Algebriac Full Homomorphic Encryption & Resisting Groebner Basis Cryptanalysis

Matthew Tamayo

Abstract:

We propose an algebriac approach to fully homomorphic encryption using multivariate cryptography and provide both theoretical and empirical evidence regarding the difficulty of constructing a secure instance. Next, we show how through careful parameterization and use of non-abelian groups we can create a fully homomorphic encryption system resistant to Groebner basis attacks. Finally, we discuss how Groebner basis algorithms are extremely effective on some other "hard" problems in non-abelian cryptography over the GL(n, F_2).

A lot of problems considered hard by some other authors [1],[2] are susceptible to Groebner basis algorithms as they can be reduced to multivariate quadratic equation in 2 n^2 variables with n^2 equations, which are easy to solve (at least over GL(n, F_2)).

[1] Lize Gu and Shihui Zheng, “Conjugacy Systems Based on Nonabelian Factorization Problems and Their Applications in Cryptography,” *Journal of Applied Mathematics*, vol. 2014, Article ID 630607, 10 pages, 2014. doi:10.1155/2014/630607

[2] Myasnikov, Alexei, Shpilrain, Vladimir, Ushakov, Alexander, "Group-based Cryptography", Advanced Courses in Mathematics, Springer, 2008