

ПДМ. Приложение. 2014. № 7.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

7–9

Бар-Гнар Р. И. , Фомичев В. М. О минимальных примитивных матрицах // ПДМ. Приложение. 2014. № 7. С. 7–9.

9–11

Бондаренко Л. Н. , Шарапова М. Л. Числа Эйлера на множествах перестановок и аналоги теоремы Вильсона // ПДМ. Приложение. 2014. № 7. С. 9–11.

11–13

Виткуп В. А. О некоторых открытых вопросах в области APN-функций // ПДМ. Приложение. 2014. № 7. С. 11–13.

13–14

Геут К. Л. , Титов С. С. Задача, эквивалентная проверке простоты чисел Ферма // ПДМ. Приложение. 2014. № 7. С. 13–14.

15–16

Городилова А. А. Характеризация APN-функций через подфункции // ПДМ. Приложение. 2014. № 7. С. 15–16.

16–19

Заец М. В. Классификация функций над примарным кольцом вычетов в связи с методом покоординатной линеаризации // ПДМ. Приложение. 2014. № 7. С. 16–19.

19–22

Ивачев А. С. Исследование класса дифференцируемых функций в кольцах классов вычетов по примарному модулю // ПДМ. Приложение. 2014. № 7. С. 19–22.

22–24

Коломеец Н. А. Верхняя оценка числа бент-функций на расстоянии 2 от произвольной бент-функции от $2k$ переменных // ПДМ. Приложение. 2014. № 7. С. 22–24.

24–26

Корсакова Е. П. Оценки нелинейности векторных булевых функций специального вида // ПДМ. Приложение. 2014. № 7. С. 24–26.

26–28

Курганский А. Н. Проблема достижимости в непрерывных кусочно-аффинных отображениях окружности степени 2 // ПДМ. Приложение. 2014. № 7. С. 26–28.

29–30

Минаков А. А. Аппроксимация распределения числа монотонных цепочек в случайной последовательности сложным пуассоновским распределением // ПДМ. Приложение. 2014. № 7. С. 29–30.

31–32

Черемушкин А. В. О числе дискретных функций на циклической группе примарного порядка с заданной степенью нелинейности // ПДМ. Приложение. 2014. № 7. С. 31–32.

33–34

Шишкин В. А. Некоторые свойства q -ичных бент-функций // ПДМ. Приложение. 2014. № 7. С. 33–34.

34–36

Шоломов Л. А. О сравнении недоопределённых алфавитов // ПДМ. Приложение. 2014. № 7. С. 34–36.

36–37

Шушуев Г. И. Векторные булевы функции на расстоянии один от APN-функций // ПДМ. Приложение. 2014. № 7. С. 36–37.

38–39

Токарева Н. Н. Каждая кубическая функция от 8 переменных представима в виде суммы не более четырёх бент-функций // ПДМ. Приложение. 2014. № 7. С. 38–39.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

40–41

Аборнев А. В. Нелинейные подстановки на пространстве, рекурсивно-порождённые над кольцом Галуа характеристики 4 // ПДМ. Приложение. 2014. № 7. С. 40–41.

42–43

Авезова Я. Э., Фомичев В. М. О примитивности перемешивающей матрицы генератора (8, t)-самоусечения // ПДМ. Приложение. 2014. № 7. С. 42–43.

43–48

Агибалов Г. П. SIBCiphers - симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // ПДМ. Приложение. 2014. № 7. С. 43–48.

48–49

Волгин А. В. Асимптотические свойства множества решений искажённых систем уравнений // ПДМ. Приложение. 2014. № 7. С. 48–49.

49–51

Пестунов А. И. Влияние веса Хэмминга разности на вероятность её сохранения после арифметических операций // ПДМ. Приложение. 2014. № 7. С. 49–51.

51–52

А

Погорелов Б. А. , Пудовкина М. А. Об обобщениях марковского подхода при изучении алгоритмов блочного шифрования // ПДМ. Приложение. 2014. № 7. С. 51–52.

52–54

Пудовкина М. А. О вероятностях t -раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием // ПДМ. Приложение. 2014. № 7. С. 52–54.

54–56

Рацев С. М. Условия существования совершенных шифров с фиксированным набором параметров // ПДМ. Приложение. 2014. № 7. С. 54–56.

56–58

Романьков В. А. Криптографический анализ аналога схемы Диффи - Хелл-мана, использующего сопряжение и возведение в степень, на матричной платформе // ПДМ. Приложение. 2014. № 7. С. 56–58.

ПСЕВДОСЛУЧАЙНЫЕ ГЕНЕРАТОРЫ

59–60

Былков Д. Н. Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент // ПДМ. Приложение. 2014. № 7. С. 59–60.

60–64

Дорохова А. М. Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов // ПДМ. Приложение. 2014. № 7. С. 60–64.

64–67

Ермилов Д. М. Алгоритм построения системы представителей циклов максимальной длины полиномиальных подстановок над кольцом Галуа // ПДМ. Приложение. 2014. № 7. С. 64–67.

67–68

Захаров В. М. , Зелинский Р. В. , Шалагин С. В. Модель функции усложнения в генераторе псевдослучайных последовательностей над полем $GF(2)$ // ПДМ. Приложение. 2014. № 7. С. 67–68.

69–70

Ковалевская А. О. Построение транзитивных полиномов над кольцом Z_{p^2} // ПДМ. Приложение. 2014. № 7. С. 69–70.

71–72

Сергеева О. Е. Распознавание рекуррентных последовательностей, порождаемых консервативными функциями // ПДМ. Приложение. 2014. № 7. С. 71–72.

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

73–74