Обновлено: 21 августа 2021 г.

Елена Киршанова

Контактная информация

БФУ им. И. Канта,
ул. Невского, 14
236016 Калининград, Россия

+7-911-855-89-80
elenakirshanova@gmail.com
elena.kirshanova@rub.de

Должность

Доцент,
научный сотрудник (75 %) Сентябрь 2019-
БФУ им. И. Канта
Институт физики, математики и информационных технологий
Лаборатория "Мат. методы защиты информации"

Научный сотрудник (25 %) Май 2021-
Рурский университет г. Бохум
Математический факультет,
Кафедра Криптологии и IT-безопасности

Пост докторат Январь 2017–Июнь 2019
ENS Лион
Факультет информатики
Лаборатория параллельных вычислений и информатики
Команда *Криптография на решетках*

Ассистент Май 2013-Декабрь 2016
Рурский университет г. Бохум
Математический факультет,
Кафедра Криптологии и IT-безопасности

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. Elena Kirshanova, Thjis Laarhoven. Lower bounds for nearest neighbor searching and post-quantum cryptanalysis. Crpyto 2021
2. Iggy van Hoof, Elena Kirshanova, Alexander May. Quantum Key Search for Ternary LWE. PQCrypto 2021
3. Киршанова Е. А. , Малыгина Е. С., Новоселов С. А., Олефиренко Д.О.. Алгоритм вычисления элемента Штикельбергера для мнимых мультиквадратичных полей // ПДМ. Приложение. 2020. № 13.

4. Киршанова, Е. А., Колесников, Н. С., Малыгина, Е. С., Новоселов, С. А. Проект стандартизации постквантовой цифровой подписи // Прикладная дискретная математика. Приложение. 2020. № 13.
5. 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
6. 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
7. E. Kirshanova. Improved Quantum Information Set Decoding, PQCrypto 2018
8. Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and the Generalized Hidden Shift Problem. PKC 2018
9. G. Herold, E.Kirshanova, T.Laarhoven. Speed-ups and time–memory trade-offs for tuple lattice sieving. PKC 2018.
10. G. Herold, E. Kirshanova. Improved Algorithms for the Approximate k-List Problem in Euclidean norm. PKC 2017
11. E. Kirshanova, A. May, and F. Wiemer. Parallel implementation of BDD enumeration for LWE. ACNS 2016.
12. E. Kirshanova. Proxy re-encryption from lattices. PKC 2014.

Публикации в журналах

1. Киршанова Е. А. , Малыгина Е. С. , Новоселов С. А. , Олефиренко Д. О. Алгоритм вычисления идеала Штикельбергера для мультиквадратичных полей. ПДМ. 2021. № 51.
2. 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*
3. G. Herold, E. Kirshanova, A. May. On the Asymptotic Complexity of Solving LWE, Jan. 2017, *Designs, Codes and Cryptography*

Преподавательский опыт

Лектор

Криптография на решётках (БФУ им. И. Канта)	Весна'21
Crypto 101 (БФУ им. И. Канта)	Весна'20, '21
Летняя практика Git + LaTeX + Sage (БФУ им. И. Канта)	Лето'20, '21
Теория кодирования (БФУ им. И. Канта)	'19, '20, 21
Криптография на эллиптических кривых (БФУ им. И. Канта)	Осень'19
Криптоанализ (M2, ENS Лион)	Осень'19

Ассистент

M1 (Магистерский курс) – Компьютерная алгебра ENS Лион	Весна 2018
L3 (Курс для бакалавров)– Теория вероятности ENS Лион	Весна 2017

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:
Crypto 2020, 2021; PQCrypto 2020, 2021; ANTS-XIV, Crypto2020; AsiaCrypt 2019, 2021; IndoCrypt 2018

ОРГАНИЗАТОР IACR Summer School "Euclidean lattices: theory and applications", Kaliningrad, Russia. 2019

Награды

- Лауреат конкурса "Молодая математика России", 2020
- Стипендия Мечникова на научный визит во Францию, 2020
- Euler Travel Grant (посещение университета г. Лейпциг) Февраль. 2012
- Best Student Paper Award, ACNS'16 Июнь 2016

Выступления

Слайды моих выступлений доступны по адресу
https://crypto-kantiana.com/elena.kirshanova/#talks

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