Aktualisiert: 2019/08/18

Elena Kirshanova

Kontakt-information

ENS Lyon, Site Monod,
46 Alle d'Italie
69364 Lyon, Frankreich

+49 (0)234 32 23259
elena.kirshanova@ens-lyon.fr
elena.kirshanova@rub.de

Stelle

Postdoctorand Januar 2017-
ENS Lyon
Fakultät für Informatik
LIP, team ARIC

Forschungs-interessen

Gitter-basierte Kryptographie, Kryptanalyse, Quantenalgorithmen.

Ausbildung

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

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

Dr. rer. nat. Dezember 2016
Ruhr Universität Bochum
Faculty für Mathematik,
Lehrstuhl Kryptologie und IT-Sicherheit

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

Publikationen

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. G. Herold, E. Kirshanova, T. Laarhoven Time – space trade – offs for tuple lattice sieving. PKC 2018
5. Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and the Generalized Hidden Shift Problem. 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.

Veröffentlichungen in Zeitschriften

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

Lehrerfahrung

Übungen

Quantum Algorithms — WS 2013–14
Lecturer: Prof. Dr. A. May
Ruhr University Bochum

Cryptanalysis I-II — WS2014-15
Lecturer: Prof. Dr. A. May
Ruhr University Bochum

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

L3 – Probability — Frühling 2017
ENS de Lyon

L3 – Computer Algebra — Frühling 2018
ENS de Lyon

Betreuung von Bachelor- und Masterarbeiten — 2013–2016
Ruhr University Bochum

Interns:

- Thanh Huyen Nguyen (ENS Lyon, Master student, zusamen mit A.Wallet, D.Stehlé) 2018

Förderungen

- Euler Travel Grant (visit at the University of Leipzig) — Feb. 2012
- Best Student Paper Award, ACNS'16 — Juni 2016

Präsentationen

- Proxy re-encryption from lattices
  in *Workshop on Public Key Cryptography*, Buenos Aires, Argentinien — März 2014
- On the asymptotical hardness of LWE
  in *Kryptotag*, Berlin, Deutschland — Juni 2014
- On the asymptotical hardness of LWE
  in *CrossFire*, Bochum, Deutschland — Juli 2014
- Parallel implementation of BDD enumeration for LWE
  in *ACNS Conference*, Surrey, UK — Juni 2016
- Improved Algorithms for the Approximate k-List Problem in Euclidean norm
  in *Workshop on Mathematical Structures in Cryptography*, Leiden — August 2016
- Improved Algorithms for the Approximate k-List Problem in Euclidean norm
  in *HNI Symposium*, Padeborn, Deutschland — Sep 2016
- Learning With Errors and Extrapolated Dihedral Cosets
  in *Quantum Cryptanalysis seminar*, Dagstuhl, Deutschland — Okt 2017
- Learning With Errors and Extrapolated Dihedral Cosets
  in *Quantum Seminar*, IRIF, Paris, Frankreich — Nov 2017
- Introduction to Cryptography,
  in Sport-Study week, Grenoble, Frankreich — Januar 2018
- Learning With Errors and Extrapolated Dihedral Cosets
  in *CCA Seminar*, Inria, Paris, France — März 2018

- Time-memory trade-offs for lattice sieving
  in *PKC*, Rio de Janeiro, Brasilien — März 2018
- Improved Quantum ISD
  in *PQCrypto, Fort Lauderdale, Florida, USA* — April 2018

Sprachen

- English (fließend)
- German (fließend)
- French (B1)
- Russian (Muttersprache)

References

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

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

Sergey Aleshnikov — sergey.aleshnikov@gmail.com
Head of the Chair Mathematical Methods in Cryptography
Faculty of Mathematics
I.Kant Baltic Federal University