

Сведения об официальных оппонентах
по диссертации Николаева Максима Владимировича
«О сложности решения некоторых обобщений задачи дискретного логарифмирования»

Ф.И.О.: Катышев Сергей Юрьевич

Ученая степень: кандидат физико-математических наук

Ученое звание:

Научная(ые) специальность(и): 20.03.04 – теоретическая криптография

Должность: доцент базовой кафедры 252 (кафедра информационной безопасности)

Место работы: МИРЭА – Российский технологический университет

Адрес места работы: 119454 г. Москва, проспект Вернадского, дом 78

E-mail: sk@v-olymp.ru

Список основных научных публикаций по специальности 20.03.04 - теоретическая криптография за последние 5 лет:

1. А. В. Зязин, С. Ю. Катышев, “Необходимые условия перестановочности степеней в конечномерных алгебрах над полем”, *Дискрет. матем.*, 29:3 (2017), 38–44
2. V. Baryshnikov, S. Yu. Katyshev, “Key agreement schemes based on linear groupoids”, *Матем. вопр. криптогр.*, 8:1 (2017), 7–12
3. С. Ю. Катышев, В. Т. Марков, А. А. Нечаев, “Использование неассоциативных группOIDов для реализации процедуры открытого распределения ключей”, *Дискрет. матем.*, 26:3 (2014), 45–64; *Discrete Math. Appl.*, 25:1 (2015), 9–24
4. С. Ю. Катышев, “Дискретное логарифмирование в конечномерной алгебре над полем”, *ПДМ*, 2014, № 4(26), 21–27
5. А. В. Зязин, С. Ю. Катышев, “Способ безопасного распределения баз данных между ограниченно доверенными облаками”, *Обозрение прикладной и промышленной математики*, 23:5 (2016).

Ф.И.О.: Михайлов Владимир Гаврилович

Ученая степень: доктор физико-математических наук

Ученое звание: старший научный сотрудник

Научная(ые) специальность(и): 01.01.09 – Дискретная математика и математическая кибернетика

Должность: Отдел дискретной математики, ведущий научный сотрудник

Место работы: Математический институт им. В.А. Стеклова РАН

Адрес места работы: 119991, Москва, ул. Губкина, д. 8

Тел.: 8(499)941-01-84

E-mail: mikhail@mi.ras.ru

Список основных научных публикаций по специальности 01.01.09 - Дискретная математика и математическая кибернетика за последние 5 лет:

1. В. Г. Михайлов, “Число разложений случайной подстановки в композицию двух инволюций с заданным циклом в одном из сомножителей”, Матем. вопр. криптогр., 8:1 (2017), 80–94
2. Н. М. Меженная, В. Г. Михайлов, “О свойствах выходной последовательности мультициклического генератора над прямой суммой групп вычетов по модулю 2”, Дискрет. матем., 29:3 (2017), 45–53
3. В. Г. Михайлов, “О вероятности наличия в случайной последовательности цепочек с одинаковой структурой”, Дискрет. матем., 28:3 (2016), 97–110
4. V. G. Mikhailov, A. V. Volgin, “The stability of sets of solutions for systems of equations with random distortions”, Матем. вопр. криптогр., 7:3 (2016), 61–72
5. Н. М. Меженная, В. Г. Михайлов, “Об асимптотической нормальности чисел появлений знаков в неравновероятной мультициклической случайной последовательности по модулю 4”, Матем. вопр. криптогр., 7:4 (2016), 81–94

Ф.И.О.: Гашков Сергей Борисович

Ученая степень: доктор физико-математических наук

Ученое звание: профессор

Научная(ые) специальность(и): 01.01.09 – Дискретная математика и математическая кибернетика

Должность: профессор по кафедре дискретной математики, Механико-математический факультет, Отделение математики

Место работы: МГУ имени М.В. Ломоносова

Адрес места работы: ул. Ленинские Горы, 1, к. 13-14, Москва, 119234

Тел.: +7(495)9394268

E-mail: sbgashkov@gmail.com

Список основных научных публикаций по специальности 01.01.09 - Дискретная математика и математическая кибернетика за последние 5 лет:

1. С. Б. Гашков, И. С. Сергеев, “Об аддитивной сложности матриц НОД и НОК”, Матем. заметки, 100:2 (2016), 196–211; *Math. Notes*, 100:2 (2016), 199–212
2. С. Б. Гашков, “Арифметическая сложность некоторых линейных преобразований”, Матем. заметки, 97:4 (2015), 529–555; *Math. Notes*, 97:4 (2015), 531–555
3. С. Б. Гашков, “Арифметическая сложность преобразований Стирлинга”, Дискрет. матем., 26:4 (2014), 23–35; *Discrete Math. Appl.*, 25:2 (2015), 83–92
4. С. Б. Гашков, “Неравенство Бернштейна, тождество Рисса и формула Эйлера для ряда обратных квадратов”, Матем. просв., сер. 3, 18, Изд-во МЦНМО, М., 2014, 143–171
5. С. Б. Гашков, И. С. Сергеев, “О сложности и глубине булевых схем для умножения и инвертирования в конечных полях характеристики 2”, Дискрет. матем., 25:1 (2013), 3–32; *Discrete Math. Appl.*, 23:1 (2013), 1–37

Учёный секретарь

диссертационного совета МГУ.05.01,

кандидат физико-математических наук

Кривчиков М.А.