

Chang Lv

Associate Professor

State Key Laboratory of Information Security (SKLOIS),
Institute of Information Engineering (IIE),
Chinese Academy of Sciences (CAS),
Beijing 100093, P.R.China
✉ lvchang@amss.ac.cn, lvchang@iie.ac.cn



Education

- 2018–Now **Associate Professor**, *Institute of Information Engineering, CAS*, Beijing, China,
• New methods for integer factorization (with Minqiang Huang and Shizhu Liu).
- 2015–2018 **Assistant Professor**, *Institute of Information Engineering, CAS*, Beijing, China,
• Crypto functions (with Minqiang Huang and Shizhu Liu).
- 2010–2015 **Ph.D.**, *Academy of Mathematics and Systems Science, CAS*, Beijing, China,
• Degree major: Applied Mathematics, Adviser: Prof. Zhexion Wan and Yingpu Deng.
• Thesis: Primality tests, ring class fields and diophantine equations, 2015
- 2006–2010 **B.S.**, *Nankai University*, Tianjin, China,
• Degree major: Mathematics and Applied Mathematics.

Area of research

I am interested in **computational number theory**, **computational arithmetic geometry** and **cryptography**.

Fundings

- 01/2018-12/2020 Existence of integral points on quadratic norm form equations over global fields and applications, NNSF of China (Grants No. 11701552)

Publications

- [DL15] Yingpu Deng and Chang Lv, *Primality test for numbers of the form $Ap^n + w_n$* , *Journal of Discrete Algorithms* **33** (2015), 81–92.
- [LD15] Chang Lv and Yingpu Deng, *On orders in number fields: Picard groups, ring class fields and applications*, *Science China Mathematics* **58** (2015), no. 8, 1627–1638.
- [LL17] Chang Lv and Jianing Li, *On the non-existence of certain classes of generalized bent functions*, *IEEE Transactions on Information Theory* **63** (2017), no. 1, 738–746.
- [LSD18] Chang Lv, Junchao Shentu, and Yingpu Deng, *On the integral representation of binary quadratic forms and the Artin condition*, *Tokyo Journal of Mathematics* **41** (2018), no. 2, 371–384. MR 3908800

- [Lv17] Chang Lv, *On the non-existence of certain classes of perfect p -ary sequences and perfect almost p -ary sequences*, IEEE Transactions on Information Theory **63** (2017), no. 8, 5350–5359.
- [Lv18] ———, *Nonexistence of generalized bent functions and the quadratic norm form equations*, arXiv preprint arXiv:1804.01292 (2018), 1–13.
- [Lv20a] ———, *Diophantine equations defined by binary quadratic forms over rational function fields*, Acta Arithmetica **196** (2020), no. 1, 35–51. MR 4129970
- [Lv20b] ———, *A note on the Brauer group and the Brauer-Manin set of a product*, Bulletin of the London Mathematical Society **52** (2020), no. 5, 932–941. MR 4171413
- [Lv21] ———, *The second descent obstruction and gerbes*, arXiv preprint arXiv:2009.06915v2 (2021), 1–31.
- [Lv22] ———, *On commutative diagrams consisting of low term exact sequences*, arXiv preprint arXiv:2112.14386v2 (2022), 1–9.
- [LW23] Chang Lv and Han Wu, *The Brauer-Manin obstruction on algebraic stacks*, arXiv preprint arXiv:2306.14426v2 (2023), 1–16.
- [WL23] Han Wu and Chang Lv, *Genus one half stacky curves violating the local-global principle*, to appear on Journal de Théorie des Nombres de Bordeaux (2023), 1–5.
- [YL18] Hairong Yi and Chang Lv, *On ring class fields of number rings*, arXiv preprint arXiv:1810.04810 (2018), 1–17.

Last update: November 15, 2023