Квантовая криптография

Автор
д.ф.-м.н С.Н.Молотков

Содержание дисциплины.
Содержание лекций 6 семестр.
Лекция 1.
Одноразовые ключи. Критерий Шеннона абсолютной секретности.
Квантово-механические запреты на копирование неизвестного квантового состояния. Основные стадии квантовых протоколов распределения ключей. Источники, детекторы, носители. Существующие достижения в квантовой криптографии.
Лекция 2. Основные протоколы квантового распределения ключей и их реализации: BB84, B92, E91, SARG04.
Лекция 3. Продолжение. Основные протоколы квантового распределения ключей и их реализации: фазово-временное кодирование, дифференциально-фазовое кодирование.
Лекция 4. Продолжение. Основные протоколы квантового распределения ключей и их реализации: релятивистское квантовое распределение ключей через открытое пространство с синхронизацией и без синхронизации часов на приемной и передающей стороне. Релятивистские квантово-механические запреты на копирование квантовых состояний..
Лекция 5. Основы математического аппарата. Определение и критерии секретности. Критическая ошибка протоколов квантового распределения ключей.
Лекция 6. Достижимая информация подслушивателя. Связь с квантовыми пропускными способностями.
Лекция 7.Индивидуальные и коллективные измерения в квантовой криптографии. Множественность атак подслушивателя, связь атак с пропускными способностями квантового канала.
Лекция 8. Фундаментальная граница Холево для достижимой классической информации.
Лекция 9. Исправление ошибок в первичных ключах в квантовой криптографии. Классические энтропии Реньи и их роль в квантовой криптографии. Усиление секретности – классический вариант.
Лекция 10. Универсальные хэш-функции второго рода, использование в процедурах усиления секретности и коррекции ошибок.
Лекция 11. Доказательство секретности квантового распределения ключей для различных протоколов. Пример протокола BB84. Первые доказательства секретности для атак: прием-перепосыл, прозрачной атаки с индивидуальными и коллективными измерениями. Критические ошибки протокола для различных видов атак в асимптотическом пределе бесконечно длинных последовательностей передаваемых ключей.
Лекция 12. Пример двухпараметрического протокола квантовой криптографии. Доказательство секретности квантового распределения ключей для квантовой криптографии с фазово-временным кодирование (асимптотический предел)). Критическая ошибка протокола при коллективной атаке.
Лекция 13. Анализ стойкости протокола квантового распределения ключей SARG04.
Лекция 14. Квантовые протоколы распределения ключей, использующие когерентные состояния. Необходимые сведения из теории когерентных состояний. Преобразование на

линейных оптических элемента, детектирование когерентных состояний, включая гомодинное детектирование.

Лекция 15. Анализ стойкости протокола квантового распределения ключей на геометрически однородных когерентных состояниях.

Лекция 16. Квантовая криптография на непрерывных переменных.

Содержание лекций 7 семестр.

Лекция 17. Методы практической чистки первичных ключей и методы сжатия (хэширования – усиления секретности) ключей в квантовой криптографии.

Лекция 18. Методы коррекции ошибок основанные на классических кодах корректирующих ошибки. Итерационные адаптивные процедуры исправления ошибок.

Лекция 19. Анализ стойкости реализаций систем квантовой криптографии с не идеальными источниками квантовых состояний, детекторами и квантовым каналом связи с потерями. Атака с расщеплением по числу фотонов.

Лекция 20. Атака с подменой фазы в системах с фазовым кодированием. Атака с ослеплением фотодетекторов.

Лекция 21. Протоколы устойчивые по отношению к атаке с ослеплением фотодетекторов. Побочные каналы утечки информации в системах квантовой криптографии, фундаментальная квантово-механическая верхняя граница на утечку информации по побочным каналам.

Лекция 22. Основы математического аппарата для анализа стойкости систем квантовой криптографии с конечными длинами передаваемых последовательностей. Критерий составной секретности ключей, основанный на следовом расстоянии.

Лекция 23. Основные свойства квантовых энтропий Реньи (min и max энтропий).

Сглаженные min и max энтропии, цепочечные правила, изменение min и max энтропий при действии супероператора, свойства min и max энтропии для составных квантовых систем.

Лекция 24. Teopems de Finetti классический и квантовые случаи. Min и max энтропий для тензорного произведения матриц плотности.

Лекция 25. Симметричные состояния. Min и max энтропий для симметричных состояний.

Лекция 26. Необходимые неравенства для различных расстояний между квантовыми состояниями.

Лекция 27. Коррекция ошибок с минимальной утечкой информации при помощи универсальных хэш-функций второго порядка.

Лекция 28. Квантовое усиление секретности. Квантовая теорема усиления секретности – теорема об остатке хэширования.

Лекция 29. Примеры доказательств секретности BB84 и фазово-временной квантовой криптографии с использованием аппарата квантовых min и max энтропий (асимптотический предел).

Лекция 30. Энтропийные соотношения неопределенностей в квантовой криптографии. Связь с min и max энтропиями.

Лекция 31. Анализ стойкости квантового протокола распределения ключей BB84 с конечными передаваемыми последовательностями (доказательство с использованием энтропийных соотношений неопределенности).

Лекция 32. Доказательства стойкости фазово-временной и релятивистской квантовой криптографии для открытого пространства с конечными длинами последовательностей с использованием аппарата квантовых min и max энтропий.