Update: 2025/11/19

Elena Kirshanova

Contact Information

TII
PO Box: 9639
Yas Island, Abu Dhabi, UAE

elenakirshanova@gmail.com

https://elenakirshanova.github.io/

Positions

Lead cryptographer June 2022-present
Cryptography Research Center
Technology Innovation Institute

Lecturer (secondary affiliation since 2022) September 2019-May 2024
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

Head of the Lab, researcher December 2019-June 2022
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, security of Fully Homomorphic Encryption.

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://elenakirshanova.github.io/

1. A. Karenin, E. Kirshanova, A. May, J. Nowakowski. Fast Slicer for Batch-CVP: Making Lattice Hybrid Attacks Practical. AsiaCrypt 2025.
2. S. Bai, H. Jangir, E. Kirshanova, T. Ngo, W. Youmans. A quasi-polynomial time algorithm for the extrapolated dihedral coset problem over power-of-two moduli. Crypto 2025.
3. O. Hanyecz, A. Karenin, E. Kirshanova, P. Kutas, S. Schaeffler. Constant time lattice reduction in dimension 4 with application to SQIsign. CHES 2025.
4. A. Karenin, E. Kirshanova. Finding dense submodules with algebraic lattice reduction. AfricaCrypt 2024
5. E. Kirshanova. C. Marcolla, S. Rovira. Guidance for efficient selection of secure parameters for fully homomorphic encryption. AfricaCrypt 2024
6. L. Ducas, A. Esser, S. Etinski, E. Kirshanova. Asymptotics and Improvements of Sieving for Codes. Eurocrypt 2024.
7. E. Kirshanova, A. May, J. Nowakowski. New NTRU Records with Improved Lattice Bases. PQCrypto 2023.
8. S. Agrawal, E. Kirshanova, D. Stehlé, A. Yadav. Practical, Round-Optimal Lattice-Based Blind Signatures. ACM CCS 2022.
9. 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.
10. E. Kirshanova, A. May. Decoding McEliece with a Hint – Secret Goppa Key Parts Reveal Everything. SCN 2022.
11. E. Kirshanova, A. May. How to Find Ternary LWE Keys Using Locality Sensitive Hashing. IMACC 2021.
12. E. Kirshanova, T. Laarhoven. Lower bounds for nearest neighbor searching and post-quantum cryptanalysis. Crpyto 2021
13. I. van Hoof, E. Kirshanova, A. May. Quantum Key Search for Ternary LWE. PQCrypto 2021
14. E. Kirshanova, E. Malygina, S. Novoselov, D. Olefirenko An algorithm for computing the Stikelberger element for imaginary multiquadratic fields, (in RUS). SybeCrypt2020
15. 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
16. 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
17. E. Kirshanova. Improved Quantum Information Set Decoding, PQCrypto 2018
18. Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and the Generalized Hidden Shift Problem. PKC 2018
19. G. Herold, E. Kirshanova, T. Laarhoven. Speed-ups and time–memory trade-offs for tuple lattice sieving. PKC 2018
20. G. Herold, E. Kirshanova. Improved Algorithms for the Approximate k-List Problem in Euclidean norm. PKC 2017.

21. E. Kirshanova, A. May, and F. Wiemer. Parallel implementation of BDD enumeration for LWE. ACNS 2016.
22. E. Kirshanova. Proxy re-encryption from lattices. PKC 2014.

Journal Publications

1. S. Bitzer, J. Delvaux, E. Kirshanova, A. May, S. Maaßen, A. Wachter-Zeh How to lose some weight: a practical template syndrome decoding attack. March 2025. *Designs, Codes and Cryptography*
2. E. Kirshanova, E. Malygina. Construction-D lattice from Garcia-Stichtenoth tower code. December 2023. *Designs, Codes and Cryptography*
3. E. Kirshanova, E. Malygina, S. Novoselov, D. Olefirenko. An algorithm for computing the Stickelberger ideal of multiquadratic number field (in RUS). Prikladnaya Diskretnaya Matematika.
4. E. Kirshanova, H. Nguyen, D. Stehlé, A. Wallet. On the smoothing parameter and last minimum of random orthogonal lattice, January 2020, *Designs, Codes and Cryptography*
5. G. Herold, E. Kirshanova, A. May. On the Asymptotic Complexity of Solving LWE, January 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 Karenin 2022–present
- Thanh Huyen Nguyen, co-supervised with D.Stehlé(ENS Lyon).

Activities

Steering Committee Member for AsiaCrypt 2025–present

PROGRAM COMMITTEES:

ANTS-XIV
ArcticCrypt 2025

AsiaCrypt	2019, 2021, 2022, 2023, 2025
CIFRIS	2024
Crypto	2020, 2021, 2024
LatinCrypt	2023, 2025
IndoCrypt	2018
PQCrypto	2020, 2021, 2022, 2023, 2024, 2025
RWC	2024
WAIFI	2024

ORGANISER:

1st Workshop on Advances in Asymmetric Cryptanalysis (affiliated to ACNS 2024), NYU Abu Dhabi, UAE. 2024.

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 and Grants

- Joint RNF (Russia)-DFG(Germany) grant 2021-2022
  Role: Principal Investigator from the Russian part
- RNF Starting grant 2021-2022
  Role: Principal Investigator
- 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 January 2020-February 2020
The Simons Institute for the Theory of Computing, Berkeley, USA

Presentations

Slides of my talks are available at
https://elenakirshanova.github.io/

Languages

- English (fluent)
- German (intermediate)
- French (intermediate)
- Russian (native)

Programming skills

- C++, Python, Sage, Maple

References

Damien Stehlé damien.stehle@gmail.com
Professor
Department of Computer Science
ENS de Lyon

Alexander May alex.may@rub.de
Professor at the University of Bochum
Faculty of Mathematics
Chair of Cryptology and IT-Security

Shi Bai shih.bai@gmail.com
Associate professor
Department of Mathematical Sciences
Florida Atlantic University