Key Recovery Attack for All Parameters of HFE-

Jeremy Vates[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

jeremy.vates@louisville.edu, daniel.smith@nist.gov

Abstract. Recently, by an interesting confluence, multivariate schemes with the minus modifier have received attention as candidates for multivariate encryption. Among these candidates is the twenty year old HFE$^-$ scheme originally envisioned as a possible candidate for both encryption and digital signatures, depending on the number of public equations removed.

HFE has received a great deal of attention and a variety of cryptanalyses over the years; however, HFE$^-$ has escaped these assaults. The direct algebraic attack that broke HFE Challenge I is provably more complex on HFE$^-$, and even after two decades HFE Challenge II is daunting, though not achieving a security level we may find acceptable today. The minors modeling approach to the Kipnis-Shamir (KS) attack is very efficient for HFE, but fails when the number of equations removed is greater than one. Thus it seems reasonable to use HFE$^-$ for encryption with two equations removed.

This strategy may not be quite secure, however, as our new approach shows. We derive a new key recovery attack still based on the minors modeling approach that succeeds for all parameters of HFE$^-$. The attack is polynomial in the degree of the extension, though of higher degree than the original minors modeling KS-attack. As an example, the complexity of key recovery for HFE$^-(q = 31, n = 36, D = 1922, a = 2)$ is 2^{52}. Even more convincingly, the complexity of key recovery for HFE Challenge-2, an HFE$^-(16, 36, 4352, 4)$ scheme, is feasible, costing around 2^{67} operations. Thus, the parameter choices for HFE$^-$ for both digital signatures and, particularly, for encryption must be re-examined.

Key words: Multivariate Cryptography, HFE, encryption, MinRank, Q-rank

1 Introduction

In the 1990s, several important developments in the history of asymmetric cryptography occured. Among these discoveries, and of the greatest significance to

forward-thinking cryptographers, was the discovery by Peter Shor of polynomial time algorithms for factoring and computing discrete logarithms on a quantum computer, see [1]. In the years since that time, we have witnessed quantum computing become a reality, while *large-scale* quantum computing has transmogrified from a dream into what many of us now see as an inevitability, if not an impending phenomenon. The call for proposals by the National Institute of Standards and Technology (NIST), see [2], charges our community with the task of protecting the integrity and confidentiality of our critical data in this time of tremendous change.

The 1990s also beheld an explosive development in public key technologies relying on mathematics of a less linear character than number theory. In particular, multivariate public key cryptography (MPKC) produced numerous schemes for public key encryption and digital signatures in the late 1990s. These schemes further fuelled the development of computational algebraic geometry, and seem to have inspired the advancement of some of the symbolic algebra techniques we now apply to all areas of post-quantum cryptography, that is, cryptography designed with quantum computers in mind.

Armed with new tools and a more developed theory, many multivariate schemes were cryptanalyzed; in particular, secure multivariate encryption seemed particularly challenging. The purpose of this disquisition is to cryptanalyze an old digital signature scheme that has been repurposed to achieve multivariate encryption.

1.1 Recent History

While the ancestor of all of the "large structure" schemes is the C^* scheme of Matsumoto and Imai, see [3], the more direct parent of multivariate encryption schemes of today is HFE, see [4]. The idea behind such systems is to define a large associative algebra over a finite field and utilize its multiplication to construct maps that are quadratic when expressed over the base field.

There have been many proposals in this area in the last five years. The Simple Matrix Schemes, see [5] for the quadratic version and [6] for the cubic version, are constructed via multiplication in a large matrix algebra over the base field. ZHFE, see [7] and Extension Field Cancellation, see [8], just as HFE, utilize the structure of an extension field in the derivation of their public keys.

Many of these "large structure" schemes have effective cryptanalyses that either break or limit the efficiency of the schemes. HFE, in its various iterations, has been cryptanalyzed via direct algebraic attack, see [9], via an attack exploiting Q-rank known as the Kipnis-Shamir, or KS, attack, see [10], and via a fusion of these techniques utilizing an alternative modeling of the Q-rank property, see [11]. The Quadratic Simple Matrix Scheme is made less efficient for parameters meeting NIST's current suggested security levels in [12], while the Cubic Simple Matrix Scheme is broken for such parameters in [13]. In addition, a low Q-rank property for ZHFE is discovered in [14] which calls in to question the security of the scheme. In light of such an array of cryptanalyses for multivariate encryption

schemes, the question of whether the correct strategy is being employed is very relevant.

Interestingly, at PQCRYPTO 2016 and the winter school prior to the conference, three independent teams of researchers in MPKC related the same idea: the idea of using the minus modifier in encryption. In fairness, the concept of using the minus modifier in encryption is not new; it was suggested as early as in the proposal of HFE. The convergence on this strategy is surprising because it is common knowledge that either the number of equations removed is too large for effective, or even fault-tolerant, encryption, or that the scheme must have parameters that are too large for the system to be efficient. The three techniques are presented in the articles [14] and [8] and in the presentation [15].

While both of the techniques in [14] and [8] are very new schemes, HFE$^-$ has been well studied for over twenty years. Using HFE$^-$ for encryption is more complicated than using the scheme for digital signatures, so careful review of theory is critical for this application.

1.2 Previous Analysis

There are a few results in the literature that are relevant in the analysis of HFE$^-$. These articles address the security of the scheme against algebraic, differential and rank attacks.

In [16], the degree of regularity for the public key of HFE$^-$ schemes is derived. The result shows that the upper bound on the degree of regularity of the public key when a equations is removed is about $\frac{a(q-1)}{2}$ higher than the same bound for a comparable HFE scheme over $GF(q)$.

In [17], information theoretic proofs of security against differential adversaries are derived for HFE$^-$. The consequence of this work is that attacks of the flavor of the attack on SFLASH, see [18], using symmetry and attacks in the manner of the attack on the Simple Matrix Scheme, see [12], exploiting invariants are not relevant for HFE$^-$.

In the other direction, in [11, Section 8.1], an attack on weak parameters of HFE$^-$ with asymptotic complexity of $\mathcal{O}(n^{(\lceil log_q(D) \rceil + 1)\omega})$ is derived, where n is the degree of the extension, D is the degree bound for HFE and ω is the linear algebra constant. The caveat here is that the attack is only successful against HFE$^-$ if only a single equation is removed. This restriction on the attack technique is fundamental and is due to theory, not computational feasibility. The existence of the attack, however, implies that at least two equations must be removed for reasonable parameters, and thus q must be quite small for encryption.

1.3 Our Contribution

We present a key recovery attack on HFE$^-$ that works for any HFE$^-$ public key. The attack is based on the Q-rank of the public key instead of the Q-rank of the private central map as in [11].

The attack works by performing key extraction on a related HFE scheme and then converting the private key of the related scheme into an equivalent private

key for the HFE$^-$ scheme. The complexity of the attack is dominated by the HFE key extraction phase and is on the order of $\mathcal{O}(\binom{n+\lceil log_q(D)\rceil+1}{\lceil log_q(D)\rceil+a+1}^{\omega})$, where D is the degree bound of the central HFE polynomial, a is the number of removed equations and ω is the linear algebra constant, for all practical parameters. We note that this value implies that the minus modification of HFE adds at most $a\omega log_2(n)$ bits of security for any parameters, though we find that it is much less for many practical parameters.

1.4 Organization

The paper is organized as follows. In the next section, we present isomorphisms of polynomials and describe the structure of HFE and HFE$^-$. The following section reviews the Q-rank of ideals in polynomial rings and discusses invariant properties of Q-rank and min-Q-rank. In section 4, we review more carefully the previous cryptanalyses of HFE and HFE$^-$ that are relevant to our technique. The subsequent section contains our cryptanalysis of HFE$^-$. Then, in section 6, we conduct a careful complexity analysis of our attack, followed by our experimental results in the following section. Finally, we conclude, noting the affect these results have on parameter selection for HFE$^-$.

2 HFE Variants

Numerous multivariate cryptosystems fall into a category known as "big field" schemes exploiting the vector space structure of a degree n extension $\mathbb{K}$ over $\mathbb{F}_q$. Let $\phi : \mathbb{F}_q^n \to \mathbb{K}$ be an $\mathbb{F}_q$-vector space isomoprhism. Since a generator of $Gal_{\mathbb{F}_q}(\mathbb{K})$ is the Frobenius automorphism, $x \mapsto x^q$, for every monomial map of the form $f(x) = x^{q^i+q^j}$ in $\mathbb{K}$, $\phi^{-1} \circ f \circ \phi$ is a vector-valued quadratic function over $\mathbb{F}_q$. By counting, one can see that any vector-valued quadratic map on $\mathbb{F}_q^n$ is thusly isomorphic to a sum of such monomials. Consequently, any quadratic map f over $\mathbb{K}$ can be written as a vector-valued map, F, over $\mathbb{F}_q$. Throughout this work, for any map $g : \mathbb{K} \to \mathbb{K}$, we denote by G the quantity $\phi^{-1} \circ g \circ \phi$.

This equivalence allows us to construct cryptosystems in conjunction with the following concept, the of isomorphisms of polynomials.

Definition 1 *Two vector-valued multivariate polynomials F and G are said to be* isomorphic *if there exist two affine maps T, U such that $G = T \circ F \circ U$.*

The equivalence and isomorphism marry in a method commonly referred to as the butterfly construction. Given a vector space isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{K}$ and an efficiently invertible map $f : \mathbb{K} \to \mathbb{K}$, we compose two affine transformations $T, U : \mathbb{F}_q^n \to \mathbb{F}_q^n$ in order to obscure our choice of basis for the input and output. This construction generates a vector-valued map $P = T \circ \phi^{-1} \circ f \circ \phi \circ U$.

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

The Hidden Field Equation Scheme was first introduced by Patarin in [4]. This scheme is an improvement on the well known C^* construction of [19], where a general polynomial with degree bound D is used in place of the C^*'s central monomial map.

Explicitly, one chooses a quadratic map $f : \mathbb{K} \to \mathbb{K}$ of the form:

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

where the coefficients $\alpha_{i,j}, \beta_i, \gamma \in \mathbb{K}$ and the degree bound D is sufficiently low for efficient inversion.

The public key is computed as $P = T \circ F \circ U$. Inversion is accomplished by first taking a cipher text $y = P(x)$, computing $v = T^{-1}(y)$, solving $\phi(v) = f(u)$ for u via the Berlekamp algorithm, see [20], and then recovering $x = U^{-1}(\phi^{-1}(u))$.

HFE$^-$ uses the HFE primitive f along with a projection Π that removes a equations from the public key. The public key is $P_\Pi = \Pi \circ T \circ F \circ U$.

3 Q-Rank

A critical quantity tied to the security of big field schemes is the Q-rank (or more correctly, the min-Q-rank) of the public key.

Definition 2 *The Q-rank of any quadratic map $f(\overline{x})$ on $\mathbb{F}_q^n$ is the rank of the quadratic form $\phi^{-1} \circ f \circ \phi$ in $\mathbb{K}[X_0, \ldots, X_{n-1}]$ via the identification $X_i = \phi(\overline{x})^{q^i}$.*

Quadratic form equivalence corresponds to matrix congruence, and thus the definition of the rank of a quadratic form is typically given as the minimum number of variables required to express an equivalent quadratic form. Since congruent matrices have the same rank, this quantity is equal to the rank of the matrix representation of this quadratic form, even in characteristic 2, where the quadratics x^{2q^i} are additive, but not linear for $q > 2$.

Q-rank is invariant under one-sided isomorphisms $f \mapsto f \circ U$, but is not invariant under isomorphisms of polynomials in general. The quantity that is often meant by the term Q-rank, but more properly called min-Q-rank, is the minimum Q-rank among all nonzero linear images of f. This min-Q-rank is invariant under isomorphisms of polynomials and is the quantity relevant for cryptanalysis.

4 Previous Cryptanalysis of HFE

HFE has been cryptanalyzed via a few techniques in the over twenty years since its inception. The principal analyses are the Kipnis-Shamir (KS) attack of [10], the direct algebraic attack of [9], and the minors modeling approach of the KS-attack of [11].

The KS-attack is a key recovery attack exploiting the fact that the quadratic form representing the central map F over $\mathbb{K}$ is of low rank. Specfically, considering an odd characteristic case, we may write the homogeneous quadratic part of F as

$$\begin{bmatrix} x & x^q & \cdots & x^{q^{n-1}} \end{bmatrix} \begin{bmatrix} \alpha_{0,0} & \alpha'_{0,1} & \cdots & \alpha'_{0,d-1} & 0 \cdots 0 \\ \alpha'_{0,1} & \alpha_{1,1} & \cdots & \alpha'_{1,d-1} & 0 \cdots 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \ddots \vdots \\ \alpha'_{0,d-1} & \alpha'_{1,d-1} & \cdots & \alpha_{d-1,d-1} & 0 \cdots 0 \\ 0 & 0 & \cdots & 0 & 0 \cdots 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \ddots \vdots \\ 0 & 0 & \cdots & 0 & 0 \cdots 0 \end{bmatrix} \begin{bmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{bmatrix},$$

where $\alpha'_{i,j} = \frac{1}{2}\alpha_{i,j}$ and $d = \lceil log_q(D) \rceil$. Using polynomial interpolation, the public key can be expressed as a quadratic polynomial G over a degree n extension, and it is known that there is a linear map T^{-1} such that $T^{-1} \circ G$ has rank d, thus there is a rank d matrix that is a $\mathbb{K}$-linear combination of the Frobenius powers of G. This turns recovery of the transformation T into the solution of a MinRank problem over $\mathbb{K}$.

In contrast to the KS-attack, the Gröbner basis attack of Faugère in [9], is a direct algebraic attack on HFE using the F4 Gröbner basis algorithm. The attack succeeds in breaking HFE Challenge 1, see [4]. The success is primarily due to the fact that the coefficients of the central map in HFE Challenge 1 were very poorly chosen. The scheme is defined over $GF(2)$ and uses only a degree 80 extension. Thus the scheme fails to brute force analysis with complexity at worst 2^{80}. The very small base field drastically limits the number of monomials of degree d and makes Gröbner basis techniques extremely powerful.

The key recovery attack of [11] combines these two approaches with some significant improvements. First, via a very clever construction, it is shown that a $\mathbb{K}$-linear combination of the *public* polynomials has low rank as a quadratic form over $\mathbb{K}$. Second, setting the unknown coefficients in $\mathbb{K}$ as variables, the polynomials representing $(d+1) \times (d+1)$ minors of such a linear combination, which must be zero due to the rank property, reside in $\mathbb{F}_q[t]$. Thus a Gröbner basis needs to be computed over $\mathbb{F}_q$ and the variety computed over $\mathbb{K}$. This technique is called minors modeling and dramatically improves the efficiency of the KS-attack. The complexity of the KS-attack with minors modeling is asymptotically $\mathcal{O}(n^{(\lceil log_q(D) \rceil + 1)\omega})$, where $2 \leq \omega \leq 3$ is the linear algebra constant.

The effect of the minus modifier on these schemes is worthy of notice. For the direct algebraic attack, the fact that the degree of regularity for a subsystem is lower bounded by the degree of regularity of the entire system shows that the minus modifier introduces no weakness. In particular, the degree of regularity of HFE$^-$ is investigated in [16] where it is shown that the best known upper bound on the degree of regularity for HFE increases with each equation removed. For the KS-attack with either the original modeling or the minors modeling, it suffices to note that though there is a method of reconstructing a single removed equation,

it is not true in general that there is a rank $\lceil log_q(D) \rceil$ $\mathbb{K}$-quadratic form in the linear span of the public key; thus, these attacks fail if the number of equations removed is at least two.

5 Key Recovery for HFE$^-$

In this section we explain our key recovery attack on HFE$^-$. The process is broken down into two main steps. The first is finding a related HFE instance of the HFE$^-$ public key. This related instance will then be the focus. Then we discuss how to systematically solve for an equivalent private key for the orignal HFE$^-$ scheme.

5.1 Reduction of HFE$^-$ to HFE

Recall that by imposing the field equations we may always assume that any affine variety associated with HFE is contained in the finite field $\mathbb{K}$. Then we may use the following definition.

Definition 3 (see Definition 1, [17]) *The* minimal polynomial*, of the algebraic set $V \subseteq \mathbb{K}$ is given by*

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

Equivalently, $\mathcal{M}_V$ is the generator of the principal ideal $I(V)$, the intersection of the maximal ideals $\langle x - v \rangle$ for all $v \in V$.

Recall that the public key of an HFE$^-$ scheme is constructed by truncating a full rank linear combination of the central polynomials. That is, with parenthetical emphasis, $P = \Pi(T \circ F \circ U)$. We now show that this singular linear transformation can be transported "past" the invertible transformation T and "absorbed" by the central map.

Lemma 1 *Let $\Pi \circ T$ be a corank a linear transformation on $\mathbb{F}_q^n$. There exist both a nonsingular linear transformation S and a degree q^a linear polynomial π such that $\Pi \circ T = S \circ \phi^{-1} \circ \pi \circ \phi$.*

Proof. Let V be the kernel of $\Pi \circ T$ and let $\pi = \mathcal{M}_V$. Note that $|V| = q^a$, thus $\mathcal{M}_V(x)$ has degree q^a and is of the form

$$x^{q^a} + c_{a-1}x^{q^{a-1}} + \cdots + c_1 x^q + c_0 x \text{ where } c_i \in \mathbb{K} \tag{1}$$

Now let $B_V = \{b_{n-a}, b_{n-a+1}, \ldots, b_{n-1}\}$ be a basis for V and extend this to a basis $B = \{b_0, \ldots, b_{n-1}\}$ of $\mathbb{F}_q^n$. Let M be the matrix transporting from the standard basis to B. Clearly the matrix representations of both $M^{-1}(\Pi \circ T)M$ and $M^{-1}(\phi^{-1} \circ \pi \circ \phi)M$ have the last a columns of 0.

Observe that there exist invertible matrices A and A', corresponding to row operations, such that both $AM^{-1}(\Pi \circ T)M$ and $A'M^{-1}(\phi^{-1} \circ \pi \circ \phi)M$ are in reduced echelon form; that is:

$$AM^{-1}(\Pi \circ T)M = \left[\begin{array}{c|c} I & 0 \\ \hline 0 & 0 \end{array}\right] = A'M^{-1}(\phi^{-1} \circ \pi \circ \phi)M \tag{2}$$

Solving for $\Pi \circ T$, we obtain

$$MA^{-1}A'M^{-1}(\phi^{-1} \circ \pi \circ \phi) = \Pi \circ T. \tag{3}$$

Let $S = MA^{-1}A'M^{-1}$ and the lemma is proven.

Lemma 1 suggests the possibility of considering an HFE$^-$ public key as a full rank basis for the low rank image of a quadratic map. In fact, Lemma 1 is powerful enough to maintain a low degree bound for this map.

Theorem 1 *Let P be the public key of an HFE$^-(q, n, D, a)$ scheme. Then*

$$P' := P \| \{p_{n-a}, p_{n-a+1} \ldots, p_{n-1}\}$$

is a public key of an HFE$(q, n, q^a D)$ scheme for any choice of $p_i \in Span(P)$ where $i \in \{n-a, n-a+1, \ldots, n-1\}$.

Proof. Let P be a public key for HFE$^-(q, n, D, a)$. Observe that P has the following form, $P = \Pi \circ T \circ F \circ U$ where $T, U : \mathbb{F}_q^n \to \mathbb{F}_q^n$ are affine transformations applied to an HFE(q, n, D) central map F. Let Π' be the natural embedding of Π as a linear map $\mathbb{F}_q^n \to \mathbb{F}_q^n$ obtained by composing the inclusion mapping $\mathbb{F}_q^{n-a} \hookrightarrow \mathbb{F}_q^n$. By Lemma 1, we can rewrite $P||\{0, 0, \ldots 0\}$ in the following way:

$$P||\{0, 0, \ldots 0\} = \Pi' \circ T \circ \phi^{-1} \circ f \circ \phi \circ U = S \circ \phi^{-1} \circ (\pi \circ f) \circ \phi \circ U, \tag{4}$$

where S is nonsingular and π is a linear polynomial of degree q^a.

Observe that $P||\{0, 0, \ldots 0\}$ now has the structure of an HFE$(q, n-a, q^a D)$, since the degree bound is increased by a factor of q^a; that is, $deg(\pi(f)) = deg(\pi)deg(f)$. Finally, construct $P' = P||\{p_{n-a}, p_{n-a+1}, \ldots, p_{n-1}\}$ where $p_i \in Span(P)$, possibly 0. Since the composition A of elementary row operations produces P' from $P||\{0, 0 \ldots, 0\}$, we obtain an HFE$(q, n, q^a D)$ key, $(AS, \pi \circ f, U)$.

Theorem 1 indicates that HFE$^-$, in some sense, *is* HFE with merely a slightly higher degree bound. Thus it is sensible to discuss recovering an equivalent key for an instance of HFE$^-$ as an HFE scheme. We can, in fact, do more and recover an equivalent HFE$^-$ key.

5.2 Key Recovery

Any HFE key recovery oracle $\mathcal{O}$, when given a public key P of an HFE instance recovers a private key of HFE "shape." By Theorem 1, such an oracle can recover a private key for the augmented public key P' which is also of HFE shape. We now show, however, that in this case, the key derived from $\mathcal{O}$ must preserve more structure.

Theorem 2 *Let P be a public key for an instance of HFE$^-(q, n, D, a)$ and let $P' = P \| \{p_{n-a}, p_{n-a+1} \ldots, p_{n-1}\}$ be a corresponding HFE$(q, n, q^a D)$ public key. Further, let (T', f', U') be any private key of P'. Then the representation of f' as a quadratic form over $\mathbb{K}$ is block diagonal of the form:*

$$\mathbf{F}' = \begin{bmatrix} F_1' & 0 \\ 0 & 0 \end{bmatrix}, \tag{5}$$

where $F_1' = [f_{i,j}]_{i,j}$ is $(\lceil log_q(D) \rceil + a) \times (\lceil log_q(D) \rceil + a)$ and has the property that $f_{i,j} = 0$ if $|i - j| \geq \lceil log_q(D) \rceil$. That is, F_1' has only a diagonal "band" of nonzero values of width $2\lceil log_q(D) \rceil - 1$.

Proof. Let (T, f, U) be a private key for P as an instance of HFE$^-(q, n, D, a)$. By Theorem 1, one private key of P' has the form (T', f', U') where $f' = \pi \circ f$ and

$$\pi(x) = \sum_{i=0}^{a} b_i x^{q^i}.$$

Therefore,

$$\begin{aligned} f'(x) = \pi \circ f(x) &= \sum_{\substack{i \leq j \\ q^i + q^j \leq D}} \sum_{\ell=0}^{a} b_\ell \alpha_{i,j}^{q^\ell} x^{q^{i+\ell} + q^{j+\ell}} \\ &= \sum_{\substack{i,j \leq \lceil log_q(D) + a \rceil \\ |i-j| < \lceil log_q(D) \rceil}} f_{i,j} x^{q^i + q^j} \end{aligned}$$

Thus there exists one private key of the required form.

Denote by Frob_i the map raising all entries of a vector to the power q^i and let M_b be the linear map $x \mapsto bx$ for $b \in \mathbb{K}$. By the homogeneous case of [11, Theorem 4], for any second private key (T'', f'', U'') of P', we have for some integer $0 \leq k < n$ and for some $a, b \in \mathbb{K}$ that

$$F'' = \mathrm{Frob}_k \circ M_b \circ F' \circ M_a \circ \mathrm{Frob}_{n-k}.$$

It is straightforward to check that the representation of F'' as a quadratic form has the shape of (5) with nonzero entries restricted to $|i - j| < \lceil log_q(D) \rceil$.

Armed with Theorem 2, we are prepared to perform a full key recovery for an instance $P = \Pi \circ T \circ \phi^{-1} \circ f \circ \phi \circ U$ of HFE$^-$. The strategy is simple. By way of Theorem 1, there exists an HFE instance with an equivalent public key. That is, there exists a $P' = T' \circ \phi^{-1} \circ f' \circ \phi \circ U'$ with T', U' invertible, f' of degree bounded by $q^a D$, and where the first $n - a$ public equations in P' form P while the remaining a equations are in the $\mathbb{F}_q$-linear span of P. We perform a key recovery on this instance of HFE via the best known attack, the KS-attack with minors modeling of [11]. Finally, we can recover a central map of degree bound D by way of the following theorem.

Theorem 3 *Let (T, f, U) be an HFE$^-(q, n, D, a)$ private key and let (T', f', U') be an equivalent HFE$(q, n, q^a D)$ key. Then a linear map T'' and a quadratic map f'' of degree bound D such that $\Pi \circ T'' \circ \phi^{-1} \circ f'' \circ \phi \circ U' = \Pi \circ T \circ \phi^{-1} \circ f \circ \phi \circ U$ can be recovered by solving two linear systems, the first of dimension a and the second of dimension $\binom{\lceil log_q(D) \rceil}{2}$.*

Proof. Let (T, f, U) be an HFE$^-(q, n, D, a)$ private key and let (T', f', U') be an equivalent HFE$(q, n, q^a D)$ key. Let $\mathbf{F}'$ denote the matrix representation of f' as a quadratic form over $\mathbb{K}$. Finally, let $d = \lceil log_q(D) \rceil$. By Theorem 2, $\mathbf{F}'$ has the diagonal band shape of width $2d - 1$. From the proof of Theorem 1, there exists a linear map $\pi(x) = \sum_{i=0}^{a} p_i x^{q^i}$, where we may sacrifice monicity and insist $p_0 = 1$ for convenience, and a degree bound D quadratic function f'' such that the composition $\pi(f'') = f'$. Let $\mathbf{F}'' = (f''_{i,j})_{i,j}$ and $\widehat{\pi\mathbf{F}''}$ denote the matrix representations of f'' and $\pi \circ f''$, respectively, as quadratic forms over $\mathbb{K}$. Then we have $\mathbf{F}' = \widehat{\pi\mathbf{F}''}$. The (i, j)th entry of $\widehat{\pi\mathbf{F}''}$ is of the form

$$\sum_{\ell=0}^{a} p_\ell (f''_{i-\ell, j-\ell})^{q^\ell},$$

thus, since $\mathbf{F}'$ is known, we obtain a bilinear system of equations in the unknowns p_i and $f''_{i,j}$.

The insistence that $p_0 = 1$ allows us to recover the values of $f''_{0,j}$ without cost. We then note that due to the fact that $f''_{i,j} = 0$ when $max\{i, j\} \geq d$, the $(i, i + d - 1)$th coefficients of $\widehat{\pi\mathbf{F}''}$ are $p_i (f''_{0,d-1})^{q^i}$ for $0 \leq i \leq a$. Thus, since $f''_{0,d-1}$ is known, we obtain *a linear* system of equations $f'_{i,i+d-1} = p_i (f''_{0,d-1})^{q^i}$ for $1 \leq i \leq a$ in the unknowns p_i, and can therefore solve for π. Once the values of p_i are known, the system of equations becomes linear in $f''_{i,j}$ for $i > 0$. Solving for the remaining unknown values can be done simply with the upper triangular segment from $(1, 1)$ to $(d - 1, d - 1)$, of size $\binom{d}{2}$.

To illustrate the attack in all of its steps, we have prepared a toy example in Appendix A.

6 Complexity of Attack

In this section we derive a tight complexity estimate of the key recovery attack for HFE$^-$ of Section 5. First, we expound upon the relationship between the computational complexity of of HFE$^-$ key recovery and that of HFE key recovery.

Theorem 4 *Let $\mathcal{O}$ be an HFE key recovery oracle that can recover a private key for any instance of HFE(q, n, D) in time $t(q, n, D)$. Then an equivalent HFE key for HFE$^-(q, n, D, a)$ can be recovered by $\mathcal{O}$ in time $t(q, n, q^a D)$.*

Proof. Let P be the public key for an instance of HFE$^-(q, n, D, a)$. Then make the following construction: $P' = P \| \{p_{n-a}, p_{n-a+1} \ldots, p_{n-1}\}$ where $p_i \in Span(P)$.

$\lceil log_q(D) \rceil$	2	3	4	5	6
d_{reg}	5	6	7	8	9

Table 1. The degree of regularity of the system arising from minors modeling on $\mathrm{HFE}^-(q, n, D, a)$ with $a = 2$, $\lceil log_q(D) \rceil$ as indicated, and n sufficiently large.

By Theorem 1, P' is an instance of $HFE(q, n, q^a D)$. Thus $\mathcal{O}$ recovers an equivalent HFE key in time $t(q, n, q^a D)$.

Thus, the complexity of deriving a key for the associated HFE scheme is bounded by the complexity of the best key recovery algorithm for HFE with a degree bound a factor of q^a larger. By Theorem 3, converting the recovered specially structured $\mathrm{HFE}(q, n, q^a D)$ key into an equivalent $\mathrm{HFE}^-(q, n, D, a)$ scheme is of complexity on the order of $\lceil log_q(D) \rceil^{2\omega}$. Since this quantity is very small, the key conversion is instantaneous for all practical parameters. Hence the complexity of the entire attack is bounded by $t(q, n, q^a D)$ from Theorem 4.

We can achieve a tight practical bound when specifying the oracle. Using the minors modeling approach to the KS-attack, which is the currently most successful algebraic attack on HFE, we can accurately determine the complexity of HFE^- key recovery. Just as in HFE, the complexity of the attack is dominated by the MinRank calculation.

Proposition 1 *Let $d = \lceil log_q(D) \rceil$. The degree of regularity of the MinRank instance with parameters $(n, a + d, n - a)$ arising from minors modeling on the public key of $HFE^-(q, n, D, a)$ is the degree of the first negative term in the series*

$$H_r(t) = (1 - t)^{(n-a-d)^2-n+a} \frac{det(\mathbf{A_{a+d}})}{t^{\binom{a+d}{2}}},$$

where $\mathbf{A_{a+d}}$ is the $(a + d) \times (a + d)$ matrix whose (i, j)-th entry is

$$a_{i,j} = \sum_{\ell=0}^{n-max\{i,j\}} \binom{n-i}{\ell} \binom{n-j}{\ell} t^\ell.$$

Proposition 1 follows immediately from [21, Corollary 3], which relies on the genericity conjecture [21, Conjecture 1] which is related to Fröberg's Conjecture, see [22]. With this proposition we can derive the degree of regularity for the MinRank instances for larger systems as well. Focusing on the case in which $a = 2$ we summarize the data in Table 1.

From these data we are prepared to make the following conjecture:

Conjecture 1 *The degree of regularity of the MinRank instance with parameters $(n, a+d, n-a)$ arising from minors modeling on the public key of $HFE^-(q, n, D, a)$ is*

$$d_{reg} = a + d + 1,$$

for all sufficiently large n.

Finally, under the above conjecture, we derive the complexity of our key recovery technique for HFE$^-$.

Theorem 5 *The complexity of key recovery for HFE$^-(q, n, D, a)$ using the minors modeling variant of the KS-attack is*

$$\mathcal{O}\left(\binom{n-a+d_{reg}}{d_{reg}}^{\omega}\right) \sim \mathcal{O}\left(\binom{n+\lceil log_q(D)\rceil+1}{\lceil log_q(D)\rceil+a+1}^{\omega}\right).$$

7 Experimental Results

We ran a series of experiments with Magma, see [23], on a 3.2 GHz Intel® Xeon™ CPU, testing the attack for a variety of values of q, n and D. In all cases, a valid private key was recovered. Table 2 summarizes some of our results for the asymptotically most costly step, the MinRank attack. The data support our complexity estimate of $\mathcal{O}\left(\binom{n+\lceil log_q(D)\rceil+1}{\lceil log_q(D)\rceil+a+1}^{\omega}\right)$.

a	$n=8$	$n=9$	$n=10$	$n=11$	$n=12$
0	37	94	235	575	1269
1	166	535	1572	3653	3374
2	764	1254	6148	26260	97838

Table 2. Average time (in ms) for 100 instances of the MinRank attack on HFE$^-(3, n, 3^2+3^2=18, a)$ for various values of n and a.

8 Conclusion

The HFE$^-$ scheme is a central figure in the development of multivariate cryptography over the last twenty years, inspiring the development of several cryptostystems. Finally, the scheme has revealed a vulnerability significant enough to affect the necessary parameters for the signature algorithm. For example, our attack breaks the HFE$^-(31, 36, 1922, 2)$ primitive in about 2^{52} operations. For an even characteristic example, consider HFE Challenge-2, HFE$^-(16, 36, 4352, 4)$. Our attack breaks HFE Challenge-2 in roughly 2^{67} operations. This efficiency far outperforms any other cryptanalysis and implies that even larger parameters are needed for security. Considering the 2015 suggestion of NIST in [24] that we migrate to 112-bit security, secure parameters for such an HFE$^-$ scheme will be very large, indeed.

Moreover, the use of HFE$^-$ for encryption, in light of this attack, seems very tricky. Presumably the choice of very large and very inefficient instances of HFE$^-$ over very large and very inefficient instances of HFE for encryption is to slightly enhance the efficiency of the scheme by lowering the degree bound. Against our attack, however, lowering $\lceil log_q(D)\rceil$ by x requires a corresponding increase in a by x to achieve *a slightly smaller* security level. This is due to the fact that this transformation preserves the degree of regularity of the MinRank system, but reduces the number of variables by a. Thus, it is reasonable to question the extent of the benefit of using HFE$^-$ over HFE for encryption.

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. Group, C.T.: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. NIST CSRC (2016) http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/call-for-proposals-final-dec-2016.pdf.
3. Matsumoto, T., Imai, H.: Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In: EUROCRYPT. (1988) 419–453
4. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: EUROCRYPT. (1996) 33–48
5. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In Gaborit, P., ed.: PQCrypto. Volume 7932 of Lecture Notes in Computer Science., Springer (2013) 231–242
6. Ding, J., Petzoldt, A., Wang, L.: The cubic simple matrix encryption scheme. [25] 76–87
7. Porras, J., Baena, J., Ding, J.: ZHFE, A new multivariate public key encryption scheme. [25] 229–245
8. Szepieniec, A., Ding, J., Preneel, B.: Extension field cancellation: A new central trapdoor for multivariate quadratic systems. [26] 182–196
9. Faugere, J.C.: Algebraic cryptanalysis of hidden field equations (HFE) using grobner bases. CRYPTO 2003, LNCS **2729** (2003) 44–60
10. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. Advances in Cryptology - CRYPTO 1999, Springer **1666** (1999) 788
11. 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
12. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. [25] 180–196
13. Moody, D., Perlner, R.A., Smith-Tone, D.: Key recovery attack on the cubic abc simple matrix multivariate encryption scheme. In: Selected Areas in Cryptography – SAC 2016: 23rd International Conference, Revised Selected Papers, LNCS, Springer (2017)
14. Perlner, R.A., Smith-Tone, D.: Security analysis and key modification for ZHFE. [26] 197–212
15. Perret, L.: Grobner basis techniques in post-quantum cryptography. Presentation - Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016 (2016) https://www.youtube.com/watch?v=0q957wj6w2I.
16. Ding, J., Kleinjung, T.: Degree of regularity for HFE-. IACR Cryptology ePrint Archive **2011** (2011) 570
17. Daniels, T., Smith-Tone, D.: Differential properties of the HFE cryptosystem. [25] 59–75
18. 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

19. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature verification and message-encryption. Eurocrypt '88, Springer **330** (1988) 419–545
20. Berlekamp, E.R.: Factoring polynomials over large finite fields. Mathematics of Computation **24** (1970) pp. 713–735
21. Faugère, J., Din, M.S.E., Spaenlehauer, P.: Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In Koepf, W., ed.: Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings, ACM (2010) 257–264
22. Fröberg, R.: An inequality for Hilbert series of graded algebras. Math. Scand. **56** (1985) 117–144
23. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24** (1997) 235–265 Computational algebra and number theory (London, 1993).
24. Barker, E., Roginsky, A.: Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths. NIST Special Publication (2015) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf.
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)
26. Takagi, T., ed.: Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings. Volume 9606 of Lecture Notes in Computer Science., Springer (2016)

A Toy Example

To illustrate the attack, we present a complete key recovery for a small odd prime field instance of HFE^-. We simplify the exposition by considering a homogeneous key.

Let $q = 7$, $n = 8$, $D = 14$ and $a = 2$. We construct the degree n extension $\mathbb{K} = \mathbb{F}_7[x]/\left\langle x^8 + 4x^3 + 6x^2 + 2x + 3 \right\rangle$ and let $b \in \mathbb{K}$ be a fixed root of this irreducible polynomial.

We randomly select $f : \mathbb{K} \to \mathbb{K}$ of degree D,

$$f(x) = b^{4100689}x^{14} + b^{1093971}x^8 + b^{5273323}x^2,$$

and two invertible linear transformations T and U:

$$T = \begin{bmatrix} 2&1&0&3&5&0&3&2 \\ 6&2&1&3&4&2&5&1 \\ 0&2&5&1&3&1&4&3 \\ 3&2&6&4&5&3&4&4 \\ 6&4&2&1&0&5&0&0 \\ 0&3&3&6&5&1&1&3 \\ 0&3&0&4&3&6&1&5 \\ 4&3&2&6&1&1&6&3 \end{bmatrix}, \text{ and } U = \begin{bmatrix} 5&1&4&1&4&2&5&3 \\ 0&6&1&5&3&5&3&2 \\ 3&3&5&0&3&4&2&2 \\ 4&0&5&4&0&6&4&1 \\ 2&6&4&0&0&5&3&5 \\ 0&2&4&0&2&0&6&5 \\ 4&3&0&3&3&2&2&6 \\ 6&2&5&3&5&4&0&0 \end{bmatrix}.$$

Since $b^{1093971}/2 = b^{4937171}$, we have

$$\mathbf{F} = \begin{bmatrix} b^{5273323} & b^{4937171} & 0\,0\,0\,0\,0\,0 \\ b^{4937171} & b^{4100689} & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \end{bmatrix}.$$

We fix $\Pi : \mathbb{F}_q^8 \to \mathbb{F}_q^6$, the projection onto the first 6 coordinates. Then the public key $P = \Pi \circ T \circ F \circ U$ in matrix form over $\mathbb{F}_q$ is given by:

$$\mathbf{P_0} = \begin{bmatrix} 5\,6\,3\,6\,6\,0\,4\,2 \\ 6\,0\,1\,3\,3\,5\,2\,1 \\ 3\,1\,4\,0\,6\,0\,4\,4 \\ 6\,3\,0\,3\,0\,2\,3\,1 \\ 6\,3\,6\,0\,4\,2\,2\,4 \\ 0\,5\,0\,2\,2\,2\,5\,1 \\ 4\,2\,4\,3\,2\,5\,1\,5 \\ 2\,1\,4\,1\,4\,1\,5\,2 \end{bmatrix}, \mathbf{P_1} = \begin{bmatrix} 1\,6\,1\,5\,4\,2\,2\,2 \\ 6\,5\,4\,4\,0\,1\,6\,2 \\ 1\,4\,3\,5\,6\,2\,1\,1 \\ 5\,4\,5\,2\,2\,3\,1\,5 \\ 4\,0\,6\,2\,2\,1\,2\,4 \\ 2\,1\,2\,3\,1\,6\,2\,6 \\ 2\,6\,1\,1\,2\,2\,5\,6 \\ 2\,2\,1\,5\,4\,6\,6\,2 \end{bmatrix}, \mathbf{P_2} = \begin{bmatrix} 2\,5\,2\,2\,2\,3\,3\,2 \\ 5\,1\,2\,1\,3\,2\,5\,4 \\ 2\,2\,2\,1\,6\,2\,1\,0 \\ 2\,1\,1\,4\,4\,5\,2\,3 \\ 2\,3\,6\,4\,4\,5\,2\,2 \\ 3\,2\,2\,5\,5\,3\,4\,6 \\ 3\,5\,1\,2\,2\,4\,5\,5 \\ 2\,4\,0\,3\,2\,6\,5\,2 \end{bmatrix},$$

$$\mathbf{P_3} = \begin{bmatrix} 1\,6\,6\,4\,0\,0\,3\,4 \\ 6\,2\,5\,5\,4\,5\,5\,6 \\ 6\,5\,4\,6\,3\,6\,4\,2 \\ 4\,5\,6\,4\,5\,2\,4\,5 \\ 0\,4\,3\,5\,6\,3\,6\,0 \\ 0\,5\,6\,2\,3\,2\,4\,1 \\ 3\,5\,4\,4\,6\,4\,4\,4 \\ 4\,6\,2\,5\,0\,1\,4\,0 \end{bmatrix}, \mathbf{P_4} = \begin{bmatrix} 4\,4\,5\,2\,6\,6\,5\,2 \\ 4\,4\,0\,0\,3\,4\,1\,6 \\ 5\,0\,5\,3\,3\,0\,1\,0 \\ 2\,0\,3\,4\,1\,3\,3\,2 \\ 6\,3\,3\,1\,6\,5\,0\,1 \\ 6\,4\,0\,3\,5\,4\,6\,0 \\ 5\,1\,1\,3\,0\,6\,2\,6 \\ 2\,6\,0\,2\,1\,0\,6\,4 \end{bmatrix}, \mathbf{P_5} = \begin{bmatrix} 0\,2\,6\,1\,6\,2\,3\,4 \\ 2\,4\,2\,0\,3\,1\,5\,0 \\ 6\,2\,5\,1\,4\,3\,1\,1 \\ 1\,0\,1\,5\,0\,0\,3\,0 \\ 6\,3\,4\,0\,1\,4\,1\,4 \\ 2\,1\,3\,0\,4\,5\,5\,5 \\ 3\,5\,1\,3\,1\,5\,1\,2 \\ 4\,0\,1\,0\,4\,5\,2\,6 \end{bmatrix}.$$

A.1 Recovering a Related HFE Key

This step in key recovery is a slight adaptation of the program of [11]. First, we recover the related private key of Theorem 2. To do this, we solve the MinRank instance on the above $6 = n - 2$ $n \times n$ matrices with target rank $\lceil log_q(D) \rceil + a = 2 + 2 = 4$. We may fix one variable to make the ideal generated by the 5×5 minors zero-dimensional. There are $n = 8$ solutions, each of which consists of the Frobenius powers of the coordinates of

$$v = (1, b^{5656746}, b^{3011516}, b^{3024303}, b^{1178564}, b^{1443785}).$$

The combination $L = \sum_{i=0}^{5} v_i \mathbf{P_i}$ is now a rank 4 matrix with entries in $\mathbb{K}$.

We next form $\widehat{v}$ from v by appending $a = 2$ random nonzero values from $\mathbb{K}$ to v. Now we compute

$$\phi^{-1} T'^{-1} \circ \phi = \sum_{i=0}^{8} \widehat{v}_i x^{q^i}.$$

Next we let K_i be the left kernel matrix of the $n - i$th Frobenius power of L for $i = 0, 1, \ldots, a + 1$. We then recover a vector w simultaneously in the right kernel of K_i for all i. For this example, each such element is a multiple in $\mathbb{K}$ of

$$w = (b^{4849804}, b^{3264357}, b^{4466027}, b^{638698}, b^{2449742}, b^{4337472}, b^{2752502}, b^{1186132}).$$

Then we may compute

$$\phi^{-1} \circ U \circ \phi = \sum_{i=0}^{8} w_i x^{q^i}.$$

At this point we can recover $\phi^{-1} \circ f' \circ \phi = T'^{-1} \circ P \circ U'^{-1}$, and have a full private key for the related instance HFE$(7, 8, 686)$. The transformations T' and U' and the matrix representation of f' as a quadratic form over $\mathbb{K}$ are given by

$$T' = \begin{bmatrix} 1&4&4&5&4&5&5&2 \\ 0&6&6&0&4&4&5&5 \\ 0&5&0&4&2&0&0&3 \\ 0&4&4&2&5&6&6&6 \\ 0&3&6&2&5&6&0&0 \\ 0&2&0&4&4&6&2&2 \\ 0&1&5&5&0&5&2&6 \\ 0&3&3&3&6&5&2&2 \end{bmatrix}, U' = \begin{bmatrix} 6&2&1&4&4&4&1&6 \\ 1&6&0&2&3&0&4&2 \\ 2&5&3&6&3&3&0&4 \\ 0&5&6&5&4&1&4&2 \\ 6&5&3&5&4&6&3&2 \\ 0&4&6&1&4&0&1&5 \\ 6&0&2&3&6&5&6&3 \\ 5&2&0&4&1&2&4&5 \end{bmatrix}$$

$$\mathbf{F}' = \begin{bmatrix} b^{416522} & b^{5402526} & 0 & 0 & 0\,0\,0\,0 \\ b^{5402426} & b^{3093518} & b^{5177024} & 0 & 0\,0\,0\,0 \\ 0 & b^{5177024} & b^{5689467} & b^{5706144} & 0\,0\,0\,0 \\ 0 & 0 & b^{5706144} & b^{3464750} & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \end{bmatrix}.$$

A.2 Recovery of Equivalent HFE$^-$ Key

Now we describe the full key recovery given the related HFE key. We know that there exists a degree $D = 14$ map $f''(x) = f''_{0,0}x^2 + 2f''_{0,1}x^8 + f''_{1,1}x^{14}$ with associated quadratic form

$$\mathbf{F}'' = \begin{bmatrix} f''_{0,0} & f''_{0,1} & 0\,0\,0\,0\,0\,0 \\ f''_{0,1} & f''_{1,1} & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \\ 0 & 0 & 0\,0\,0\,0\,0\,0 \end{bmatrix},$$

and a polynomial $\pi(x) = x + p_1 x^7 + p_2 x^{49}$ such that $f' = \pi \circ f''$. Thus we obtain the bilinear system of equations by equating $\mathbf{F}'$ to:

$$\widehat{\pi\mathbf{F}''} = \begin{bmatrix} f''_{0,0} & f''_{0,1} & 0 & 0 & 0\,0\,0\,0 \\ f''_{0,1} & f''_{1,1} + p_1(f''_{0,0})^7 & p_1(f''_{0,1})^7 & 0 & 0\,0\,0\,0 \\ 0 & p_1(f''_{0,1})^7 & p_1(f''_{1,1})^7 + p_2(f''_{0,0})^{49} & p_2(f''_{0,1})^{49} & 0\,0\,0\,0 \\ 0 & 0 & p_2(f''_{0,1})^{49} & p_2(f''_{1,1})^{49} & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \\ 0 & 0 & 0 & 0 & 0\,0\,0\,0 \end{bmatrix}.$$

We clearly have the values of $f''_{0,0}$ and $f''_{0,1}$. Then the equations on the highest diagonal are linear in p_i. We obtain $\pi = x + b^{1948142}x^7 + b^{398370}x^{49}$ and continue to solve the now linear system to recover $f''(x) = b^{416522}x^2 + b^{1559326}x^8 + b^{1121420}x^{14}$.

We then obtain the matrix form of π over $\mathbb{F}_q$ and compose with T':

$$\widehat{\pi} = \begin{bmatrix} 2\,6\,6\,0\,2\,2\,5\,5 \\ 6\,3\,5\,3\,1\,4\,5\,0 \\ 5\,2\,6\,0\,6\,6\,6\,1 \\ 1\,1\,3\,6\,4\,1\,1\,6 \\ 5\,6\,2\,4\,6\,6\,1\,6 \\ 5\,3\,1\,5\,0\,1\,0\,4 \\ 3\,2\,1\,3\,3\,1\,3\,5 \\ 4\,2\,1\,1\,1\,4\,4\,2 \end{bmatrix}, T' \circ \widehat{\pi} = \begin{bmatrix} 0\,0\,1\,2\,0\,5\,4\,0 \\ 1\,2\,4\,4\,2\,1\,0\,4 \\ 0\,2\,2\,1\,1\,6\,1\,0 \\ 3\,3\,1\,0\,6\,3\,2\,0 \\ 0\,1\,3\,1\,0\,2\,2\,2 \\ 3\,4\,5\,0\,1\,3\,4\,2 \\ 0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix}.$$

Replacing the last two rows of $T' \circ \widehat{\pi}$ to make a full rank matrix produces T''. Then the original public key P is equal to $\Pi \circ T'' \circ \phi^{-1} \circ f'' \circ \phi \circ U'$.