Algebraic Algorithms for LWE Problems

Martin R. Albrecht[1], Carlos Cid[1], Jean-Charles Faugère[2], Robert Fitzpatrick[1], and Ludovic Perret[2]

[1] Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom
[2] INRIA, Paris-Rocquencourt Center, POLSYS Project
UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France
CNRS, UMR 7606, LIP6, F-75005, Paris, France
martin.albrecht@rhul.ac.uk, carlos.cid@rhul.ac.uk, jean-charles.faugere@inria.fr,
robert.fitzpatrick.2010@live.rhul.ac.uk, ludovic.perret@lip6.fr

Abstract. We analyse the complexity of algebraic algorithms for solving systems of linear equations with *noise*. Such systems arise naturally in the theory of error-correcting codes as well as in computational learning theory. More recently, linear systems with noise have found application in cryptography. The *Learning with Errors* (LWE) problem has proven to be a rich and versatile source of innovative cryptosystems, such as fully homomorphic encryption schemes. Despite the popularity of the LWE problem, the complexity of algorithms for solving is not very well understood, particularly when variants of the original problem are considered. Here, we focus on and generalise a particular method for solving these systems, due to Arora & Ge, which reduces the problem to non-linear but noise-free system solving. Firstly, we provide a refined complexity analysis for the original Arora-Ge algorithm for LWE. Secondly, we study the complexity of applying algorithms for computing Gröbner basis, the fundamental tool in computational commutative algebra, to solving Arora-Ge-style systems of non-linear equations. We show positive and negative results. On the one hand, we show that the use of Gröbner bases yields an exponential speed-up over the basic Arora-Ge approach. On the other hand, we give a negative answer to the natural question whether the use of such techniques can yield a subexponential algorithm for the LWE problem. Under mild assumptions – which we experimentally verified – we show that it is highly unlikely that such an improvement exists.

We also consider a variant of LWE known as BinaryError-LWE introduced by Micciancio and Peikert recently. By combining Gröbner basis algorithms with the Arora-Ge modelling, we show – under a mild, experimentally verified assumption – that BinaryError-LWE can be solved in subexponential time as soon as the number of samples is quasi-linear, e.g. $m = \mathcal{O}\left(n \log\log n\right)$. We also derive precise complexity bounds for BinaryError-LWE with $m = \mathcal{O}\left(n\right)$, showing that this new approach yields better results than best currently-known generic (exact) CVP solver as soon as $m/n \geq 6.6$. More generally, our results provide a good picture of the hardness degradation of BinaryError-LWE for a number of samples ranging from $m = n\left(1 + \Omega\big(1/\log(n)\big)\right)$ (a case for which BinaryError-LWE is as hard as solving some lattice problem in the worst case) to $m = \mathcal{O}\left(n^2\right)$ (a case for which it can be solved in polynomial-time). This addresses an open question from Micciancio and Peikert. Whilst our results do not contradict the hardness results obtained by Micciancio and Peikert, they should rule out BinaryError-LWE for many cryptographic applications.