

Analysis of HFE from a BDD point of view

J.F Michon
LIFAR*

J.B. Yunes
LIAFA†

P. Valarcher
LIFAR‡

Key words: BDD, Hidden Fields Equations, cryptanalysis, boolean functions.

BDDs (Binary Decision Diagram) have been introduced by Bryant and are used in verification and still some years in cryptanalysis. BDD are, of course, connected to boolean functions. The BDD structure allows us to represent boolean functions with a *graph*. ... boolean function can be represented by trees of exponential size (in the number of nodes, as a truth table) many one can be represented polynomially (or linearly) by sharing subtree and representing by a graph the structure. The construction of the BDD is obtained by choosing a particular order on the function variables and using iteration on the following Shannon decomposition:

$$f(x_1, \dots, x_n) = x_1 \cdot f(1, x_2, \dots, x_n) + \neg x_1 \cdot f(0, x_2, \dots, x_n)$$

The HFE (Hidden Fields Equations) public key encryption is a public key cryptosystem using polynomial operations over finite fields. It has been proposed by J. Patarin (*Eurocrypt 96*). It may be described as follows:

- Choose a finite field $F_q, q = p^e$, and a basis $(\beta_1, \dots, \beta_e)$ for F_q over F_p . Select a polynomial P of *relatively small degree* with the shape: $P(X) = \sum_{i,j} a_{ij} X^{p^i + p^j}$ for $a_{ij} \in F_q$ for all i, j .
- Choose two p -polynomials, S and T , that permute F_q . Calculate $E(X) = S \circ P \circ T(X) \bmod (X^q - X)$.
- Calculate $n_1, \dots, n_e \in F_p[X_1, \dots, X_e]$ satisfying, $E(X) = \sum_{i=1}^e \beta_i n_i(X_1, \dots, X_e)$ and publish F_q and the $n_i, 1 \leq i \leq e$. The polynomials S, T and P are the secret keys.

If we take $p = 2$ (as for the challenge proposed by Patarin) then E is a set of quadratic boolean equations. The resolution of such a system has been tried using a BDD library.

An *ad hoc* BDD library has been constructed for that purpose. First, we mention that the constructed library has similar performance on such problem than the CuDD library and has better result than the CMU BDD library. Unfortunately, this *naive* approach can't solve, in reasonable time, system with $e > 30$ (the challenge fixed $e = 80$). Nevertheless this approach has given some intermediate results such that the variables order doesn't influence the complexity of the computation (variable ordering has an important status in BDD study) and that such approach is insensible on the degree of the hidden polynomial P . We show that we can cryptanalysis all HFE system defined on $F_{2^{30}}$ (the high quasiquadratic degree constructible in that field is $2^{29} + 2^{28} = 805306368$) in less than 20 minutes (on a SUN).

*Rouen University, Mont Saint-Aignan 76821 FRANCE. Jean-Francis.Michon@univ-rouen.fr

†University Paris 7, 112 rue Chevaleret FRANCE Jean-Baptiste.Yunes@liafa.jussieu.fr

‡Rouen University, Mont Saint-Aignan 76821 FRANCE. Pierre.Valarcher@univ-rouen.fr