Breaking the Symmetry: a Way to Resist the New Differential Attack

Jintai Ding[1], Bo-Yin Yang[2,4], Chen-Mou Cheng[3], Owen Chen[4], and Vivien Dubois[5]

[1] Dept. of Mathematics and Computer Sciences, University of Cincinnati
[2] Institute of Information Sciences, Academia Sinica
[3] Dept. of Electrical Engineering, National Taiwan University
[4] Taiwan Information Security Center
[5] Ecole Normale Superieur

Abstract. SFLASH had recently been broken by Dubois, Stern, Shamir, etc., using a differential attack on the public key. The C^{*-} signature schemes are hence no longer practical. In this paper, we will study the new attack from the point view of symmetry, then (1) present a simple concept (projection) to modify several multivariate schemes to resist the new attacks; (2) demonstrate with practical examples that this simple method could work well; and (3) show that the same discussion of attack-and-defence applies to other big-field multivariates. The speed of encryption schemes is not affected, and we can still have a big-field multivariate signatures resisting the new differential attacks with speeds comparable to SFLASH.

Keywords: multivariate public key cryptography, Matsumoto-Imai, differential, symmetry, projection, fixing

1 Introduction

Late last year the École Normale Supérieure group led by Jacques Stern, along with Adi Shamir, found a way to break all Matsumoto-Imai-minus (or C^{*-}, [15]) cryptosystems [8, 9]. The attack relies on a hidden symmetry of the corresponding public key, which is fundamentally due to the M-I family of cryptosystems being built on the structure of a large field. The associated public keys even of modified systems still contain substantial information that exposes the structure of this large field. This residual field structure is exploited to break the systems. In principle, this means that to secure these systems, one must break the hidden field structure of the field. This is our main idea, expanded below.

1.1 Questions

The SFLASH signature scheme ([3]), one of the best-known multivariate cryptosystems, had stood for a decade and was even recommended by the New European Schemes for Signatures, Integrity, and Encryption (NESSIE, [13]) as a signature scheme for constrained environments. However, this scheme and all related C^{*-} schemes had recently been broken by Dubois, Stern, Shamir, etc.

Due to this new and ingenious application of the differential attack, it seems that the family of C^{*-} and related signature schemes, are no longer of any practical value. It seems then reasonable to wonder whether similar big-field multivariate schemes have the same or a related weakness, and are such multivariate cryptosystem is worth exploring further.

Also another obvious question is: will countermeasures to protect against the new differential attacks make the schemes too slow, in which case (given that one of the rationales for using multivariates is efficiency) the cure may well be worse than the disease.

1.2 Conclusions

We show that the simple multiplicative symmetry that is used by the new attack is vital, and therefore we can protect against these new attacks and make the new attack invalid by breaking the symmetry. The simple trick that we use is called in mathematics a projection map. In practical terms, we take a set of public keys and fix one of the component variables to be zero. This does not affect the speed of encryption schemes but slows down signature schemes by a fairly significant amount. We will argue why the symmetry is broken and we will show with computer experiments that this is indeed so. Furthermore, since variants of C^*, such as ℓIC [7], can be very fast, it is possible to do a moderate amount of guessing. Given that, we show that although a similar weakness is found in all similar big-field schemes, we can have a fix with essentially the same speeds for encryption and acceptable speeds in a big-field multivariate signature scheme (of the embedded minus type).

1.3 A Note on Previous and Future Work

Part of the catch-22 facing multivariate systems is that not enough effort has been spent to make them better. Therefore, despite their uncertain futures, it still seems like a good idea to work on optimizing multivariate cryptosystems more as in [2], and especially for embedded systems.

The idea of using projection as a modifier was mentioned first by Courtois [5, 16] and termed "fixing" but was not seriously considered as a defensive measure.

The concept of compounding several modifiers is not new and can be seen for example in QUARTZ [4] (HFE, with vinegar variables and minus).

It seems that the new differential attacks increased greatly our understanding of multivariate PKCs, and one should be more confident about MPKCs and not be too quickly dismissive of further adventures in this area.

2 Matsumoto-Imai-Minus and SFLASH

We describe briefly the Matsumoto-Imai multivariate public-key cryptosystem and its major variant, the Matsumoto-Imai-Minus signature scheme (C^{*-}).

Multivariate PKCs provides an alternative for which CPUs that don't have fast operations with large integers can do equally well. In the last ten years, there has been significant effort put into realizing practical implementations. One instance, SFLASH version 2, was even recommended by NESSIE [1, 13].

2.1 The original Matsumoto-Imai

Let $\mathbb{E}$ be a finite field of size q and characteristic 2, and fix an irreducible polynomial of $g(t) \in k[t]$ of degree n. Then $\mathbb{F} = \mathbb{E}[t]/(g(t))$ is an extension of degree n over $\mathbb{E}$, and we have an isomorphism $\phi : \mathbb{F} \longrightarrow \mathbb{E}^n$ defined by $\phi(a_0+a_1t\cdots+a_{n-1}t^{n-1}) = (a_0, \ldots, a_{n-1})$. Fix α so that $\gcd(1+q^\alpha, q^n-1) = 1$ and define $F : \mathbb{F} \longrightarrow \mathbb{F}$ by

$$F(X) = X^{1+q^\alpha}.$$

Then F is invertible and $F^{-1}(X) = X^t$, where $t(1+q^\alpha) \equiv 1 \bmod (q^n-1)$. Define the map $\tilde{F} : \mathbb{E}^n \longrightarrow \mathbb{E}^n$ by $\tilde{F}(x_1, \ldots, x_n) = \phi \circ F \circ \phi^{-1}(x_1, \ldots, x_n) = (\tilde{F}_1, \ldots, \tilde{F}_n)$. In this case, the $\tilde{F}_i(x_1, \ldots, x_n)$ are quadratic polynomials in the variables $x = (x_1, \ldots, x_n)$. Finally, let L_1 and L_3 be two randomly chosen invertible affine linear maps over $\mathbb{E}^n$ and define $\bar{F} : \mathbb{E}^n \longrightarrow \mathbb{E}^n$ by

$$P(x_1, \ldots, x_n) = L_3 \circ \tilde{F} \circ L_1\,(x_1, \ldots, x_n) = (P_1, \ldots, P_n).$$

The public keys of a Matsumoto-Imai cryptosystem (referred to as C^* or MI) consists of the polynomials $P_i(x_1, \ldots, x_n)$. See [12] for more details.

2.2 Matsumoto-Imai-Minus

It is well-known since [14] that C^* is susceptible to the linearization equations attack. To counter this, one can make a new signature scheme using the minus method. Fix a integer r. In this case, the public key P^- is given as:

$$P^- = (P_1, \ldots, P_{n-r}).$$

Namely drop a few components. SFLASH is one C^{*-} cryptosystem, where $q = 2^7$ and $n = 37, \theta = 11, r = 11$ (ver. 2) or $n = 67, \theta = 33, r = 11$ (ver. 3).

3 The Symmetry in M-I and SFLASH

It is often said that the security of an MPKC (multivariate public-key cryptosystem) depends on the difficulty of solving multivariate quadratic systems (MQ problem). But since all MPKC public keys have the form $\phi_3 \circ \phi_2 \circ \phi_1$, where ϕ_1 and ϕ_3 are linear or affine, we can try to distill these linear mappings (extended isomorphism of polynomials or EIP problem) instead of trying to solve the systems. These kind of attacks are referred to as structural. Of course, the lines are a little blurry at times: The bilinear (Patarin) relations attack looks structural, but it can be considered a special situation for the $\mathbf{F_4}$ algorithm.

Structural attack on MPKC are of two related types:

Invariants: invariants (mostly, subspaces) that can be guessed.
Symmetries: transformations that leave certain quantities unchanged and hence can be computed by a system of equations.

Of course, these two are related, given that invariants are defined according to symmetry. Previous designers sometimes neglected the importance of symmetry. In this section we present the symmetry or invariants used in the new differential attacks on the M-I family of cryptosystems.

3.1 The Skew Symmetric Transformation

The symmetry found by Stern etc. can be explained by considering the case of C^* cryptosystem. We will first look at the the differential of the central map F. We define the differential of any map G, denoted $DG(a,x)$, formally as follows:

$$DG(a,x) := G(x+a) - G(x) - G(a) + G(0).$$

Clearly regardless of G, $DG(a,x)$ is bilinear and symmetric in a and x.

The first new attack [9] is to use the so-called skew-symmetric maps with respect to this bilinear function, namely, the linear maps M such that

$$DP^{-}(a, M(x)) + DP^{-}(M(a), x) = 0$$

The reason that this works is that the central map $\tilde{F}$ and the public key, which encapsulates the vital information in the central map, unfortunately has very strong symmetry in the sense that all the differentials from these maps share some common nontrivial skew-symmetric map M. Since

$$F(x) = x^{1+q^{\alpha}},$$

its differential is

$$DF(a,x) = a^{q^{\alpha}}x + ax^{q^{\alpha}}.$$

It was pointed out in [9] that the skew-symmetric maps M with respect to this $DF(a,x)$ are precisely the linear maps induced from the multiplication by some element ζ satisfying the condition

$$\zeta^{q^{\alpha}} + \zeta = 0.$$

It can be seen that this skew-symmetry will continue to hold even when we discard some components of F. In terms of the public key, this means that if we write

$$DP(a,x) := (a^T M_1 x,\, a^T M_2 x, \ldots,\, a^T M_n x)$$

and try to solve $M^T M_i + M_i M = 0$ for all $i = 1 \cdots n$ simultaneously, we should find just k-multiples of the identity if n and α are coprime, and a d-dimensional subspace in the space of linear maps if $d = \gcd(n, \alpha) > 1$.

For a randomly chosen map F, it is clear that only trivial solutions $M = u1_n$, where $u \in \mathbb{E}$ are expected to satisfy this condition. This means that there is a very strong condition on C^{*-} cryptosystems. This symmetry can be utilized to break C^{*-} systems for which $d = \gcd(n, \alpha) > 1$.

3.2 The Multiplicative Symmetry

We call the second symmetry the multiplicative symmetry, which again comes from the differential $DF(a,x)$. Let ζ be an element in the big field $\mathbb{F}$. Then we have

$$DF(\zeta \cdot a, x) + DF(a, \zeta \cdot x) = (\zeta^{q^\alpha} + \zeta) DF(a, x).$$

This is also a very strong symmetry, namely it implies that if

$$M_\zeta = L_1^{-1} \circ \phi \circ (X \mapsto \zeta X) \circ \phi^{-1} \circ L_1$$

is the linear map in $\mathbb{E}^n$ corresponding to multiplication by ζ, then

$$\mathrm{span}\{M_\zeta^T M_i + M_i M_\zeta : i = 1 \cdots n\} = \mathrm{span}\{M_i : i = 1 \cdots n\}.$$

I.e., the space spanned by the quadratic polynomials from the central map is invariant under the skew-symmetric action as defined above.

Clearly the public key of C^{*-} inherits some of that symmetry. Now not every skew-symmetric action by a matrix M_ζ that corresponds to an $\mathbb{F}$-multiplication that result in $M_\zeta^T M_i + M_i M_\zeta$ being in the span of the public-key differential matrices, because $S := \mathrm{span}\{M_i : i = 1 \cdots n - r\}$ as compared to $\mathrm{span}\{M_i : i = 1 \cdots n\}$ is missing r of the basis matrices. However, as the authors of [8] argued heuristically and backed up with empirical evidence, if we just pick the first three $M_\zeta^T M_i + M_i M_\zeta$ matrices, or any three random linear combinations of the form $\sum_{i=1}^{n-r} b_i (M_\zeta^T M_i + M_i M_\zeta)$ and demand that they fall in S, then

1. there is a good chance to find a nontrivial M_ζ satisfying that requirement;
2. this matrix really correspond to a multiplication by ζ in $\mathbb{F}$;
3. applying the skew-symmetric action of this M_ζ to the public-key matrices leads to other matrices in $\mathrm{span}\{M_i : i = 1 \cdots n\}$ that is not in S.

Why *three*? There are $n(n-1)/2$ degrees of freedom in the M_i, so to form a span of $n-r$ matrices takes $n(n-3)/2+r$ linear relations among its components ($n-r$ and not n because if we are attacking C^{*-}, we are missing r components of the public key). There are n^2 degrees of freedom in an $n \times n$ matrix U. So, if we take a random public key, it is always possible to find a U such that

$$U^T M_1 + M_1 U,\, U^T M_2 + M_2 U \in S = \mathrm{span}\{M_i : i = 1 \cdots n - r\},$$

provided that $3n > 2r$. However, if we ask that

$$U^T M_1 + M_1 U,\, U^T M_2 + M_2 U,\, U^T M_3 + M_3 U \in S,$$

there are many more conditions than degrees of freedom, hence it is unlikely to find a nontrivial solution for truly random M_i. Conversely, for a set of public keys from C^*, the result of tests in [8] shows that it is almost sure for this attack eventually to recover the missing r equations and break the scheme.

4 Fixing the Schemes by Breaking the Symmetry

It looks obvious, after looking at Sections 3 and 4.4 that the the attack of Dubois *et al* is tied to the symmetries in Section 3.1 and 3.2, and in trying to defend against the attacks, one must modify the central map in such a way that the symmetries in Section 3.1 and 3.2 are no longer present.

4.1 Projection: Eliminating One Variable

The idea we propose has been mentioned before under the name "fixing" [5, 16], but in reality it means a projection onto an affine or linear subspace (usually a hyperplane) that eliminates one independent variable from the public key.

Intuitively, we can say that the differential attacks actually utilize the field structure of the big field to break SFLASH and related cryptosystems, and the reason why projection could work against these attacks is that the subspace where we project into can not possibly inherit any field structure from the big space as we all know. This conceptually explains why the idea of projection should work against the differential attack, which relies solely on the field structure. Projection destroys the original field structure.

In terms of an original cryptosystem which starts with the public map of $P := (P_1(x_1, x_2, \ldots, x_n),\, P_2(x_1, x_2, \ldots, x_n),\, \ldots, P_m(x_1, \ldots, x_n)))$, the public map of the singly projected (or fixed) system is

$$P' := (P_1(x_1, \ldots,\, x_{n-1},\, 0),\, P_2(x_1, \ldots,\, x_{n-1},\, 0),\, \ldots, P_m(x_1, \ldots,\, x_{n-1},\, 0)))$$

How does projection or fixing affect the operation of the scheme?

Digital Signature Scheme: for multivariate signature schemes, typically one start with the m-block (each block in $\mathbb{E} = \mathrm{GF}(q)$) long hash and add $n - m$ blocks of random numbers in the staged process of inverting the public map. With projected (fixated) public keys, whenever the final result doesn't have a 0 in the appropriate position, we have to discard the result and redo the signing. So one projected coordinate makes it q times slower.

Encryption Scheme: Here we start with $n - 1$ blocks of plaintext instead of n, but neither the encryption nor the decryption is affected.

Before we rush to implement idea, we need to verify that this is in fact a good thing that defends against the differential attack, as below.

Note also that for simplicity we are fixing to zero. Suppose we fix x_n to the value b. If L_1 is affine and has non-linear parts, then we can just shift L_1 by the constant b instead. If L_1 (as is likely L_3 also) is linear, we can infer that this is only for homogeneous central maps [11], in which case we can homogenize and read off the original public key.

4.2 Projection Breaks the Skew-Symmetry in C^*

Let us assume that $f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)$ are the quadratic polynomial derived in the central map of the C^*. Here we do not have any linear map composed on either the left or the right side.

Let $g_1(x_1, \ldots, x_{n-1}), \ldots, g_n(x_1, \ldots, x_{n-1})$ be quadratic polynomial obtained on substituting $x_n := \sum_1^{n-1} a_i x_i$, a random linear functions of $x_i, i = 1, ..., n-1$:

$$g_i(x_1, ..., x_{n-1}) = f_i(x_1, ..., x_{n-1}, \sum_1^{n-1} a_i x_i).$$

Let the space spanned by the g_i be G. We need to pick random elements $G_i = \sum a_{ij} g_i$ from G. For each G_i, we can associate an unique symmetric $(n-1) \times (n-1)$ matrix M_i whose diagonal entries are zero.

The skew symmetry of G_i are given by the invertible matrix M such that

$$MM_i = M_i M^T.$$

For any fixed M_i, this is a linear system of equations in the coefficients of M.

We need to show that for randomly chosen M_1 and M_2, the intersection of the solutions $MM_1 = M_1 M^t, MM_2 = M_2 M$, behaves just as if M_1 and M_2 are randomly chosen symmetric matrix with zero diagonal entries. What we can do is to find the dimension of the space of the solutions for the set of equations above, when M_i are from G_i, and when M_i are randomly chosen.

Furthermore, we need to show that if we choose three polynomials from G, say G_1, G_2 and G_3, the common skew symmetry or say the set of the equations:

$$MM_1 = M_1 M^t, MM_2 = M_2 M, MM_3 = M_3 M,$$

have only the trivial solution $M = a1$, where $1 = 1_n$ is the identity matrix.

n	α	s	#	W	H	AR	RR	n	α	s	#	W	H	AR	RR	n	α	s	#	W	H	AR	RR
37	11	0	2	1369	1332	1332	1332	38	10	0	2	1444	1406	1386	1387	39	11	0	2	1521	1482	1482	1482
			3		1998	1368	1368				3		2109	1442	1443				3		2223	1520	1520
			4		2664	1368	1368				4		2812	1442	1443				4		2964	1520	1520
		1	2	1296	1260	1242	1242			1	2	1369	1332	1332	1332			1	2	1444	1406	1387	1387
			3		1890	1295	1295				3		1998	1368	1368				3		2109	1443	1443
			4		2520	1295	1295				4		2664	1368	1368				4		2812	1443	1443
		2	2	1225	1190	1190	1190			2	2	1296	1260	1242	1242			2	2	1369	1332	1332	1332
			3		1785	1224	1224				3		1890	1295	1295				3		1998	1368	1368
			4		2380	1224	1224				4		2520	1295	1295				4		2664	1368	1368

Table 1. Example Tests in $\mathrm{GF}(256)^{37}$

Let $h_1(x_1, \ldots, x_{n-2}), \ldots, h_n(x_1, \ldots, x_{n-2})$ be the quadratic polynomial derived from substituting $x_{n-1} = \sum_1^{n-2} b_i x_i$, another random linear function:

$$g_i(x_1, \ldots, x_{n-1}) = f_i(x_1, \ldots, x_{n-1}, \sum_1^{n-1} b_i x_i).$$

Let the space spanned by h_i be called H. Repeat the tests for H.

We ran tests for many n, s (the number of fixed variables), and α, and $q = 2^4, 2^7, 2^8$. Tab. 1 above are three cases that involves 37 variables in GF(256). Here W and H are the height and width of the matrices that we are checking. AR is the rank we find from the matrices associated with a C^{*-} system, and RR is the rank we find after we repeat the same test with random matrices. When $s = 0$ and $d = \gcd(n, \alpha) > 1$ do we observe a difference in the dimension of the intersection of 3 or more matrices between associated matrices of C^* and random. Otherwise we don't. The reader can verify this with MAGMA or Maple.

n	α	s	#	W	H	AR	RR
44	12	0	2	1936	1892	1820	1870
			3		2838	1932	1935
			4		3784	1932	1935
		1	2	1849	1806	1760	1806
			3		2709	1848	1848
			4		3612	1848	1848
		2	2	1764	1722	1701	1701
			3		2583	1763	1763
			4		3444	1763	1763

Table 2. Other Example Tests over GF(256)

Here is another examples (in Table 2) for a different combination of parameters, checking the same thing.

4.3 Other Experiments

With the same basic notations as above, let $Df_i(A, X)$, $Dg_i(A_1, X_1)$, $Dh_i(A_2, X_2)$ be the differentials of f_i, g_i and h_i, where $A = (a_1, \ldots, a_n)$, $X = (x_1, \ldots, x_n)$, $A_1 = (a_1, \ldots, a_{n-1})$, $X_1 = (x_1, \ldots, x_{n-1})$, $A_2 = (a_1, \ldots, a_{n-2})$, $X_2 = (x_1, \ldots, x_{n-2})$.

Let the space spanned by the Dg_i be DG, and U be a *random indeterminate* linear transformation on $\mathbb{E}^{n-1}$. Let the space spanned by the Ug_i be UG,

$$Ug_i(A_1, X_1) = Dg_i(U(A_1), X_1) + Dg_i(A_1, U(X_1)).$$

We need to show that the intersection of UG and DG is very small except when U is a multiple of the identity map, but this is too hard. Instead, we randomly choose coefficients and take three linear combinations of the Ug_i. Demand that they are in the span of DG and solve for the components of U.

Let the space spanned by Dh_i called DH, V be a linear transformation on the space of $n-2$ dimension. Let

$$Vh_i(A_2, X_2) = Dh_i(V(A_2), X_2) + Dh_i(A_2, V(X_2)).$$

Let the space spanned by the Vh_i be VH. Repeat test for VH and DH.

We tested many cases and the behavior is consistent. Except when $s = 0$, for any three matrices Ug_i, the solution space that they are

simultaneously in $\operatorname{span} UG$ **is of dimension 1, and we know that is the trivial solution — the multiples of the identity map.**

The same tests as in Sec. 4.2 are also run for $3IC$, except that we ensured the linear map chosen not to intersect with the k-dimensional subspaces corresponding to the bigger field variables X_1, X_2, X_3. *Same results.*

Though we can not yet prove in theory that projections completely destroy the symmetries utilized in the differential attack, the experiments above clearly show that it is indeed so.

4.4 Similar Effects on Some Other Big-Field MPKCs

The basic trapdoor ℓIC (ℓ-invertible cycles, [7]) can be considered an extension of C^*. In the same manner as above, an ℓIC- signature scheme can be attacked. We will describe the example of $3IC$, the signature scheme $3IC^-$ and the attack briefly as follows: follows: Take the field $\mathbb{E} = \mathrm{GF}(q)$, $\mathbb{F} \cong \mathbb{E}^k$. The central map is $F : \mathbb{F}^3 \to \mathbb{F}^3$, $F(X_1, X_2, X_3) = (X_1X_2, X_2X_3, X_2X_3)$ expressed as a map $\tilde{F} : \mathbb{E}^{3k} \to \mathbb{E}^{3k}$. The inversion from (Y_1, Y_2, Y_3) is $X_1 = \sqrt{Y_1Y_2/Y_3}$, $X_2 = Y_1/X_1$, $X_3 = Y_2/X_1$. There are singularities at any of the $Y_i = 0$.

We put an invertible linear map L_1 and L_3 on either side to make the public key P. Since $3IC$ clearly is susceptible to the same kind of linearization attacks, we do $3IC^-$. I.e., we remove k of the $n = 3k$ public polynomials.

A similar symmetry exists in this trapdoor just as in C^*. If M_ζ corresponds to the linear map $(X_1, X_2, X_3) \mapsto (\zeta_1X_1, \zeta_2X_2, \zeta_3X_3)$, then we have $DP(M_\zeta x, a) + DP(x, M_\zeta a) = 0$. So we should be able break $3IC^-$ in the same way as in [9].

We have only considered signature schemes so far. We can consider encryption schemes, represented by Perturbed Matsumoto-Imai Plus. In this system, we have $q = 2$, and a central map of $G = (\tilde{F} + Q \circ R, R') : \mathbb{F} = \mathrm{GF}(2)^n \to \mathrm{GF}(2)^{n+c}$, where R is a random linear map of $\mathbb{F} \to (\mathrm{GF}(2))^r$ and Q is a random quadratic. Then we affix a random quadratics $R' : \mathbb{F} \to (\mathrm{GF}(2))^c$. In the original differential attacks of [10], a distinguisher is constructed that identifies a differential $DF(x, a)$ as corresponding to $L_1(a) \in \ker R$. The extra random quadratics defend against this. Since $q = 2$, embedding or projection in one variable only loses a bit from the input, loses no speed, and prevents any use of the symmetries as described in Sec. 3.2 and Section 3.1, we would suggest to do it on general principles regardless.

5 Some Tests of the New Schemes

Having affirmed that the projection (fixing) defends against the symmetry attacks, we will present new schemes by applying the projection method to the related known schemes SFLASH, $3IC^-$ and PMI+.

When we apply the projection method to a signature scheme, we need to do a search of the size of the lost dimension in the signing process, which will slow down the signing speed. Therefore, we prefer, in this case, to do a projection that we will lower the dimension by 1. In the case of encryption schemes, we do not have such a problem at all, so we in general propose to do a projection that we will lower the dimension by 2 or more.

5.1 Projected FLASH, GF(16)

SFLASH is about 30 or so times faster in signing than RSA-1024 on 32-bit x86. After we apply the projection, we have to guess 128 times, which will make the signing speed 128 times of the original signing speed, which is too slow.

We switch to GF(16) with the FLASH scheme. A rush implementation with $r = 22$, $n = 74$, and $s = 1$ is still faster than RSA-1024. For example, with $n = 73$, $m = 52$, $q = 16$, we can do one 292-bit signature of a 208-bit digest in around 70ms on our ancient 500MHz Pentium III, while RSA takes 84ms. The drawbacks? Key size is doubled, with a 30kB public key and 4.8kB private key.

5.2 Projected $3IC^-$, GF(256)

The first attempt is to take $3IC^-$ with $k = r = 12$, $q = 256$, $s = 1$ for $3IC^-$. We have $n = 35$, $m = 24$, public key 14kB, private key 2.6kB, signature length 280 bits, hash size 224 bits.

We can choose to implement the multiplication as log-exp tables or a big multiplication table of 64kB. We choose the latter as being more all-around suitable. Signing speed is about 25ms on the Pentium III 500MHz, a few times faster than RSA-1024 (log-exp tables time at around 20ms). On an Opteron 2.2GHz, signing takes about 2.8ms, again significantly faster than RSA-1024.

5.3 Projected $3IC^-$, GF(16)

We come up with the idea that we will use a base field of GF(16). L_1 and L_3 will be implemented in GF(16), but the central map is unchanged. Instead of logarithms and exponentials, we will always implement the scheme using a 64kB multiplication table (which for modern day processors with large cache is tolerable) of GF(256), because the initial 4kB of this table can double as a 2-way SIMD multiplication table for GF(16) if we choose an encoding of GF(256) in a byte as (low nybble) + (high nybble) t, where t is the extension element in $\mathrm{GF}(256) \cong \mathrm{GF}(16)[t]/(\text{irreducible polynomial})$.

With this setup, we have $n = 71$, $m = 48$, public key 28kB, private key 5.2kB, signature length 284 bites, hash size 224 bits. Each signing action takes about 2.6ms on a P3/500, and 0.36ms on an Opteron 2.2GHz.

We may choose to project away another variable (to be really safe), in which case it takes about 40ms and 5.9ms respectively on the P3 and the Opteron, a speed comparable to the original SFLASH scheme.

5.4 P^3MI – Projected Perturbed Plus Matsumoto-Imai

PMI+ [6] is a family of multivariate encryption cryptosystems, which come from applying the plus modification and internal perturbation to the MI cryptosystems. As a variant of the MI cryptosystem, which can also been seen as a MI plus and minus system, it is evident that the new differential attack can also be applied to attack it, though the complexity will be much higher due to the need to do a search. We propose to apply the projection method to the PMI+ cryptosystem, which we will call the Projected Perturbed Plus Matsumoto-Imai or P^3MI.

In this case, we specify that we will project the cryptosystem to a subspace of two dimension lower, or more precisely we will specify two bits of the input to be 0. The speed of the new cryptosystems will be identical to the original PMI+. In this case, as we argue above, there cannot be a differential attack based on symmetry.

References

1. M.-L. Akkar, N. T. Courtois, R. Duteuil, and L. Goubin. A fast and secure implementation of SFlash. In *Public Key Cryptography — PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 267–278. Y. Desmedt, editor, Springer, 2002.
2. C. Berbain, O. Billet, and H. Gilbert. Efficient implementations of multivariate quadratic systems. In *Proc. SAC 2006*. Springer, in press, dated 2006-09-15.
3. N. Courtois, L. Goubin, and J. Patarin. *Quartz: Primitive specification (second revised version)*, Oct. 2001. https://www.cosic.esat.kuleuven.be/nessie Submissions, Quartz, 18 pages.
4. N. Courtois, L. Goubin, and J. Patarin. *Quartz: Primitive specification (second revised version)*, Oct. 2001. https://www.cosic.esat.kuleuven.be/nessie Submissions, Quartz, 18 pages.
5. N. T. Courtois. The security of Hidden Field Equations (HFE). In *The Cryptographer's Track at RSA Conference 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 266–281. D. Naccache, editor, Springer, 2001. http://www.minrank.org/hfesec.ps—dvi—pdf.
6. J. Ding and J. Gower. Inoculating multivariate schemes against differential attacks. In *PKC*, volume 3958 of *LNCS*. Springer, April 2006. Also available at http://eprint.iacr.org/2005/255.
7. J. Ding, C. Wolf, and B.-Y. Yang. ℓ-invertible cycles for multivariate quadratic public key cryptography. In *PKC*, volume 4450 of *LNCS*, pages 266–281. Springer, April 2007.
8. V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical cryptanalysis of sflash. In *Crypto*. Springer, to appear, 2007.
9. V. Dubois, P.-A. Fouque, and J. Stern. Cryptanalysis of sflash with slightly modified parameters. In *Eurocrypt*. Springer, to appear, 2007. ECrypt Electronic Newsletter, www.ecrypt.eu.org/webnews/webnews1206.htm.
10. P.-A. Fouque, L. Granboulan, and J. Stern. Differential cryptanalysis for multivariate schemes. In *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science. Ronald Cramer, editor, Springer, 2005. 341–353.
11. W. Geiselmann, R. Steinwandt, and T. Beth. Attacking the affine parts of SFlash. In *Cryptography and Coding - 8th IMA International Conference*, volume 2260 of *Lecture Notes in Computer Science*, pages 355–359. B. Honary, editor, Springer, 2001. Extended version: http://eprint.iacr.org/2003/220/.
12. T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature verification and message-encryption. In *Advances in Cryptology — EUROCRYPT 1988*, volume 330 of *Lecture Notes in Computer Science*, pages 419–545. Christoph G. Günther, editor, Springer, 1988.
13. NESSIE: New European Schemes for Signatures, Integrity, and Encryption. Information Society Technologies programme of the European commission (IST-1999-12324). http://www.cryptonessie.org/.
14. J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *Advances in Cryptology — CRYPTO 1995*, volume 963 of *Lecture Notes in Computer Science*, pages 248–261. Don Coppersmith, editor, Springer, 1995.
15. J. Patarin, L. Goubin, and N. Courtois. C^*_{-+} and HM: Variations around two schemes of T.Matsumoto and H.Imai. In *Advances in Cryptology — ASIACRYPT 1998*, volume 1514 of *Lecture Notes in Computer Science*, pages 35–

49. Kazuo Ohta and Dingyi Pei, editors, Springer, 1998. Extended Version: http://citeseer.nj.nec.com/patarin98plusmn.html.

16. C. Wolf and B. Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 12^{th} of May 2005. http://eprint.iacr.org/2005/077/, 64 pages.