Update: 2020/09/22

Semyon Novoselov

Contact Information

I. Kant BFU
Nevskogo St. 14
236016 Kaliningrad, Russia

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

Positions

PhD-student 2013-present
Topic: "Counting points on hyperelliptic curves over finite field"
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Teaching assistant 2013-present
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Research Interests

Algebraic geometry, cryptography, hyperelliptic curves, point-counting algorithms.

Education

Dipl. Math. January 2013
I. Kant Baltic Federal University
Kaliningrad, Russia

- Topic: *Hyperelliptic cryptography*
- Advisor: Yurii Boltnev

Journal Publications

1. S. A. Novoselov, "Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$". 2020. (Accepted in journal Finite Fields and Their Applications). Preprint: https://arxiv.org/abs/1902.05992
2. N. S. Kolesnikov, S. A. Novoselov, "On the distribution of orders of Frobenius action on ℓ-torsion of abelian surfaces", Prikl. Diskr. Mat., 2020, no. 48, 22–33
3. S. A. Novoselov, "Hyperelliptic curves, Cartier-Manin matrices and Legendre polynomials", Prikl. Diskr. Mat., 2017, no. 37, 20–31
4. S. A. Novoselov, "On bounds for balanced embedding degree", Prikl. Diskr. Mat., 2016, no. 2(32), 63–86

Conference Publications

1. N. S. Kolesnikov, S. A. Novoselov, "On the order of the Frobenius endomorphism action on ℓ-torsion subgroup of abelian surfaces", Prikl. Diskr. Mat. Suppl., 2019, no. 12, 11–12. SibeCrypt'2019.
2. 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.
3. 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.
4. 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
5. S. A. Novoselov, "Hyperelliptic curves, Cartier–Manin matrices and Legendre polynomials", PDM. Prilozhenie, 2017, no. 10, 29–32. SibeCrypt'2017

Teaching Experience

Lecturer at I. Kant BFU

Master – Algorithms for elliptic curve cryptography	Autumn 2020
Master – Network Security	2013-2018
Master – Security Models	Spring 2018
Master – Operating systems security	Spring 2018

Activities

ORGANIZER:
IACR Summer School "Euclidean lattices: theory and applications", Kaliningrad, Russia. 2019

Grants

- Russian Foundation for Basic Research (RFBR). Project no. 18-31-00244.
  "Counting points on hyperelliptic curves over finite fields"
  Role: Project Lead, Principal Researcher 2018-2020
- Euler Travel Grant (visit at the University of Leipzig) Jul. 2014

Presentations

- Counting points on hyperelliptic curves with geometrically split Jacobians [poster].
  Fourteenth Algorithmic Number Theory Symposium, ANTS-XIV,
  University of Auckland, New Zealand June 30 - July 4, 2020
- Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields
  SibeCrypt, Tomsk, Russia September 2019
- Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$
  SibeCrypt, Abakan, Russia September 2018
- Hyperelliptic curves, Cartier–Manin matrices and Legendre polynomials
  SibeCrypt, Krasnoyarsk, Russia September 2017

Languages

- English (intermediate)
- Russian (native)

Programming skills

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