Update: 2020/03/01

# Elena Kirshanova


**Contact Information**

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

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


**Positions**

**Postdoctoral researcher, lecturer** — September 2019-present
Immanuel Kant Baltic Federal University
Institute of Physics, Mathematics and Information Technology

**Short-term research visitor** — January 2020-February 2020
The Simons Institute for the Theory of Computing
Berkeley, USA

**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.

**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. 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
2. 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
3. E. Kirshanova. Improved Quantum Information Set Decoding, PQCrypto 2018

4. Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and the Generalized Hidden Shift Problem. PKC 2018

5. G. Herold, E. Kirshanova, T. Laarhoven. Speed-ups and timememory trade-offs for tuple lattice sieving. PKC 2018

6. G. Herold, E. Kirshanova. Improved Algorithms for the Approximate $k$-List Problem in Euclidean norm. *Public-Key Cryptography – PKC 2017: 20th IACR International Conference on Practice and Theory in Public-Key Cryptography 2017, Proceedings, Part I*, pages 16–40, Springer Berlin Heidelberg.

7. E. Kirshanova, A. May, and F. Wiemer. Parallel implementation of BDD enumeration for LWE. In *Applied Cryptography and Network Security: 14th International Conference*, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings, pages 580–591. Springer International Publishing, 2016.

8. E. Kirshanova. Proxy re-encryption from lattices. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 7794, Buenos Aires, Argentina, March, pages 26–28, 2014. Springer, Heidelberg, Germany.

## Journal Publications

1. 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*

2. G. Herold, E. Kirshanova, A. May. On the Asymptotic Complexity of Solving LWE, Jan. 2017, *Designs, Codes and Cryptography*

## Teaching Experience

Lecturer

Crypto 101 — Spring 2020
I. Kant BFU

Master – Coding Theory — Autumn 2019
I. Kant BFU

Master – Algorithms for elliptic curve cryptography — Autumn 2019
I. Kant BFU

M2 – Cryptanalysis — Autumn 2018
ENS de Lyon

Teaching Assistant

M1 – Computer Algebra — Spring 2019
ENS de Lyon

M1 – Computer Algebra — Spring 2018
ENS de Lyon

L3 – Probability — Spring 2017
ENS de Lyon

Quantum Random Walks (seminar) — Winter term 2016–17
Ruhr University Bochum

Cryptanalysis I-II 2014-15
Lecturer: Prof. Dr. A. May
Ruhr University Bochum

Quantum Algorithms Winter term 2013–14
Lecturer: Prof. Dr. A. May
Ruhr University Bochum

Internship supervisions :

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

## Activities

PROGRAM COMMITTEES: ANTS-XIV, Crypto2020, PQCrypto 2020, AsiaCrypt 2019, 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

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

## Languages

- English (fluent)
- German (professional proficiency)
- 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