Polynomials with Error (PWE)

Martin R. Albrecht[1], Jean-Charles Faugère[1], Dongdai Lin[2] and Ludovic Perret1

[1] INRIA, Paris-Rocquencourt Center, SALSA Project
UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France.
CNRS, UMR 7606, LIP6, F-75005, Paris, France

[2] SKLOIS, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China.

malb@lip6.fr, jean-charles.faugere@inria.fr,d_d_lin@yahoo.com.cn,ludovic.perret@lip6.fr

We present in this talk a new problem which consists in solving non-linear equations modulo a prime $q = \text{poly}(n)$ with noise (typically a Gaussian), i.e., some equations of the algebraic system are erroneous. This problem, that we have called *Polynomial With Errors* (PWE), is a non-linear (and rather natural) generalization of the well-known *Learning With Errors* (LWE) problem [1, 2, 3]. We recall that LWE is the problem of solving linear equation with noise.

We present in this talk theoretical complexity results on PWE. Note that the hardness of PWE is supported by the hardness of solving algebraic equations without errors ; the PoSSo problem. Solving non-linear system being significantly harder than solving a linear system, it is reasonable to expect that solving PWE will be harder than LWE. However, it can be shown that if the number of equations is $\geq \text{poly}(n)$ (n being the number of variables) then PWE is essentially equivalent to an instance of PWE with bigger parameters. Therefore, the most interesting case to consider is PWE for a fixed and small number $\big(\text{i.e. } < \text{poly}(n)\big)$ of equations. We denote by boundPWE this problem, i.e. PWE with a bounded $(< \text{poly}(n))$ number of samples. We prove that boundPWE has a decision/search equivalence (deciding that a solution exists is equivalent to find a solution) a weak average-case/worst-case reduction. As a by-product, we show that these results also hold for the noiseless version of this problem, i.e. PoSSo.

Finally, we will briefly sketch an algorithm for solving boundPWE/PWE and discuss about the possibly to construct cryptographic schemes based on our new problems.

Références

[1] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *STOC*, pages 84–93. ACM, 2005.

[2] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[3] Oded Regev. The learning with errors problem (invited survey). In *IEEE Conference on Computational Complexity*, pages 191–204. IEEE Computer Society, 2010.

[4] Markus Rückert and Michael Schneider. Estimating the security of lattice-based cryptosystems. *Cryptology ePrint Archive*, (2010/137), 2010.