ПДМ. Приложение. 2014. № 7.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

ŋqdqɐeɎ bɆ dəqɆbɎзə b ɕɔɑɓɔɏ Ɉqdqɏqɐè

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 r-раундовых пар разностей XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием // ПДМ. Приложение. 2014. № 7. С. 52–54.

54–56

Рацеев 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