Моделирование релятивистской системы квантового распределения ключей

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.

Речь пойдет о квантовом распределении ключей, что является синонимом квантовой криптографии. Квантовая криптография решает центральную проблему классической криптографии — секретное распределение ключей через открытые каналы, причем секретность гарантируется фундаментальными законами природы, что позволяет делать предположения о неограниченных вычислительных возможностях злоумышленника.

Моделирование релятивистской системы квантового распределения ключей

Проблемы практических реализаций

Основные практические проблемы имеющихся на данный момент протоколов:

- лазер испускает когерентное состояние: $|\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\sqrt{\mu}}{\sqrt{n!}} |n\rangle = e^{-\frac{\mu}{2}} (|0\rangle + \sqrt{\mu}|1\rangle + \frac{\mu}{\sqrt{2}}|2\rangle + \dots)$, где μ — среднее число фотонов в одном импульсе;
- потери в канале связи.

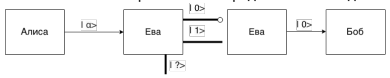
Носителем *ключевой* информации в идеале должны быть одиночные фотоны, но на данный момент не существует строго однофотонного источника. Реально же используется сильно ослабленное лазерное излучение, которое представляет из себя суперпозицию состояний с различным числом фотонов (см формулу).

Нестрогая однофотонность источника *совместно* с потерями в канале связи приводят к ряду новых атак, например, к атаке с расщеплением по числу фотонов.

Моделирование релятивистской системы квантового распределения ключей

Атака на нерелятивистские протоколы

При указанных проблемах становится осуществима атака, основанная на измерениях с неопределенным исходом.



Если $Pr_{loss} > Pr_?$ — подслушиватель знает весь ключ и остается незамеченным.

Эта атака устроена следующим образом. Ева (злоумышленник) может разорвать канал в двух местах и проводить так называемые измерения с неопределенным исходом.

Эти измерения приводят к тому, что, начиная с некоторого уровня потерь, Ева знает ключ, не производит ошибок на приемной стороне и не детектируется.

Моделирование релятивистской системы квантового распределения ключей

Решение проблем

Нерелятивистские протоколы используют только ограничения квантовой механики.
Но:

- фотоны движутся со скоростью света (как все безмассовые частицы),
- а скорость света — предельно допустимая скорость распространения взаимодействий.

Квантовая механика + СТО = релятивистский протокол.

Поэтому фундаментальных ограничений *только* квантовой механики на измеримость квантовых состояний оказывается недостаточно, чтобы обеспечить секретность ключей при больших потерях. А при передаче через открытое пространство потери достигают 5-6 порядков.

Но в открытом пространстве есть еще ограничение на движение со скоростью света, а именно — никакое взаимодействие не может распространяться быстрее скорости света.

Поэтому в релятивистских протоколах детектируются не только ошибки, но и задержки на приемной стороне.

Моделирование релятивистской системы квантового распределения ключей

Цель дипломной работы

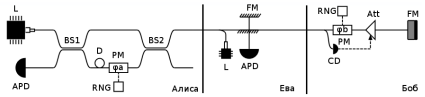
Целью данной дипломной работы является создание программных средств:

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.

Моделирование релятивистской системы квантового распределения ключей

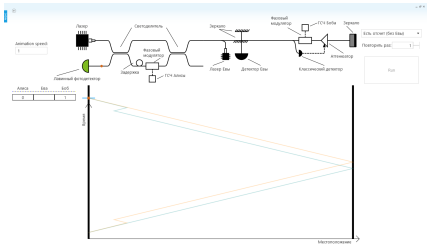
Схема релятивистского протокола



Принципиальная схема протокола показана на слайде. Суть протокола сводится к, скажем так, «размазыванию» информации в протяженное квантовое состояние таким образом, что по отдельности части этого состояния не несут никакой полезной информации. Для того, чтобы получить информацию о ключе, эти части нужно свести в одну точку пространства, на что требуется конечное время.

Моделирование релятивистской системы квантового распределения ключей

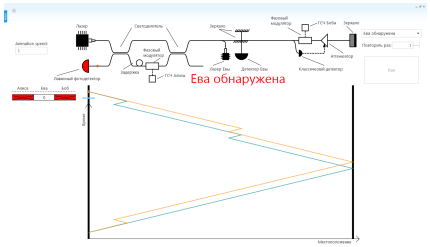
Схема релятивистского протокола



Расстояние между участниками коммуникации всем известно и является параметром протокола. Алиса (слева) включает свой детектор только в определенные временные промежутки, когда, по ее расчетам, должно прийти ответное состояние.

Моделирование релятивистской системы квантового распределения ключей

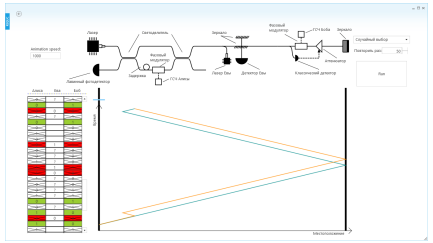
Схема релятивистского протокола



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

Моделирование релятивистской системы квантового распределения ключей

Схема релятивистского протокола



В результате в ключ попадет информация только из тех посылок, где Алиса получила состояние вовремя, все остальные будут отброшены

Моделирование релятивистской системы квантового распределения ключей

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). После чистки ошибок требуется хэширования ключа.

Моделирование релятивистской системы квантового распределения ключей

Каскадный метод коррекции ошибок

Каскадный протокол коррекции ошибок является итерационной процедурой в отличие от стандартных процедур коррекции. Протокол проходит в несколько шагов, на каждом из которых исходный ключ случайным образом перемешивается, разбивается на блоки, сравниваются их четности. В блоках с несовпадающими четностями содержится как минимум одна ошибка. Каскадным он называется из-за того, что если была найдена ошибка в каком-либо блоке, то инициируется поиск ошибки во всех блоках, которые до этого содержали найденную позицию, ситуация поясняется на слайде.

Моделирование релятивистской системы квантового распределения ключей

Сжатие полученного ключа

Определение

Семейство $\mathcal{F}$ функций $\mathcal{A} \to \mathcal{B}$ 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.

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 которого приведено на слайде. Сама хеш функция выбирается случайным образом из заранее заданного универсального семейства хеш-функций, то есть является случайной величиной. В результате Алиса и Боб получат ключ меньшей длины, но информация Евы о нем будет бесконечно малой. В итоге цель достигнута: две легитимные стороны имеют общий секретный ключ, о котором злоумышленник ничего не знает.

Моделирование релятивистской системы квантового распределения ключей

Полученные результаты

1. Проведен детальный анализ, моделирование и визуализация протокола квантовой криптографии, обеспечивающего безусловную секретность в условиях потерь в линии связи и неоднофотонности источника с обоснованием секретности.
2. Рассмотрен и смоделирован (в виде отдельной программы) один из протоколов коррекции ошибок, который в настоящее время является стандартом в квантовом распределении ключей.

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.