

«УТВЕРЖДАЮ»

И.о. декана физического факультета МГУ

профессор Белокуров В.В.



БИЛЕТЫ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Направление подготовки 03.04.02 «Физика»

Магистерская программа

«ПРИКЛАДНАЯ КВАНТОВАЯ СВЯЗЬ»

Билет №1

1. Структура волоконных световодов. Контраст показателя преломления и полное внутреннее отражение. Числовая апертура.
2. Алгоритм Гравера для поиска в неструктурированной базе данных.
3. Связь статистики фотоотчетов со статистикой фотонов при квантовом и полуклассическом подходах в теории детектирования оптических полей.

Билет №2

1. Моды волоконных световодов. Длина волны отсечки второй моды. Одномодовые и многомодовые световоды, их типичные характеристики.
2. Гейтовая модель квантовых вычислений- одно- и двухкубитные вентили, условные вентили, описание измерений.
3. Оптические потери в оптоволоконных линиях связи. Дисперсия в световодах: межмодовая дисперсия, материальная дисперсия, волноводная дисперсия.

Билет №3

1. Универсальные наборы квантовых вентилей.
2. Приготовление перепутанных состояний света в процессе спонтанного параметрического рассеяния света: перепутывание по поляризации, пространству и по частоте-времени.
3. Интерпретация следового расстояния и фиделити, связь с вероятностью угадывания.

Билет № 4

1. Способы визуализации квантовых состояний света. Измерение квадратурных наблюдаемых в условиях конечной квантовой эффективности детекторов фотонов. Дробное преобразование Фурье.
2. Основные понятия классической теории информации. Энтропия Шеннона, условная энтропия, взаимная информация, свойства. Понятие типичных последовательностей, теорема об асимптотической равномерности.
3. Атаки на системы КРК с активным зондированием (Trojan horse) и с ослеплением однофотонного детектора. Цели атак, принципы реализации, методы защиты.

Билет №5

1. Двухмодовый однофотонный кубит: поляризационное, пространственное и временное кодирование. Приготовление, преобразование и измерение.
2. Квантовое преобразование Фурье И алгоритм оценки фазы.
3. Протокол квантовой криптографии BB84

Билет №6

1. Фазовая модуляция (BPSK, QPSK). Амплитудно-фазовая модуляция (QAM). Квадратурная диаграмма. Спектральная эффективность канала.
2. Квантовые коды коррекции ошибок. Девятикубитный код Шора.
3. Функции Вигнера, Хусими и Глаубера-Судоршана, их характеристические функции, связь между ними.

Билет №7

1. Квантование электромагнитного поля в вакууме: разложение по модам, обобщенные координаты (квадратуры), операторы рождения и уничтожения фотонов. Физический смысл квадратур поля для бегущей и для стоячей волны. Способ их измерения. Соотношение неопределенностей для квадратур.
2. Спектральное уплотнение каналов (WDM). Сетка частот ITU. Временное уплотнение каналов (TDM).
3. Свойства энтропии фон Неймана квантовой системы и составных квантовых систем. Фундаментальная граница информации Холево для квантового ансамбля.

Билет №8

1. Физические источники случайности. Классическая и квантовая случайность. Связь с нарушением неравенств Белла и теорией скрытых переменных.
2. Супероператор - вполне положительное отображение матриц плотности. Представление Крауса. Представление супероператора через совместную эволюцию составной квантовой системы. Связь представления Крауса с POVM.
3. Базис фоковских состояний света. Базис квадратурных состояний света. Когерентные состояния света.

Билет № 9

1. Квантовое описание светоделителя: преобразование фоковских и когерентных состояний. Преобразование функций распределения по когерентным состояниям. Описание потерь. Изменение функций распределения по когерентным состояниям под действием потерь, Гамильтониан светоделителя. Реализация операторов рождения, уничтожения и сдвига с помощью светоделителя.
2. Экстракция случайности с помощью детерминистических алгоритмов. Метод Фон-Неймана и его обобщение для большего размера алфавита.
3. Примеры источников неклассического света.

Билет № 10

1. Основные информационные протоколы - квантовая телепортация, сверхплотное кодирование, квантовое распределение ключей.
2. Квантовые вычисления, устойчивые к ошибкам: основные понятия, пороговая теорема.

3. Обобщенные неортогональные измерения, положительно-значные операторные меры (POVM). Измерения с определенным исходом. Связь неортогональных измерений с составными системами.

Билет № 11

1. Базис фоковских состояний. Понятие неразличимости. Эффект Хонга-Оу-Манделя. N-портовый интерферометр. Имманант, перманент и детерминант матрицы. Преобразование входного фоковского состояния линейным интерферометром, связь коэффициентов выходного состояния в фоковском базисе и перманентов матрицы. Постселекция выходных состояний. Протокол квантовой криптографии B92. Тестирование на случайность. Различие истинно-случайных и псевдослучайных последовательностей. Принципы тестирования. Примеры вариантов тестов.

Билет № 12

1. Протокол квантовой криптографии BB84
2. Функции Вигнера, Хусими и Глаубера-Судоршана, их характеристические функции, связь между ними.
3. Когерентные состояния, основные свойства. Преобразование когерентных состояний на линейных оптических элементах (светоделитель, канал с потерями, интерферометр Маха-Цандера, детектирование).

Билет № 13

1. Энтропийные соотношения неопределенности
2. Протокол квантовой криптографии E91.
3. Теорема о запрете клонирования (no cloning). Протокол квантовой телепортации. Телепортация в системе тождественных частиц.

Билет № 14

1. Принципы оценки угроз взлома систем КРК. Атаки на протоколы КРК. Атаки на техническую реализацию.
2. Парадокс ЭПР и неравенства Белла.
3. Модель источника фотонов. Современные источники фотонов. Примеры. Принципы работы.

Билет № 15

1. Модель детектора фотонов. Учет конечной квантовой эффективности. Учет временных характеристик детектора. Детектор с разрешением по числу

- фотонов. Типы современных детекторов одиночных фотонов.
2. Атаки на протоколы КРК. Различия между однофотонными и когерентными состояниями в вопросе гарантии секретности распределяемых ключей. Возможные модификации однофотонных протоколов для работы с когерентными состояниями.
 3. Когерентные состояния, основные свойства. Преобразование когерентных состояний на линейных оптических элементах (светоделитель, канал с потерями, интерферометр Маха-Цандера, детектирование).

Билет № 16

1. Меры близости квантовых состояний. Следовое расстояние, свойства. Фиделити, свойства. Связь фиделити и следового расстояния.
2. Атаки на системы КРК с активным зондированием (Trojan horse) и с ослеплением однофотонного детектора. Цели атак, принципы реализации, методы защиты.
3. Приготовление перепутанных состояний света в процессе спонтанного параметрического рассеяния света: перепутывание по поляризации, пространству и по частоте-времени.

Билет № 17

2. Спонтанное параметрическое рассеяние света. Пространственный спектр СПР. Частотно-временной спектр СПР
3. Квантование электромагнитного поля в вакууме: разложение по модам, обобщенные координаты (квадратуры), операторы рождения и уничтожения фотонов. Физический смысл квадратур поля для бегущей и для стоячей волны. Способ их измерения. Соотношение неопределенностей для квадратур.
4. Принципы оценки угроз взлома систем КРК. Атаки на протоколы КРК. Атаки на техническую реализацию.