Título "Criptoanálisis algebraico con bases de Groebner"

Tutor: Ignacio Luengo Velasco

La teoría de bases de Groebner ([1]) proporciona un método algorítmico muy eficiente para encontrar las soluciones de un sistema de ecuaciones polinómicas en varias variables. El sicoanalista algebraico con bases de Groebner de un esquema criptográfico consiste en el ataque directo mediante la resolución de sistema de ecuaciones polinómicas cuando el esquema se puede representar como un conjunto de aplicaciones polinómicas. La dificultad del ataque se mide fundamentalmente con la complejidad. La complejidad de sistemas genéricos está bien estudiada ([3]) pero en el caso de sistemas especiales como los que aparecen en el criptoanálisis algebraico la complejidad es menos clara.

En este trabajo se estudiará la complejidad de los algoritmos de bases de Groebner para los sistemas que aparecen los esquemas de cifrado multivariable ([2]). En particular se estudiará el caso del algoritmo F4 de Fauguere los sistemas dispersos (sparse) y sus consecuencias para los esquemas que usan polinomios dispersos ([4]).

Referencias:

[1] D. Cox, J. Little, D.O. O'Shea, Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra,
Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
[2] J. Ding, J.E. Gower, D.S. Schmidt:
Multivariate Public Key Cryptosystems. Springer, 2006
[3] J.C. Faugère,A. Joux: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using
Groebner Bases. CRYPTO 2003, LNCS vol. 2729, pp. 44-60. Springer, 2003
construction, J. Lond. Math. Soc. (2) 90 (2014), no. 3, 675–694.
[4] J.-C. Faugère, P.-J. Spaenlehauer, and J. Svartz, Sparse Grobner bases: The unmixed case, New
York, NY, USA, 2014. ACM., 2014, pp. 178–185.