Properties of the Discrete Differential with Cryptographic Applications

Daniel Smith-Tone

Department of Mathematics, Indiana University
smithdc@indiana.edu

Abstract. Recently, the C^{*-} signature scheme has been completely broken by Dubois et al. [2, 3]. As a consequence, the security of SFLASH and other multivariate public key systems have been impaired. The attacks presented in [2, 3] rely on a symmetry of the differential of the encryption mapping. In [1], Ding et al. experimentally justify the use projection as a method of avoiding the new attack. In this paper, we derive some properties of the discrete differential, give a theoretical justification for the reparation in [1], and establish the exact context in which this attack is applicable.

Key words: Matsumoto-Imai, multivariate public key cryptography, discrete, differential, SFLASH, symmetry, HFE

1 Introduction

In recent years much focus in public key cryptography has shifted to multivariate systems. This change is due to several factors: the problem of solving a system of quadratic equations is hard, particularly over a field of characteristic greater than zero; to date, no great reduction of the complexity of this problem has been found in the quantum model; there are very efficient implementations of multivariate systems; and finally, it is easy to parameterize many multivariate systems in such a way that vastly different schemes are derived with potentially vastly different resistances to specialized attacks.

One multivariate scheme which has recently been broken by Dubois et al. in [2, 3] is the C^{*-} signature scheme. In particular, the attack breaks the SFLASH signature scheme and some variants of the scheme by using a special property of the differential of the encryption map to recover a full C^* public key, compatible with the C^{*-} public key, to which Patarin's attack in [6] may be applied.

More recently, Ding et al., see [1], have repaired the SFLASH scheme using projection, which has also, ironically, been called "fixing," see [9]. They were able to show strong experimental evidence that projection protects the scheme from the differential attack; however, no theoretical explanation was available.

This paper is organized as follows. First, we review the C^*, HFE, C^{*-}, and SFLASH schemes. Next, we look at the new attack on C^{*-} of Dubois, et al. In the following section, we present some useful results on the differential of a field map and establish limits for the effectivity of the new attack in the more general

HFE setting. We then present a theoretical analysis of the claim by Ding et al. in [1] that projection avoids the new attack. Finally, we discuss the implications of these results.

2 C^*, HFE, and SFLASH

The SFLASH signature scheme can be considered a special case of the C^{*-} signature scheme which is derived from the Matsumoto-Imai cryptosystem, often called the C^* scheme, originally presented in [4]. Each of these schemes was designed to take advantage of the difficulty of solving a nonlinear system of equations over a finite field.

2.1 The C^* Scheme

The idea of the C^* scheme is to use affine maps to hide a "quadratic" monomial map. This can be accomplished by composing functions, each of which is easily invertible.

Choose a finite field $\mathbb{F}_q$ of even characteristic and a degree n extension k. The map $f : k \to k$ defined by $f(x) = x^{1+q^\theta}$ is a permutation polynomial for coprime values of n and θ. Choosing two $\mathbb{F}_q$-affine transformations, U and T, we can encrypt via the composition

$$P = T \circ f \circ U. \tag{1}$$

Note that the map $x \mapsto x^{q^\theta}$, a Frobenius map, is $\mathbb{F}_q$-linear since

$$(x+a)^{q^\theta} = (x+a)^{p^{k\theta}} = \sum_{i=0}^{p^{k\theta}} \binom{p^{k\theta}}{i} a^i x^{p^{k\theta}-i} = x^{q^\theta} + a^{q^\theta}, \tag{2}$$

where the last equality is due to the fact that $\binom{p^{k\theta}}{i} = 0$ for $0 < i < p^{k\theta}$ in a field of characteristic p, and the fact that $x \mapsto x^{q^\theta}$ is the identity map on $\mathbb{F}_q$. Therefore, we can represent f as $f(x) = x(L_\theta x)$, where $L_\theta x = x^{q^\theta}$ is the exponentiation expressed as an $\mathbb{F}_q$-linear transformation. For this reason we call f $\mathbb{F}_q$-quadratic or simply "quadratic." Encryption can thus be expressed as a system of n multivariate quadratic equations over $\mathbb{F}_q$. On the other hand, decryption is accomplished by inverting each of the above maps, circumventing the problem of solving a nonlinear system of equations:

$$P^{-1} = U^{-1} \circ f^{-1} \circ T^{-1}. \tag{3}$$

In [6], Patarin showed that C^* is insecure. His attack is based on a relation on the input and output of the monomial map. Given $v = f(u)$ we have the following:

$$v^{q^\theta} u = v u^{q^{2\theta}}. \tag{4}$$

By composing with the affine maps, T and U, we have $T^{-1}y = f(Ux)$ which we can express as the following bilinear relation on the plaintext, x, and ciphertext, y:

$$(T^{-1}y)^{q^\theta}(Ux) = (T^{-1}y)(Ux)^{q^\theta}. \tag{5}$$

Once such a bilinear relation between x and y is obtained by computing a large number of plaintext-ciphertext pairs, we have an efficient alternate means of decryption.

2.2 HFE

The HFE cryptosystem, introduced by Patarin [7] is a generalization of C^*. HFE still uses the setting of a finite field, $\mathbb{F}_q$, and an n-dimensional extension k over $\mathbb{F}_q$. There is one main difference. Specifically, the hidden mapping, f, is no longer necessarily a monomial; it can be a more general quadratic polynomial. While general HFE schemes have the desirable quality of being resistant to Patarin's attack on C^*, there are some problems as well.

It is difficult to find permutation polynomials which are not translations of monomial maps. Some conditions are known which guarantee that a polynomial is a permutation polynomial, such as those given in [5], but no criteria are known for the construction of general quadratic permutation polynomials. For this reason, the HFE scheme is implemented with an encryption map which is not, in general, bijective. This quality of the cryptosystem has the effect of making collisions possible and rendering decryption and signature generation much less efficient.

2.3 The C^{*-} Scheme

To prevent an attack exploiting the bilinear relation, (5), it was suggested in [8] to remove some of the coordinate equations. The resulting scheme, suitable for signatures, is commonly called the C^{*-} scheme.

Suppose we delete the last r equations in the public key of a C^* scheme. Let P_Π denote the projection of P onto the first $n - r$ coordinates. To sign, a user needs only compute a preimage of $y = P_\Pi(x)$ which is easily accomplished by padding y with r random coordinate values and using the decryption algorithm. Since $|\{x|P_\Pi(x) = y\}| = q^r$, it is apparent that allowing r to be too large renders the scheme inefficient in the sense that the size of the field must be quite large to maintain the improbability of collision detection. If r is too small, however, there are methods to reduce the C^{*-} scheme to a C^* scheme, as shown in [8].

The difficulty in removing r of the public equations lies in the fact that, although (4) is still valid, (5) can no longer be used. We don't know r of the coordinates of y, and therefore, we are missing terms in each equation we generate over $\mathbb{F}_q$. Alternatively, we may consider T to be an $r \times n$ matrix, since the new encryption mapping does not have access to r of the rows of T. As a consequence, it is impossible to deterministically compute coefficients involving T^{-1}.

2.4 SFLASH

SFLASH is a signature scheme based on the C^{*-} scheme. The choice of parameters which were considered secure by the New European Schemes for Signature, Integrity, and Encryption, NESSIE, consortium are $q = 2^7$, $[k : \mathbb{F}_q] = 37$, $\theta = 11$, and $r = 11$. This scheme was widely heralded for nearly ten years until more recently SFLASH and some possible variants were broken completely in [2, 3].

3 The New Attacks on C^{*-} Schemes

Dubois et al. in [2] and [3] based the attacks on C^{*-} on a property of the bilinear differential, $Df(a, x) = f(a + x) - f(a) - f(x) + f(0)$, of the encryption map, f, which they called "multiplicative." The attacks utilize a linear symmetry of f which guarantees the existence of $L : k \to k$, an $\mathbb{F}_q$-linear map, satisfying the following relation:

$$Df(La, x) + Df(a, Lx) = p(L)Df(a, x), \tag{6}$$

where p is a polynomial, which we call the *separation polynomial*.

In particular, the attacks focus on finding L which correspond to left multiplication by an element $\sigma \in k$. Therefore, we are interested in discovering properties of f guaranteeing the existence of the following *multiplicative symmetry*:

$$Df(\sigma a, x) + Df(a, \sigma x) = p(\sigma)Df(a, x). \tag{7}$$

Notice that if an $\mathbb{F}_q$-linear transformation is found which corresponds, when factored through the encryption, to a nontrivial multiplication, it is likely that new linearly independent relations on the output of the monomial function will be found. Specifically, we have the following:

$$DP_{\Pi}(N_\sigma a, x) + DP_{\Pi}(a, N_\sigma x) = \Pi \circ T \circ M_{p(\sigma)} \circ Df(Ua, Ux)), \tag{8}$$

where $N_\sigma = U^{-1} M_\sigma U$ and M_τ is the matrix of multiplication by τ. In practice, equation (8) is used to find relations satisfied by these multiplication map conjugates. If enough new relations are derived in this manner to generate such a N_σ, it is likely that a new full rank C^* scheme may be constructed by gathering new linearly independent relations from the following mapping, where f specifically is multiplicative, as is the case for SFLASH,

$$\begin{aligned} P_\Pi \circ N_\sigma &= \Pi \circ T \circ f \circ U \circ N_\sigma \\ &= \Pi \circ T \circ f \circ M_\sigma \circ U \\ &= \Pi \circ T \circ M_{f(\sigma)} \circ f \circ U. \end{aligned} \tag{9}$$

At this point, Patarin's attack may be applied. If the system is not full rank, or close enough to full rank to apply another attack, the process of finding a nontrivial multiplication is repeated.

Dubois et al. use this method in [3] to break variants of SFLASH in which the θ parameter and the degree of the extension are not coprime. In [2] the same method is used to break SFLASH with the NESSIE parameters. Both of these attacks may be considered instances of the same attack since both use the multiplicative symmetry above. The only difference is that in the former the attack focuses specifically on finding multiplications by roots of the separation polynomial, whereas in the latter the focus is on finding multiplications by elements which are not roots of the separation polynomial.

The question was asked in [2] to what extent these methods involving the differential can be applied to the HFE^- scheme, i.e., to what extent can we use such a symmetry relation when the monomial function is replaced by a more general polynomial?

4 Multiplicative Symmetric Properties of the Differential

To answer the questions posed in [2], we form a classification of polynomial maps $f : k \to k$ having the multiplicative symmetry. We first need to establish some basic definitions and ground work. Here we establish the convention that, unless otherwise specified, the terms "linearity," "bilinearity," etc. refer to linearity over a base field.

Definition 1. *Given a field $\mathbb{F}$, a field extension k, and a multivariate function $f : k^m \to k$, the* discrete partial differential *of f with respect to x_i is given by*

$$\begin{aligned} D_{x_i} f(x_1, \ldots, x_{i-1}, a, x_i, \ldots, x_m) = & f(x_1, \ldots, x_{i-1}, a + x_i, x_{i+1}, \ldots, x_m) \\ & - f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_m) \\ & - f(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_m) \\ & + f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_m). \end{aligned} \tag{10}$$

We should note that the discrete partial differential operator has the desired property of $\mathbb{F}$-linearity. Using this property we are able to prove the following useful result about bilinear maps, the proof of which generalizes to the multilinear case.

Theorem 1 *Let k be an extension field of $\mathbb{F}$, $f : k^2 \to k$ be a polynomial, and $g : k^2 \to k$ be a monomial summand of f. If f is bilinear, then g is bilinear.*

Proof. For specificity, let $f = \sum_i g_i = \sum_i c_i x_1^{\alpha_{i,1}} x_2^{\alpha_{i,2}}$, where this representation is not equivalent to another expression of f with monomials of smaller multidegree. Without loss of generality suppose that g_0 is not bilinear; in particular, suppose that g_0 is not linear with respect to x_1. Since the discrete partial differential operator is linear, we have the following identity:

$$D_{x_1} f = D_{x_1} \sum_i g_i = \sum_i D_{x_1} g_i. \tag{11}$$

Also, by the linearity of D_{x_1} and the bilinearity of f, $D_{x_1} f = 0$. Therefore, applying the definition of D_{x_1} to the right side of (11), we have the following:

$$0 = \sum_i D_{x_1} g_i = \sum_i c_i \sum_{j=1}^{\alpha_{i,1}-1} \binom{\alpha_{i,1}}{j} a^j x_1^{\alpha_{i,1}-j} x_2^{\alpha_{i,2}}, \tag{12}$$

where, of course, the binomial coefficients are taken modulo the characteristic of k. Note, first, that since the multidegree of each g_i is unique, the multidegree of each term in this expression is also unique, and, second, that since g_0 is not linear with respect to x_1, not all $\binom{\alpha_{0,1}}{j}$ are zero. Since this polynomial is identically zero, we can fix $a = 1$, which gives us the following identity for all $(x_1, x_2) \in k^2$:

$$0 = \sum_i c_i \sum_{j=1}^{\alpha_{i,1}} \binom{\alpha_{i,1}}{j} x_1^{\alpha_{i,1}-j} x_2^{\alpha_{i,2}}. \tag{13}$$

In the characteristic zero case, we have a polynomial identically equal to zero, while in the characteristic p setting, we have a polynomial identically equal to zero which has no equivalent representation with monomials of smaller multidegree; therefore, the coefficient of each monomial in (13) is zero. The fact that there exists a nonzero $\binom{\alpha_{0,1}}{j}$ implies that $c_0 = 0$. Consequently, $g_0 = 0$. This contradicts our assumption that g_0 is not bilinear. Thus every monomial summand of f is bilinear.

This theorem offers the following important result as a corollary.

Corollary 1 *Let $f : k \to k$ be a polynomial, and let $g : k \to k$ be a monomial summand of f. If Df is bilinear, then Dg is bilinear.*

Proof. Given $f = \sum_i g_i$, by the linearity of the discrete differential operator, we have

$$Df = \sum_i Dg_i. \tag{14}$$

Note that, since each g_i has a unique degree, each term in the right side of (14) has a unique multidegree. Now by Theorem 1, since Df is bilinear, each monomial summand of Df is bilinear, and therefore, any sum of such summands is bilinear. Thus Dg_i is bilinear for all i.

Now we focus on the multiplicative symmetry and restrict to the finite field setting. Notice that the above corollary is as general as possible in this setting because finite fields have the distinguishing quality of being the only rings for which every function from the ring to itself is a polynomial. In the following results, k denotes a degree n extension of the finite field $\mathbb{F}_q$.

Lemma 1 *Let g be a monomial function with an $\mathbb{F}_q$-bilinear differential. Then g has the multiplicative symmetry. Furthermore, two such monomial functions g_1 and g_2 share the same separation polynomial if and only if $g_1 = cg_2$ for some constant $c \in k$.*

Proof. Since g is a monomial function, $Dg(a,x) = c\sum_{i=1}^{k-1}\binom{k}{i}a^i x^{k-i}$. Dg is bilinear and thus, any monomial with nonzero coefficient in this sum must be linear in both a and x. Therefore $k = q^{\theta_1} + q^{\theta_2}$ for some $0 \leq \theta_1, \theta_2 \leq n$. Hence, $g(x) = cx^{q^{\theta_1}+q^{\theta_2}}$. As a consequence, we have $Dg(a,x) = ca^{q^{\theta_1}}x^{q^{\theta_2}} + ca^{q^{\theta_2}}x^{q^{\theta_1}}$. Letting $p(x) = x^{q^{\theta_1}} + x^{q^{\theta_2}}$, we obtain $Dg(\sigma a, x) + Dg(a, \sigma x) = p(\sigma)Dg(a,x)$. By the above construction of the separation polynomial, two quadratic monomial functions share the same separation polynomial if and only if they are constant multiples of each other.

The following theorem gives a classification of polynomial functions with the multiplicative symmetry.

Theorem 2 *A polynomial $f : k \to k$ with a bilinear differential has the multiplicative symmetry if and only if it has one quadratic monomial summand.*

Proof. ($\Leftarrow$) Suppose that f has exactly one quadratic monomial summand, g, and all other monomial summands are linear. Then $Df = Dg$. Thus f has the multiplicative symmetry with the same separation polynomial as that of g.

($\Rightarrow$) By Corollary 1, we know that all monomial summands of f have a bilinear differential. Suppose by way of contradiction that f has r distinct quadratic monomial summands, g_m, with $r > 1$. We know $Df = \sum_{m=1}^{r} Dg_m$. Therefore,

$$Df(\sigma a, x) + Df(a, \sigma x) = p_f(\sigma)\sum_{m=1}^{r} Dg_m(a,x) \tag{15}$$

On the other hand,

$$\begin{aligned} Df(\sigma a, x) + Df(a, \sigma x) &= \sum_{m=1}^{r}(Dg_m(\sigma a, x) + Dg_m(a, \sigma x)) \\ &= \sum_{m=1}^{r} p_{g_m}(\sigma)Dg_m(a,x). \end{aligned} \tag{16}$$

Therefore, taking the difference of 15 and 16,

$$\sum_{m=1}^{r}(p_f - p_{g_m})(\sigma)Dg_m(a,x) = 0, \tag{17}$$

for all $\sigma, a, x \in k$. Since the g_m are not constant multiples of each other, by Lemma 1, $p_{g_i} \neq p_{g_j}$ for $i \neq j$. We can therefore fix a $\sigma \in k$ such that for some $s \in \{1, \ldots, r\}$ we have $p_f(\sigma) - p_{g_s}(\sigma) \neq 0$. Thus

$$\sum_{m=1}^{r} t_m(a^{j_m}x^{k_m-j_m} + a^{k_m-j_m}x^{j_m}) = 0, \tag{18}$$

where $t_m = c_m(p_f - p_{g_m})(\sigma)$ are constants. Rewriting this sum by collecting powers of x and indexing by the powers of x we have the following:

$$\sum_l P_l(a)x^l = 0, \tag{19}$$

for all x, where the P_l are polynomials in a. Since the P_l are not identically zero, there is a value of a such that not all of the P_l are simultaneously zero. Fix such an a. Then we have a nonzero polynomial in x the degree of which is less than q^n. But this contradicts (19). Thus, f has at most one quadratic monomial summand.

Now we have an answer to the questions posed in [2]. Both of the attacks presented in [3, 2] require the existence of a hidden field map with the multiplicative symmetry. In particular, the experiments in [2] suggest that for large field extensions the general linear and multiplicative symmetries of equations 6 and 7 are intertwined, i.e., f has a linear symmetry only if there is a nonsingular linear map, L, such that $f \circ L$ has the multiplicative symmetry. The above results show that the multiplicative symmetry is only present for field maps which differ from a C^* monomial by an affine map; thus, HFE is not, in general, susceptible to the multiplicative symmetry attack.

5 The Effect of Projection

In [1], Ding et al. proposed projection as a method of securing the C^{*-} scheme from the attack based on the multiplicative symmetry. Experimentally, it has been verified that the projection onto a codimension 1 or more affine space breaks the symmetry. In light of the results of the previous section, we can give a more categorical explanation for the observed behavior.

In the case of fixing m variables, projecting corresponds to the following mapping:

$$P(x) = T \circ f \circ M_{a_1,\ldots,a_m} \circ U, \tag{20}$$

where $M_{a_1,\ldots,a_m}$ is the linear transformation which acts as the identity on the first $n - m$ coordinates and replaces the last m coordinates with $a_i \cdot x$, where $a_i \in \mathbb{F}_q^n$ has last m coordinates zero.

Let us first consider the singularity of $M_{a_1,\ldots,a_m}$ to be subsumed by f. We prove that the composition of f with a singular factor of $M_{a_1,\ldots,a_m}$ cannot have the multiplicative symmetry.

Theorem 3 *Let M be an $\mathbb{F}_q$-linear transformation and let f be a C^* monomial map, $f(x) = x^{1+q^\theta}$. The composition $f \circ M$ has the multiplicative symmetry if and only if M is a linear monomial map, i.e. $Mx = cx^{q^i}$ for some $i < n$.*

Proof. ($\Leftarrow$) Suppose M is a linear monomial map, $Mx = c_M x^{q^i}$ for some $i < n$. Therefore, $f \circ M(x) = c_M^{q^\theta+1} x^{q^{\theta+i}+q^i}$, where, of course, the sum in the exponents

of q is taken modulo n. As a consequence of Theorem 2, $f \circ M$ has the multiplicative symmetry.

($\Rightarrow$) Let $\hat{f} = f \circ M$. Since every $\mathbb{F}_q$-linear transformation, M, can be written $M = \sum_{i=0}^{n-1} c_i x^{q^i}$, we have the following:

$$\begin{aligned}
\hat{f}(x) &= f \circ M(x) \\
&= f \circ \sum_{i=0}^{n-1} c_i x^{q^i} \\
&= (\sum_{i=0}^{n-1} c_i x^{q^i})^{1+q^\theta} \\
&= \sum_{i,j<n} c_i c_{j-\theta}^{q^\theta} x^{q^i+q^j} \\
&= \sum_{i=0}^{n} c_i c_{i-\theta}^{q^\theta} x^{2q^i} + \sum_{i<j<n} (c_i c_{j-\theta}^{q^\theta} + c_j c_{i-\theta}^{q^\theta}) x^{q^i+q^j}.
\end{aligned} \tag{21}$$

Note that the right hand side expression is simplified because the equality $q^i + q^j = q^k + q^l$ implies either $(i, j) = (k, l)$ or $(i, j) = (l, k)$.

We have two distinct types of coefficients. The first, $c_i c_{i-\theta}^{q^\theta}$, corresponds to a product along a column in the following matrix, while the second, $c_i c_{j-\theta}^{q^\theta} + c_j c_{i-\theta}^{q^\theta}$, corresponds to a minor.

$$\begin{pmatrix} c_0 & c_1 & \dots & c_n \\ c_{-\theta}^{q^\theta} & c_{1-\theta}^{q^\theta} & \dots & c_{n-\theta}^{q^\theta} \end{pmatrix} \tag{22}$$

Suppose $\hat{f}$ has the multiplicative symmetry. By Theorem 2, the coefficient of at most one power of x is nonzero. Therefore, the coefficient matrix must have either one column with a nonzero product and no nonzero minors, no column with a nonzero product and exactly one nonzero minor, or no nonzero entries, in which case M is trivial.

In the first case, in which the one nonzero coefficient is of the form $c_i c_{i-\theta}^{q^\theta}$, the coefficient matrix must be of the form

$$\begin{pmatrix} 0 \dots 0 & c_i & 0 \dots 0 \\ 0 \dots 0 & c_{i-\theta}^{q^\theta} & 0 \dots 0 \end{pmatrix}. \tag{23}$$

since otherwise the matrix would have a nonzero minor. This, however, implies that $\theta = 0$ and $Mx = c_i x^{q^i}$. Thus, in this case, M is a linear monomial map and, specifically, $f(x) = cx^2$. Clearly, this case is impossible if q is even.

In the other case, i.e. the one nonzero coefficient is of the form $c_i c_{j-\theta}^{q^\theta} + c_j c_{i-\theta}^{q^\theta}$, we have one nonzero minor and no column with a nonzero product. Therefore,

the coefficient matrix has the form

$$\begin{pmatrix} 0 \dots c_i \dots & 0 & \dots 0 \\ 0 \dots 0 \dots & c_{j-\theta}^{q^\theta} & \dots 0 \end{pmatrix}, \tag{24}$$

or

$$\begin{pmatrix} 0 \dots & 0 & \dots c_j \dots 0 \\ 0 \dots & c_{i-\theta}^{q^\theta} \dots 0 & \dots 0 \end{pmatrix}. \tag{25}$$

This case is only possible when $c_i = c_{j-\theta}$ or $c_j = c_{i-\theta}$; furthermore, only one of c_i and c_j is nonzero. This fact again implies that Mx is a nonzero linear monomial map. Thus the composition of a quadratic monomial and a nonzero $\mathbb{F}_q$-linear map, M, has the multiplicative symmetry if and only if M is a linear monomial map.

Therefore, projection indeed does break the symmetry over the large field. The only remaining possible application of the methods of Dubois et al. is if we consider the matrix $M_{a_1,\dots,a_m}$ to be absorbed by U, in which case we must accept that $S = M_{a_1,\dots,a_m}U$ is singular.

In this case, it is conceivable that the attack of Dubois et al. may be applied by using a pseudoinverse, S^+ instead of an inverse in the definition, $N_\sigma = S^+ M_\sigma S$. The only restriction is that we require $SS^+ M_\sigma S = M_\sigma S$, which occurs only when the image of S in k, which we denote Sk, is σ-invariant.

Theorem 4 *Let k be a finite extension of $\mathbb{F}_q$ and let $S : k \to k$ be a singular $\mathbb{F}_q$-linear transformation. There exists a $\sigma \in k$ such that Sk is σ-invariant if and only if Sk is an ℓ-subspace of k, where ℓ is the smallest intermediate extension of $\mathbb{F}_q$ containing σ.*

Proof. ($\Leftarrow$) If Sk is an ℓ-subspace of k then it is trivially σ-invariant for all $\sigma \in \ell$. ($\Rightarrow$) Sk is an $\mathbb{F}_q$-subspace of k, and is consequently $\mathbb{F}_q$-closed. Since $Sk \subset k$ is σ-invariant, it is a union of sets of the form $\langle\sigma\rangle\, v$ for $v \in k$. Since the $\mathbb{F}_q$-closure of any such set, $\langle\sigma\rangle\, v$, is an ℓ-subspace, by additive closure, Sk is an ℓ-subspace of k.

Therefore, projection does not exactly "break" the multiplicative symmetry in general; rather, it "pushes down" the symmetry into a subspace over a smaller field. It should be noted that, given a random choice of singular map, S, it is extremely unlikely for Sk to be an ℓ-subspace of k. In particular, as in the case of SFLASH, if k is a prime extension of $\mathbb{F}_q$, then there does not exist a nontrivial intermediate extension, ℓ, and the multiplicative symmetry is completely broken.

6 Conclusion

We conclude from the preceding facts that the method using multiplicative symmetry can be applied only when the hidden permutation polynomial has exactly one nonlinear monomial summand. If this condition is not met, as is the case

for the general HFE scheme, the polynomial has no multiplicative symmetry in this sense.

In addition, we give theoretical justification for the effectiveness of projection as a means of removing the multiplicative symmetry. We prove that projection is a legitimate method of avoiding the new attacks; however, more study is needed to confirm that a projected SFLASH will be secure.

References

1. J. Ding, B.-Y. Yang, C.-M. Cheng, O. Chen, and V. Dubois, *Breaking the symmetry: a way to resist the new differential attack.* Cryptology ePrint Archive, Report 2007/366, 2007. http://eprint.iacr.org/.
2. V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern, *Practical cryptanalysis of SFLASH*, Advances in Cryptology - CRYPTO 2007, Springer, 4622 (2007), pp. 1–12.
3. V. Dubois, P. A. Fouque, and J. Stern, *Cryptanalysis of SFLASH with slightly modified parameters*, Eurocrypt 07, Springer, 4515 (2007), pp. 264–275.
4. T. Matsumoto and H. Imai, *Public quadratic polynomial-tuples for efficient signature verification and message-encryption*, Eurocrypt '88, Springer, 330 (1988), pp. 419–545.
5. R. A. Mollin and C. Small, *On permutation polynomials over finite fields*, Internat. J. Math. and Math. Sci., 10 (1987), pp. 535–543.
6. J. Patarin, *Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88*, Crypto 1995, Springer, 963 (1995), pp. 248–261.
7. ——, *Hidden Field Equations (HFE) and Isomorphisms of Polynomials: two new Families of Asymmetric Algorithms*, Eurocrypt '96, Springer, 1070 (1996), pp. 33–48.
8. J. Patarin, L. Goubin, and N. Courtois, C^{*}_{-+} *and HM: Variations around two schemes of T.Matsumoto and H.Imai*, Asiacrypt 1998, Springer, 1514 (1998), pp. 35–49.
9. C. Wolf and B. Preneel, *Taxonomy of public key schemes based on the problem of multivariate quadratic equations.* Cryptology ePrint Archive, Report 2005/077, 2005. http://eprint.iacr.org/.