

Jingwei CHEN

Curriculum Vitae

CIGIT, CAS
Chongqing 400714, China
☎ +86-23-65 93 56 58
✉ chenjingwei@cigit.ac.cn
🌐 arcnl.org/jchen/



Research Interests

- Computer Algebra, especially in polynomial factorization
- Symbolic-numeric Computation, especially in integer relation finding
- Computational Number Theory, especially in algorithms for geometry of numbers
- Lattice-based Cryptography, especially in FHE and its application

Positions

- 17.12– Chongqing Key Lab of Automated Reasoning and Cognition, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences. Associate Professor
- 15.10–15.11 Fields Institute, University of Toronto. Academic Visitor
- 13.07–17.12 Chongqing Key Lab of Automated Reasoning and Cognition, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences. Assistant Professor

Education

- 12.01–12.12 Laboratoire de l'Informatique du Parallélisme, CNRS-ENSL-UCBL, Lyon, France.
Visiting Ph.D. student
Supervisors: Damien STEHLÉ and Gilles VILLARD
- 07.09–13.07 Chengdu Institute of Computer Applications, Chinese Academy of Sciences
Degree: Ph.D. in Computer Science
Dissertation: Study on Theories and Algorithms for Several Problems in Symbolic-Numeric Hybrid Computation
Advisor: Yong FENG
- 03.09–07.06 College of Mathematics and Statistics, Southwest University, Chongqing, China
Degree: Bachelor of Science in Mathematics and Applied Mathematics
Advisor: Jia WANG

Awards and Honors

- 11.10 CAS-CNRS (France): China-France Joint Doctoral Promotion Program
- 08.07 Graduate University, CAS: Excellent Graduate Student
- 07.06 Southwest University: Excellent Graduates
- 07.03 COMAP (USA): Honorable Mention of The Mathematical Contest in Modeling
- 05.11/06.11 CSIAM: Second Prizes of China Undergraduate Mathematical Contest in Modeling
- 05.12 Ministry of Education: National Scholarship

Grants

- 18.01-21.12 Youth Innovation Promotion Association CAS: *Lattice reduction algorithms and its application*, RMB 800,000.
- 16.01-18.12 National Natural Science Foundation of China (Grant No.: 11501540): *Error-controllable algorithms for integer relation finding and applications*, RMB 180,000.
- 15.01-17.12 “Light of the West” project of Chinese Academy of Sciences: *Lattice reduction and application in homomorphic encryption*, RMB 100,000.
- 12.01-12.12 “Miaozi” Project of Sichuan Province: *Implementation of efficient symbolic-numeric algorithms for polynomial factorization*, RMB 15,000.

Publications

- [1] Jingwei Chen, Yong Feng, and Wenyuan Wu. Reducing lattice bases with Bergman exchange. In Yang Xiao and Maode Ma, editors, *Proceedings of the 9th IEEE International Conference on Communication Software and Network (May 6–8, 2017, Guangzhou, China)*, volume II, pages 630–634. IEEE, Piscataway, 2017.
- [2] Jingwei Chen, Yong Feng, Yang Liu, and Wenyuan Wu. Faster binary arithmetic operations on encrypted integers. In Yifei Chen, editor, *Proceedings of the 7th International Workshop on Computer Science and Engineering (June 25–27, 2017, Beijing, China)*, volume III, pages 956–960. The Science and Engineering Institute, Rowland Heights, LA, 2017.
- [3] Chen Xu, Jingwei Chen, Wenyuan Wu, and Yong Feng. Homomorphically encrypted arithmetic operations over the integer ring. In Feng Bao, Liqun Chen, Robert H. Deng, and Guojun Wang, editors, *Proceedings of the 12th International Conference on Information Security Practice and Experience (November 16–18, 2016, Zhangjiajie, China)*, volume 10060, pages 167–181. Springer, Cham, 2016.
- [4] Jingwei Chen, Yong Feng, Yang Liu, Bing Tang, and Wenyuan Wu. Sparse non-negative matrix factorization with generalized Kullback-Leibler divergence. In Hujun Yin, Yang Gao, Bin Li, Daoqiang Zhang, Ming Yang, Yun Li, Frank Klawonn, and Antonio Tallón, editors, *Proceedings of the 17th International Conference on Intelligent Data Engineering and Automated Learning (October 12–14, 2016, Yangzhou, China)*, volume 9937, pages 353–360. Springer, Cham, 2016.
- [5] Yong Feng, Wenyuan Wu, Jingzhong Zhang, and Jingwei Chen. Exact bivariate polynomial factorization over \mathbb{Q} by approximation of roots. *Journal of Systems Science and Complexity*, 28(1):243 – 260, 2015.
- [6] Wenyuan Wu, Jingwei Chen, and Yong Feng. Sparse bivariate polynomial factorization. *Science China Mathematics*, 57(10):2123–2142, 2014.
- [7] Yong Feng, Jingwei Chen, and Wenyuan Wu. Two variants of HJLS-PSLQ with applications. In *Proceedings of the 2014 Symposium on Symbolic-Numeric Computation*, pages 88–96, Shanghai, China, 2014. ACM.
- [8] Xiaolin Qin, Yong Feng, Jingwei Chen, and Jingzhong Zhang. Parallel computation of real solving bivariate polynomial systems by zero-matching method. *Applied Mathematics and Computation*, 219(14):7533–7541, 2013.

- [9] Yong Feng, Jingwei Chen, and Wenyuan Wu. Incremental PSLQ with application to algebraic number reconstruction. *ACM Communications in Computer Algebra*, 47(3):112–113, 2013.
- [10] Jingwei Chen, Damien Stehlé, and Gilles Villard. A new view on HJLS and PSLQ: Sums and projections of lattices. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 149–156, Boston, USA, 2013. ACM.
- [11] Wenyuan Wu, Jingwei Chen, and Yong Feng. An efficient algorithm to factorize sparse bivariate polynomials over the rationals. *ACM Communications in Computer Algebra*, 46(3):125–126, 2012.
- [12] Xiaolin Qin, Yong Feng, Jingwei Chen, and Jingzhong Zhang. A complete algorithm to find exact minimal polynomial by approximations. *International Journal of Computer Mathematics*, 89(17):2333–2344, 2012.
- [13] Jingwei Chen, Yong Feng, Xiaolin Qin, and Jingzhong Zhang. SIRD: An algorithm for simultaneous integer relations detection (in Chinese). *Journal of Sichuan University (Engineering Science Edition)*, 43(6):127–132, 2011.
- [14] Jingwei Chen, Yong Feng, Xiaolin Qin, and Jingzhong Zhang. Reconstructing minimal polynomial from approximate algebraic numbers (in Chinese). *Journal of System Science and Mathematical Sciences*, 31(8):903–912, 2011.
- [15] Xiaolin Qin, Yong Feng, Jingwei Chen, and Jun Li. Exact representation of real algebraic number by approximations and its applications (in Chinese). *Journal of Sichuan University (Engineering Science Edition)*, 42(2):126–131, 2010.
- [16] Xiaolin Qin, Yong Feng, Jingwei Chen, and Jingzhong Zhang. Finding exact minimal polynomial by approximations. In *Proceedings of the 2009 Conference on Symbolic Numeric Computation*, pages 125–132, Kyoto, Japan, 2009. ACM.
- [17] Jingwei Chen, Yong Feng, Xiaolin Qin, and Jingzhong Zhang. Exact polynomial factorization by approximate high degree algebraic numbers. In *Proceedings of the 2009 Conference on Symbolic Numeric Computation*, pages 21–28, Kyoto, Japan, 2009. ACM.
- [18] Jingwei Chen. The distribution of eigenvalues of a matrix (in Chinese). *Journal of Southwest University (Natural Science Edition)*, 29(11):45–47, 2007.

Talks

- 18.03 Finding integer relation via lattice reduction. Seminar on Error-free Computation, Chongqing
- 17.10 An integer relation finding algorithm based on Lovász exchange. CM'17, Xiangtan
- 17.05 Reducing lattice bases with Bergman exchange. ICCSN'17, Guangzhou
- 16.10 Sparse non-negative matrix factorization with generalized Kullback-Leibler divergence. IDEAL'16, Yangzhou
- 15.08 On integer relation finding problem: reducing knapsack lattice bases. 3rd HMSNC – 8th ICIAM, Beijing
- 14.07 Two variants of HJLS-PSLQ with applications. SNC'14, Shanghai
- 13.06 A new view on HJLS and PSLQ: Sums and projections of lattices. ISSAC'13, Boston

- 12.12 A new view on PSLQ: Computing with projections of lattices. AriC work session, Lyon
- 10.10 Reconstructing minimal polynomial from approximate algebraic numbers. CM'10, Shanghai

Posters

- 13.06 Incremental PSLQ with application to algebraic number reconstruction. ISSAC'13, Boston
- 12.07 An efficient algorithm to factorize sparse bivariate polynomials over the rationals. ISSAC'12, Grenoble

Committees

- Program Committees, ICCSN'17
- Local Arrangements Committees, CM'14

Referee

- International Journal of Foundations of Computer Science

Conferences Participated in

- 17.10 ChinaCrypt'17, Ji'nan
- 17.10 9th Conference on Computer Mathematics, Xiangtan
- 17.06 7th International Workshop on Computer Science and Engineering, Beijing
- 17.05 Workshop on Cryptographic Algorithms, Guilin
- 17.05 9th International Conference on Communication Software and Networks, Guangzhou
- 16.12 Tsinghua-Cornell Workshop on Security and Cryptography, Beijing
- 16.11 Symposium on Mathematical Mechanization and Education Information Technology, Chengdu
- 16.11 12th International Conference on Information Security Practice and Experience, Zhangjiajie
- 16.10 17th International Conference on Intelligent Data Engineering and Automated Learning, Yangzhou
- 15.08 8th International Congress on Industrial and Applied Mathematics, Beijing
- 14.11 6th Conference on Computer Mathematics, Chongqing
- 14.07 International Workshop on Symbolic-Numeric Computation, Shanghai
- 13.06 38th International Symposium on Symbolic and Algebraic Computation, Boston
- 12.10 ECRYPT II Summer School on Lattices, Porto
- 12.07 37th International Symposium on Symbolic and Algebraic Computation, Grenoble
- 10.10 3rd Conference on Computer Mathematics, Shanghai

References

- Y. FENG Professor in Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences
Address: 266, Fangzheng Avenue, Chongqing 400714, China

Phone: +86-23-65 93 55 17
Email: yongfeng@cigit.ac.cn

D. STEHLÉ Professor in École Normale Supérieure de Lyon
Address: 46 Allée d'Italie F69364 Lyon Cedex 07, France
Phone: +33 4 26 23 39 32
Email: damien.stehle@ens-lyon.fr

G. VILLARD Directeur de recherche in CNRS
Address: 46 Allée d'Italie F69364 Lyon Cedex 07, France
Phone: +33 6 61 14 99 02
Email: gilles.villard@ens-lyon.fr

W. WU Professor in Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences
Address: 266, Fangzheng Avenue, Chongqing 400714, China
Phone: +86-23-65 93 55 16
Email: wuwenyuan@cigit.ac.cn