

Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Большаков Роман Алексеевич
Научный руководитель: профессор,
д.ф-м.н. Молотков С.Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

Москва, 2015

- 1 Введение в предметную область
- 2 Исследование релятивистского протокола квантового распределения ключей
- 3 Исследование каскадного протокола коррекции ошибок
- 4 Описание практической реализации и полученных результатов

Проблемы классической криптографии

Проблемы классической криптографии

- проблема обнаружения подслушивателя;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует бóльших вычислительных мощностей, чем симметричная;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует бóльших вычислительных мощностей, чем симметричная;
- абсолютная криптостойкость доказана только для шифрования по методу Вернама «одноразовый блокнот»;

Проблемы классической криптографии

- проблема обнаружения подслушивателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует бóльших вычислительных мощностей, чем симметричная;
- абсолютная криптостойкость доказана только для шифрования по методу Вернама «одноразовый блокнот»;
- проблема первоначальной секретности.

Моделирование релятивистской системы квантового распределения ключей

└ Введение в предметную область

└ Проблемы классической криптографии

- проблема обнаружения подслушателя;
- основанность на предположениях об ограниченности злоумышленника в средствах, мощностях, интеллекте и др.;
- асимметричная криптография требует больших вычислительных мощностей, чем симметричная;
- абсолютная криптостойкость доказана только для шифрования по методу Вернама «одноразовый блокнот»;
- проблема первоначальной секретности.

В данной работе речь пойдет о квантовом распределении ключей, что является синонимом квантовой криптографии. Как известно, классическая криптография делится на симметричную и асимметричную. У каждой имеются свои достоинства и недостатки, однако потребность в квантовой криптографии возникает из следующих предпосылок: на слайде

В симметричной криптографии используется один и тот же ключ как для шифрования, так и для расшифровки сообщения, что приводит к проблеме: как передать участникам передачи секретный ключ?

Эту проблему и решает квантовая криптография.

Квантовое распределение ключей — механизм:

- использующий фундаментальные принципы квантовой механики,
- в результате работы которого:
 - либо получается **общая** для двух участников коммуникации строка **случайных бит**, известная **только им**;
 - либо происходит детектирование злоумышленника в канале связи

2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Введение в предметную область

└ Квантовая криптография

Квантовое распределение ключей — механизм:

- использующий фундаментальные принципы квантовой механики,
- в результате работы которого:
 - * либо получается *общая* для двух участников коммуникации строка *случайных бит*, известная *только им*;
 - * либо происходит детектирование злоумышленника в канале связи

Суть квантовой криптографии сводится к следующему. Имеются два легитимных пользователя, каждый из которых обладает случайной строкой бит. По определенному протоколу квантовой криптографии (фундаментальные принципы квантовой механики), а затем протоколу коррекции ошибок (в канале присутствуют помехи) эти строки приводятся к общему виду. В итоге получается секретный ключ, который можно использовать с любым методом шифрования. Если в канале связи присутствует подслушиватель, он же злоумышленник, то обе стороны будут об этом достоверно знать, могут оценить уровень информации, доступный злоумышленнику о ключе, и в случае превышения некоторой критической величины, зависящей от протокола, не станут использовать полученный ключ.

2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Введение в предметную область

└ Квантовая криптография

Квантовое распределение ключей — механизм:

- использующий фундаментальные принципы квантовой механики;
- в результате работы которого:
 - * либо получается *общая* для двух участников коммуникации строка *случайных бит*, известная *только им*;
 - * либо происходит детектирование злоумышленника в канале связи

Важно, квантовая криптография не позволяет передать какой либо секретной информации, а лишь получить ключ шифрования, секретность которого гарантирована.

Протоколы квантовой криптографии, в отличие от классических протоколов, опираются не на вычислительную сложность каких-либо алгоритмов, а на фундаментальные законы природы, что позволяет делать предположения о неограниченных возможностях злоумышленника относительно канала связи и передаваемых по нему данных, вычислительных мощностях и т.п.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.

Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.

Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.

Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Нерелятивистские протоколы используют **только** ограничения квантовой механики.

Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов.

Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Нерелятивистские протоколы используют **только** ограничения квантовой механики.

Релятивистский протокол = квантовая механика + специальная теория относительности.

2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Исследование релятивистского протокола квантового распределения ключей

└ Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много разработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Нерелятивистские протоколы используют только ограничения квантовой механики.
Релятивистский протокол — квантовая механика + специальная теория относительности.

Работы в области квантовой криптографии начали появляться с 1984 года, и с тех пор было предложено несколько различных протоколов, теоретическая секретность которых была строго доказана. Однако на практике реализовать эти протоколы не удается в силу несовершенства используемой аппаратуры, в частности имеются две основные проблемы:

- Лазер не может выдать ровно один фотон, как это требуется в теории. С некоторой, пусть и маленькой, но ненулевой вероятностью, он может испустить два, три и больше фотонов одновременно, чем может воспользоваться злоумышленник (т.н. PNS атака).
- В канале связи, особенно если это открытое пространство, присутствуют потери пакетов, чем также может воспользоваться злоумышленник, производя некоторые действия над посылаемыми данными и в случае неудовлетворительного для себя результата блокируя посылку,

2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Исследование релятивистского протокола квантового распределения ключей

└ Актуальность релятивистского протокола

В области квантовой криптографии уже имеется много наработок и разработано достаточное число протоколов. Основные практические проблемы:

- лазеры не могут испустить ровно один фотон,
- потери в канале связи.

Нерелятивистские протоколы используют только ограничения квантовой механики.
Релятивистский протокол — квантовая механика + специальная теория относительности.

Все описанные протоколы крк используют ограничения квантовой механики на невозможность достоверного различения неортогональных состояний и на невозможность копирования произвольного квантового состояния. И все они не учитывают тот факт, что **фотоны движутся со скоростью света**, а СТО утверждает, что передать информацию быстрее, чем со скоростью света - невозможно. Если воспользоваться этим ограничением СТО, получим релятивистский протокол квантового распределения ключей, **который делает указанные проблемы несущественными**.

Целью данной дипломной работы является создание программных средств:

- 1 моделирования и визуализации релятивистского протокола квантового распределения ключей в открытом пространстве,
- 2 моделирования и визуализации каскадного протокола коррекции ошибок по аутентичному каналу.

Моделирование релятивистской системы квантового распределения ключей

└ Исследование релятивистского протокола квантового распределения ключей

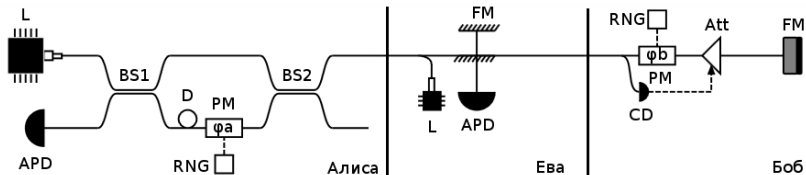
└ Цель дипломной работы

Целью данной дипломной работы является создание программных средств:

- 1 моделирования и визуализации релятивистского протокола квантового распределения ключей в открытом пространстве,
- 2 моделирования и визуализации каскадного протокола коррекции ошибок по аутентичному каналу.

Целью данной дипломной работы является моделирование и визуализация такого протокола квантового распределения ключей, а также моделирование и визуализация наиболее используемого в реальных приложениях каскадного протокола коррекции ошибок.

Схема релятивистского протокола



Моделирование релятивистской системы квантового распределения ключей

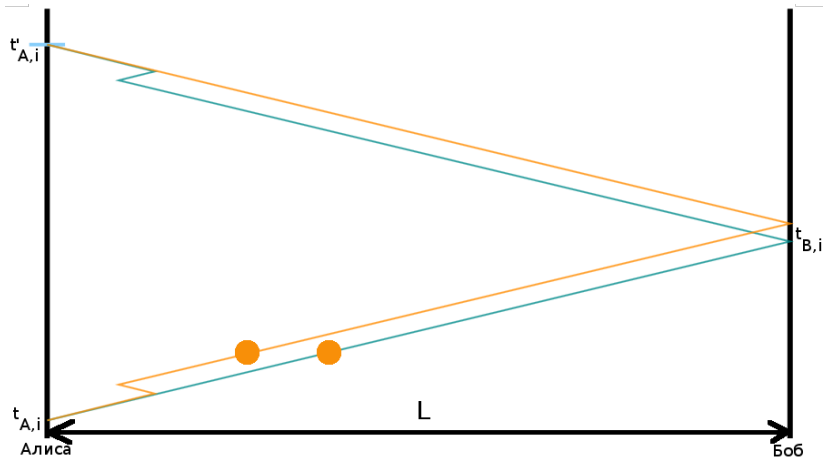
└ Исследование релятивистского протокола квантового распределения ключей

└ Схема релятивистского протокола



Принципиальная схема протокола показана на слайде. Суть протокола сводится к разведению частей состояния в пространстве-времени так, что по отдельности они не несут никакой полезной информации. Для того, чтобы получить информацию о ключе, эти части нужно свести вместе в одну точку пространства Минковского, на что требуется конечное время.

Схема релятивистского протокола



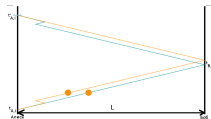
2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Исследование релятивистского протокола квантового распределения ключей

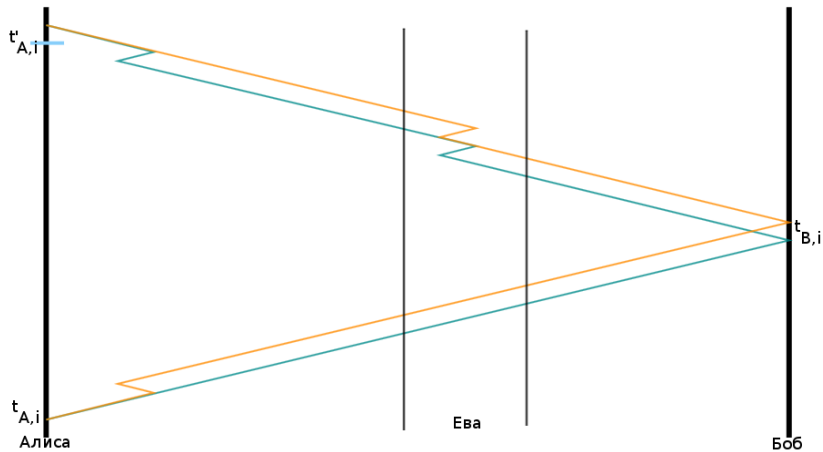
└ Схема релятивистского протокола

Схема релятивистского протокола



Алиса (слева) включает свой детектор только в определенные временные промежутки, когда, по ее расчетам, должно прийти ответное состояние.

Схема релятивистского протокола



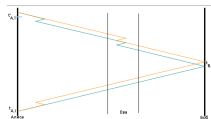
2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Исследование релятивистского протокола кван-
тового распределения ключей

└ Схема релятивистского протокола

Схема релятивистского протокола



Если в канале передачи присутствует злоумышленник, то он потратит некоторое время сначала на сведение частей состояния вместе, получение необходимой ему информации, а затем на разведение частей обратно. В результате состояние придет к Алисе с задержкой, которая будет задетектирована.

Каскадный метод коррекции ошибок

В канале связи (в частности если это открытое пространство) неизбежно присутствуют помехи, вносящие ошибки в ключ. Их необходимо исправить, выдав как можно меньше информации о ключе возможному подслушивателю.

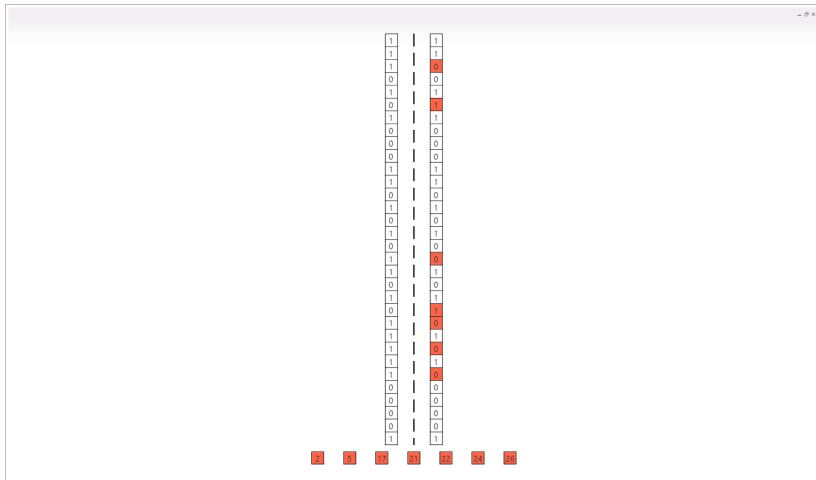
Моделирование релятивистской системы квантового распределения ключей

- └ Исследование каскадного протокола коррекции ошибок
 - └ Каскадный метод коррекции ошибок

В канале связи (в частности если это открытое пространство) неизбежно присутствуют помехи, вносящие ошибки в ключ. Их необходимо исправить, выдав как можно меньше информации о ключе возможному подслушивателю.

После проведения квантовой части протокола, требуется коррекция ошибок в силу наличия помех в канале связи. Коррекция ошибок производится по аутентичному каналу, то есть который можно свободно прослушивать, но невозможно изменить передаваемые по нему данные (газеты, twitter итд).

Каскадный метод коррекции ошибок



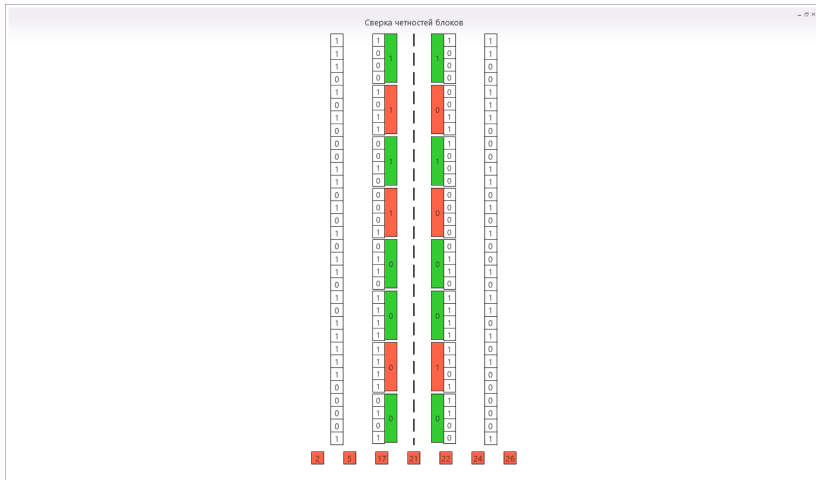
Каскадный метод коррекции ошибок

Выполнение случайной перестановки

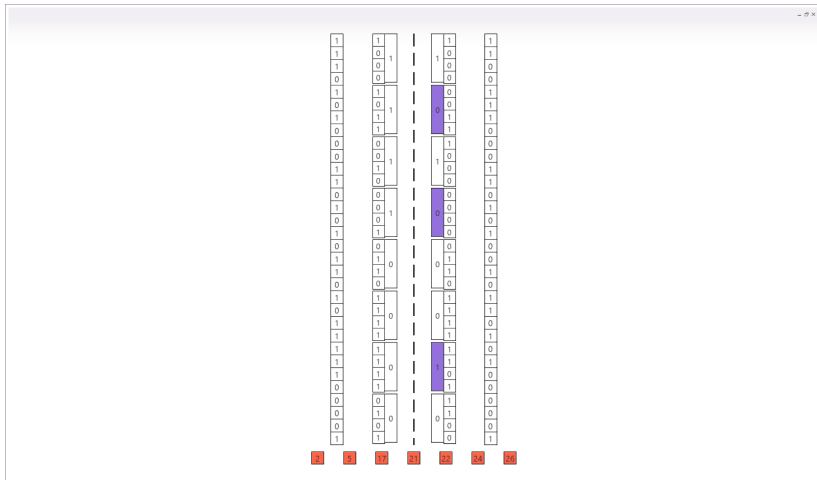
1	1 10	10 1	1
1	0 3	3 0	1
1	0 19	19 0	0
0	0 14	14 0	0
1	1 22	22 0	1
0	0 7	7 0	1
1	1 11	11 1	1
0	1 4	4 1	0
0	0 21	21 1	0
0	0 28	28 0	0
1	1 26	26 0	1
1	0 8	8 0	1
0	0 27	27 0	0
1	0 30	30 0	1
0	0 12	12 0	0
1	1 17	17 0	1
0	0 29	29 0	0
1	1 6	6 1	0
1	1 13	13 1	1
0	0 9	9 0	0
1	1 25	25 1	1
0	1 15	15 1	1
1	1 1	1 1	0
1	1 31	31 1	1
1	1 0	0 1	0
1	1 18	18 1	1
1	1 2	2 0	0
0	1 23	23 1	0
0	0 5	5 1	0
0	1 20	20 1	0
0	0 16	16 0	0
1	1 24	24 0	1

2 3 37 31 23 24 26

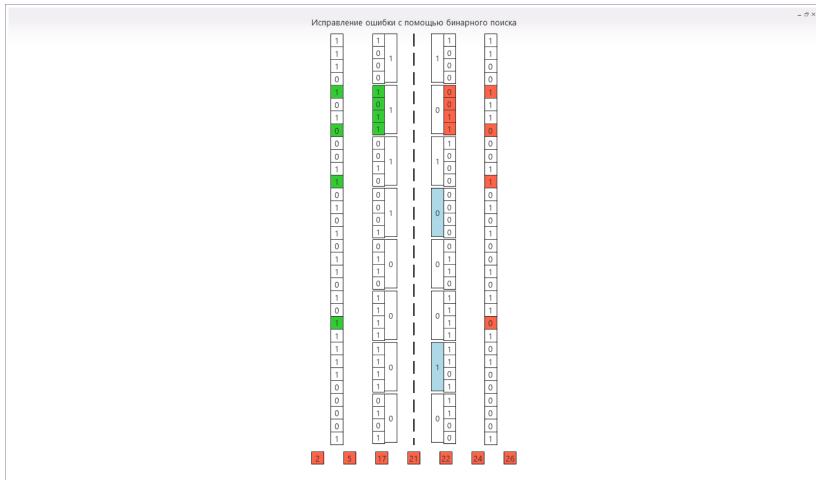
Каскадный метод коррекции ошибок



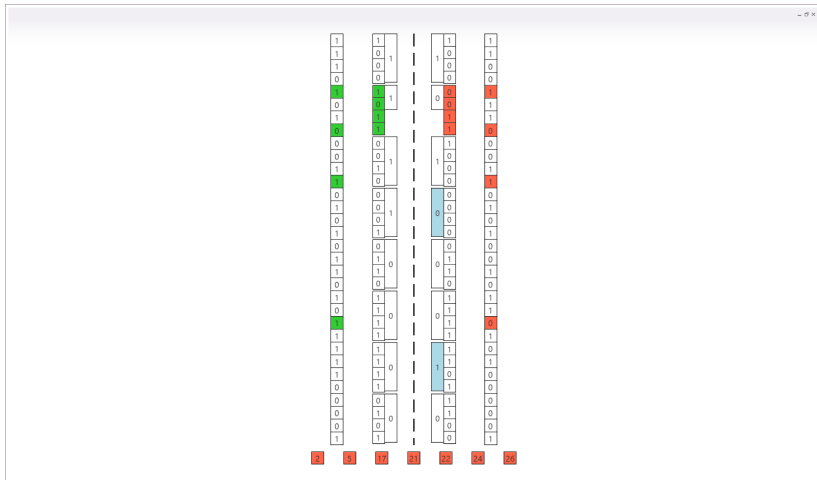
Каскадный метод коррекции ошибок



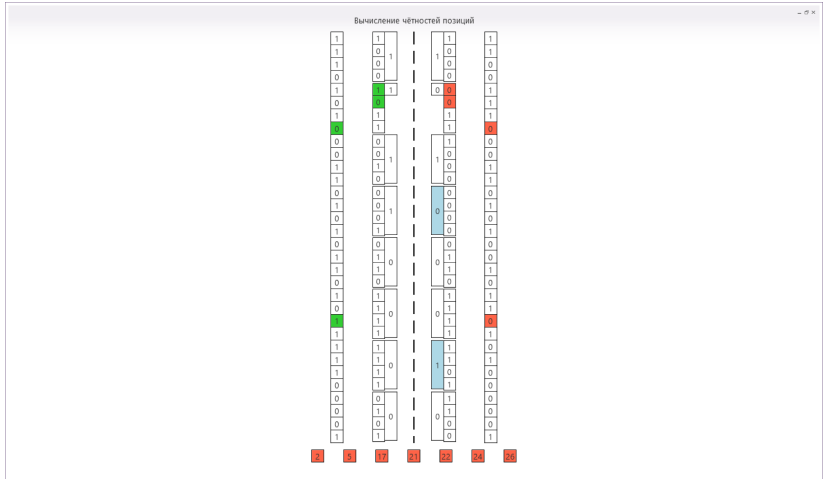
Каскадный метод коррекции ошибок



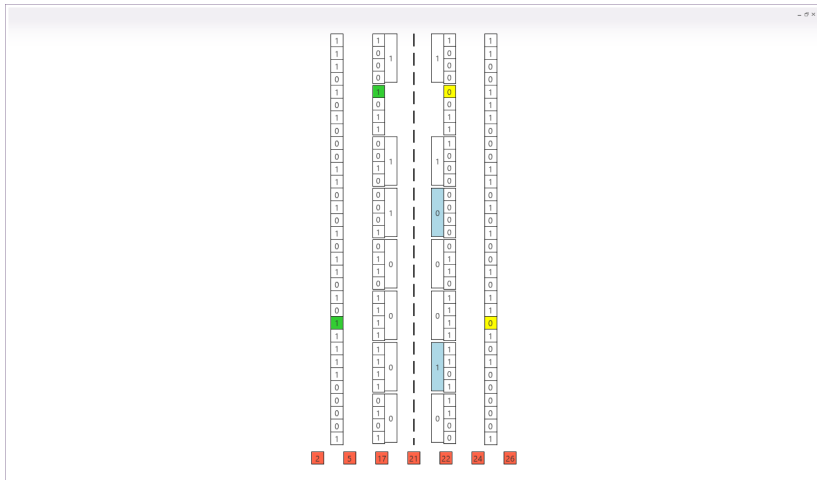
Каскадный метод коррекции ошибок



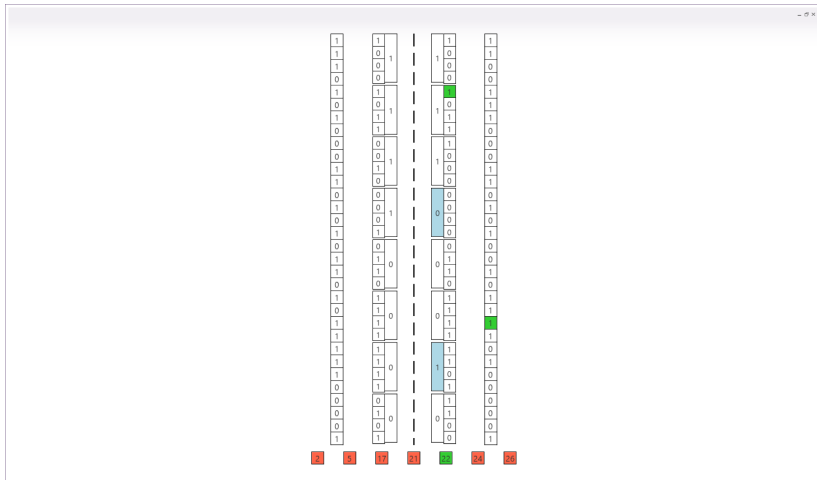
Каскадный метод коррекции ошибок



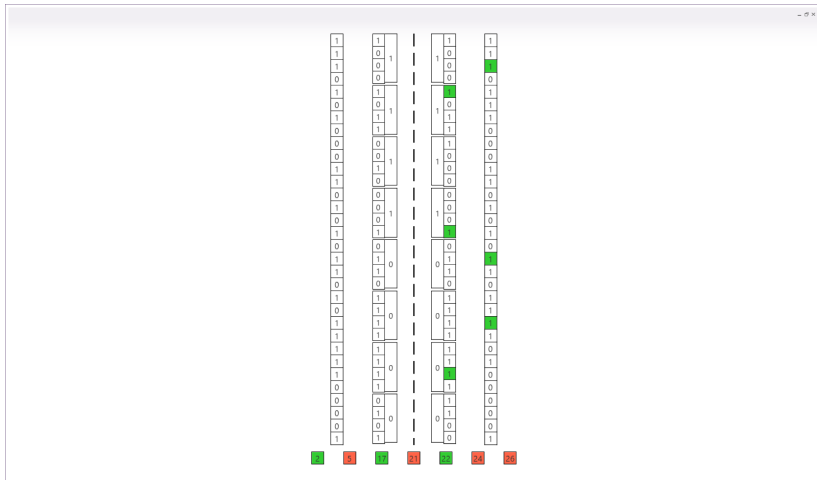
Каскадный метод коррекции ошибок



Каскадный метод коррекции ошибок



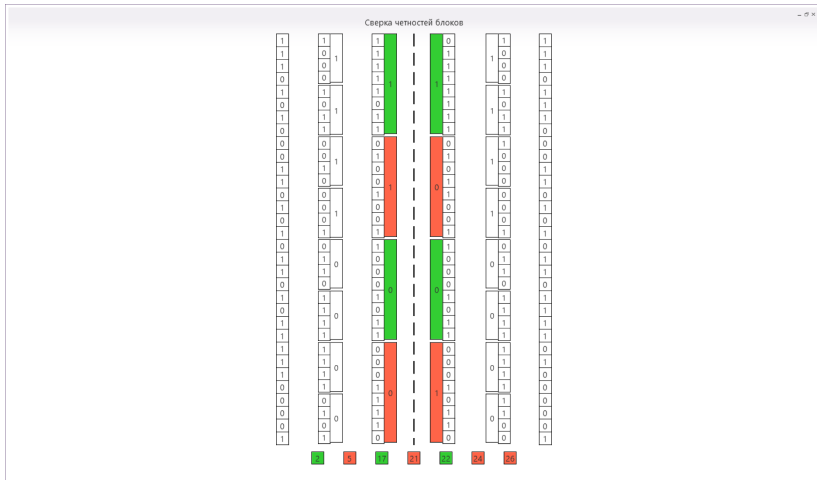
Каскадный метод коррекции ошибок



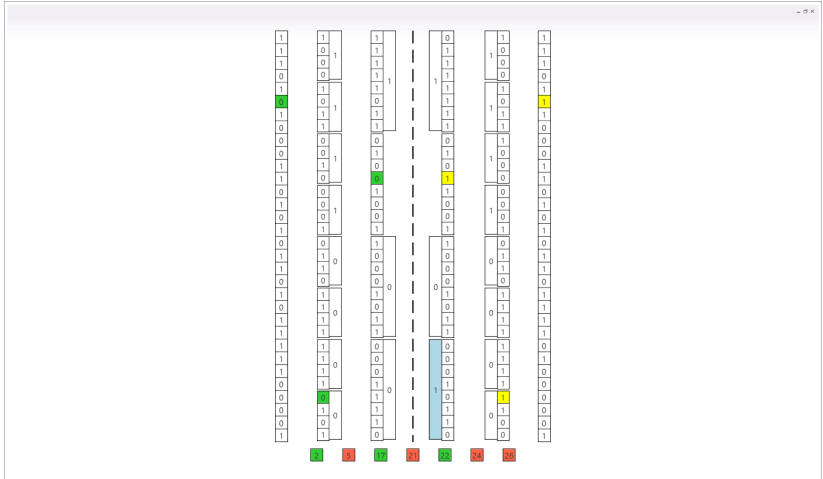
Каскадный метод коррекции ошибок

Выполнение случайной перестановки

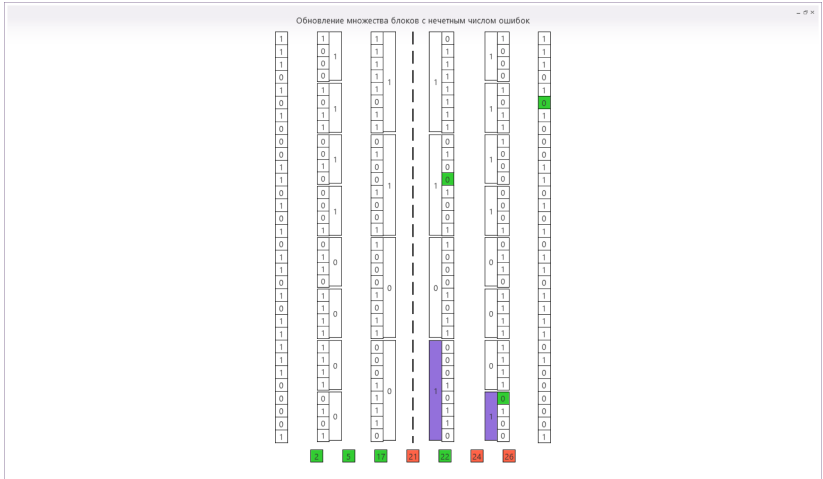
Каскадный метод коррекции ошибок



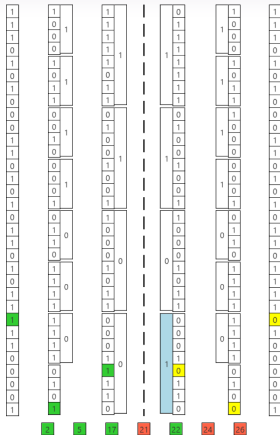
Каскадный метод коррекции ошибок



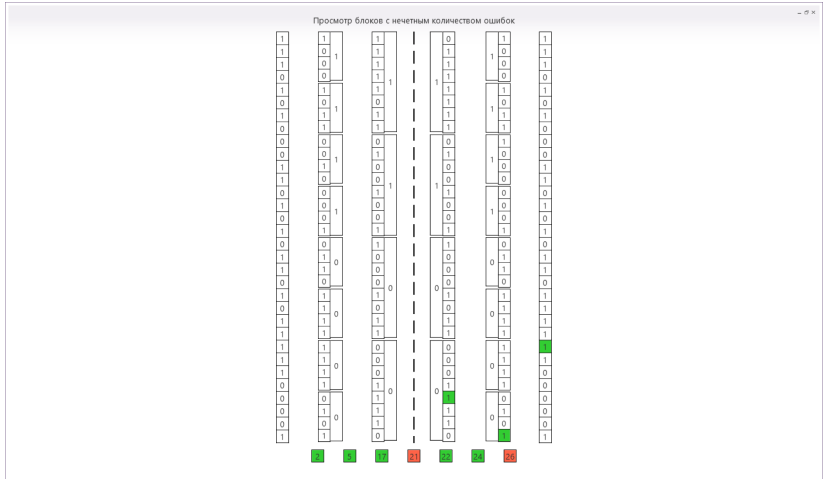
Каскадный метод коррекции ошибок



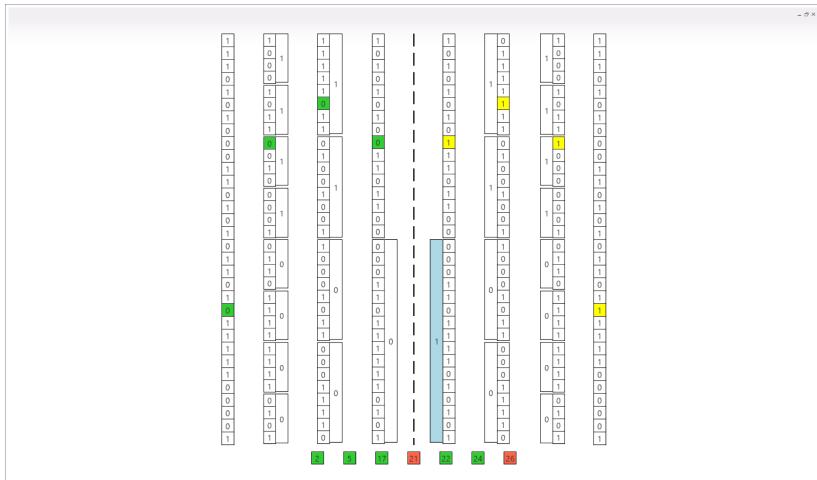
Каскадный метод коррекции ошибок



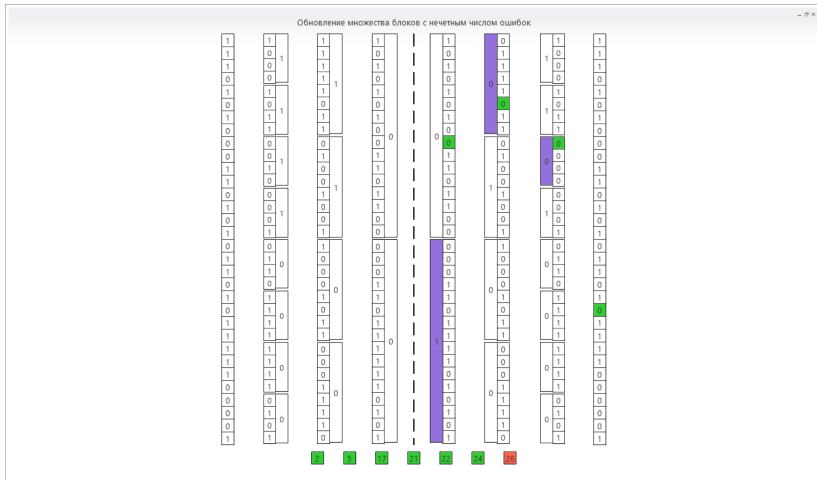
Каскадный метод коррекции ошибок



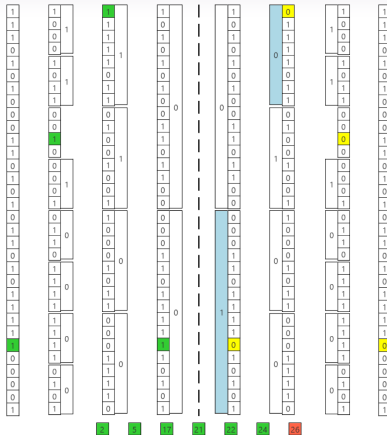
Каскадный метод коррекции ошибок



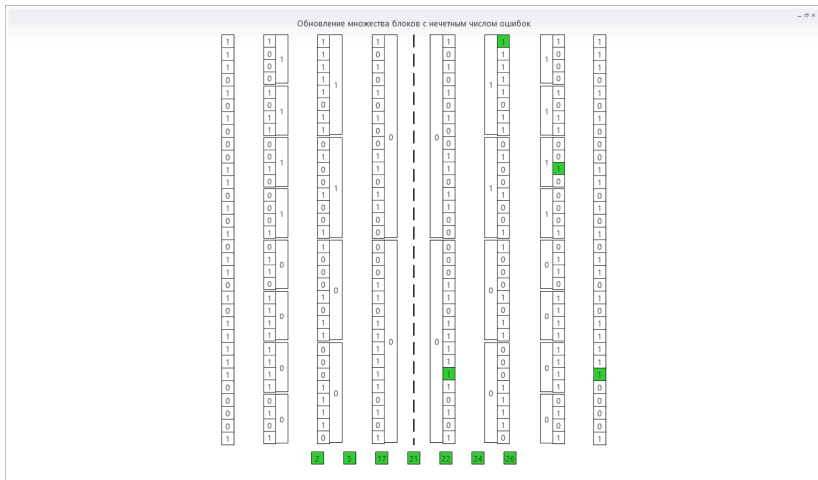
Каскадный метод коррекции ошибок



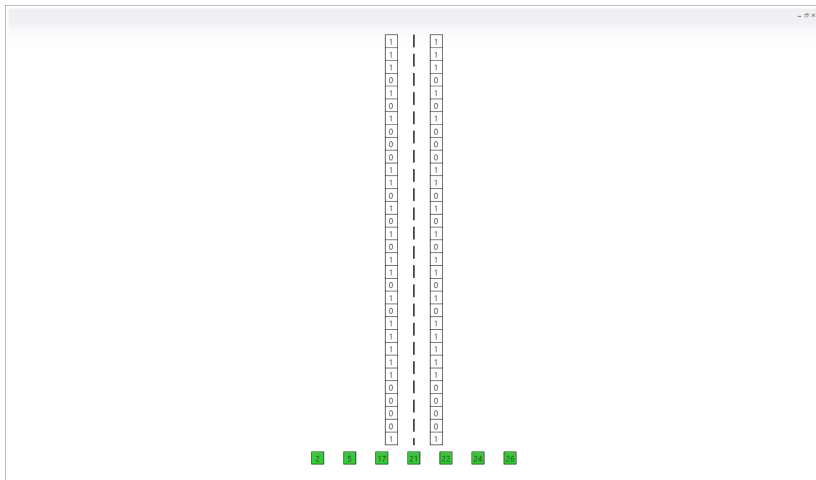
Каскадный метод коррекции ошибок



Каскадный метод коррекции ошибок



Каскадный метод коррекции ошибок



Моделирование релятивистской системы квантового распределения ключей

- └ Исследование каскадного протокола коррекции ошибок
 - └ Каскадный метод коррекции ошибок



Рассматриваемый каскадный протокол коррекции ошибок проходит в несколько шагов. Происходит разбитие ключа на несколько блоков, вычисляется некоторая характеристика каждого блока (например, четность), Алиса посылает свои четности, Боб сверяет со своими, и сообщает, в каких блоках четность не совпала. Эти блоки формируют множество блоков с нечетным числом ошибок, с которым происходит вся дальнейшая работа.

Моделирование релятивистской системы квантового распределения ключей

- Исследование каскадного протокола коррекции ошибок

- Каскадный метод коррекции ошибок



До тех пор, пока это множество не пусто, из него выбирается один блок наименьшего размера, и производится дихотомический поиск ошибки, то есть сначала сравниваются четности первых половин соответствующих блоков. Если они совпадают, то ошибка кроется во второй половине, если различаются — в первой. Таким образом находится позиция, содержащая ошибку.

Моделирование релятивистской системы квантового распределения ключей

- └ Исследование каскадного протокола коррекции ошибок
 - └ Каскадный метод коррекции ошибок



Каскадным протокол называется из-за следующей схемы работы. Все блоки, которые на прошлых проходах содержали в себе только что исправленную позицию, вносятся в множество с нечетным числом ошибок. Если же они там уже были, то удаляются. Таким образом обнаружение ошибки в блоке третьего прохода вызовет каскадное обнаружение ошибки в блоках первого или второго прохода, что в свою очередь вызовет обнаружение ошибки в еще каком-либо блоке, и так до тех пор, пока множество блоков с нечетным числом ошибок не окажется пустым.

Определение

Семейство \mathcal{F} функций $\mathcal{A} \rightarrow \mathcal{B}$ называется *универсальным*, если

$$[f(x_1) = f(x_2)] < \frac{1}{|\mathcal{B}|} \quad \forall x_1, x_2 \in \mathcal{A} : x_1 \neq x_2,$$

а f выбирается из \mathcal{F} в соответствии с равномерным распределением.

Теорема

Пусть X — случайная величина в алфавите \mathcal{X} с вероятностным распределением P_X и энтропией Реньи $R(X)$. Кроме того, пусть G — случайная величина, отвечающая случайному выбору (внутри равномерного распределения) члена универсального семейства хеш-функций, отображающих $\mathcal{X} \rightarrow \{0, 1\}^r$. Тогда

$$H(G(X)|G) \geq R(G(X)|G) \geq r - \frac{2^{r-R(X)}}{\ln 2}. \quad (1)$$

2015-04-27

Моделирование релятивистской системы квантового распределения ключей

└ Исследование каскадного протокола коррекции
ошибок

└ Сжатие полученного ключа

Теорема

Пусть X — случайная величина в алфавите \mathcal{X} с вероятностным распределением P_X и энтропией Ренни $H(X)$. Кроме того, пусть G — случайная величина, отвечающая случайному выбору (внутреннему равномерному распределению) члена универсального семейства хеш-функций, отображающих $\mathcal{X} \rightarrow \{0, 1\}^r$. Тогда

$$H(G(X)|G) \geq R(G(X)|G) \geq r - \frac{2^r - R(X)}{\ln 2}. \quad (1)$$

После проведения процедуры коррекции ошибок Алисе и Бобу известно примерное количество информации, которое могло стать доступным Еве в ходе работы протокола распределения ключей и коррекции ошибок. Зная эту величину, они могут провести сжатие ключа путем хеширования функциями из универсального семейства хеш-функций, определение которых вы видите на слайде. Сама хеш-функция выбирается случайным образом из заранее известного универсального семейства хеш-функций, то есть является случайной величиной. В результате Алиса и Боб получают ключ меньшей длины, но информация Евы о нем будет бесконечно малой. В итоге цель достигнута: стороны имеют общий секретный ключ, о котором злоумышленник ничего не знает.

- 1 Показано существование и дано обоснование секретности протокола квантовой криптографии, обеспечивающего безусловную секретность в условиях потерь в линии связи и неоднофотонности источника.
- 2 Рассмотрен и проанализирован один из протоколов коррекции ошибок, который в настоящее время является стандартом в квантовом распределении ключей.
- 3 Разработаны программы, визуализирующие процессы:
 - распределения ключей по релятивистскому протоколу с имитацией атак подслушателя и последующим детектированием возникающих из-за этого задержек,
 - коррекции ошибок по протоколу Cascade.

Моделирование релятивистской системы квантового распределения ключей

└ Описание практической реализации и полученных результатов

└ Полученные результаты

- 1 Показано существование и дано обоснование секретности протокола квантовой криптографии, обеспечивающего безусловную секретность в условиях потерь в линии связи и неоднотонности источника.
- 2 Рассмотрен и проанализирован один из протоколов коррекции ошибок, который в настоящее время является стандартом в квантовом распределении ключей.
- 3 Разработаны программы, визуализирующие процессы:
 - распределение ключей по релятивистскому протоколу с имитацией атак подслушателя и последующим детектированием возникающих из-за этого задержек,
 - коррекции ошибок по протоколу Cascade.

Для моделирования и визуализации релятивистского протокола квантового распределения ключей и каскадного протокола коррекции ошибок было написано две программы. Обе написаны на языке C#, требуют установленного .NET 4.5, используют шаблон проектирования MVVM, и богатые возможности платформы Windows Presentation Framework (WPF) по анимации контента. Снимки экрана программы коррекции ошибок были показаны ранее, а сейчас я хочу продемонстрировать основную разработку - визуализация релятивистского протокола, пока позволяет время.

Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Большаков Роман Алексеевич
Научный руководитель: профессор,
д.ф-м.н. Молотков С.Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

Москва, 2015