Retrieving short generators of principal ideals in real Kummer extensions

Introduction: The simplest versions of encryption using ideal lattices such as in [4, 7] is as follow. Consider a number field K and $I = g\mathcal{O}_K$ a principal ideal with a short g when I is considered as a lattice i.e. the euclidean norm of g is small compared to the determinant of I. Then K and I are public and g is private. The private key security relies on the hardness of finding g or another short generator. Finding a generator is called the *Principal Ideal Problem* (PIP). Finding a short generator is referred as the *Short Principal Ideal Problem* (SPIP). By default an attack to recover the generator g is done in two steps

1. recover a generator h of I;
2. find a short generator given h.

The first step corresponds to the PIP which is considered a hard problem in classical computational number theory. However it is shown that it can be efficiently done by using quantum computing as in [2]. The second is a reduction phase which is the kind of tasks that seem difficult even for quantum computers. In order to solve it, one may use the structure of the set of generators of I and the Log-unit lattice. Indeed $\mathrm{Log}(h) = \mathrm{Log}(g) + \mathrm{Log}(u) \in \mathrm{Log}(g) + \mathrm{Log}(\mathcal{O}_K^\times)$ so recovering g can be seen as solving a BDD problem with respect to $\mathrm{Log}(\mathcal{O}_K^\times)$. An analysis over cyclotomic fields has been done in [3] where the authors gave a bound for the norm of the vectors of the dual basis. In [1] the authors studied another family of fields, namely the multiquadratic fields, and were able to recover a short generator of an ideal in classical polynomial time for a wide range of fields.

Our work: We first generalised the approach of [1] to multicubic fields in [5] then to real Kummer extensions of $\mathbb{Q}$ with a prime exponent i.e of the form $\mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r})$ where $m_i \in \mathbb{Q}$. The lattice of subfields and the set of complex field morphisms of these fields have a structure similar to the ones of multiquadratic fields. Thus the algorithms to compute the unit group and a generator of a principal ideal can be adapted. Moreover, in order to break the structure a little, we also considered the combination of two Kummer extensions with distinct exponents i.e. of the form $\mathbb{Q}(\sqrt[p]{m_1}, \ldots, \sqrt[p]{m_r}, \sqrt[q]{n_1}, \ldots, \sqrt[q]{n_s})$. Again the structure of such fields allows to design algorithms more efficient than the standard ones. From the experimental data that we computed, general Kummer extension of $\mathbb{Q}$ with only one exponent seem to show the same properties than multiquadratic and multicubic fields i.e. high probabilities to retrieve the private key. This probability seems to be smaller over Kummer extensions with two exponents. However the fact that relatively fast classical computations (when compared to standard algorithms) can be done over the number fields in this work seems to indicate that one should be careful with very structured fields.

Future work: In order to obtain practical results, improvements on classical number theoretical computations are needed. Further work can also consist on studying other tasks of computational number theory over these fields such as computing the class group and S-units. It could be possible to implement and have practical examples of the attack to solve the *Ideal Shortest Vector Problem* (ISVP) presented in [6]. Another direction would be to study number fields with more complicated structures in order to look whether we can again find a good basis for the Log-unit lattice or not.

References

[1] Jens Bauch, Daniel J. Bernstein, Henry de Valence, Tanja Lange, and Christine van Vredendaal. Short generators without quantum computers: The case of multiquadratics. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 27–59, Cham, 2017. Springer International Publishing.

[2] J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902, 2016.

[3] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 559–585, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[4] Craig Gentry. *A Fully Homomorphic Encryption Scheme.* PhD thesis, Stanford, CA, USA, 2009. AAI3382729.

[5] Andrea Lesavourey, Thomas Plantard, and Willy Susilo. On ideal lattices in multicubic fields. `http://nutmic2019.imj-prg.fr/confpapers/MultiCubic.pdf`, 2019.

[6] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. Approx-svp in ideal lattices with preprocessing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 685–716, Cham, 2019. Springer International Publishing.

[7] N. P. Smart and F. Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC 2010*, pages 420–443, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.