A Classification of Differential Invariants for Multivariate Post-Quantum Cryptosystems

Ray Perlner[1] and Daniel Smith-Tone[1,2]

[1]National Institute of Standards and Technology,
Gaithersburg, Maryland, USA
[2]Department of Mathematics, University of Louisville,
Louisville, Kentucky, USA

ray.perlner@nist.gov, daniel.smith@nist.gov

Abstract. Multivariate Public Key Cryptography(MPKC) has become one of a few options for security in the quantum model of computing. Though a few multivariate systems have resisted years of effort from the cryptanalytic community, many such systems have fallen to a surprisingly small pool of techniques. There have been several recent attempts at formalizing more robust security arguments in this venue with varying degrees of applicability. We present an extension of one such recent measure of security against a differential adversary which has the benefit of being immediately applicable in a general setting on unmodified multivariate schemes.

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

1 Introduction

Since Peter Shor's discovery of quantum algorithms for factoring and computing discrete logarithms quickly with quantum computers, there has been a growing community with the goal of establishing a replacement for RSA or Diffie-Hellman in the quantum realm. The last two decades have witnessed a great deal of progress towards realizing that quantum computing world, indicating that Shor's discovery is a great deal more than a mathematical curiosity; instead, his discovery marks the need for an eventual paradigm shift in our public key infrastructure.

Multivariate Public Key Cryptography(MPKC) has emerged as one of a few serious candidates for security in the post-quantum world. This emergence is due to several facts. First, the problem of solving a system of quadratic equations is known to be NP-hard, and seems to be hard even in the average case. No great reduction of the complexity of this problem has been found in the quantum model of computing, and, indeed, if this problem is discovered to be solvable in the quantum model, we can solve all NP problems, which seems

particularly wishful. Second, multivariate systems are very efficient, often having speeds dozens of times faster than RSA, [1–3]. Finally, several theoretical advances have resulted in the development of modification techniques which allow multiple parameters to be hidden within a system which can be altered to achieve different performance or security properties.

One of the great challenges facing MPKC is the task of establishing reasonable security assurance. Though there have been some recent attempts at forming a new model in which to offer provable security for encryption and signatures, see for example [4, 5], it seems apparent that these models are not as general as we would like or require modifications of realistic protocols to carry their full meaning. The task of quantifying indistinguishability between general classes of systems of multivariate equations seems exceptionally difficult in light of the fact that even with a great deal of structure in the construction of a multivariate cryptosystem, the coefficients can appear to have a uniform distribution. Although history has shown that once a way to distinguish a class of systems of structured multivariate equations from a collection of randomly generated equations is discovered, a method of solving this system is often quickly developed, it is not clear that the techniques for distinguishing such systems are indicative of an underlying theme powerful enough to establish a general method of security proof.

The many cryptanalyses of various big field multivariate cryptosystems have, however, pointed out weaknesses in the predominant philosophy for the construction of such multivariate public key cryptosystems. Several systems, SFLASH, Square, for example, which are based on simple modifications of the prototypical Matsumoto-Imai public key cryptosystem, have been broken by very similar differential attacks exploiting some symmetry which is inherent to the field structure these systems utilize. See [6–9]. Even in the small field milieu, various attacks, for example the oil-vinegar attack, see [10], can be viewed as an attack on differential structure; specifically, discovering a differential invariant.

In [11], a measure of security against attacks exploiting differential symmetry was advanced. This methodology allows one to construct proofs that a cryptosystem is secure against a differential symmetry adversary by classifying the differential symmetric structure of the cryptosystem. By identifying all possible initial general linear differential symmetries possessed by a field map, one can determine which linear relations involving the differential of a public key are accessible to any adversary, and thus guarantee security against such an attack model. Although this result is not as robust as a reduction theoretic proof of security, it has the benefit, first, of being far stronger than the traditional model of checking the vulnerability of new schemes against old attacks, second, of being immediately applicable in the design of cryptosystems, and third, of perhaps being a more realistic goal than that of reduction theoretic proof.

In this article, we introduce a technique which is dual to that of [11] in the sense that it assures security against any first-order differential invariant adversary. Specifically, we establish a model for classifying first-order differential invariants of a field map and apply the model, providing classifications of such in-

variants for specific cryptosystems. This characterization, in conjunction with an analogous classification in the symmetric setting, provides a model for security against any first-order differential adversary, and is the first step towards establishing general differential security via an existence criterion. We suggest such an analysis of differential invariant security as a reasonable criterion and pragmatic tool for cryptographers in the development of future multivariate schemes.

The paper is organized as follows. The next section illustrates the ubiquitous nature of the differential attack by recasting the attack on the balanced oil and vinegar scheme in the differential setting. In the following section, we focus on differential invariants, presenting the first-order differential invariant and discussing the technique for realizing the theoretical differential invariant structure of any class of MPKC. The subsequent section restricts the analysis of this space to the case in which the hidden field map of the cryptosystem is a C^* monomial. The differential invariant structure is then determined for projected systems such as the projected SFLASH analogue, pSFLASH. Finally, we review these results and suggest a general model for differential security.

2 Differential Symmetries and Invariants

Differential attacks play a crucial role in multivariate public key cryptography. Such attacks have not only broken many of the so called "big field" schemes, they have directed the further development of the field by inspiring modifiers — Plus (+), Minus (-), Projection (p), Perturbation (P), Vinegar (v) — and the creation of newer more robust techniques.

The differential of a field map, f, is defined by $Df(a,x) = f(a+x) - f(a) - f(x) + f(0)$. The use of this discrete differential appears to occur in very many cryptanalyses of post-quantum multivariate schemes. In fact, we can even consider Patarin's initial attack, in [12], on Imai and Matsumoto's C^* scheme, see [13], as the exploitation of a trivial differential symmetry. Suppose $f(x) = x^{q^\theta+1}$ and let $y = f(x)$. Since the differential of f, Df, is a symmetric bilinear function, $0 = Df(y,y) = Df(y, x^{q^\theta+1}) = yx^{q^{2\theta}+q^\theta} + y^{q^\theta}x^{q^\theta+1} = x^{q^\theta}(yx^{q^{2\theta}} + y^{q^\theta}x)$. Dividing by x^{q^θ} we have Patarin's linear relation, $yx^{q^{2\theta}} = y^{q^\theta}x$; see [12] for details.

Differential methods provide powerful tools for decomposing a multivariate scheme. To illustrate the nearly universal nature of differential attacks, we review the attack of Kipnis and Shamir, see [10], on a non-big-field system, the oil and vinegar scheme. Though they use differing terminology, the attack exploits a symmetry hidden in the differential structure of the scheme.

Recall that the oil and vinegar scheme is based on a hidden quadratic system of equations, $f : k^n \to k^o$, in two types of variables, $x_1, ..., x_o$, the oil variables, and $x_{o+1}, ..., x_{o+v=n}$, the vinegar variables. We focus on the balanced oil and vinegar scheme, in which $o = v$. Let $c_1, ..., c_v$ be random constants. The map f has the property that $f(x_1, ..., x_v, c_1, ..., c_v)$ is affine in $x_1, ..., x_v$. The encryption map, $\overline{f}$ is the composition of f with an n-dimensional invertible affine map, L.

Let O represent the subspace generated by the first v basis vectors, and let V denote the cosummand of O. Notice that the discrete differential given by $Df(a,x) = f(x+a) - f(x) - f(a) + f(0)$ has the property that for all a and x in O, $Df(a,x) = 0$. Thus for each coordinate, i, the differential coordinate form Df_i can be represented:

$$Df_i = \begin{bmatrix} 0 & Df_{i1} \\ Df_{i1}^T & Df_{i2} \end{bmatrix}.$$

Let M_1 and M_2 be two invertible matrices in the span of the Df_i. Then $M_1^{-1}M_2$ is an O-invariant transformation of the form:

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

Now the Df_i are not known, but $D(f \circ L)_i = L^T Df_i L$, so the $L^T Df_i L$ are known. Notice that if M is in the span of the Df_i, then $L^T ML$ is in the span of the $L^T Df_i L$. Also, since $(L^T M_1 L)^{-1}(L^T M_2 L) = L^{-1}M_1^{-1}M_2 L$, there is a large space of matrices leaving $L^{-1}O$ invariant, which Kipnis and Shamir are able to exploit to effect an attack against the balanced oil and vinegar scheme; see [10] for details. Making the oil and vinegar scheme unbalanced, see [14], corrects this problem by making any subspace which is invariant under a general product $M_1^{-1}M_2$ very small, see [15].

3 First-Order Differential Invariants

Let $f : k \to k$ be an arbitrary fixed function on k, a degree n extension of the Galois field $\mathbb{F}_q$. Consider the differential $Df(a,x) = f(a+x) - f(a) - f(x) + f(0)$. We can express the differential as an n-tuple of differential coordinate forms in the following way:

$$[Df(a,x)]_i = a^T Df_i x,$$

where Df_i is a symmetric matrix representation of the action on the ith coordinate of the bilinear differential. A first-order differential invariant of f is a subspace $V \subseteq k$ with the property that there exists a $W \subseteq k$ of dimension at most $dim(V)$ for which simultaneously $AV \subseteq W$ for all $A \in Span_i(Df_i)$.

We note that any simultaneous invariant of all $Span_i(Df_i)$ satisfies the above definition, as well the situation for balanced oil and vinegar, in which the invariant was found in the product of an element and an inverse of an element in $Span_i(Df_i)$. A first-order differential invariant is thus a more general construct than a simultaneous invariant among all differential coordinate forms. We present a proof theoretic technique for classifying the first-order differential invariants of such a multivariate map $f : k \to k$ which can specify parameters admitting such invariant structure.

Suppose f has a first-order differential invariant V. Let $V^\perp$ represent the set of all elements x in k such that the dot product $< x, Ay >= 0$ for all $y \in V$ and for all $A \in Span_i(Df_i)$. We should note that in positive characteristic there is a great deal of freedom in membership in $V^\perp$; there is no reason that $V \cap V^\perp$ should

be empty in general or even that $V \oplus V^{\perp}$ be contained in k. Let $M : k \to V$ be an arbitrary linear map. Choosing an arbitrary linear map $M^{\perp} : k \to V^{\perp}$ we have the following (non-linear) symmetric relation, a dual expression of the differential invariance:

$$[Df(M^{\perp}a, Mx)]_i = a^T (M^{\perp})^T Df_i Mx = 0,$$

for all i. Thus $Df(M^{\perp}a, Mx)$ is identically zero for all $a, x \in k$.

Consequently, the existence of a first-order differential invariant for a map f implies the existence of a nonlinear symmetry on f, that is, a symmetry induced by linear maps such that the system of equations expressing the symmetric relation are nonlinear in the coefficients of the maps. Note that the converse implication is false, so that having a first-order differential invariant is a stronger property than having this manner of nonlinear differential symmetry. By explicitly constructing the polynomial map $\overline{f}(a, x) = Df(M^{\perp}a, Mx) \equiv 0$ over k^2, we can derive relations permitting the existence of this nonlinear symmetry, and hence the first-order differential invariant.

4 Invariants in the Prototypical Case

As an illustration of this technique we examine the case when $f : k \to k$ is a C^* monomial map. Specifically, we let $f(x) = x^{q^{\theta}+1}$ where $(\theta, [k : \mathbb{F}_q]) = 1$. This case in particular applies to the famously broken, see [9], SFLASH signature scheme, which was constructed by composing f with two affine transformations: $P = T \circ f \circ U$, where T is singular and U is of full rank.

Theorem 1 *Let $f : k \to k$ be a C^* monomial map. Then f has no nontrivial first-order differential invariant.*

Proof. Suppose by way of contradiction that f has a first-order differential invariant $\{0\} \subsetneq V \subsetneq k$. Define $V^{\perp} = \{x | < x, Ay >= 0, \forall y \in V \text{ and } \forall A \in Span_i(Df_i)\}$. Then f satisfies the relation $Df(M^{\perp}a, Mx) = 0$ for all $a, x \in k$.

$$\begin{aligned} Df(M^{\perp}a, Mx) &= f(M^{\perp}a + Mx) - f(M^{\perp}a) - f(Mx) + f(0) \\ &= f(\sum_{i=0}^{n-1} m_i^{\perp} a^{q^i} + \sum_{i=0}^{n-1} m_i x^{q^i}) - f(\sum_{i=0}^{n-1} m_i^{\perp} a^{q^i}) - f(\sum_{i=0}^{n-1} m_i x^{q^i}) + f(0) \\ &= (\sum_{i=0}^{n-1} m_i^{\perp} a^{q^i} + \sum_{i=0}^{n-1} m_i x^{q^i})^{q^{\theta}+1} - (\sum_{i=0}^{n-1} m_i^{\perp} a^{q^i})^{q^{\theta}+1} - (\sum_{i=0}^{n-1} m_i x^{q^i})^{q^{\theta}+1} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (m_j (m_{i-\theta}^{\perp})^{q^{\theta}} + m_i^{\perp} m_{j-\theta}^{q^{\theta}}) a^{q^i} x^{q^j}. \end{aligned} \tag{1}$$

Since the collection of monomials $\{a^{q^i} x^{q^j}\}$ are algebraically independent, the fact that the above function is identically zero implies that,

$$m_j (m_{i-\theta}^{\perp})^{q^{\theta}} + m_i^{\perp} m_{j-\theta}^{q^{\theta}} = 0,$$

for all $0 \leq i, j \leq n-1$. This fact implies that all 2×2 minors of the following matrix are zero:

$$\begin{bmatrix} m_0 & m_0^{\perp} & m_1 & \cdots & m_{n-1} & m_{n-1}^{\perp} \\ m_{-\theta}^{q^\theta} & (m_{-\theta}^{\perp})^{q^\theta} & m_{1-\theta}^{q^\theta} & \cdots & m_{n-1-\theta}^{q^\theta} & (m_{n-1-\theta}^{\perp})^{q^\theta} \end{bmatrix}.$$

Thus, the rank of this matrix is one, and we have that the second row is a multiple of the first, say $m_i^* = r(m_{i-\theta}^*)^{q^\theta}$, as well as the fact that each column is a multiple of the first, implying, for example, $m_0^{\perp} = sm_0$.

Consequently, for all $0 \leq i \leq n-1$, $m_{i\theta}^* = r^{\frac{q^{i\theta}-1}{q^\theta-1}}(m_0^*)^{q^{i\theta}}$. Moreover, we can specify that $m_{i\theta} = r^{\frac{q^{i\theta}-1}{q^\theta-1}} m_0^{q^{i\theta}}$ and $m_{i\theta}^{\perp} = r^{\frac{q^{i\theta}-1}{q^\theta-1}} s^{q^{i\theta}} m_0^{q^{i\theta}}$, which implies that $m_i^{\perp} = s^{q^i} m_i$ for all $0 \leq i \leq n-1$. Thus

$$\begin{aligned} M^{\perp}x &= \sum_{i=0}^{n-1} m_i^{\perp} x^{q^i} \\ &= \sum_{i=0}^{n-1} m_i s^{q^i} x^{q^i} \\ &= \sum_{i=0}^{n-1} m_i (sx)^{q^i} \\ &= M(sx). \end{aligned} \tag{2}$$

Hence, the fact that $Df(M(sa), Mx) = 0$ for all $a, x \in k$ implies that $Df(Ma, Mx) = 0$ for all $a, x \in k$. This result implies that $dim(Mk) \leq 1$, that is, the dimension of the image of M in k is one, by the following argument.

If $Df(\overline{a}, \overline{x}) = 0$, then $\overline{ax}\left(\overline{x}^{q^\theta-1} + \overline{a}^{q^\theta-1}\right) = 0$, and $\overline{a}^{q^\theta-1} = -\overline{x}^{q^\theta-1}$ implies that $\overline{a}^{q-1} = -\overline{x}^{q-1}$ since $(q^\theta - 1, q^n - 1) = q - 1$. This equation is satisfied exactly when there exists $\alpha \in \mathbb{F}_q$ such that $\overline{a} = \alpha\overline{x}$.

Since this nonlinear differential symmetry exists for any map $g : k \to k$, there exists no nontrivial differential invariant of f.

We can therefore conclude that C^* has no first-order differential invariant weaknesses, even though it is fraught with linear differential symmetric weaknesses. The significance of this result is that we can prove that the cryptosystem in question is secure against all first-order differential invariant adversaries, even those employing attacks yet undiscovered.

5 Invariant Properties under Projection

After SFLASH was broken, it was suggested in [16] that the affine map U be made singular. We continue, establishing security bounds for this suggestion, one of the last unbroken C^* variants, pC^{*-}, or pSFLASH. We recall that in [11] it was

established that pSFLASH with appropriately chosen parameters has no general linear differential symmetries and is thus immune to any type of differential attack relying on the accumulation of linear equations involving the differential of the public key. While it has been established in [17] that the projection in pSFLASH can be removed, the structure when the projection modifier is removed is no longer that of a C^* function; rather, it is an HFE^- scheme. Thus pSFLASH is no more secure than HFE^-, which remains unbroken. For the security details of HFE^-, please see [18].

Theorem 2 *Let $f : k \to k$ be a C^* monomial, and let $\pi : k \to k$ be a linear projection onto a codimension r subspace. Then every nontrivial first-order differential invariant V satisfies $dim(V) \leq dim(V \cap ker(\pi)) + 1$. Consequently, if $r = 1$, there is no nontrivial first-order differential invariant structure beyond the obvious $ker(\pi)$.*

Proof. Let V be a first-order differential invariant of $f \circ \pi$, and let $M : k \to V$ be an arbitrary linear map. Then $\pi \circ M$ is a first-order differential invariant of f, and there exist maps $\overline{M} = \pi \circ M$ and $\overline{M}^{\perp}$ such that:

$$D(f \circ \pi)(M^{\perp}a, Mx) = Df(\pi M^{\perp}a, \pi Mx) = Df(\overline{M}^{\perp}a, \overline{M}x) = 0,$$

for all $a, x \in k$. We note that there are exactly as many possible maps $\overline{M}^{\perp}$ as maps $\pi \circ M^{\perp}$; indeed, the proof of Theorem 1 shows us that $\overline{M}^{\perp}x = \pi \circ M^{\perp}(sx)$ for some s. As in the proof of Theorem 1, $dim(\overline{M}k) \leq 1$, and since π is of codimension r, $dim(Mk) \leq dim(Mk \cap ker(\pi)) + 1$. We note that since any map $g : k \to k$ has this property, $f \circ \pi$ has no nontrivial first-order differential invariant structure beyond $ker(\pi)$.

We can conclude from the above theorem that pSFLASH is secure against any first-order differential invariant adversary.

6 Conclusion

Multivariate public key cryptography has several desirable traits as a potential candidate for post-quantum security. Unfortunately, a standard metric by which we can judge the security of a multivariate scheme has yet to be determined. One consequence of this current status of the field is the similar cryptanalyses of several promising ideas.

We suggest the classification of first-order differential invariants as a second benchmark for the determination of differential security for multivariate public key cryptosystems. We note that while the lack of the symmetric and invariant differential security argument does not imply that a cryptosystem is insecure against a differential adversary, the presence of such an assurance guarantees the resistance against any future first-order differential attack.

The case of pSFLASH is particularly interesting because while retaining the prototypical C^* underlying structure which plagued other variants, the modifications implemented in the scheme seem to perform their intended tasks perfectly.

Most significantly, the projection modifier has provably removed the linear symmetric differential structure, as shown in [11], while retaining the flawless differential invariant structure. On the other hand, the reduction provided by the algorithm in [17] to remove the projection modifier succeeds in transforming pSFLASH into an HFE^- scheme. Although the transformation removes the C^* properties of the core map, it may well prove to be the case that the extra structure the resultant particular HFE^- scheme retains may reveal a weakness. Any new attack on this system will be very exciting, as it will indicate a fundamentally new cryptanalytic technique.

References

1. Chen, A.I.T., Chen, M.S., Chen, T.R., Cheng, C.M., Ding, J., Kuo, E.L.H., Lee, F.Y.S., Yang, B.Y.: Sse implementation of multivariate pkcs on modern x86 cpus. CHES 2009, LNCS, Springer, IACR **5747** (2009) 33–48
2. Chen, A.I.T., Chen, C.H.O., Chen, M.S., Cheng, C.M., Yang, B.Y.: Practical-sized instances of multivariate pkcs: Rainbow, tts, and ℓic-derivatives. Post-Quantum Crypto, LNCS **5299** (2008) 95–106
3. Yang, B.Y., Cheng, C.M., Chen, B.R., Chen, J.M.: Implementing minimized multivariate public-key cryptosystems on low-resource embedded systems. 3rd Security of Pervasive Computing Conference, LNCS **3934** (2006) 73–88
4. Sakumoto, K., Shirai, T., Hiwatari, H.: On provable security of uov and hfe signature schemes against chosen-message attack. [19] 68–82
5. Huang, Y.J., Liu, F.H., Yang, B.Y.: Public-key cryptography from new multivariate quadratic assumptions. In Fischlin, M., Buchmann, J., Manulis, M., eds.: Public Key Cryptography. Volume 7293 of Lecture Notes in Computer Science., Springer (2012) 190–205
6. Clough, C., Baena, J., Ding, J., Yang, B.Y., Chen, M.S.: Square, a New Multivariate Encryption Scheme. In Fischlin, M., ed.: CT-RSA. Volume 5473 of Lecture Notes in Computer Science., Springer (2009) 252–264
7. Baena, J., Clough, C., Ding, J.: Square-vinegar signature scheme. PQCRYPTO 2008, LNCS **5299** (2008) 17–30
8. Billet, O., Macario-Rat, G.: Cryptanalysis of the square cryptosystems. ASIACRYPT 2009, LNCS **5912** (2009) 451–486
9. Dubois, V., Fouque, P.A., Shamir, A., Stern, J.: Practical Cryptanalysis of SFLASH. In Menezes, A., ed.: CRYPTO. Volume 4622 of Lecture Notes in Computer Science., Springer (2007) 1–12
10. Shamir, A., Kipnis, A.: Cryptanalysis of the oil & vinegar signature scheme. CRYPTO 1998. LNCS **1462** (1998) 257–266
11. Smith-Tone, D.: On the differential security of multivariate public key cryptosystems. [19] 130–142
12. Patarin, J.: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88. Crypto 1995, Springer **963** (1995) 248–261
13. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature verification and message-encryption. Eurocrypt '88, Springer **330** (1988) 419–545
14. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. EUROCRYPT 1999. LNCS **1592** (1999) 206–222
15. Patarin, J.: The oil and vinegar algorithm for signatures. Presented at the Dagsthul Workshop on Cryptography (1997)

16. Ding, J., Dubois, V., Yang, B.Y., Chen, C.H.O., Cheng, C.M.: Could SFLASH be Repaired? In Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I., eds.: ICALP (2). Volume 5126 of Lecture Notes in Computer Science., Springer (2008) 691–701
17. Bettale, L., Faugère, J.C., Perret, L.: Cryptanalysis of multivariate and odd-characteristic hfe variants. In Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A., eds.: Public Key Cryptography. Volume 6571 of Lecture Notes in Computer Science., Springer (2011) 441–458
18. Ding, J., Kleinjung, T.: Degree of regularity for hfe-. IACR Cryptology ePrint Archive **2011** (2011) 570
19. Yang, B.Y., ed.: Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings. In Yang, B.Y., ed.: PQCrypto. Volume 7071 of Lecture Notes in Computer Science., Springer (2011)