Cryptanalysis of the Hidden Matrix Cryptosystem

Jean-Charles Faugère[1], Antoine Joux[2,3], Ludovic Perret[1], and Joana Treger[2]

[1] INRIA, Centre Paris-Rocquencourt, SALSA Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
104, avenue du Président Kennedy
75016 Paris, France
jean-charles.faugere@grobner.org, ludovic.perret@lip6.fr
[2] Université Versailles-Saint Quentin
joana.treger@uvsq.prism.fr
[3] DGA
antoine.joux@m4x.org

Abstract. In this paper, we present an efficient cryptanalysis of the so-called HM cryptosystem which was published at Asiacrypt'1999, and one perturbed version of HM. Until now, this scheme was exempt from cryptanalysis. We first present a distinguisher which uses a differential property of the public key. This distinguisher permits to break one perturbed version of HM. After that, we describe a practical message-recovery attack against HM using Gröbner bases. The attack can be mounted in few hundreds seconds for recommended parameters. It turns out that algebraic systems arising in HM are easier to solve than random systems of the same size. Note that this fact provides another distinguisher for HM. Interestingly enough, we offer an explanation why algebraic systems arising in HM are easy to solve in practice. Briefly, this is due to the apparition of many new linear and quadratic equations during the Gröbner basis computation. More precisely, we provide an upper bound on the maximum degree reached during the Gröbner basis computation (a.k.a. the degree of regularity) of HM systems. For $\mathbb{F}_2$, which is the initial and usual setting of HM, the degree of regularity is upper-bounded by 3. In general, this degree of regularity is upper-bounded by 4. These bounds allow a polynomial-time solving of the system given by the public equations in any case. All in all, we consider that the HM scheme is broken for all practical parameters.

1 Introduction

Multivariate cryptography comprises all the cryptographic schemes that use multivariate polynomials. The use of polynomial systems in cryptography dates back to the mid eighties with the design of C* [16], later followed by many other proposals [19,23,22,14,24,25]. At first glance, many aspects of such systems are

M. Abdalla and P.S.L.M. Barretto (Eds.): LATINCRYPT 2010, LNCS 6212, pp. 241–254, 2010.

tempting for cryptographers. First, basing schemes on the hard problem of solving a system of multivariate equations is very appealing. Indeed, generic algorithms to solve this problem are exponential in the worst case, and solving random system of algebraic equations is also known to be difficult (i.e. exponential) in the average case. Moreover, no quantum algorithm allowing to solve non linear equations exists. Finally, multivariate schemes usually require computations with rather small integers leading to rather efficient smart-card implementations (see for example [5])

Unfortunately, it appears that most multivariate public-key schemes suffer from obvious to less obvious weaknesses ([17,13,9,7] for instance). One reason is that the public-key equations are constructed from a highly structured system of equations. Although the structure is hidden, it can be exploited for instance via differential or Gröbner based techniques. Regarding the intensity of such attacks these last years, it is rather remarkable that the HM cryptosystem [20,21], despite a "special property" pointed out in the original paper, is still standing. In this paper, we use both a property of the differential of the public key and Gröbner basis techniques to attack the HM scheme. The common point between these attacks is that both take advantage on the non-commutativity of the matrices. In particular, we present a message-recovery attack against HM which works on all practical parameters. In addition and in contrast to many cryptanalytic results against multivariate schemes, we are able to theoretically explain why algebraic systems arising in HM are easy to solve in practice.

1.1 Organization of the Paper. Main Results

This paper is organized as follows. In Section 2, we give an introduction on multivariate cryptography and specifically detail the HM construction. In Section 3, we show that the public key equations of HM are distinguishable from a random quadratic system of equations. This property appears by simply considering the differential of the public key. Thanks to this differential, we can mount an attack against a perturbed version of HM [25]. The technique is essentially similar to [10]. Section 4 focuses on the message-recovery. We notice that when applying a Gröbner-based resolution of the system given by the public key, the resolution succeeds for any practical choice of parameters. To illustrate this, we provide experimental results using Gröbner bases, in particular on recommended parameters for HM [20,21]. For instance, our attack can be mounted in few hundreds seconds on previously assumed secure parameters. Besides, we observe that the so-called "degree of regularity", which is the key-parameter for the complexity of Gröbner bases computations, is upper-bounded by 3 when $\mathbb{K} = \mathbb{F}_2$ and 4 otherwise. This allows to obtain a computation in polynomial time in the number of variables. Interestingly enough, we bring elements that help explaining this behavior. Briefly, we show the apparition of many linear and quadratic equations during the Gröbner basis computation. To us, this is very interesting since besides from HFE [18,9,11] multivariate schemes broken by Gröbner based techniques didn't offer such an explanation.

2 Multivariate Cryptology and Hidden Matrix Cryptosystem

A frequently used one-way function in multivariate cryptography is based on the evaluation of a set of algebraic polynomials $\mathbf{p} = \big(p_1(x_1, \ldots, x_N), \ldots, p_m(x_1, \ldots, x_N)\big) \in \mathbb{K}[x_1, \ldots, x_N]^m$, namely:

$$\mathbf{m} = (m_1, \ldots, m_N) \in \mathbb{K}^n \longmapsto \mathbf{p}(\mathbf{m}) = \big(p_1(\mathbf{m}), \ldots, p_m(\mathbf{m})\big) \in \mathbb{K}^m.$$

The mathematical hard problem underlying this one-way function is :

Polynomial System Solving
INSTANCE : **polynomials** $p_1(x_1, \ldots, x_N), \ldots, p_m(x_1, \ldots, x_N)$ **of** $\mathbb{K}[x_1, \ldots, x_N]$**.**
QUESTION : **Does there exists** $(z_1, \ldots, z_N) \in \mathbb{K}^n$ **such that**

$$p_1(z_1, \ldots, z_n) = 0, \ldots, p_m(z_1, \ldots, z_n) = 0$$

To introduce a trapdoor in schemes based on such a one-way function, we start from a carefully chosen algebraic system:

$$\mathbf{f} = (f_1(x_1, \ldots, x_N), \ldots, f_m(x_1, \ldots, x_N)),$$

which is *easy* to solve. That is, for all $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{K}^m$, there is an efficient method for describing or computing the zeroes of $(f_1(x_1, \ldots, x_N) = c_1, \ldots, f_m(x_1, \ldots, x_N) = c_m)$. Then, in order to hide the specific structure of $\mathbf{f}$, we compose it by two linear (or affine) transformations – represented by invertible matrices – $(S, T) \in GL_N(\mathbb{K}) \times GL_m(\mathbb{K})$, to create a seemingly difficult system of public equations:

$$\mathbf{g}(\mathbf{x}) = (g_1(\mathbf{x}), \ldots, g_m(\mathbf{x})) = T\left(f_1(S(\mathbf{x})), \ldots, f_m(S(\mathbf{x}))\right) = T\left(\mathbf{f}(S(\mathbf{x}))\right),$$

with $\mathbf{x} = (x_1, \ldots, x_N)$.
The public key of such systems consists of the polynomials of $\mathbf{g}$, and the secret key is made up of the two matrices (S, T) and sometimes also includes $\mathbf{f}$.
To encrypt a message $\mathbf{m} \in \mathbb{K}^N$, we evaluate $\mathbf{g}$ at m, *i.e.*, we compute:

$$\mathbf{c} = (g_1(\mathbf{m}), \ldots, g_m(\mathbf{m})).$$

To recover the correct plaintext from $\mathbf{c}$, the legitimate recipient uses the bijectivity of the linear transformations combined with the particular structure of the polynomials of $\mathbf{f}$. Namely, he computes a value $\mathbf{m}' \in \mathbb{K}^n$ such that $\mathbf{f}(\mathbf{m}') = T^{-1}(\mathbf{c})$. This can be efficiently done due to the particular choice of $\mathbf{f}$. Finally, he recovers the message by evaluating $\mathbf{m} = S^{-1}(\mathbf{m}')$.

Note that this kind of cryptosystem can also be used to compute signatures. To generate the signature $\mathbf{s} \in \mathbb{K}^m$ of a message $\mathbf{m}$, the decryption process is applied to $\mathbf{m}$. To verify a signature $\mathbf{s} \in \mathbb{K}^m$ of a digest $\mathbf{m} \in \mathbb{K}^m$, one checks whether the equality $\mathbf{g}(\mathbf{s}) = \mathbf{m}$ holds.

There are plenty of proposals [19,23,22,14,24] based on this principle which basically differ in the way of constructing the polynomial $\mathbf{f}$. In particular, the so-called Hidden-Matrix (or HM) cryptosystem, which we consider in the present paper, follows this general paradigm. We now detail the construction of $\mathbf{f}$ in this case.

For the record, the HM scheme is based on the former [C] scheme [12]. It was introduced in [20] to thwart an attack presented in this same paper. As pointed in [20], it is possible to construct bi-linear relations relating any pair (plaintext, ciphertext). In HM, the message $\mathbf{m}$ is a vector of length $N = n^2$ over $\mathbb{K}$. Let $\mathcal{M}_n(\mathbb{K})$ be the set of matrices of size $n \times n$ over $\mathbb{K}$. The set of $m = n^2$ polynomials $\mathbf{f}$ corresponds to the application F over $\mathcal{M}_n(\mathbb{K})$ defined as follows:

$$F : X \mapsto X^2 + M \cdot X,$$

where $M \in \mathcal{M}_n(\mathbb{K})$ is a given constant matrix. The public key $\mathbf{g}$ is as "usual" $T \circ F \circ S$, with $S : \mathbb{K}^{n^2} \to \mathcal{M}_n(\mathbb{K})$ and $T : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}^{n^2}$ two secret invertible affine transformations.

Note that [25] proposes a perturbed [6] version of [C] and HM. The idea is to add randomness in the polynomials of the public key. To do so, we randomly generate a set of m polynomials $\tilde{\mathbf{f}}$ with N variables and a linear transform $\mathbf{R} : \mathbb{K}^N \to \mathbb{K}^r$. The inner polynomial $\tilde{\mathbf{f}}$, constructed as in [C] or HM, is then perturbed by adding $\tilde{\mathbf{f}} \circ R$ to $\mathbf{f}$, i.e. the inner polynomial is now:

$$\mathbf{f} + \tilde{\mathbf{f}} \circ \mathbf{R}.$$

The rank of r must be small to make the image of $\tilde{\mathbf{f}} \circ \mathbf{R}$ sufficiently small. This is a necessary condition for being able to decrypt [25,6].

3 Differential Property of HM, First Distinguisher

In this part, we present a differential property of the HM cryptosystem. This allows us to efficiently distinguish the equations composing the public key of a HM cryptosystem from a random system of quadratic equations. As previously explained (section 2), the inner function of HM is:

$$F : X \in \mathcal{M}_n(\mathbb{K}) \mapsto X^2 + M \cdot X \in \mathcal{M}_n(\mathbb{K}),$$

with M a secret constant matrix of $\mathcal{M}_n(\mathbb{K})$.The differential of a function f is defined by:

$$\mathrm{D}\, f(x, y) = f(x + y) - f(x) - f(y) + f(0).$$

For a fixed x, this expression also defines the differential of f at the point x in the y variable $\mathrm{D}_x f(y)$. Going back to the HM scheme, it follows from this that:

$$\mathrm{D}\, F(X, Y) = X \cdot Y + Y \cdot X. \tag{1}$$

It is interesting to remark that the differential of F is the same as the one of $X \mapsto X^2$ used in [C] ([20,21]). We now arbitrarily fix $X = X_0 \in \mathcal{M}_n(\mathbb{K})$ and consider the following equation in Y:

$$\mathrm{D}_{X_0} F(Y) = X_0 \cdot Y + Y \cdot X_0 = 0. \tag{2}$$

This equations yields n^2 linear equations in the n^2 coefficients of Y. For random linear equations, the expected number of solutions is 1. In our case, the solutions of these linear equations correspond to the matrices that commute with X_0 (here, we assume that the characteristic of $\mathbb{K}$ is two). Indeed, thanks to (1), we find that:

$$\begin{aligned} &\mathrm{D}_{X_0} F(Y) = 0 \\ \Leftrightarrow\ & X_0 \cdot Y \quad\ = Y \cdot X_0. \end{aligned}$$

First of all, any polynomial in X_0 commutes with X_0. For a well-chosen X_0, the dimension of the set of all polynomials in X_0 over $\mathbb{K}$ is n. The exact number of linearly independent matrices that commute with a given matrix can be found in [15], chapter VIII. This number is given by the formula $n_1 + 3n_2 + \cdots + (2t-1)n_t$, where $n_1, \ldots, n_t$ are the degrees of the non constant invariant polynomials. This number is between n and n^2 and about n in most cases. In any case, we can clearly distinguish the set of equations deduced from (2) from a set of random linear equations.

So far, we only considered the inner polynomials of the HM scheme, but the same kind of property propagates throughout the public key $\mathbf{g}$. We consider here, for some fixed vector $\mathbf{x_0}$:

$$\mathrm{D}_{\mathbf{x_0}} \mathbf{g}(\mathbf{y}) = c_0, \tag{3}$$

where $c_0 = T_L(S(0))$, with T_L standing for the linear component of T and c_0 obtained as $\mathrm{D}\,\mathbf{g}(0,0)$ over $\mathbb{F}_2$. Equation (3) then yields:

$$\begin{aligned} \mathrm{D}_{\mathbf{x_0}} \mathbf{g}(\mathbf{y}) = c_0 &\Leftrightarrow T_L\left(S(\mathbf{x_0}) \cdot S(\mathbf{y}) + S(\mathbf{y}) \cdot S(\mathbf{x_0})\right) = 0 \\ &\Leftrightarrow S(\mathbf{x_0}) \cdot S(\mathbf{y}) + S(\mathbf{y}) \cdot S(\mathbf{x_0}) = 0. \end{aligned}$$

S being an invertible application, the same reasoning as for F implies that equation (3) has the same number of solutions than equation (2).

This gives an efficient distinguisher between n^2 random quadratic equations in n^2 unknowns and the quadratic equations composing the public key $\mathbf{g}$ of the HM scheme.

In addition, this permits to attack the perturbed version of [C], which correspond to a HM scheme with a zero matrix M ([25]). We have all the tools to adapt the attack described in [10] on a perturbed version of C*. The attack being very similar, we just outline it. The main goal is to recover the linear space $\mathcal{K}$ that cancels the noise. More precisely, $\mathcal{K}$ is defined as the kernel of the affine space $\mathbf{R} \circ S$. As in [10], it is possible to use a differential distinguisher to detect whether a vector $\mathbf{x}$ is in $\mathcal{K}$ or not. Then, a basis of $\mathcal{K}$ can be found. As explained in [10], once in possession of such a basis, one can cancel the noise and mount an attack as against the basic [C] (i.e. find bilinear relations).

4 Message-Recovery Attack

In this part, we first present experimental results when mounting a Gröbner-based message-recovery attack against HM. As already mentioned, this attack works in practice for (previously assumed) secure parameters of HM. This is due to the fact that systems arising in HM are much easier to solve than random algebraic systems of the same size. In particular, the maximum degree reached during the computation of a Gröbner basis is bounded from above by a small constant (3 or 4). This is supported by experimental and theoretical observations.

4.1 Experimental Results and Observations

We take interest in the message-recovery attack, which consists in recovering a message from a given ciphertext. More precisely, let $\mathbf{c} = \mathbf{g}(\mathbf{m})$ be an encryption of a message $\mathbf{m}$. To directly recover $\mathbf{m}$ from $\mathbf{c}$, we have to solve a quadratic system of equations induced by the polynomials of the public key. Namely, we have to solve the following system of n^2 quadratic equations in n^2 variables:

$$\mathbf{g}(\mathbf{x}) - \mathbf{g}(\mathbf{m}) = 0.$$

Here, we assume that the algebraic system is over $\mathbb{F}_2$, as specified in [20] .

In the following table 2 we quote several experimental results obtained when performing a Gröbner-based message-recovery attack on HM, using the F_4 algorithm available in the Magma Computational Algebra System. These results have been obtained with a Xeon 4.2 Ghz 128 Gb of Ram. The attack have been implemented with Magma (v. 15.7). In the table, we include:

- q: the size of the base field $\mathbb{K}$
- n^2: the number of variables of the system
- T: the total time needed for our attack
- Mem: the maximum memory usage
- $\mathrm{D}_{\mathrm{reg}}$: the maximal degree reached during the Gröbner basis computation.

In the initial paper [12,20,21], the authors advised to take the parameter n such as $n^2 \geq 64$ (which would correspond to $n^2 \geq 80$ nowadays). Hence, the first major observation is that the attack can be mounted in practice. In fact, the scheme is broken for all practical parameters. A second important remark is that

q	n^2	T	Mem	$\mathrm{D}_{\mathrm{reg}}$
2	64	138 s.	1.4 Gb.	3
2	81	685 s.	5.8 Gb.	3
2	100	6249 s.	19 Gb.	3
2	121	6 h.	56 Gb.	3
2	144	26 h.	171 Gb.	3

Fig. 1. Experimental results for the Gröbner-based message-recovery attack over $\mathbb{F}_2$

q	n^2	T	Mem	$\mathrm{D_{reg}}$
65521	25	13 s.	60 Mb.	4
65521	36	790 s.	500 Mb.	4
65521	49	2.7h	3 Gb.	4

Fig. 2. Experimental results for the Gröbner-based message-recovery attack

$\mathrm{D_{reg}}$ is always equal to the same value 3. In the next section, we will explain this systematic behavior. Namely, the maximum degree reached during the Gröbner basis computation is upper-bounded by 3 over $\mathbb{F}_2$. In general ($\mathbb{K} \neq \mathbb{F}_2$), it is bounded by 4. This makes our attack polynomial (in the number of variables).

4.2 Explaining the Degree of Regularity

In this part, we explain the experimental behavior observed in Subsection 4.1. Namely, we explain why the maximum degree reached during a Gröbner basis computation is so low for HM (experimentally bounded by 3 or 4), compared with random algebraic equations. This degree, called *degree of regularity*, is the key parameter for understanding the complexity of Gröbner basis computations Indeed, the complexity of computing a Gröbner basis is polynomial in the degree of regularity D_{reg}, namely the complexity is:

$$\mathcal{O}(N^{\omega D_{\mathrm{reg}}}),$$

which basically correspond to the complexity of reducing a matrix of size $N^{D_{\mathrm{reg}}}$ ($2 < \omega \leq 3$ is the "linear algebra constant", and N the number of variables of the system). The behavior of the degree of regularity D_{reg} is well understood for regular (and semi-regular) systems of equations [1,3,2,4]. On the contrary, as soon as the system has some kind of structure, this degree is much more difficult to predict. In some particular cases, it is however possible to bound the degree of regularity (see the works done on HFE [9,11]). But it is an hard tack in general. We show here that we can predict the apparition of many quadratic or linear polynomials during the computation of a Gröbner basis of the ideal generated by the public equations of HM. This permits to explain why the degree of regularity is bounded from above by 3 over $\mathbb{F}_2$ and 4 otherwise.

To simplify the analysis, it is sufficient to restrict our attention to the equations generated by the "secret" (or inner) polynomials. Indeed, the degree of regularity of an ideal is generically left invariant by any linear change of the coordinates or generators, that is to say, in our case, we can omit S and T and bound the degree of regularity of the ideal generated by the secret polynomials given by F. Let A be a matrix of $\mathcal{M}_n(\mathbb{K})$. We consider the ideal I generated by the inner equations $F(X) - F(A)$:

$$I = \left\langle X^2 + M \cdot X - A^2 - M \cdot A \right\rangle.$$

In the following, we set $B = F(A)$, *i.e.*, $A^2 + M \cdot A = B$. We also define Δ as:

$$\Delta = X^2 + MX - B = 0.$$

The ideal I considered is the ideal generated by all the components of $\Delta_{i,j} = 0,\ 1 \leq i,j \leq n$. Our goal is to explain the bound on the degree of regularity of this ideal.

Case $M = 0$. To give an intuition of the phenomena observed regarding this degree of regularity, let us start with the easy case where $M = 0$ (note that this case corresponds in fact to the $[C]$ scheme broken in [20] in a quite similar way). We have $F(X) = X^2$ and $\Delta = X^2 - B = 0$. Let us consider the two following matrix equations:

$$X \cdot \Delta = X^3 - X \cdot B = 0$$
$$\Delta \cdot X = X^3 - B \cdot X = 0.$$

If we subtract them, we obtain the new equation $X \cdot \Delta - \Delta \cdot X = X \cdot B - B \cdot X = 0$, which provides n^2 linear equations in the $X_{i,j}$ unknowns and allow to solve the system.

Going back to Gröbner bases, these equations would appear when using a Gröbner-based algorithm. Such an algorithm applied on I, starts by generating equations of degree one more (namely 3) from the equations given by $\Delta = 0$. In particular, the equations constituting the matrix equation $X \cdot \Delta = 0$ as well as the ones corresponding to $\Delta \cdot X = 0$ appear. Notice that by reductions, the equations given by $X \cdot \Delta - \Delta \cdot X = 0$ also appear during computation. In other words, after just one step of computation, we get the n^2 linear equations which allow to solve the system.

In the previous case $M = 0$, we proved that many linear equations appear when considering equations of degree 3. In the general case $M \neq 0$, something similar is not necessarily likely to happen. However, we will show that also many new quadratic (and sometimes linear) equations appear when considering equations of degree 3 in the general case.

To generalize the previous observation, we need to introduce the following definition:

Definition 1. *We denote by $I_{\leq d}$ the set of all polynomials of I, of degree less or equal to d.*

During the computation, the polynomials generated are obtained by multiplying previously obtained polynomials by monomials and applying possible reductions. Thus, the degree of the polynomials generated during the computation keeps growing until new low-degree polynomials appear, due to reductions of polynomials of higher total degree. In the case of HM, we rapidly (in the sense that we do not need to generate polynomials of high degree) obtain many low-degree polynomials, which explains that the computation ends quickly. This fact is developed in the following parts.

Field of Arbitrary Characteristic. We show here that plenty of new quadratic equations are generated during the computation of a Gröbner basis of I. This result remains valid whatever the characteristic of $\mathbb{K}$ is. Additional properties occur when $\mathbb{K} = \mathbb{F}_2$, that are given later.

Proposition 1 shows that n^2 quadratic equations are obtained at every new step of the Gröbner basis computation. Moreover, the polynomials generated are obtained by multiplying previously obtained matrix equations of degree 2 by X.

Proposition 1. *For all $k \geq 1$, there exist matrices A_k, B_k, C_k and D_k such that:*

$$P_k = X(M^k + A_k)X + B_k \cdot X + X \cdot C_k + D_k \in I_{\leq 3}.$$

This result is obtained by using the same idea as for the case $M = 0$. Proofs of this proposition is given in appendix A.

In this general case, we experimentally observe that the degree of regularity is bounded by 4, *i.e.*, the Gröbner basis algorithm doesn't need to generate polynomials of degree higher than 4 to terminate.

Case $\mathbb{K} = \mathbb{F}_2$. We now focus on the specific case where $\mathbb{K} = \mathbb{F}_2$, which is the classical setting. In this case, not only we get the quadratic equations of the general case, but we also get additional linear equations, described in the propositions below. Here again, all these equations appear while generating polynomials of degree at most 3 in the Gröbner basis computation.

Proposition 2. *Let $Q_0 = tr((M+I)X) - tr(B)$, tr denoting the trace operator. We have that the equations composing Q_0 are in $I_{\leq 3}$.*

Proposition 3. *Let the notations be as in Proposition 1. For all $k \geq 1$, we define $Q_k = (X + B_k \cdot X + X \cdot C_k + D_k)(M^k + A_k)$. For all $k \geq 1$, the linear equation given by the trace of Q_k, $tr(Q_k)$, is in $I_{\leq 3}$:*

$$tr((X + B_k X + X \cdot C_k + D_k)(M^k + A_k)) \in I_{\leq 3}.$$

The Q_k polynomials are deduced from the P_k. Proofs of these propositions can be found in the appendix A.2.

We experimentally observe that the degree of regularity is only 3 in the case where $\mathbb{K} = \mathbb{F}_2$, which means that these low-degree equations even allow to end the computation after generating polynomials of total degree no higher than 3.

Summary. To summarize, the table below gives the number of low-degree equations generated during the Gröbner basis process and their degree, depending on the different cases studied. The index $k_{\max}$ is the number of steps needed in the F_4/F_5 algorithm[1] to compute $I_{\leq d}$. The value of $k_{\max}$ sometimes dictates the number of low-degree polynomials appearing during the computation. For instance, the polynomials indexed by k described in proposition 3 or proposition 1 are obtained at some step k of the establishment of $I_{\leq d}$. Once again, $\mathrm{D_{reg}}$ stands for the degree of regularity reached. The validity of the results below have been experimentally verified for up to $n^2 = 144$ for $\mathbb{K} = \mathbb{F}_2$ (and $n = 49$ in other cases).

[1] *i.e.*, the $\mathrm{F_4}$ algorithm which uses the $\mathrm{F_5}$ criteria [8].

Case	$M = 0$	$\mathbb{K} = \mathbb{F}_2$	$\mathbb{K} \neq \mathbb{F}_2$
Nb of quadratic eqs	0	$k_{\max} \cdot n^2$	$k_{\max} \cdot n^2$
Nb of linear eqs	n^2	$k_{\max}$	0
Total Nb of quadratic eqs	0	n^3	n^3
Total Nb of linear eqs	n^2	n	0
$\mathrm{D}_{\mathrm{reg}}$	3	3	4

Remark 1. Notice that we assume $k_{\max}$ to be equal to n. Indeed, the equations obtained at step k are related to M^k as explained in the propositions above. Hence, after n steps, the equations obtained may then be related to previous ones since M^n reduces to a combinations of powers of M of lower degree[2]. It is then reasonable to set $k_{\max} = n$. In this case, we obtain many new low-degree equations (as quoted in the second part of the table), which allow to understand why the computation ends quickly, and also the difference with $\mathbb{K} \neq \mathbb{F}_2$, and $\mathbb{K} = \mathbb{F}_2$.

Finally, we have computed for several parameters the theoretical degree $\mathrm{D}_{\mathrm{reg}}^{\mathrm{Theo}}$ of a semi-regular system [1,3,2,4] having the same number of variables and the same number of equations than an instance of HM (but including the new equations generated).

q	n^2	$\mathrm{D}_{\mathrm{reg}}^{\mathrm{Theo}}$
2	64	3
2	81	4
2	100	4
2	121	4
2	144	4
65521	36	4
65521	49	4

This is another indication that the maximum degree reached in HM should be small.

5 Conclusion

In this paper we showed that the Hidden Matrix of [20] is broken. We presented two very efficient distinguishers. The first one is based on solving a system of linear equations deduced from the differential of the public key. The second distinguisher is much stronger since it allows to recover a plaintext from a ciphertext. We observed a very specific behavior during the computation, which we were able to theoretically explain, as for the HFE cryptanalysis [9,11]. Moreover, we derive an attack on the perturbed version of $[C]$ described in [25]. In the original paper [20], the authors did not recommend the use of their scheme, because they suspected not to have noticed some weaknesses; this paper confirms the fears of the authors.

[2] This comes from the Cayley-Hamilton theorem.

References

1. Bardet, M.: Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie. PhD thesis, Université de Paris VI (2004)
2. Bardet, M., Faugère, J.-C., Salvy, B.: Complexity study of Gröbner basis computation. Technical report, INRIA (2002), `http://www.inria.fr/rrrt/rr-5049.html`
3. Bardet, M., Faugère, J.-C., Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proc. International Conference on Polynomial System Solving (ICPSS), pp. 71–75 (2004)
4. Bardet, M., Faugère, J.-C., Salvy, B., Yang, B.-Y.: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry (2005)
5. Bogdanov, A., Eisenbarth, T., Rupp, A., Wolf, C.: Time-area optimized public-key engines: $\mathcal{MQ}$-cryptosystems as replacement for elliptic curves? In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 45–61. Springer, Heidelberg (2008)
6. Ding, J.: A new variant of the matsumoto-imai cryptosystem through perturbation. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 305–318. Springer, Heidelberg (2004)
7. Dubois, V., Fouque, P.-A., Shamir, A., Stern, J.: Practical cryptanalysis of sflash. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 1–12. Springer, Heidelberg (2007)
8. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Mora, T. (ed.) Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation ISSAC, July 2002, pp. 75–83. ACM Press, New York (2002) ISBN: 1-58113-484-3
9. Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
10. Fouque, P.-A., Granboulan, L., Stern, J.: Differential cryptanalysis for multivariate schemes. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 341–353. Springer, Heidelberg (2005)
11. Granboulan, L., Joux, A., Stern, J.: Inverting HFE is quasipolynomial. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 345–356. Springer, Heidelberg (2006)
12. Imai, H., Matsumoto, T.: Algebraic Methods for Constructing Asymmetric Cryptosystems. In: Calmet, J. (ed.) AAECC 1985. LNCS, vol. 229, pp. 108–119. Springer, Heidelberg (1986)
13. Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 257–266. Springer, Heidelberg (1998)
14. Koblitz, N.: Algebraic Aspects of Cryptography. Algorithms and Computation in Mathematics, vol. 3. Springer, Heidelberg (1998)
15. Liddl, R., Niederreiter, H.: Introduction to Finite Fields. Longman Higher Education (1983)
16. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
17. Patarin, J.: Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt'88. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995)

18. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
19. Patarin, J.: The Oil and Vinegar signature scheme. Presented at the Dagstuhl Workshop on Cryptography (1997)
20. Patarin, J., Courtois, N., Goubin, L.: C^*_{-+} and HM: Variations on Two Schemes of T.Matsumoto and H.Imai. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 35–50. Springer, Heidelberg (1998)
21. Patarin, J., Courtois, N., Goubin, L.: C^*_{-+} and HM: Variations on Two Schemes of T.Matsumoto and H.Imai, Extended Version. Available From the Authors (1998)
22. Patarin, J., Courtois, N., Goubin, L.: Quartz, 128-bit long digital signatures. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 282–297. Springer, Heidelberg (2001)
23. Patarin, J., Goubin, L., Courtois, N.: C* − + and hm: Variations around two schemes of t.matsumoto and h.imai. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 35–49. Springer, Heidelberg (1998)
24. Wolf, C., Preneel, B.: Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. Cryptology ePrint Archive, Report 2005/077 (2005), `http://eprint.iacr.org/`
25. Wu, Z., Ding, J., Gower, J.E., Ye, D.F.: Perturbed hidden matrix cryptosystems. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3481, pp. 595–602. Springer, Heidelberg (2005)

A Proofs of the Propositions

This annex gathers the proofs of the propositions of Section 4.2.

A.1 Proofs of the Propositions in the General Case

Lemma 1. *We have the following n^2 quadratic equations in $I_{\leq 3}$:*

$$P_1 = X \cdot M \cdot X + (B + M^2)X - X \cdot B - M \cdot B \in I_{\leq 3}.$$

Proof. Let Δ be as defined in 4.2. The idea is to write $X^2 = B - M \cdot X$. We then remark that there are two ways to obtain X^3, multiplying the previous equation by X on the left or on the right:

$$\begin{aligned} X^3 &= X \cdot B - X \cdot M \cdot X, \\ X^3 &= B \cdot X - M \cdot X^2 \\ &= B \cdot X - M \cdot X^2 + M\Delta \\ &= B \cdot X - M\,(B - M \cdot X) \\ &= B \cdot X - M \cdot B + M^2 \cdot X \end{aligned}$$

By subtracting the two equations we obtain $\Delta \cdot X - X \cdot \Delta - M \cdot \Delta = X \cdot M \cdot X + \left(B + M^2\right) X - X \cdot B - M \cdot B \in I_{\leq 3}$.

It is actually possible to generalize this idea.

Proposition 1. *For all $k \geq 1$ there exist matrices A_k, B_k, C_k and D_k such that:*

$$P_k = X(M^k + A_k)X + B_k \cdot X + X \cdot C_k + D_k \in I_{\leq 3}.$$

Proof. We will proof this result by induction on k. According to lemma 1, the equations induced by P_1 are in $I_{\leq 3}$. Thus, we have:

$$\begin{aligned} A_1 &= 0 \\ B_1 &= B + M^2 \\ C_1 &= -B \\ D_1 &= -M \cdot B. \end{aligned}$$

We suppose that property is true for $P_k, k \geq 1$. It then holds that:

$$\begin{aligned} -P_k \cdot X &= X(M^{k+1} + A_k \cdot M - C_k)X - X(M^k \cdot B + A_k \cdot B) \\ &\quad +(B_k \cdot M - D_k)X - B_k \cdot B \\ &= X(M^{k+1} + A_{k+1})X + B_{k+1} \cdot X + X \cdot C_{k+1} + D_{k+1} \\ &= P_{k+1}, \end{aligned}$$

with the relations:

$$\begin{aligned} D_{k+1} &= -B_k \cdot B \\ A_{k+1} &= A_k \cdot M - C_k \\ C_{k+1} &= -M^k \cdot B - A_k \cdot B \\ B_{k+1} &= B_k \cdot M - D_k. \end{aligned}$$

The equations constituting the components of P_{k+1} are clearly in I_3. This proves the proposition.

A.2 Proofs of the Propositions from the Case $\mathbb{K} = \mathbb{F}_2$

We start by presenting a general lemma on matrices in $\mathcal{M}_n(\mathbb{K})$. Let $D \in \mathcal{M}_n(\mathbb{K})$. In the following, $tr(D)$ stands for the trace of $D \in \mathcal{M}_n(\mathbb{K})$ and C_D for the characteristic polynomial of D. From now on, we always assume that $\mathbb{K} = \mathbb{F}_2$.

Lemma 2. *It holds that $C_D(z) = C_{D^2}(z)$ and $tr(D^2) = tr(D)$.*

Proof. Let $\lambda \in \overline{\mathbb{K}}$ be an eigenvalue of D. That is to say, there exists $u \neq 0$ such that $D \cdot u = \lambda u$. Then we have $D^2 \cdot u = M \cdot \lambda u = \lambda^2 u$. Hence λ^2 is an eigenvalue of D^2. We also denote:

$$\begin{aligned} C_D(z) &= (z - \lambda_1) \cdots (z - \lambda_n) \\ &= z^n + s_1 z^{n-1} + \ldots + s_n, \end{aligned}$$

and

$$\begin{aligned} C_{D^2}(z) &= (z - \lambda_1^2) \ldots (z - \lambda_n^2) \\ &= z^n + \sigma_1 z^{n-1} + \ldots + \sigma_n, \end{aligned}$$

with s_i (resp. σ_i) the i-th elementary symmetric polynomial in λ_i (resp. in λ_i^2). Remark that we have $\sigma_i = s_i^2 = s_i$. Indeed, all these elements are in $\mathbb{F}_2$. This proves the first claim, namely that $C_D(z) = C_{D^2}(z)$.

For the second claim of this lemma, we notice that $tr(D)$ (resp. $tr(D^2)$) is the coefficient of z^{n-1} in $C_D(z)$ (resp. in $C_{D^2}(z)$). As $C_D(z) = C_{D^2}(z)$, the result follows.

From that, we can predict the appearing of new equations during the Gröbner basis computation.

Proposition 2. *Let $Q_0 = (M+I)X - B$. The linear equation $tr(Q_0)$ is in $I_{\leq 3}$.*

Proof. The application tr being a linear form and since $X^2 + M \cdot X = B$, we have $tr(X^2) + tr(M \cdot X) = tr(B)$. Thanks to lemma 2, we have that $tr(X^2) = tr(X)$; which gives the result announced.

More generally:

Lemma 3. *If $Q_1 = X \cdot M + (B + M^2)X \cdot M - X \cdot B \cdot M - M \cdot B \cdot M$, then the linear equation $tr(Q_1)$ is in $I_{\leq 3}$.*

Proof. According to Lemma 1, we know that:

$$P_1 = X \cdot M \cdot X + (B + M^2)X - X \cdot B - M \cdot B \in I_{\leq 3}$$

More precisely, the n^2 equations given by the components of P_1 are in $I_{\leq 3}$). Now, multiplying P_1 by M on the right yields:

$$X \cdot M \cdot X \cdot M + (B + M^2)X \cdot M - X \cdot B \cdot M - M \cdot B \cdot M \in I_{\leq 3} \qquad (\star).$$

Thanks to Lemma 2 on the trace, we have that $tr(X \cdot M \cdot X \cdot M) = tr((X \cdot M)^2) = tr(X \cdot M)$. Thus applying the trace to $(\star)$ implies:

$$tr\left(X \cdot M + (B + M^2)X \cdot M - X \cdot B \cdot M - M \cdot B \cdot M\right) \in I_{\leq 3},$$

as announced.

The preceding result was deduced from the existence of P_1 (Lemma 1). However, it is possible to obtain a similar result for all P_k's of Proposition 1.

Proposition 3. *Let the notations be as in Lemma 1 of Section 4.2. For all $k \geq 1$, we have that:*

$$Q_k = tr((X + B_k X + X \cdot C_k + D_k)(M^k + A_k)) \in I_{\leq 3}.$$

Proof. From Proposition 1, we deduce that for all $k \geq 1$:

$$P_k = X(M^k + A_k)X + B_k \cdot X + X \cdot C_k + D_k \in I_{\leq 3}.$$

By multiplying on the right by $M^k + A_k$, we have:

$$(X(M^k + A_k))^2 + (B_k \cdot X + X \cdot C_k + D_k)(M^k + A_k) \in I_{\leq 3}.$$

Now $tr((X(M^k + A_k))^2) = tr(X(M^k + A_k))$ by lemma 2. Finally, we obtain:

$$tr((X + B_k \cdot X + X \cdot C_k + D_k)(M^k + A_k)) \in I_{\leq 3}.$$