Квантовая связь

Содержание курса**:**

1. Вводная лекция. Классический и квантовый мир. История криптографии. Демонстрация разрушения квантового состояния при измерении. Обзор содержания курса.
2. Основы квантовой оптики. Квантовые состояния света и операции с ними. Кубиты и способы их оптического кодирования. Сфера Блоха.
3. Основы квантовой оптики (продолжение). Квантовые измерения. Теорема о запрете клонирования.
4. Компоненты однофотонных систем. Источники фотонов и когерентных состояний. Модуляторы. Интерферометры в однофотонном режиме. Детекторы фотонов. Примеры применений: детектор бомбы (измерение без воздействия на объект), квантовые генераторы случайных чисел.
5. Введение в квантовую криптографию. Протокол BB84. Последовательность процедур извлечения секретного ключа. Неидеальность источника и протокол с состояниями-ловушками. Протоколы с дифференциальным фазовым кодированием.
6. Реализации квантовой криптографии. Свойства оптического волокна и открытого оптического канала. Волоконные, атмосферные и спутниковые системы и их основные характеристики. Сети передачи ключей. Сопряжение с шифраторами. Коммерциализация.
7. Квантовая перепутанность. Теория перепутанных (связанных) состояний. Способы генерации перепутанных состояний фотонов. Улучшенный источник одиночных фотонов, пассивное приготовление случайных состояний. Примеры применений: квантовая телепортация, квантовые повторители.
8. Доказательства безопасности. Энтропия, пропускная способность каналов, граница Холево, оптимальное клонирование. Доказательство безопасности протокола BB84 с состояниями-ловушками.
9. Классическая обработка данных для извлечения секретного ключа. Математические функции обработки данных с доказанными свойствами. Коррекция ошибок. Хэш-функции и усиление доверительности. Аутентификация.
10. Доказательство квантовой природы мира. Неравенства Белла и их экспериментальное тестирование. Устройство-независимые протоколы квантовой криптографии: E91, полностью устройство-независимые, с независимым измерительным устройством.
11. Квантовый взлом. Практические уязвимости устройств квантовой связи. Примеры неидеальностей реализации, атак и способов защиты.
12. Сертификация коммерческих криптографических устройств. Государственные требования к качеству реализации и процедурам сертифицирования. Анализ безопасности реализации квантовой части систем криптографии на примере полной системы квантовой передачи ключа.
13. Другие задачи квантовой связи. Принципиальные преимущества квантовой связи перед классической. Прямое квантовое шифрование. Распределенное хранение ключа и данных. Квантовая контрольная сумма. Квантовая подпись. Квантовое делегированное вычисление. Квантовая блочная цепь.
14. Последние достижения в области.
15. Дискуссия и консультации.