МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ
КАФЕДРА СУПЕРКОМПЬЮТЕРОВ И КВАНТОВОЙ ИНФОРМАТИКИ

Моделирование релятивистской системы квантового распределения ключей

Промежуточный отчет по дипломной работе

Студент 523 группы
Большаков Роман

Научный руководитель
профессор Молотков С.Н.

Москва
2014

Содержание

1 Классическая криптография

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

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

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

Традиционно для шифрования информации используются два подхода: симметричные криптосистемы и асимметричные. В симметричных методах шифрования применяется один и тот же ключ как для шифрования, так и для расшифрования данных. Обе стороны коммуникации должны знать этот ключ и хранить его в секрете. При асимметричном шифровании используется два ключа: открытый и закрытый. Открытый ключ передаётся по незащищённому каналу и используется для проверки электронной подписи и шифрования сообщения. Закрытый ключ используется для расшифрования сообщений и генерации электронной подписи.

Асимметричные криптосистемы имеют ряд преимуществ перед симметричными:

- не нужно предварительно передавать секретный ключ по надёжному каналу,
- этот секретный ключ известен только одной стороне,
- пару ключей можно долгое время не менять.

Однако есть и серьезные недостатки, которые не позволяют полностью перейти на использование асимметричных систем:

- в алгоритм сложно внести изменения,
- ключи имеют большую длину,
- по сравнению с симметричными криптосистемами процесс шифрования и расшифрования медленнее на порядки,
- требуются значительно большие вычислительные мощности для функционирования асиметричной криптосистемы.

Для симметричных криптосистем была доказана абсолютная криптостойкость [1], в то время как разработка квантовых компьютеров полностью разрушит асимметричные схемы шифрования. Остается одна проблема: как передать секретный ключ для симметричного шифрования. В классической физике этот вопрос не решается. Однако квантовая теория способна предложить некоторые решения.

2 Основные результаты, важные для квантовой криптографии

2.1 Коллапс волновой функции

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

$$\rho_i' = \frac{\sqrt{M_i}\rho\sqrt{M_i}}{\operatorname{Tr} M_i\rho}. \tag{1}$$

Это одно из важнейших для квантовой криптографии свойств, поскольку оно говорит о том, что попытки измерить систему ведут к помехам. Из этого следует, что попытки перехвата информации всегда можно детектировать по ошибкам на приёмной стороне.

2.2 Невозможность достоверного различения неортогональных состояний

Невозможность достоверного различения неортогональных квантовых состояний [2] — важный результат, на котором также во многом основывается секретность протоколов квантовой криптографии.

Этот результат можно сформулировать следующим образом: для чистых состояний $|\psi_0\rangle$ и $|\psi_1\rangle$ таких, что $\langle\psi_0|\psi_1\rangle = \cos\alpha \neq 0$, не существует измерения $\{M_0, M_1\}$, которое давало бы точный результат, то есть соответствовало бы условиям

$$\begin{aligned} \langle\psi_0| M_0 |\psi_0\rangle = 1, \quad \langle\psi_1| M_0 |\psi_1\rangle = 0, \\ \langle\psi_0| M_1 |\psi_0\rangle = 0, \quad \langle\psi_1| M_1 |\psi_1\rangle = 1. \end{aligned} \tag{2}$$

2.3 Чёткие и нечёткие наблюдаемые

Обычно под наблюдаемой подразумевают только ортогональное разложение единицы. Такие наблюдаемые будем называть *чёткими наблюдаемыми* [3]. В то же время требование взаимной ортогональности всех операторов не является обязательным, а в некоторых случаях выгоднее пользоваться наблюдаемыми, в которых не все операторы ортогональны друг другу, в целях получения максимального количества информации. Такие наблюдаемые называются *нечёткими*.

На первый взгляд нечёткие наблюдаемые просто смешивают вероятности разных исходов и не могут принести дополнительной пользы. Однако это не так. Рассмотрим пример, как нечёткая наблюдаемая может помочь различить неортогональные состояния $|\varphi\rangle$ и $|\psi\rangle$: $\langle\varphi|\psi\rangle = \cos\eta \neq 0$.

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

$$\begin{aligned} M_0 = \frac{\left|\psi^\perp\right\rangle\left\langle\psi^\perp\right|}{1+\cos\eta} = \frac{I - |\psi\rangle\langle\psi|}{1+\cos\eta}, \\ M_1 = \frac{\left|\varphi^\perp\right\rangle\left\langle\varphi^\perp\right|}{1+\cos\eta} = \frac{I - |\varphi\rangle\langle\varphi|}{1+\cos\eta}, \\ M_? = I - M_0 - M_1. \end{aligned} \tag{3}$$

Несложно обнаружить, что

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

и аналогично $\operatorname{Tr} M_1 \left|\varphi\right\rangle \left\langle\varphi\right| = 0$. Это значит, что при применении такого измерения нет шансов получить исход 0 при измерении состояния $|\psi\rangle$, а при измерении состояния $|\varphi\rangle$ не может получиться исход 1. Это означает, что такое измерение позволяет различать неортогональные состояния без ошибок. Цена этого — некоторая вероятность (равная $\cos\eta$) получить несовместный исход «?», который соответствует уклонению от ответа.

2.4 Невозможность клонирования квантовых состояний

В квантовой криптографии важен еще один результат из теории составных квантовых систем. Выше было показано, что неортогональные квантовые состояния нельзя достоверно различить. Здесь будет показано, что такие состояния нельзя и клонировать [4] — например, чтобы собрать более полную статистику результатов измерений.

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

$$U \left|\psi\right\rangle \otimes \left|A\right\rangle = \left|\psi\right\rangle \otimes \left|\psi\right\rangle, \tag{4}$$

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

Чтобы показать невозможность такого преобразования, достаточно рассмотреть его действие на базисные состояния $|0\rangle$ и $|1\rangle$:

$$\begin{aligned} U \left|0\right\rangle \otimes \left|A\right\rangle &= \left|0\right\rangle \otimes \left|0\right\rangle, \\ U \left|1\right\rangle \otimes \left|A\right\rangle &= \left|1\right\rangle \otimes \left|1\right\rangle, \end{aligned} \tag{5}$$

а также на состояние $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. В силу линейности оператора U и соотношений (5) должно выполняться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |A\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle). \tag{6}$$

С другой стороны, по определению U (4) должно получаться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |A\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle). \tag{7}$$

Полученное противоречие доказывает невозможность клонирования произвольных квантовых состояний. Стоит отметить, что клонировать состояния из ортогонального набора можно: для этого достаточно их измерить и приготовить состояние, соответствующее результату измерения.

3 Базовые протоколы квантового распределения ключей

К 1984 году основная часть описанных результатов уже была известна, и их оказалось достаточно для того, чтобы сформулировать принципы квантовой криптографии и предоставить доводы в пользу секретности такого способа распределения ключей.

Основные факты квантовой теории информации, на которых основывается квантовая криптография — связанные между собой утверждения о невозможности клонирования произвольных квантовых состояний (2.4) и о невозможности достоверного различения неортогональных состояний (2.2). В сочетании эти результаты дают тот факт, что попытки различения

квантовых состояний из неортогонального набора ведут к помехам, а значит, действия перехватчика могут быть детектированы по величине ошибки на приёмной стороне.

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

3.1 Протокол BB84

Неформально принцип действия всех протоколов квантовой криптографии можно описать следующим образом. Передающая сторона (Алиса) на каждом шаге посылает одно из состояний из неортогонального набора, а принимающая сторона (Боб) производит такое измерение, что после дополнительного обмена классической информацией между сторонами они должны иметь битовые строки, полностью совпадающие в случае идеального канала и отсутствия перехватчика. Ошибки в этих строках могут говорить как о неидеальности канала, так и о действиях подслушивателя. При величине ошибки, превышающей некоторый предел, действие протокола прерывается, иначе же легитимные пользователи могут извлечь полностью секретный ключ из этих частично совпадающих битовых строк.

3.1.1 Общая схема протокола

Протокол BB84 [5] использует два базиса:

$$\begin{aligned} + : \left|0^+\right\rangle = |0\rangle\,, \quad \left|1^+\right\rangle = |1\rangle\,, \\ \times : \left|0^\times\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \left|1^\times\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{8}$$

На этапе приготовления состояний Алиса случайным образом выбирает один из указанных базисов, а затем случайно выбирает значение бита: 0 или 1, и в соответствии с этим выбором посылает один из четырёх сигналов. При посылке каждого из этих сигналов Алиса запоминает свой выбор базиса и выбор бита, что приводит к появлению на ее стороне двух случайных битовых строк.

Боб, получая каждый из присланных Алисой сигналов, производит над ним одно из двух измерений случайным образом. Каждое из них способно дать достоверный резлуьтат из-за ортогональности состояний внутри каждого базиса:

$$\begin{aligned} M_0^+ = \left|0^+\right\rangle\left\langle 0^+\right|, \qquad M_1^+ = \left|1^+\right\rangle\left\langle 1^+\right|, \\ M_0^\times = \left|0^\times\right\rangle\left\langle 0^\times\right|, \qquad M_1^\times = \left|1^\times\right\rangle\left\langle 1^\times\right|. \end{aligned} \tag{9}$$

В результате он получает две строки: с выбором базисов и с исходами этих измерений.

Итак, после передачи всех состояний и проведения измерений Алиса и Боб имеют по две строки каждый. Теперь происходит согласование базисов: по открытому каналу Алиса и Боб объявляют друг другу свои строки с выбором базисов. Те посылки, в которых базисы не совпали, выбрасываются. Если базис Алисы совпал с базисом Боба, то в случае отсутствия помех в канале связи результаты в их битовых строках на соответствующей позиции также будут совпадать, поэтому после этапа согласования в случае идеального канала и отсутствия действий со стороны перехватчика Алиса и Боб обладают одними и теми же битовыми строками.

Но если в канале были ошибки или перехватчик пытался подслушать информацию, битовые строки Алисы и Боба могут не совпадать, поэтому для проверки они должны согласованно раскрыть примерно половины своих битовых строк. Согласно центральной предельной теореме, ошибка в раскрытой битовой последовательности дает достаточно точную оценку ошибки во всей последовательности, и по ней можно достаточно точно оценить вероятность ошибки в оставшихся позициях. Если величина ошибки оказывается больше некоторой величины (параметра протокола), передача данных прекращается: это означает, что перехватчик обладает слишком большой информацией о ключе. В противном случае перед Алисой и Бобом стоит задача получения общего секретного ключа, которую можно разбить на два этапа: сначала производится коррекция ошибок [6], после чего у Алисы и Боба оказываются совпадающие битовые строки; затем происходит усиление секретности [7], которое ставит своей целью исключить информацию о ключе, которая могла попасть к перехватчику в результате действий над состояниями или в ходе коррекции ошибок. В конечном итоге у перехватчика не должно остаться информации об общей битовой строке Алисы и Боба.

3.1.2 Стойкость протокола

При предложении протокола BB84 его стойкость была показана только на интуитивном уровне: попытка Евы измерить передаваемые состояния влечет к их разрушению, что приводит к ошибкам на приёмной стороне. Однако только измерениями посылаемых сигналов действия Евы не ограничиваются. Более того, непросто рассчитать информацию, способную попасть к Еве при всех возможных действиях с её стороны. Однако оказалось, что можно доказать стойкость протокола BB84, не прибегая к оценкам информационных величин для всех возможных атак Евы. В 2000 году было показано [8], что секретность квантовой криптографии можно свести к свойствам квантовых кодов коррекции ошибок: если ошибки, возникающие в квантовом канале связи, можно достоверно исправить, то можно добиться и секретной передачи данных. Это даёт критическую величину ошибки, до которой возможно секретное распределение ключей.

Доказательство стойкости протокола проще всего провести, введя несколько дополнительных протоколов. Так, стойкость введенного первым ЭПР-протокола [9] легко вытекает из теории квантовых измерений, а последовательным изменением некоторых действий легитимных пользователей он может быть сведен к более строго описанному протоколу BB84 без нарушения исходной секретности [10, 11].

Схема протокола, рассмотренная в [11], незначительно отличающаяся от описанной выше, использует для коррекции ошибок и усиления секретности свойства CSS-кодов, который не являются оптимальными. Теоретическая оценка на величину ошибки q, которую можно исправить в квантовом канале, дается границей Шеннона: $1 - 2h(q) > 0$. Достижение этой границы сводится к использованию случайных классических кодов. Теоретический предел ошибки, до которой возможно секретное распределение информации, равен примерно 11%, а именно корню уравнения $1 - 2h(q) = 0$.

3.1.3 Стратегии подслушивателя

Итак, утверждается, что при величине ошибки на приемной стороне менее 11% возможна секретная передача данных. В то же время не говорится о том, каким образом протокол теряет секретность при большей величине ошибки. В этом разделе рассмотрены некоторые схемы атаки, на одной из которых достигается теоретический предел ошибки на приемной стороне.

3.1.3.1 Прием-перепосыл

Наиболее простой сценарий действий Евы — измерение передаваемого по квантовому каналу состояния с дальнейшей пересылкой получившегося результата дальше. Именно таким образом прослушиваются классические каналы. В квантовом случае такая стратегия не работает.

Если Ева стремится произвести те же действия, что производит у себя Боб, то, не зная исходного состояния, она сталкивается с нерешаемой проблемой различения состояний из неортогонального набора. Применяя случайным образом одно из измерений (9) к посланному состоянию, в половине случаев Ева будет неверно угадывать базис. В силу свойства несмещенности базисных состояний при неверно угаданном базисе вероятность ошибки Евы состоавляет 50%, то есть Ева не получает полезной информации о сигнале.

Но это не все проблемы Евы. Неверно угаданный базис при проведении измерения вследствие коллапса волновой функции неизбежно приведет к тому, что Бобу будет послано ошибочное состояние. При применении измерения "$+$" вне зависимости от исходного состояния дальше будет послано одно из состояний набора $\{|0^+\rangle, |1^+\rangle\}$, аналогично с диагональным базисом "$\times$" будет послано одно из состояний набора $\{|0^\times\rangle, |1^\times\rangle\}$. Измеряя эти состояния в «верном» для них базисе, Боб получит ошибку, по которой действия Евы будут обнаружены.

Величину ошибки на приёмной стороне можно вычислить так. Допустим, Ева подвергала атаке не все состояния, а только их часть, атакуя каждый сигнал с вероятностью p. Тогда доля $1-p$ сигналов приходит к Бобу без ошибки (а Еве приходится просто угадывать значение бита в таких посылках, что вносит в её ошибку вклад, равный $(1-p)/2$). Для посылок, атакованных Евой, существует два равновероятных развития событий:

- Ева верно угадала базис, значит, точно получила информацию и не внесла возмущения.
- Ева ошиблась в выборе базиса. Тогда с вероятностью $1/2$ она получила ошибочный результат. Кроме того, совершенно точно она передала ошибочное состояние Бобу, что приводит к появлению ошибки на его стороне, вероятность которой также равна $1/2$.

Вероятность каждого из этих сценариев равна $p/2$, и нетрудно видеть, что доля ошибок на приёмной стороне будет равна $p/4$, а доля ошибок у Евы составит

$$\frac{1}{2} - \frac{p}{4}. \tag{10}$$

Это значит, что при всех значениях параметра p, меньших единицы, Ева имеет больше ошибок, чем Боб, и тогда её информация о ключе строго меньше. При $p = 1$ доли ошибок у Боба и Евы совпадают и равны 25%. Так как ошибка Боба однозначно связана с параметром p, то 25% — пороговая величина ошибки для такой атаки, до которой возможно секретное распределение ключей.

3.1.3.2 Коллективная атака

Критическая ошибка индивидуального подслушивания, равная 25% превосходит теоретический порог в 11%. Возникает вопрос, как Еве нужно изменить схему атаки, чтобы добиться лучших результатов? Оказывается, что слабая сторона индивидуальной атаки — в проведении измерений над каждым передаваемым состоянием по отдельности. Из свойства супераддитивности классически-квантового канала [3] следует, что выгоднее проводить измерение над всей последовательностью полученных состояний сразу. В [12] показано, что критическая ошибка Q_c для коллективной атаки равна корню уравнения $1 - h(Q_c) = h(Q_c)$, что совпадает с полученным выше теоретическим пределом.

3.2 Протокол B92

Протокол BB84 является первым и наиболее изученным протоколом квантовой криптографии. Однако попытки его практической реализации столкнулись с рядом технологических трудностей (о них ниже), в результате чего Ева может провести перехват информации, невозможный при строгой реализации всех принципов протокола BB84. Появилась необходимость разработки протоколов, способных противостоять Еве и на современном уровне развития технологий.

В протоколе BB84 при отсутствии действий перехватчика и помех в канале вероятность ошибки на приёмной стороне до согласования базисов составляет 25%. Это вызвано использованием строго зафиксированной конфигурации двух пар базисных векторов. Цель протокола B92 [2] состоит в возможности изменения этого параметра в зависимости от, например, длины канала или его качества. В ряде случаев это позволяет добиться большей скорости передачи данных.

На каждом шаге протокола B92 Алиса посылает Бобу одно из двух неортогональных состояний $|\psi_0\rangle$, $|\psi_1\rangle$, где $\langle\psi_0|\psi_1\rangle = \cos\eta$ — основной параметр протокола. На стороне Боба производится измерение с тремя исходами (3)

$$\begin{aligned} M_0 &= \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta}, \\ M_1 &= \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta}, \\ M_? &= I - M_0 - M_1. \end{aligned} \tag{11}$$

Посылки, в которых был получен несовместный исход $M_?$, отбрасываются.

После передачи всех сообщений Алиса и Боб, так же как в BB84, согласованно раскрывают часть своих битовых последовательностей и оценивают число ошибок. Если их оказалось больше некоторой величины, выполнение протокола прерывается, иначе из оставшейся части можно получить полностью секретный ключ. Стойкость протокола относительно наиболее эффективной атаки Евы (коллективной) была исследована в [13].

4 Проблемы практических реализаций

Несмотря на заявления о теоретической секретности указанных протоколов, на практике возникают различные трудности. Первая из них — в настоящее время не существует строго однофотонного источника. Современные лазеры выдают так называемые когерентные состояния:

$$|\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = e^{-\frac{\mu}{2}} (|0\rangle + \alpha\,|1\rangle + \frac{\alpha^2}{2}\,|2\rangle + \cdots), \tag{12}$$

где $\mu = |\alpha|^2$ — среднее число фотонов, $|0\rangle \equiv |vac\rangle$ — вакуумное состояние с числом фотонов 0. Значение параметра μ находится в районе $0.1 - 0.2$, что дает вероятность вакуумного состояния примерно 0.9, вероятность, что в посылке будет ровно один фотон — 0.09, ровно два фотона — 0.009 и т. д.

Проблема неоднофотонных источников дополняется второй — помехи и потери в квантовом канале связи. Эти два фактора дают возможность провести атаку с расщеплением по числу фотонов [14]. Вкратце, Ева может определить число фотонов в посылке. Если их более одного, то она отщепляет себе один фотон, а оставшуюся часть отправляет Бобу. Если фотон в посылке ровно один, эта посылка блокируется и Бобу ничего не посылается, таким образом имитируется потеря посылки из-за плохого качества канала. После передачи всех состояний у Евы будут храниться фотоны на каждую из принятых Бобом посылок. После раскрытия

базисов она проводит соответствующие измерения и полностью знает секретный ключ, не вызвав при этом никаких ошибок на приёмной стороне.

Однако, даже если в распоряжении Алисы имеется строго однофотонный источник, то при наличии потерь в канале Ева все равно может узнать [15] секретный ключ и остаться незамеченной следующим образом. Над каждой посылкой проводится измерение с тремя исходами. Если был получен совместный результат, Ева точно знает, какое состояние приготовила Алиса, поэтому может приготовить такое же и послать его Бобу. В случае несовместного результата посылка блокируется. Такая стратегия не производит никаких ошибок на приёмной стороне и оставляет подслушивателя незамеченным.

5 Релятивистское квантовое распределение ключей

Возникает принципиальный вопрос: существуют ли такие протоколы квантового распределения ключей, которые обеспечивают безусловную секретность при не строго однофотонном источнике и произвольных потерях в канале связи? Ответ на этот вопрос: да, существуют. Но для их построения недостаточно опираться исключительно на законы квантовой механики, как это делают все базовые протоколы (BB84 [5], B92 [2], SARG04 [16], phase-time coding [18]).

Все эти протоколы не используют тот факт, что фотоны движутся с предельно возможной скоростью света. В релятивитской схеме квантового распределения ключей всё взаимодействие происходит в пространстве-времени Минковского, и существенно используется ограничение специальной теории относительности на невозможность движения со скоростями больше скорости света. Основная идея релятивистской схемы состоит в том, чтобы «растянуть» информацию и в пространстве, и во времени. Для того, чтобы Ева смогла получить эту информацию, ей придется собрать все части вместе, так как по отдельности они абсолютно бесполезны. Для такого сбора потребуется некоторое время. После получения данных эту информацию потребуется снова разнести в пространстве-времени для соблюдения протокола, на что так же потребуется время. В итоге Ева будет вызывать детектируемые задержки прихода состояний.

6 Постановка задачи дипломной работы

Требуется смоделировать релятивистский протокол квантового распределения ключей в виде программного средства, визуализирующего различные состояния протокола, реализующей его аппаратуры, а также окружающей среды с учетом известных на данный момент физических взаимодействий и ограничений.

Более подробно, программное средство должно отображать процесс распределения ключей, как он происходит в реальном мире (с необходимыми допущениями). Необходимо смоделировать как поведение протокола в идеальном случае отсутствия злоумышленника, так и при его наличии.

Целью работы ставится объяснить и показать основные принципы работы релятивистской квантовой криптографии.

7 Основные результаты

Была разработана версия программного обеспечения, демонстрирующая схему работы релятивистского протокола квантового распределения ключей. В этой программе

- реализована подсистема визуализации времени и пространства протокола,

- реализована подсистема внутренней работы протокола,
- смоделировано поведение протокола по словесному описанию в идеальном случае,
- смоделировано поведение протокола в условиях наличия перехватчика в канале связи при различных его действиях.

Ниже будут даны снимки экранов с необходимыми пояснениями.

Для завершения работы еще необходимо

- улучшить физическую составляющую подсистемы моделирования,
- исправить различные ошибки в программном коде,
- улучшить представление данных на экране,
- внести в сценарии для моделирования больше нестандартных ситуаций.

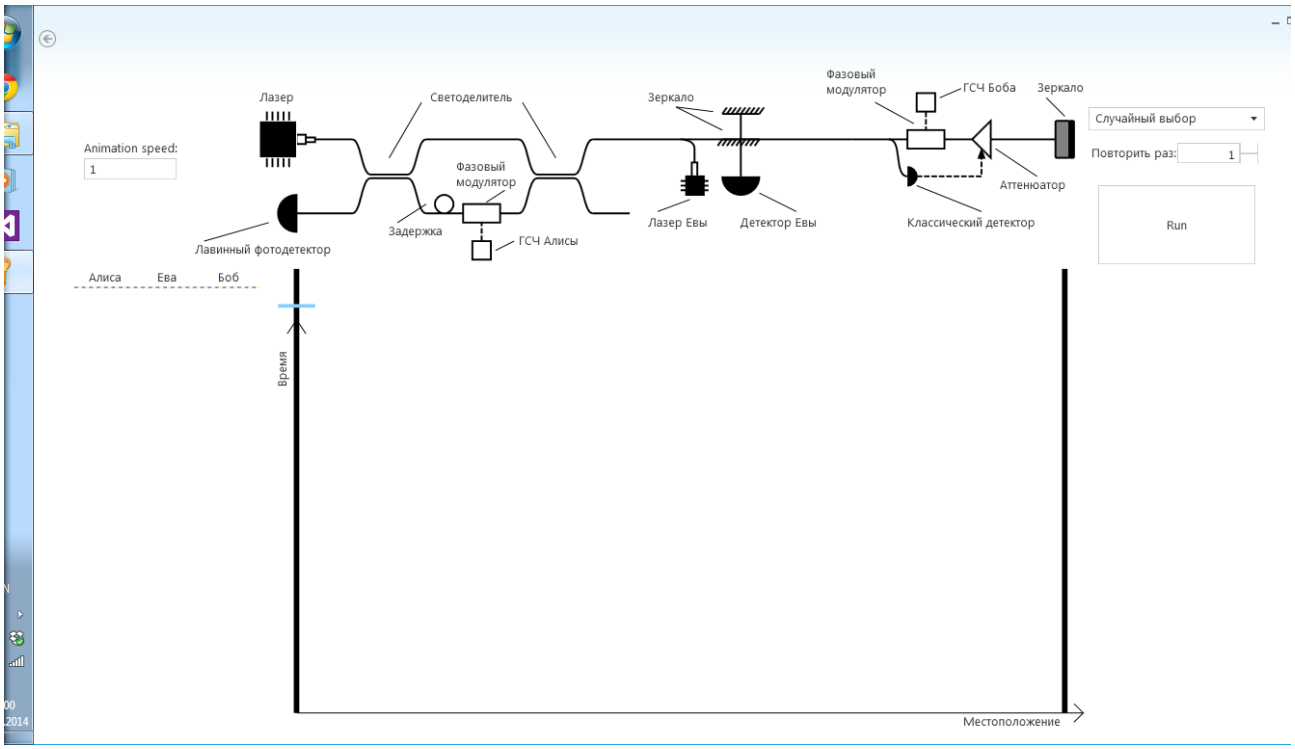

Рисунок 1: Начальное состояние системы

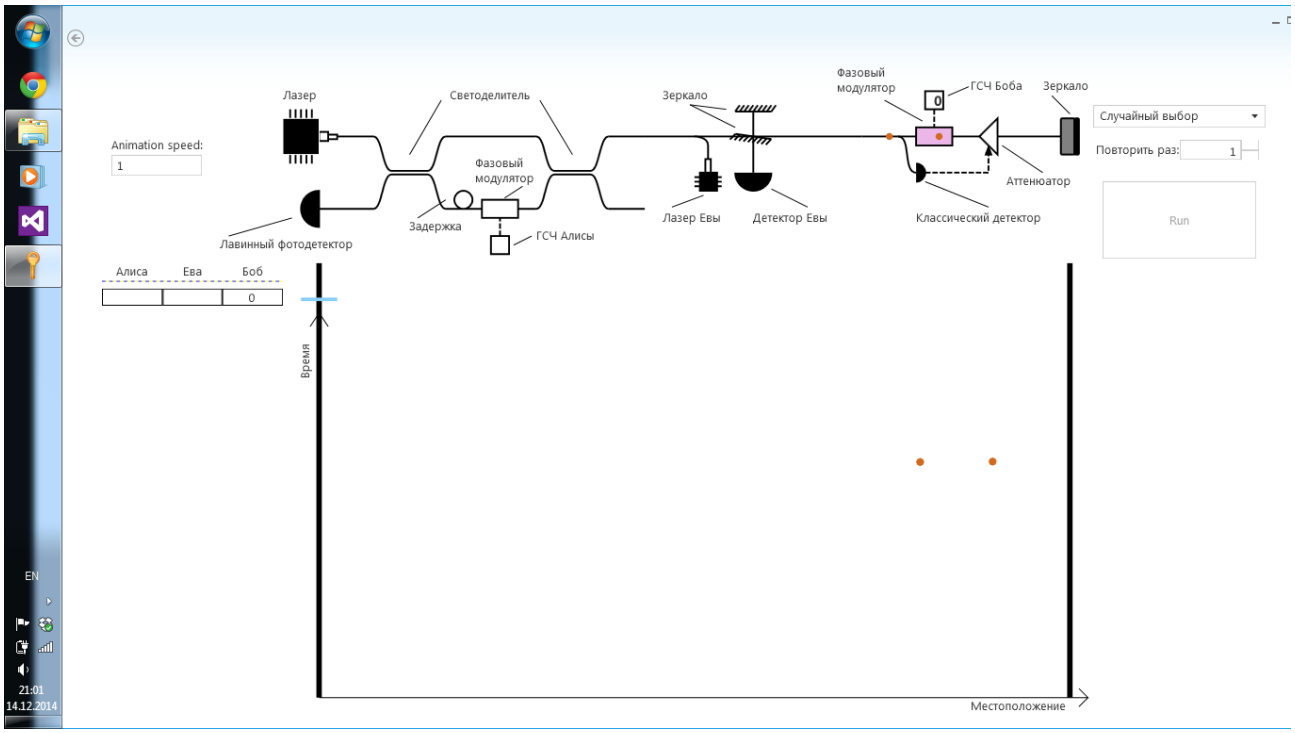

Рисунок 2: Система в процессе работы

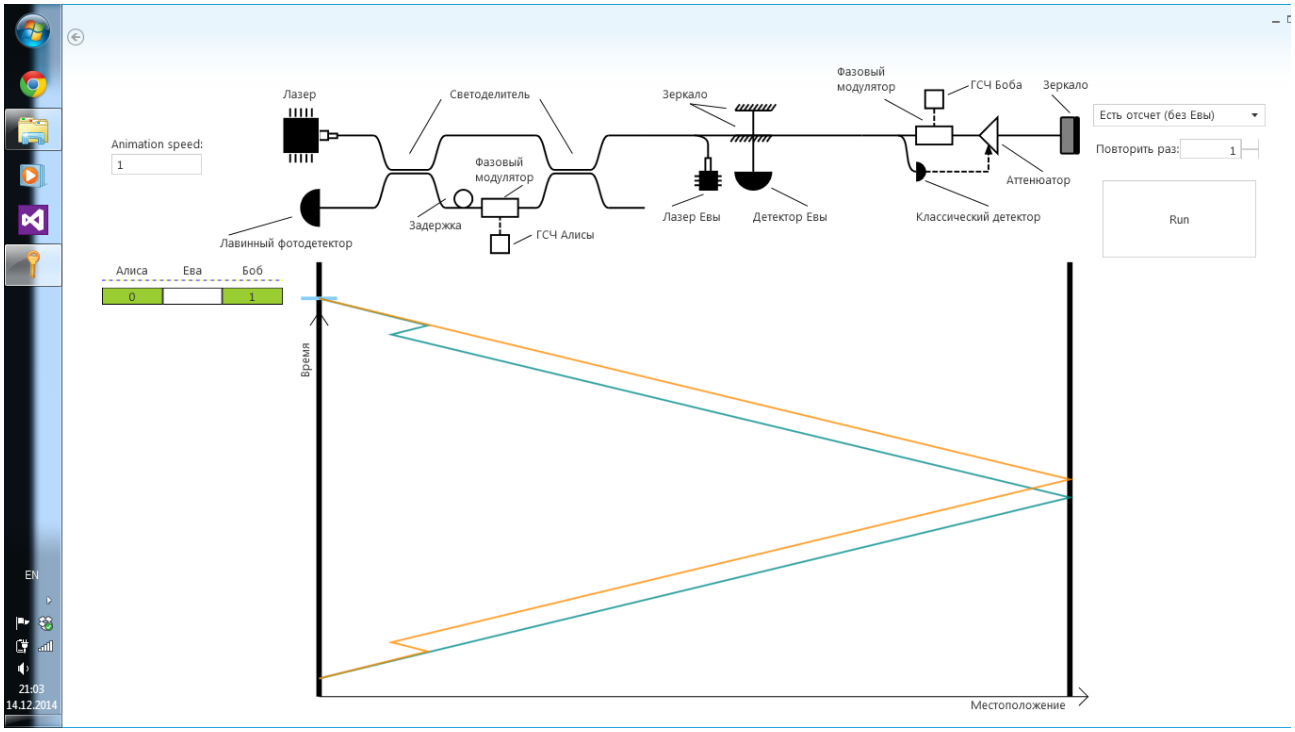

Рисунок 3: На этой итерации все прошло успешно и получен еще один бит ключа

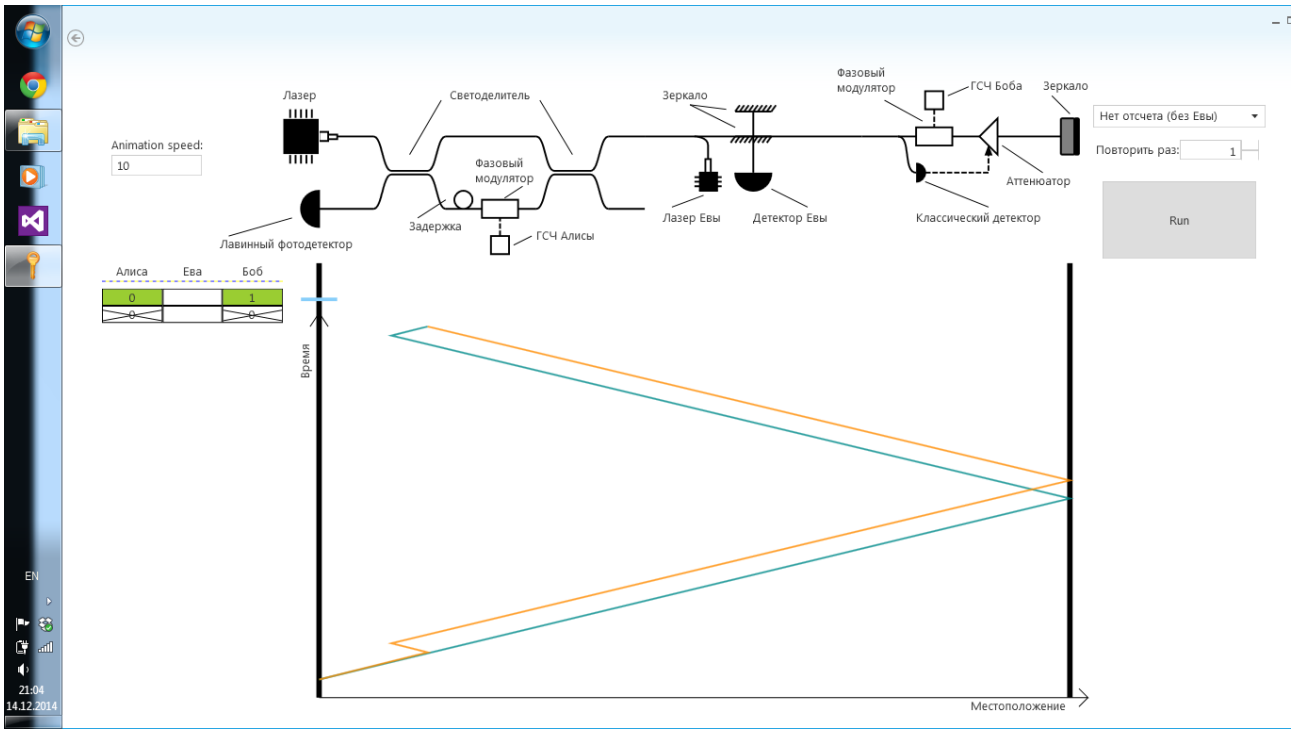

Рисунок 4: На этой итерации бит ключа получен НЕ будет

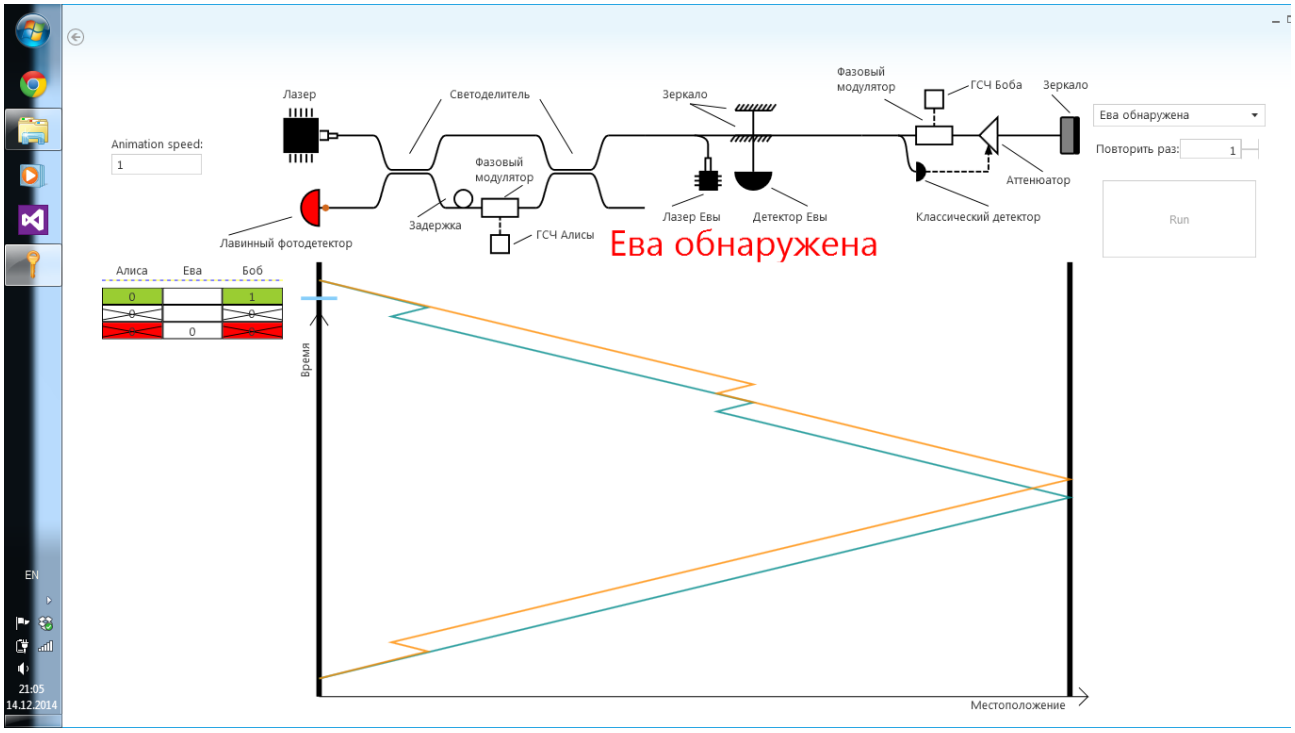

Рисунок 5: Если в канале возникнет злоумышленник, система об этом узнает и предупредит

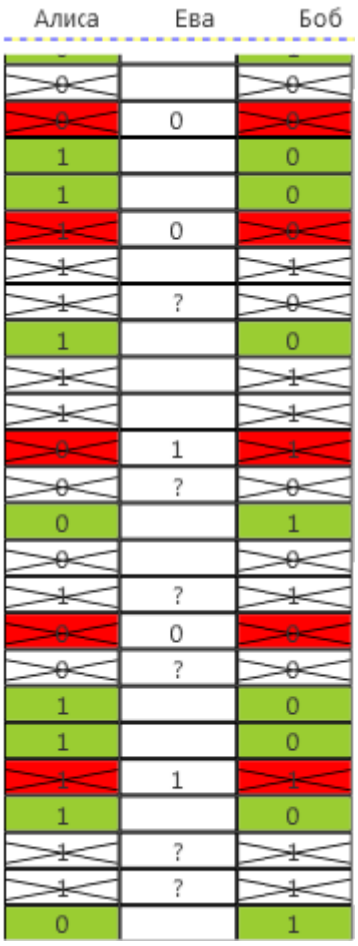

Рисунок 6: Серия посылок. Из зеленых ячеек в дальнейшем будет получен секретный ключ, остальные посылки будут отброшены

Список литературы

1. Э.М. Габидулин, А.С. Кшевецкий, А.И. Колыбельников. Защита информации. МФТИ, 2011.
2. Bennett Charles H. Quantum cryptography using any two nonorthogonal states // Physical Review Letters. 1992. Т. 68, № 21. С. 3121.
3. А.С. Холево. Квантовые системы, каналы, информация. МЦНМО, 2010.
4. Wootters W. K., Zurek W. H. A single quantum cannot be cloned // Nature. 1982. oct. Т. 299, № 5886. С. 802–803.
5. Bennett Charles H, Brassard Gilles [и др.]. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing / New York. Т. 175. 1984. С. 8.
6. Brassard Gilles, Salvail Louis. Secret-Key Reconciliation by Public Discussion. // EUROCRYPT / под ред. Tor Helleseth. Т. 765 из *Lecture Notes in Computer Science*. Springer, 1993. С. 410–423.
7. Generalized privacy amplification. / Charles H. Bennett, Gilles Brassard, Claude Crépeau [и др.] // IEEE Transactions on Information Theory. 1995. Т. 41, № 6. С. 1915–1923.
8. Shor Peter W, Preskill John. Simple proof of security of the BB84 quantum key distribution protocol // Physical Review Letters. 2000. Т. 85, № 2. С. 441.
9. Ekert Artur K. Quantum cryptography based on Bell's theorem // Physical review letters. 1991. Т. 67, № 6. С. 661–663.
10. Lo Hoi-Kwong, Chau H. F., Ardehali M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. // J. Cryptology. 2005. Т. 18, № 2. С. 133–165.
11. Baigneres Thomas. Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol: Tech. Rep.: : 2003.
12. Molotkov SN, Timofeev AV. Explicit attack on the key in quantum cryptography (BB84 protocol) reaching the theoretical error limit Q c 11% // JETP Letters. 2007. Т. 85, № 10. С. 524–529.
13. Molotkov S.N. On a collective attack on the key in quantum cryptography on two nonorthogonal states // Journal of Experimental and Theoretical Physics Letters. 2004. Т. 80, № 8. С. 563–567.
14. Acín Antonio, Gisin Nicolas, Scarani Valerio. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Physical Review A. 2004. Т. 69, № 1. С. 012309.
15. Dusek Miloslav, Jahma Mika, Lütkenhaus Norbert. Unambiguous state discrimination in quantum cryptography with weak coherent states. 2000. С. Physical Review A.
16. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations / Valerio Scarani, Antonio Acin, Gregoire Ribordy [и др.] // Phys. Rev. Lett. 2004. Т. 92. С. 057901.
17. Kronberg DA, Molotkov SN. Security of a two-parameter quantum cryptography system using time-shifted states against photon-number splitting attacks // Journal of Experimental and Theoretical Physics. 2009. Т. 109, № 4. С. 557–584.