Two-Face: New Public Key Multivariate Schemes

Gilles Macario-Rat[1] and Jacques Patarin[2]

[1] Orange gilles.macariorat@orange.com
[2] Université Versailles Saint-Quentin jpatarin@club-internet.fr

Abstract. We present here new multivariate schemes that can be seen as HFE generalization having a property called 'Two-Face'. Particularly, we present five such families of algorithms named 'Dob', 'Simple Pat', 'General Pat', 'Mac', and 'Super Two-Face'. These families have connections between them, some of them are refinements or generalizations of others. Notably, some of these schemes can be used for public key encryption, and some for public key signature. We introduce also new multivariate quadratic permutations that may have interest beyond cryptography.

Keywords: Multivariate Cryptography, HFE Generalization, new multivariate quadratic permutations (=new DO permutation polynomials).

1 Introduction, The Two-Face Technique

In the search for post-quantum cryptography, multivariate schemes are still interesting options. Plenty of them have been proposed but unfortunately most of them were cryptographically broken, such as the Matsumoto Imai scheme C^* or its variant SFLASH [GM02,FMS08,DDY$^+$09]. However, some of these schemes are still valid such as UOV or HFE with well chosen perturbations [FP09,HBH06]. At present, it seems more difficult to build secure multivariate encryption scheme than multivariate signature schemes. In this paper, we present new families of public key multivariate schemes for encryption or signature, inspired by HFE.

We first recall here a simple description of the HFE scheme. See [Pat96]. As generally in the multivariate schemes, the context is a finite field $\mathbb{F}_q$ (the ground field) and one of its extensions $\mathbb{F}_{q^n}$ of degree n. A natural isomorphism between $\mathbb{F}_q^n$ (or more precisely $\mathbb{F}_q[x]/g(x)$ for any irreducible polynomial g over $\mathbb{F}_q$ of degree n, see [LN96]) and $\mathbb{F}_{q^n}$ allows to consider simultaneously univariate and multivariate versions of polynomials. The starting point of the HFE scheme is an univariate polynomial $P(a)$ over $\mathbb{F}_{q^n}$, having the two following main properties.

(1) Its multivariate version is a set of quadratic multivariate polynomials. This means that its univariate version has the following form.

$$P(a) = \sum_{i,j} \alpha_{i,j} a^{q^i+q^j} + \sum_i \beta_i a^{q^i} + \gamma.$$

Such polynomials are sometimes called (extended) Dembowski-Ostrom polynomials [DO68,DY13]. In this paper we will call them simply 'DO', or will refer to their multivariate counterparts as 'quadratic multivariate' polynomials.

(2) The degree of $P(a)$ in a is small.

From (1), with the help of two more secret affine polynomials S and T, the product $S \circ P \circ T$ is also DO, so it can be publicly output as a set of multivariate quadratic equations. Moreover, some "perturbations" can be applied to this set of equations, in order to increase the security of the HFE obtained. For example, some of the n equations can be kept secret, this is called the perturbation "$-$" (minus). From (2), the solutions in a of the equations $P(a) = b$ can be efficiently computed.

The so called Two-Face technique we present now, can be seen as a generalization of HFE in the sense that the two previously mentioned properties (1) and (2) are held by two different but related polynomials. More generally, we are interested in cases where it is possible to find two equivalent faces of polynomial equations, having the prescribed properties, thereafter described.

Face (1) $E_1(a) = b$ where E_1 is DO. Its role is to allow two additional permutations S and T to hide the inner structure of E_1 into a set of quadratic polynomial equations, multivariate version the composition product $S \circ E_1 \circ T(x) = y$. Unlike in HFE, the degree of E_1 is high.

Face (2) $E_2(a, b) = 0$. Its role is to allow the extraction of solutions in a, since its degree in a is low, even though its degree in b may be high. Conversely, Face 2 is not DO in a and cannot be used to output multivariate quadratic equations.

We will explain later on how E_1 and E_2 are related.

In this article, we will present:

- How to design a multivariate scheme named 'Dob' from the Dobbertin polynomial that resist as far as we know, all known attacks by introducing some "perturbations" in Sec. 2.
- More general "Two-Face" schemes where we use polynomials that are not necessarily permutations, named 'Simple Pat' and 'General Pat', in Sec. 3 and 4.
- Two-Face schemes where we use precisely permutation polynomials, named 'Mac', in Sec. 5.
- Generalization of the 'Two-Face' concept, in Sec. 6.

2 The "Dob" Schemes

2.1 Dobbertin Permutation

This is the original family from which we imagined the Two-face properties. Dobbertin in [Dob99] proved that $P(x) = x^{2^m+1} + x^3 + x$ is a permutation polynomial over $\mathbb{F}_2^n$ for every odd n, where $n = 2m - 1$. The "Two-face" name comes from the fact that from the first equation

$$E_1(x) = x^{2^m+1} + x^3 + x = y, \tag{1}$$

we can get a second one:

$$E_2(x, y) = x^9 + x^6 y + x^5 + x^4 y + x^3 (y^{2^m} + y^2) + xy^2 + y^3 = 0. \tag{2}$$

A proof that we can get (2) from (1) can be obtained by hand easily. Introduce an intermediate variable $z = x^{2^m}$. Use the fact that since $n = 2m - 1$, we get $z^{2^m} = x^{2^{2m}} = x^2$ (implicitly, polynomial computations over $\mathbb{F}_{q^n}$ are done modulo $x^{q^n} - x$). Then eliminate z between the two equations $y = xz + x^3 + x$ and $y^{2^m} = x^2 z + z^3 + z$. This gives $(x^4 + x^2)(x^3 + x + y) + (x^3 + x + y)^3 + x^3 y^{2^m} = 0$ and then (2). We see from (1) that we have a DO polynomial in x. However, its degree in x is high, which makes difficult to solve the equation in x directly. Nevertheless, from (2) it is possible to compute x knowing y, by solving a polynomial equation of degree 9 only.

2.2 Cryptanalysis of the 'nude Dob'

If we used directly (1) into a 'nude Dob' scheme i.e. without any perturbation, we would get a weak scheme, totally broken by Gröbner basis computation. More precisely the degree of regularity obtained in a Gröbner basis attack is always only 3 in the experiments we conducted. (The degree of regularity is the highest degree that must be used in order to the Gröbner basis computation to succeed). The reason is most probably related to the fact that from $E_1(x) = y$, one may derive equations of the kind $E(x, y) = 0$, linear in x, and of small degree in y. We have looked for equations of the kind $\sum \alpha_i x_i + \sum \beta_i y_i + \sum \gamma_{i,j} x_i y_j = 0$ that may be satisfied by the multivariate version of x and y, that is to say the kind of equations 'à la Patarin' (see [Pat00]) used for the cryptanalysis of the Matsumoto-Imai C* scheme. We founded no such equations, nor equations in degree 2 in y, valid for the Dobbertin permutations (more precisely for $n \geq 11$, in fact some of them exist for $n \leq 10$). However, it is more likely that due to the simple form of the Dobbertin permutation, such equations with higher degree in y may exist. In practice, such equations are sufficient to retrieve x from y, since they are linear in x, and this explains why the 'Dob' scheme without perturbation is weak.

However, with adequate perturbations the modified scheme resists so far all the attacks we know. Precisely, we recommend the perturbations $+$, $\oplus$, $-$, ⓥ, described hereafter. They lead to what we call the "Dob" schemes.

2.3 Need for perturbations

HFE is a well studied system. We will call 'nude HFE' the scheme with no perturbations. Today's best attacks on 'nude HFE' are quasi-polynomial. However, with some well chosen modifications, HFE seems much more strong. Similarly for Two-Face that is inspired from HFE, it seems reasonable to recommend a choice of perturbations that aim to thwart known attacks. Here are the main ones we would like to recommend.

"$\oplus$", circle plus Let k be a small integer. Let $v_1, \ldots, v_k$ be k secret linear combinations of $x_1, \ldots, x_n$. This perturbation $\oplus$ adds n secret quadratic combinations of $v_1, \ldots, v_k$ to each variable $y_1, \ldots, y_n$. This can be removed when the secret key is known, by an exhaustive search on $v_1, \ldots, v_k$, at a cost in q^k.

"$+$", plus Let k be a small integer. Let $q_1, \ldots, q_k$ be k secret quadratic combinations of $x_1, \ldots, x_n$. This perturbation $+$ adds n secret linear combinations of $q_1, \ldots, q_k$ to each variable $y_1, \ldots, y_n$. This can be removed when the secret key is known by an exhaustive search on $q_1, \ldots, q_k$, at a cost in q^k.

"$-$", minus This is simply the forgetting operator that removes a small amount of k equations. This perturbation cost almost nothing in signature, but it has a cost in q^k in encryption, this is why it is more often used in signature.

"ⓥ", circle v Let k be a small integer. Let $v_1, \ldots, v_k$ be k secret linear combinations of $x_1, \ldots, x_n$. This perturbation ⓥ turns a multiplicative constant of the variable x in a vector of n random secret linear combinations of the k variables $v_1, \ldots, v_k$. This can be removed when the secret key is known, by an exhaustive search on $v_1, \ldots, v_k$, at a cost in q^k.

Since the introduction of perturbations is critical for the security, these perturbations must be considered as an essential part of the design of the scheme.

2.4 "Dob" Encryption Schemes

For the encryption schemes, we suggest the perturbations $+$ and $\oplus$. Perturbations $+$ and $\oplus$ combined thwart the Minrank attack and attacks against the kernels of the differential equations. See [FGS05,DGS07].

Formally the public polynomial is $Pub = S \circ P \circ T + H \circ R + U \circ L$, where

- R is a set of r random quadratic polynomials in n variables;
- H is a set of n random linear polynomials in r variables;
- L is a set of s random linear polynomials in n variables;
- U is a set of n random quadratic polynomials in s variables.

For encryption of a message x of n bits, compute and publish $y = Pub(x)$. For decryption of a message y of n bits, guess by exhaustive search two vectors p_1 and p_2 of respectively r and s bits. Solve in x the equation $S \circ P \circ T(x) = y - H(p_1) - U(p_2)$. Stop when $R(x) = p_1$ and $L(x) = p_2$.

Example of parameters. For example, the parameters $n = 129$, $r = s = 6$ give a very efficient scheme with a security level of 2^{80}. Decryption costs 2^{12} root computations of a 9 degree polynomial. At present we do not know any specific attack that could defeat it.

2.5 "Dob" Signature Schemes

For the signature schemes, we suggest the perturbation $-$. Formally the public polynomial is $Pub = (S \circ P \circ T)_{n-r}$, where $(.)_{n-r}$ are the first $n-r$ equations. For the signature of a message y of $n-r$ bits, expand the message to n bits in $y*$, solve in x the equation $S \circ P \circ T(x) = y*$, then publish the message and its signature (y, x). For the verification of a signed message (y, x) of $(n-r, n)$ bits, compute and check if $y = Pub(x)$.

We mention that the devastating attack based on a property of the differential of the central polynomial of SFLASH (see [BFM11]) does not apply in our case. Indeed, since the Dobertin polynomial holds 2 quadratic monomials instead of one in the case of SFLASH, then the kernel of the public key has no exploitable expression. For the same reason, the attack based on another property of the differential (searching for multiplications) (see [DFSS07]) is also ineffective in the Dobbertin case.

Example of parameters. The example of parameters $n = 257$, $r = 129$ seems to be a possible implementation for a security level of 2^{128}, and again we do not know any specific attack that could apply.

Remark 1. In this section, we could have considered the polynomial $E_1(x) = x^{2^m+1} + x^3 + ax$ with $a \neq 1$, and then used the perturbation ⓥ on a. However in this case, E_1 is generally not a permutation any more. We have preferred for 'Dob' to use other perturbations and keep the permutation property.

3 The (Simple) Pat Polynomial Family

This is the generic family that can be obtained from any suitable polynomial P using the Two-Face technique and generalizing the 'Dob' family. In this case, the degree n is odd, and as for the 'Dob' family and we note $n = 2m - 1$. The polynomial P has the particular following form.

$$E_1(x) = P(x) = x^{q^m+1} + \sum_{i=0,\ i=q^j,\ i=q^j+q^k}^{i \leq d} \alpha_i x^i. \qquad (1)$$

In other words, we have $P(x) = x^{q^m+1} + Q(x)$, where Q is DO ans its degree is bounded by a small value d. Using the same remark as for the 'Dob' family, we can derive also a second equation by eliminating an intermediate variable $z = x^{q^m}$ between $y = P(x)$ and $y^{q^m} = P(x)^{q^m}$. The elimination gives

$$E_2(x, y) = x^{d+q-1}(y - Q(x)) + \sum_{i=0}^{d} \alpha_i^{q^m} x^{d-i} (y - Q(x))^i - y^{q^m} x^d = 0. \qquad (2)$$

We can also easily see that the degree in x of this equation is bounded by $\max(2d + q - 1, d^2)$.

From this polynomial P of the simple 'Pat' family, we can obviously define in the same way a Two-Face scheme, as with the 'Dob' family, using also the same kind of perturbations. However, since the polynomials of the 'Pat' family are not permutations in general, performance of the secret key is slowed since computation of roots of a polynomial may retrieve several values, up to the degree of the polynomial in theory, a small amount in practise, and so stays attractive. From a security point of view, none of the known attacks apply to the 'Pat' Two-Face schemes, nor the 'Dob' family, which is a special case of the 'Pat' family, however the bijective property of 'Dob' may become the target of future attacks. Therefore, it is good to have some options as backup.

Here are some examples.

Example 1.

$$\begin{aligned} q = 2, \quad d = 5, \quad B(x,z) &= xz + x^5 + x^3 \\ E_1(x) = B(x, x^{q^m}) &= x^{2^m+1} + x^5 + x^3 \\ E_2(x,y) &= x^{25} + x^{23} + x^{20}y + x^{13} + x^9 + x^8y + x^7y^2 + x^6y + x^5y^4 + x^5y^2 \\ &\quad + x^5y^{2^m} + x^3y^4 + x^2y^3 + y^5 \end{aligned}$$

Example 2.

$$\begin{aligned} q = 2, \quad d = 6, \quad B(x,z) &= xz + x^6 + x^5 \\ E_1(x) = B(x, x^{q^m}) &= x^{2^m+1} + x^6 + x^5 \\ E_2(x,y) &= x^{36} + x^{34} + x^{32} + x^{31} + x^{27} + x^{26} + x^{25}y + x^{24}y^2 + x^{21}y + x^{20}y^2 \\ &\quad + x^{13} + x^{12}y^4 + x^{12} + x^{10}y^4 + x^7y^4 + x^7y + x^6y^4 + x^6y^{2^m} + xy^5 + y^6 \end{aligned}$$

The examples above illustrate how E_1 and E_2 seem very different, yet related to the same solutions in x, since precisely, solutions in x of $E_1(x) = y$ are by design solutions of $E_2(x,y) = 0$. The polynomial E_2 has many monomials with various degrees in x, and its multivariate counterpart has therefore a high degree.

Experiments show that random 'Simple Pat' schemes with parameter d have similar regularity degree as random HFE with parameter d^2. We shall investigate in the future if there is a way to increase the degree of regularity.

Experimental Results. See Table 1: 'd2' is the degree in x of E_2, 'dreg' is the degree of regularity, 'deg' is the degree of the HFE polynomial.

4 The (General) Pat Polynomial Families

We generalize one step ahead the previous definition by selecting a polynomial B in two variables over $\mathbb{F}_{q^n}$, say x and z. We choose B to have the special form:

$$B(x,z) = \sum_{i=0,\ i=q^j,\ i=q^j+q^k}^{i \le d} \alpha_i x^i + \sum_{i=q^j,\ i=q^j+q^k}^{i \le d} \beta_i z^i + \sum_{i=q^k,\ j=q^l}^{i+j \le d} \gamma_{i,j} x^i z^j$$

Simple Pat					Original HFE		
d	q	d2	n	dreg	deg	n	dreg
9	2	81	39	4	36	25	4
10	2	100	39	5	36	32	4
12	2	144	23	5	36	41	4
20	2	400	25	5	81	41	4
24	2	576	25	5	128	25	4
32	2	1024	25	5	129	25	5
33	2	1089	25	6	257	25	5
34	2	1156	25	6	513	25	6

Table 1. Comparison 'Simple Pat' vs HFE

That is, we require that B has an extended 'Dembowski-Ostrom' form in two variables, and its total degree is bounded by d. Again we choose an odd degree n and set m such that $n = 2m-1$. Then we define our Face (1) with the polynomial E_1 given by:

$$E_1(x) = B(x, x^{q^m}). \tag{1}$$

Then E_1 is by design DO. The special form of B has been chosen in such a way that we can also mimic the idea of the 'Dob' and simple 'Pat' family; that is introduce on purpose an intermediate variable $z = x^{q^m}$. Therefore we have $y = E_1(x) = B(x, z)$. This gives also $y^{q^m} = B(x, z)^{q^m}$. In this latter, we can replace each occurrence of x^{q^m} by z, and each occurrence of z^{q^m} by x^q. Formally, this is equivalent to replace z by x^{q^m} and x by $z^{q^{m-1}}$. Therefore we get $y^{q^m} = B(z^{q^{m-1}}, x^{q^m})^{q^m}$. Now, the same idea to get a second equation is to eliminate z between those two equations. It becomes difficult to get the result by hand, but the classical tool called 'Resultant' or 'Eliminant' (see [Sal99,GCL92]) does perfectly the job on a computer (see 'Resultant' on 'Magma', [BCP97]). We use the notation Res for 'Resultant'. So our second equation is given by:

$$E_2(x, y) = \operatorname*{Res}_z(B(x, z) - y, B(z^{q^{m-1}}, x^{q^m})^{q^m} - y^{q^m}) = 0. \tag{2}$$

One of the interests of (2) should be that its degree in x is small, otherwise it would be useless. It is possible to estimate this degree. Let us consider one generic monomial $x^i z^j$ of $B(x, z)$, then in $B' = B(z^{q^{m-1}}, x^{q^m})^{q^m}$, it becomes $x^{qj} z^i$. Since the degree of B is bounded by d, then the degree of B' is bounded by qd. The theory of resultants gives us that the degree in x of (2), that is $\mathrm{Res}_z(B(x, z) - y, B'(x, y) - y^{q^m})$, is bounded by qd^2.

Example 1.

$$
\begin{aligned}
&q = 2 \quad d = 3 \quad n = 2m-1\\
&z = x^{2^m} \quad t = y^{2^m}\\
E_1(x) &= B(x,z) = x^3 + xz + z^3\\
E_2(x,y) &= x^{18} + x^{15} + x^{12}y + x^{12}t + x^{11} + x^9 + x^7 + x^6y^2 + x^6t^2 +\\
&x^6t + x^5t + x^4y + x^3y^2 + x^3t^2 + x^3t + y^3 + y^2t + yt^2 + t^3
\end{aligned}
$$

Example 2.

$$
\begin{aligned}
&q = 2 \quad d = 5 \quad n = 2m-1\\
&z = x^{2^m} \quad t = y^{2^m}\\
E_1(x) &= B(x,z) = x^4z + xz + x + z^5\\
E_2(x,y) &= x^{50} + x^{40}t + x^{35} + x^{34}y + x^{34} + x^{33} + x^{32}y + x^{31} + x^{30}y + x^{29} +\\
&x^{28}y + x^{28} + x^{27}y + x^{27} + x^{26}y + x^{26} + x^{25}y + x^{25}t + x^{25} +\\
&x^{24}yt + x^{24}y + x^{24}t + x^{23}t + x^{23} + x^{22}yt + x^{22}y + x^{19}y +\\
&x^{18}y^2 + x^{18}y + x^{18} + x^{17}y + x^{17}t + x^{17} + x^{16}yt + x^{16}y +\\
&x^{15}t^2 + x^{15}t + x^{15} + x^{14}yt^2 + x^{14}yt + x^{14}y + x^{14} + x^{13}y +\\
&x^{13}t^2 + x^{13} + x^{12}yt^2 + x^{11}y^2 + x^{11}y + x^{11}t^2 + x^{11}t +\\
&x^{10}y^4 + x^{10}y^2 + x^{10}yt^2 + x^{10}yt + x^{10}y + x^{10}t^4 + x^{10}t +\\
&x^9t^2 + x^8y^2t + x^8yt^2 + x^8yt + x^8y + x^8t^2 + x^7y^2 +\\
&x^7yt^2 + x^6t^2 + x^6t + x^5yt^2 + x^5t^3 + x^4y^2t + x^4yt^3 +\\
&x^4t + x^3t^3 + x^3 + x^2yt^3 + x^2y + xt + x + y + t^5
\end{aligned}
$$

4.1 Scheme construction

We describe how to construct a Two-Face cryptosystem, using the special families we have just introduced. The first step is the selection of the following parameters: the values of q, n, the polynomial B and two secret affine permutations of $\mathbb{F}_q^n$, S and T. For the perturbations, we can use "$+$", "$\bigoplus$", and "ⓥ" as defined above. Then we have to make public the coordinates of $P = S \circ E_1 \circ T$ over $\mathbb{F}_q$ as quadratic multivariate polynomials. Then as usual, the public key can be used either, given x, to compute y such that $P(x) = y$, or given (x, y), to check that $P(x) = y$. The secret key is used, given y, to compute x such that $P(x) = y$. To do so, one first uses S to translate the problem into the hidden space, then uses E_2 instead of E_1 to find a solution, then uses T to translate the solution back into the public space. One may argue here that E_2 may have several solutions. It is sufficient to consider that the number of solutions is bounded and in practice it is low, and therefore it is possible to enumerate them all and select the suitable one.

4.2 Practical Experiments

See Table 2.

General MacPat					Original HFE		
d	q	deg	n	dreg	deg	n	dreg
9	2	162	25	5	36	25	4
10	2	200	25	5	36	32	4
14	2	200	25	5	36	41	4
16	2	512	25	5	81	41	4
17	2	578	25	6	128	25	4
17	2	578	29	6	129	25	5
17	2	578	31	6	257	25	5
17	2	578	33	6	513	25	6
18	2	648	25	6	1025	32	6
20	2	800	25	6	2049	33	6
30	2	1152	33	6	3072	33	6
50	2	4608	33	7	4097	33	7

Table 2. Comparison 'General Pat' vs HFE

5 The Mac Polynomial Family

This is the generalization of the Dobbertin family, and also the specialization of the general 'Pat' families, to special families for which the corresponding polynomial $P(x)$ is specially a permutation polynomial. For these families, we found that only $q = 2^p$ is possible. Indeed, we point out here that such permutation polynomials families are very sparse and the ones we give here were found by exhaustive search. Here are some examples.

Example 1.

$$\begin{aligned} q = 2 \quad d = 4 \quad n = 2m - 1, \quad n \not\equiv 0 \pmod 3, \text{ and } n \not\equiv 0 \pmod 5 \\ z = x^{2^m} \quad t = y^{2^m} \\ E_1(x) = B(x,z) = x^2z^2 + x^2z + xz \\ E_2(x,y) = x^4y^2 + x^4y + x^4t + x^3y + x^2t + xy + xt + y^2 + t^2 + t \end{aligned}$$

Example 2.

$$\begin{aligned} q = 2 \quad d = 6 \quad n = 2m - 1, \quad n \not\equiv 0 \pmod 7 \\ z = x^{2^m} \quad t = y^{2^m} \\ E_1(x) = B(x,z) = x^4z^2 + x^2z + xz \\ E_2(x,y) = x^8y + x^8t^2 + x^8t + x^7t + x^6y + x^6t + x^5y + x^4y + x^3y^2 + \\ x^3y + x^2y^2 + x^2y + xy + y^4 + y^2 + t \end{aligned}$$

Example 3.

$$\begin{aligned}
q &= 2 \quad d = 8 \quad n = 2m-1, \quad n \not\equiv 0 \pmod{15} \\
z &= x^{2^m} \quad t = y^{2^m} \\
E_1(x) &= B(x,z) = x^4z^4 + x^2z + xz \\
E_2(x,y) &= x^{16}y^4 + x^{16}y + x^{16}t + x^{15}y + x^{14}y^2 + x^{14}y + x^{13}y + x^{12}y^2 + \\
& x^{12}y + x^{11}t + x^{10}y^2 + x^{10}y + x^{10}t + x^9y^2 + x^9t + x^8y + \\
& x^8t + x^7y + x^6t^2 + x^6t + x^4y + x^4t^2 + x^4t + x^3t + x^2y + \\
& x^2t^2 + x^2t + xy + xt^2 + y^2 + t^4 + t
\end{aligned}$$

Example 4.

$$\begin{aligned}
q &= 4 \quad d = 5 \quad n = 2m-1, \quad n \not\equiv 0 \pmod{3} \\
z &= x^{2^m} \quad t = y^{2^m} \\
f &= \text{generator of } \mathbb{F}_4 \\
E_1(x) &= B(x,z) = fx^5 + x^4z + xz^4 + f^2z^5 \\
E_2(x,y) &= x^{100} + f^2x^{97} + x^{80}y + fx^{80}t + fx^{76} + x^{73} + f^2x^{68}y + \\
& x^{68}t + fx^{60}yt + x^{57}yt + f^2x^{54}yt + f^2x^{52} + fx^{51}yt + fx^{49} \\
& + x^{48}yt + f^2x^{45}yt + fx^{42}yt + fx^{40}y^2t + f^2x^{40}yt^2 + \\
& x^{39}yt + f^2x^{36}yt + f^2x^{34}y^2t + x^{34}yt^2 + fx^{33}yt + \\
& f^2x^{32}y + x^{32}t + x^{30}yt + x^{28} + f^2x^{27}yt + f^2x^{25} + \\
& fx^{24}yt + x^{21}yt + x^{20}y^4 + fx^{20}y^3t + f^2x^{20}y^2t^2 + \\
& x^{20}yt^3 + fx^{20}y + fx^{20}t^4 + f^2x^{20}t + f^2x^{18}yt + f^2x^{17}y^4 + \\
& x^{17}y^3t + fx^{17}y^2t^2 + f^2x^{17}yt^3 + x^{17}t^4 + f^2x^{16}y^2t + \\
& x^{16}yt^2 + fx^{15}yt + x^{10}y^2t + fx^{10}yt^2 + f^2x^8y^4 + \\
& x^8y^3t + fx^8y^2t^2 + f^2x^8yt^3 + x^8t^4 + fx^5y^4 + \\
& f^2x^5y^3t + x^5y^2t^2 + fx^5yt^3 + f^2x^5t^4 + y^5 + fy^4t + \\
& fyt^4 + ft^5
\end{aligned}$$

Remark 1. As for the proven case of Dobbertin's polynomial family, in the Mac cases (permutation polynomials), the two faces are equivalent, that is given y, $E_1(x) = y$ and $E_2(x,y) = 0$ have exactly the same solutions in x.

Remark 2. Example 3 present a family of DO permutation polynomials for $q = 4$. This opens the possibility of finding infinite families of DO permutation polynomials over $\mathbb{F}_q$ for $q = 2^p$. This might be of cryptographic interest, since bigger q may give smaller public keys, and of mathematical interest as well.

6 Other Generalizations

6.1 Three or a few more Blocks, 'Super Two-Face'

Taking back the idea of the 'Pat' schemes, let consider that the variable x is 'duplicated' more than twice, a small number of times, three times for instance. We then consider $B(x, z_1, z_2)$ a DO polynomial of small degree, in 3 variables. We can then define $E_1(x) = B(x, x^{q^m}, x^{q^{2m}})$. Let suppose that $n = 3m - 1$. We have then $x^{q^m} \circ x^{q^m} \circ x^{q^m} = x^{q^{3m}} = x^q$. Therefore, by letting $z_1 = x^{q^m}$, $z_2 = z_1^{q^m}$, we have also $x^q = z_2^{q^m}$. Then by eliminating z_1 and z_2 in the following system,

$$
\begin{aligned}
B(x, z_1, z_2) &= y \\
B(z_1^{q^{2m-1}}, z_2^{q^{2m-1}}, x^{q^{2m}})^{q^m} &= y^{q^m} \\
B(z_2^{q^{m-1}}, x^{q^m}, z_1^{q^m})^{q^{2m}} &= y^{q^{2m}}
\end{aligned}
$$

we get similarly $E_2(x, y) = 0$. We call this scheme 'Super Two-Face' as it shows that it can expand the family very largely. By this mean, we also discovered new DO permutation polynomials. Experiments are still undergoing.

6.2 More Blocks

Ultimately, by using a quadratic polynomial $B(x, z_1, \ldots, z_{n-1})$, and the implicit equations $z_1 = x^q$, $z_2 = z_1^q$, $\ldots$, $z_{n-1} = z_{n-2}^q$, $x = z_{n-1}^q$, one can define similarly $E_1(x) = B(x, x^q, x^{q^2}, \ldots, x^{q^{n-1}})$. An open problem is to find possible values of B such that finding E_2 is easy.

7 Conclusion

HFE ([Pat96]) is one of the main multivariate schemes existing nowadays. In the state of the art of cryptanalysis, ([FJ03,BFP11b,BFP11a]) 'nude' HFE (i.e. without perturbation) has a "quasi-polynomial" attack. With addition of well chosen perturbations, HFE seems very efficient (mostly in signature scheme), and no realistic attacks are known. In this article, we have largely widen the family of public-key schemes that can be created from multivariate polynomials close to HFE. For this we have introduced the 'Two-Face' concept, that is, we have split the equation of HFE, into two different but related ones, with separated roles, equations (1) and (2) in this article, which is maybe the most important point in this article, from a cryptographic point of view. This enabled us to design many variants ('Dob', 'Simple Pat', 'General Pat', 'Mac', 'Super Two-Face'...). We have then tested attacks by Gröbner basis computation on these variants. Unfortunately, as for HFE, most of these 'nude Two-Face' variants (without perturbation) show a small regularity degree very similar to the behavior of 'nude HFE'. However, we still have many polynomials to test.

Nevertheless, as for HFE (and some others generalizations like 'Intermediate Field System' [BPS08]) as soon as some appropriate perturbations are added, the regularity degree increases and then Gröbner basis attacks don't work any more.

We have started our study by the Dobbertin permutation polynomial family and our 'Dob' scheme. For cryptographic applications, the permutation property is not required and this led us to our 'Pat' schemes. Surprisingly, we were able to discover easily new DO permutation polynomials and then it led us to the 'Mac' schemes, and it seems that such more polynomials could be easily found. This of course has a mathematical interest per se, since it is quite surprising because the probability that a random DO polynomial is a permutation is very small. It seems that our 'Two-Face' technique gave us a 'gold mine' of DO permutations as their probability is much higher. Moreover, all those new DO permutation polynomials have like the Dobbertin one a generic form which makes them infinite families.

Permutations present also a cryptographic interest, since it speeds up the cryptographic computations, since there is only one root to compute. For example our scheme 'Dob' based on the Dobbertin permutation polynomials seems currently very efficient and resistant to all known attacks as soon as it includes perturbations.

We have also looked at the attacks against the Matsumoto-Imai C^* scheme and its variant SFLASH ([DFSS07,BFM11]) and explain why they can't a priori apply to 'Dob'. In this article we have also suggested some possible realistic parameters for our schemes.

8 Acknowledgements

We thank Ludovic Perret and Jean Charles Faugère, INRIA, for fruitful discussions and help for the experimental computations.

References

[BCHO01] Aart Blokhuis, Robert S. Coulter, Marie Henderson, and Christine M. O'Keefe. Permutations amongst the dembowski-ostrom polynomials. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Applications: Proceedings of The Fifth International Conference on Finite Fields and Applications FQ5, held at the University of Augsburg, Germany, August 2–6, 1999*, pages 37–42, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BDZ04] Feng Bao, Robert H. Deng, and Jianying Zhou, editors. *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*. Springer, 2004.

[BFM11] Charles Bouillaguet, Pierre-Alain Fouque, and Gilles Macario-Rat. Practical key-recovery for all possible parameters of SFLASH. In *ASIACRYPT*, volume 7073 of *Lecture Notes in Computer Science*, pages 667–685. Springer, 2011.

[BFP11a] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. *IACR Cryptology ePrint Archive*, 2011:399, 2011.

[BFP11b] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of multivariate and odd-characteristic HFE variants. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*, pages 441–458. Springer, 2011.

[BPS08] Olivier Billet, Jacques Patarin, and Yannick Seurin. Analysis of intermediate field systems. In *First Conference on Symbolic Computation and Cryptography, Beijing, China, April 28–30 2008*, pages 110–117, 2008.

[Cra05] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.

[DDY$^+$09] Jintai Ding, Vivien Dubois, Bo-Yin Yang, Chia-Hsin Owen Chen, and Chen-Mou Cheng. Could SFLASH be repaired? *IACR Cryptology ePrint Archive*, 2009:596, 2009.

[DFSS07] Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. Practical cryptanalysis of sflash. In *Proceedings of the 27th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO'07, pages 1–12, Berlin, Heidelberg, 2007. Springer-Verlag.

[DGS$^+$05] Jintai Ding, Jason E. Gower, Dieter Schmidt, Christopher Wolf, and Zhijun Yin. Complexity Estimates for the F_4 Attack on the Perturbed Matsumoto-Imai Cryptosystem. In Smart [Sma05], pages 262–277.

[DGS07] Vivien Dubois, Louis Granboulan, and Jacques Stern. Cryptanalysis of HFE with Internal Perturbation. In Okamoto and Wang [OW07], pages 249–265.

[Din04] Jintai Ding. A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. In Bao et al. [BDZ04], pages 305–318.

[DO68] Peter Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103(3):239–258, Jun 1968.

[Dob99] Hans Dobbertin. Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Welch Case. *IEEE Trans. Information Theory*, 45(4):1271–1275, 1999.

[DY13] Jintai Ding and Bo-Yin Yang. Degree of regularity for hfev and hfev-. In *PQCrypto*, volume 7932 of *Lecture Notes in Computer Science*, pages 52–66. Springer, 2013.

[EHZ14] Keita Emura, Goichiro Hanaoka, and Yunlei Zhao, editors. *ASIAPKC'14, Proceedings of the 2nd ACM Wookshop on ASIA Public-Key Cryptography, June 3, 2014, Kyoto, Japan*. ACM, 2014.

[FGS05] Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. Differential Cryptanalysis for Multivariate Schemes. In Cramer [Cra05], pages 341–353.

[FJ03] 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, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.

[FMS08] Pierre-Alain Fouque, Gilles Macario-Rat, and Jacques Stern. Key recovery on hidden monomial multivariate schemes. In Smart [Sma08], pages 19–30.

[FP09] Jean-Charles Faugère and Ludovic Perret. On the security of UOV. *IACR Cryptology ePrint Archive*, 2009:483, 2009.

[GC00] Louis Goubin and Nicolas Courtois. Cryptanalysis of the TTM Cryptosystem. In Okamoto [Oka00], pages 44–57.

[GCL92] Keith O. Geddes, Stephen R. Czapor, and George Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, Norwell, MA, USA, 1992.

[GM02] Henri Gilbert and Marine Minier. Cryptanalysis of SFLASH. In Knudsen [Knu02], pages 288–298.

[HBH06] Omessaad Hamdi, Ammar Bouallegue, and Sami Harari. Hidden field equations cryptosystem performances. In *AICCSA*, pages 308–311. IEEE Computer Society, 2006.

[Hou15] Xiang-dong Hou. Permutation polynomials over finite fields - a survey of recent advances. *Finite Fields Appl.*, 32(C):82–119, March 2015.

[Knu02] Lars R. Knudsen, editor. *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*. Springer, 2002.

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[Mac02] F. S. MacAulay. Some formulæ in elimination. *Proceedings of the London Mathematical Society*, s1-35(1):3–27, 1902.

[Mau96] Ueli M. Maurer, editor. *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*. Springer, 1996.

[Oka00] Tatsuaki Okamoto, editor. *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings*, volume 1976 of *Lecture Notes in Computer Science*. Springer, 2000.

[OW07] Tatsuaki Okamoto and Xiaoyun Wang, editors. *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings*, volume 4450 of *Lecture Notes in Computer Science*. Springer, 2007.

[Pat96] Jacques Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In Maurer [Mau96], pages 33–48.

[Pat00] Jacques Patarin. Cryptanalysis of the matsumoto and imai public key scheme of eurocrypt'98. *Designs, Codes and Cryptography*, 20(2):175–209, Jun 2000.

[PFM14] Jérôme Plût, Pierre-Alain Fouque, and Gilles Macario-Rat. Solving the "isomorphism of polynomials with two secrets" problem for all pairs of quadratic forms. *CoRR*, abs/1406.3163, 2014.

[Sal99] G. Salmon. *Lessons Introductory to the Modern Higher Algebra*. Elibron Classics Series. Adegi Graphics LLC, 1999.

[Sma05] Nigel P. Smart, editor. *Cryptography and Coding, 10th IMA International Conference, Cirencester, UK, December 19-21, 2005, Proceedings*, volume 3796 of *Lecture Notes in Computer Science*. Springer, 2005.

[Sma08] Nigel P. Smart, editor. *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*. Springer, 2008.

[ZT14] Wenbin Zhang and Chik How Tan. A New Perturbed Matsumoto-Imai Signature Scheme. In Emura et al. [EHZ14], pages 43–48.

[ZT15] Wenbin Zhang and Chik How Tan. MI-T-HFE, A New Multivariate Signature Scheme. Cryptology ePrint Archive, Report 2015/890, 2015. http://eprint.iacr.org/2015/890.