Differential Properties of the *HFE* Cryptosystem

Taylor Daniels[1] and Daniel Smith-Tone[1,2]

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

tsdani02@louisville.edu, daniel.smith@nist.gov

Abstract. Multivariate Public Key Cryptography (MPKC) has been put forth as a possible post-quantum family of cryptographic schemes. These schemes lack provable security in the reduction theoretic sense, and so their security against yet undiscovered attacks remains uncertain. The effectiveness of differential attacks on various field-based systems has prompted the investigation of differential properties of multivariate schemes to determine the extent to which they are secure from differential adversaries. Due to its role as a basis for both encryption and signature schemes we contribute to this investigation focusing on the HFE cryptosystem. We derive the differential symmetric and invariant structure of the HFE central map and provide a collection of parameter sets which make HFE provably secure against a differential adversary.

1 Introduction and Outline

Along with the discovery of polytime quantum algorithms for factoring and computing discrete logarithms, see [1], came a rising interest in "quantum-resistant" cryptographic protocols. For the last two decades this interest has blossomed into a large international effort to develop post-quantum cryptography, a term which elicits visions of a post-apocalyptic world where quantum computing machines reign supreme. While progress in quantum computing indicates that such devices are not precluded by the laws of physics, it is not at all clear when we may see large-scale quantum computing devices becoming a cryptographic threat. Nevertheless, the potential and the uncertainty of the situation clearly establish the need for secure post-quantum options.

One of a few reasonable candidates for security in a quantum computing world is multivariate cryptography. We already rely heavily on the difficulty of inverting nonlinear systems of equations in symmetric cryptography, and we quite reasonably suspect that that security will remain in the quantum paradigm. Multivariate Public Key Cryptography (MPKC) has the added challenge of resisting quantum attack in the asymmetric setting.

While it is difficult to be assured of a cryptosystems's post-quantum security in light of the continual evolution of the relatively young field of quantum algorithms, it is reasonable to start by developing schemes which resist classical attack and for which there is no known significant weakness in the quantum realm. Furthermore, the establishment of security metrics provide insight which educate us about the possibilities for attacks and the correct strategies for the development of cryptosystems.

In this vein, some classification metrics are introduced in [2, 3] which can be utilized to rule out certain classes of attacks. While not reduction theoretic attacks, reducing the task of breaking the scheme to a known (or often suspected) hard problem, these metrics can be used to prove that certain classes of attacks fail or to illustrate specific computational challenges which an adversary must face to effect an attack.

Many attacks on multivariate public key cryptosystems can be viewed as differential attacks, in that they utilize some symmetric relation or some invariant property of the public polynomials. These attacks have proved effective in application to several cryptosystems. For instance, the attack on SFLASH, see [4], is an attack utilizing differential symmetry, the attack of Kipnis and Shamir [5] on the oil-and-vinegar scheme is actually an attack exploiting a differential invariant, even Patarin's initial attack on C^* [6] can be viewed as an exploitation of a trivial differential symmetry, see [3]. These attacks are evidence that the work in [2, 3] is worthy of continuation and further development.

This task leads us to an investigation of the HFE cryptosystem, see [7], and a characterization of its differential properties. Results similar to those of [2, 3] will allow us to make conclusions about the differential security of HFE, and provide some insight into the properties of some of its variants such as HFE^- and $HFEv^-$, see [8] and [9].

To this end, we derive the differential symmetry and differential invariant structure of HFE. Specifically, we are able to bound the probability that an HFE primitive has a nontrivial differential structure and to provide parameter sets for which HFE is provably secure against a differential adversary. In conjunction with degree of regularity results such as [10, 11], these results provide a proof of security against all known attacks of any form as well as any future differential attack.

The paper is organized as follows. First, we recall the HFE scheme from [7]. In the following section, we provide criteria for the nonexistence of a linear differential symmetric relation on the private key. We next review the notion of a differential invariant and a method of classifying differential invariants. We continue, analyzing the differential invariant structure of HFE, deriving bounds on probability of the existence of a nontrivial differential invariant in the general case. Finally, we conclude, noting parameters which provide provable differential security.

2 HFE

The Hidden Field Equations (HFE) scheme was first presented by Patarin in [7] as a method of avoiding his linearization equations attack on the C^* scheme of Matsumoto and Imai, see [6] and [12]. The basic idea of the system is to use the butterfly construction to hide an easily invertible polynomial over an extension field.

More specifically, let $\mathbb{F}_q$ be a finite field and let $\mathbb{K}$ be a degree n extension of $\mathbb{F}_q$. Given an easily invertible "quadratic" map $f : \mathbb{K} \to \mathbb{K}$, quadratic in the sense that f is a sum of products of pairs of $\mathbb{F}_q$-linear functions of x, one constructs a system of quadratic formulae over $\mathbb{F}_q$ by composing two $\mathbb{F}_q$-affine transformations $T, U : \mathbb{K} \to \mathbb{K}$ thusly, $P = T \circ f \circ U$, and then expressing the composition over the base field, $\mathbb{F}_q$. Explicitly any such "core" map f has the form:

$$f(x) = \sum_{\substack{i \leq j \\ q^i + q^j < D}} \alpha_{i,j} x^{q^i + q^j} + \sum_{\substack{i \\ q^i < D}} \beta_i x^{q^i} + \gamma,$$

with the degree bound D established to allow for easy inversion.

To encrypt given the public key $P(x)$, one simply evaluates every public polynomial at the plaintext vector $x \in \mathbb{F}_q^n \approx \mathbb{K}$. Decryption is accomplished by inverting each of the three private components individually. The most interesting inversion is that of f, which is inverted via a polynomial system solver such as the Berlekamp algorithm.

3 Linear Differential Symmetry

The discrete differential of a field map $f : \mathbb{K} \to \mathbb{K}$ is given by:

$$Df(y, x) = f(x + y) - f(x) - f(y) + f(0).$$

It is simply a normalized difference equation with variable interval. In [4], the SFLASH signature scheme was broken by exploiting a symmetric relation of the differential of the public key. This relation was inherited from the core map of the scheme. Specifically, a linear differential symmetry is an equation in which linear maps are applied to the differential in such a way that the equation is linear in the unknown coefficients of the linear maps. We can always express the symmetry in the following form:

$$Df(My, x) + Df(y, Mx) = \Lambda_M Df(y, x), \tag{1}$$

where M and Λ_M are linear maps. To evaluate the potential for a differential symmetric attack on HFE, we consider conditions for the existence of a linear differential symmetry on the core map f of an HFE scheme.

Consider the differential of the core map:

$$Df(y, x) = \sum_{\substack{i \leq j \\ q^i + q^j < D}} \alpha_{i,j} (y^{q^i} x^{q^j} + y^{q^j} x^{q^i}). \tag{2}$$

Df is a $\mathbb{K}$-bilinear form. We choose a convenient representation for $\mathbb{K}$:

$$x \mapsto \begin{bmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{bmatrix}.$$

Under this representation we can express Df as the $n \times n$ symmetric matrix with (i,j)th and (j,i)th entries $\alpha_{i,j}$ for $i \neq j$ and (i,i)th entry $2\alpha_{i,i}$ (which may be zero depending on the characteristic of $\mathbb{K}$).

Since any linear map $M : \mathbb{K} \to \mathbb{K}$ can be written $Mx = \sum_{i=0}^{n-1} m_i x^{q^i}$, under our representation M can be expressed:

$$M = \begin{bmatrix} m_0 & m_1 & \dots & m_{n-1} \\ m_{n-1}^q & m_0^q & \dots & m_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ m_1^{q^{n-1}} & m_2^{q^{n-1}} & \dots & m_0^{q^{n-1}} \end{bmatrix}.$$

In this representation, we have the formula

$$Df(My, x) + Df(y, Mx) = y(M^T Df + DfM)x.$$

Consider the action of Λ_M on Df. $\Lambda_M Df(y,x) = \sum_{k=0}^{n-1} \lambda_k Df(y,x)^{q^k}$. Notice specifically that in our representation the matrix for Df^{q^k} is the same as the matrix representing Df shifted to the right and down k units with all entries raised to the q^kth power. This shift is due to the fact that

$$Df(y,x)^{q^k} = \sum_{\substack{i \leq j \\ q^i + q^j < D}} \alpha_{i,j}^{q^k} (y^{q^{i+k}} x^{q^{j+k}} + y^{q^{j+k}} x^{q^{i+k}}).$$

Specifically, the (i,j)th entry of Df^{q^k} is $\alpha_{i-k,j-k}^{q^k}$ if $i \neq j$, and (i,i)th entry $(2\alpha_{i-k,i-k})^{q^k} = 2\alpha_{i-k,i-k}^{q^k}$ (0 in characteristic two).

Thus the possibility of a differential symmetry can be deduced simply by setting the matrix $M^T Df + DfM$ equal to the matrix $\Lambda_M Df$. With certain constraints it is easy to deduce whether there exists a solution.

Theorem 1 *Let $f(x)$ be an HFE polynomial (in particular f is not a monomial function). Suppose that f has the following properties:*

1. *no power of q is repeated among the exponents of f, and*
2. *the difference of the powers of q in each exponent is unique.*

Then f has no nontrivial differential symmetry.

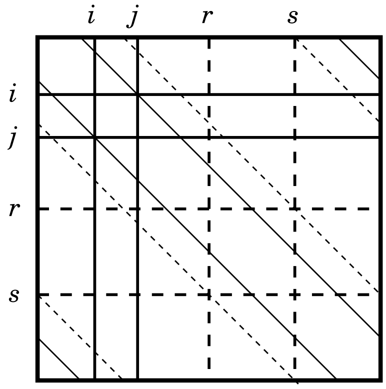

Fig. 1. Graphical representation of the equation $M^T Df + DfM = \Lambda_M Df$ for the HFE polynomial $f(x) = \alpha_{i,j}x^{q^i+q^j} + \alpha_{r,s}x^{q^r+q^s}$. Horizontal and vertical lines represent nonzero entries in $M^T Df + DfM$ while diagonal lines represent nonzero entries in $\Lambda_M Df$. Solid lines correspond to the (i, j) monomial while dotted lines correspond to the (r, s) monomial.

Proof. First consider computing DfM. From the condition on the monomials of f, Df has at most a single nonzero entry in any row or column. Therefore each row of DfM is a multiple of a row in M. In particular, if $\alpha_{i,j}x^{q^i+q^j}$ is a monomial of f, then the ith row of DfM is

$$\left[\alpha_{i,j}m_{-j}^{q^j}\ \alpha_{i,j}m_{1-j}^{q^j}\ \dots\ \alpha_{i,j}m_{-1-j}^{q^j}\right],$$

and the jth row is

$$\left[\alpha_{i,j}m_{-i}^{q^i}\ \alpha_{i,j}m_{1-i}^{q^i}\ \dots\ \alpha_{i,j}m_{-1-i}^{q^i}\right].$$

Consider the ith row of $M^T Df + DfM$. For all k not occurring as a power of q in f, the (i, k)th entry is $\alpha_{i,j}m_{k-j}^{q^j}$. Consider the (i, j)th entry of $M^T Df + DfM$. This quantity is the sum of the (i, j)th entry of DfM and the (j, i)th entry, specifically $\alpha_{i,j}(m_0^{q^i} + m_0^{q^j})$. Let $\alpha_{r,s}x^{q^r+q^s}$ be another monomial of f. Then the (i, r)th entry of $M^T Df + DfM$ is $\alpha_{i,j}m_{r-j}^{q^j} + \alpha_{r,s}m_{i-s}^{q^s}$, and the (i, s)th entry is $\alpha_{i,j}m_{s-j}^{q^j} + \alpha_{r,s}m_{i-r}^{q^r}$.

In $\Lambda_M Df$, for all $\alpha_{i,j}x^{q^i+q^j}$ a monomial in f, the $(i + k, j + k)$th entry is equal to the $(j + k, i + k)$th entry and takes the value $\alpha_{i,j}^{q^k}\lambda_k$ while all other entries are zero.

Therefore consider the elements in the ith row of the equation $M^T Df + DfM = \Lambda_M Df$. For every monomial $\alpha_{r,s}x^{q^r+q^s}$ in f, we have that the $s-r+i$th element and the $r - s + i$th element of row i in $\Lambda_M Df$ are nonzero. All other entries of that row are zero. Therefore, for all k not occurring as a power of q in f or as a difference of the powers of q in an exponent of a monomial in f

plus i, $m_{k-j} = 0$. Given the condition that the differences of powers of q in the exponents are unique, and the equations $m_{k-t} = 0$ for all other t occurring as powers of q, we obtain $m_i = 0$ for all $i \neq 0$. Therefore M is a multiplication map. But as proven in Theorem 2 in [13], if $m_0 \notin \mathbb{F}_q$ this implies that the polynomial is a C^* monomial, a contradiction. Thus M is simply multiplying by a scalar which induces a symmetry for every map $g : \mathbb{K} \to \mathbb{K}$. Thus f has no nontrivial differential symmetry.

We note that the conditions of the above theorem are very easy to satisfy in actual implementations, though for very small D there may be some issues regarding a lack of entropy in the private key space. With proper selection of the extension, however, it is unlikely that this adjustment will lead to a successful attack based on the isomorphism of polynomials problem, see [7].

4 Differential Invariants

4.1 Setup

The discrete differential Df is a symmetric, bilinear *function* on $\mathbb{F}_q^n$ (using the vector space representation of $\mathbb{K}$), but each coordinate of Df is a symmetric, bilinear *form* on $\mathbb{K}$. Because of this, we may express each coordinate of Df, $[Df(y,x)]_i$ as

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

Maintaining our definitions of $\mathbb{K}$ and f, we define a "first order differential invariant" of f.

Definition 1 *Let $f : \mathbb{K} \to \mathbb{K}$ be a function. A* differential invariant *of f is a subspace $V \subseteq \mathbb{K}$ with the property that there is a subspace $W \subseteq \mathbb{K}$ such that $dim(W) \leq dim(V)$ and $\forall A \in Span_{\mathbb{F}_q}(Df_i)$, $AV \subseteq W$.*

Informally speaking, a function has a differential invariant if the image of a subspace under all differential coordinate forms lies in a fixed subspace of dimension no larger. This definition captures the notion of *simultaneous invariants*, subspaces which are simultaneously invariant subspaces of Df_i for all i, and detects when large subspaces are acted upon linearly.

If we assume the existence of a first order differential invariant V, we can define a corresponding subspace $V^\perp$ as the set of all elements $x \in \mathbb{K}$ such that the dot product $\langle x, Av \rangle = 0$ $\forall v \in V, \forall A \in Span(Df_i)$. This is not quite the usual definition of an orthogonal complement. $V^\perp$ is not the set of everything orthogonal to V, but rather everything orthogonal to AV, which may or may not be in V.

With our definitions of V and $V^\perp$, we can establish the following useful result. Assume there is a first order differential invariant $V \subseteq \mathbb{K}$, and pick a linear projection $M : \mathbb{K} \to V$ and another linear projection $M^\perp : \mathbb{K} \to V^\perp$. Examining one of the differential coordinate-forms,

$$[Df(M^\perp y, Mx)]_i = (M^\perp y)^T \left(Df_i(Mx)\right) \tag{3}$$

Since $M^{\perp}y$ is in $V^{\perp}$, and $Df_i Mx \in AV$, we must then have that

$$[Df(M^{\perp}y, Mx)]_i = (M^{\perp}a)^T\,(Df_i(Mx)) = 0 \tag{4}$$

The "i" in Df_i did not matter, meaning that for all i (from 1 to n), i.e. for all coordinates of Df, the above equation is true. We can then simply say that:

$$\forall y, x \in \mathbb{K}, Df(M^{\perp}y, Mx) = 0 \quad \text{or equivalently,} \quad Df(M^{\perp}\mathbb{K}, M\mathbb{K}) = 0 \tag{5}$$

This fact will restrict what M and $M^{\perp}$ can be.

4.2 $M^{\perp} = SMT$

We can make our investigation of $M, M^{\perp}$ easier by employing a small result from linear algebra. Our idea is to express $M^{\perp} = SMT$, where S may be singular, but T is nonsingular (or vice versa if $rank(M) < rank(M^{\perp})$). The result we use is:

Proposition 1. *If A, B are two $m \times n$ matrices, then $rank(A) = rank(B)$ if and only if there exist nonsingular matrices C, D, such that $A = CBD$.*

Proof. Let A be an $m \times n$ matrix of rank r. With row operations $(P, m \times m)$ we can get A into row echelon form, PA. Then we can use column operations $(Q, n \times n)$ to "zero-out" the remaining nonleading elements and permute the leading 1's to the first r columns. Thus PAQ is the $m \times n$ matrix with the $r \times r$ identity matrix in the upper-left region, and zeros everywhere else. Denote this matrix as I'. Thus $PAQ = I'$. We can also do this with B, so that $P'BQ' = I' = PAQ$. Thus $A = (P^{-1}P')B(Q'Q^{-1})$, with $P^{-1}P'$ and $Q'Q^{-1}$ nonsingular.

Without loss of generality, due to the symmetry of Df, we may assume that $rank(M^{\perp}) \leq rank(M)$. If the ranks are equal, then we may apply the proposition and write $M^{\perp} = SMT$, with S and T nonsingular. If $rank(M^{\perp}) < rank(M)$, compose M with a singular matrix X so that $rank(XM) = rank(M^{\perp})$, and *then* apply the result so that $M^{\perp} = S(XM)T$. Then we can express $M^{\perp} = S'MT$, where S' is singular. The matrix T is included to ensure that the kernels of $M, M^{\perp}$ are properly aligned. Restating our differential result (5) in this manner, we have that if $M^{\perp} = SMT$, and $M : \mathbb{K} \to V$, then

$$\forall x, y \in \mathbb{K}, Df(SMTy, MTx) = 0 \tag{6}$$

4.3 Minimal Polynomial

Definition 1. *We define the* minimal polynomial *of a subspace $V \subseteq \mathbb{K}$ as*

$$\mathcal{M}_V(x) = \prod_{v \in V}(x - v)$$

The term "minimal polynomial" is used since this is the polynomial of minimal degree of which every element of V is a root. We note that the equation $\mathcal{M}_V(x) = 0$ is an $\mathbb{F}_q$-linear equation.

Suppose that V has $\mathbb{F}_q$-dimension d, so that $|V| = q^d$. Then $\mathcal{M}_V(x)$ has degree q^d and, in keeping with our previous descriptions, must have form

$$x^{q^d} + b_{d-1}x^{q^{d-1}} + \cdots + b_2x^{q^2} + b_1x^q + b_0x \quad b_i \in \mathbb{K} \tag{7}$$

More generally, we can characterize all functions from V to $\mathbb{K}$:

Proposition 2. *Let $\mathcal{F}_V$ be the ring of all functions from the $\mathbb{F}_q$-subspace V of $\mathbb{K}$ to $\mathbb{K}$. Then $\mathcal{F}_V$ is isomorphic to $\mathbb{K}[x]/\left\langle \mathcal{M}_V(x)\right\rangle$.*

Proof. The ring of all functions from $\mathbb{K}$ to itself is $\mathbb{K}[x]/\left\langle x^{q^n} - x\right\rangle$. Suppose that $f, g \in \mathbb{K}[x]/\left\langle x^{q^n} - x\right\rangle$ are identical on V. Then for all $v \in V$, v is a root of $(f-g)(x)$. Thus $(x-v)$ is a linear factor of $(f-g)(x)$ for all $v \in V$. Thus $\mathcal{M}_V(x)|(f-g)(x)$. Consequently, $\left\langle \mathcal{M}_V(x)\right\rangle$ is the ideal of functions which send V to zero. Thus $\mathbb{K}[x]/\left\langle x^{q^n} - x, \mathcal{M}_V(x)\right\rangle$ is the ring of nontrivial functions from V to $\mathbb{K}$. Since $\mathcal{M}_V(x)$ splits in $\mathbb{K}$, $\mathcal{M}_V(x)|x^{q^n} - x$. To see that all functions from V to $\mathbb{K}$ are polynomials note that there are $(q^n)^{q^d}$ functions from V (of $\mathbb{F}_q$-dimension d) to $\mathbb{K}$, and $|\mathbb{K}[x]/\left\langle \mathcal{M}_V(x)\right\rangle| = (q^n)^{q^d}$.

4.4 Differential Invariant Structure of HFE

If f has non-trivial invariant V we know that $\forall A \in Span(Df_i)$, $dim(AV) \leq dim(V)$. Since the dot-product is non-degenerate on $\mathbb{K}$, and remembering that $V^\perp$ is defined slightly differently, we can say $dim(V^\perp) + dim(AV) = n$. This fact implies that $dim(V^\perp) + dim(V) \geq n$, so either $dim(V^\perp) \geq n/2$ or $dim(V) \geq n/2$, possibly both.

If $dim(V) \geq n/2$, we maintain $MT : \mathbb{K} \to V$ and characterize $S : V \to V^\perp$. If we deduce S maps V to $\{0\}$, that is, $V^\perp = \{0\}$, this would mean $dim(AV) = n$ and consequently $AV = \mathbb{K}$. If $V \neq \mathbb{K}$, we contradict $dim(AV) \leq dim(V)$, and if $V = \mathbb{K}$, we contradict the non-triviality of V.

If $dim(V^\perp) \geq n/2$, we take $M'T' : \mathbb{K} \to V^\perp$ instead and characterize $S' : V^\perp \to V$. If S' is the zero map on $V^\perp$, i.e. $S'V^\perp = V = \{0\}$, then we contradict the non-triviality of V.

Without loss of generality we assume $dim(V) \geq n/2$ because the following analysis and results can be achieved just as easily if we have $dim(V^\perp) \geq n/2$.

For notational convenience, we now fix $MTx = \hat{x}$, $MTy = \hat{y}$, and $MT\mathbb{K} = V$. Starting with the core map

$$f(x) = \sum_{\substack{i \leq j \\ q^i + q^j < D}} \alpha_{i,j} x^{q^i + q^j} + \sum_{\substack{i \\ q^i < D}} \beta_i x^{q^i} + \gamma,$$

we compute:

$$Df(S\hat{y}, \hat{x}) = \sum_{\substack{i \leq j \\ q^i + q^j < D}} \alpha_{i,j} \left[(S\hat{y})^{q^i} \hat{x}^{q^j} + (S\hat{y})^{q^j} \hat{x}^{q^i} \right]. \tag{8}$$

For practical parameters, D is far smaller than $|V|$, see for example [7], and so for $Df(S\hat{y},\hat{x})=0$, every coefficient of $\hat{x}^{q^j}$ must be in $\langle\mathcal{M}_V(\hat{y})\rangle$. Expanding (8) we obtain:

$$\begin{aligned} D(S\hat{y},\hat{x}) &= \sum_{\substack{i\le j\\ q^i+q^j<D}} \alpha_{i,j}\left[(S\hat{y})^{q^i}\hat{x}^{q^j}+(S\hat{y})^{q^j}\hat{x}^{q^i}\right] \\ &= \sum_{\substack{i,j\\ q^i+q^j<D}} \left[(\alpha_{i,j}+\alpha_{j,i})\,(S\hat{y})^{q^i}\right]\hat{x}^{q^j}, \end{aligned} \tag{9}$$

where we specifically note in the last expression that if $i\neq j$ exactly one of $\alpha_{i,j}$ and $\alpha_{j,i}$ may be nonzero. Thus for each j such that $q^j<D$ we have the following polynomial:

$$\sum_{i:q^i+q^j<D}(\alpha_{i,j}+\alpha_{j,i})(S\hat{y})^{q^i}. \tag{10}$$

The membership of the jth polynomial of the form (10) in $\langle\mathcal{M}_V(\hat{y})\rangle$ provides the relation

$$\sum_{i:q^i+q^j<D}(\alpha_{i,j}+\alpha_{j,i})(S\hat{y})^{q^i}=0. \tag{11}$$

Relation (11) has $\ell=\lfloor log_q(D)\rfloor$ degrees of freedom on S as a linear action on V. Therefore, there are $d-\ell$ $\mathbb{F}_q$-linearly independent relations on S from a single monomial of (9). For a practically chosen D, two linearly independent relations of this form on S force S to be the zero map on V. Consequently, we have that $V^\perp=\{0\}$, a contradiction. Specifically, the probability that two such given relations are independent is approximately $1-q^{-n\ell}$; thus with very high probability f has no differential invariant structure.

In particular, we provide a specific strategy for provably eliminating differential invariants.

Theorem 2 *Let f be an HFE polynomial with degree bound $D<q^{n/2}$. If there is a power of q which is unique, f has no non-trivial invariant structure.*

Proof. Assume by way of contradiction that f has a non-trivial differential invariant. Let j be the unique power of q occurring in an exponent in f. By the above discussion it suffices to analyze membership of the jth polynomial of the form (10) in $\langle\mathcal{M}_V(\hat{y})\rangle$. Given the condition on j, this polynomial has the form $(\alpha_{rj}+\alpha_{jr})(S\hat{y})^{q^r}$. If this polynomial is in $\langle\mathcal{M}_V(\hat{y})\rangle$, then so is $S\hat{y}$, since $\mathcal{M}_V(\hat{y})$ has no repeated factors, and we have $SV=\{0\}$, a contradiction.

5 IP, Degree of Regularity, Other Factors

The restrictions suggested in Theorems 1 and 2 reduce the entropy of the private key space, which might raise concerns about vulnerability to attacks based on a “guess-then-IP” strategy, or to direct inversion via Gröbner bases. As it turns out, for even modest parameters these issues are not realized.

Consider, for example, using the parameter set for HFE Challenge 2 without the minus modification; specifically, we have $q = 16, n = 36$, and $D = 4352 = 16^2 + 16^3$. Thus $\mathbb{K} = \mathbb{F}_{16^{36}}$, and our HFE map must have the form :

$$\begin{aligned} f(x) = \quad & \alpha_{0,0}x^{q^0+q^0} + \alpha_{0,1}x^{q^0+q^1} + \alpha_{1,1}x^{q^1+q^1} + \alpha_{0,2}x^{q^0+q^2} + \alpha_{1,2}x^{q^1+q^2} \\ & + \alpha_{2,2}x^{q^2+q^2} + \alpha_{0,3}x^{q^0+q^3} + \alpha_{1,3}x^{q^1+q^3} + \beta_0 x^{q^0} \\ & + \beta_1 x^{q^1} + \beta_2 x^{q^2} + \beta_3 x^{q^3} + \gamma \end{aligned}$$

We may choose $\alpha_{1,2}$ and $\alpha_{0,3}$ to be the only non-zero α, so that no exponents are repeated and the differences $2-1 = 1$ and $3-0 = 3$ are unique. By Theorems 1 and 2, f has no nontrivial differential structure, and is therefore secure against any differential adversary. The private key space is reduced from containing q^{13n} HFE polynomials to only containing q^{7n} such maps.

For weak parameters, in particular when the $\alpha_{i,j}$ are chosen from the base field, an attack based on the IP problem is presented in [14]. The symmetries used in that method, however, are not present when both $\alpha_{1,2}$ and $\alpha_{0,3}$ are chosen randomly from $\mathbb{K}$. While we may consider the coefficient of $\alpha_{1,2}$ to be "absorbed" by the affine map T, the effect of the remaining coefficient breaks the symmetry. Without the commutativity of the Frobenius map with the HFE polynomial, the parameters supplied are out of range for an IP-based attack.

Another concern is that the rank of the scheme may be so low as to make the scheme susceptible to attack via Gröbner basis methods. However, using the theorem from [11], we compute the degree of regularity of the adjusted scheme to be:

$$\frac{(16-1)4}{2} + 2 = 32,$$

based on the fact that the rank of the central map is only four. Using the formula from [15], we obtain an estimated complexity of

$$\binom{36+32}{32}^{\omega}$$

where $\omega = 2.3766$. Thus, we estimate the complexity of directly inverting this concrete example to be $O(2^{153})$.

6 Conclusion

HFE is the oldest surviving mainstream multivariate public key cryptosystem. For eighteen years, it has been studied, influencing cryptanalysis, symbolic computation, and the development of new cryptographic schemes. As a platform for the development of various signature schemes, HFE has excelled, utilizing several modifiers to spawn new systems, some of which are leading candidates for secure post-quantum signatures.

Our analysis contributes to the HFE legacy, elucidating the differential structure inherent to the scheme. The results indicate that given practical parameters, HFE systems lack non-trivial differential invariant structure. Further, we have established that with a simple choice of parameters we can *provably* eliminate non-trivial differential symmetric and invariant structure while maintaining security against attacks exploiting a diminished private key space. Thus, HFE is provably secure against a differential adversary.

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Sci. Stat. Comp. **26, 1484** (1997)
2. Smith-Tone, D.: On the differential security of multivariate public key cryptosystems. In Yang, B.Y., ed.: PQCrypto. Volume 7071 of Lecture Notes in Computer Science., Springer (2011) 130–142
3. Perlner, R.A., Smith-Tone, D.: A classification of differential invariants for multivariate post-quantum cryptosystems. In Gaborit, P., ed.: PQCrypto. Volume 7932 of Lecture Notes in Computer Science., Springer (2013) 165–173
4. 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
5. Shamir, A., Kipnis, A.: Cryptanalysis of the oil & vinegar signature scheme. CRYPTO 1998. LNCS **1462** (1998) 257–266
6. Patarin, J.: Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In Coppersmith, D., ed.: CRYPTO. Volume 963 of Lecture Notes in Computer Science., Springer (1995) 248–261
7. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: EUROCRYPT. (1996) 33–48
8. Patarin, J., Goubin, L., Courtois, N.: C^{*}_{-+} and HM: Variations around two schemes of T.Matsumoto and H.Imai. Asiacrypt 1998, Springer **1514** (1998) 35–49
9. Patarin, J., Courtois, N., Goubin, L.: Quartz, 128-bit long digital signatures. In Naccache, D., ed.: CT-RSA. Volume 2020 of Lecture Notes in Computer Science., Springer (2001) 282–297
10. Dubois, V., Gama, N.: The degree of regularity of hfe systems. In Abe, M., ed.: ASIACRYPT. Volume 6477 of Lecture Notes in Computer Science., Springer (2010) 557–576
11. Ding, J., Hodges, T.J.: Inverting hfe systems is quasi-polynomial for all fields. In Rogaway, P., ed.: CRYPTO. Volume 6841 of Lecture Notes in Computer Science., Springer (2011) 724–742
12. Matsumoto, T., Imai, H.: Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In: EUROCRYPT. (1988) 419–453
13. Smith-Tone, D.: Properties of the discrete differential with cryptographic applications. In Sendrier, N., ed.: PQCrypto. Volume 6061 of Lecture Notes in Computer Science., Springer (2010) 1–12
14. Bouillaguet, C., Fouque, P.A., Joux, A., Treger, J.: A family of weak keys in hfe and the corresponding practical key-recovery. J. Mathematical Cryptology **5** (2012) 247–275
15. Bardet, M., Faugere, J.C., Salvy, B.: On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving. (2004)