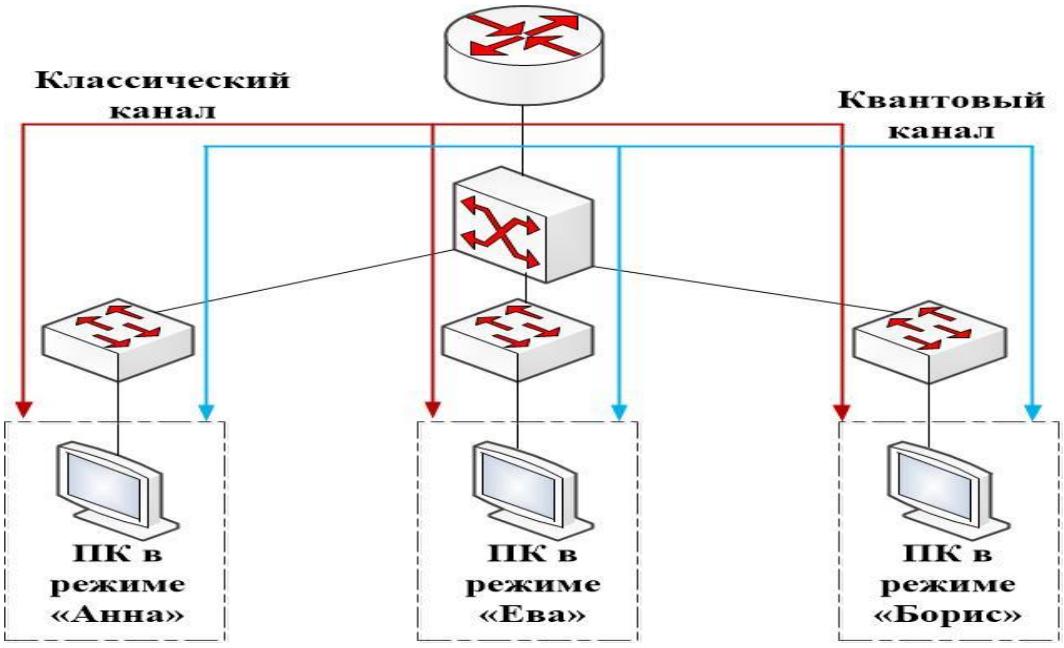

Рис. 3. Типовая схема стенда для запуска системы «Велес».

Система работает в трёх разных режимах:

1. Анна – посылающий сообщения;

2. Борис – принимающий сообщения;

3. Ева – криптоаналитик, пытающийся перехватить сообщения.

Режим моделирования системы выбирается во время запуска системы. Для начала работы следует запустить систему на двух ПК в режимах - «Анна» и «Борис». Режим «Ева» используется в том случае, если требуется вести работу с присутствием криптоаналитика в канале передачи данных.

Анна и Борис получают некоторые квантовые состояния (кубиты) и измеряют их. После обмена кубитами и согласования базисов Анна и Борис получают просеянные ключи. В идеале эти ключи идентичны. Но в реальных условиях эксплуатации всегда есть некоторые несоответствия, поэтому Анна и Борис должны применять классические протоколы обработки информации для исправления ошибок с целью получения идентичных ключей и повышения конфиденциальности передаваемых сообщений для получения секретного ключа. Проблема перехвата ключа заключается в том, чтобы найти протоколы, которые предоставляют Алисе и Борису либо проверенный ключ, либо останавливают работу и информируют их о том, что распределение ключа не удалось. Это отдельная проблема, решаемая на стыке квантовой физики и теории информации.

Для КРК-протокола имеется несколько проблем с перехватом сообщений, связанных с точностью реализации протокола, техническими возможностями нарушителя, технической и эксплуатационной надёжностями оборудования пользователей. Сразу отметим, что исследования по возможностям перехвата сообщений в квантовом канале не потеряли актуальности.

В рассматриваемых протоколах квантовой криптографии передача должна происходить без использования потока фотонов, а только посредством одиночных фотонов. В таком случае для Евы становится невозможным ответвление части сигнала для его анализа и обработки. Чтобы

упростить проблему, было определено и проанализировано несколько стратегий перехвата сообщений [14-16]. Особый интерес представляет предположение, что Ева прикрепляет независимые зонды к каждому кубиту и измеряет свои зонды один за другим. Её атаки можно классифицировать следующим образом: индивидуальные и коллективные.

В индивидуальной атаке Ева выполняет атаку на каждый сигнал независимо, примером такой атаки является атака с перехватом-отправкой.

Рассмотрим пример перехвата-пересылки атаки криптоаналитика Евы, которая измеряет каждый фотон в случайно выбранном базисе, а затем повторно отправляет полученное состояние Борису. Например, если Ева выполняет прямолинейное измерение, фотоны, подготовленные Алисой на диагональных основаниях, будут искажены измерениями Евы и дадут случайные ответы. Когда Ева отправляет Борису прямолинейные фотоны, если Борис выполняет диагональное измерение, он получает случайные ответы. Поскольку каждая из сторон выбирает два базиса случайным образом, такая атака с перехватом-отправкой даст частоту ошибок по битам $0,5 \times 0,5 + 0,5 \times 0 = 25\%$, которую легко обнаружат Анна и Борис.

К индивидуальным относят также атаку перепутывания, при которой Ева выполняет запутывание полученных квантовых измерений с пересылаемыми по каналу фотонами. При этом каждый фотон Алисы перепутывается с отдельно измеренным Евой состоянием независимо от других, и после этого фотоны посылаются Борису. Затем Ева хранит измерения в квантовой памяти и измеряет их состояния по отдельности после того, как закончится открытый обмен сообщениями между Алисой и Борисом на этапе просеивания ключа. В результате прослушивания, открытых сообщений между Алисой и Борисом у Евы существует возможность определить базисы, используемые Алисой, и, соответственно, выбрать оптимальные процедуры для проведения измерений.

Состояние фотонов Алисы, с которыми Ева перепутывает свои фотоны, изменяются, но уровень вносимых Евой ошибок может быть сделан меньше, чем при атаке перехвата-пересылки.

При коллективных атаках каждый фотон Алисы индивидуально перепутывается с отдельным измерением Евы, как и при индивидуальной атаке, но измерение осуществляется не индивидуально для каждого фотона, а на всех фотонах сразу, рассматриваемых как большая единая квантовая система. Ева откладывает свой выбор измерений. Только услышав публичное обсуждение между Алисой и Борисом, Ева принимает решение о том, какое измерение провести на её вспомогательной линии, чтобы извлечь информацию об окончательном ключе.

Для коллективных атак обычное предположение состоит в том, что Ева производит своё исследование только после того, как Анна и Борис завершили все публичные обсуждения о согласовании базисов, исправлении ошибок и усилении конфиденциальности. Что касается более реалистичных индивидуальных атак, то предполагается, что Ева ждёт только до этапа согласования базисов публичного обсуждения. Справедливо предположить, что в отдельных атаках Ева должна произвести измерения до согласования базисов [17]. Такое предположение основано на том, что едва ли Ева могла бы получить информацию, подождав до публичного обсуждения исправления ошибок и усиления конфиденциальности, прежде чем производить измерения, поскольку они будут независимыми. Некоторые предположения о безопасности практического применения КРК изложены в [18-19].

При выборе схемы перехвата моделируемой в системе считается, что криптоаналитик Ева обладает неограниченными возможностями и может использовать любое оборудование. Поэтому считаем, что Евой был произведён разрыв квантового канала и установлены криптошюзы 1 и 2 ,

аналогичные используемым Алисой и Борисом. Схема приведена на Рис. 4. Схема перехвата следующая: криптошлюз 1 производит замер в случайном базисе и передаёт результат и базис в криптошлюз 2, который производит отправку фотона в соответствии с базисом и результатом замера. Ева сохраняет базисы и результаты замеров и пытается использовать их для анализа данных, передаваемых через публичный канал связи. Перехват данных в публичном канале осуществляется посредством установки оборудования перехвата трафика на маршруте между Алисой и Борисом.

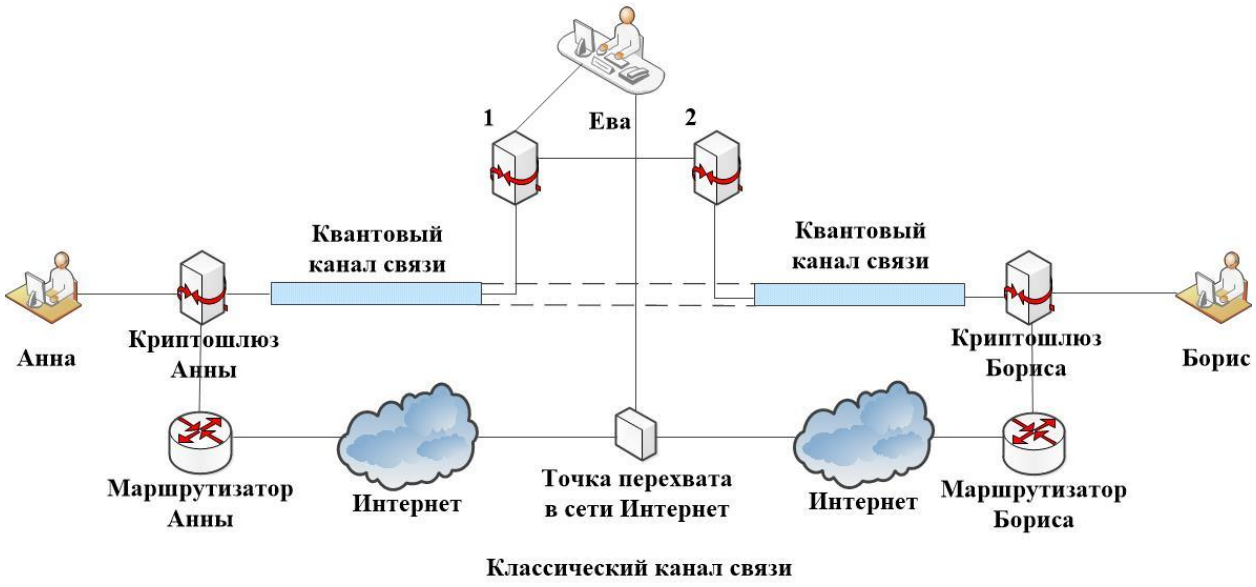

Рис. 4. Схема перехвата ключей, реализованная в системе «Велес».

Пользователь в режиме «Анна» вводит сообщение для передачи, выбирает вид криптографического протокола и алгоритма шифрования. После нажатия кнопки «Отправить» посредством криптографического протокола происходит синхронизация ключа между пользователями в режимах «Анна» и «Борис».

В настоящее время доступно шифрование по алгоритму Вернера с бесконечным шифроблокнотом и по алгоритму ГОСТ Р 34.11-2012. Для алгоритма Вернера с бесконечным шифроблокнотом математически доказана абсолютная криптостойкость, но в нём нет средств проверки целостности сообщения, поэтому для решения данной проблемы используем алгоритм

ГОСТ Р 34.11-2012. При выборе алгоритма ГОСТ Р 34.11-2012 доступна возможность установки длины используемого ключа.

Синхронизация ключа шифрования считается выполненной, если длина синхронизированного ключа достигла заданной пользователем величины. После синхронизации ключа сообщение шифруется при помощи алгоритма ГОСТ Р 34.11-2012 и передаётся по сети пользователю, работающему в режиме «Борис». Если длина сообщения больше длины ключа, то от сообщения отделятся часть равная длине ключа и пересылается. Для оставшейся части сообщения алгоритм повторяется до тех пор, пока сообщение не будет переслано.

Пользователь в режиме «Борис» не может производить настройки, а может только следить за процессом передачи данных. После синхронизации режима работы с пользователем «Анна» происходит процедура получения ключа от системы, работающей в режиме «Анна».

Затем происходит расшифровка исходного сообщения синхронизированным ключом.

Для режима «Ева» имеется два варианта:

1) можно задавать процент перехватываемых фотонов, в этом случае генератором случайный чисел определяется детектор и момент его применения;

2) можно задавать детектор перехвата фотонов пользователем.

Все пользователи системы «Велес» могут видеть, как перехватываемые фотоны влияют на процесс передачи данных и проводить анализ, позволяют ли перехваченные фотоны получить передаваемые ключи и как перехват фотонов может воздействовать на процесс передачи ключей.

Для улучшения восприятия студентами процесса работы по протоколу BB84 система обеспечивает графическое представление работы. Пример приведен на Рис 5.

Фаза квантового общения. Анна генерирует случайный ключ: 110001001010 и случайный набор базисов. Анна посылает Борису последовательность фотонов через незащищенный квантовый канал поляризация которых определяется выбранным базисом и битом ключа.

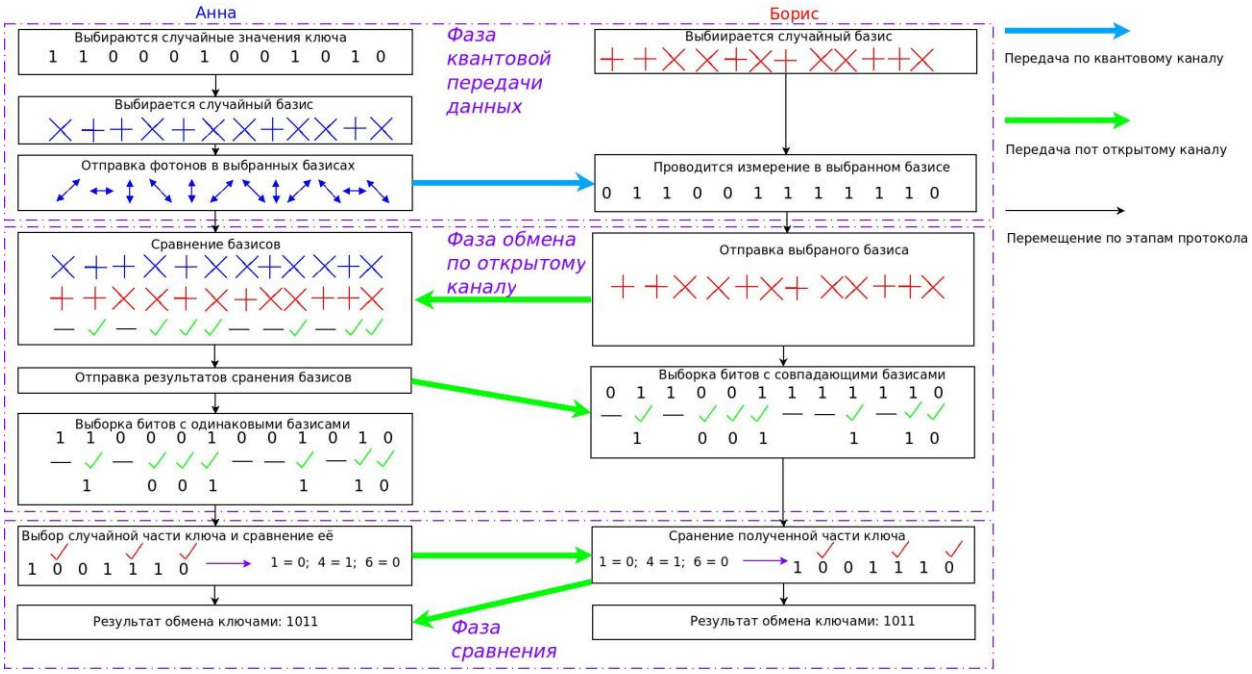

Рис. 5. Графическое представление работы по протоколу BB84 в системе «Велес».

Для каждого фотона Борис случайным образом выбирает один из двух базисов измерения прямолинейный или диагональный. Борис записывает свои базисы измерений и результаты 011001111110. Борис публично подтверждает получение сигналов.

Фаза совместного сравнения. По открытому каналу Борис передаёт использованные базисы Алисе. Анна производит сравнение и передаёт результат сравнения Борису. Анна и Борис отбрасывают в своих ключах все случаи, в которых они используют разные базисы для сигнала. На рисунке просеянный ключ равен 1001110.

Фаза проверки. Чтобы проверить полученные просеянные ключи на фальсификацию, Анна случайным образом выбирает долю из просеянного

ключа (на рисунке выбраны биты 1,4 и 6) и отправляет Борису для проверки позицию бита и его значение 010 по открытому каналу. Борис отправляет результат сравнения Алисе — ошибок не найдено. Анна и Борис вычисляют частоту ошибок тестовых битов, то есть, часть данных, для которых их значение не совпадает.

Если вычисленная частота ошибок превышает 11%, они прерываются, так как при этом считается, что канал прослушивается. В противном случае они отбрасывают использованные биты и переходят к использованию полученного ключа 1011.

Заключение

В ходе работы были рассмотрены основные принципы квантовой механики, на основании которых возможна реализация квантовой криптографии.

Разработана программная система «Велес», реализующая эмуляцию квантового распределения ключей по протоколам BB84, B92 и BB84(4+2) с возможностью эмуляции действия злоумышленника. Система эмулирует рабочие места передающей стороны, принимающей стороны и криптоаналитика, пытающегося перехватить данные. Созданная система облегчает изучение принципов квантовых криптографических протоколов и полностью отвечает потребностям обучения студентов современным квантовым технологиям защиты информации.

Литература

1. Официальный сайт «Кафедра информационной безопасности ЮРГПУ(НПИ)». – URL: wi.npi-tu.ru/index.php?id=258 (дата обращения: 29.04.2020).

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. с.806.

3. Фейнман Р.Ф. Квантово-механические ЭВМ // Успехи физических наук, УФН 149. — 1986. — URL: ufn.ru/ru/articles/1986/8/c/ (дата обращения 29.04.2020). С. 671–688.

4. Waldrop M.M. The chips are down for Moore's law // Nature. — 2016. — Vol. 530. — p. 144.

5. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. — 1997. — N. 26. — p. 1484.

6. Preskill J. Quantum Computing in the NISQ era and beyond // Quantum. — 2018. — N. 2. — p. 79.

7. Ключкарев П.Г., Квантовый компьютер и криптографическая стойкость современных систем шифрования. Весник МГТУ им Н.Э. Баумана. Сер. «Естественные науки». 2007. №2. С. 113-120.

8. Arute Frank, Kunal Arya, Babbush Ryan, Bacon Dave. Quantum supremacy using a programmable superconducting processor. URL: nature.com/articles/s41586-019-1666-5

9. Стенограмма круглого стола, который состоялся в январе 2020 в Русском доме на полях Всемирного экономического форума в Давосе. URL: globalaffairs.ru/articles/kvan-revolyucziya/, свободный (дата обращения: 29.04.2020)

10. New crypto-cracking record reached, with less help than usual from Moore’s Law. URL: arstechnica.com/information-technology/2019/12/new-crypto-cracking-record-reached-with-less-help-than-usual-from-moores-law/

11. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". URL: arxiv.org/abs/quant-ph/9508027.

12. Mayers, D. Unconditional security in quantum cryptography,” J. ACM, 2001, 48(3), pp. 351-406.

13. Lo, H. -K, Chau, H. F. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances,” Science, March 26, 1999, 283(5410), pp.2050-2056. Introduction to Quantum Cryptography URL: dx.doi.org/10.5772/56092143

14. Herong Yang, Java Swing Tutorials Herong's Tutorial Examples, 2018. URL: herongyang.com/Swing/

15. Lütkenhaus, N. Security against eavesdropping in quantum cryptography, Physical Review A, (1996), 54(1), pp. 97-111.

16. Gisin, N, Ribordy, G, & Tittel, W. et al., Quantum cryptography, Reviews of Modern Physics, (2002), 74(1), pp. 145-195.

17. Gisin, N, Ribordy, G, & Tittel, W. et al., Quantum cryptography, Reviews of Modern Physics, (2002), 74(1), pp. 145-195.

18. Barrett, J, Hardy, L, Kent, A. No signaling and quantum key distribution,” Physical Review Letters, Jul 1, 2005, 95(1). URL: arxiv.org/pdf/quant-ph/0405101v3.pdf

19. Stebila, D, Mosca, M, & Lütkenhaus, N. The Case for Quantum Key Distribution," Quantum Communication and Quantum Networking, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering A. Sergienko, S. Pascazio and P. Villoresi, eds., Springer Berlin Heidelberg, 2010, pp. 283-296.

References

1. Oficial'nyj sajt «Kafedra informacionnoj bezopasnosti YURGPU(NPI)». [Official site "Department of Information Security YRSPU (NPI)"], URL: wi.npi-tu.ru/index.php?id=258. (Date assessed 29.04.2020).

2. SHnajer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si. [Schneier B. Applied Cryptography. Protocols, algorithms, source texts in the C language.] M.: Triumf, 2003, p 806.

3. Fejnman R.F. Kvantovo-mekhanicheskie EVM, Uspekhi fizicheskih nauk [Quantum-mechanical computers]. UFN 149, 1986. URL: ufn.ru/ru/articles/1986/8/c/ (Date assessed 29.04.2020) pp. 671–688.

4. Waldrop M.M. Nature. 2016, Vol. 530, p. 144.

5. Shor P.W. SIAM J. Comput. 1997. N. 26. p. 1484.

6. Preskill J. Quantum Computing in the NISQ era and beyond, Quantum. 2018. N. 2, p. 79.

7. Klyuchkarev P.G. Vestnik MGTU im N.E. Baumana. Ser. «Estestvennye nauki». 2007. №2. pp. 113-120.

8. Arute Frank, Kunal Arya, Babbush Ryan, Bacon Dave. Quantum supremacy using a programmable superconducting processor. URL: nature.com/articles/s41586-019-1666-5

9. Stenogramma kruglogo stola, kotoryj sostoyalsya v yanvare 2020 v Russkom dome na polyah Vsemirnogo ekonomicheskogo foruma v Davose. [Transcript of the roundtable held in January 2020 at the Russian House on the sidelines of the World Economic Forum in Davos]. URL: globalaffairs.ru/articles/kvan-revolyucziya/, svobodnyj (Date assessed 29.04.2020).

10. New crypto-cracking record reached, with less help than usual from Moore’s Law. URL: arstechnica.com/information-technology/2019/12/new-crypto-cracking-record-reached-with-less-help-than-usual-from-moores-law/

11. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. URL: arxiv.org/abs/quant-ph/9508027.

12. Mayers, D. Unconditional security in quantum cryptography, J. ACM, 2001, 48(3), pp. 351-406.

13. Lo, H.K, Chau, H. F. Science, March 26, 1999, (1999). 283(5410), 2050-2056. Introduction to Quantum Cryptography. URL: dx.doi.org/10.5772/56092143

14. Herong Yang, Java Swing Tutorials Herong's Tutorial Examples, 2018. URL: herongyang.com/Swing/.

15. Lütkenhaus, N. Physical Review A, 1996, 54(1), pp.97-111.

16. Gisin, N, Ribordy, G, & Tittel, W. et al., Quantum cryptography, Reviews of Modern Physics, 2002 , 74(1), pp.145-195.

17. Gisin, N, Ribordy, G, & Tittel, W. et al., Quantum cryptography, Reviews of Modern Physics, (2002). , 74(1), pp.145-195.

18. Barrett, J, Hardy, L, & Kent, A. Physical Review Letters, Jul 1, 2005, 95(1).

19. Stebila, D, Mosca, M, & Lütkenhaus, N. Quantum Communication and Quantum Networking, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering A. Sergienko, S. Pascazio and P. Villoresi, eds., Springer Berlin Heidelberg, 2010, pp.283-296.