Update: 2021/08/19

Семен Новоселов

Контакты

БФУ им.И.Канта, ИФМНиИТ
ул. А. Невского 14
236016 Калининград, Россия

+79622574189
snovoselov@kantiana.ru
novsem@gmail.com
https://crypto-kantiana.com/semyon.novoselov

Работа

Старший преподаватель 2020-н.в.
БФУ им.И.Канта,
Институт физико-математических наук и информационных технологий

Младший научный сотрудник без ученой степени 2020-н.в.
БФУ им.И.Канта,
Лаборатория "Математические методы защиты и обработки информации"

Инженер (проект 5-100) 2021-н.в.
БФУ им.И.Канта,
Лаборатория "Математические методы защиты и обработки информации"

Ассистент 2013-2020
БФУ им.И.Канта,
Институт физико-математических наук и информационных технологий

Аспирант 2013-2016
Тема: "Подсчёт числа точек на гиперэллиптических кривых с геометрически разложимым якобианом"
БФУ им.И.Канта,
Институт физико-математических наук и информационных технологий

Научные интересы

Алгебраическая геометрия, теория чисел, криптография, гиперэллиптические кривые, подсчёт точек, изогении

Образование

Высшее (специалист) Январь 2013
БФУ им.И.Канта
Калининград, Россия

- Тема: *Гиперэллиптическая криптография*
- Научный руководитель: Юрий Болтнев

Публикации в журналах

1. Е. А. Киршанова, Е. С. Малыгина, С. А. Новоселов, Д. О. Олефиренко, "Алгоритм вычисления идеала Штикельбергера для мультиквадратичных полей", ПДМ, 2021, № 51, 9–30
2. S. A. Novoselov, "Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$", Finite Fields and Their Applications, vol. 68, 2020, no. 101757. Scopus/WoS: **Q1**.
3. N. S. Kolesnikov, S. A. Novoselov, "On the distribution of orders of Frobenius action on ℓ-torsion of abelian surfaces", ПДМ, 2020, № 48, 22–33
4. S. A. Novoselov, "Hyperelliptic curves, Cartier-Manin matrices and Legendre polynomials", PDM, 2017, no. 37, 20-31
5. S. A. Novoselov, "On bounds for balanced embedding degree", PDM, 2016, no. 2(32), 63-86

Публикации в трудах конференций

1. Е. А. Киршанова, Н. С. Колесников, Е. С. Малыгина, С. А. Новоселов, “Проект стандартизации постквантовой цифровой подписи”, ПДМ. Приложение, 2020, № 13, 44–51
2. Д. О. Олефиренко, Е. А. Киршанова, Е. С. Малыгина, С. А. Новоселов, “Алгоритм вычисления элемента Штикельбергера для мнимых мультиквадратичных полей”, ПДМ. Приложение, 2020, № 13, 12–17
3. E. S. Malygina, S. A. Novoselov, “Division polynomials for hyperelliptic curves defined by Dickson polynomials”, Матем. вопр. криптогр., 11:2 (2020), 69–81. CTCrypt’2019.
4. S. A. Novoselov, Y. F. Boltnev, “Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields”, PDM. Prilozhenie, 2019, no. 12, 44–46. SibeCrypt’2019.
5. E. M. Melnichuk, S. A. Novoselov, “On characteristic polynomials for some genus 2 and 3 curves with p-rank 1”, Prikl. Diskr. Mat. Suppl., 2019, no. 12, 21–24. SibeCrypt’2019.
6. N. S. Kolesnikov, S. A. Novoselov, “On the order of the Frobenius endomorphism action on l-torsion subgroup of abelian surfaces”, PDM. Suppl., 2019, no. 12, 11–12. SibeCrypt’2019.
7. S. A. Novoselov, “Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$”, PDM. Prilozhenie, 2018, no. 11, 30–33. SibeCrypt’2018
8. S. A. Novoselov, “Hyperelliptic curves, Cartier–Manin matrices and Legendre polynomials”, PDM. Prilozhenie, 2017, no. 10, 29–32. SibeCrypt’2017

Преподаваемые дисциплины

Лекции

Специалитет – Компьютерный практикум по криптографии на эллиптических кривых 2020
БФУ им.И.Канта

Специалитет – Внешний аудит безопасности корпоративных сетей 2020-2021
БФУ им.И.Канта

Специалитет – Модели безопасности Весна 2018
БФУ им.И.Канта

Специалитет – Защита в ОС Весна 2018
БФУ им.И.Канта

Специалитет – Защита в сетях 2013-2018
БФУ им.И.Канта

Мероприятия

ОРГАНИЗАТОР:
Летняя школа IACR: “Euclidean lattices: theory and applications”, Калининград, Россия. 2019

Гранты

- Стипендия Эйлера фонда DAAD (визит в университет г.Лейпцига) Июль 2014
- Грант РФФИ №18-31-00244 на выполнение научного исследования "Разработка эффективных алгоритмов для подсчёта точек в якобианах гиперэллиптических кривых над конечным полем" 2018-2019

Выступления

- Counting points on hyperelliptic curves with geometrically split Jacobians [poster].
  Fourteenth Algorithmic Number Theory Symposium, ANTS-XIV,
  University of Auckland, New Zealand — Июль 2020
- Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields
  SibeCrypt, Томск, Россия — Сентябрь 2019
- Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$
  SibeCrypt, Абакан, Россия — Сентябрь 2018
- Hyperelliptic curves, Cartier-Manin matrices and Legendre polynomials
  SibeCrypt, Красноярск, Россия — Сентябрь 2017

Языки

- Английский (B1)
- Русский (родной)

Владение языками программирования

- C/C++, Python, Ruby, Sage, Maple, Maxima