

## TIME COMPLEXITY OF SOME ATTACKS ON A GRÖBNER BASIS CRYPTOSYSTEM

**Marian Hernández-Viera, University of Puerto Rico-Humacao; Ariel Rivera-Torres, University of Puerto Rico-Río Piedras; Ray Sardo, Loyola Marymount University.**

Faculty Advisor: Reinhard Laubenbacher, New Mexico State University

In his book *Algebraic Aspects of Cryptography*, N. Koblitz proposes a public-key cryptosystem based on solving the Ideal Membership Problem: for a given polynomial ideal  $I = \langle f_1, \dots, f_n \rangle$ , determine whether a given polynomial  $h$  belongs to  $I$ . One known method of finding a solution to this problem is to compute a Gröbner basis for  $I$ , that is, a set of generators for  $I$ , the leading terms of which generate all leading terms of elements in  $I$ . This proposed cryptosystem relies on the well-known fact that the computation of a Gröbner basis for a polynomial ideal is EXPSPACE-hard. An attack on this cryptosystem has been proposed in a recently-published commentary, in which the authors claim that it is not necessary to compute a Gröbner basis to solve the Ideal Membership Problem. Their claim rests on the computation of a “partial” Gröbner basis for  $I$ , which yields an attack with complexity  $O(\tau^4)$ , where  $\tau$  is the number of terms of the encryption polynomial. We explore the feasibility of this attack by computing numerous examples as evidence to support their claim. Finally, we offer a proposal for an improved attack, and show that this attack has a time complexity of  $O(\tau^4)$ .