Механико-математический факультет МГУ

Программа курса естественно-научного содержания
«Дискретные функции и их приложения в криптографии»,
обязательного для студентов 5 курса специализации
«Математические методы защиты информации»,
лектор — доцент Ю. В. Таранников, 2015/2016 уч. год.

1. Булевы функции. Полином Жегалкина. Преобразование Мебиуса. Явная формула для преобразования Мебиуса. Зависимость веса булевой функции от ее алгебраической степени. Разложение функции веса $2^{n-\deg f}$ в произведение аффинных. Быстрое преобразование Мебиуса.
2. Числовая нормальная форма булевой функции. Связь числовой нормальной формы с полиномом Жегалкина. Теорема Мак–Элиса.
3. Быстрое построение полиномов над $\mathbf{F}_q$.
4. Функция след в конечном поле и ее свойства. Представление булевой функции с помощью функции следа. Представление булевой функции полиномом одной переменной над $\mathbf{F}_{2^n}$. Циклотомические классы. Представление булевой функции в виде суммы следов. Нахождение полинома Жегалкина и алгебраической степени функции исходя из ее представления полиномом одной переменной над $\mathbf{F}_{2^n}$. Мономиальная функция и ее алгебраическая степень. Трэйс-форма булевой функции и ее единственность.
5. Преобразование Фурье и преобразование Уолша. Их связь. Формула обращения для преобразования Уолша. Равенство Парсеваля. Теорема Титсворта. Формула, связывающая суммы по сдвигам подпространства и ортогонального к нему. Тождество Саркара. Нелинейность булевой функции, ее выражение через коэффициенты Уолша. Быстрое преобразование Уолша. Преобразование Уолша как умножение на матрицу Адамара–Сильвестра.
6. Производная булевой функции по направлению. Взаимная корреляция булевых функций. Автокорреляция. Автокорреляционные коэффициенты. Умножение вектор-строк коэффициентов взаимной корреляции на матрицу Адамара–Сильвестра. Функции с непересекающимися носителями спектра, связь со взаимной корреляцией. Формулы и оценки для выражений с коэффициентами взаимной корреляции.
7. Групповая эквивалентность на множестве. Орбиты, эквивалентные элементы, группы инерции, их свойства. Лемма Бернсайда. Групповая эквивалентность булевых функций. Пять криптографически важных групп преобразований булевых функций. Инварианты. Полные инварианты. Почти все булевы функции имеют тривиальную группу инерции в $\mathcal{GU}_n$. Теорема Диксона.
8. Бент-функции. Дуальная функция. Характеризация бент-функций через автокорреляционные коэффициенты. Связь бент-функций и матриц Адамара. Характеризация бент-функций через ассоциированные коды. Ограниченность алгебраической степени бент-функций. Семейство бент-функций Майораны–Мак-Фарланда. PS-семейство бент-функций.
9. Корреляционная иммунность. Спектральная характеризация корреляционно-иммунных 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.
10. Алгебраическая атака. Аннигиляторы функций. Пространство аннигиляторов функции как идеал в кольце булевых функций. Алгебраическая иммунность. Верхняя граница алгебраической иммунности. Пространство аннигиляторов аффинной функции и его размерность. Оценки веса функции в зависимости от ее алгебраической иммунности. Оценка Лобанова. Неулучшаемость оценки Лобанова.