An Efficient Provable Distinguisher for HFE

Vivien Dubois, Louis Granboulan, and Jacques Stern*

École normale supérieure
Département d'Informatique, 45 rue d'Ulm, 75230 Paris cedex 05, France
{dubois,granboulan,stern}@di.ens.fr

Abstract. The HFE cryptosystem was the subject of several cryptanalytic studies, sometimes successful, but always heuristic. To contrast with this trend, this work goes back to the beginnning and achieves *in a provable way* a first step of cryptanalysis which consists in distinguishing HFE public keys from random systems of quadratic equations. We provide two distinguishers: the first one has polynomial complexity and subexponential advantage; the second has subexponential complexity and advantage close to one.

These distinguishers are built on the differential methodology introduced at Eurocrypt'05 by Fouque & *al.* Their rigorous study makes extensive use of combinatorics in binary vector spaces. This combinatorial approach is novel in the context of multivariate schemes. We believe that the alliance of both techniques provides a powerful framework for the mathematical analysis of multivariate schemes.

Keywords. Multivariate cryptography, HFE, differential cryptanalysis.

1 Introduction

While quantum computers, if they are ever built, would threaten most popular public-key cryptosystems such as RSA [17], alternative families of systems are currently designed and evaluated. One such family is based on multivariate quadratic polynomials on finite fields, and demonstrated very fruitful. Initiated in the early 80's by Matsumoto-Imai and Fell-Diffie [19] [5], multivariate cryptography received interest after the work of Shamir [3] and Patarin [10,11]. Since then, about four basic trapdoors along with a large number of non-exclusive additional modifications have been invented [4]. These modifications, called *variations*, are designed to prevent structural attacks against the trapdoor.

HFE, probably the most promising of these cryptosystems, was proposed by Patarin [11] as a repair of the broken Matsumoto-Imai cryptosystem [20]. A little later, Kipnis and Shamir found a structural attack reducing the recovery of the private key to a MinRank problem [1]. Unfortunately, no known method to solve MinRank problems is practical for usual parameter sizes; still, the attack reveals weaknesses in the hiding of the trapdoor. Next, Courtois discovered that the multivariate quadratic equations coming from an HFE public key satisfy many

* This work is supported in part by the French government through X-Crypt, in part by the European Commission through ECRYPT

low degree polynomial implicit equations [15]. Finally, Faugère and Joux demonstrated experimentally that systems of multivariate quadratic equations coming from HFE keys have good elimination properties that allow much easier Gröbner bases computations [6] — they broke the basic HFE for the first suggested parameters. Nevertheless, the attack did not extend to some major variations, requires a huge workload both in time and memory for the suggested parameter sizes and its complexity is unclear. Also all mentioned cryptanalytic approaches are heuristic and none provides a provable distinguisher.

Recently, Fouque-Granboulan-Stern proposed a new technique of analysis for multivariate schemes [16]. The method consists in studying the rank of the differential of the public key in order to extract information about the internal structure. The *differential* methodology already proved useful by providing an enhanced cryptanalysis of the Matsumoto-Imai cryptosystem and by breaking its Internal Perturbation variation [16] proposed by Ding [7].

Our results In this paper, we present a further application of the differential approach. It provides a provable distinguisher of HFE public keys, with polynomial complexity and subexponential advantage. This distinguisher can be improved into an algorithm with subexponential complexity and proven advantage close to one. This is the first cryptanalytic insight into the internal structure of HFE which is both entirely proven and practical for standard parameters. Our study requires combinatorics in finite fields of characteristic 2, which we believe to provide a new powerful approach for the analysis of multivariate schemes.

Organization of the paper In Section 2 of this paper, we recall the basic mathematical setting of multivariate cryptography and set up some combinatorial results related to the distribution of ranks of linear maps. In Section 3, we recall the definitions of HFE and its differential, and using the previous combinatorial tools, we show how the HFE internal structure can be detected from a public key with a precisely estimated complexity. A few proofs are sketched in this paper; they appear in details in the appendices of the full paper.

2 Mathematical setting

2.1 Univariate-Multivariate correspondence

Finite Fields [13] We note $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. All fields with 2^n elements are isomorphic, and can be considered as instantiations of the same entity, called *the degree n extension field of* $\mathbb{F}_2$, denoted $\mathbb{F}_{2^n}$. $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-vector space of dimension n and every choice of a basis of $\mathbb{F}_{2^n}$ defines a linear isomorphism from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^n$. Besides, the non-zero elements of $\mathbb{F}_{2^n}$ form a multiplicative group of size $2^n - 1$ and every element a of $\mathbb{F}_{2^n}$ satisfies $a^{2^n} = a$. Last, $\mathbb{F}_{2^n}$ has characteristic 2, that is for all x of $\mathbb{F}_{2^n}$, $x + x = 0$.

$\mathbb{F}_2$-Linear and $\mathbb{F}_2$-quadratic polynomials over $\mathbb{F}_{2^n}$ Characteristic 2 implies that for any a, b in $\mathbb{F}_{2^n}$ and any integer i, $(a+b)^{2^i} = a^{2^i} + b^{2^i}$. As a consequence, for any integer i, the polynomial X^{2^i} defines an $\mathbb{F}_2$-linear map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Besides, since for all a in $\mathbb{F}_{2^n}$, $a^{2^n} = a$, polynomials X^{2^i} and $X^{2^{i+n}}$ define the same function. Thus, we can focus on monomials X^{2^i} for i restricted to $[0, n-1]$. Next, linear combinations over $\mathbb{F}_{2^n}$ of these monomials again define $\mathbb{F}_2$-linear maps from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and we define the set

$$\mathcal{L} = \left\{ \sum_{i=0}^{n-1} a_i X^{2^i};\ a_i \in \mathbb{F}_{2^n}, \forall i \in [0, n-1] \right\}$$

that we call the $\mathbb{F}_2$-*linear polynomials over* $\mathbb{F}_{2^n}$. The same way, it is easy to check that linear combinations over $\mathbb{F}_{2^n}$ of monomials in two variables of the form $X^{2^i} Y^{2^j}$ for i, j in $[0, n-1]$ define $\mathbb{F}_2$-bilinear maps from $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Taking $Y = X$ defines a subset of $\mathbb{F}_{2^n}[X]$

$$\mathcal{Q} = \left\{ \sum_{i,j=0: i \leq j}^{n-1} a_{ij} X^{2^i + 2^j}; a_{ij} \in \mathbb{F}_{2^n}, \forall i, j \in [0, n-1], i \leq j \right\}$$

that we call the $\mathbb{F}_2$-*quadratic polynomials over* $\mathbb{F}_{2^n}$.

Univariate-Multivariate correspondence Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is the evaluation of a polynomial over $\mathbb{F}_{2^n}$, and this polynomial is unique in the quotient ring $\mathbb{F}_{2^n}[X]/(X^{2^n} - X)$. This allows to identify any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ to a univariate polynomial in $\mathbb{F}_{2^n}[X]/(X^{2^n} - X)$. The same way, a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is defined by n coordinate-functions, which are boolean functions in n variables. Each coordinate-function is the evaluation of a polynomial in $\mathbb{F}_2[x_1, \dots, x_n]$, which is unique in the quotient-ring $\mathbb{F}_2[x_1, \dots, x_n]/\{x_1^2 - x_1, \dots, x_n^2 - x_n\}$. This allows to define any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ by its multivariate representation in $(\mathbb{F}_2[x_1, \dots, x_n]/\{x_1^2 - x_1, \dots, x_n^2 - x_n\})^n$. Further, these two sets are isomorphic, by an extension of the isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$. In particular the set of linear maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, denoted $\mathcal{L}_n$, is in bijection with $\mathcal{L}$. Also, the set of quadratic maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, denoted $\mathcal{Q}_n$, is in bijection with $\mathcal{Q}$.

2.2 Combinatorics in $\mathbb{F}_2^n$

Linearly independent sequences and subspaces of $\mathbb{F}_2^n$ We denote by $S(n, d)$ the number of linearly independent sequences of length d of vectors of $\mathbb{F}_2^n$; it is easily seen that $S(n, d) = \prod_{i=0}^{n-1} (2^n - 2^i)$. Each such sequence generates a subspace of dimension d which is also generated by $S(d, d)$ other linearly independent sequences of length d. Therefore the number $E(n, d)$ of subspaces of dimension d in $\mathbb{F}_2^n$ is $S(n, d)/S(d, d)$. Defining $\lambda(n) = \prod_{i=1}^{n} \left(1 - \frac{1}{2^i}\right)$, we have

$$S(n, d) = \frac{\lambda(n)}{\lambda(n-d)} 2^{nd} \qquad \text{and} \qquad E(n, d) = \frac{\lambda(n)}{\lambda(n-d)\lambda(d)} 2^{d(n-d)}$$

$S(n,d)$ is similar to the *number of permutations of size d over n elements*, and $E(n,d)$ is similar to the *number of combinations of size d over n elements*. These quantities sparsely appear in the literature [9,2,18,12], however we could not find any enumerative results dealing with algebraic aspects of binary vector spaces.

Number of linear maps of a given rank We consider a fixed integer r in $[0,n]$ and we enumerate the number of linear maps of rank r. Let $\mathcal{K}$ be the kernel of a map of rank r, and let $\mathcal{B}$ a basis of a complement of $\mathcal{K}$. Any linear map of kernel $\mathcal{K}$ is uniquely defined by the image of $\mathcal{B}$, which is a linearly independent sequence of length r. Therefore, the number of linear maps with kernel $\mathcal{K}$ is $S(n,r)$. This depends only on the dimension $n-r$ of $\mathcal{K}$, and there are $E(n,n-r)$ such subspaces. Finally, the number of linear maps of rank r is

$$E(n,n-r)S(n,r) = \frac{\lambda(n)^2}{\lambda(n-r)^2\lambda(r)}2^{r(n-r)}2^{nr}$$

Dividing by 2^{n^2} provides the proportion of linear maps of rank r. The collection of these proportions for all ranks defines the distribution of ranks of linear maps.

Distribution of ranks of $\mathbb{F}_2$-linear polynomials of constrained degree We close this section by explaining how to compute the distribution of ranks of a random $\mathbb{F}_2$-linear polynomial of a given degree. While only the easy part of our results will be used in the sequel, it gives an other application of the combinatorial approach, which will later show interesting in the context of HFE.

An $\mathbb{F}_2$-linear polynomial P has as many roots as the number of elements in its kernel. Hence, if r is the rank of the $\mathbb{F}_2$-linear polynomial P considered as a linear map, it is easily seen that P has 2^{n-r} roots. Fixing an integer D in $[0,n-1]$, we denote $\mathcal{L}^D$ the subset of $\mathbb{F}_2$-linear polynomials of degree 2^D. A polynomial of degree 2^D has at most 2^D roots, or is the zero polynomial. Then, the rank of a non-zero $\mathbb{F}_2$-linear polynomial P in $\mathcal{L}^D$ is at least $n-D$. The distribution of ranks of $\mathbb{F}_2$-linear polynomials of degree 2^D is given by the following theorem. Although, the theorem does not provide a closed form for these numbers, it allows to compute them for any choice of the parameters.

Theorem 1. *Let D an integer in the interval $[0,n-1]$. A non-zero $\mathbb{F}_2$-linear polynomial of degree 2^D has rank at least $n-D$. The proportions $p_D(0),\dots,p_D(D)$ of elements of $\mathcal{L}^D$ of ranks respectively $n,\dots,n-D$ satisfy the following invertible triangular system*

$$d \in [0,D], \quad E(n,d)2^{-nd} = \sum_{m=d}^{D} E(m,d)p_D(n-d)$$

Sketch of proof. The number of $\mathbb{F}_2$-linear polynomials of degree 2^D is $(2^n-1)2^{nD}$. Given a subspace of dimension d with d in $[0,D]$, the vanishing of an $\mathbb{F}_2$-linear polynomial of degree 2^D results in d linear constraints over its $D+1$ coefficients.

It implies that for each subspace of dimension d, there are exactly $(2^n-1)2^{n(D-d)}$ $\mathbb{F}_2$-linear polynomials which vanish on it. In the product $E(n,d)(2^n-1)2^{n(D-d)}$, the $\mathbb{F}_2$-linear polynomials whose kernel has dimension m with $m \geq d$ are counted $E(m,d)$ times. Therefore, the proportions $p_D(n-d)$ of $\mathbb{F}_2$-linear polynomials of degree 2^D which have rank $n-d$ satisfy the above invertible triangular system.

3 Distinguishers for HFE

The distinguishers that we provide are built on the observation of the previous section: a $\mathbb{F}_2$-linear polynomial of degree at most 2^D has large rank at least $n-D$, while there is a very small albeit non-zero probability that a random linear map of any rank appears. Applying this observation to the differential yields a distinguisher. Even if the idea appears straightforward, the technicalities required to turn it into a precise mathematical proof and to estimate the advantage of the distinguisher are non-trivial and require the previously introduced combinatorial framework. This is especially true of the enhanced distinguisher, where the advantage is made close to one by iteration: the difficulty here is that we have to play with non pairwise independent random variables, whose precise relationship can only be understood through this combinatorial framework.

3.1 Description of HFE

At the basis of multivariate cryptography is the problem of solving a set of multivariate polynomial equations over a finite field. This problem is proven NP-hard [14] and considered very hard in practice for systems of equations at least quadratic with about the same number of equations and unknowns. For such systems, the best algorithms use Gröbner bases theory, have at least exponential complexity, and are impractical for even a few unknowns (or equations).

Informally, the general construction of multivariate cryptosystems consists in hiding an easily solvable multivariate quadratic system into a random-looking system by a secret transformation. More precisely, one considers a quadratic map $\boldsymbol{P}$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ defined by n polynomials of degree 2 in n unknowns of a specific form, which allows to easily solve the system $\boldsymbol{P}(x_1,\ldots,x_n)=(a_1,\ldots,a_n)$ for any element $(a_1,\ldots,a_n)$ of $\mathbb{F}_2^n$. Then, one chooses two invertible affine maps $\boldsymbol{S},\boldsymbol{T}$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, each defined by n multivariate equations of degree 1. Clearly, the composition $\boldsymbol{T}\circ\boldsymbol{P}\circ\boldsymbol{S}$ is again a multivariate quadratic map $\boldsymbol{P'}$ of $\mathbb{F}_2^n$, and any related system $\boldsymbol{P'}(x_1,\ldots,x_n)=(a_1,\ldots,a_n)$ where $(a_1,\ldots,a_n)$ is an element of $\mathbb{F}_2^n$ is impractical to solve by the dedicated algorithms for a prescribed parameter n. To create an asymmetric cryptosystem, the user randomly picks $\boldsymbol{P}$ of the specific form and two invertible affine maps $\boldsymbol{S},\boldsymbol{T}$, and keeps them secret. Then, he publishes $\boldsymbol{P'}=\boldsymbol{T}\circ\boldsymbol{P}\circ\boldsymbol{S}$. A message $\boldsymbol{a}$ encrypted into $\boldsymbol{b}=\boldsymbol{P'}(\boldsymbol{a})$ can only be decrypted by the legitimate user since the multivariate quadratic system $\boldsymbol{P'}(x_1,\ldots,x_m)=\boldsymbol{b}$ can only be solved by inverting the secret process.

HFE is a way to generate easily solvable multivariate quadratic systems. As seen in Section 2.1, the set of quadratic maps, called $\mathcal{Q}_n$, is isomorphic to a specific subset of the univariate polynomials over $\mathbb{F}_{2^n}$, namely $\mathcal{Q}$. It implies that solving a given multivariate quadratic system is equivalent to finding the roots of the related univariate polynomial. In HFE, the latter is made easy by generating quadratic systems from *low degree* univariate polynomials of $\mathcal{Q}$. Parameters for the first challenge of HFE are $n = 80$ and degree 96.

3.2 Differential analysis of multivariate quadratic maps

The differentials of a multivariate quadratic map Given a quadratic map $\boldsymbol{P}$, its *differential* at a point $\boldsymbol{a}$ of $\mathbb{F}_2^n$ is the linear map defined by

$$\boldsymbol{DP_a}(\boldsymbol{x}) = \boldsymbol{P}(\boldsymbol{a}+\boldsymbol{x}) + \boldsymbol{P}(\boldsymbol{x}) + \boldsymbol{P}(\boldsymbol{a}) + \boldsymbol{P}(\boldsymbol{0})$$

It vanishes at $\boldsymbol{a}$. If $\boldsymbol{P}$ is seen as a polynomial, $\boldsymbol{DP_a}$ is an $\mathbb{F}_2$-linear polynomial.

For any element $\boldsymbol{a}$, the rank of $\boldsymbol{DP_a}$ can be evaluated. We call *distribution of ranks of the differentials of* $\boldsymbol{P}$ the collection for all rank r in $[0, n]$ of the proportions of elements $\boldsymbol{a}$ at which the rank of $\boldsymbol{DP_a}$ is r. The distribution of ranks of the differentials is *a major element of analysis of multivariate schemes* because it is invariant in the hiding process. Indeed, for $\boldsymbol{P}$ a quadratic map, $\boldsymbol{S}, \boldsymbol{T}$ two affine bijections of linear parts respectively $\underline{\boldsymbol{S}}, \underline{\boldsymbol{T}}$ (bijective), and $\boldsymbol{P'}$ the quadratic map $\boldsymbol{T} \circ \boldsymbol{P} \circ \boldsymbol{S}$, then it can be checked that for any point $\boldsymbol{a}$

$$\boldsymbol{DP'_a} = \underline{\boldsymbol{T}} \circ \boldsymbol{DP}_{\underline{\boldsymbol{S}}(\boldsymbol{a})} \circ \underline{\boldsymbol{S}}$$

Consequently, the internal function $\boldsymbol{P}$ and the public key $\boldsymbol{P'}$ have the same distribution of ranks of the differentials. Hence, whenever the distribution of ranks of the differentials of $\boldsymbol{P}$ has some property, it can be seen from $\boldsymbol{P'}$.

Distribution of ranks of the differentials of a random quadratic map We consider a random quadratic map $\boldsymbol{P}$ of $\mathbb{F}_2^n$ and we are interested in the rank $r_{\boldsymbol{a}}$ of its differential $\boldsymbol{DP_a}$ at $\boldsymbol{a}$.

Theorem 2. *Given a non-zero element $\boldsymbol{a}$ of $\mathbb{F}_2^n$, and a random quadratic map $\boldsymbol{P}$, the rank of $\boldsymbol{DP_a}$ follows the distribution of ranks of linear maps vanishing at $\boldsymbol{a}$. Therefore, for any t in $[1, n]$ the probability that $\boldsymbol{DP_a}$ has rank $n - t$ is $\alpha_t 2^{-t(t-1)}$ where α_t is a constant in the interval* $[0.16, 3.58]$.

Proof. Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ a non-zero element of $\mathbb{F}_2^n$ and $\boldsymbol{L}$ a linear map that cancels at $\boldsymbol{a}$: $\sum_{i=1}^n \boldsymbol{l}_i a_i = \boldsymbol{0}$ (Note that $\boldsymbol{l}_i \in \mathbb{F}_2^n$ and $a_i \in \mathbb{F}_2$). A quadratic map $\boldsymbol{P}(x_1, \ldots, x_n) = \sum_{i=1}^n \sum_{j=i+1}^n \boldsymbol{p}_{ij} x_i x_j$ has for differential at $\boldsymbol{a}$

$$\boldsymbol{DP_a}(x_1, \ldots, x_n) = \sum_{i=1}^n \left(\sum_{j=1}^{i-1} \boldsymbol{p}_{ji} a_j + \sum_{j=i+1}^n \boldsymbol{p}_{ij} a_j \right) x_i$$

Therefore, $\boldsymbol{DP_a} = \boldsymbol{L}$ is equivalent to

$$\begin{bmatrix} \boldsymbol{l}_1 \\ \\ \vdots \\ \\ \boldsymbol{l}_n \end{bmatrix} = \begin{bmatrix} 0 & \boldsymbol{p}_{12} & \boldsymbol{p}_{13} & \cdots & \boldsymbol{p}_{1n} \\ \boldsymbol{p}_{12} & 0 & \boldsymbol{p}_{23} & \cdots & \boldsymbol{p}_{2n} \\ \boldsymbol{p}_{13} & \boldsymbol{p}_{23} & 0 & & \boldsymbol{p}_{3n} \\ \vdots & \vdots & & \ddots & \vdots \\ \boldsymbol{p}_{1n} & \boldsymbol{p}_{2n} & \boldsymbol{p}_{3n} & \cdots & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ \\ \vdots \\ \\ a_n \end{bmatrix}$$

Up to a reordering of coordinates, one can assume $a_n \neq 0$. Then any choice of coefficients $\boldsymbol{p}_{ij}$ for $i < j < n$ can be completed in a quadratic map such that $\boldsymbol{DP_a} = \boldsymbol{L}$. Indeed, we define for all i in $[1, n-1]$

$$\boldsymbol{p}_{in} = \boldsymbol{l}_i + \sum_{j=1}^{i-1} \boldsymbol{p}_{ji} a_j + \sum_{j=i+1}^{n-1} \boldsymbol{p}_{ij} a_j$$

and we can check that the last row equation $\sum_{i=1}^{n-1} \boldsymbol{p}_{in} a_i = \boldsymbol{l}_n$ is satisfied, using the vanishing at $\boldsymbol{a}$ of both $\boldsymbol{L}$ and $\boldsymbol{DP_a}$. Hence the number of $\boldsymbol{P}$ in $\mathcal{Q}_n$ such that $\boldsymbol{DP_a} = \boldsymbol{L}$ is independent of $\boldsymbol{a}$ and $\boldsymbol{L}$, and the first point of the theorem follows.

Next, for any t in $[1, n]$, a linear map of rank $n - t$ which vanishes at $\boldsymbol{a}$ is a map whose kernel has dimension t and contains $\boldsymbol{a}$. Since the number of such subspaces is $E(n-1, t-1)$, the number of linear maps of rank $n-t$ vanishing at $\boldsymbol{a}$ is $E(n-1, t-1)S(n, n-t)$. Finally the overall number of linear maps vanishing at $\boldsymbol{a}$ is $2^{n(n-1)}$. Among them, those of rank $n - t$ are in proportion

$$\Pr_{\boldsymbol{L} \in \mathcal{L}_n; \boldsymbol{L}(\boldsymbol{a})=\boldsymbol{0}} [rk\, \boldsymbol{L} = (n-t)] = \alpha_t 2^{-t(t-1)} \quad \text{with} \quad \alpha_t = \frac{\lambda(n)\lambda(n-1)}{\lambda(t)\lambda(t-1)\lambda(n-t)}$$

Since the sequence λ decreases towards a value over 0.28 [18], α_t lies in $[0.16, 3.58]$.

3.3 A Fast Distinguisher for HFE

A specific property of HFE We denote $\boldsymbol{P}$ the hidden internal function in HFE and we let $D = \lceil \log_2 \deg(\boldsymbol{P}) \rceil$ where $\deg(\boldsymbol{P})$ is the degree of $\boldsymbol{P}$ considered as a polynomial over $\mathbb{F}_{2^n}$. For any element $\boldsymbol{a}$ of $\mathbb{F}_2^n$, $\boldsymbol{DP_a}$ is an $\mathbb{F}_2$-linear polynomial of degree at most 2^D. Unless it is the zero function, its rank is at least $n - D$. In contrast, we saw in the previous paragraph that the differential of a random quadratic system has rank $n - D - 1$ with probability of the order of $2^{-D(D+1)}$.

A fast distinguisher for HFE For any parameter D in $[0, n]$, we define the algorithm T_D which takes as input a quadratic map $\boldsymbol{P}$ and a non-zero point $\boldsymbol{a}$, computes the differential of $\boldsymbol{P}$ at $\boldsymbol{a}$ and evaluates its rank, finally answers 1 when this rank is $n - D - 1$ and 0 otherwise. The running time of this algorithm is polynomial, more precisely it is $\mathcal{O}(n^3)$.

Using algorithm T_D, we can devise a distinguisher for any non-zero arbitrary value $\boldsymbol{a}$, defined the following way

`INPUT:` a quadratic function $\boldsymbol{P}$ which is
- either a HFE function of degree $\leq 2^D$ (probability 1/2)
- or a random quadratic function (probability 1/2)

`DO:` compute $T_D(\boldsymbol{P}, \boldsymbol{a})$
if $T_D(\boldsymbol{P}, \boldsymbol{a}) = 1$ output `random`, else output `HFE`

The distinguisher always answers `HFE` on HFE functions, but it may answer `HFE` on a random quadratic map which is not HFE. Following Theorem 2, the distinguisher answers `random` on a random quadratic maps with a probability of the order of $2^{-D(D+1)}$. This probability is the advantage of the distinguisher and does not depend on $\boldsymbol{a}$. Since 2^D is polynomial in the security parameter to allow decryption of the HFE cryptosystem, $2^{D(D+1)}$ is subexponential. Hence, any non-zero element of $\mathbb{F}_2^n$ yields a distinguisher for HFE with proven subexponential advantage, or more accurately with advantage the inverse of a subexponential function. A test answering 1 when the rank is $\leq n-D-1$ is a little more efficient but its study is more complicated without changing the order of complexity.

3.4 Enhanced distinguisher

For any parameter D in $[0,n]$ and a fixed integer N, we define the algorithm T_D^N which takes as input a quadratic map $\boldsymbol{P}$ and N distinct non-zero points $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_N$ of $\mathbb{F}_2^n$, computes the values of $T_D(\boldsymbol{P},\boldsymbol{a}_i)$ for all i, finally answers 1 if $T_D(\boldsymbol{P},\boldsymbol{a}_i)=1$ was found for at least one $\boldsymbol{a}_i$, and 0 otherwise. The running time of this algorithm is $\mathcal{O}(Nn^3)$.

The intention behind this algorithm is simple ; it aims at increasing the probability to detect a non-HFE quadratic map by testing for multiple points, yielding a distinguisher with improved advantage. Using algorithm T_D^N, we can devise as before such an improved distinguisher from any arbitrary distinct non-zero values $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_N$.

Let fix N such points $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_N$ and define the random variable

$$S_N^D(\boldsymbol{P})=\sum_{i=1}^{N} T_D(\boldsymbol{P},\boldsymbol{a}_i)$$

over the set $\mathcal{Q}_n$ of quadratic maps. All $T_D(\boldsymbol{P},\boldsymbol{a}_i)$ are $\{0,1\}$ valued random variables over $\mathcal{Q}_n$ and the advantage of the distinguisher is

$$\mathrm{Pr}_{\boldsymbol{P}\in\mathcal{Q}_n}[S_N^D(\boldsymbol{P})\geq 1]$$

From Theorem 2, we deduce that all $T_D(\boldsymbol{P},\boldsymbol{a}_i)$ have the same law, of mean value $\mu_D\simeq 2^{-D(D+1)}$. Hence, we could easily determine the advantage of the distinguisher, if the random variables $T_D(\boldsymbol{P},\boldsymbol{a}_i)$ were independent; unfortunately these random variables are even not pairwise independent. In the sequel, we give more details about this fact and show that this difficulty can be overcome: using our combinatorial framework, the standard deviation of S_N^D can be actually computed. Next, using Chebychev inequality, we prove that for $N=2^{D(D+2)}$, *the advantage of the distinguisher is close to one.*

Mean Value and Standard Deviation of S_N^D

Theorem 3. *The mean value and the standard deviation of S_N^D satisfy respectively*

$$\begin{cases} A_N^D = N\mu_D \\ (\sigma_N^D)^2 = N\mu_D - N\mu_D^2(1+\epsilon_D)+\epsilon_D N^2\mu_D^2 \end{cases}$$

where ϵ_D is lower than $2^{2D+2}/(2^n-1)$ and μ_D is of the order of $2^{-D(D+1)}$.

Proof. For the reader's convenience, we omit the D superscripts and write X_i in place of $T_D(\boldsymbol{P}, \boldsymbol{a}_i)$.

The mean value comes from linearity. The standard deviation satisfies

$$(\sigma_N)^2 = \mathrm{E}_{\boldsymbol{P}\in\mathcal{Q}_n}[(S_N)^2] - (A_N)^2$$

where $\mathrm{E}_{\boldsymbol{P}\in\mathcal{Q}_n}$ denotes the expectation. Further, since the X_i are $\{0,1\}$ valued and the expectation is linear,

$$\mathrm{E}_{\boldsymbol{P}\in\mathcal{Q}_n}[(S_N)^2] = A_N + \sum_{i=1}^{N}\sum_{j\neq i} \mathrm{E}_{\boldsymbol{P}\in\mathcal{Q}_n}[X_i X_j]$$

where for each pair $i \neq j$,

$$\mathrm{E}_{\boldsymbol{P}\in\mathcal{Q}_n}[X_i X_j] = \mathrm{Pr}_{\boldsymbol{P}\in\mathcal{Q}_n}[rk\, DP_{\boldsymbol{a}_i} = n - D - 1\,,\, rk\, DP_{\boldsymbol{a}_j} = n - D - 1] \quad (1)$$

As already mentioned, random variables X_i and X_j are not independent, for any pair $i \neq j$. Indeed, the differentials of $\boldsymbol{P}$ at $\boldsymbol{a}_i$ and $\boldsymbol{a}_j$ satisfy $\boldsymbol{DP}_{\boldsymbol{a}_i}(\boldsymbol{a}_j) = \boldsymbol{DP}_{\boldsymbol{a}_j}(\boldsymbol{a}_i)$. Therefore, the vanishing (or not) of $\boldsymbol{DP}_{\boldsymbol{a}_i}$ at $\boldsymbol{a}_j$ is correlated to the vanishing (or not) of $\boldsymbol{DP}_{\boldsymbol{a}_j}$ at $\boldsymbol{a}_i$. It follows that the ranks of $\boldsymbol{DP}_{\boldsymbol{a}_i}$ and $\boldsymbol{DP}_{\boldsymbol{a}_j}$ are not independent. Fortunately, the distribution of ranks of pairs $(\boldsymbol{DP}_{\boldsymbol{a}_i}, \boldsymbol{DP}_{\boldsymbol{a}_j})$ can be fully understood: defining the set $D(\boldsymbol{a}, \boldsymbol{b})$ of pairs of linear maps $(\boldsymbol{L}, \boldsymbol{L'})$ such that $\boldsymbol{L}(\boldsymbol{a}) = \boldsymbol{0}, \boldsymbol{L'}(\boldsymbol{b}) = \boldsymbol{0}, \boldsymbol{L}(\boldsymbol{b}) = \boldsymbol{L'}(\boldsymbol{a})$, we can prove the following lemma whose proof is very similar to that of Theorem 2.

Lemma 1. *Given two distinct non-zero elements $\boldsymbol{a}$ and $\boldsymbol{b}$ of $\mathbb{F}_2^n$, and a random quadratic map $\boldsymbol{P}$, the rank of the pair $(\boldsymbol{DP}_{\boldsymbol{a}}, \boldsymbol{DP}_{\boldsymbol{b}})$ follows the distribution of ranks of pairs of linear maps in $D(\boldsymbol{a}, \boldsymbol{b})$.*

Lemma 1 implies that

$$\mathrm{Pr}_{\boldsymbol{P}\in\mathcal{Q}_n}\begin{bmatrix} rk\,\boldsymbol{DP}_{\boldsymbol{a}_i} = n - D - 1 \\ rk\,\boldsymbol{DP}_{\boldsymbol{a}_j} = n - D - 1 \end{bmatrix} = \mathrm{Pr}_{(\boldsymbol{L},\boldsymbol{L'})\in D(\boldsymbol{a}_i,\boldsymbol{a}_j)}\begin{bmatrix} rk\,\boldsymbol{L} = n - D - 1 \\ rk\,\boldsymbol{L'} = n - D - 1 \end{bmatrix} \quad (2)$$

It remains to compute the probability on the right hand-side of the above. This probability is part of the distribution of ranks of pairs of linear maps in $D(\boldsymbol{a}, \boldsymbol{b})$, which can be computed by the same combinatorial methods.

As a preliminary, let $N_k(r)$ denote the number of linear maps of rank r vanishing on a prescribed subspace of dimension k. The values $N_1(r)$ for all r were computed in the proof of the Theorem 2. In the following, we will need in addition the values $N_2(r)$ for all r, which can be computed the same way. This computation is systematic and can be done at no cost for a general k : for r in $[0, n-k]$, the number of subspaces of dimension $n - r$ containing the prescribed subspace is $E(n-k, n-k-r)$, and the number of linear maps of rank r having one of these subspaces as kernel is $S(n, r)$. Therefore $N_k(r) = E(n-k, n-k-r)S(n, r)$ for r in $[0, n-k]$, and 0 otherwise.

The distribution of ranks of pairs of linear maps in $D(\boldsymbol{a}, \boldsymbol{b})$ is given by the following lemma.

Lemma 2. *Given two non-zero distinct points $\boldsymbol{a}, \boldsymbol{b}$ in $\mathbb{F}_2^n$, and for any integers r and s in $[0, n-1]$, the proportion of pairs $(\boldsymbol{L}, \boldsymbol{L'})$ of linear maps in $D(\boldsymbol{a}, \boldsymbol{b})$ which have rank (r, s) is*

$$\frac{1}{2^{n(2n-3)}} \times \left(N_2(r)N_2(s) + \frac{1}{2^n - 1}(N_1(r) - N_2(r))(N_1(s) - N_2(s)) \right)$$

Proof. A pair $(\boldsymbol{L}, \boldsymbol{L'})$ in $D(\boldsymbol{a}, \boldsymbol{b})$ must satisfy $\boldsymbol{L}(\boldsymbol{a}) = 0, \boldsymbol{L'}(\boldsymbol{b}) = 0, \boldsymbol{L}(\boldsymbol{b}) = \boldsymbol{L'}(\boldsymbol{a})$, which are three independent linear constraints over the $2n$ coefficients in $\mathbb{F}_2^n$ defining $\boldsymbol{L}$ and $\boldsymbol{L'}$. Consequently $D(\boldsymbol{a}, \boldsymbol{b})$ has $2^{n(2n-3)}$ elements.

We define $V_{\boldsymbol{a}}$ as the set of linear maps which vanish at $\boldsymbol{a}$ and $V_{[\boldsymbol{a},\boldsymbol{b}]}$ as the set of linear maps which vanish on the subspace generated by $\boldsymbol{a}$ and $\boldsymbol{b}$. Some fraction of functions $\boldsymbol{L} \in V_{\boldsymbol{a}}$ also vanish at $\boldsymbol{b}$, and when it happens, the functions $\boldsymbol{L'}$ such that $(\boldsymbol{L}, \boldsymbol{L'}) \in D(\boldsymbol{a}, \boldsymbol{b})$ are those in $V_{[\boldsymbol{a},\boldsymbol{b}]}$. Conversely, for each function $\boldsymbol{L} \in V_{\boldsymbol{a}} \setminus V_{[\boldsymbol{a},\boldsymbol{b}]}$, functions $\boldsymbol{L'}$ such that $(\boldsymbol{L}, \boldsymbol{L'}) \in D(\boldsymbol{a}, \boldsymbol{b})$ are those in $V_{\boldsymbol{b}} \setminus V_{[\boldsymbol{a},\boldsymbol{b}]}$ with $\boldsymbol{L'}(\boldsymbol{a}) = \boldsymbol{L}(\boldsymbol{b})$; these functions represent a fraction $1/(2^n - 1)$ of all functions in $V_{\boldsymbol{b}} \setminus V_{[\boldsymbol{a},\boldsymbol{b}]}$ since $\boldsymbol{L}(\boldsymbol{b})$ is one of the $2^n - 1$ equally possible non-zero values for $\boldsymbol{L'}(\boldsymbol{a})$. □

Applying Lemma 2 with $r = s = (n - D - 1)$ provides the probability of equation (2). Using the relation

$$N_1(n - D - 1) = \frac{2^{n-1} - 1}{2^D - 1} N_2(n - D - 1)$$

this probability is

$$\frac{N_1(n - D - 1)^2}{2^{n(2n-3)}} \times \left(\left(\frac{2^D - 1}{2^{n-1} - 1} \right)^2 + \frac{1}{2^n - 1} \left(1 - \frac{2^D - 1}{2^{n-1} - 1} \right)^2 \right) \tag{3}$$

Besides, the proportion of linear maps of rank $n - D - 1$ vanishing at $\boldsymbol{a}$, denoted μ_D, is $N_1(n - D - 1)/2^{n(n-1)}$. Therefore, the factor in (3) equals $\mu_D^2 2^n$ and after a few steps, we get for the above probability

$$\mu_D^2 \left(1 + \epsilon_D\right) \qquad \text{with} \quad \epsilon_D = \frac{1}{2^n - 1} \left(\frac{2^n(2^D - 1)}{2^{n-1} - 1} - 1 \right)^2$$

As a remark, since the proportion of pairs of linear maps in $V_{\boldsymbol{a}} \times V_{\boldsymbol{b}}$ of rank $(n - D - 1, n - D - 1)$ is μ_D^2, ϵ_D is a correcting term which measures the distance between the distribution of ranks in $D(\boldsymbol{a}, \boldsymbol{b})$ and in $V_{\boldsymbol{a}} \times V_{\boldsymbol{b}}$ at the pair of ranks $(n - D - 1, n - D - 1)$. From

$$\epsilon_D = \frac{1}{2^n - 1} \left(2^{D+1} - 1 - 2 \left(1 - \frac{2^D - 1}{2^{n-1} - 1} \right) \right)^2$$

we see that the correcting term ϵ_D is less than $2^{2(D+1)}/(2^n - 1)$.

We can now come back to equation (1)

$$\mathrm{E}_{\boldsymbol{P} \in \mathcal{Q}_n}[X_i X_j] = \mu_D^2 \left(1 + \epsilon_D\right)$$

to finally obtain

$$(\sigma_N)^2 = N\mu_D - N\mu_D^2(1 + \epsilon_D) + \epsilon_D N^2 \mu_D^2$$

Lower Bound on the Advantage Using Chebychev inequality, we can upper-bound $\Pr_{\boldsymbol{P}\in\mathcal{Q}}[S_N^D(\boldsymbol{P})=0]$. Indeed, for all t in the interval $(0, A_N^D/\sigma_N^D]$

$$\Pr_{\boldsymbol{P}\in\mathcal{Q}}[S_N^D(\boldsymbol{P})=0] \leq \Pr_{\boldsymbol{P}\in\mathcal{Q}}[\left|S_N^D(\boldsymbol{P})-A_N^D\right| \geq t\,\sigma_N^D] \leq \frac{1}{t^2}$$

We take $t = A_N^D/\sigma_N^D$; then

$$\frac{1}{t^2} = \frac{(\sigma_N^D)^2}{(A_N^D)^2} = \frac{1}{N\mu_D} - \frac{1}{N}(1+\epsilon_D) + \epsilon_D < \frac{1}{N\mu_D} + \epsilon_D$$

Now let fix $N\mu_D = 2^a$, for some integer a. Then

$$\frac{1}{t^2} < \frac{1}{2^a} + \epsilon_D$$

and the advantage is

$$\Pr_{\boldsymbol{P}\in\mathcal{Q}}[S_N^D(\boldsymbol{P}) \geq 1] = 1 - \Pr_{\boldsymbol{P}\in\mathcal{Q}}[S_N^D(\boldsymbol{P})=0] > 1 - \frac{1}{2^a} - \epsilon_D$$

For instance, for $N = 2^D/\mu_D$, our distinguisher has running time $\mathcal{O}(2^{D(D+2)}n^3)$ and advantage at least of the order of

$$1 - \frac{1}{2^D} - \frac{4}{2^{n-2D}}$$

For $N = 2^{D^2}/\mu_D$, the complexity becomes $\mathcal{O}(2^{D(2D+1)}n^3)$ and the advantage is made at least $1 - 2^{-D^2} - 4.2^{-(n-2D)}$.

4 Conclusion

In this paper, we provide two distinguishers of HFE public keys: the first one has polynomial complexity and subexponential advantage; the second has subexponential complexity and advantage close to one. Though the cryptanalytic impact is smaller than the work of Faugere and Joux [6], our work is the first which shows without heuristics how the internal structure of HFE yields some particularities. It aims in particular at initiating a process of mathematical analysis of multivariate primitives, enlightened by the precedent heuristic approachs. The methodology used in this paper is new and widely applicable in the context of multivariate schemes. It should provide a solid framework of analysis for the numerous variations, which mostly escape all previous heuristic approachs. In particular, it is well suited to analyze the Internal Perturbation of HFE [21] suggested by Ding [8].

This study used differential properties of quadratic maps over an $\mathbb{F}_2$-extension $\mathbb{F}_{2^n}$, and combinatorics in $\mathbb{F}_2$-linear spaces. We showed that HFE public keys have very specific differential properties. This raises an interesting open problem: is the set of public keys such that all differentials have rank at least $n-D$ larger than the set of public keys affinely equivalent to an $\mathbb{F}_2$-linear polynomial of degree at most 2^D ? Another open problem is the existence of a polynomial time distinguisher for HFE public keys.

References

1. A.Kipnis and A.Shamir. Cryptanalysis of the HFE Public Key Cryptosystem. In *Crypto'99*, LNCS 1666, pages 19–30. Springer-Verlag, 1999.
2. A.E.Solow A.Nijenhuis and H.S.Wilf. Bijective methods in the theory of finite vector spaces. *J. Combin. Theory (A)*, 37:80–84, 1984.
3. A.Shamir. Efficient signature schemes based on Birational Permutations. In *Crypto'93*, LNCS 773, pages 1–12. Springer-Verlag, 1994.
4. C.Wolf and B.Preneel. Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. http://eprint.iacr.org/.
5. H.Fell and W.Diffie. Analysis of a Public Key Approach based on Polynomial Substitution. In *Crypto'85*, LNCS 218, pages 340–349. Springer-Verlag, 1985.
6. J-C.Faugère and A.Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner Bases. In *Crypto'03*, LNCS 2729, pages 44–60. Springer-Verlag, 2003.
7. J.Ding. A new variant of the Matsumoto-Imai Cryptosystem through Perturbation. In *PKC'04*, LNCS 2947, pages 305–318. Springer-Verlag, 2004.
8. J.Ding and D.Schmidt. Cryptanalysis of HFEv and Internal Perturbation of HFE. In *PKC'05*, LNCS 3386, pages 288–301. Springer-Verlag, 2005.
9. J.Goldman and G-C.Rota. The number of subspaces of a vector space. In W.T.Tutte, editor, *Recent progress in Combinatorics*, pages 75–83. Academic Press, 1969.
10. J.Patarin. Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In *Crypto'95*, LNCS 963, pages 248–261. Springer-Verlag, 1995.
11. J.Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two families of asymetric algorithms. In *Eurocrypt'96*, LNCS 1070, pages 33–46. Springer-Verlag, 1996.
12. K.E.Morrison. An introduction to q-species. *The Electronic Jounral of Combinatorics*, 12(R62), 2005.
13. K.Ireland and M.Rosen. *A Classical Introduction to Modern Number Theory*, chapter 7. Springer-Verlag, second edition, 1998.
14. M.Garey and D.Johnson. *Computer and Intractability: A guide to the theory of NP-completeness*. Freeman, 1979.
15. N.Courtois. The security of Hidden Field Equations (HFE). In *CT-RSA'01*, LNCS 2020, pages 266–281. Springer-Verlag, 2001.
16. P-A.Fouque, L.Granboulan, and J.Stern. Differential cryptanalysis for Multivariate Schemes. In *Eurocrypt'05*, LNCS 3386, pages 341–353. Springer-Verlag, 2005.
17. P.Shor. Polynomial-time algorithms for prime factorzation and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
18. S.Finch. *Mathematical Constants*, pages 354–361. Cambridge, 2003.
19. T.Matsumoto and H.Imai. A class of asymetric cryptosystems based on Polynomials over Finite Rings. In *ISIT'83*, pages 131–132, 1983.
20. T.Matsumoto and H.Imai. Public Quadratic Polynomial-tuples for efficient signature-verification and message encryption. In *Eurocrypt'88*, LNCS 330, pages 419–453. Springer-Verlag, 1988.
21. V.Dubois, L.Granboulan, and J.Stern. Cryptanalysis of HFE with Internal Perturbation. work in progress, 2006.