

ПДМ. Приложение. 2010. № 3.

Секция 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

6–7

Алексеев Е. С., Алешников С. И., Зайцев А. И. Оптимальные кривые рода 3 над конечным полем с дискриминантом - 19 // ПДМ. Приложение. 2010. № 3. С. 6–7.

7–9

Гришин А. М. Некоторые свойства дискретного преобразования Фурье в поле комплексных чисел и полях конечной характеристики // ПДМ. Приложение. 2010. № 3. С. 7–9.

10–11

Иванов А. В., Романов В. Н. Построение классов булевых функций с заданными криптографическими свойствами на основе координатных функций степенных преобразований конечных полей // ПДМ. Приложение. 2010. № 3. С. 10–11.

11–12

Коломеец Н. А. Связь подпространств, на которых аффинны бент-функция и дуальная к ней // ПДМ. Приложение. 2010. № 3. С. 11–12.

13–14

Токарева Н. Н. Новая комбинаторная конструкция бент-функций // ПДМ. Приложение. 2010. № 3. С. 13–14.

14–15

Тужилин М. Э. О скорости порождения знакопеременной группы полурегулярными инволюциями // ПДМ. Приложение. 2010. № 3. С. 14–15.

15–19

Фомичев В. М. Свойства внешних управляющих последовательностей // ПДМ. Приложение. 2010. № 3. С. 15–19.

Секция 2. МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

20–21

Золотухин В. Ю., Чалкин Т. А. Разработка методики оценки зависимости криптостойкости алгоритма ГОСТ 28147-89 от выбранной ключевой информации // ПДМ. Приложение. 2010. № 3. С. 20–21.

21–23

Киселев С. А. О сокращении ключевого пространства поточного шифра А5/1 при тактировании // ПДМ. Приложение. 2010. № 3. С. 21–23.

Милошенко А. В. Аппаратная реализация шифрсистемы, основанной на автомате Закревского // ПДМ. Приложение. 2010. № 3. С. 23–24.

Пестунов А. И. Оценки сложности дифференциальной атаки при различных параметрах блочного шифра // ПДМ. Приложение. 2010. № 3. С. 25–27.

Пудовкина М. А. О слабом классе алгоритмов развёртывания ключа относительно метода связанных ключей // ПДМ. Приложение. 2010. № 3. С. 27–29.

Пудовкина М. А. , Хоруженко Г. И. Атаки на алгоритм блочного шифрования ГОСТ 28147-89 с двумя и четырьмя связанными ключами // ПДМ. Приложение. 2010. № 3. С. 29–30.

Пудовкина М. А. Разностная атака на 6-раундов Whirlpool-подобных алгоритмов блочного шифрования // ПДМ. Приложение. 2010. № 3. С. 30–31.

Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // ПДМ. Приложение. 2010. № 3. С. 32–34.

Чижов И. В. Связь структуры множества открытых ключей со стойкостью криптосистемы Мак-Элиса-Сидельников // ПДМ. Приложение. 2010. № 3. С. 34–35.

Широков И. В. Модель симметричного шифра на основе некоммутативной алгебры полиномов // ПДМ. Приложение. 2010. № 3. С. 35–36.

Секция 3. МАТЕМАТИЧЕСКИЕ МЕТОДЫ СТЕГАНОГРАФИИ

Моденова О. В. Стеганография и стегоанализ в видеофайлах // ПДМ. Приложение. 2010. № 3. С. 37–39.

Разинков Е. В. , Латыпов Р. Х. О правиле выбора элементов стеганографического контейнера в скрывающем преобразовании // ПДМ. Приложение. 2010. № 3. С. 39–41.

Соловьёв Т. М. , Черняк Р. И. Стегосистемы идентификационных номеров, устойчивые к атаке сговором // ПДМ. Приложение. 2010. № 3. С. 41–44.

Шойтов А. М. О выявлении факта зашумления конечной цепи Маркова с неизвестной матрицей переходных вероятностей // ПДМ. Приложение. 2010. № 3. С. 44–45.

Секция 4. МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

46–47

Бречка Д. М. Поиск tg-путей и островов для модели безопасности Take-Grant // ПДМ. Приложение. 2010. № 3. С. 46–47.

47–49

Грищенко К. А. Моделирование управления доступом и информационными потоками в электронных почтовых системах // ПДМ. Приложение. 2010. № 3. С. 47–49.

49–51

Девянин П. Н. Результаты анализа безопасности систем с простыми траекториями функционирования в рамках базовой ролевой ДП-модели // ПДМ. Приложение. 2010. № 3. С. 49–51.

52–53

Качанов М. А. Об информационных потоках по времени в компьютерных системах // ПДМ. Приложение. 2010. № 3. С. 52–53.

53–55

Колегов Д. Н. Обучение на платформе Cisco основам построения защищенных вычислительных сетей // ПДМ. Приложение. 2010. № 3. С. 53–55.

55–58

Ниссенбаум О. В. , Присяжнюк А. С. Адаптивный алгоритм отслеживания аномальной активности в компьютерной сети на основании характерных изменений оценок альтернирующего потока // ПДМ. Приложение. 2010. № 3. С. 55–58.

59–60

Паутов П. А. Аутентификация в многоуровневой системе на основе коммутативного шифрования // ПДМ. Приложение. 2010. № 3. С. 59–60.

61–62

Смит И. В. Внедрение кода в процесс в операционной системе семейства GNU/Linux // ПДМ. Приложение. 2010. № 3. С. 61–62.

62–64

Ткаченко Н. О. , Чернов Д. В. Разработка и реализация сервера игры CTF // ПДМ. Приложение. 2010. № 3. С. 62–64.

65–66