Update: 2021/08/21

Ekaterina Malygina

Contact Information

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

+79622546654
EMalygina@kantiana.ru
https://crypto-kantiana.com/ekaterina.malygina/

Positions

Associate Professor, Researcher October 2016-present
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Senior Lecturer September 2010-September 2016
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Teaching assistant September 2005-August 2010
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Research Interests

Algebraic geometry, elliptic and hyperelliptic curves, algebraic number theory, function fields, coding theory, cryptography.

Education

Dipl. Math. June 2005
I. Kant Baltic Federal University
Kaliningrad, Russia

- Topic: *Ray class group of number fields*
- Advisor: Dr. Sergey Aleshnikov

Dr. rer. nat. January 2016
Institute for Information Transmission Problems (Russian Academy of Sciences)

- Topic: *Explicit constructions of optimal curves of genus three*
- Advisor: Dr. Alexey Zaytsev

Journal Publications

1. Kirshanova E. A., Malygina E. S., Novoselov S. A., Olefirenko D. O. *An algorithm for computing the Stickelberger ideal for imaginary multiquadratic fields.* Prikl. Diskr. Math. No. 51, 9—30, 2021.
2. E. S. Malygina, S. A. Novoselov. *Division polynomials for hyperelliptic curves defined by Dickson polynomials.* Mathematical Aspects of Cryptography, Volume 11:2, 69—81, 2020.
3. E. Alekseenko, A. Zaytsev. *Explicit equations of optimal curves of genus 3 over certain fields with three parametrs.* Contemporary Mathematics, Volume: 637, 245–251, 2015.
4. E. Alekseenko, S. Aleshnikov, N. Markin, A. Zaytsev. *Optimal curves over finite fields with discriminant* −19. Finite Fields and Their Applications, 17(4): 350–358, 2011.
5. Е. Алексеенко. *Алгебро-геометрический код, ассоциированный с кривой рода* 3 *над конечным полем с дискриминантом* −19. Вестник Российского государственного университета им. И. Канта, (10): 104–107, 2010.

6. Е. С. Алексеенко, С. И. Алешников, А. И. Зайцев. *Общие уравнения оптимальных кривых над конечным полем с дискриминантом* −19. Вестник Российского государственного университета им. И. Канта, (10): 73–79, 2008.

7. Е. С. Каменских. *Структура группы лучевых классов числового поля и алгоритм ее вычисления.* Вестник Российского государственного университета им. И. Канта, (10): 112–115, 2006.

Conference Publications

1. Olefirenko D. O., Kirshanova E. A., Malygina E. S., Novoselov S. A. An algorithm for computing the Stickelberger elements for imaginary multiquadratic fields. SibeCrypt 2020.

2. Kirshanova E. A., Kolesnikov N. S, Malygina E. S., Novoselov S. A. Post-qauntum signature proposal for standardisation. SibeCrypt 2020.

3. E. S. Malygina. Calculation of 3-torsion ideal for some class of hyperelliptic curves. SibeCrypt 2019.

4. E. Malygina, S. Novoselov. Division polynomials for hyperelliptic curves defined by Dickson polynomials. CTCrypt 2019.

5. E. S. Malygina. Investigation of automorphism group for code associated with optimal curve of genus three. SibeCrypt 2018.

6. E. Alekseenko. A method of finding explicit equation for optimal curve of genus 4. ACCT 2014.

7. E. Alekseenko, A. Zaytsev. New method of constructing optimal curves of genus 3 over certain finite fields. AGCT 2013.

8. E. S. Alekseenko. Algorithm for calculation of D-gap numbers and D-Weierstrass points. SibeCrypt 2011.

9. E. S. Alekseenko, S. I. Aleshnikov, A. I. Zaytsev. Optimal curves of genus 3 over finite field of discriminant -19. SibeCrypt 2010.

10. Kamenskikh E. S. Ray class group of number field like a base of cryptosystem. The III International Scientific Practical Conference: Research, working out and application of high technologies in the industry 2007.

11. Kamenskikh E. S. Data security system based on ray class group of number field. The IV All-Russian Conference: Irreversible processes in the nature and the technician 2007.

Teaching Experience

Lecturer at I. Kant BFU

Master – Applied Algebra	2010–2021
Master – Number Theory	2016–2021
Master – Theoretical-Number Methods in Cryptography	2010–2021
Master – Fast Multipliers	2013–2021
Master – Methods of Algebraic Number Theory in Cryptography	2010–2021

Master – Methods and Algorithms for Generation of Elliptic Curves in Cryptography 2016–2021

Master – Calculation Methods of Discrete Logarithm 2010–2021

Master – Algorithms for Hyperelliptic Curves Cryptography 2016–2019

Master – Theory of Pseudo-Random Generators 2010–2013

Teaching Assistant at I. Kant BFU

Master – Applied Algebra 2005–2009

Master – Linear Algebra 2005–2009

Master – Methods of Algebraic Number Theory in Cryptography 2005–2009

Master – Algorithms for Elliptic Curve Cryptography 2005–2009

Master – Algorithms for Hyperelliptic Curve Cryptography 2005–2009

Master – Theory of Finite Fields 2005–2009

Activities

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

Awards

- Euler Travel Grant (visit at the Technical University of Munich) Jan. 2008
- Best Research Work between Young Mathematicians of Russia (Stipendium of Foundation "Dynasty") 2013–2015

Presentations

- Introduction in theory of elliptic curves and cryptography
  Summer school-conference on cryptography and information security, Novosibirsk, Russia July 2020
- Calculation of 3-torsion ideal for some class of hyperelliptic curves
  SibeCrypt, Tomsk, Russia September 2019
- Division polynomials for hyperelliptic curves defined by Dickson polynomials
  CTCrypt, Svetlogorsk, Russia June 2019
- Investigation of automorphism group for code associated with optimal curve of genus three
  SibeCrypt, Abakan, Russia September 2018
- Properties and explicit equations of optimal curves of genus 3
  Meeting of generations by Foundation "Dynasty", Moscow, Russia June 2015
- A method of finding explicit equation for optimal curve of genus 4
  ACCT, Svetlogorsk, Russia September 2014
- New method of constructing optimal curves of genus 3 over certain finite fields
  AGCT, *CIRM*,Marseille, France June 2013
- About one method of constructing optimal curves of genus 3 over finite fields
  Arithmetic days, Saint Petersburg, Russia May 2013

Languages

- English (intermediate)

- Russian (native)

PROGRAMMING SKILLS

- Sage, Maple, Magma