actualisé : 13 septembre 2019

Elena Kirshanova

Coordonnées

I. Kant BFU
Nevskogo Rue. 14
236016 Kaliningrad, Russie

+33 (0)7 87 236537
elena.kirshanova@ens-lyon.fr
elena.kirshanova@rub.de
http://perso.ens-lyon.fr/elena.kirshanova/

Sujets de recherche

Cryptographie fondée sur les réseaux, cryptanalyse, algorithmes dans les réseaux euclidiens, algorithmes quantiques.

Formation

Dr. rer. nat (Doctor rerum naturalium) décembre 2016
Département de Mathématiques, Ruhr Université Bochum, Allemagne

- Sujet de thèse : *Complexity of the Learning with Errors Problem and Memory-Efficient Lattice Sieving*
- Directeur de thèse : Prof. Dr. Alexander May

Diplôme de mathéematiques [1] janvier 2013
Département de Mathématiques, Université fédérale Immnuel Kant, Russie

- Sujet de thèse : *Lattice-based cryptography*
- Directeur de thèse : Dr. Sergey Aleshnikov

Situation actuelle

Post-doctorante septembre 2019 –
Département de Physique. Mathématiques et Informatique
Immanuel Kant Baltic Federal University

Expérience de recherche

Post-doctorante janvier 2017 – juin 2019
Équipe AriC
Département d'Informatique
École Normale Supérieure de Lyon

- Mes activités de recherche portent sur la cryptonalyse des cryptosystèmes basés sur les réseaux euclidiens. Je travaille principalement sur le probléme du *vecteur le plus court*, le probléme algorithmique central portant sur les réseaux euclidiens. Je travaille également sur les algorithmes quantiques pour les problémes permettant de résoudre ces problémes, dont la complexité algorithmique est le fondement des hypothéses de sécurite, sur lesquelles reposent les cryptosystémes post-quantiques.

Articles de conférences internationales, avec comité de relecture

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. 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

1. Équivalent au dimplôme de master français, délivré par les universités

6. G. Herold, E. Kirshanova. Improved Algorithms for the Approximate k-List Problem in Euclidean norm. PKC 2017
7. E. Kirshanova, A. May, and F. Wiemer. Parallel implementation of BDD enumeration for LWE. ACNS 2016
8. E. Kirshanova. Proxy re-encryption from lattices. In Hugo Krawczyk, editor, PKC 2014

Articles de journaux

1. G. Herold, E. Kirshanova, A. May. On the Asymptotic Complexity of Solving LWE, 2017, pages 1–29 *Designs, Codes and Cryptography*

Articles soumis ou en préparation

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

Expérience professionnelle

- Professeure
  - Master – Coding Theory — 2019
    I. Kant BFU
  - Master – Algorithms for elliptic curve cryptography — 2019
    I. Kant BFU
  - M2 – Cryptanalysis — 2018
    ENS de Lyon
- Assistante d'enseignement (TD)
  - M1 – Algorithmes Efficaces en Calcul Formel — 2019
    ENS de Lyon
  - M1 – Algorithmes Efficaces en Calcul Formel — 2018
    ENS de Lyon
  - L3 – Probabilités — 2017
    ENS de Lyon
  - Quantum Random Walks (séminaire) — 2016-17
    Ruhr University Bochum
  - Cryptanalysis I-II — 2014-15
    Professeur : Prof. Dr. A. May
    Ruhr University Bochum
  - Algorithmes Quantiques — 2013-14
    Professeur : Prof. Dr. A. May
    Ruhr University Bochum

Interns :

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

Activités

COMITÉS SCIENTIFIQUES : IndoCrypt 2018, AsiaCrypt 2019, ANTS XIV, PQCrypto 2020
ORGANISATRICE : IACR Summer School "Euclidean lattices : theory and applications", Kaliningrad, Russia. 2019

Prix et bourses

- Best Student Paper Award, ACNS'16 — juin 2016
- Euler Travel Grant (un stage de 1 mois dans l'Université Leipzig) — février 2012

Communications internationales et séminaires

- Introduction to cryptanalysis of lattice-based schemes
  SibeCrypt, Tomsk, Russie — septembre 2019
- Quantum speed-ups for sieving algorithms
  Post-Quantum Cryptography Workshop, Oxford, UK — mars 2019
- Introduction to Lattice-based cryptography
  à *Seminar in American Institute of Mathematics*, San Jose, USA — février 2019
- Practical sieving algorithms
  Crypto seminar in *XLIM, Limoges*, France — janvier 2019
- Sieving algorithms for the Shortest Vector Problem
  à *DIAMANT Symposium*, Veenendaal, the Netherlands — novembre 2018
- Low memory sieving algorithms for the Shortest Vector Problem
  à*Cypto Seminar*, Montpelier, France — novembre 2018
- Sieving algorithms for the Shortest Vector Problem
  à *Journées C2*, Aussois, France — octobre 2018
- Sieving algorithms for the Shortest Vector Problem
  à *KMS Meeting*, Seoul, South Korea — octobre 2018
- Improved Quantum ISD
  à *PQCrypto, Fort Lauderdale, Floride, Etats-Unis* — avril 2018
- Time-memory trade-offs for lattice sieving
  à *PKC*, Rio de Janeiro, Brésil — mars 2018
- Learning With Errors and Extrapolated Dihedral Cosets
  à *CCA Seminar*, Inria, Paris, France — mars 2018
- Introduction to Cryptography
  à *Sport-Study week*, Grenoble, France — janvier 2018
- Learning With Errors and Extrapolated Dihedral Cosets
  à *Séminaire de l'IRIF*, Université Paris-Diderot, Paris — novembre 2017
- Learning With Errors and Extrapolated Dihedral Cosets
  à *Séminaire 'Quantum Cryptanalysis'*, Dagstuhl, Allemagne — octobre 2017
- Improved Algorithms for the Approximate k-List Problem in Euclidean norm
  à *HNI Symposium*, Padeborn, Allemagne — septembre 2016
- Improved Algorithms for the Approximate k-List Problem in Euclidean norm
  à *Workshop on Mathematical Structures in Cryptography*, Leiden — août 2016
- Parallel implementation of BDD enumeration for LWE
  à *ACNS Conference*, Surrey, Royaume-Uni — juin 2016
- On the asymptotical hardness of LWE
  à *CrossFire*, Bochum, Allemagne — juillet 2014
- On the asymptotical hardness of LWE
  à *Kryptotag*, Berlin, Allemagne — juin 2014
- Proxy re-encryption from lattices
  à *Workshop on Public Key Cryptography*, Buenos Aires, Argentina — mars 2014

Langues

- Anglais (courant)
- Allemand (courant)
- Français (intermédiaire)
- Russe (langue maternelle)

Références

Damien Stehlé — damien.stehle@ens-lyon.fr
Professor
Department of Computer Science

ENS de Lyon

Alexander May alex.may@rub.de
Professeur, Laboratoire de Cryptographie et Sécurité
Département de Mathématiques
Ruhr University, Bochum

Articles pertinents pour le projet "Algebraic lattices in cryptograph"

1. Albrecht M.R., Ducas L., Herold G., Kirshanova E., Postlethwaite E.W., Stevens M. (2019) The General Sieve Kernel and New Records in Lattice Reduction. In : Ishai Y., Rijmen V. (eds) Advances in Cryptology âĂŞ EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11477. Springer
2. Herold G., Kirshanova E., Laarhoven T. (2018) Speed-Ups and TimeâĂŞMemory Trade-Offs for Tuple Lattice Sieving. In : Abdalla M., Dahab R. (eds) Public-Key Cryptography âĂŞ PKC 2018. PKC 2018. Lecture Notes in Computer Science, vol 10769. Springer
3. Herold G., Kirshanova E. (2017) Improved Algorithms for the Approximate k-List Problem in Euclidean Norm. In : Fehr S. (eds) Public-Key Cryptography âĂŞ PKC 2017. PKC 2017. Lecture Notes in Computer Science, vol 10174. Springer