Обновлено: 19 сентября 2020 г.

Елена Киршанова

Контактная информация

ENS Lyon, Site Monod,
46 Allée d'Italie
69364 Lyon, France

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

Должность

Пост докторат Январь 2017–
ENS Лион
Факультет информатики
Лаборатория параллельных вычислений и информатики
Команда *Криптография на решетках*

Научные интересы

Криптография на решетках, криптанализ, алгоритмы для трудных задач на решетках (асимптотика и практика), квантовые алгоритмы в криптанализе.

Образование

Диплом *Математик* Январь 2013
Балтийский Федеральный университет им. И. Канта
Калининград, Россия

- Тема: *Криптография на решетках*
- Научный руководитель: к.т.н. доцент С.И. Алешников

Dr. rer. nat. Декабрь 2016
Рурский университет г. Бохум
Математический факультет,
Кафедра Криптологии и IT-безопасности

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

Публикации на конференциях

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 time–memory 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 77–94, Buenos Aires, Argentina, March, pages 26–28, 2014. Springer, Heidelberg, Germany.

Публикации в журналах

1. E. Kirshanova, H. Nguyen, D. Stehlé, A. Wallet. On the smoothing parameter and last minimum of random orthogonal lattices. 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*

Преподавательский опыт

Лектор

M2 (Магистерский курс) – Криптоанализ — Осень 2019
ENS Лион

Ассистент

M1 (Магистерский курс) – Компьютерная алгебра — Весна 2018
ENS Лион

L3 (Курс для бакалавров)– Теория вероятности — Весна 2017
ENS Лион

Квантовые блуждения (семинар) — Зимний семестр 2016-17
Рурский университет г. Бохум

Криптоанализ I-II — 2014-15
Лектор: Prof. Dr. A. May
Рурский университет г. Бохум

Квантовые алгоритмы — Зимний семестр 2013-14
Лектор: Prof. Dr. A. May
Рурский университет г. Бохум

Ассистент выпускных работ бакалавров и магистров
Рурский университет г. Бохум

Организатор

ПРОГРАММНЫЙ КОМИТЕТ: IndoCrypt 2018, AsiaCrypt 2019
ОРГАНИЗАТОР IACR Summer School “Euclidean lattices: theory and applications”, Kaliningrad, Russia. 2019

Награды

- Euler Travel Grant (посещение университета г. Лейпциг) — Февраль. 2012
- Best Student Paper Award, ACNS’16 — Июнь 2016

Выступления

- Квантовые ускорения алгоритмов просеивания
  Post-Quantum Cryptography Workshop, Оксфорд, UK — март 2019
- Introduction to Lattice-based cryptography
  Seminar in American Institute of Mathematics, San Jose, USA — февраль 2019
- Practical sieving algorithms

Crypto seminar in *XLIM, Limoges*, France январь 2019
- Sieving algorithms for the Shortest Vector Problem
- Алгоритмы просеивания для задачи короткого вектора в евклидовой решетке, *DIAMANT Symposium*, Veenendaal, Нидерланды Ноябрь 2018
- Алгоритмы с малым требованиям к памяти для задачи короткого вектора в евклидовой решетке
  at *Крипто-семинар*, Монпелье, Франция Ноябрь 2018
- Алгоритмы просеивания для задачи короткого вектора в евклидовой решетке
  at *KMS Meeting*, Сеул, Южная Корея October 2018
- Post Quantum Cryptography, Форт-Лодердейл, Флорида, США Апрель 2018
- Workshop on Public Key Cryptography, Рио де Жанейро, Бразилия Март 2018
- Семинар CCA, Inria, Париж, Франция Март, 2018
- Лекция *Введение в современную криптографию*, Франция Январь, 2018
- Семинар в IRIF, Université Paris-Diderot, Париж Ноябрь, 2017
- Квантовый криптанализ, Дагштуль, Германия Октябрь 2017
- HNI Symposium, Падеборн, Германия Сентябрь 2016
- Workshop on Mathematical Structures in Cryptography, Ляйден Август 2016
- ACNS Conference, Саррей, Великобритания Июнь 2016
- Dagstuhl, Вадерн, Центр информатики им. Лейбница Май 2015
- CrossFire, Бохум, Германия Июль 2014
- Kryptotag, Берлин, Германия Июнь 2014
- Workshop on Public Key Cryptography, Буэнос-Айрес, Аргентина Март 2014

Языки

- Английский (свободный)
- Немецкий (продвинутый)
- Французский (средний)
- Русский (родной)

References

Prof. Dr. Alexander May alex.may@rub.de
Профессор Рурского университета г. Бохум
Математический факультет
Кафедра Криптологии и IT-безопасности

Prof. Dr. Damien Stehlé damien.stehle@gmail.com
Профессор
Факультет информатики
Лаборатория параллельных вычислений и информатики
ENS Лион

к.т.н. доцент Сергей Иванович Алешников sergey.aleshnikov@gmail.com
Зав. кафедрой компьютерной безопасности
Математический факультет
Балтийский Федеральный университет им. И. Канта