Update: 2023/11/10

Semyon Novoselov

Contact Information

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

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

Positions

Researcher 2022-present
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Lecturer 2020-present
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Research assistant 2020-2022
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Teaching assistant 2013-2020
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

PhD-student 2013-2016
Topic: "Counting points on hyperelliptic curves with geometrically split Jacobians"
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology
Defense in May 2022

Student 2008-2013
Computer Security (Specialist[1])
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Research Interests

Number theory, cryptography, cryptanalysis, isogenies, (hyper)elliptic curves, ideal lattices.

Education

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

- Topic: *Computing discrete logarithm on elliptic curve using Weil pairing*
- Advisor: Yurii Boltnev

PhD[2] in Math. May 2022
Siberian Branch of the Russian Academy of Sciences
Sobolev Institute of Mathematics

- Topic: *Counting points on hyperelliptic curves with geometrically split Jacobians*
- Advisor: Dr. Ekaterina Malygina

[1] This specialist degree is issued after completing 5.5 year studying program and is equivalent to master degree.

[2] I have "Candidate of Sciences in Physics and Mathematics" degree. This is Russian equivalent to PhD degree.

Journal Publications

1. S. A. Novoselov, "On ideal class group computation of imaginary multiquadratic fields", Prikl. Diskr. Mat., no. 58, pp. 22–30 (2022)
2. S. A. Novoselov and Yu. F. Boltnev, "On the number of points on the curve $y^2 = x^7 + ax^4 + bx$ over a finite field", J. Appl. Ind. Math., vol. 16, pp. 302–312 (2022)
3. E. A. Kirshanova, E. S. Malygina, S. A. Novoselov, D. O. Olefirenko, "An algorithm for computing the Stickelberger ideal for multiquadratic number fields", Prikl. Diskr. Mat., no. 51, pp. 9–30 (2021)
4. S. A. Novoselov, "Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$", Finite Fields and Their Applications, 68, 101757 (2020)
5. N. S. Kolesnikov, S. A. Novoselov, "On the distribution of orders of Frobenius action on ℓ-torsion of abelian surfaces", Prikl. Diskr. Mat., no. 48, pp. 22–33 (2020)
6. S. A. Novoselov, "Hyperelliptic curves, Cartier-Manin matrices and Legendre polynomials", Prikl. Diskr. Mat., no. 37, pp. 20–31 (2017)

Conference Publications

1. S. A. Novoselov, "On the Discrete Logarithm Problem in the Ideal Class Group of Multiquadratic Fields". LNCS, vol. 14168, 192–211. LatinCrypt 2023.
2. Yu. F. Boltnev, S. A. Novoselov, V. A. Osipov, "On construction of maximal genus 3 hyperelliptic curves", Prikl. Diskr. Mat. Suppl., 2021, no. 14, 24–30. SibeCrypt 2021
3. E. A. Kirshanova, N. S. Kolesnikov, E. S. Malygina, S. A. Novoselov, "Post-quantum signature proposal for standardisation", Prikl. Diskr. Mat. Suppl., 2020, no. 13, 44-51. SibeCrypt 2020
4. 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
5. E. S. Malygina, S. A. Novoselov, "Division polynomials for hyperelliptic curves defined by Dickson polynomials", Matem. vopr. kriptogr., 11:2 (2020), 69–81. CTCrypt 2019
6. 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
7. 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
8. 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
9. 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	2020-present
Master – Security Audit	2013-2022
Master – Network Security	2013-present

Activities

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

SUBREVIEWER: Crypto 2021, PKC 2022, ANTS-XV 2022, AsiaCrypt 2022-2023, LatinCrypt 2023.

Grants

- Russian Science Foundation. Project no. 22-41-04411.
  "Cryptanalysis of post-quantum lattice- and code-based primitives: practical records and theoretical improvements"
  Role: Researcher 2022-present
- 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

- On construction of maximal genus 3 hyperelliptic curves September 2021,
  SibeCrypt, Novosibirsk, Russia
- 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, Pari/GP, Maxima, Maple.

References

Elena Kirshanova elenakirshanova@gmail.com
Lead Cryptographer
Technology Innovation Institute (TII)
Cryptography Research Center

Ekaterina Malygina ekkat82@gmail.com
Associate Professor, Researcher
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology