Linear and Multilinear Forms in Cryptography*

Guillermo Morales Luna
José de Jesús Angel Angel
Computer Science Department
CINVESTAV-IPN Mexico
gmorales@cs.cinvestav.mx
jjangel@computacion.cs.cinvestav.mx

September 25, 2007

Abstract

In Cryptography one of the most important properties for ciphering maps is the notion of "one-way": The maps should be effectively and efficiently computed while the calculation of their inverses should pose even non-computable problems. Thus linear maps are avoided within this context. However, since 2000 the so called *Pairing Cryptography* has been increasingly important. It is based on bilinear maps indeed. This is essentially due to the difficulty in solving the *Bilinear Diffie-Hellman Problem*: Let $e : G_0 \times G_1 \to G_2$ be a bilinear homomorphism, where G_0, G_1 are finite Abelian groups and G_2 is a cyclic finite group, then given the elements P, aP, bP, cP (obviously the "exponents" a, b, c are supposed unknown) it is required to compute $e(P, P)^{abc}$. Protocols profiting the difficulty of this problem for particular bilinear maps are due to Boneh and Franklin (Identity Based Cryptography), Joux (Three-party Key Distribution) and Boneh, Lynn and Shacham (Short Signatures) among others. Weil and Tate bilinear maps, defined over the groups of elliptic curves, render hard the Bilinear Diffie-Hellman Problem.

*Title to be redefined.

At present time it is still an open problem to find concrete multilinear forms aiming to generalize these constructions. In spite that the generalization problem seems to appear quite naturally, it is difficult to extend the Weil or Tate bilinear maps. But is not difficult to design some cryptography schemes.

In this talk we mentioned the relation between algebra linear and the cryptography