Retrieving short generators of principal ideals in real Kummer extensions

Andrea Lesavourey*[1], Thomas Plantard[2], and Willy Susilo[1]

[1]University of Wollongong – Australie
[2]CCISR, University of Wollongong, NSW, Australia (CCISR, UOW) – Northfields Ave Wollongong NSW 2522 Australia, Australie

Résumé

The simplest versions of encryption using ideal lattices is as follow.
Consider a number field K and I = (g) a principal ideal with a short g 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. 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. 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 Q with a prime exponent i.e generated by pth roots of integers. Moreover, in order to break the structure a little, we also considered the combination of two Kummer extensions with distinct exponents. 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 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.

*Intervenant