Math-Net.Ru

Общероссийский математический портал

Указатель статей,
опубликованных в томах 1–10 (2010–2019), *Матем. вопр.
криптогр.*, 2019, том 10, выпуск 4, 117–134

DOI: <https://doi.org/10.4213/mvk310>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.209.52.79

26 апреля 2023 г., 13:33:38

Указатель статей, опубликованных в томах 1–10 (2010–2019)

Аборнев А. В., Нелинейные подстановки, рекурсивно порожденные над кольцом Галуа характеристики 4, **5:4** (2014), 5–15.

Акишин А. В., Об одном классе подстановочных многочленов над кольцами вычетов по модулю 2^n , **4:2** (2013), 5–15.

Алексеев Е. К., Ошкин И. Б., Попов В. О., Смышляев С. В., О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, **7:1** (2016), 5–38.

Алексеев Е. К., Ахметзянова Л. Р., Ошкин И. Б., Смышляев С. В., Обзор уязвимостей некоторых протоколов выработки общего ключа с аутентификацией на основе пароля и принципы построения протокола *SESPAKEY*, **7:4** (2016), 7–28.

Анашкин А. В., Полное описание одного класса MDS-матриц над конечным полем характеристики 2, **8:4** (2017), 5–28.

Арбеков И. М., Критерии секретности ключа, **7:1** (2016), 39–56.

Афанасьева А. В., Балакирский В. Б., Беззатеев С. В., Протокол конфиденциального получения информации, **6:4** (2015), 5–21.

Ахметзянова Л. Р., см. Алексеев Е.К., **7:4** (2016), 7–28.

Балакин Г. В., Линейные псевдобулевы неравенства, **1:3** (2010), 5–18.

Балакин Г. В., О структуре решений системы из линейных псевдобулевых неравенств, **3:3** (2012), 5–19.

Балакин Г. В., О решении некоторых классов систем булевых уравнений рекуррентного типа, **4:1** (2013), 5–25.

Балакин Г. В., О возможности частичного восстановления некоторых последовательностей по наблюдениям, **4:4** (2013), 7–25.

Балакирский В. Б., см. Афанасьева А. В., **6:4** (2015), 5–21.

Барышников А. В., Катышев С. Ю., Использование неассоциативных структур для построения алгоритмов открытого распределения ключей, **9:4** (2018), 5–30.

Беззатеев С. В., см. Афанасьева А. В., **6:4** (2015), 5–21.

Богонатов Р. В., Максимальные и минимальные представления над кольцом Галуа линейной рекуррентной последовательности максимального периода над полем Галуа, **3:4** (2012), 5–23.

Борисенко В. В., О трансверсалих распавшихся латинских квадратов четного порядка, **5:1** (2014), 5–25.

Борисенко В. В., О трансверсалих однородных латинских квадратов, **6:3** (2015), 5–17.

Бугров А. Д., Камловский О. В., Параметры одного класса функций, заданных на конечном поле, **9:4** (2018), 31–52.

Былков Д. Н., Камловский О. В., Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент, **3:4** (2012), 25–53.

Былков Д. Н., Построение новых классов фильтрующих генераторов, не имеющих эквивалентных состояний, **5:4** (2014), 17–39.

Василенко О. Н., Об алгоритмах построения изогений эллиптических кривых над конечными полями и их приложениях, **1:1** (2010), 7–22.

Василенко О. Н., О вычислении кратных точек на эллиптических кривых над конечными полями с использованием нескольких оснований систем счисления и новых видов координат, **2:1** (2011), 5–28.

Ватутин В. А., Условная предельная теорема для близких к критическим ветвящихся процессов с финальным типом частиц, **9:4** (2018), 53–72.

Ватутин В. А., Асимптотические свойства числа инверсий в раскрашенных деревьях, **10:4** (2019), 9–24.

Викторенков В. Е., Цикловая структура случайных подстановок на множестве двухцветных элементов. I, **10:3** (2019), 9–32.

Глухов М. М., Об использовании групп классов идеалов квадратичных полей для построения криптографических систем с открытым ключом, **1:1** (2010), 23–54.

Глухов М. М., К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах, **1:4** (2010), 5–22.

Глухов М. М., О рассеивающих линейных преобразованиях для блочных шифр-систем, **2:2** (2011), 5–40.

Глухов М. М., О методах построения систем ортогональных квазигрупп с использованием групп, **2:4** (2011), 5–24.

Глухов М. М., О матрицах переходов разностей при использовании некоторых модулярных групп, **4:4** (2013), 27–47.

Глухов М. М., О приближении дискретных функций линейными функциями, **7:4** (2016), 29–50.

Глухов М. М., О 2-транзитивных произведениях трех регулярных групп подстановок конечного поля, **10:1** (2019), 11–26.

Гольтваница М. А., Методы построения скрученных линейных рекуррентных последовательностей максимального периода, базирующиеся на факторизации многочленов Галуа в кольце матричных многочленов, **10:4** (2019), 25–51.

Горшков С. П., Функции из классов Шефера, переходящие при отрицании в другие классы Шефера, **6:4** (2015), 23–48.

Горшков С. П., Исследование некоторых подклассов мультиаффинных, биюнктивных, слабо положительных и слабо отрицательных булевых функций, **7:4** (2016), 51–66.

Горшков С. П., Тарасов А. В., О весах булевых функций, представимых в виде 2-КНФ или 3-КНФ, **9:1** (2018), 5–26.

Грибов А. В., Золотых П. А., Михалев А. В., Построение алгебраической криптосистемы над квазигрупповым кольцом, **1:4** (2010), 23–32.

Гусев В. В., Легальные сообщения для некоторых функций имитозащиты блочных шифров, **9:1** (2018), 27–46.

Гусев В. В., Легальные сообщения для режимов работы блочных шифров ГОСТ Р 34.13-2015, **10:3** (2019), 33–47.

Гуселев А. М., Применение теории решеток к анализу схем цифровой подписи, **9:4** (2018), 73–84.

Денисов О. В., Статистическая оценка множества существенных аргументов двоичной вектор-функции с искаженными значениями, **5:4** (2014), 41–61.

Денисов О. В., Об алгоритме поиска существенных аргументов случайных булевых функций, **6:3** (2015), 19–32.

Денисов О. В., Спектральный критерий для проверки гипотез о случайных подстановках, **7:3** (2016), 19–28.

Дмух А. А., Об использовании подобия подстановок при определении ключа в сетях Фейстеля, **9:3** (2018), 33–44.

Дорофеев А. Я., Решение систем линейных уравнений при вычислении логарифмов в конечном простом поле, **3:1** (2012), 5–51.

Дрелихов В. О., Круглов И. А., Локальные характеристики выравнивающих свойств эпиморфизмов конечных абелевых групп, **6:3** (2015), 33–45.

Елизаров В. П., О классах разрешимых колец, **1:3** (2010), 19–26.

Ермилов Д. М., Козлитин О. А., Цикловая структура полиномиального генератора над кольцом Галуа, **4:1** (2013), 27–57.

Ермилов Д. М., Козлитин О. А., О строении графа полиномиального преобразования кольца Галуа, **6:3** (2015), 47–73.

Ермилов Д. М., Количество полиномиальных преобразований максимального периода над кольцами Галуа нечетной характеристики, **9:4** (2018), 85–100.

Ерохин А. В., Малышев Ф. М., Тришин А. Е., Многомерный линейный метод и показатели рассеивания линейной среды шифрпреобразований, **8:4** (2017), 29–62.

Жуков К. Д., Об обобщении метода Дюжелла, **4:3** (2013), 7–19.

Заец М. В., Никонов В. Г., Шишков А. Б., Класс функций с вариационно-координатной полиномиальностью над кольцом $\mathbb{Z}_{2^m}$ и его обобщение, **4:3** (2013), 21–47.

Заец М. В., Построение подстановок с использованием вариационно-координатно полиномиальных функций над примарным кольцом вычетов, **6:1** (2015), 5–32.

Закревский П. Н., Вычисление коэффициента аддитивности для некоторых биюнктивных, слабо положительных и слабо отрицательных булевых функций, **6:3** (2015), 75–88.

Золотых П. А., см. Грибов А. В., **1:4** (2010), 23–32.

Зубков А. М., Вычисление распределений чисел компонент и циклических точек случайного отображения, **1:2** (2010), 5–18.

Зубков А. М., Круглов В. И., Моментные характеристики весов векторов в случайных двоичных линейных кодах, **3:4** (2012), 55–70.

Зубков А. М., Круглов В. И., Статистические характеристики весовых спектров случайных линейных кодов над $\text{GF}(p)$, **5:1** (2014), 27–38.

Зубков А. М., Моменты весов случайных неравновероятных булевых функций, **5:3** (2014), 5–15.

Зубков А. М., Миронкин В. О., Распределение длины отрезка аperiodичности в графе k -кратной итерации случайного равновероятного отображения, **8:4** (2017), 63–74.

Зубков А. М., Новые оценки расстояния по вариации между двумя распределениями выборки, **9:3** (2018), 45–60.

Зубов А. Ю., Коды аутентификации с секретностью (обзор), **8:3** (2017), 5–40.

Иванов А. В., Незамкнутость класса гипер-бент-функций относительно действия полной линейной группы, **3:2** (2012), 5–26.

Иванов А. В., Асимптотически оптимальные критерии в задаче различения параметрических гипотез о распределении случайного вектора. I, **6:3** (2015), 89–116.

Иванов А. В., Асимптотически оптимальные критерии в задаче различения параметрических гипотез о распределении случайного вектора. II, **6:4** (2015), 49–64.

Ивченко Г. И., Медведев Ю. И., Спектр случайной булевой функции и его производящая функция, **2:2** (2011), 41–54.

Ивченко Г. И., Медведев Ю. И., Стохастические булевы функции и их спектры, **3:3** (2012), 21–34.

Ивченко Г. И., Медведев Ю. И., Миронова В. А., Анализ спектра случайных симметрических булевых функций, **4:1** (2013), 59–76.

Ивченко Г. И., Медведев Ю. И., Миронова В. А., Симметрические булевы функции и их метрические свойства, **4:4** (2013), 49–63.

Ивченко Г. И., Медведев Ю. И., Миронова В. А., Многочлены Кравчука и их применения в задачах криптографии и теории кодирования, **6:1** (2015), 33–56.

Ивченко Г. И., Медведев Ю. И., Миронова В. А., Структура спектров булевых функций, **7:1** (2016), 57–70.

Ивченко Г. И., Медведев Ю. И., Параметрические модели случайных комбинаторных объектов экспоненциального типа и вопросы их вероятностно-статистического анализа, **8:3** (2017), 41–56.

Ивченко Г. И., Медведев Ю. И., Параметрические модели случайных r -подстановок и r -разбиений и их вероятностно-статистический анализ, **9:1** (2018), 47–64.

Ивченко Г. И., Медведев Ю. И., Разбиения без малых блоков и r -присоединенные полиномы Белла в параметрической модели: вероятностно-статистический анализ, **10:1** (2019), 27–40.

Камловский О. В., Метод тригонометрических сумм для исследования частот r -грамм в старших координатных последовательностях линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$, **1:4** (2010), 33–62.

Камловский О. В., см. Былков Д. Н., **3:4** (2012), 25–53.

Камловский О. В., Количество различных мультиграмм в линейных рекуррентных последовательностях над кольцами Галуа, **4:3** (2013), 49–82.

Камловский О. В., Неабсолютные оценки для неполных тригонометрических сумм от линейных рекуррент и их приложения, **5:3** (2014), 17–34.

Камловский О. В., Свойства распределений строк и столбцов для матричных линейных рекуррентных последовательностей первого порядка, **6:4** (2015), 65–76.

Камловский О. В., Расстояние между двоичными представлениями линейных рекуррент над полем $\text{GF}(2^k)$ и кольцом $\mathbb{Z}_{2^n}$, **7:1** (2016), 71–82.

- Камловский О. В.**, Нелинейность одного класса булевых функций, построенных с использованием двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_2^n$, **7:3** (2016), 29–46.
- Камловский О. В.**, Суммы модулей коэффициентов Уолша–Адамара некоторых сбалансированных булевых функций, **8:4** (2017), 75–98.
- Камловский О. В.**, см. Бугров А. Д., **9:4** (2018), 31–52.
- Катышев С. Ю.**, см. Барышников А. В., **9:4** (2018), 5–30.
- Козлитин О. А.**, Параллельная декомпозиция неавтономных 2-линейных регистров сдвига, **2:3** (2011), 5–29.
- Козлитин О. А.**, 2-линейный регистр сдвига над кольцом Галуа четной характеристики, **3:2** (2012), 27–61.
- Козлитин О. А.**, см. Ермилов Д. М., **4:1** (2013), 27–57.
- Козлитин О. А.**, Использование 2-линейного регистра сдвига для выработки псевдослучайных последовательностей, **5:1** (2014), 39–72.
- Козлитин О. А.**, см. Ермилов Д. М., **6:3** (2015), 47–73.
- Козлитин О. А.**, Вероятностные линейные соотношения в двоичных рекуррентных последовательностях, **8:3** (2017), 57–84.
- Козлитин О. А.**, Периодические свойства многомерного полиномиального генератора над кольцом Галуа. I, **9:3** (2018), 61–98.
- Козлитин О. А.**, Генераторы псевдослучайных последовательностей, использующие регистровые преобразования конечных цепных колец, **10:3** (2019), 49–65.
- Копытцев В. А., Михайлов В. Г.**, Теоремы пуассоновского типа для числа решений случайных включений, **1:4** (2010), 63–84.
- Копытцев В. А., Михайлов В. Г.**, О распределении чисел решений случайных включений, **2:2** (2011), 55–80.
- Копытцев В. А., Михайлов В. Г.**, Условия сходимости к распределению Пуассона для чисел решений случайных включений, **3:3** (2012), 35–55.
- Копытцев В. А., Михайлов В. Г.**, Об одном асимптотическом свойстве сфер в дискретных пространствах большой размерности, **5:1** (2014), 73–83.
- Копытцев В. А., Михайлов В. Г.**, Явные оценки точности пуассоновской аппроксимации для распределения числа решений случайных включений, **6:1** (2015), 57–79.
- Копытцев В. А.**, Многомерная теорема Пуассона для чисел решений случайных включений, близких к заданным векторам, **7:4** (2016), 67–80.
- Копытцев В. А.**, О пороговом эффекте для среднего числа решений системы случайных уравнений, **10:3** (2019), 67–80.
- Косолапов Ю. В.**, Схема разделения секрета типа схемы Блэкли, основанная на пересечении подпространств, **8:1** (2017), 13–30.
- Круглов И. А.**, Условия предельной равновероятности состояний регистров сдвига, **1:2** (2010), 19–29.
- Круглов И. А.**, О гомоморфизмах сильно связанных конечных автоматов на подстановочные автоматы, **2:3** (2011), 31–46.
- Круглов И. А.**, Авторегрессия на конечной абелевой группе с марковской входной последовательностью, **2:4** (2011), 25–36.

Круглов И. А., Оценка скорости сходимости к равномерному распределению для произведений элементов конечной группы, управляемых цепью Маркова, **5:1** (2014), 85–94.

Круглов И. А., см. Дрелихов В. О., **6:3** (2015), 33–45.

Круглов И. А., см. Сачков В. Н., **7:4** (2016), 95–116.

Круглов И. А., Сходимость матриц переходных вероятностей некоторых цепей Маркова на конечной абелевой группе к равномерной матрице, **8:1** (2017), 31–50.

Круглов И. А., Скорость сходимости к равномерному распределению в схеме авторегрессии на конечной абелевой группе, **9:1** (2018), 65–74.

Круглов И. А., см. Сачков В. Н., **9:4** (2018), 101–124.

Круглов И. А., см. Сачков В. Н., **10:3** (2019), 101–116.

Круглов И. А., **Чередник И. В.**, О существовании неотрицательных базисов в подгруппах свободных групп шрейеровых многообразий, **10:4** (2019), 53–65.

Круглов В. И., Пуассоновская аппроксимация для распределения числа «параллелограммов» в случайной выборке из $\mathbb{Z}_N^q$, **3:2** (2012), 63–78.

Круглов В. И., см. Зубков А. М., **3:4** (2012), 55–70.

Круглов В. И., см. Зубков А. М., **5:1** (2014), 27–38.

Круглов В. И., **Михайлов В. Г.**, О ранге случайной двоичной матрицы с заданными весами независимых строк, **10:4** (2019), 67–76.

Кузьмин А. С., **Маршалко Г. Б.**, **Нечаев А. А.**, Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению, **1:2** (2010), 31–56.

Кузьмин А. С., **Маршалко Г. Б.**, Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению. II, **2:2** (2011), 81–93.

Куракин В. Л., Свободные регистры сдвига. IV, **1:2** (2010), 57–92.

Куракин В. Л., Семейство последовательностей над кольцом из 8 элементов с низкой корреляцией, **1:4** (2010), 85–109.

Куракин В. Л., Семейство последовательностей максимального периода над кольцом из 8 элементов с низкой кросс-корреляцией, **2:3** (2011), 47–73.

Литвиненко В. С., **Тарасов А. В.**, Классы Шефера, классы Поста и соответствия Галуа, **6:1** (2015), 81–107.

Максимовский А. Ю., О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам, **7:1** (2016), 83–92.

Мальшев Ф. М., Дважды транзитивные XSL-семейства подстановок, **1:2** (2010), 93–102.

Мальшев Ф. М., Базисы множества целых чисел относительно многоместных операций сдвига, **2:1** (2011), 29–74.

Мальшев Ф. М., Метрические свойства вложений множества целых чисел в цилиндр, **3:3** (2012), 57–79.

Мальшев Ф. М., Три семейства 5-конфигураций, **4:3** (2013), 83–97.

Мальшев Ф. М., Четыре бесконечные серии k -конфигураций, **4:4** (2013), 65–75.

Мальшев Ф. М., Двойственность разностного и линейного методов в криптографии, **5:3** (2014), 35–47.

- Малышев Ф. М.**, Сложность восстановления начальных знаков фильтрующих генераторов одного класса, **6:1** (2015), 109–116.
- Малышев Ф. М., Трифонов Д. И.**, Рассеивающие свойства XSLP-шифров, **7:3** (2016), 47–60.
- Малышев Ф. М.**, Криптографически слабые функции усложнения для трехчленных линейных рекуррентных последовательностей, **8:1** (2017), 69–80.
- Малышев Ф. М.**, см. Ерохин А. В., **8:4** (2017), 29–62.
- Малышев Ф. М.**, Вероятностные характеристики разностных и линейных соотношений для неоднородной линейной среды, **10:1** (2019), 41–72.
- Малышев Ф. М.**, Функциональные схемы, задающие семейства подстановок на пространстве $GF(2)^N$, **10:3** (2019), 81–87.
- Мартынов С. С.**, NP-полнота специальных задач редактирования слов, **4:4** (2013), 77–93.
- Маршалко Г. Б.**, см. Кузьмин А. С., **1:2** (2010), 31–56.
- Маршалко Г. Б.**, см. Кузьмин А. С., **2:2** (2011), 81–93.
- Матюхин Д. В., Шишкин В. А.**, Некоторые методы анализа функций хеширования и их применение к алгоритму ГОСТ Р 34.11-94, **3:4** (2012), 71–89.
- Медведев Ю. И.**, см. Ивченко Г. И., **2:2** (2011), 41–54.
- Медведев Ю. И.**, см. Ивченко Г. И., **3:3** (2012), 21–34.
- Медведев Ю. И.**, см. Ивченко Г. И., **4:1** (2013), 59–76.
- Медведев Ю. И.**, см. Ивченко Г. И., **4:4** (2013), 49–63.
- Медведев Ю. И.**, см. Ивченко Г. И., **6:1** (2015), 33–56.
- Медведев Ю. И.**, см. Ивченко Г. И., **7:1** (2016), 57–70.
- Медведев Ю. И.**, см. Ивченко Г. И., **8:3** (2017), 41–56.
- Медведев Ю. И.**, см. Ивченко Г. И., **9:1** (2018), 47–64.
- Медведев Ю. И.**, см. Ивченко Г. И., **10:1** (2019), 27–40.
- Меженная Н. М., Михайлов В. Г.**, О распределении числа единиц в выходной последовательности генератора Пола над полем $GF(2)$, **4:4** (2013), 95–107.
- Меженная Н. М., Михайлов В. Г.**, Об асимптотической нормальности чисел появлений знаков в неравновероятной мультициклической случайной последовательности по модулю 4, **7:4** (2016), 81–94.
- Миронкин В. О.**, см. Зубков А. М., **8:4** (2017), 63–74.
- Миронкин В. О., Михайлов В. Г.**, О множестве образов k -кратной итерации равновероятного случайного отображения, **9:3** (2018), 99–108.
- Миронкин В. О.**, Слои в графе k -кратной итерации равновероятного случайного отображения, **10:1** (2019), 73–82.
- Миронкин В. О.**, Распределение длины отрезка аперiodичности в графе композиции независимых равновероятных случайных отображений, **10:3** (2019), 89–99.
- Миронова В. А.**, см. Ивченко Г. И., **4:1** (2013), 59–76.
- Миронова В. А.**, см. Ивченко Г. И., **4:4** (2013), 49–63.
- Миронова В. А.**, см. Ивченко Г. И., **6:1** (2015), 33–56.
- Миронова В. А.**, см. Ивченко Г. И., **7:1** (2016), 57–70.
- Михайлов В. Г.**, Изучение предельного поведения числа решений систем уравнений со случайным вхождением неизвестных, **1:3** (2010), 27–43.
- Михайлов В. Г.**, см. Копытцев В. А., **1:4** (2010), 63–84.
- Михайлов В. Г.**, см. Копытцев В. А., **2:2** (2011), 55–80.

- Михайлов В. Г., см. Копытцев В. А., **3:3** (2012), 35–55.
- Михайлов В. Г., Шойтов А. М., О числах множеств эквивалентных цепочек в последовательности независимых случайных величин, **4:1** (2013), 77–86.
- Михайлов В. Г., см. Меженная Н. М., **4:4** (2013), 95–107.
- Михайлов В. Г., см. Копытцев В. А., **5:1** (2014), 73–83.
- Михайлов В. Г., Пуассоновская аппроксимация для распределения числа появлений заданной цепочки знаков в выходной последовательности генератора Пола, **5:4** (2014), 63–71.
- Михайлов В. Г., см. Копытцев В. А., **6:1** (2015), 57–79.
- Михайлов В. Г., Шойтов А. М., Многократные повторения длинных цепочек в конечной цепи Маркова, **6:3** (2015), 117–133.
- Михайлов В. Г., см. Меженная Н. М., **7:4** (2016), 81–94.
- Михайлов В. Г., Число разложений случайной подстановки в композицию двух инволюций с заданным циклом в одном из сомножителей, **8:1** (2017), 81–94.
- Михайлов В. Г., Управляемая полиномиальная схема размещения, **9:1** (2018), 75–88.
- Михайлов В. Г., см. Миронкин В. О., **9:3** (2018), 99–108.
- Михайлов В. Г., см. Круглов В. И., **10:4** (2019), 67–76.
- Михалев А. В., см. Грибов А. В., **1:4** (2010), 23–32.
- Михалев А. В., Нечаев А. А., Цикловые типы семейств полилинейных рекуррент и датчики псевдослучайных чисел, **5:1** (2014), 95–125.
- Нестеренко А. Ю., Об одном подходе к построению защищенных соединений, **4:2** (2013), 101–111.
- Нестеренко А. Ю., Об одном семействе универсальных функций хеширования, **6:3** (2015), 135–151.
- Нестеренко А. Ю., Об одном подходе к разложению иррациональных чисел, **9:1** (2018), 89–106.
- Нечаев А. А., см. Кузьмин А. С., **1:2** (2010), 31–56.
- Нечаев А. А., см. Михалев А. В., **5:1** (2014), 95–125.
- Николаев В. Д., Атаки на схемы электронной подписи, не учитываемые традиционными определениями стойкости, и меры противодействия им, **7:1** (2016), 93–118.
- Никонов В. Г., Саранцев А. В. О сложности совместной реализации в базисе ДНФ регулярных систем булевых функций, **1:3** (2010), 45–65.
- Никонов В. Г., О строении строго выпуклых k -значных функций, **2:1** (2011), 75–96.
- Никонов В. Г., О числе существенных переменных равновероятной булевой функции с фиксированным количеством элементарных конъюнкций в ДНФ, **2:4** (2011), 37–47.
- Никонов Н. В., Полиэдральные классы функций k -значной логики с обобщенными запретами и полужапретами, **3:1** (2012), 53–69.
- Никонов В. Г., см. Заец М. В., **4:3** (2013), 21–47.
- Ошкин И. Б., см. Алексеев Е. К., **7:1** (2016), 5–38.
- Ошкин И. Б., см. Алексеев Е. К., **7:4** (2016), 7–28.

- Панков К. Н.**, Локальная предельная теорема для распределения части вектора весов подфункций компонент случайного двоичного отображения, **5:3** (2014), 49–80.
- Панков К. Н.**, Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами, **5:4** (2014), 73–97.
- Пильщиков Д. В.**, Анализ сложности алгоритма параллельного поиска «золотой» коллизии, **6:4** (2015), 77–97.
- Пильщиков Д. В.**, Асимптотическое поведение мощности полного прообраза образа случайного множества при итерациях отображений конечного множества, **8:1** (2017), 95–106.
- Пильщиков Д. В.**, Исследование сложности метода радужных таблиц с маркерами цепочек, **8:4** (2017), 99–116.
- Пильщиков Д. В.**, Об одном теоретико-вероятностном подходе к обоснованию надежности метода Хеллмана, **10:1** (2019), 83–114.
- Пичкур А. Б.**, Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек, **3:2** (2012), 79–95.
- Пичкур А. Б.**, Описание класса подстановок, представимых в виде произведения двух подстановок с фиксированным числом мобильных точек. II, **4:1** (2013), 87–109.
- Погорелов Б. А., Пудовкина М. А.**, Свойства графов орбиталов надгрупп группы Джевонса, **1:1** (2010), 55–84.
- Погорелов Б. А., Пудовкина М. А.**, Натуральные метрики и их свойства. Ч. 1. Подметрики и надметрики, **2:4** (2011), 49–74.
- Погорелов Б. А., Пудовкина М. А.**, Натуральные метрики и их свойства. Ч. 2. Метрики типа Хемминга, **3:1** (2012), 71–95.
- Погорелов Б. А., Пудовкина М. А.**, Факторструктуры преобразований, **3:3** (2012), 81–104.
- Погорелов Б. А., Пудовкина М. А.**, Комбинаторная характеристика XL-слоев, **4:3** (2013), 99–129.
- Погорелов Б. А., Пудовкина М. А.**, Орбитальные производные над кольцом вычетов. Часть I. Общие свойства, **5:4** (2014), 99–127.
- Погорелов Б. А., Пудовкина М. А.**, Орбитальные производные над кольцом вычетов. Часть II. Вероятностно-комбинаторные свойства, **6:1** (2015), 117–133.
- Погорелов Б. А., Пудовкина М. А.**, Разбиения на биграммах и марковость алгоритмов блочного шифрования, **8:1** (2017), 107–142.
- Погорелов Б. А., Пудовкина М. А.**, Подстановочные гомоморфизмы алгоритмов блочного шифрования и $\otimes_W$ -марковость, **9:3** (2018), 109–126.
- Погорелов Б. А., Пудовкина М. А.**, $\otimes_W$ -марковость XSL-алгоритмов блочного шифрования, связанная со свойствами слоев раундовой функции, **10:1** (2019), 115–142.
- Погорелов Б. А., Пудовкина М. А.**, Характеризация отображений через свойство неизометричности, **10:4** (2019), 77–116.
- Полин С. В.**, Решение уравнений методом последовательного группирования и его оптимизация, **3:1** (2012), 97–123.
- Полин С. В.**, Заведомо разрешимые уравнения на алгебраических системах, **3:4** (2012), 91–125.
- Полин С. В.**, Системы уравнений и решетки конгруэнций универсальных алгебр, **4:4** (2013), 109–144.

Полин С. В., Перестановочные решетки отношений эквивалентности декартовых произведений, **5:3** (2014), 81–116.

Полин С. В., Перестановочные решетки отношений эквивалентности на декартовых произведениях и согласованные с ними системы уравнений. I, **6:1** (2015), 135–158.

Полин С. В., Перестановочные решетки отношений эквивалентности на декартовых произведениях и согласованные с ними системы уравнений. II, **8:3** (2017), 85–108.

Попов В. О., см. Алексеев Е. К., **7:1** (2016), 5–38.

Пудовкина М. А., см. Погорелов Б. А., **1:1** (2010), 55–84.

Пудовкина М. А., см. Погорелов Б. А., **2:4** (2011), 49–74.

Пудовкина М. А., см. Погорелов Б. А., **3:1** (2012), 71–95.

Пудовкина М. А., см. Погорелов Б. А., **3:3** (2012), 81–104.

Пудовкина М. А., Хоруженко Г. И., О классах слабых ключей обобщенной шифрсистемы PRINT, **4:2** (2013), 113–125.

Пудовкина М. А., Хоруженко Г. И., Атака на шифрсистему ГОСТ 28147-89 с 12 связанными ключами, **4:2** (2013), 127–152.

Пудовкина М. А., см. Погорелов Б. А., **4:3** (2013), 99–129.

Пудовкина М. А., см. Погорелов Б. А., **5:4** (2014), 99–127.

Пудовкина М. А., см. Погорелов Б. А., **6:1** (2015), 117–133.

Пудовкина М. А., см. Погорелов Б. А., **8:1** (2017), 107–142.

Пудовкина М. А., см. Погорелов Б. А., **9:3** (2018), 109–126.

Пудовкина М. А., см. Погорелов Б. А., **10:1** (2019), 115–142.

Пудовкина М. А., см. Погорелов Б. А., **10:4** (2019), 77–116.

Ролдугин П. В., Редукция графа при поиске реберного покрытия минимальным числом клик, **3:3** (2012), 105–128.

Ролдугин П. В., Тарасов А. В., О булевых функциях без верхних бионктивных аналогов, **4:1** (2013), 111–128.

Ролдугин П. В., Об одном методе построения булевых функций малого веса, не имеющих имплицит от фиксированного числа переменных, **7:3** (2016), 73–92.

Рыбаков А. С., Модификация алгоритма оценки количества целых чисел, имеющих не более трех больших простых делителей, **4:3** (2013), 131–158.

Рыбаков А. С., Оценки количества чисел со специальным разложением на простые множители, **7:1** (2016), 119–142.

Саранцев А. В., см. Никонов В. Г., **1:3** (2010), 45–65.

Сачков В. Н., Цикловая структура элементов централизаторов подстановок симметрической группы, **1:1** (2010), 85–100.

Сачков В. Н., Случайные отображения с неподвижными элементами, **2:2** (2011), 95–118.

Сачков В. Н., Случайные преобразования множеств с ограничениями на параметры. I, **3:1** (2012), 125–144.

Сачков В. Н., Случайные преобразования множеств с ограничениями на параметры. II, **3:2** (2012), 97–116.

- Сачков В. Н.**, Случайные подстановки с трансформированными циклами, **3:4** (2012), 127–150.
- Сачков В. Н.**, Разностные спецификации подстановок и разбиения в кольце вычетов, **5:1** (2014), 127–150.
- Сачков В. Н.**, Случайные подстановки с циклами ограниченной длины и трансформированием, **5:3** (2014), 117–136.
- Сачков В. Н.**, Комбинаторные свойства дифференциально 2-равномерных подстановок, **6:1** (2015), 159–179.
- Сачков В. Н., Круглов И. А.**, Весовые дефициты инволюций и подстановок, **7:4** (2016), 95–116.
- Сачков В. Н.**, Инволюции с данным весовым дефицитом, соответствующие таблице Кэли конечной абелевой группы, **8:4** (2017), 117–134.
- Сачков В. Н., Круглов И. А.**, Моменты весового дефицита случайной равновероятной инволюции, действующей на векторном пространстве над полем из двух элементов, **9:4** (2018), 101–124.
- Сачков В. Н., Круглов И. А.**, Дисперсия аддитивного весового дефицита равновероятной инволюции на группе вычетов, **10:3** (2019), 101–116.
- Седов Г. К.**, Стойкость ГОСТ Р 34.11-2012 к атаке поиска прообраза и к атаке поиска коллизий, **6:2** (2015), 79–98.
- Серов А. А.**, Оценки объемов окрестностей двоичных кодов в терминах их весовых спектров, **4:2** (2013), 17–42.
- Смирнов В. Г.**, Методы решения систем квазисимметрических уравнений и их применение к анализу генераторов с управляемым движением, **1:3** (2010), 67–92.
- Смирнов В. Г.**, Слои конечного автомата, **2:1** (2011), 97–118.
- Смирнов В. Г.**, Слои и циклические факторы конечных полугрупп, **2:4** (2011), 75–95.
- Смирнов В. Г.**, Дискретные функции и разреженные системы дискретных уравнений, **7:3** (2016), 93–114.
- Смирнов В. Г.**, Методы решения систем дискретных уравнений над кольцом целых чисел, основанные на построении графов решений, **9:1** (2018), 107–126.
- Смышляев С. В.**, см. Алексеев Е. К., **7:1** (2016), 5–38.
- Смышляев С. В.**, см. Алексеев Е. К., **7:4** (2016), 7–28.
- Солодовников В. И.**, О примарных функциях, минимально близких к линейным, **2:4** (2011), 97–108.
- Солодовников В. И.**, Три подхода к понятию функций, максимально отличающихся от гомоморфизмов, **7:3** (2016), 115–136.
- Тараканов В. Е.**, О сходимости итераций в методе решения задачи представления дискретного логарифма методом рациональных аппроксимаций, **1:4** (2010), 111–125.
- Тарасов А. В.**, Универсальные алгебры, порождаемые множествами выполняющих векторов бионктивных и τ -юнктивных булевых функций, **2:3** (2011), 75–98.
- Тарасов А. В.**, Свойства систем образующих универсальных алгебр, порождаемых булевыми бионктивными функциями, **3:2** (2012), 117–130.
- Тарасов А. В.**, см. Ролдугин П. В., **4:1** (2013), 111–128.
- Тарасов А. В.**, см. Литвиненко В. С., **6:1** (2015), 81–107.

Тарасов А. В., Стабилизаторы некоторых семейств булевых функций, образующих Галуа-замкнутые подалгебры алгебры Шефера, **6:4** (2015), 99–125.

Тарасов А. В., Стабилизаторы некоторых семейств булевых функций от n переменных, образующих Галуа-замкнутые подалгебры алгебры Шефера. II, **8:4** (2017), 135–156.

Тарасов А. В., см. Горшков С. П., **9:1** (2018), 5–26.

Тарасов А. В., Два метода оценивания веса булевых бионктивных функций, **9:4** (2018), 125–142.

Тимашев А. Н., Об одной аддитивной задаче теории чисел со случайным числом слагаемых, **4:1** (2013), 129–150.

Тихомирова М. И., Чистяков В. П., Статистический критерий типа критерия пустых ящиков, **1:1** (2010), 101–108.

Тихомирова М. И., Чистяков В. П., Асимптотическая нормальность числа непооявившихся значений m -зависимых случайных величин, **2:1** (2011), 119–129.

Трифонов Д. И., см. Малышев Ф. М., **7:3** (2016), 47–60.

Тришин А. Е., см. Ерохин А. В., **8:4** (2017), 29–62.

Федченко В. А., Показатели рассеивания линейной среды AES-подобных алгоритмов шифрования, **8:3** (2017), 109–126.

Федченко В. А., Минимальные согласованные системы локальных вероятностных соотношений в AES-подобных алгоритмах шифрования, **9:3** (2018), 127–142.

Хоруженко Г. И., см. Пудовкина М. А., **4:2** (2013), 113–125.

Хоруженко Г. И., см. Пудовкина М. А., **4:2** (2013), 127–152.

Цыпышев В. Н., Нижние оценки рангов координатных последовательностей линейных рекуррент максимального периода над собственным кольцом Галуа, **7:3** (2016), 137–143.

Чередник И. В., см. Круглов И. А., **10:4** (2019), 53–65.

Чистяков В. П., см. Тихомирова М. И., **1:1** (2010), 101–108.

Чистяков В. П., см. Тихомирова М. И., **2:1** (2011), 119–129.

Чистяков В. П., Об асимптотической нормальности числа пустых ячеек в одной схеме размещения частиц комплектами, **5:4** (2014), 129–138.

Шаповалов А. В., Характеристики случайных систем дискретных уравнений при неравновероятной выборке неизвестных, **1:3** (2010), 93–118.

Шаповалов А. В., Совместность случайных систем уравнений с неравновероятной выборкой двузначных неизвестных, **2:4** (2011), 109–146.

Шишкин В. А., см. Матюхин Д. В., **3:4** (2012), 71–89.

Шишков А. Б., см. Заец М. В., **4:3** (2013), 21–47.

Шишков А. Б., О бент-функциях на группе $\mathbb{Z}_{p^n}$, **6:4** (2015), 127–138.

Шойтов А. М., Структурно эквивалентные цепочки в равновероятной полиномиальной схеме, **3:3** (2012), 129–151.

Шойтов А. М., см. Михайлов В. Г., **4:1** (2013), 77–86.

Шойтов А. М., см. Михайлов В. Г., **6:3** (2015), 117–133.

Шуваев Д. В., Вычисление распределения одной комбинаторной статистики, заданной на последовательностях с фиксированным составом знаков, **2:3** (2011), 99–109.

Шуваев Д. В., О подпоследовательностях марковских последовательностей, **7:4** (2016), 133–142.

Ablayev F. M., Ablayev M. F., On the concept of quantum hashing, **7:2** (2016), 7–20.

Ablayev M. F., см. Ablayev F. M., **7:2** (2016), 7–20.

Abornev A. V., см. Nechaev A. A., **4:2** (2013), 81–100.

Abornev A. V., Recursively-generated permutations of a binary space, **5:2** (2014), 7–20.

Agievich S. V., Marchuk V. V., Maslau A. S., Semenov V. I., Bash-f: another LRX sponge function, **8:2** (2017), 7–28.

Agievich S. V., XS-circuits in block ciphers, **10:2** (2019), 7–30.

Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., Smyshlyaev S. V., Sonina L. A., On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing, **8:2** (2017), 39–50.

Ahmetzyanova L. R., Alekseev E. K., Karpunin G. A., Smyshlyaev S. V., On cryptographic properties of the CVV and PVV parameters generation procedures in payment systems, **9:2** (2018), 23–46.

Ahmetzyanova L. R., Alekseev E. K., Sedov G. K., Smyshlyaeva E. S., Smyshlyaev S. V., Practical significance of security bounds for standardized internally re-keyed block cipher modes, **10:2** (2019), 31–46.

Ahmetzyanova L. R., Karpunin G. A., Sedov G. K., Near birthday attack on “8 bits” AEAD mode, **10:2** (2019), 47–60.

Alekseev E. K., Popov V. O., Prokhorov A. S., Smyshlyaev S. V., Sonina L. A., On the performance of one perspective LSX-based block cipher, **6:2** (2015), 7–17.

Alekseev E. K., см. Ahmetzyanova L. R., **8:2** (2017), 39–50.

Alekseev E. K., Karelina E. K., Logachev O. A., On construction of correlation-immune functions via minimal functions, **9:2** (2018), 7–22.

Alekseev E. K., см. Ahmetzyanova L. R., **9:2** (2018), 23–46.

Alekseev E. K., Nikolaev V. D., Smyshlyaev S. V., On the security properties of Russian standardized elliptic curves, **9:3** (2018), 5–32.

Alekseev E. K., см. Ahmetzyanova L. R., **10:2** (2019), 31–46.

Altawy R., Duman O., Youssef A. M., Fault analysis of Kuznyechik, **7:2** (2016), 21–34.

Antipkin V. G., Smashing MASH-1, **5:2** (2014), 21–28.

Arbekov I. M., Lower bounds for the practical secrecy of a key, **8:2** (2017), 29–38.

Aref M. R., см. Karimani S., **10:2** (2019), 97–106.

Baryshnikov A. V., Katyshev S. Yu., Key agreement schemes based on linear groupoids, **8:1** (2017), 7–12.

Bogdanov D. S., Mironkin V. O., Data recovery for a neural network-based biometric authentication scheme, **10:2** (2019), 61–74.

Burov D. A., Pogorelov B. A., An attack on 6 rounds of Khazad, **7:2** (2016), 35–46.

Burov D. A., Pogorelov B. A., The influence of linear mapping reducibility on the choice of round constants, **8:2** (2017), 51–64.

Burov D. A., Pogorelov B. A., The permutation group insight on the diffusion property of linear mappings, **9:2** (2018), 47–58.

Bylkov D. N., Reconstruction of a linear recurrence of maximal period over a Galois ring of characteristic p^3 by its highest digital sequence, **5:2** (2014), 29–35.

Danilov B. R., см. Lozhkin S. A., **8:2** (2017), 87–96.

Dmukh A. A., Dygin D. M., Marshalko G. B., A lightweight-friendly modification of GOST block cipher, **5:2** (2014), 47–55.

Duman O., см. AlTawy R., **7:2** (2016), 21–34.

Dygin D. M., Grebnev S. V., Efficient implementation of the GOST R 34.10 digital signature scheme using modern approaches to elliptic curve scalar multiplication, **4:2** (2013), 47–57.

Dygin D. M., см. Dmukh A. A., **5:2** (2014), 47–55.

Dygin D. M., Lavrikov I. V., Marshalko G. B., Rudskoy V. I., Trifonov D. I., Shishkin V. A. On a new Russian Encryption Standard, **6:2** (2015), 29–34.

Eghlidos T., см. Karimani S., **10:2** (2019), 97–106.

Fedorov S. N., On a new classification of Boolean functions, **10:2** (2019), 159–168.

Fomichev V. M., Koreneva A. M., Miftakhutdinova A. R., Zadorozhny D. I., Evaluation of the maximum performance of block encryption algorithms, **10:2** (2019), 181–190.

Fomin D. B., Implementation of an XSL block cipher with MDS-matrix linear transformation on NVIDIA CUDA, **6:2** (2015), 99–108.

Fomin D. B., A timing attack on CUDA implementations of an AES-type block cipher, **7:2** (2016), 121–130.

Fomin D. B., New classes of 8-bit permutations based on a butterfly structure, **10:2** (2019), 169–180.

Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., Skew LRS of maximal period over Galois rings, **4:2** (2013), 59–72.

Goltvanitsa M. A., A construction of skew LRS of maximal period over finite fields based on the defining tuples of factors, **5:2** (2014), 37–46.

Goltvanitsa M. A., Digit sequences of skew linear recurrences of maximal period over Galois rings, **6:2** (2015), 19–27.

Goltvanitsa M. A., The first digit sequence of skew linear recurrence of maximal period over Galois ring, **7:3** (2016), 5–18.

Goltvanitsa M. A., Non-commutative Hamilton–Cayley theorem and roots of characteristic polynomials of skew maximal period linear recurrences over Galois rings, **8:2** (2017), 65–76.

- Goltvanitsa M. A.**, Equidistant filters based on skew ML-sequences over fields, **9:2** (2018), 71–86.
- Grebnev S. V.**, см. Dygin D. M., **4:2** (2013), 47–57.
- Grebnev S. V.**, Optimizing memory cost of multi-scalar multiplication, **7:2** (2016), 53–60.
- Hoang Dinh Linh**, см. Nguyen Bui Cuong, **8:1** (2017), 51–68.
- Kaplan M.**, Quantum attacks against iterated block ciphers, **7:2** (2016), 71–90.
- Karelina E. K.**, см. Alekseev E. K., **9:2** (2018), 7–22.
- Karimani S., Naghdabadi Z., Eghlidos T., Aref M. R.**, An LWE-based verifiable threshold secret sharing scheme, **10:2** (2019), 97–106.
- Karpunin G. A.**, см. Ahmetzyanova L. R., **9:2** (2018), 23–46.
- Karpunin G. A.**, см. Ahmetzyanova L. R., **10:2** (2019), 47–60.
- Katyshev S. Yu.**, см. Baryshnikov A. V. **8:1** (2017), 7–12.
- Kazymyrov A. V., Kazymyrova V. N., Oliynykov R. V.**, A method for generation of high-nonlinear S-boxes based on gradient descent, **5:2** (2014), 71–78.
- Kazymyrova V. N.**, см. Kazymyrov A. V., **5:2** (2014), 71–78.
- Kharin Yu. S.**, Parsimonious models of high-order Markov chains for evaluation of cryptographic generators, **7:2** (2016), 131–142.
- Kiryukhin V. A.**, Exact maximum expected differential and linear probability for 2-round Kuznyechik, **10:2** (2019), 107–116.
- Kolomeec N. A.**, On a property of quadratic Boolean functions, **5:2** (2014), 79–85.
- Kolomeec N. A.**, A graph of minimal distances between bent functions, **7:2** (2016), 103–110.
- Koreneva A. M.**, см. Fomichev V. M., **10:2** (2019), 181–190.
- Kozhevnikov A. A., Polikarpov S. V., Rummyantsev K. E.**, On differential properties of a symmetric cryptoalgorithm based on pseudo-dynamic substitutions, **7:2** (2016), 91–102.
- Kravtsov K. S., Kulik S. P., Radchenko I. V.**, Quantum random number generator, **7:2** (2016), 111–114.
- Kronberg D. A.**, New methods of error correction in quantum cryptography using low-density parity-check codes, **8:2** (2017), 77–86.
- Kruglov V. I.**, см. Zubkov A. M., **9:2** (2018), 99–102.
- Kulik S. P.**, см. Kravtsov K. S., **7:2** (2016), 111–114.
- Kurochkin A. V.**, On some properties of an XSL-network, **10:2** (2019), 117–124.
- Lavrikov I. V.**, см. Dygin D. M., **6:2** (2015), 29–34.
- Lavrikov I. V., Shishkin V. A.**, How much data may be safely processed on one key in different modes? **10:2** (2019), 125–134.
- Lebedev P. A.**, Comparison of old and new cryptographic hash function standards of the Russian Federation on CPUs and NVIDIA GPUs, **4:2** (2013), 73–80.
- Logachev O. A.**, см. Alekseev E. K., **9:2** (2018), 7–22.
- Lozhkin S. A., Shupletsov M. S., Danilov B. R.**, Synthesis of asymptotically size-optimal Boolean circuits protected from functionality inference, **8:2** (2017), 87–96.

- Marchuk V. V.**, см. Agievich S. V., **8:2** (2017), 7–28.
- Marshalko G. B.**, см. Dmukh A. A., **5:2** (2014), 47–55.
- Marshalko G. B.**, On the security of a neural network-based biometric authentication scheme, **5:2** (2014), 87–98.
- Marshalko G. B.**, см. Dygin D. M., **6:2** (2015), 29–34.
- Maslau A. S.**, см. Agievich S. V., **8:2** (2017), 7–28.
- Matveev S. V.**, GOST 28147-89 masking against side channel attacks, **6:2** (2015), 35–43.
- Menyachikhin A. V.**, Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters, **8:2** (2017), 97–116.
- Miftakhutdinova A. R.**, см. Fomichev V. M., **10:2** (2019), 181–190.
- Mikhailov V. G.**, **Volgin A. V.**, The stability of sets of solutions for systems of equations with random distortions, **7:3** (2016), 61–72.
- Minakov A. A.**, Poisson approximation for the number of non-decreasing runs in Markov chains, **9:2** (2018), 103–116.
- Mironkin V. O.**, см. Bogdanov D. S., **10:2** (2019), 61–74.
- Mouha N.**, см. Sekar G., **5:2** (2014), 117–125.
- Naghdabadi Z.**, см. Karimani S., **10:2** (2019), 97–106.
- Nechaev A. A.**, см. Goltvanitsa M. A., **4:2** (2013), 59–72.
- Nechaev A. A.**, **Abornev A. V.**, Nonlinear permutation of a space over a finite field induced by linear transformations of a module over a Galois ring, **4:2** (2013), 81–100.
- Nesterenko A. Yu.**, Constructions off elliptic curves endomorphisms, **5:2** (2014), 99–102.
- Nesterenko A. Yu.**, Some remarks on the elliptic curve discrete logarithm problem, **7:2** (2016), 115–120.
- Nesterenko A. Yu.**, A new authenticated encryption mode for arbitrary block cipher based on universal hash function, **8:2** (2017), 117–130.
- Nesterenko A. Yu.**, Construction of strong elliptic curves suitable for cryptographic applications, **10:2** (2019), 135–144.
- Nguyen Bui Cuong**, **Nguyen Van Long**, **Hoang Dinh Linh**, Analyzing the influence of linear redundancy in S-boxes on the affine equivalence within XSL-like round functions, **8:1** (2017), 51–68.
- Nguyen Van Long**, см. Nguyen Bui Cuong, **8:1** (2017), 51–68.
- Nikolaev M. V.**, On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism, **6:2** (2015), 45–57.
- Nikolaev V. D.**, см. Alekseev E. K., **9:3** (2018), 5–32.
- Oliynykov R. V.**, см. Kazymyrov A. V., **5:2** (2014), 71–78.
- Oshkin I. B.**, см. Ahmetzyanova L. R., **8:2** (2017), 39–50.
- Phong T. Q.**, **Toan N. Q.**, **Thanh K. X.**, A security proof for key exchange protocols, **7:4** (2016), 117–132.
- Pilshchikov D. V.**, Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number of particles and the total number of particles in the Galton-Watson process, **5:2** (2014), 103–108.

- Pilshchikov D. V.**, On the limiting mean values in probabilistic models of time-memory-data tradeoff methods, **6:2** (2015), 59–65.
- Pogorelov B. A.**, см. Burov D. A., **7:2** (2016), 35–46.
- Pogorelov B. A.**, см. Burov D. A., **8:2** (2017), 51–64.
- Pogorelov B. A.**, см. Burov D. A., **9:2** (2018), 47–58.
- Polikarpov S. V.**, см. Kozhevnikov A. A., **7:2** (2016), 91–102.
- Popov V. O.**, **Smyshlyaev S. V.**, Construction of RNG using random automata and “one-way” functions, **5:2** (2014), 109–115.
- Popov V. O.**, см. Alekseev E. K., **6:2** (2015), 7–17.
- Preneel B.**, см. Sekar G., **5:2** (2014), 117–125.
- Prokhorov A. S.**, см. Alekseev E. K., **6:2** (2015), 7–17.
- Pudovkina M. A.**, см. Vlasova V. V., **9:2** (2018), 59–70.
- Radchenko I. V.**, см. Kravtsov K. S., **7:2** (2016), 111–114.
- Rudskoy V. I.**, см. Dygin D. M., **6:2** (2015), 29–34.
- Rumyantsev K. E.**, см. Kozhevnikov A. A., **7:2** (2016), 91–102.
- Rybkin A. S.**, On software implementation of Kuznyechik on Intel CPUs, **9:2** (2018), 117–127.
- Saarinen M.-J. O.**, StriBob: authenticated encryption from GOST R 34.11-2012 LPS permutation, **6:2** (2015), 67–78.
- Sedov G. K.**, см. Ahmetzyanova L. R., **10:2** (2019), 31–46.
- Sedov G. K.**, см. Ahmetzyanova L. R., **10:2** (2019), 47–60.
- Sekar G.**, **Mouha N.**, **Preneel B.**, Meet-in-the-middle attacks on reduced-round GOST, **5:2** (2014), 117–125.
- Semenov A. M.**, Analysis of Russian key-agreement protocols using automated verification tools, **8:2** (2017), 131–142.
- Semenov V. I.**, см. Agievich S. V., **8:2** (2017), 7–28.
- Serov A. A.**, см. Zubkov A. M., **10:2** (2019), 89–96.
- Shishkin V. A.**, см. Dygin D. M., **6:2** (2015), 29–34.
- Shishkin V. A.**, см. Lavrikov I. V., **10:2** (2019), 125–134.
- Shupletsov M. S.**, см. Lozhkin S. A., **8:2** (2017), 87–96.
- Smyshlyaev S. V.**, см. Popov V. O., **5:2** (2014), 109–115.
- Smyshlyaev S. V.**, On the invariance of perfect balancedness property under the choice of tapping sequence, **5:2** (2014), 127–135.
- Smyshlyaev S. V.**, см. Alekseev E. K., **6:2** (2015), 7–17.
- Smyshlyaev S. V.**, см. Ahmetzyanova L. R., **8:2** (2017), 39–50.
- Smyshlyaev S. V.**, см. Ahmetzyanova L. R., **9:2** (2018), 23–46.
- Smyshlyaev S. V.**, см. Alekseev E. K., **9:3** (2018), 5–32.
- Smyshlyaev S. V.**, см. Ahmetzyanova L. R., **10:2** (2019), 31–46.
- Smyshlyaeva E. S.**, см. Ahmetzyanova L. R., **10:2** (2019), 31–46.
- Sonina L. A.**, см. Alekseev E. K., **6:2** (2015), 7–17.
- Sonina L. A.**, см. Ahmetzyanova L. R., **8:2** (2017), 39–50.
- Thanh K. X.**, см. Phong T. Q., **7:4** (2016), 117–132.
- Toan N. Q.**, см. Phong T. Q., **7:4** (2016), 117–132.

Trieu Quang Phong, Considering two MAC under SIG variants of the basic SIGMA protocol, **10:2** (2019), 145–158.

Trifonov D. I., см. Dygin D. M., **6:2** (2015), 29–34.

Vasiliev A. V., Ziatdinov M. T., Minimizing collisions for quantum hashing, **7:2** (2016), 47–52.

Vlasova V. V., Pudovkina M. A., Group Properties of Block Ciphers of the Russian Standards GOST R 34.11-2012 and GOST R 34.12-2015, **9:2** (2018), 59–70.

Volgin A. V., см. Mikhailov V. G., **7:3** (2016), 61–72.

Vysotskaya V. V., Some properties of modular addition, **10:2** (2019), 75–88.

Youssef A. M., см. AlTawy R., **7:2** (2016), 21–34.

Zadorozhny D. I., см. Fomichev V. M., **10:2** (2019), 181–190.

Zaitsev S. N., см. Goltvanitsa M. A., **4:2** (2013), 59–72.

Zaitsev S. N., Description of maximal skew linear recurrences in terms of multipliers, **5:2** (2014), 57–70.

Zhukov K. D., Approximate common divisor problem and continued fractions, **7:2** (2016), 61–70.

Zhukov K. D., Approximate common divisor problem and lattice sieving, **9:2** (2018), 87–98.

Ziatdinov M. T., см. Vasiliev A. V., **7:2** (2016), 47–52.

Zubkov A. M., Kruglov V. I., On quantiles of minimal codeword weights of random linear codes over $\mathbb{F}_p$, **9:2** (2018), 99–102.

Zubkov A. M., Serov A. A., Testing the NIST Statistical Test Suite on artificial pseudorandom sequences, **10:2** (2019), 89–96.