On the Differential Security of the $HFEv^-$ Signature Primitive

Ryann Cartor[1], Ryan Gipson[1], Daniel Smith-Tone[1,2], and Jeremy Vates[1]

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

ryann.cartor@louisville.edu, ryan.gipson@louisville.edu,
jeremy.vates@louisville.edu, daniel.smith@nist.gov

Abstract. Multivariate Public Key Cryptography (MPKC) is one of the most attractive post-quantum options for digital signatures in a wide array of applications. The history of multivariate signature schemes is tumultuous, however, and solid security arguments are required to inspire faith in the schemes and to verify their security against yet undiscovered attacks. The effectiveness of "differential attacks" on various field-based systems has prompted the investigation of the resistance of schemes against differential adversaries. Due to its prominence in the area and the recent optimization of its parameters, we prove the security of $HFEv^-$ against differential adversaries. We investigate the newly suggested parameters and conclude that the proposed scheme is secure against all known attacks and against any differential adversary.

Key words: Multivariate Cryptography, HFEv-, Discrete Differential, MinRank, Q-rank

1 Introduction and Outline

In the mid 1990s, Peter Shor discovered a way to efficiently implement quantum period finding algorithms on structures of exponential size and showed how the modern world as we know it will change forever once the behemoth engineering challenge of constructing a large scale quantum computing device is overcome. His polynomial time quantum Fourier transforms for smooth integers can be employed to factor integers, to compute discrete logarithms and is powerful enough to efficiently solve hidden subgroup problems for well behaved (usually Abelian) groups. Given the ubiquity of these problems in deployed technologies, our e-society is confronted with the possibility that its public key infrastructure is terminally ill.

It is not known how far this computational cancer may spread, how pervasive exponential quantum speed-ups will prove to be nor how fundamentally wide the gap between feasibility in the classical and quantum world are. Thus we

face the task in a rapidly maturing twenty-first century, with ever expanding interconnectivity, of securing open channel communication between unknown future devices, against machines with unknown capabilities, with an unknown date of inception.

Charged with this challenge is a growing international community of experts in quantum-resistant cryptography. The world-wide effort has spawned international standardization efforts including the European Union Horizon 2020 Project, "Post-Quantum Cryptography for Long-Term Security" PQCRYPTO ICT-645622 [1], ETSI's Quantum Safe Cryptography Specification Group [2], and NIST's Post-Quantum Cryptography Workgroup [3]. The dedication of these resources is evidence that the field of post-quantum cryptography is evolving into a state in which we can identify practical technologies with confidence that they will remain secure in a quantum computing world.

One of a few reasonable candidates for post-quantum security 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 cryptosystem'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 provides insight that educates us about the possibilities for attacks and the correct strategies for the development of cryptosystems.

In this vein, some classification metrics are introduced in [4–6] which can be utilized to rule out certain classes of attacks. While not reduction theoretic proof, 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 [7], is an attack utilizing differential symmetry, the attack of Kipnis and Shamir [8] on the oil-and-vinegar scheme is actually an attack exploiting a differential invariant, the attack on the ABC matrix encryption scheme of [9] utilizes a subspace differential invariant; even Patarin's initial attack on C^* [10] can be viewed as an exploitation of a trivial differential symmetry, see [5].

As is demonstrated in [4, 6, 11], many general polynomial schemes can have nontrivial linear differential symmetries. Specifically, in [6], systems of linear equations are presented which can have solution spaces large enough to guarantee the existence of nontrivial linear differential symmetries, while in both [4] and

[11] explicit constructions of maps with nontrivial symmetries are provided. The existence of such symmetries in abundance is the basis of attacks removing the minus modifier as in [7], and depending on the structure of the maps inducing the symmetry, may even provide a direct key recovery attack. Furthermore, the attack of [9] on the ABC simple matrix scheme teaches us that differential invariant techniques are a current concern as well. These facts along with the ubiquity of differential attacks in the literature are evidence that the program developed in [4–6] to verify security against differential adversaries is a necessary component of any theory of security for practical and desirable multivariate cryptosystems.

This challenge leads us to an investigation of the $HFEv$ and $HFEv^-$ cryptosystems, see [12], and a characterization of their differential properties. Results similar to those of [4–6] will allow us to make conclusions about the differential security of $HFEv$, and provide a platform for deriving such results for $HFEv^-$.

Specifically, we reduce the task of verifying trivial differential symmetric structure for a polynomial f to the task of verifying that the solution space of a large system of linear equations related to f has a special form. We elucidate the structure of these equations in the case of the central map of $HFEv$ and provide an algorithm for generating keys which provably have trivial differential symmetric structure. In conjunction with our later results on differential invariants, the proof of concept algorithm verifies that information theoretic security against differential adversaries, as defined in [6], is possible with an instantaneous addition to key generation while maintaining sufficient entropy in the key space to avoid "guess-then-IP" attacks. We then extend these methods to the case of $HFEv^-$, deriving the same conclusion.

Expanding on the methods of [6], we prove the following.

Theorem 1 *Let k be a degree n extension of the finite field $\mathbb{F}_q$. Let f be an $HFEv$ central maps. With high probability, f has no nontrivial differential invariant structure.*

With a minimal augmentation of this method we extend this result to the case of $HFEv^-$.

Theorem 2 *Let f be an $HFEv$ central map and let π be a linear projection. With high probability, $\pi \circ f$ has no nontrivial differential invariant structure.*

Thus, with proper parameter selection, $HFEv^-$ is provably secure against differential adversaries. Together with the existant literature on resistance to algebraic and rank attacks, this security argument provides significant theoretical support for the security of aggressive $HFEv^-$ parameters, such as those presented in [13].

The paper is organized as follows. First, we recall big field constructions in multivariate public key cryptography. Next we review the HFE scheme from [14] and the $HFEv^-$ scheme from [12]. In the following section, we provide criteria for the nonexistence of a differential symmetric relation on the private key of both $HFEv$ and $HFEv^-$ and discuss an efficient addition to key generation

that allows provably secure keys to be generated automatically. We next review the notion of a differential invariant and a method of classifying differential invariants. We continue, analyzing the differential invariant structure of $HFEv$ and $HFEv^-$, deriving bounds on the probability of differential invariants in the general case. Next, we review the Q-rank and degree of regularity of $HFEv^-$, and discuss resistance to attacks exploiting equivalent keys. Finally, we conclude, discussing the impact of these results on the $HFEv^-$ pedigree.

2 Big Field Signature Schemes

At Eurocrypt '88, Matsumoto and Imai introduced the first massively multivariate cryptosystem which we now call C^*, in [15]. This contribution was based on a fundamentally new idea for developing a trapdoor one-way function. Specifically, they used finite extensions of Galois fields to obtain two representations of the same function: one, a vector-valued function over the base field; the other, an univariate function over the extension field.

One benefit of using this "big field" structure, is that Frobenius operations in extensions of conveniently sized Galois fields can be modeled as permutations of elements in the small field while computations in the small field can be cleverly coded to utilize current architectures optimally. Thus, one can compute a variety of exponential maps and products with great efficiency and obfuscate a simple structure by perturbing the vector representation.

Typically, a big field scheme is built using what is sometimes called the butterfly construction. Given a finite field $\mathbb{F}_q$, a degree n extension $\mathbb{K}$, and an $\mathbb{F}_q$-vector space isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{K}$, one can find an $\mathbb{F}_q$-vector representation of the function $f : \mathbb{K} \to \mathbb{K}$. To hide the choice of basis for the input and output of f, we may compose two affine transformations $T, U : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The resulting composition $P = T \circ \phi^{-q} \circ f \circ \phi \circ U$ is then the public key. The construction is summarized in the figure below:

$$\begin{array}{ccccccc} & & \mathbb{K} & \xrightarrow{f} & \mathbb{K} & & \\ & & \phi \downarrow & & \downarrow \phi^{-1} & & \\ \mathbb{F}_q^n & \xrightarrow{U} & \mathbb{F}_q^n & \xrightarrow{F} & \mathbb{F}_q^n & \xrightarrow{T} & \mathbb{F}_q^n \end{array}$$

2.1 *HFE*

The Hidden Field Equations (HFE) scheme was first presented by Patarin in [14] as a method of avoiding his linearization equations attack which broke the C^* scheme of Matsumoto and Imai, see [10] and [15]. The basic idea of the system is to use the butterfly construction to hide the structure of a low degree polynomial that can be inverted efficiently over $\mathbb{K}$ via the Berlekamp algorithm [16], for example.

More specifically, we select an effectively invertible "quadratic" map $f : \mathbb{K} \to \mathbb{K}$, quadratic in the sense that every monomial of f is a product of a constant

and two Frobenius multiples of x. Explicitly any such "core" map f has the form:

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

The bound D on the degree of the polynomial is required to be quite low for efficient inversion.

One generates a signature by setting $y = h$, a hash digest, and computing, successively, $v = T^{-1}y$, $u = f^{-1}(v)$ and $x = U^{-1}u$. The vector x acts as the signature.

For verification, one simply evaluates the public polynomials, P, at x. If $P(x)$ which is equal to $T \circ f \circ U(x)$ is equal to y, the signature is authenticated. Otherwise, the signature is rejected.

2.2 $HFEv^-$

Taking the HFE construction one step further, we may apply the vinegar modifier, adding extra variables $\tilde{x}_1, \ldots \tilde{x}_v$ to be assigned random values upon inversion. The effect of adding vinegar variables is that new quadratic terms, formed from both products of vinegar variables and HFE variables and products among vinegar variables, increase the rank of the public key. The central map of the $HFEv$ scheme has the form:

$$f(\mathbf{x}) = \sum_{\substack{i\leq j \\ q^i+q^j\leq D}} \alpha_{i,j}x^{q^i+q^j} + \sum_{\substack{i \\ q^i\leq D}} \beta_i(\tilde{x}_1, \ldots, \tilde{x}_v)x^{q^i} + \gamma(\tilde{x}_1, \ldots, \tilde{x}_v),$$

where $\alpha_{i,j} \in \mathbb{K}$, $\beta_i : \mathbb{F}_q^v \to \mathbb{K}$ is linear, and $\gamma : \mathbb{F}_q^v \to \mathbb{K}$ is quadratic.

In contrast to HFE, f is a vector-valued function mapping $\mathbb{F}_q^{n+v}$ to $\mathbb{F}_q^n$. The work of [17, 18, 6] show that representations of such functions over $\mathbb{K}$ are quite valuable. Thus it is beneficial to employ an augmentation of f, adding $n - v$ additional vinegar variables, and say $\hat{y} = \{\tilde{x}_1, \ldots, \tilde{x}_v, \ldots, \tilde{x}_n\}$, where $\tilde{x}_{v+1} = \tilde{x}_{v+2} = \ldots = \tilde{x}_n = 0$. Thus, our core map becomes

$$f(\mathbf{x}) = \hat{f}\begin{pmatrix}\hat{x} \\ \hat{y}\end{pmatrix}.$$

which algebraically identifies f as a bivariate function over $\mathbb{K}$. We may now write f in the following form:

$$f(x,y) = \sum_{\substack{0\leq i\leq j<n \\ q^i+q^j\leq D}} \alpha_{ij}x^{q^i+q^j} + \sum_{\substack{0\leq i,j<n \\ q^i\leq D}} \beta_{ij}x^{q^i}y^{q^j} + \sum_{0\leq i\leq j<n} \gamma_{ij}y^{q^i+q^j}. \quad (1)$$

Here we see an obvious distinction among the types of monomials. We will label the monomials with α coefficients the "HFE monomials," those with β coefficients the "mixing monomials" and the monomials with γ coefficients the "vinegar monomials."

The $HFEv^-$ scheme uses the $HFEv$ primitive f above and augments the public key with the minus modifier. The minus modifier removes r of the public equations. This alteration is designed to destroy some of the information of the big field operations latent in the public key.

3 Differential Symmetry

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

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

It is simply a normalized difference operator with variable interval. In [7], 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.

Definition 1 *A* general linear differential symmetry *is a relation of the form*

$$Df(Mx, a) + Df(x, Ma) = \Lambda_M Df(a, x),$$

where $M, \Lambda_M : \mathbb{K} \to \mathbb{K}$ *are* $\mathbb{F}_q$*-linear maps.*

A differential symmetry exists when linear maps may be applied to the discrete differential inputs in such a way that the effect can be factored out of the differential. Furthermore, we say that the symmetry is *linear* when the relation is linear in the unknown coefficients of the linear maps. It can be shown that any such linear symmetric relation implies the existence of a symmetry of the above form, hence the term "general."

While attacks similar to that of [7, 19] exploited some multiplicative relation on central maps of schemes with some algebraic structure over the base field, it was shown in [4] that general linear differential symmetries based on more complex relations exist, in general. Therefore, when analyzing the potential threat of a differential adversary, as defined in [6], it becomes necessary to classify the possible linear differential symmetries. If we succeed in characterizing parameters which provably eliminate nontrivial differential symmetric relations, we prove security against the entire class of differential symmetric attacks, even those utilizing relations not yet discovered.

To this end, we evaluate the security of $HFEv$ against such adversaries. We explicitly consider parameter restrictions which necessarily preclude the existence of any nontrivial differential symmetry.

3.1 Linear Symmetry for HFEv

In our analysis, we will begin by considering the differential of our core map. From the perspective of our adversary, the discrete differential would be

$$D\hat{f}\left(\begin{bmatrix}\hat{a}\\ \hat{b}\end{bmatrix}, \begin{bmatrix}\hat{x}\\ \hat{y}\end{bmatrix}\right) = Df(a, b, x, y).$$

By the bilinearity of $D\hat{f}$ we see that Df is multi-affine; Df is affine in each of its inputs when the remaining inputs are fixed. Evaluating this differential we obtain

$$\begin{aligned} Df(a,b,x,y) = &\sum_{\substack{0\le i\le j<n \\ q^i+q^j\le D}} \alpha_{i,j}(x^{q^i}a^{q^j} + x^{q^j}a^{q^i}) \\ &+ \sum_{\substack{0\le i,j<n \\ q^i\le D}} \beta_{i,j}(x^{q^i}b^{q^j} + a^{q^i}y^{q^j}) \\ &+ \sum_{0\le i\le j<n} \gamma_{i,j}(y^{q^i}b^{q^j} + y^{q^j}b^{q^i}), \end{aligned} \tag{2}$$

noting that Df is a $\mathbb{K}$-bilinear form in $[a\ b]^T$ and $[x\ y]^T$. For ease of computation, we will choose the following representation for $\mathbb{K}$:

$$x \mapsto [x \ \ x^q \ \ x^{q^2} \ \ \ldots \ \ x^{q^{n-1}}]^T.$$

Similarly, we may map our oil-vinegar vector as

$$[x \ \ y] \mapsto [x \ \ x^q \ \ x^{q^2} \ \ \ldots \ \ x^{q^{n-1}} \ \ y \ \ y^q \ \ y^{q^2} \ \ \ldots \ \ y^{q^{n-1}}]^T,$$

and Df is thus represented by the $2n \times 2n$ matrix where the (i,j)th and (j,i)th entries in the upper left $n \times n$ block are the coefficients $\alpha_{i,j}$, and the (i,j)th entries in the upper right block and the (j,i)th entries in the lower left block are the coefficients $\beta_{i,j}$, while the (i,j)th and the (j,i)th entries in the lower right block are the coefficients $\gamma_{i,j}$.
Note, that any $\mathbb{F}_q$-linear map $M : \mathbb{K} \to \mathbb{K}$ can be represented by $Mx = \sum_{i=0}^{n-1} m_i x$. Thus, as demonstrated in [6], under our representation,

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

However, when viewing an $\mathbb{F}_q$-linear map over our vector $\begin{bmatrix} \hat{x} \\ \hat{y} \end{bmatrix}$, we may consider the $2n \times 2n$ matrix

$$\overline{M} = \begin{pmatrix} m_{00,0} & m_{00,1} & \cdots & m_{00,n-1} & m_{01,0} & m_{01,1} & \cdots & m_{01,n-1} \\ m^q_{00,n-1} & m^q_{00,0} & \cdots & m^q_{00,n-2} & m^q_{01,n-1} & m^q_{01,0} & \cdots & m^q_{01,n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m^{q^{n-1}}_{00,1} & m^{q^{n-1}}_{00,2} & \cdots & m^{q^{n-1}}_{00,0} & m^{q^{n-1}}_{01,1} & m^{q^{n-1}}_{01,2} & \cdots & m^{q^{n-1}}_{01,0} \\ m_{10,0} & m_{10,1} & \cdots & m_{10,n-1} & m_{11,0} & m_{11,1} & \cdots & m_{11,n-1} \\ m^q_{10,n-1} & m^q_{10,0} & \cdots & m^q_{10,n-2} & m^q_{11,n-1} & m^q_{11,0} & \cdots & m^q_{11,n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ m^{q^{n-1}}_{10,1} & m^{q^{n-1}}_{10,2} & \cdots & m^{q^{n-1}}_{10,0} & m^{q^{n-1}}_{11,1} & m^{q^{n-1}}_{11,2} & \cdots & m^{q^{n-1}}_{11,0} \end{pmatrix}.$$

For computational reference, we will label each row and column $modulo(n)$, i.e., each coordinate of the entry (i, j), will be represented by a residue class modulo n.

If we assume that f is vulnerable to a differential attack, then there exists a non-trivial linear mapping $\overline{M}$ such that the differential symmetry in (1) is satisfied. To compute such a symmetry inducing map requires the solution of $4n^2$ highly dependent but random equations in the $8n$ unknown coefficients of $\overline{M}$ and $\overline{\Lambda_M}$ over $\mathbb{K}$. Since trivial symmetries (such as multiplication by scalars) are exhibited by every map, we know that there exist nontrivial solutions. Even assuming unit time for $\mathbb{K}$-arithmetic operations, for realistic parameters this process is very inefficient; with the more realistic assumption of costly $\mathbb{K}$-arithmetic operations, this task is unsatisfactory in key generation.

To make the solution of such systems of equations more efficient, we derive the structure of the equations and develop a two step process for verifying trivial differential symmetric structure. The first step involves finding equations which only involve a subset of the variables. The existence of such equations is guaranteed by the degree bound of the HFE monomials. This information is then bootstrapped to eliminate many unknown coefficients of $\overline{M}$ resulting in a very small system of equations which can be solved explicitly.

We remark here that this methodology also suggests a method for estimating the probability of the existence of a differential symmetry for the $HFEv$ primitive. The existence of a nontrivial symmetry corresponds to systems for which the rank of the system of equations is less than $8n$. Under the heuristic that under row reduction these systems of equations behave like random $8n \times 8n$ matrices, we obtain a probability of roughly $1 - q^{-1}$ that the scheme has no nontrivial differential symmetry. We note that this heuristic is almost certainly false since trivial symmetries do exist. This quantity does represent a lower bound, however, and thus may offer support for larger base fields.

We begin by considering the entries of the matrix $\overline{M}^T D_f + D_f \overline{M}$. The contribution of any monomial $\alpha_{i,j} x^{q^i+q^j}$ to the ith row of $D_f \overline{M}$ is given by

$$\left(\alpha_{i,j} m^j_{00,-j}\ \alpha_{i,j} m^j_{00,1-j} \cdots \alpha_{i,j} m^j_{00,-1-j}\ \alpha_{i,j} m^j_{01,-j}\ \alpha_{i,j} m^j_{01,1-j} \cdots \alpha_{i,j} m^j_{01,-1-j}\right)$$

while the contribution to the jth row is

$$\left(\alpha_{i,j}m^i_{00,-i}\ \alpha_{i,j}m^i_{00,1-i}\cdots\ \alpha_{i,j}m^i_{00,-1-i}\ \alpha_{i,j}m^i_{01,-i}\ \alpha_{i,j}m^i_{01,1-i}\cdots\ \alpha_{i,j}m^i_{01,-1-i}\right).$$

By symmetry, the ith and and jth columns of $\overline{M}^T Df$ are the same as their respective rows.

It is clear that the rows and columns associated with coefficients of vinegar monomials as well as terms associated with mixing monomials may be represented similarly. However, it should be noted that those terms associated with mixing monomials will be multiplied by linear coefficients $m_{00,\cdot}$, $m_{01,\cdot}$, $m_{10,\cdot}$, and $m_{11,\cdot}$, while coefficients associated with vinegar variables are multiplied only by linear coefficients $m_{10,\cdot}$ and $m_{11,\cdot}$.

The above patterns can be extended to characterize the contribution to the ith row and jth row of monomials of the form $\beta_{i,j}x^{q^i}y^{q^j}$ and $\gamma_{i,j}y^{q^i+q^j}$, as well. We note, however, that γ coefficients interact with entries from the lower block matrices while β coefficients interact with coefficients from all block matrices.

Now that we have characterized the left side of (1), we will consider the entries of $\Lambda_{\overline{M}}Df$. For every monomial of f, say $\alpha_{i',j'}x^{q^i+q^j}$, $\beta_{r,s}x^{q^r}y^{q^s}$, or $\gamma_{u,v}y^{q^s+q^v}$, we have under the mapping of $\Lambda_{\overline{M}}$ terms of the form: $l_\ell\alpha^{q^\ell}_{i,j}x^{q^{i+\ell}+q^{j+\ell}}$, $l_\ell\beta^{q^{r+\ell}}_{r,s}x^{q^{s+\ell}}y^{q^j}$, and $l_\ell\gamma^{q^\ell}_{u,v}y^{q^{u+\ell}+q^{v+\ell}}$. Clearly, this results in every nonzero entry, say (r,s), of our Df matrix being raised to the power of q^ℓ and shifted along a forty-five degree angle to entry $(r+\ell, s+\ell)$. Thus, for each monomial in f there are two possible nonzero entries in the ith row, with possible overlap.

This discrete geometrical interpretation of the action of M and D on the coefficients of f is central to this analysis. A graphical representation of these relations is provided in Figure 1.

As in [6], the possibility of a differential symmetry can be determined by setting the matrix representation of $M^TDf + DfM$ equal to the matrix $\Lambda_M Df$. We will demonstrate an algorithm, given some specific constraints, that will help provide secure keys to be generated automatically.

Due to the structure of our M matrix, we need to work within each $m_{i,j}$ matrix independently. The following algorithm for $m_{0,0}$ extends very naturally to the other 3 matrices. For clarity, all m terms in description below are $m_{0,0}$ terms.

Let $\alpha_{i,j}, \beta_{r,s}, \gamma_{u,v}$ represent the coefficients of our monomials in our core map. Consider the ith row of $M^TDf+DfM$. For all w not occurring as a power of q of our HFE or mixing monomials in f, or difference of powers of q in an exponent of a monomial in f plus i, the (i,w) entry is $\alpha_{i,j}m^{q^j}_{w-j} = 0$ (resp. $\beta_{i,j}m^{q^j}_{w-j}$). Consider the rth row. For all w not occuring as an exponent of q in a vinegar monomial or as a difference of powers of q in an exponent of a monomial in f plus s, the (r,w)th entry is $\beta_{r,s}m^{q^s}_{k-s} = 0$. Hence, we can use those relations to look for non-zero entries of $m_{0,0}$.

After putting those relations into Algorithm 1, see Figure 3a, you can generate a set for every i and r, exponents that occur in your core map. Each set provides a list of indices of all possible non-zero m's. For each index not occuring

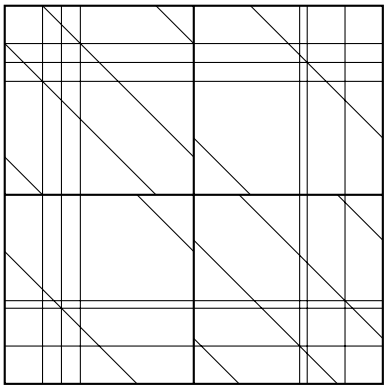

Fig. 1: Graphical representation of the equation $M^T Df + DfM = \Lambda_M Df$ for the $HFEv$ (actually, vC^*) polynomial $f(x) = \alpha_{i,j} x^{q^i+q^j} + \beta_{r,s} x^{q^r} y^{q^s} + \gamma_{u,v} y^{q^u+q^v}$. Horizontal and vertical lines represent nonzero entries in $M^T Df + DfM$ while diagonal lines represent nonzero entries in $\Lambda_M Df$. We may consider this diagram as a genus 4 surface containing straight lines.

in any such set, the corresponding coefficient m must equal zero due to the fact that there must be a coordinate in the equation $M^T Df + DfM = \Lambda_M Df$ setting a constant multiple of m to zero. Thus, the intersection off all sets generated produces a list of all possible non-zero entries for the sub-matrix $m_{0,0}$.

Once this list is obtained, the variables shown to have value zero are eliminated from the system of equations. After repeating a similar algorithm for each of the remaining three submatrices a significantly diminished system of equations is produced which is then solved explicitly.

After running this algorithm with realistic values satisfying the above constraints and matching the parameter sizes of [13] along with using mild restrictions on the powers of the mixing and vinegar monomials, the only non-zero value obtained is m_0.

We note that it is possible that these restrictions, especially the restriction for these experiments on the number of monomials, place a lower bound on the number of vinegar variables required to achieve such a structure. On the other hand, with numerous small-scale experiments without parameter restrictions and using the full number of monomials we found that structurally the only nonzero value for the matrix $m_{0,0}$ is the m_0 term.

Since we have only a single non-zero term, our $m_{0,0}$ matrix is a diagonal matrix. A similar analysis for each of the remaining submatrices reveals the same structure. Thus we find that the only possible structure for $\overline{M}$ under these constraints satisfying a differential symmetry for $HFEv$ is

$$\overline{M} = \left[\begin{array}{c|c} cI & dI \\ \hline dI & cI \end{array}\right].$$

Furthermore, we can prove by way of Theorem 2 from [20], that the coefficients $c, d \in \mathbb{F}_q$.

We note that this map induces a trivial differential symmetry. To see this, note that the (nonpartial) differential of any bivariate function is bilinear in its vector inputs. Thus

$$\begin{aligned} Dg(\overline{M}[a\ b]^T, [x\ y]^T) &= Dg([ca+db\ da+cb]^T, [x\ y]^T) \\ &= Dg([ca+db\ cb+da]^T, [x\ y]^T) \\ &= Dg(c[a\ b]^T, [x\ y]^T) + Dg(d[b\ a]^T, [x\ y]^T) \\ &= cDg(a,b,x,y) + dDg(b,a,x,y) \\ &= (c+d)Dg(a,b,x,y). \end{aligned} \tag{3}$$

Consequently, for the parameters provided by Algorithm 1, $HFEv$ provably has no nontrivial differential symmetric structure.

It should be noted that the restrictions provided on the powers of q of the monomials of our f does lower the entropy of our key space and likely raise the number of required vinegar variables to a level which is either unsafe or undesirable. However, there is still plenty of entropy with these restrictions and we obtain provable security against the differential symmetric attack. The restrictions provided are just a base line for this technique and our experiments with small scale examples indicate that even when we insist that every possible monomial satisfying the HFE degree bound is required to have a nonzero coefficient, the generalized algorithm still outputs only the trivial solution. Thus we can achieve provable security with minimal loss of entropy.

3.2 $HFEv^-$

Now, the algorithm extends naturally to $HFEv^-$. Every non-zero entry from the system generated by $HFEv$ is also in that generated by $HFEv^-$, but with a few more, see Figure 2. We choose a basis in which an example minus projection is a polynomial of degree q^2. For every ith row, we also have for any w not a power of $\alpha+n$ or $\beta+n$ where $n<2$, the (i,w)th entry is $\alpha_{i,j}m_{w-j}^{q^j}=0$. For the sth row, for all w not being a power of $\beta+n$ or $r+n$ where $n<2$, the (s,w)th entry is $\beta_{r,s}m_{w-r}^{q^r}=0$. A visualization is provided in Figure 2.

Again, we can use these relations, along with the relations described in the $HFEv$ system, to create a list of sets of all non-zero areas on $m_{0,0}$ using Algorithm 2, see Figure **??**. Each of these sets contains indices which are possibly non-zero, thus entries not in that set are definitively equal to zero.

By taking the intersection of all the sets, you can find the final locations of non-zero entries for our sub matrix $m_{0,0}$. In doing so, with realistic values from [13], the only non-zero value obtained is m_0. This again gives us security against symmetrical attacks by having M being a block matrix consisting of diagonal matrices with an argument similar to [6].

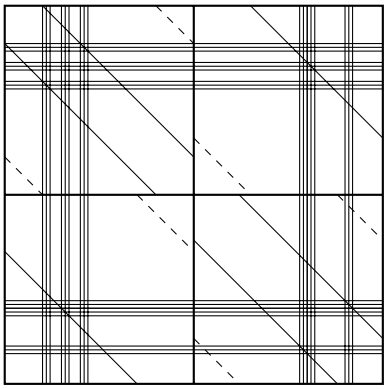

Fig. 2: Graphical representation of the equation $M^T Df + DfM = \Lambda_M Df$ for the $HFEv^-$ with the minus modifier given by the projection $\pi(x) = x^{q^2} + \rho x^q + \tau x$. Horizontal and vertical lines represent nonzero entries in $M^T Df + DfM$ while diagonal lines represent nonzero entries in $\Lambda_M Df$. We note that each triple of lines corresponds to a single monomial in the central map.

HFEvKeyCheck
Input: An $HFEv$ central map f, a flag flg
Output: Set of indices of coefficients m_i of submatrix m_{00} which are possibly nonzero in a linear map inducing differential symmetry for f.
01. **for** monomial $\alpha_{i,j} x^{q^i + q^j}$ in f
02. $S_i = \{\}$;
03 $S_j = \{\}$;
04. **for** monomial with powers r and s in f
05. $S_i = S_i \cup \{r - j, s - j, i - j + r - s, i - j + s - r\}$;
06. $S_j = S_j \cup \{r - i, s - i, j - i + r - s, j - i + s - r\}$;
07. **end for;**
08. **end for;**
09. **if** flg
10. **then**
11. **return** all S_i;
12. **else**
13. **return** $\bigcap S_i$;
14. **end if;**

(a) Algorithm 1: $HFEv$

HFEv-KeyCheck
Input: An $HFEv^-$ central map $\pi(f)$, the corank of π, r
Output: Set of indices of coefficients m_i of submatrix m_{00} which are possibly nonzero in a linear map inducing differential symmetry for $\pi(f)$.
01. **Call:** HFEvKeyCheck(f,1);
02. **for** all S_i
03 $T_i = \{\}$;
04. **for** j from 0 to $r - 1$
05. $T_i = T_i \cup (j + S_i)$;
06. **end for;**
07. **end for;**
08. **return** $\bigcap T_i$;

(b) Algorithm 2: $HFEv^-$

Fig. 3: Algorithms 1 and 2

4 Differential Invariants

Definition 2 *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ 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 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 $\langle x, Av \rangle = 0\ \forall v \in V, \forall A \in Span(Df_i)$. We note that this is not the standard 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. By definition, it is clear that V and $V^\perp$ satisfy the relation

$$dim(V) + dim(V^\perp) \geq n.$$

Assume there is a differential invariant $V \subseteq \mathbb{F}_q^n$, and choose linear maps $M : \mathbb{F}_q^n \to V$ and $M^\perp : \mathbb{F}_q^n \to V^\perp$. For any differential-coordinate-form, we have

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

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

$$[Df(M^\perp y, Mx)]_i = (M^\perp a)^T \left(Df_i(Mx)\right) = 0 \tag{5}$$

Thus, as derived in [5],

$$\forall y, x \in \mathbb{F}_q^n, Df(M^\perp y, Mx) = 0 \quad \text{or equivalently,} \quad Df(M^\perp \mathbb{F}_q^n, M\mathbb{F}_q^n) = 0 \tag{6}$$

This relation restricts the structure of M and $M^\perp$, and provides a direct means of classifying the differential invariant structure of f.

We follow an analogous strategy to that of [6], adapted to the structure of the central $HFEv^-$ map f. First, we recall a result of [6].

Proposition 1. *([6]) 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 $A = CBD$.*

Without loss of generality we 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 above result so that $M^\perp = S(XM)T$. Then we can express $M^\perp = S'MT$, where S' is singular. Restating our differential result (6) in this manner, we have that if $M^\perp = SMT$, and $M : \mathbb{F}_q^{n+v} \to V$, then

$$\forall x, y \in \mathbb{F}_q^n, Df(SMTy, MTx) = 0. \tag{7}$$

4.1 Minimal Generators over Intermediate Subfield

For lack of a good reference, we prove the following statement about the structure of the coordinate ring of a subspace of an extension field over an intermediate extension.

Lemma 1 *Let $\mathbb{L}/\mathbb{K}/\mathbb{F}_q$ be a tower of finite extensions with $|\mathbb{L} : \mathbb{K}| = m$ and $|\mathbb{K} : \mathbb{F}_q| = n$. Let V be an $\mathbb{F}_q$-subspace of $\mathbb{L}$. Then $I(V)$ has m multivariate generators over $\mathbb{K}$ of the form*

$$\mathcal{M}_V^{(k)}(x_0, \ldots, x_{m-1}) = \sum_{\substack{0 \leq i < n \\ 0 \leq j < m}} a_{ijk} x_j^{q^i}.$$

Proof. Choose a basis $\{\overline{e_0} = \overline{1}, \overline{e_1}, \ldots, \overline{e_{m-1}}\}$ for $\mathbb{L}$ over $\mathbb{K}$. Since V is an $\mathbb{F}_q$-subspace of $\mathbb{L}$, the minimal polynomial of V over $\mathbb{L}$, $\mathcal{M}_V(\overline{X}) = \sum_{i=0}^{mn-1} \overline{\alpha_i} \overline{X}^{q^i}$, is $\mathbb{F}_q$-linear. Note that the operations of addition and left multiplication by elements in $\mathbb{L}$ are $\mathbb{K}$-linear, whereas the Frobenius maps are merely $\mathbb{F}$-linear.

Now, since $\mathcal{M}_V(\overline{X})$ is linear it is additive, hence

$$\mathcal{M}_V(\overline{X}) = \mathcal{M}_V\left(\begin{bmatrix} x_0 \\ \vdots \\ x_{m-1} \end{bmatrix}\right) = \sum_{i=0}^{m-1} \mathcal{M}_V(x_i \overline{e_i}).$$

In each summand of $\mathcal{M}_V(x_j \overline{e_j})$, we have

$$(x_j \overline{e_j})^{q^i} = x_j^{q^i} \overline{e_j}^{q^i} = x_j^{q^i} \sum_{i=0}^{m-1} r_i \overline{e_i}$$

for some $r_0, \ldots, r_{m-1} \in \mathbb{K}$. As a vector over $\mathbb{K}$ this quantity is

$$\begin{bmatrix} r_0 x_j^{q^i} \\ \vdots \\ r_{m-1} x_j^{q^i} \end{bmatrix}.$$

Thus $\mathcal{M}_V(x_j \overline{e_j})$ is an m-dimensional vector of $\mathbb{K}$-linear combinations of $x_j, x_j^q, \ldots, x_j^{q^{n-1}}$. Thus $\mathcal{M}_V(\overline{X})$ is of the form

$$\mathcal{M}_V(\overline{X}) = \begin{bmatrix} \mathcal{M}_V^{(0)}(x_0, \ldots, x_{m-1}) \\ \vdots \\ \mathcal{M}_V^{(m-1)}(_0, \ldots, x_{m-1}) \end{bmatrix} = \begin{bmatrix} \sum_{\substack{0 \leq i < n \\ 0 \leq j < m}} a_{ij0} x_j^{q^i} \\ \vdots \\ \sum_{\substack{0 \leq i < n \\ 0 \leq j < m}} a_{ij(m-1)} x_j^{q^i} \end{bmatrix},$$

as required.

We note that the minimal polynomials studied in [6] correspond to the special case of the above lemma in which $m = 1$. Given our characterization from Section 2.2 of the central map of $HFEv^-$ as a bivariate polynomial over $\mathbb{K}$, we are primarily interested in the $m = 2$ case of Lemma 1.

4.2 Invariant Analysis of $HFEv$

As in [6], we consider $Df(SMTa, MTx)$, where T is nonsingular, S is a possibly singular map which sends V into $V^\perp$ and $M : k \to k$ is a projection onto V. Without loss of generality we'll assume that M projects onto V. Then MT is another projection onto V. SMT is a projection onto $V^\perp$. An important distinction is that for this case, the a and x above are actually two dimensional vectors over k. Thus $dim(V) + dim(V^\perp) \geq n$.

Proof (of Theorem 1). Let us denote by $[\hat{x}\ \hat{y}]^T$ the quantity $MT[x\ y]^T$.

Suppose we have

$$f(x,y) = \sum_{\substack{0\leq i\leq j<n \\ q^i+q^j\leq D}} \alpha_{ij} x^{q^i+q^j} + \sum_{\substack{0\leq i,j<n \\ q^i\leq D}} \beta_{ij} x^{q^i} y^{q^j} + \sum_{0\leq i\leq j<n} \gamma_{ij} y^{q^i+q^j}.$$

Applying the differential (w.r.t. the vector $[x\ y]^T$) as described in Section 3.1, we obtain:

$$\begin{aligned} Df(a,b,x,y) = &\sum_{\substack{0\leq i\leq j<n \\ q^i+q^j\leq D}} \alpha_{ij} \left(a^{q^i} x^{q^j} + a^{q^j} x^{q^i} \right) \\ &+ \sum_{\substack{0\leq i,j<n \\ q^i\leq D}} \beta_{ij} \left(a^{q^i} y^{q^j} + x^{q^i} b^{q^j} \right) \\ &+ \sum_{0\leq i\leq j<n} \gamma_{ij} \left(b^{q^i} y^{q^j} + b^{q^j} y^{q^i} \right). \end{aligned} \tag{8}$$

Substituting $SMT[a\ b]^T$ and $MT[x\ y]^T$, we derive

$$Df(S[\hat{a}\ \hat{b}]^T, \hat{x}, \hat{y}) = Df(S_{11}\hat{a} + S_{12}\hat{b}, S_{21}\hat{a} + S_{22}\hat{b}, \hat{x}, \hat{y}).$$

For notational convenience let $\hat{\hat{a}} = S_{11}\hat{a} + S_{12}\hat{b}$ and $\hat{\hat{b}} = S_{21}\hat{a} + S_{22}\hat{b}$. Plugging in these values in the previous equation we get

$$\begin{aligned} Df(\hat{\hat{a}}, \hat{\hat{b}}, \hat{x}, \hat{y}) = &\sum_{\substack{0\leq i\leq j<n \\ q^i+q^j\leq D}} \alpha_{ij} \left((\hat{\hat{a}})^{q^i} \hat{x}^{q^j} + (\hat{\hat{a}})^{q^j} \hat{x}^{q^i} \right) \\ &+ \sum_{\substack{0\leq i,j<n \\ q^i\leq D}} \beta_{ij} \left((\hat{\hat{a}})^{q^i} \hat{y}^{q^j} + \hat{x}^{q^i} (\hat{\hat{b}})^{q^j} \right) \\ &+ \sum_{0\leq i\leq j<n} \gamma_{ij} \left((\hat{\hat{b}})^{q^i} \hat{y}^{q^j} + (\hat{\hat{b}})^{q^j} \hat{y}^{q^i} \right). \end{aligned} \tag{9}$$

In contrast to the situation with HFE, these monomials are not necessarily independent. By Lemma 1, the generators of $I(V)$ have the form

$$\sum_{0\leq i<n} r_{ij} x^{q^i} + \sum_{0\leq i<n} s_{ij} y^{q^i} \text{ for } j \in \{1, 2\},$$

where $r_{ij}, s_{ij} \in \mathbb{K}$. Clearly, these expressions evaluate to zero on $(\hat{x}, \hat{y})$. Evaluating (9) modulo $I(V)$ (only on the variables $\hat{x}$ and $\hat{y}$), we obtain:

$$\begin{aligned} Df(\hat{a}, \hat{\hat{b}}, \hat{x}, \hat{y}) = &\sum_{\substack{0 \leq i < n \\ 0 \leq j < d_x}} \left[\alpha'_{ij} (\hat{a})^{q^i} + \beta'_{ij} (\hat{\hat{b}})^{q^i} \right] \hat{x}^{q^j} \\ &+ \sum_{\substack{0 \leq i < n \\ 0 \leq j < d_y}} \left[\gamma'_{ij} (\hat{a})^{q^i} + \delta'_{ij} (\hat{\hat{b}})^{q^i} \right] \hat{y}^{q^j}, \end{aligned} \tag{10}$$

where d_x and d_y are the largest powers of $\hat{x}$ (resp. $\hat{y}$) occuring. After the reduction modulo $I(V)$, the remaining monomials $\hat{x}, \ldots, \hat{x}^{q^{d_x}}$ and $\hat{y}, \ldots, \hat{y}^{q^{d_y}}$ are independent. Thus, for $Df(\hat{a}, \hat{\hat{b}}, \hat{x}, \hat{y}) = 0$, each polynomial expression multiplied by a single $\hat{x}^{q^j}$ or $\hat{y}^{q^j}$ must be identically zero, that is to say that for all $0 \leq j \leq d_x$

$$\sum_{0 \leq i < n} \left[\alpha'_{ij} (\hat{a})^{q^i} + \beta'_{ij} (\hat{\hat{b}})^{q^i} \right] = 0 \tag{11}$$

and for all $0 \leq j \leq d_y$

$$\sum_{0 \leq i < n} \left[\gamma'_{ij} (\hat{a})^{q^i} + \delta'_{ij} (\hat{\hat{b}})^{q^i} \right] = 0. \tag{12}$$

The left hand sides of (11) and (12) are $\mathbb{F}$-linear functions in $S[\hat{a}\ \hat{b}]^T$. Thus we can express each such equality over $\mathbb{F}$ as

$$LS \left[\hat{a}_0 \ \cdots \ \hat{a}_{n-1}\ \hat{b}_0 \ \cdots \ \hat{b}_{n-1} \right]^T = 0,$$

where L is an $n \times 2n$ matrix with entries in $\mathbb{F}$. We note specifically that the coefficients of L depend on V and the choices of coefficients in the central map f. For randomly chosen coefficients retaining the $HFEv$ structure, we expect an L derived from an equation of the form (11) or (12) to have high rank with very high probability, more than $1 - q^{-n}$. Thus the dimension of the intersections of the nullspaces of each L is zero with probability at least $1 - 2q^{-n}$.

Clearly, the condition for these equations to be satisfied is that S sends V to the intersection of the nullspaces of each such L. Thus S is with high probability the zero map on V and so $V^\perp = \{0\}$. This generates a contradiction, however, since $2n \leq dim(V) + \dim(V^\perp) < 2n$. Thus, with probability greater than $1 - 2q^{-n}$, f has no nontrivial differential invariant structure.

4.3 $HFEv^-$

The situation for $HFEv^-$ is quite similar, but the probabilities are slightly different. Specifically one must note that since the condition of being a differential invariant is a condition on the span of the public differential forms, under projection this condition is weaker and easier to satisfy. For specificity, we consider

the removal of a single public equation, though, critically, a very similar though notationally messy analysis is easy to derive in the general case.

We may model the removal of a single equation as a projection of the form $\pi(x) = x^q + x$ applied after the central map.

Proof (of Theorem 2). Consider

$$\begin{aligned}\pi(f(x,y)) = &\sum_{\substack{0\le i\le j<n\\ q^i+q^j\le D}} \alpha_{ij}x^{q^i+q^j} + \sum_{\substack{0\le i,j<n\\ q^i\le D}} \beta_{ij}x^{q^i}y^{q^j} + \sum_{0\le i\le j<n} \gamma_{ij}y^{q^i+q^j}\\ &+ \sum_{\substack{0\le i\le j<n\\ q^i+q^j\le D}} \alpha_{ij}^q x^{q^{i+1}+q^{j+1}} + \sum_{\substack{0\le i,j<n\\ q^i\le D}} \beta_{ij}^q x^{q^{i+1}}y^{q^{j+1}} + \sum_{0\le i\le j<n} \gamma_{ij}^q y^{q^{i+1}+q^{j+1}}.\end{aligned} \tag{13}$$

Taking the differential, we obtain

$$\begin{aligned}D(\pi\circ f)(\hat{a},\hat{b},\hat{x},\hat{y}) = &\sum_{\substack{0\le i\le j<n\\ q^i+q^j\le D}} \alpha_{ij}\left((\hat{a})^{q^i}\hat{x}^{q^j} + (\hat{a})^{q^j}\hat{x}^{q^i}\right)\\ &+ \sum_{\substack{0\le i,j<n\\ q^i\le D}} \beta_{ij}\left((\hat{a})^{q^i}\hat{y}^{q^j} + \hat{x}^{q^i}(\hat{b})^{q^j}\right)\\ &+ \sum_{0\le i\le j<n} \gamma_{ij}\left((\hat{b})^{q^i}\hat{y}^{q^j} + (\hat{b})^{q^j}\hat{y}^{q^i}\right)\\ &+ \sum_{\substack{0\le i\le j<n\\ q^i+q^j\le D}} \alpha_{ij}^q\left((\hat{a})^{q^{i+1}}\hat{x}^{q^{j+1}} + (\hat{a})^{q^{j+1}}\hat{x}^{q^{i+1}}\right)\\ &+ \sum_{\substack{0\le i,j<n\\ q^i\le D}} \beta_{ij}^q\left((\hat{a})^{q^{i+1}}\hat{y}^{q^{j+1}} + \hat{x}^{q^{i+1}}(\hat{b})^{q^{j+1}}\right)\\ &+ \sum_{0\le i\le j<n} \gamma_{ij}^q\left((\hat{b})^{q^{i+1}}\hat{y}^{q^{j+1}} + (\hat{b})^{q^{j+1}}\hat{y}^{q^{i+1}}\right).\end{aligned} \tag{14}$$

Again, we may evaluate modulo $I(V)$ and collect the terms for the distinct powers of $\hat{x}$ and $\hat{y}$. By the independence of these monomials we obtain the relations

$$\begin{aligned}\sum_{0\le i<n}\left[\alpha''_{ij}(\hat{a})^{q^i} + \beta'_{ij}(\hat{b})^{q^i}\right] = 0\\ \sum_{0\le i<n}\left[\gamma''_{ij}(\hat{a})^{q^i} + \delta'_{ij}(\hat{b})^{q^i}\right] = 0.\end{aligned} \tag{15}$$

At this point, the analysis proceeds exactly as in the case of $HFEv$. We once again arrive at the conclusion that with high probability S is the zero map on V, contradicting the existence of a differential invariant. We note here that this analysis works for any projection, though the exact values of the α''_{ij} and γ''_{ij} depend on the specific projection and the structure of f.

5 Degree of Regularity, Q-rank and Parameters

Further considerations for the security of $HFEv^-$ are the degree of regularity, a quantity closely connected to the complexity of algebraic attacks, and the Q-rank of the public key. A careful analysis of each of these quantities reveals that they support the security of $HFEv^-$ against an algebraic attack such as [21] and against the Kipnis-Shamir methodology and its improvements, see [17, 18].

In [22], it is shown that an upper bound for the Q-rank of an $HFEv^-$ system is given by the sum of the Q-rank of the HFE component, the number of removed equations, and the Q-rank of the vinegar component. For Gui-96(96,5,6,6), here $q = 2$, $n = 96$, $D = 5$, $v = 6$ and $r = 6$, this quantity is roughly 15. Furthermore, in [13], experimental evidence in the form of analysis of toy variants is provided indicating that this estimate is tight. Thus the complexity of a Kipnis-Shamir style attack is roughly $O(n^3 q^{15n})$.

Also in [22], a formula for an upper bound on the degree of regularity for $HFEv^-$ systems is derived. Given the parameters of Gui-96(96,5,6,6), the degree of regularity is expected to be 9. Further, experiments are provided in [13] supporting the tightness of this approximation formula for toy schemes with n as large as 38. With this degree of regularity the expected complexity of inverting the system via Gröbner basis techniques is given by

$$\binom{96 - 6 + 9}{9}^{2.3766} \approx 2^{93}.$$

We note that an error in the approximation of the degree of regularity can easily change this estimate by a factor of a few thousand. Still, it seems clear that each of these avenues of attack is unviable.

Still another attack vector is to put the entropy of the key space to the test with techniques such as those mentioned in [23] for deriving equivalence classes of keys. With our most restrictive instance of the key verification algorithm in Section 3.2, we have a key space consisting of roughly q^{13n} central maps, roughly q^{6n} of which can be seen as equivalent keys as in [23]. Thus provable security against the differential adversary can be achieved with a key space of size far beyond the reach of the "guess-then-IP" strategy. =

6 Conclusion

$HFEv^-$ is rapidly approaching twenty years of age and stands as one of the oldest post-quantum signature schemes remaining secure. With the new parameters suggested in [13], $HFEv^-$ has metamorphosed from the very slow form of QUARTZ into a perfectly reasonable option for practical and secure quantum-resistant signatures.

Our analysis contributes to the confidence and optimism which $HFEv^-$ inspires. By elucidating the differential structure of the central map of $HFEv^-$, we have verified that a class of attacks which has proven very powerful against multivariate schemes in the past cannot be employed against $HFEv^-$. In conjunction

with the careful analysis of the degree of regularity and Q-rank of the scheme already present in the literature, we have succeeded in showing that $HFEv^-$ is secure against every type of attack known. If the future holds a successful attack against $HFEv^-$ it must be by way of a fundamentally new advance.

References

1. Lange, T., et al.: Post-quantum cryptography for long term security. Horizon2020 ICT-645622 (2015) http://cordis.europa.eu/project/rcn/194347_en.html.
2. Campagna, M., Chen, L., et al.: Quantum safe cryptography and security. ETSI White Paper No. 8 (2015) http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.
3. Moody, D., Chen, L., Liu, Y.K.: Nist pqc workgroup. Computer Security Resource Center (2015) http://csrc.nist.gov/groups/ST/crypto-research-projects/#PQC.
4. 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
5. Perlner, R.A., Smith-Tone, D.: A classification of differential invariants for multivariate post-quantum cryptosystems. [24] 165–173
6. Daniels, T., Smith-Tone, D.: Differential properties of the HFE cryptosystem. [25] 59–75
7. 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
8. Shamir, A., Kipnis, A.: Cryptanalysis of the oil & vinegar signature scheme. CRYPTO 1998. LNCS **1462** (1998) 257–266
9. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. [25] 180–196
10. 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
11. Perlner, R., Smith-Tone, D.: Security analysis and key modification for zhfe. In: Post-Quantum Cryptography - 7th International Conference, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016. Proceedings. (2016)
12. 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
13. Petzoldt, A., Chen, M., Yang, B., Tao, C., Ding, J.: Design principles for hfev-based multivariate signature schemes. In Iwata, T., Cheon, J.H., eds.: Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I. Volume 9452 of Lecture Notes in Computer Science., Springer (2015) 311–334
14. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: EUROCRYPT. (1996) 33–48
15. Matsumoto, T., Imai, H.: Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In: EUROCRYPT. (1988) 419–453

16. Berlekamp, E.R.: Factoring polynomials over large finite fields. Mathematics of Computation **24** (1970) pp. 713–735
17. Kipnis, A., Shamir, A.: Cryptanalysis of the hfe public key cryptosystem by relinearization. Advances in Cryptology - CRYPTO 1999, Springer **1666** (1999) 788
18. Bettale, L., Faugère, J., Perret, L.: Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. Des. Codes Cryptography **69** (2013) 1–52
19. Fouque, P.A., Macario-Rat, G., Perret, L., Stern, J.: Total break of the ℓic- signature scheme. PKC 2008, LNCS **4939** (2008) 1–17
20. 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
21. Faugere, J.C.: Algebraic cryptanalysis of hidden field equations (hfe) using grobner bases. CRYPTO 2003, LNCS **2729** (2003) 44–60
22. Ding, J., Yang, B.Y.: Degree of regularity for hfev and hfev-. [24] 52–66
23. Wolf, C., Preneel, B.: Equivalent keys in multivariate quadratic public key systems. J. Mathematical Cryptology **4** (2011) 375–415
24. Gaborit, P., ed.: Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings. In Gaborit, P., ed.: PQCrypto. Volume 7932 of Lecture Notes in Computer Science., Springer (2013)
25. Mosca, M., ed.: Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings. Volume 8772 of Lecture Notes in Computer Science., Springer (2014)