Bibliography in relation with the PEPR Cryptanalyse engineer position in Bordeaux

Aurel Page

The software Pari/GP implements a version of Buchmann's algorithm for computing class groups and units of number fields (`bnfinit`). We would like to improve the linear algebra step of this computation, by implementing documented algorithms and evaluating their usefulness in this context.

References directly related with the position:

- Filtering algorithms [Cav00, Cav02, Bou13, Tea17];
- Linear algebra over $\mathbb{Z}$ [SL96, GJS01];
- Sparse linear algebra [Lam19, BD16].

Other references provided for context:

- Computation of class groups: [Buc90, BF14, BFHP22];
- Class group based cryptography: [Cas19].

URL for applications

References

[BD16] Charles Bouillaguet and Claire Delaplace. Sparse Gaussian elimination modulo p: an update. In *Computer algebra in scientific computing. 18th international workshop, CASC 2016, Bucharest, Romania, September 19–23, 2016. Proceedings*, pages 101–116. Cham: Springer, 2016.

[BF14] Jean-François Biasse and Claus Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS J. Comput. Math.*, 17A:385–403, 2014.

[BFHP22] Jean-François Biasse, Claus Fieker, Tommy Hofmann, and Aurel Page. Norm relations and computational problems in number fields. *J. Lond. Math. Soc., II. Ser.*, 105(4):2373–2414, 2022.

[Bou13] Cyril Bouvier. The filtering step of discrete logarithm and integer factorization algorithms. Preprint, June 2013.

[Buc90] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. Sémin. Théor. Nombres, Paris/Fr. 1988-89, Prog. Math. 91, 27-41 (1990)., 1990.

[Cas19] Guilhem Castagnos. *Cryptography based on quadratic fields: cryptanalyses, primitives and protocols.* Habilitation à diriger des recherches, Université de Bordeaux, November 2019.

[Cav00] Stefania Cavallar. Strategies in filtering in the number field sieve. In *Algorithmic number theory. 4th international symposium. ANTS-IV, Leiden, the Netherlands, July 2–7, 2000. Proceedings*, pages 209–231. Berlin: Springer, 2000.

[Cav02] Stefania Hedwig Cavallar. *On the number field sieve integer factorisation algorithm. Thesis.* Leiden: Univ. Leiden, 2002.

[GJS01] Mark Giesbrecht, Michael jun. Jacobson, and Arne Storjohann. Algorithms for large integer matrix problems. In *Applied algebra, algebraic algorithms and error-correcting codes. 14th international symposium, AAECC-14, Melbourne, Australia, November 26–30, 2001. Proceedings*, pages 297–307. Berlin: Springer, 2001.

[Lam19] Leon Lampret. Chain complex reduction via fast digraph traversal. Preprint, arXiv:1903.00783 [math.AT] (2019), 2019.

[SL96] Arne Storjohann and George Labahn. Asymptotically fast computation of Hermite normal forms of integer matrices. In *Proceedings of the 1996 international symposium on symbolic and algebraic computation, ISSAC '96, Zürich, Switzerland, July 24–26, 1996*, pages 259–266. New York, NY: ACM Press, 1996.

[Tea17] The CADO-NFS Development Team. CADO-NFS, an implementation of the number field sieve algorithm, 2017. Release 2.3.0.