Update: 2024/03/18

Elena Kirshanova

Contact Information

TII
PO Box: 9639
Masdar City, Abu Dhabi, UAE

elenakirshanova@gmail.com
elena.kirshanova@rub.de
https://crypto-kantiana.com/elena.kirshanova/

Positions

Lead cryptographer (primal affiliation) — June 2022-present
Cryptography Research Center
Technology Innovation Institute

Lecturer (secondary affiliation) — September 2019-present
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Researcher (secondary affiliation) — December 2019-present
Laboratory of "Mathematical methods in information security"
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Postdoctoral researcher (25%) — May 2021-December 2021
Ruhr University Bochum
Faculty of Mathematics
Chair of Cryptology and IT-Security

Postdoctoral researcher — January 2017-June 2019
ENS Lyon
Department of Computer Science
LIP, team ARIC

Teaching assistant — May 2013-December 2016
Ruhr University Bochum
Faculty of Mathematics
Chair of Cryptology and IT-Security

Research Interests

Lattice-based cryptography, cryptanalysis, algorithms for hard problems on lattices (practical and theoretical), quantum algorithms, cryptanalysis of code-based cryptographic constructions.

Education

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

- Topic: *Lattice-based cryptography*
- Advisor: Dr. Sergey Aleshnikov

Dr. rer. nat. — December 2016
Ruhr University Bochum
Faculty of Mathematics,
Chair of Cryptology and IT-Security

- Topic: *Complexity of the Learning with Errors Problem and Memory-Efficient Lattice Sieving*
- Advisor: Prof. Dr. Alexander May

Conference Publications

Full texts of all publications can be accessed via
https://crypto-kantiana.com/elena.kirshanova/

1. L. Ducas, A. Esser, S. Etinski, E. Kirshanova. Asymptotics and Improvements of Sieving for Codes. Eurocrypt 2024.
2. E. Kirshanova, A. May, J. Nowakowski. New NTRU Records with Improved Lattice Bases. PQCrypto 2023.
3. S. Agrawal, E. Kirshanova, D. Stehlé, A. Yadav. Practical, Round-Optimal Lattice-Based Blind Signatures. ACM CCS 2022.
4. J.-F. Biasse, X. Bonnetain, E. Kirshanova, A. Schrottenloher, F. Song Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. IET Information Security Journal.
5. E. Kirshanova, A. May. Decoding McEliece with a Hint – Secret Goppa Key Parts Reveal Everything. SCN 2022.
6. E. Kirshanova, A. May. How to Find Ternary LWE Keys Using Locality Sensitive Hashing. IMACC 2021.
7. E. Kirshanova, T. Laarhoven. Lower bounds for nearest neighbor searching and post-quantum cryptanalysis. Crpyto 2021
8. I. van Hoof, E. Kirshanova, A. May. Quantum Key Search for Ternary LWE. PQCrypto 2021
9. E. Kirshanova, E. Malygina, S. Novoselov, D. Olefirenko An algorithm for computing the Stikelberger element for imaginary multiquadratic fields, (in RUS). SybeCrypt2020
10. E. Kirshanova, E. Mårtensson, E. W. Postlethwaite, Subhayan Roy Moulik. Quantum Algorithms for the Approximate k-List Problem and their Application to Lattice Sieving. AsiaCrypt 2019
11. M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, M. Stevens. The General Sieve Kernel and New Records in Lattice Reduction. EuroCrypt 2019
12. E. Kirshanova. Improved Quantum Information Set Decoding, PQCrypto 2018
13. Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and the Generalized Hidden Shift Problem. PKC 2018
14. G. Herold, E. Kirshanova, T. Laarhoven. Speed-ups and time–memory trade-offs for tuple lattice sieving. PKC 2018
15. G. Herold, E. Kirshanova. Improved Algorithms for the Approximate k-List Problem in Euclidean norm. PKC 2017.
16. E. Kirshanova, A. May, and F. Wiemer. Parallel implementation of BDD enumeration for LWE. ACNS 2016.
17. E. Kirshanova. Proxy re-encryption from lattices. PKC 2014.

Journal Publications

1. E. Kirshanova, E. Malygina. Construction-D lattice from Garcia-Stichtenoth tower code. Dec. 2023. *Designs, Codes and Cryptography*
2. E. Kirshanova, E. Malygina, S. Novoselov, D. Olefirenko. An algorithm for computing the Stickelberger ideal of multiquadratic number field (in RUS). Prikladnaya Diskretnaya Matematika.
3. E. Kirshanova, H. Nguyen, D. Stehlé, A. Wallet. On the smoothing parameter and last minimum of random orthogonal lattice, Jan. 2020, *Designs, Codes and Cryptography*
4. G. Herold, E.Kirshanova, A. May. On the Asymptotic Complexity of Solving LWE, Jan. 2017, *Designs, Codes and Cryptography*

Teaching Experience

Lecturer

Lattice-based cryptography (I. Kant BFU)	Spring'21–'24
Crypto 101(I. Kant BFU)	Spring'20 – 23
Short summer course Git + LaTeX + Sage (I. Kant BFU)	Summer'20, '21
Coding Theory (I. Kant BFU)	Autumn'19 – '23
Algorithms for elliptic curve cryptography (I. Kant BFU)	Autumn'19, 20
Cryptanalysis (M2, ENS de Lyon)	Autumn'18

Teaching Assistant

Computer Algebra (M1, ENS de Lyon)	Spring'18,'19
Probability (L3, ENS de Lyon)	Spring'17
Quantum Random Walks (seminar) (RUB)	Winter'16,'17
Cryptanalysis I-II (RUB)	Spring'14,'15
Quantum Algorithms (RUB)	Winter'13,'14

Internship supervisions :

- Thanh Huyen Nguyen (ENS Lyon, Master student, co-supervision with A.Wallet, D.Stehlé) 2018

PhD supervisions:

- Alexander Karening (BFU) 2022 – 2025 (tentative)
- Thanh Huyen Nguyen, co-supervised with D.Stehlé (ENS Lyon).

Activities

PROGRAM COMMITTEES: LatinCrypt 2023; Crypto 2020, 2021; PQCrypto 2020, 2021, 2022, 2023; ANTS-XIV, AsiaCrypt 2019, 2021, 2022, 2023; IndoCrypt 2018

ORGANISER:
Quantum Cryptanalysis of Post-Quantum Cryptography, The Simons Institute for the Theory of Computing, Berkeley, USA, 2020.
IACR Summer School "Euclidean lattices: theory and applications", Kaliningrad, Russia. 2019

Awards

- Metchnikov travel grant 2020
- The Young Mathematician Award 2020
- Best Student Paper Award, ACNS'16 June 2016
- Euler Travel Grant (visit at the University of Leipzig) Feb. 2012

VISITS	**Short-term research visitor** The Simons Institute for the Theory of Computing Berkeley, USA	January 2020-February 2020
PRESENTATIONS	Slides of my talks are available at https://crypto-kantiana.com/elena.kirshanova/#talks	
LANGUAGES	• English (fluent) • German (intermediate) • French (intermediate) • Russian (native)	
PROGRAMMING SKILLS	• C++, Python, Sage, Maple	
REFERENCES	Damien Stehlé Professor Department of Computer Science ENS de Lyon	damien.stehle@gmail.com
	Alexander May Professor at the University of Bochum Faculty of Mathematics Chair of Cryptology and IT-Security	alex.may@rub.de