

ПДМ. Приложение. 2012. № 5.

Секция 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

6–7

Глуско К. Л. , Титов С. С. О решении квадратных уравнений в бинарных полях // ПДМ. Приложение. 2012. № 5. С. 6–7.

8–9

Едемский В. А. , Антонова О. В. Линейная сложность обобщённых циклотомических последовательностей с периодом $2p$ // ПДМ. Приложение. 2012. № 5. С. 8–9.

10–11

Зубков А. М. , Круглов В. И. О распределениях весовых спектров случайных линейных двоичных кодов // ПДМ. Приложение. 2012. № 5. С. 10–11.

11–13

Зубков А. М. , Серов А. А. Оценки числа булевых функций, имеющих аффинные и квадратичные приближения заданной точности // ПДМ. Приложение. 2012. № 5. С. 11–13.

13–14

Колмеец Н. А. О нелинейности некоторых булевых функций с максимальной алгебраической иммунностью // ПДМ. Приложение. 2012. № 5. С. 13–14.

14–15

Колчева О. Л. , Панкратова И. А. О статистической независимости суперпозиции булевых функций. II // ПДМ. Приложение. 2012. № 5. С. 14–15.

15–16

Кузнецова А. С. , Сафонов К. В. Об одной задаче комбинаторной оптимизации // ПДМ. Приложение. 2012. № 5. С. 15–16.

16–18

Кяжин С. Н. , Фомичев В. М. Структурные свойства примитивных наборов натуральных чисел // ПДМ. Приложение. 2012. № 5. С. 16–18.

19–21

Мурин Д. М. О порядке роста числа инъективных и сверхрастающих векторов и некоторых особенностях сильного модульного умножения // ПДМ. Приложение. 2012. № 5. С. 19–21.

21–22

Пичкур А. Б. Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек. II // ПДМ. Приложение. 2012. № 5. С. 21–22.

Погорелов Б. А. , Пудовкина М. А. О комбинаторных свойствах группы, порождённой XL-слоями // ПДМ. Приложение. 2012. № 5. С. 22–23.

Потапов В. Н. О булевых функциях, почти уравновешенных в гранях // ПДМ. Приложение. 2012. № 5. С. 23–25.

Пудовкина М. А. Структурные свойства X , S -слоёв // ПДМ. Приложение. 2012. № 5. С. 26–28.

Смышляев С. В. Совершенная уравновешенность дискретных функций и условие Голича // ПДМ. Приложение. 2012. № 5. С. 28–30.

Токарева Н. Н. О разложении булевой функции в сумму бент-функций // ПДМ. Приложение. 2012. № 5. С. 30–30.

Тужилин М. Э. Латинские квадраты и их применение в криптографии // ПДМ. Приложение. 2012. № 5. С. 30–32.

Фролова А. А. Свойство кратных производных бент-функций Касами // ПДМ. Приложение. 2012. № 5. С. 32–34.

Шоломов Л. А. Декомпозиция и аппроксимация недоопределённых данных // ПДМ. Приложение. 2012. № 5. С. 34–36.

Секция 2 МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

Борисенко Б. Б. О поиске подобных изображений при обнаружении ЦВЗ // ПДМ. Приложение. 2012. № 5. С. 37–38.

Волгин А. В. , Иванов А. В. Метод восстановления начального состояния линейного генератора над конечным полем, усложнённого наложением маски // ПДМ. Приложение. 2012. № 5. С. 39–39.

Глухов М. М. О системе Мак-Элиса на некоторых алгебро-геометрических кодах // ПДМ. Приложение. 2012. № 5. С. 39–41.

Камаева А. А. Усечённые дифференциальные характеристики с минимальным количеством активных байт для упрощённой хэш-функции Whirlpool // ПДМ. Приложение. 2012. № 5. С. 41–43.

Карпунин Г. А. , Ермолаева Е. З. Оценки сложности поиска коллизий для хэш-функции RIPEMD // ПДМ. Приложение. 2012. № 5. С. 43–44.

Ковалев Д. С. Реализация на ПЛИС шифра FAPKC-4 // ПДМ. Приложение. 2012. № 5. С. 44–46.

Когос К. Г. , Фомичев В. М. Криптографические свойства разветвлений функций векторных пространств // ПДМ. Приложение. 2012. № 5. С. 46–48.

Коренева А. М. , Фомичев В. М. Криптографические свойства блочных шифров, построенных на основе регистров сдвига // ПДМ. Приложение. 2012. № 5. С. 49–51.

Лошкарёв С. Д. Разностные уравнения для алгоритмов хэширования семейства MDx // ПДМ. Приложение. 2012. № 5. С. 51–53.

Медведев Н. В. , Титов С. С. Проблемы почти пороговых схем разделения секрета // ПДМ. Приложение. 2012. № 5. С. 53–54.

Столлов Е. Л. Математическая модель генератора случайных чисел на основе трёхзначной логики // ПДМ. Приложение. 2012. № 5. С. 54–56.

Чижишев Г. О. Одноразовая кольцевая подпись и её применение в электронной наличности // ПДМ. Приложение. 2012. № 5. С. 56–58.

Шушуев Г. И. Оптимальные линейные приближения сетей Фейстеля. Оценка стойкости шифра SMS4 к линейному криптоанализу // ПДМ. Приложение. 2012. № 5. С. 58–60.

Секция 3 МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Бернштейн А. Ю. , Шилов Н. В. Мультиагентная задача о роботах в пространстве: информационный и криптографический аспекты // ПДМ. Приложение. 2012. № 5. С. 61–63.