

Оглавление

Введение	3
1. Постановка задачи и обзор методов классической криптографии	11
Контрольные вопросы по разделу 1	27
2. Квантовая теория информации и ее основные понятия	29
2.1. Основные определения, связанные с квантовыми состояниями	30
2.2. Процедура измерения квантовых состояний	34
2.3. Квантовые системы из нескольких частиц	37
2.4. Квантовые каналы передачи информации	43
2.4.1. Представление Крауса и определение квантового канала	45
2.4.2. Основные примеры квантовых каналов	46
2.4.3. Пропускная способность s - q -канала	49
2.5. Коды коррекции ошибок в квантовом случае	51
2.5.1. Коды, исправляющие ошибку в одном кубите	52
2.5.2. Линейные коды	54
2.5.3. Коды Кальдербанка–Шора–Стина	55
Контрольные вопросы по разделу 2	56
3. Классический протокол квантового распределения ключей BB84	58
3.1. Схема протокола BB84	59
3.1.1. Этап передачи сигнальных состояний	59
3.1.2. Этап коррекции ошибок	62
3.1.3. Этап усиления секретности	63
3.2. Обоснование стойкости протокола BB84	64
3.2.1. Описание протокола E91	65

3.2.2. Описание протокола Ло-Чу	66
3.2.3. Описание протокола CSS-кодов	68
3.2.4. Сведение протокола CSS-кодов к протоколу BB84	69
3.3. Стратегии противника, подслушивающего информацию	71
3.3.1. Стратегия приема-перепосыла	72
3.3.2. Стратегия прозрачного индивидуального подслушивания	74
3.3.3. Стратегия коллективной атаки	79
3.3.4. Стратегия когерентной атаки	81
Контрольные вопросы по разделу 3	82
4. Иные протоколы квантовой криптографии	83
4.1. Описание протокола B92	83
4.2. Атака с расщеплением по числу фотонов	85
4.2.1. Операция разделения (расщепления) фотонов ...	85
4.2.2. PNS-атака на протокол BB84	86
4.2.3. PNS-атака на протокол B92	86
4.2.4. Критическая длина линии связи при PNS-атаке на протокол BB84	87
4.3. Описание протокола 4+2	88
4.3.1. Описание сигнальных состояний протокола 4+2 ..	89
4.3.2. Описание атаки на протокол 4+2	90
4.4. Описание протокола SARG04	91
4.4.1. Невозможность различающего измерения	91
4.4.2. Описание протокола	93
4.5. Протоколы непрерывных переменных	95
4.5.1. Описание протокола на основе когерентных состояний	96
4.5.2. Вторичная обработка ключей	98
4.5.3. Безусловная защищенность	99
Контрольные вопросы по разделу 4	103
5. Квантовая генерация случайных чисел	104
5.1. Генераторы случайных чисел	104
5.1.1. Обеспечение потребностей систем квантового распределения ключа	105
5.1.2. Классы генераторов случайных чисел	107
5.1.3. Квантовая система, подходящая для построения квантового генератора случайных чисел	114

5.2. Математические основы функционирования квантового генератора случайных чисел	118
5.2.1. Связь энтропии Шеннона и количества случайности	119
5.2.2. Метод фон Неймана извлечения случайных битов	122
5.2.3. Предельное распределение числа равновероятных битов	124
5.2.4. Метод двоичного кодирования Бабкина	126
5.2.5. Сложность метода двоичного кодирования Бабкина	128
5.2.6. Процесс извлечения случайности	130
5.2.7. Истинная случайность, возникающая при реализации метода Бабкина	132
5.3. Пример физической реализации квантового генератора случайных чисел	133
5.3.1. Модель квантового генератора случайных чисел	134
5.3.2. Обоснование качества работы генератора в квантовом режиме	138
5.4. Статистические тесты	140
5.4.1. Система тестирования	140
5.4.2. Проверка статистик на однородность	145
Контрольные вопросы по разделу 5	147
6. Квантовые аналоги традиционных криптографических механизмов и систем	148
6.1. Квантовые хеш-функции	148
6.2. Квантовые электронные подписи	153
6.3. Квантовые системы шифрования	159
6.3.1. Квантовые системы симметричного шифрования	160
6.3.2. Квантовые системы с открытым ключом	168
6.4. Концепция квантового блокчейна	172
Контрольные вопросы по разделу 6	178
Приложение А. Основные положения квантовой механики	179
Приложение Б. Математические основы квантовых методов	190
Литература	202