

ПДМ. Приложение. 2013. № 6.

Секция 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

6–7

Аборнев А. В. Разрядно-инъективные преобразования модуля над кольцом Галуа // ПДМ. Приложение. 2013. № 6. С. 6–7.

7–8

Бондаренко Л. Н. Свойства статистики var на группе перестановок // ПДМ. Приложение. 2013. № 6. С. 7–8.

9–10

Былков Д. Н. Вторая координатная последовательность линейной рекурренты максимального периода над кольцом \mathbb{Z}_g // ПДМ. Приложение. 2013. № 6. С. 9–10.

11–12

Волгин А. В. Оценка скорости сходимости в многомерной центральной предельной теореме // ПДМ. Приложение. 2013. № 6. С. 11–12.

12–13

Геут К. Л. , Титов С. С. О поликвадратичном расширении бинарных полей // ПДМ. Приложение. 2013. № 6. С. 12–13.

13–15

Заец М. В. Классы полиномиальных и вариационно-координатно полиномиальных функций над кольцом Галуа // ПДМ. Приложение. 2013. № 6. С. 13–15.

15–16

Коломеец Н. А. Об аффинности булевых функций на подпространствах и их сдвигах // ПДМ. Приложение. 2013. № 6. С. 15–16.

16–18

Курганский А. Н. Об алгоритмических и топологических свойствах орбит кусочно-аффинных отображений // ПДМ. Приложение. 2013. № 6. С. 16–18.

18–19

Мироненко О. Л. О статистической независимости произвольной суперпозиции булевых функций // ПДМ. Приложение. 2013. № 6. С. 18–19.

19–20

Филюзин С. Ю. Верхняя оценка алгебраической иммунности некоторых бентфункций Диллона // ПДМ. Приложение. 2013. № 6. С. 19–20.

20–24

А
Фомичев В. М. Эквивалентность примитивных множеств // ПДМ. Приложение. 2013. № 6. С. 20–24.

24–25

Фролова А. А. Итеративная конструкция APN-функций // ПДМ. Приложение. 2013. № 6. С. 24–25.

26–27

Черемушкин А. В. К определению степени нелинейности дискретной функции на циклической группе // ПДМ. Приложение. 2013. № 6. С. 26–27.

27–29

Шоломов Л. А. Экономное представление недоопределённых данных и дизъюнктивные коды // ПДМ. Приложение. 2013. № 6. С. 27–29.

Секция 2. МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

30–32

Виткуп В. А. О представлении S-блоков при реализации в блочных шифрах // ПДМ. Приложение. 2013. № 6. С. 30–32.

32–33

Калужин А. К. , Чижов И. В. Алгоритм восстановления открытого текста по шифртексту в криптосистеме Мак-Элиса // ПДМ. Приложение. 2013. № 6. С. 32–33.

33–35

Карпунин Г. А. О вероятностных характеристиках случайных графов, порождаемых алгоритмами поиска коллизий криптографических хэш-функций // ПДМ. Приложение. 2013. № 6. С. 33–35.

35–36

Катеринский Д. А. Об обратимости конечных автоматов с конечной задержкой // ПДМ. Приложение. 2013. № 6. С. 35–36.

36–38

Ковалев Д. С. Реализация на ПЛИС симметричного аналога FAPKC // ПДМ. Приложение. 2013. № 6. С. 36–38.

39–41

Коренева А. М. О блочных шифрах, построенных на основе регистров сдвига с двумя обратными связями // ПДМ. Приложение. 2013. № 6. С. 39–41.

41–42

Медведев Н. В. , Титов С. С. Конструкции идеальных схем разделения секрета // ПДМ. Приложение. 2013. № 6. С. 41–42.

42–44

А

Медведева Н. В. , Титов С. С. О неминимальных совершенных шифрах // ПДМ. Приложение. 2013. № 6. С. 42–44.

44–48

Пестунов А. И. О связях между основными понятиями разностного анализа итеративных блочных шифров // ПДМ. Приложение. 2013. № 6. С. 44–48.

48–49

Чижов И. В. , Бородин М. А. Уязвимость криптосистемы Мак-Элиса, построенной на основе двоичных кодов Риды — Маллера // ПДМ. Приложение. 2013. № 6. С. 48–49.

Секция 3. МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ И НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

50–51

Алехина М. А. , Барсукова О. Ю. Об оценках ненадёжности схем при инверсных неисправностях и отказах функциональных элементов // ПДМ. Приложение. 2013. № 6. С. 50–51.

52–56

Анисеня Н. И. , Стефанцов Д. А. , Торгаева Т. А. Сервис BlackBox для проведения соревнований по защите компьютерной информации Capture The Flag // ПДМ. Приложение. 2013. № 6. С. 52–56.

56–57

Васин А. В. О базисах с коэффициентом ненадёжности 1 // ПДМ. Приложение. 2013. № 6. С. 56–57.

58–59

Девянин П. Н. Корректность правил преобразования состояний системы в рамках мандатной сущностно-ролевой ДП-модели ОС семейства Linux // ПДМ. Приложение. 2013. № 6. С. 58–59.

60–62

Зайцев Г. Ю. , Потапкин А. И. , Стефанцов Д. А. Модификация скомпилированных приложений для платформы Android методом аспектно-ориентированного программирования // ПДМ. Приложение. 2013. № 6. С. 60–62.

62–67

Колегов Д. Н. , Ткаченко Н. О. , Чернов Д. В. Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL // ПДМ. Приложение. 2013. № 6. С. 62–67.

68–70

Щерба Е. В. , Волков Д. А. Разработка системы обнаружения распределённых сетевых атак типа «отказ в обслуживании» // ПДМ. Приложение. 2013. № 6. С. 68–70.

Секция 4. ПРИКЛАДНАЯ ТЕОРИЯ ГРАФОВ