МАТЕМАТИЧЕСКИЕ ОСНОВЫ КВАНТОВОЙ КРИПТОГРАФИИ

к.ф.-м.н. Д. А. Кронберг
к.ф.-м.н. А. С. Трушечкин

Аннотация

Квантовая криптография – современное направление науки, в котором изучаются методы обеспечения безопасной связи, основанные на принципах квантовой механики. В отличие от традиционной криптографии, в которой эта задача решается при помощи математических преобразований информации, квантовая криптография основывается на невозможности в общем случае считывания информации с квантового носителя без внесения в неё шума. Это позволяет обнаружить факт прослушивания ещё до того, как будет передана собственно полезная информация.

Несмотря на простоту этого принципа, строгое доказательство стойкости квантовой криптографии потребовало построения сложной и красивой математической теории, в основе которой лежат теория различения квантовых состояний, теория квантовых сцепленных состояний, теория исправления квантовых ошибок (в частности, фундаментальную роль играют так называемые фазовые, неклассические ошибки), квантовые энтропийные характеристики, в частности энтропийные соотношения неопределённостей. Целью курса является ознакомление слушателей с методами доказательства стойкости протоколов квантовой криптографии.

От слушателей требуется знание математического анализа, линейной алгебры, теории вероятностей. Знание квантовой механики необязательно.

Курс не ставит своей целью ознакомление со всем многообразием современных направлений квантовой криптографии: с различными протоколами, элементной базой, проблемами практических реализаций и т.д. Мы ограничимся только наиболее широко используемым (и исторически первым) протоколом квантовой криптографии BB84, включая случаи несовершенного оборудования, но сами методы применимы и к анализу стойкости других протоколов.

Предполагается, что после прохождения курса слушатели будут понимать основные методы доказательства стойкости протоколов квантовой криптографии, уметь применять эти методы, понимать современные работы, посвящённые этим вопросам.

Предварительная программа

Часть I. Введение. Цель этой части – дать введение в квантовую криптографию, понять на простых примерах её принципы и особенности, установить количественную характеристику степени стойкости протоколов квантовой криптографии.

Неделя 1. Проблема распределения ключей в криптографии. Аксиоматика квантовой информатики (состояния, наблюдаемые, унитарные преобразования). Протокол квантовой криптографии (квантового распределения ключей) BB84.

Практические задачи: вычисление вероятностей исходов измерений, различение квантовых состояний.

Неделя 2. Простейшая атака “перехват–перепосыл”. Виды атак: индивидуальные, коллективные, когерентные. Классически-квантовые состояния. Параметр стойкости протокола.

Практические задачи: различные атаки на протокол BB84, иллюстрация принципа, что прослушивание вносит ошибки.

Неделя 3. Параметр стойкости протокола (продолжение): следовое расстояние и его свойства. Вероятность различения и вероятность угадывания. Теорема Холево–Хельстрома. Точность воспроизведения (“fidelity”).

Практические задачи: вычисление следового расстояния и точности воспроизведения, различение квантовых состояний.

Часть II. Доказательство стойкости протокола BB84 через сведение к дистилляции сцепленности. Цель этой части – дать простое и наглядное доказательство стойкости протокола BB84, распространить и обобщить его на случай различных несовершенств оборудования. В этой части мы выведем формулу, которую можно считать основной формулой квантовой криптографии, связывающую информацию подслушивающей стороны с долей фазовых (т.е. неклассических) ошибок. Формула Деветака–Винтера и энтропийные соотношения неопределённостей обобщают эту формулу и будут даны в этой части без доказательства. Также в конце этого раздела будет рассказано об одной из новейших техник: сведении вычисления предельной скорости генерации секретного ключа к решению задачи выпуклого программирования. Ряд результатов здесь принадлежит одному из лекторов.

Недели 4. Сцепленные состояния и их свойства. Энтропия как мера неопределённости. Энтропия фон Неймана и энтропия Шеннона. Теоремы кодирования.

Практические задачи: определение, сцепленное ли состояние или разделимое. Вычисление энтропий.

Недели 5–7. Классическое и квантовое исправление ошибок. Доказательство стойкости протокола BB84 через сведение к дистилляции сцепленности. Основная формула квантовой криптографии.

Неделя 8. Протокол BB84 с когерентными состояниями. Метод обманных состояний (состояний-ловушек).

Практические задачи: атака расщеплением по числу фотонов, расчет максимальной длины линии связи при отсутствии обманных состояний.

Недели 9–10. Методы доказательства стойкости BB84 при неидеальном источнике.

Неделя 11. Формула Деветака–Винтера и энтропийные соотношения неопределённостей. Квантовая относительная энтропия. Скорость генерации секретного ключа как решение задачи выпуклого программирования.

Практические задачи: вычисление предельной скорости генерации секретного ключа при различных атаках.

Неделя 12. Скорость генерации секретного ключа как решение задачи выпуклого программирования (продолжение). Доказательство стойкости протокола BB84 при неравных эффективностях однофотонных детекторов.

Часть III. Доказательство стойкости протокола BB84 через энтропийные характеристики. Эта часть будет посвящена уже более общей и более математически сложной теории, связанной с квантовыми энтропиями Реньи. Целью является доказательство стойкости процедуры усиления секретности (одна из ключевых процедур в протоколах квантовой криптографии) и, следовательно, вывод одного из двух слагаемых в формуле Деветака–Винтера, и доказательство энтропийных соотношений неопределенностей. Завершим мы курс рассказом об одной из новейших техник – теореме о накоплении энтропии, которая позволяет обобщать доказательство стойкости к коллективным атакам на случай атак общего вида (когерентных атак) и учитывать эффекты конечной длины ключа (в отличие от асимптотического анализа стойкости, который излагался до этого).

Неделя13. Мин-энтропия и макс-энтропия. Сглаженные энтропии. Теорема об асимптотической равнораспределённости на языке квантовых сглаженных мин- и макс-энтропий.

Практические задачи: вычисление мин- и макс-энтропий.

Неделя 14. Усиление секретности. Теорема об остаточной информации после хеширования. Переход к формуле Деветака–Винтера.

Неделя 15. Доказательство энтропийных соотношений неопределённостей. Теорема о накоплении энтропии и её применение к квантовой криптографии.