Программа курса “Односторонние функции и их применения” (2016).

1. Одноленточные машины Тьюринга. Время работы и память как меры сложности. Оценка времени работы машин Тьюринга, выполняющих арифметические операции над натуральными числами. Равнодоступные адресные машины, меры сложности: количество операций, длина машинного слова, количество использованных регистров. Полиномиальные PAM (по всем трем мерам сложности). Полиномиальные PAM для нахождения НОД и возведения в степень по данному модулю.
2. Моделирование многоленточных машин Тьюринга на одноленточных машин Тьюринга. Классы полиномиально вычислимых функций и полиномиально разрешимых предикатов. Независимость этих классов от вычислительной модели.
3. Схемы из функциональных элементов. Верхняя оценка $O(n2^n)$ схемной сложности любой булевой функции. Нижняя оценка $2^n/3n$ схемной сложности некоторой булевой функции от n переменных. Схемы полиномиального размера для сложения и умножения.
4. Вероятностные полиномиальные алгоритмы. Уменьшение вероятности ошибки с помощью повторения. Классы BPP и FBPP. Вероятностный полиномиальный алгоритм проверки полиномиального тождества.
5. Класс nuP. Включение P в nuP. Включение BPP в nuP.
6. Односторонние функции (сильно и слабо). Теорема Левина - Гольдрайха о преобразовании слабо односторонней функции в сильно одностороннюю. Обобщение понятия односторонней функции — частичные односторонние функции (с равномерным распределением). Односторонние перестановки. Функция Рабина, функция RSA, дискретная экспонента.
7. Статистически и вычислительно неотличимые случайные величины. Свойства вычислительно неотличимых случайных величин. Полиномиально генерируемые и доступные последовательности случайных величин. Генераторы псевдослучайных чисел (ПСЧ). Слабая необратимость генераторов ПСЧ.
8. Понятие трудного бита для данной функции. Лемма о трудном бите (конкатенация значения функции и трудного бита неотличима от конкатенации значения функции и случайного бита).
9. Построение генератора ПСЧ, исходя из односторонней перестановки с трудным битом.
10. Теорема о вероятностном декодировании списком кода Адамара.
11. Теорема Левина-Гольдрайха о трудном бите для односторонних функций (доказательство по модулю теоремы о вероятностном декодировании списком кода Адамара).
12. Семейства псевдослучайных функций (ПСФ). Сильный и слабый варианты определения. Построение псевдослучайных функций исходя из генератора ПСЧ.
13. Односторонние перестановки с секретом (trapdoor permutations). Примеры. Трудный бит для необратимой перестановки с секретом.
14. Одноразовые схемы шифрования с закрытым ключом (СШЗК, симметричные схемы). Построение СШЗК на основе генератора ПСЧ.

15. Многоразовые схемы шифрования с закрытым ключом. Построение многоразовой СШЗК на основе семейства ПСФ и одноразовой СШЗК.
16. Схемы шифрования с открытым ключом (ШОК, асимметричные схемы). Конструкция ШОК на основе необратимой перестановки с секретом.
17. Неинтерактивные протоколы привязки к биту (НПБ). Построение НПБ на основе односторонней перестановки.
18. Интерактивные алгоритмы. Интерактивные протоколы привязки к биту (ИПБ). Построение ИПБ на основе генератора ПСЧ
19. Протоколы бросания монетки. Построение таких протоколов на основе протокола привязки к биту.

Литература.

0. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. Изд-во МЦНМО.

1. Введение в криптографию. Под общей редакцией В.В.Ященко. — 3-е изд. доп. — М.: МЦНМО: "ЧеРо 2000. — 288 с.

2. М.И. Анохин, Н.П.Варновский, В.М.Сидельников, В.В. Ященко. Криптография в банковском деле. М.: МИФИ, 1997.

3. O. Goldreich. Foundations of cryptography. Basic tools. Cambridge Univ. Press. 2001. 400 p.

4. O. Goldreich. Foundations of cryptography. Basic applications. Cambridge Univ. Press. 2004.