# Analysis of Intermediate Field Systems

Olivier Billet, Jacques Patarin and Yannick Seurin

*Extended abstract. A full version of this paper is in preparation.*

**Abstract.** We study a new generic trapdoor for public key multivariate cryptosystems, called IFS for Intermediate Field Systems, which can be seen as dual to HFE. This new trapdoor relies on the possibility to invert a system of quadratic multivariate equations with few (logarithmic with respect to the security parameter) unknowns on an intermediate field thanks to Gröbner bases algorithms. We provide a comprehensive study of the security of this trapdoor and show that it is equivalent to the security provided by HFE. Therefore, while insecure in its basic form, this trapdoor may reveal quite attractive when used with, *e.g.*, the minus modifier.

**Keywords.** Multivariate Cryptography, HFE, Gröbner basis.

## 1. Introduction

Multivariate cryptography dates back to the Matsumoto-Imai scheme [14] proposed in 1985 and has been evolving fast during the past two decades. Many new trapdoors (HFE [15], UOV [13], . . . ) have been introduced, along with modifiers (+, −, internal perturbation [16, 2], . . . ) to enhance the security of the schemes (see [18] for an overview). Though many of these multivariate public key schemes have recently been broken [9, 12, 6, 5] and some cryptographers are beginning to question the possibility of asymmetric multivariate cryptography, there seems to remain some potential interest in studying new schemes of this type. There are at least two reasons for this: the underlying hard problem MQ is NP-complete and appears to be hard for any practical instance (which is not the case for most of the currently used public key schemes), and the multivariate schemes obtained are often very efficient.

Among the multivariate schemes still thwarting the significant cryptanalytic efforts of the cryptographic community are UOV and HFE$^-$ (that is, HFE when some public equations are removed). In this paper, we study a new trapdoor which carries much similarity with HFE.

## 2. Hidden Field Equations

We first briefly recall the structure of the HFE trapdoor proposed by Patarin [15]. Let $\mathbb{F} = \mathrm{GF}(q)$ be some finite field and let $\mathbb{E}$ be an extension of degree $n$ over $\mathbb{F}$. HFE uses as its secret internal transformation, a mapping $\mathbf{F} : \mathbb{E} \longrightarrow \mathbb{E}$ of the following form:

$$\mathbf{F} : X \longmapsto F(X) = \sum_{\substack{0 \le i < j \le n \\ q^i + q^j \le D}} a_{i,j} X^{q^i + q^j} + \sum_{\substack{0 \le k \le n \\ q^k \le D}} b_k X^{q^k} + c \ , \qquad (1)$$

where the coefficients $a_{i,j}$, $b_k$, and $c$ are randomly drawn from $\mathbb{E}$. The overall degree of the polynomial $F(X)$ is upper bounded by some reasonable value (logarithmic in the security parameter) so that the owner of the secret key can efficiently invert this polynomial. The structure of this transformation is then hidden thanks to a pair of one-to-one affine mappings $S$ and $T$ from $\mathbb{E}$ to $\mathbb{E}$. Now recall that $\mathbb{E} \simeq \mathbb{F}^n$ so that $S$ and $T$ can be expressed as $n \times n$ matrices over $\mathbb{F}$; Further, using the fact that $X \mapsto X^{q^l}$ is $\mathbb{F}$-linear for any integer $l$, the composition: $\mathbf{G} = T \circ \mathbf{F} \circ S$, can be expressed as a set of $n$ quadratic multivariate polynomials in $n$ unknowns defined over $\mathbb{F}$. This mapping $\mathbf{G}$ constitutes the public mapping.

Faugère and Joux showed in [9] that HFE cryptosystems are susceptible to Gröbner basis attacks. A theoretical investigation of this fact was later given by Granboulan *et al.* in [12]: the public set of equations arising from HFE has a lower degree of regularity (which determines the complexity of computing a Gröbner basis) than what is expected from a generic (randomly chosen) system. More precisely, if $D$ is the upper bound of the degree of the HFE polynomial, then the degree of regularity is $\Delta = \mathcal{O}(D)$. Since the complexity of a Gröbner basis computation for a system with $n$ equations and $n$ unknowns is given by $n^{\mathcal{O}(\Delta)}$, and since $D$ was chosen so that $D = \mathcal{O}(\log n)$ in order to enable efficient decryption, the complexity of a Gröbner basis attack is sub-exponential.

## 3. Intermediate Field Systems

In the previous section we have reviewed the basic properties of the HFE cryptosystem. The best attack currently known against HFE [1, 9, 12] uses the fact that the univariate equation in the extension field has a total degree that is much lower than for a randomly chosen equation. Therefore, a natural thing to ask is: Are there multivariate cryptosystems that are similar to HFE and for which the total degree of the univariate representation in the highest extension field $\mathbb{E}$ can be as large as $|\mathbb{E}| - 1$? We now describe such a cryptosystem.

### 3.1. IFS: General Construction

This section exposes a new type of multivariate cryptosystems that we call Intermediate Field Systems. It is based on the very natural idea of using intermediate fields, as was already suggested in [17, 4] for instance. However, as the attacks [3, 11] against these two previous schemes suggest, it is fundamental for the security of the cryptosystem that no strong structure exists. Therefore, we strive to consider as generic cryptosystems as possible.

To describe the construction, let us consider some base finite field $\mathbb{F} = \mathrm{GF}(q)$ and some extension field $\mathbb{K} \simeq \mathbb{F}^d$ of degree $d$ over $\mathbb{F}$. We also consider a non-zero integer $N$ and let $n = Nd$. Eventually, we let $\mathbb{E}$ denote some finite field of degree $N$ over $\mathbb{K}$.

As usual with asymmetric multivariate cryptosystems, the public map $\mathbf{G}$ is given as a set of $n$ multivariate quadratic polynomials $(g_1, \ldots, g_n)$ in $n$ unknowns defined over $\mathbb{F}$. This public map results from the composition of a secret internal transformation $\mathbf{F}$ and two secret linear one-to-one mappings $S$ and $T$ that are used to hide the actual value of $\mathbf{F}$:

$$\mathbf{G} = T \circ \mathbf{F} \circ S \ . \tag{2}$$

The secret internal transformation $\mathbf{F}$ is given by a set of $N$ multivariate polynomials $(f_1, \ldots, f_N)$ in $N$ unknowns defined over $\mathbb{K}$, and is of the following specific form:

$$\begin{aligned} f_k(Z_1, \ldots, Z_N) = \sum_{1 \le i \le j \le N} \ \sum_{\substack{0 \le u,v \le d-1 \\ q^u + q^v \le D}} a_{ijuv}^{(k)} Z_i^{q^u} Z_j^{q^v} \\ + \sum_{1 \le i \le N} \ \sum_{\substack{0 \le u \le d-1 \\ q^u \le D}} b_{iu}^{(k)} Z_i^{q^u} + c^{(k)} \end{aligned} \tag{3}$$

for some fixed parameter $D$, and where the coefficients are randomly chosen in $\mathbb{K}$.

Though there might be some interest in letting the degree $D$ of the secret polynomials being greater than 2, we will focus on simpler secret transformations for which $u$ and $v$ have been set to zero, in which case we will write:

$$f_k(Z_1, \ldots, Z_N) = \sum_{1 \le i \le j \le N} a_{ij}^{(k)} Z_i Z_j + \sum_{1 \le i \le N} b_i^{(k)} Z_i + c^{(k)} \ . \tag{4}$$

Note that in this case, the secret transformation takes the following special form when expressed in the extension field $\mathbb{E} \simeq \mathbb{K}^N$:

$$F(X) = \sum_{1 \le i \le j \le N-1} \alpha_{ij} X^{q^{d \cdot i} + q^{d \cdot j}} + \sum_{1 \le i \le N-1} \beta_i X^{q^{d \cdot i}} + \gamma \ . \tag{5}$$

One might wonder why upper bound the degree $D$ of the polynomials of the secret transformation from (3); It is simply because if $D$ were not bounded, the resulting public set of polynomials would be as generic as possible, and therefore nobody could efficiently invert it, not even the owner of the secret key. However, note that,

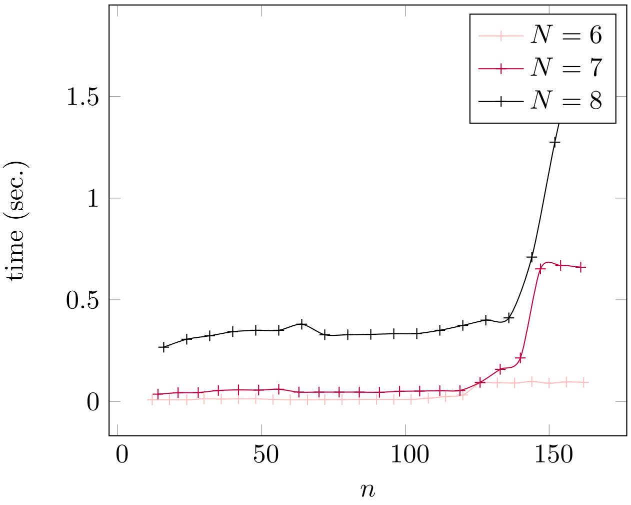

Figure 1. Decryption times for IFS with $N \in \{6, 7, 8\}$.

contrary to HFE, even when $D = 2$ the degree of the univariate representation over $\mathbb{E}$ given in (5) is *not* upper bounded.

A typical set of parameters could be $q = 2$, $d = 16$, and $N = 8$ so that the public set of polynomials has $n = 128$ unknowns defined over GF(2).

### 3.2. Complexity of Decryption

We analyse in this section what are the conditions on the parameters $d$ and $N$ for the cryptosystem to allow efficient decryption. As inverting a randomly chosen set of polynomials in $n$ unknowns has complexity $2^{\mathcal{O}(n)}$, it makes sense to use $n$ as the security parameter. The heavy computation during decryption obviously consists of inverting the secret set of polynomials. This is done through the computation of a Gröbner basis. Since this again has a complexity $2^{\mathcal{O}(N)}$, we must choose $N = \mathcal{O}(\log n)$ in order to be able to decrypt efficiently. Sample timings for IFS with $N \in \{6, 7, 8\}$ variables defined over various base fields $\mathbb{F}^{\lfloor n/N \rfloor}$ so that the public set of polynomials defined over $\mathbb{F} = \mathrm{GF}(2)$ has a number of unknowns $n$ ranging from 16 to 160 are given in Figure 1.

Anticipating the security discussion, we can tell from Fig. 2 and 3 that HFE and IFS provide a similar level of security for carefully chosen parameters.

## 4. Security Analysis

### 4.1. Susceptibility to Gröbner basis attacks

It is possible to carry out the analysis of the degree of regularity of the public system arising from an IFS trapdoor in a similar way as was done for HFE [12]

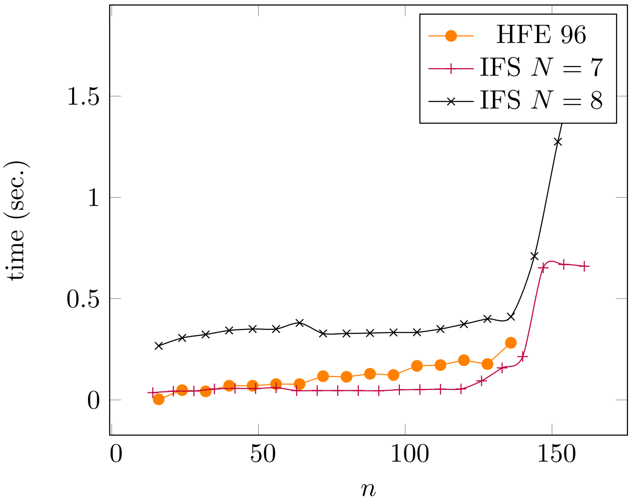

Figure 2. Comparison between the decryption times for IFS with $N \in \{7, 8\}$ and HFE with $D = 96$.

and to show that the degree of regularity of such a system is $\Delta = \mathcal{O}(N)$. Since the number of variables in the intermediate field must verify $N = \mathcal{O}(\log n)$ to allow efficient decryption, it turns out that the complexity of a Gröbner basis computation is sub-exponential just like for HFE cryptosystems. A detailed analysis will be given in the full version of the paper.

We carried out some timing experiments using MAGMA 2.13 in order to assess the difficulty of computing a Gröbner basis for a public system arising from an IFS cryptosystem. The results are depicted in Figure 3. Timing experiments for HFE are also given for comparison.

### 4.2. Differential properties

Differential analysis has arisen as a fundamental tool for studying multivariate schemes. It was successively used to cryptanalyse PMI [10], IPHFE [8], and recently SFLASH [5]. The main observation is that the distribution of the rank of the differentials of the public key of a multivariate scheme is not random.

Given an $\mathbb{F}$-quadratic map $\boldsymbol{G}$ over $\mathbb{F}^n$, its differential at point $\boldsymbol{a} \in \mathbb{F}^n$ is the linear map defined by

$$\boldsymbol{DG_a}(\boldsymbol{x}) = \boldsymbol{G}(\boldsymbol{a} + \boldsymbol{x}) - \boldsymbol{G}(\boldsymbol{x}) - \boldsymbol{G}(\boldsymbol{a}) + \boldsymbol{G}(\boldsymbol{0}) \ .$$

It can be checked that when $\boldsymbol{G} = T \circ \boldsymbol{F} \circ S$, the differential of $\boldsymbol{G}$ is

$$\boldsymbol{DG_a} = T \circ \boldsymbol{DF}_{S(\boldsymbol{a})} \circ S \ .$$

Hence the distribution of the rank of the differentials of the secret map $\boldsymbol{F}$ and the public map $\boldsymbol{G}$ are the same.

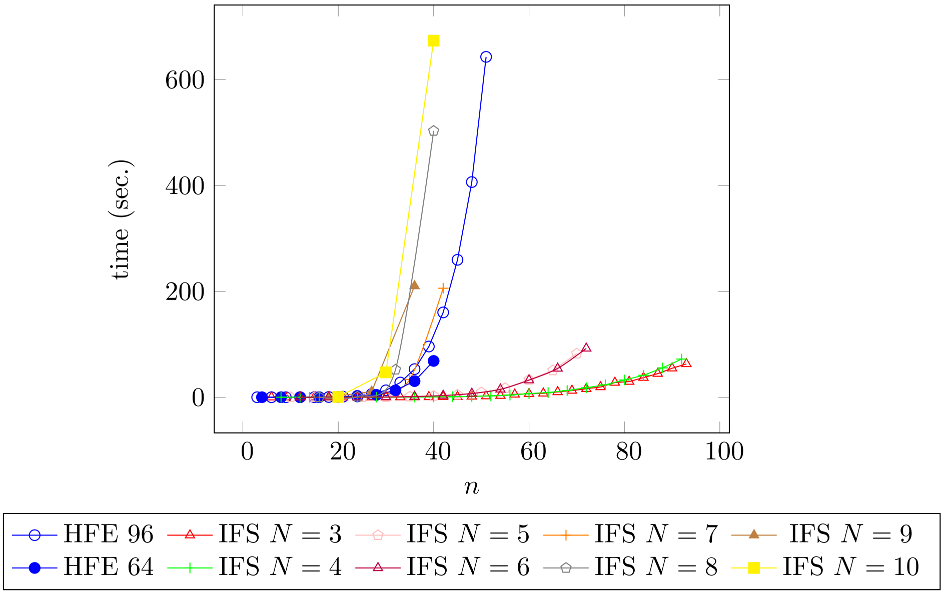

Figure 3. Timings for Gröbner basis computation on public sets of polynomials for IFS cryptosytems as a function of $n = N \cdot d$. Experiments were conducted with algorithm F4 of MAGMA 2.13.

For HFE, the fact that the degree of the secret polynomial is upper bounded by $D$ implies that $\boldsymbol{DF_a}$ is a polynomial of degree less than $D$ as well, hence has less than $D$ roots. This implies that $\boldsymbol{DF_a}$ has rank at least $n - \lceil \log_q(D) \rceil$. As the differential of a random quadratic map has a non-negligible probability of having a smaller rank, this leads to an efficient distinguisher for HFE [7]. It also enabled to cryptanalyse HFE with internal perturbation, IPHFE [8].

It can be shown that for IFS, similar distinguishing properties will arise. Namely, the number of roots of the polynomial $\boldsymbol{DF}$ must necessarily be a multiple of $q^d$. This can be seen from Eq. (5): let $x \in \mathbb{E}$ be a root of $\boldsymbol{DF}$; then for any $\alpha \in \mathbb{K}$, it can be verified that $\boldsymbol{DF}(\alpha x) = 0$ since $\alpha^{q^d} = 1$. A detailed analysis of the consequences of this observation will be given in the full paper.

## 5. Conclusion

We presented a new trapdoor for multivariate public key schemes based on the possibility to efficiently invert a set of quadratic multivariate polynomials with few unknowns on an intermediate field with Gröbner basis algorithms. We initiated the security analysis of such schemes and found that in its basic form, it is equivalent to the security of HFE with respect to known attacks. While this new trapdoor may reveal an interesting companion to HFE, its interaction with classical modifiers remains to be studied. We hope that the investigation of this new trapdoor will enhance the understanding of multivariate public key schemes in general.

## References

[1] Nicolas Tadeusz Courtois. The Security of Hidden Field Equations (HFE). In David Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 266–281. Springer, 2001.

[2] Jintai Ding. A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. In Feng Bao, Jianying Zhou, and Robert Deng, editors, *Public key cryptography – PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 2004.

[3] Jintai Ding, Lei Hu, Xuyun Nie, Jianyu Li, and John Wagner. High Order Linearization Equation (HOLE) Attack on Multivariate Public Key Cryptosystems. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography – PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 233–248. Springer, 2007.

[4] Jintai Ding, Christopher Wolf, and Bo-Yin Yang. $\ell$-Invertible Cycles for Multivariate Quadratic (MQ) Public Key Cryptography. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography – PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 266–281. Springer, 2007.

[5] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. Practical Cryptanalysis of SFLASH. In Alfred Menezes, editor, *Advances in Cryptology – CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.

[6] Vivien Dubois, Pierre-Alain Fouque, and Jacques Stern. Cryptanalysis of SFLASH with Slightly Modified Parameters. In Moni Naor, editor, *Advances in Cryptology – EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 264–275. Springer, 2007.

[7] Vivien Dubois, Louis Granboulan, and Jacques Stern. An Efficient Provable Distinguisher for HFE. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 2006.

[8] Vivien Dubois, Louis Granboulan, and Jacques Stern. Cryptanalysis of HFE with Internal Perturbation. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography*, volume 4450 of *Lecture Notes in Computer Science*, pages 249–265. Springer, 2007.

[9] Jean-Charles Faugère and Antoine Joux. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems using Gröbner Bases. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.

[10] Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. Differential Cryptanalysis for Multivariate Schemes. In Ronald Cramer, editor, *Advances in cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 341–353. Springer, 2005.

[11] Pierre-Alain Fouque, Gilles Macario-Rat, Ludovic Perret, and Jacques Stern. Total Break of the $\ell$-IC Signature Scheme. In Ronald Cramer, editor, *Public Key Cryptography – PKC 2008*, volume 4939 of *Lecture Notes in Computer Science.* Springer, 2008.

[12] Louis Granboulan, Antoine Joux, and Jacques Stern. Inverting HFE is Quasipolynomial. In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 345–356. Springer, 2006.

[13] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar Signature Schemes. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999.

[14] Tsutomu Matsumoto and Hideki Imai. Public Quadratic Polynominal Tuples for Efficient Signature Verification and Message Encryption. In C. G. Günther, editor, *Advances in Cryptology – EUROCRYPT '88*, volume 330 of *Lecture Notes in Computer Science*, pages 419–453. Springer, 1988.

[15] Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In Ueli M. Maurer, editor, *Advances in Cryptology – EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[16] Jacques Patarin, Louis Goubin, and Nicolas Tadeusz Courtois. SFLASH, a Fast Asymmetric Signature Scheme for Low Cost Smart-Cards. `http://www.nessie.org`.

[17] Lih-Chung Wang, Bo-Yin Yang, Yuh-Hua Hu, and Feipei Lai. A "Medium-Field" Multivariate Public-Key Encryption Scheme. In David Pointcheval, editor, *Topics in Cryptology – CT-RSA 2006*, volume 3860 of *Lecture Notes in Computer Science*, pages 132–149. Springer, 2006.

[18] Christopher Wolf and Bart 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/2005/077`.

Olivier Billet
Orange Labs
38–40 rue du Général Leclerc
F-92794 Issy-les-Moulineaux, France
e-mail: `billet@eurecom.fr`

Jacques Patarin
Université de Versailles
45 avenue des États-Unis
F-78035 Versailles, France
e-mail: `jacques.patarin@uvsq.prism.fr`

Yannick Seurin
Orange Labs
38–40 rue du Général Leclerc
F-92794 Issy-les-Moulineaux, France
e-mail: `yannick.seurin@m4x.org`