# Теоретико-сложностные проблемы в криптографии

Н.К. Верещагин, В.Н. Крупский.

Уточненная программа.

Теория сложности вычислений является одной из центральных областей теоретической информатики. В курсе излагаются её основные результаты и их применения в криптографии. Главным из таких применений является возможность дать точные определения надёжности криптографических протоколов и схем и доказательство в ряде случаев их надёжности.

1. Многоленточные машины Тьюринга. Время и объём памяти (зона) как меры сложности вычислений. Возможные упрощения многоленточной модели, их цена.
2. Универсальные машины Тьюринга. Теорема о иерархии по зоне. Теорема о иерархии по времени.
3. P — класс проблем, разрешимых за полиномиальное время. Примеры проблем из класса P: целочиселнная арифметика, арифметика остатков, сложение и умножение матриц, связность графа.
4. Булевы схемы, их размер и глубина. Класс P/poly. Включение $\mathrm{P} \subset \mathrm{P/poly}$.
5. Класс NP. Примеры проблем из класса NP: выполнимость булевых формул, существование гамильтонова цикла, задача о клике, полимино (краевая задача), решение системы линейных неравенств в целых числах.
6. Полиномиальная сводимость (сводимость Карпа) и NP-полные проблемы. Теорема Кука — Левина об NP-полноте проблемы выполнимости пропозициональных формул. Другие NP-полные проблемы.
7. Вероятностные вычисления за полиномиальное время и класс BPP. Вложение $\mathrm{BPP} \subset \mathrm{P/poly}$.
8. Вероятностый алгоритм проверки простоты числа.
9. Полиномиальные игры с ограниченным количеством ходов и полиномиальная иерархия сложностных классов. Полные проблемы в классах полиномиальной иерархии.
10. Включение BPP в $\Sigma_2$.
11. Вычисления на полиномиальной зоне и класс PSPACE. Игровая характеризация класса PSPACE. PSPACE-полнота проблемы истинности булевских формул с кванторами.
12. Необратимые функции: определение и четыре кандидата (произведение двух простых чисел, возведение в степень по простому модулю, функция RSA, функция Рабина).

13. Слабо необратимые функции. Построение необратимой функции из слабо необратимой функции.
14. Генераторы псевдослучайных чисел (расширители): определение и теорема Яо об эквивалентности двух определений расширителя.
15. Построение генератора псевдослучайных чисел на основе любой необратимой перестановки.
16. Шифрование с закрытым ключом на основе расширителя.
17. Необратимые функции с секретом. Шифрование с открытым ключом на основе необратимой функции с секретом.
18. Интерактивные доказательства и класс IP. Интерактивное доказательство неизоморфности данных графов. Совпадение классов IP и PSPACE.
19. Доказательства с нулевым разглашением. Доказательство с нулевым разглашением изоморфности данных графов.
20. Процедура аутентификации на основе необратимой функции с секретом.
21. Генерация ключей на основе необратимой функции с секретом.
22. Криптографические хеш-функции.
23. Протоколы цифровой подписи на основе необратимой функции с секретом. Схема Лампорта.
24. Протоколы "запечатывания конверта" (bit committment). Построение протокола запечатывания конверта на основе генератора псевдослучайных чисел.
25. Надежные протоколы бросания монетки по телефону на основе расширителя.
26. Разделение секрета между несколькими участниками.
27. Протоколы конфиденциальных вычисления на основе необратимой функции с секретом.

**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.