Механико-математический факультет МГУ

Программа специального курса естественно-научного содержания
«Дискретные функции и их приложения в криптографии»,
обязательного для студентов 5 курса специализации
«Математические методы защиты информации»,
10 семестр, лектор — доцент Ю. В. Таранников, 2014/2015 уч. год.

1. Булевы функции. Расстояние Хэмминга. Полиномы Жегалкина. Преобразование Мебиуса. Явная формула для преобразования Мебиуса. Обратное преобразование Мебиуса. Быстрое преобразование Мебиуса. Зависимость веса булевой функции от ее алгебраической степени. Разложение функции веса $2^{n-\deg f}$ в произведение аффинных. Производная булевой функции по направлению. Теорема Мак-Элиса.
2. Преобразование Фурье и преобразование Уолша. Их связь. Формула обращения для преобразования Уолша. Равенство Парсеваля. Теорема Титсворта. Формула, связывающая суммы по сдвигам подпространства и дуального к нему. Тождество Саркара. Нелинейность булевой функции, ее выражение через коэффициенты Уолша.
3. Взаимная корреляция булевых функций. Автокорреляция. Автокорреляционные коэффициенты. Умножение вектор-строк корреляционных и автокорреляционных коэффициентов на матрицу Адамара–Сильвестра. Функции с непересекающимися носителями спектра, связь со взаимной корреляцией. Формулы и оценки для выражений с корреляционными коэффициентами.
4. Групповая эквивалентность булевых функций. Орбиты, эквивалентные функции, группы инерции, их свойства. Криптографически важные подгруппы симметрической группы. Инварианты группы преобразований. Почти все булевы функции имеют тривиальную группу инерции. Теорема Диксона.
5. Бент-функции. Характеризация бент-функций через автокорреляционные коэффициенты. Дуальная функция. Связь бент-функций и матриц Адамара. Характеризация бент-функций через ассоциированные коды. Ограниченность алгебраической степени бент-функций. Семейство Майораны–Мак-Фарланда. Доказательство принадлежности функций семейства Майораны–Мак-Фарланда классу бент-функций. PS-семейство и его принадлежность классу бент-функций.
6. Корреляционно-иммунные и устойчивые булевы функции. Вероятностная и комбинаторная формулировки. Использование устойчивых функций в поточных шифрах. Спектральная характеризация корреляционно-иммунных и устойчивых функций. Делимость коэффициентов Уолша корреляционно-иммунных и устойчивых функций на степени двойки. Оценки нелинейности корреляционно-иммунных и устойчивых функций. Неравенства Зигенталера. Теорема Фон-Дер-Флаасса. Оценки максимального числа нелинейных переменных у $(n-k)$-устойчивых функций.
7. Алгебраическая атака на поточные шифры. Аннигиляторы функций. Алгебраическая иммунность.Пространство аннигиляторов функции как идеал в кольце булевых функций. Верхняя граница алгебраической иммунности. Размерность пространства аннигиляторов аффинной функции. Оценки веса функции в зависимости от ее алгебраической иммунности. Оценка Лобанова, ее неулучшаемость.