Программа экзамена по курсу "Теоретико-сложностные проблемы в криптографии". Вторая часть: необратимые функции и криптографические протоколы (схемы)

Чтобы получить 3 или 4 достаточно знать определения, построение всех схем (протоколов) и формулировки теорем. Чтобы получить 5 надо знать также и доказательства.

1. Генераторы псевдослучайных чисел (расширители): два определения и теорема Яо об эквивалентности этих двух определений.
2. Построение генератора, растягивающего случайное зерно из n битов в псевдослучайную последовательность из $\mathrm{poly}(n)$ битов на основе произвольного генератора, растягивающего случайное зерно из n битов в псевдослучайную последовательность из $n+1$ бита.
3. Необратимые функции. Определение и три основных предположительно необратимых функции: возведение в степень по простому модулю, функция RSA, функция Рабина.
4. Слабо необратимые функции. Построение необратимой функции из слабо необратимой функции.
5. Построение генератора псевдослучайных чисел на основе любой необратимой перестановки.
6. Теорема об эквивалентности гипотезы о существовании генератора и гипотезы о существовании необратимой функции (в одну сторону без доказательства).
7. Два определения надежной схемы шифрования с закрытым ключом. Эквивалентность этих определений.
8. Построение надежной схемы шифрования с закрытым ключом на основе генератора.
9. Необратимые перестановки с секретом. Определение и две основных предположительно необратимх перестановки с секретом: функция RSA, функция Рабина.
10. Определение надежной схемы шифрования с открытым ключом. Построение такой схемы на основе необратимой перестановки с секретом.
11. Интерактивные доказательства и класс IP. Последовательное повторение интерактивного доказательства уменьшает вероятность ошибки.
12. Интерактивное доказательство неизоморфности данных графов.
13. Интерактивные доказательства с нулевым разглашением. Доказательство с нулевым разглашением изоморфности данных графов.

14. Определение надежной схемы аутентификации. Построение такой схемы в предположении необратимости функции Рабина, функции возведения в степень по простому модулю или функции, дающей по данному графу и данной перестановке его вершин исходный граф и граф с переставленными вершинами.
15. Определение надежного протокола “запечатывания конверта” (bit committment). Построение такого протокола на основе генератора псевдослучайных чисел.
16. Определение надежной схемы бросания монетки по телефону. Построение такой схемы на основе схемы “запечатывания конверта”.
17. Определение надежной схемы цифровой подписи. Определение универсального семейства односторонних хэш-функций. Схема цифровой подписи Наора и Юнга на основе необратимой функции и универсального семейства односторонних хэш-функций (без доказательства).

Литература.

1. М. Гэри, Д. Джонсон. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

2. А. Китаев, А. Шень, М. Вялый. Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999.

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

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