HFERP - A New Multivariate Encryption Scheme

Yasuhiko Ikematsu[3], Ray Perlner[2], Daniel Smith-Tone[1,2], Tsuyoshi Takagi[3], and Jeremy Vates[1]

[1]Department of Mathematics, University of Louisville, Louisville, Kentucky, USA
[2]National Institute of Standards and Technology, Gaithersburg, Maryland, USA
[3]Kyushu University, Institute of Mathematics for Industry, Fukuoka, Japan

y-ikematsu@imi.kyushu-u.ac.jp, ray.perlner@nist.gov, daniel.smith@nist.gov, takagi@imi.kyushu-u.ac.jp, jeremy.vates@louisville.edu

Abstract. In 2016, Yasuda et al. presented a new multivariate encryption technique based on the Square and Rainbow primitives and utilizing the plus modifier that they called Square Rainbow Plus (SRP). The scheme achieved a smaller blow-up factor between the plaintext space and ciphertext space than most recent multivariate encryption proposals, but proved to be too aggressive and was completely broken by Perlner et al. in 2017. The scheme suffered from the same MinRank weakness that has allowed effective attacks on several notable big field multivariate schemes: Hidden Field Equations (HFE), multi-HFE, HFE-, for example. We propose a related new encryption scheme retaining the desirable traits of SRP and patching its weaknesses. We call the scheme HFE Rainbow Plus (HFERP) because it utilizes a similar construction as SRP with an HFE primitive replacing the Square polynomial. The effect of this substitution is to increase the Q-rank of the pubic key to such a degree that the MinRank attack is impossible. HFERP still retains the relatively small blow-up factor between the plaintext space and ciphertext space, and is thus a candidate for secure multivariate encryption without an essential doubling in size between plaintext and ciphertext.

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

1 Introduction

Ever since the discovery of polynomial time algorithms for factoring and computing discrete logarithms on a quantum computer by Peter Shor [1], creating schemes that resist such developments has fallen upon the shoulders of today's

cryptographers. In recent years, quantum computing has made significant advances leading some experts to make more confident predictions that the post-quantum world will soon be upon us, see, for example, [2].

There has also been an explosive development in public key technologies relying on mathematics for which there is no known significant computational advantage quantum computers possess. In particular, multivariate public key cryptography (MPKC) produced numerous schemes for public key encryption and digital signatures in the late 1990s. These schemes further fueled 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.

With the development of such techniques, many multivariate schemes have been cryptanalyzed and broken. Specifically, multivariate encryption seems to be challenging. The purpose of this article is to confront this challenge, advancing a new multivariate encryption scheme Hidden Field Equations Rainbow Plus (HFERP), based on Square Rainbow Plus (SRP), see [3], developed to eradicate the deficiencies of its predecessor.

1.1 Recent History

While there may be many trustworthy candidates for multivariate signatures, such as Unbalanced Oil and Vinegar (UOV) [4], Rainbow [5], and Gui [6], developing multivariate schemes for encryption has been a bit of a struggle. While some older ideas have have been reborn with better parameter sets due to the advancement of the science, such as applying HFE-, see [7], to encryption, most of the surviving multivariate encryption schemes are relatively young.

In the last few years, there have been a few new proposals for multivariate encryption, mostly following the idea that it is easier to hide the structure of an injective mapping into a large codomain than to hide the structure of a bijection, as is needed for any encryption mapping into a codomain of the same size as the domain. The ABC Simple Matrix encryption scheme of [8, 9] and ZHFE, see [10] are examples of this idea. Most of these encryption ideas, both new and old, have inspired recent surprising cryptanalyses that affect parameter selection or outright break the scheme, see [11–15], for example.

Such a tale describes the life of SRP, see [3], the design of which aimed to be very efficient and holds a comparably small blow up factor between the plaintext and ciphertext sizes. The scheme also claimed security against attacks efficient against the Square and Rainbow schemes by combining them into one. Unfortunately, SRP is also the victim of a new cryptanalysis, see [16]. The attack exploits the low Q-rank of the Square map, a vulnerability inherited by the public key. A modified MinRank attack was able to pull apart the Square polynomials from the Rainbow and Plus polynomials in the public key.

1.2 Our Contribution

We present a new composite scheme in the manner of SRP by replacing the weaker Square layer with an HFE polynomial of higher Q-rank and finding the correct balance in the sizes of the HFE, Rainbow and Plus layers for efficiency and security. We call our scheme HFERP. We further establish the complexity of the relevant attack models: the algebraic attack, the MinRank attack, and the invariant attack.

1.3 Organization

The paper is organized as follows. In the next section, we present isomorphisms of polynomials and describe the structure of HFE and SRP. The subsequent 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 SRP. We then present HFERP in the next section. Section 6 discusses the complexity of all known relevant attacks on HFERP. Our choice of parameters to optimize security and performance along with experimental results are then presented in the following section. Finally, we conclude discussing why a similar approach to SRP seems to produce such a different technology in HFERP.

2 Big Field Schemes

HFE and SRP are members of a family of cryptosystems known as "big field" schemes. This term is based on the system exploiting the vector space structure of a degree n extension of $\mathbb{K}$ over a finite field $\mathbb{F}_q$. Using core maps within the extension field allows us to take advantage of Frobenius automorphisms $x \mapsto x^q$ for any function of the form $f(x) = x^{q^i+q^j}$, noting that $\phi^{-1} \circ f \circ \phi$ is a vector-valued quadratic function over $\mathbb{F}_q$ where $\phi : \mathbb{F}_q^n \to \mathbb{K}$ is an $\mathbb{F}_q$-vector space isomorphism. By observing that any vector-valued quadratic function on $\mathbb{F}_q^n$ is isomorphic to a sum of such monomials, it is clear that any quadratic function f over $\mathbb{K}$ can be represented as a vector-valued function, F, over $\mathbb{F}_q$.

This equivalence allows us to construct cryptosystems in conjunction with the following concept, the 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 $P = T \circ \phi^{-1} \circ f \circ \phi \circ U = T \circ F \circ U$,

where $F = \phi^{-1} \circ f \circ \phi$.

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

2.1 HFE

The Hidden Field Equation Scheme was first introduced by Patarin, see [17], as an improvement on the well known C^* construction of [18]. Patarin's contribution was to use a general polynomial with degree bound D in place of the central monomial map of C^*.

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

$$f(x) = \sum_{\substack{i \leq j \\ q^i + q^j \leq D}} \alpha_{i,j} x^{q^i + q^j} + \sum_{\substack{i \\ q^i \leq D}} \beta_i x^{q^i} + \gamma, \tag{1}$$

where the coefficients $\alpha_{i,j}, \beta_i, \gamma \in \mathbb{K}$ and the degree bound D is sufficiently low for efficient inversion using the Berlekamp algorithm, see [19] .

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

2.2 Rainbow

The Rainbow scheme is a generalization of Patarin's UOV, see [4]. The key idea, introduced by Ding, see [5], was constructing multiple layers of UOV.

Let $\mathbb{F}$ be a finite field with a degree n extension $\mathbb{F}^n$. Let $\mathcal{V} = \{1, 2, \ldots, n\}$. For a chosen u, let $v_1, \ldots, v_u$ be integers such that $0 < v_1 < \cdots < v_u = n$ and let $\mathcal{V}_l = \{1, \ldots, v_l\}$ for each $l \in \{1, \ldots, u\}$. Note that $|\mathcal{V}_i| = v_i$.

Let $o_i = v_{i+1} - v_i$ for each $i \in \{1, \ldots, u-1\}$ and $\mathcal{O}_i = S_{i+1} - S_i$ for each $i \in \{1, \ldots, u-1\}$. Define P_l to be the space generated by the span of polynomials of the following form:

$$f(x_1, \ldots, x_n) = \sum_{i \in \mathcal{O}_l, j \in \mathcal{V}_l} \alpha_{i,j} x_i x_j + \sum_{i,j \in \mathcal{V}_l} \beta_{i,j} x_i x_j + \sum_{i \in \mathcal{V}_l} \gamma_i x_i + \eta$$

One can refer to the previous constructions using the following terminology: $\mathcal{O}$ is the collection of oil variables, $\mathcal{V}$ is the collection of vinegar variables, and a polynomial $f \in P_l$ is an l-th layer Oil and Vinegar polynomial.

The Rainbow map $F : \mathbb{F}^n \to \mathbb{F}^{n-v_1}$ is defined as (with $x_1, \ldots, x_n$ being referred to as $\bar{x}$ for convenience)

$$F(\bar{x}) = (\tilde{F}_1(\bar{x}), \ldots, \tilde{F}_{u-1}(\bar{x})) = (F_1(\bar{(}x), \ldots, F_{n-v_1}(\bar{x})$$

where each $\tilde{F}_i$ consists of o_i randomly chosen quadratic polynomials from P_i. F is a Rainbow polynomial map with $u-1$ layers. The public key is generated in the usual fashion by applying two affine transformations, T and U, where $T : \mathbb{F}^{n-v_1} \to \mathbb{F}^{n-v_1}$ and $U : \mathbb{F}^n \to \mathbb{F}^n$: $T \circ F \circ U$

2.3 SRP

In Section 5, we present in detail the construction of our proposed scheme, HFERP. For reference, we will include the Square Map definition as well as method of inversion presented in the original SRP paper, see [3].

Instead of using the HFE core map described in section 5, SRP uses the Squaring map where the Square component is defined as $\mathcal{F}_S : \mathbb{F}_q^{n'} \to \mathbb{F}_q^d$ (where $q^d + 1$ is divisible by 4) and it is the result of the following composition:

$$\mathbb{F}_q^{n'} \xrightarrow{\pi_d} \mathbb{F}_q^d \xrightarrow{\phi} \mathbb{K} \xrightarrow{X \mapsto X^2} \mathbb{K} \xrightarrow{\phi^{-1}} \mathbb{F}_q^d$$

Upon inversion step 3, the user would compute

$$R_{1,2} = \pm X^{(q^d+1)/4}$$

and use it to find $\mathbf{y} = (y_1^{(i)}, \ldots, y_d^{(i)}) = \phi^{-1}(R_i) \in \mathbb{F}_q^d$. The choice of the Square map was made because of the speed of inversion it provided when compared to any other quadratic maps. Unfortunately, due to this choice, SRP was quickly broken in [16] by isolating the squaring public polynomials and exploiting its low Q-rank.

3 Q-Rank

The min-Q-rank of the public key is a critical quantity when analizing the security of big field schemes within multivariate cryptography. For clarification, the definition is as follows:

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 $X_i = \phi(\overline{x})^{q^i}$.*

Usually, the definition of the rank of a quadratic form is given as the minimum number of variables required to express an equivalent quadratic form due to quadratic form equivalences corresponding to matrix congruence. Note that congruent matrices have the same rank. This same quantity is equal to the rank of the matrix representations of the 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 Relevant Schemes

SRP was a designed as a concatenation of two known multivariate schemes and a scheme modifier. The first component was Square, see [20], which can be seen as a degenerate version of HFE. The second component was oil-and-vinegar (OV) or, more generally, Rainbow, see [21, 5]. The final component was the plus modifier, first proposed in [22]. The algebraic properties of these schemes were intended to complement their weaknesses when used in conjunction. This patchwork design requires, however, a careful consideration of the relevant cryptanalyses within all of these families.

The original oil-and-vinegar (OV) scheme, proposed in [21], was completely broken in [23] by what we call the invariant method. Specifically, the balanced OV scheme contains an equal number of oil variables, variables which only occur linearly in the central map, and vinegar variables, which occur quadratically. Thus, the differential of any central polynomial has the shape

$$Df_i = \begin{bmatrix} a_{1,1} & \cdots & a_{1,v} & a_{1,v+1} & \cdots & a_{1,2v} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{1,v} & \cdots & a_{v,v} & a_{v,v+1} & \cdots & a_{v,2v} \\ a_{1,v+1} & \cdots & a_{v,v+1} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{1,2v} & \cdots & a_{v,2v} & 0 & \cdots & 0 \end{bmatrix},$$

under an appropriate basis of $\mathbb{F}^{2v} = V \oplus O$, where V is the subspace spanned by the vinegar variables and O is the subspace spanned by the oil variables.

The invariant attack proceeds by computing the differential of random linear combinations of the public polynomials until two full rank differentials, Df_1 and Df_2, are produced. Then O is left invariant by $Df_1^{-1}Df_2$ and is thus easily recovered. A similar technique has been used in conjunction with rank attacks to assault schemes with a similar structure whenever $\dim(V) \leq \dim(O)$, see, in particular, [11, 24, 13].

HFE and some of its modifications have been the target of effective cryptanalyses utilizing the low Q-rank property of the central map. Each of these cryptanalyses can be described as a big field MinRank attack, recovering a low rank quadratic form over the extension $\mathbb{E}$ from which an isomorphism relating the public key to an equivalent private key can be derived.

The earliest iteration of this technique is the well-known Kipnis-Shamir (KS) attack of [25], also known by the name MinRank, due to the close relationship between the attack and the MinRank problem in algebraic complexity theory, see [26]. The KS-attack recovers a private key for HFE by exploiting the fact that the low Q-rank of the central map is a property preserved by isomorphisms. Considering an odd characteristic instance of HFE. We may write the homogeneous

quadratic part of the central map 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 $d = \lceil \log_q(D) \rceil$. The KS-attack first interpolates an univariate representation of the public key over $\mathbb{E}$. This representation of the public key is isomorphic to the central map of Q-rank bounded by the ceiling of the logarithm of the degree bound. Thus, there is a linear map T^{-1} which when composed with the public key has Q-rank d, and so there is a low rank matrix that is an $\mathbb{E}$-linear combination of the Frobenius powers of G. This turns recovery of the transformation T into the solution of a MinRank problem over $\mathbb{E}$.

Another version of this attack, utilizing the same property, is the key recovery attack of [27]. The authors prove the existence of an $\mathbb{E}$-linear combination of the *public* key with low rank over $\mathbb{E}$. Setting the unknown coefficients of this linear combination as variables, they construct the ideal $I \subseteq R = \mathbb{F}[T]$ of minors of this sum of the appropriate dimension such that $V(I) \cap \mathbb{E}^{\dim(R)}$ consists of exactly such linear coefficients. Thus a Gröbner basis needs to be computed over $\mathbb{F}$ and the variety computed over $\mathbb{E}$. This modeling of the KS-attack is called minors modeling and dramatically improves the efficiency of the KS-attack in many circumstances.

The KS-attack with either KS modeling or with minors modeling has also been used to break other HFE descendants. In [27], the minors modeling approach is used to break multi-HFE. In [15], the KS-attack is extended to provide key recovery for HFE-. In [14], both the KS modeling and minors modeling versions of the KS-attack are used to undermine the security of ZHFE.

The MinRank methodology is also employed in [16], where an effective key recovery attack on SRP is presented. It was shown that the low Q-rank of Square is exposed by the SRP construction. Specifically, the Q-rank of the square map $f(x) = x^2$ is one over an odd characteristic field. Since this low Q-rank map is in the span of the public polynomials, there is an $\mathbb{E}$-linear combination of the public polynomials of rank one! Thus the ideal generated by the two-by-two minors is resolved at degree two and the complexity of the attack is $\mathcal{O}(\binom{m+1}{2}^{\omega})$, where $2 \leq \omega \leq 3$ is the linear algebra constant. The attack is applied practically, breaking the 80-bit parameters in about 8 minutes.

5 HFERP

In this section, we present a significant modification of SRP that we call HFERP. The key observation is that by replacing the Square map with a higher Q-rank instance of HFE, one can make the MinRank attack inefficient while maintaining efficient inversion. For simplicity of the exposition, we present the scheme with a single layer UOV component, noting that it is trivial to replace UOV with a multi-layer Rainbow via the same construction.

Choose a finite field $\mathbb{F}_q$ and let $\mathbb{E}$ be a degree d extension field over $\mathbb{F}_q$. Let $\phi : \mathbb{F}_q^d \to \mathbb{E}$ be an $\mathbb{F}_q$-vector space isomorphism. Also, let $o, r, s,$ and l be non-negative integers.

Key Generation Let $n = d + o - l$, $n' = d + o$ and $m = d + o + r + s$. The central map of HFERP is the concatenation of an HFE core map, $\mathcal{F}_{HFE}$, an UOV (or alternatively, Rainbow) section, $\mathcal{F}_R$, and the plus modifier, $\mathcal{F}_P$. Formal definitions of the maps are provided below:

- The HFE component is defined as $\mathcal{F}_{HFE} : \mathbb{F}_q^{n'} \to \mathbb{F}_q^d$ and is the result of the following composition:

$$\mathbb{F}_q^{n'} \xrightarrow{\pi_d} \mathbb{F}_q^d \xrightarrow{\phi} \mathbb{E} \xrightarrow{f} \mathbb{E} \xrightarrow{\phi^{-1}} \mathbb{F}_q^d$$

  where f is the HFE core map described in (1) and $\pi_d : \mathbb{F}_q^{d+o} \to \mathbb{F}_q^d$ is the projection onto the first d coordinates.
- The UOV (or alternatively, Rainbow) component is defined as

$$\mathcal{F}_R = (g^{(1)}, \ldots, g^{(o+r)}) : \mathbb{F}_q^{n'} \to \mathbb{F}_q^{o+r}$$

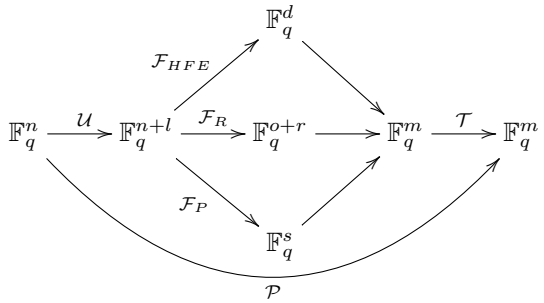
  following the normal construction of the UOV signature scheme where $\mathcal{V} = \{1, \ldots, d\}$ and $\mathcal{O} = \{d+1, \ldots, d+o\}$. For every $k \in \{1, \ldots, o+r\}$, the quadratic polynomial $g^{(k)}$ is of the following form:

$$g^{(k)}(x_1, \ldots, x_{n'}) = \sum_{i \in \mathcal{O}, j \in \mathcal{V}} \alpha^{(k)} x_i x_j + \sum_{i,j \in \mathcal{V}, i \leq j} \beta_{i,j}^{(k)} x_i x_j + \sum_{i \in \mathcal{V} \cup \mathcal{O}} \gamma_i^{(k)} x_i + \eta^{(k)}$$

  where $\alpha^{(k)}$, $\beta_{i,j}^{(k)}$, $\gamma_i^{(k)}$, and $\eta^{(k)}$ are chosen at random from $\mathbb{F}_q$.
- The Plus modification is defined as $\mathcal{F}_P = (h^{(1)}, \ldots, h^{(s)}) : \mathbb{F}_q^{n'} \to \mathbb{F}_q^s$ which consists of s randomly generated quadratic polynomials.

An affine embedding $\mathcal{U} : \mathbb{F}_q^n \to \mathbb{F}_q^{n'}$ of full rank and an affine isomorphism $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ are chosen for the butterfly construction as is common in big field schemes. The public key is given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{U} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, where $\mathcal{F} = \mathcal{F}_{HFE} \| \mathcal{F}_R \| \mathcal{F}_P$ ($\|$ being the concatination function), and the private key

is represented by the following figure:



Encryption Given a message $M \in \mathbb{F}_q^n$, the ciphertext is computed as $C = \mathcal{P}(M) \in \mathbb{F}_q^m$.
Decryption Given a ciphertext $C = (c_1, \ldots, c_m) \in \mathbb{F}_q^m$, the decryption process is the following:

1. Compute $\mathbf{x} = (x_1, \ldots, x_m) = \mathcal{T}^{-1}(C)$.
2. Compute $\mathbf{X} = \phi(x_1, \ldots, x_d) \in \mathbb{E}$.
3. Use the Berlekamp algorithm to compute the inverse of the HFE polynomials to recover $\mathbf{y} = (y_1, \ldots, y_d)$.
4. Given the vinegar values $y_1, \ldots, y_d$, solve the system of $o+r$ linear equations in the $n' - d = o$ variables $u_{d+1}, \ldots, u_{n'}$ given by
$$g^{(k)}(y_1, \ldots, y_d, u_{d+1}, \ldots, u_{n'}) = x_{d+k}$$
for $k = 1, \ldots, o + r$. The solution is denoted $(y_{d+1}, \ldots, y_{n'})$.
5. Compute the plaintext $M \in \mathbb{F}_q^n$ by finding the preimage of $(y_1, \ldots, y_{n'})$ under the affine embedding $\mathcal{U}$.

6 Complexity of Attack

In this section we derive tight complexity estimates or proofs of resistance for the principal relevant attacks on HFERP. These attacks include the direct algebraic attack, the MinRank attack, the small field MinRank and dual rank attacks, and the invariant attack.

6.1 Algebraic Attack

The algebraic attack attempts to invert the public key at a ciphertext directly via the calculation of a Gröbner basis. It is commonly believed that the closeness of the solving degree of a polynomial system, the degree at which the Gröbner basis is resolved, and the degree of regularity, the degree at which a non-trivial syzygy producing a degree fall first occurs, is a generic property. Thus the lower bound on the complexity of the algebraic attack that the degree of regularity provides is likely a tight bound, and is consequently a critical quantity for analyzing the security of the scheme.

Theorem 1 *The degree of regularity of the public key of HFERP is bounded by*

$$d_{reg} \leq \begin{cases} \frac{(q-1)\lceil \log_q(D) \rceil}{2} + 2 \text{ if } q \text{ is odd or } \lceil \log_q(D) \rceil \text{ is even,} \\ \frac{(q-1)\left(\lceil \log_q(D) \rceil + 1\right)}{2} + 1 \text{ otherwise.} \end{cases}$$

Proof. There is a linear function of the public key separating the HFE polynomials $\mathcal{H}$ from the non-HFE polynomials $\mathcal{N}$. Trivially, the d_{reg} is bounded by the degree of regularity of the system $\mathcal{H}$, which, via [28, Theorem 4.2], produces the above bound.

One must note that the above bound is not what is needed to ensure security. Instead we require a lower bound. Extensive experimentation shows that for very small q, the above estimate is tight. We have, however, a further complication. In general, adding more polynomials to an ideal may decrease its degree of regularity. To address this issue we have conducted small scale experiments showing that the degree of regularity and solving degree behave similarly to those of random systems, see Section 7.

Conjecture 1 *Under the assumption that the degree of regularity is at least* $\lceil \log_q(D) \rceil + 2$ *for small odd* q *and sufficiently large* n*, the complexity of the algebraic attack is given by*

$$Comp._{alg} = \mathcal{O}\left(\binom{n + d_{reg}}{d_{reg}}^2 \binom{n}{2} \right) = \mathcal{O}\left(n^{2\lceil \log_q(D) \rceil + 6} \right).$$

6.2 MinRank Attack

The min-rank attack proposed in [16] is so successful due to the Q-rank of the squaring map within SRP being equal to one. By changing the square map component to an HFE core map, we are able to thwart such an attack on HFERP. This subsection walks through the attack proposed in [16] , with HFERP in mind, and proves that the min-Q-rank of HFERP differs from SRP.

Note that, similar to SRP, the public key of HFERP has an analogous scheme without embedding as long as $\pi_d \circ \mathcal{U}$ is of full rank, which it is defined to be in this scheme. Let $\pi'_d : \mathbb{F}_q^n \to \mathbb{F}_q^d$ be the projection onto the first d coordinates and find a projection $\rho : \mathbb{F}_q^{n+l} \to \mathbb{F}_q^n$ such that $\mathcal{U}' = \rho \circ \mathcal{U}$ has full rank and $\pi'_d \circ \mathcal{U}' = \pi_d \circ \mathcal{U}$. Let $\mathcal{F}^* : \mathbb{E} \to \mathbb{E}$ represent the chosen high Q-rank HFE core map so that $\mathcal{F}_{HFE} = \phi^{-1} \circ \mathcal{F}^* \circ \phi \circ \pi_d$. Then identify the Rainbow and random components as $\mathcal{F}'_R : \mathcal{F}_R \circ \mathcal{U} \circ {\mathcal{U}'}^{-1}$ and $\mathcal{F}'_P : \mathcal{F}_P \circ \mathcal{U} \circ {\mathcal{U}'}^{-1}$ respectively. Thus, one can see that

$$\mathcal{T} \circ \begin{bmatrix} \phi \circ \mathcal{F}^* \circ \phi^{-1} \circ \pi_d \\ \mathcal{F}_R \\ \mathcal{F}_P \end{bmatrix} \circ \mathcal{U} = \mathcal{T} \circ \begin{bmatrix} \phi \circ \mathcal{F}^* \circ \phi^{-1} \circ \pi'_d \\ \mathcal{F}'_R \\ \mathcal{F}'_P \end{bmatrix} \circ \mathcal{U}'.$$

Notice that the attack on SRP was not just a min-rank attack on the public key of SRP, but on a linear combination of public forms of SRP that had low Q-rank over the degree d extension used by the squaring component. This method allowed the attack to ignore the fact that the public key of an instance of SRP was expected to be of high rank. Thus, to demonstrate that HFERP resists such an attack, we briefly outline the method of deriving the linear combination of public forms from [16] for HFERP and prove that the min-Q-Rank of the result is sufficiently high to resist such an attack.

Let α be a primitive element of the degree d extension $\mathbb{E}$ of $\mathbb{F}_q$. Fix a vector space isomorphism $\phi : \mathbb{F}_q^d \to \mathbb{E}$ defined by $\phi(\bar{x}) = \sum_{i=0}^{d-1} x_i \alpha^i$. Then, fix a one dimensional representation $\Phi : \mathbb{E} \to \mathbb{A}$ defined by $a \overset{\Phi}{\mapsto} (a, a^q, \ldots, a^{q^{d-1}})$. Next, define $\mathcal{M}_d : \mathbb{F}_q^d \to \mathbb{A}$ by $\mathcal{M}_d = \Phi \circ \phi$. It was demonstrated you can look at this map through the following matrix representation

$$\mathbf{M}_d = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha & \alpha^q & \ldots & \alpha^{q^{d-1}} \\ \alpha^2 & \alpha^{2q} & \ldots & \alpha^{2q^{d-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{d-1} & \alpha^{(d-1)q} & \ldots & \alpha^{(d-1)q^{d-1}} \end{bmatrix} \in \mathcal{M}_{d\times d}(\mathbb{E})$$

This matrix allows the passage from $\mathbb{F}_q^d$ and $\mathbb{A}$ easily by right multiplication with $\mathbf{M}_d$ or $\mathbf{M}_d^{-1}$. Next are a few more definitions necessary to be able to look at a matrix representation of the public key:

$$\widetilde{\mathbf{M}}_d = \begin{bmatrix} \mathbf{M}_d & 0 \\ 0 & \mathbf{I}_{o+r+s} \end{bmatrix} \in \mathcal{M}_{m\times m}(\mathbb{E})$$

$$\widehat{\mathbf{M}}_d = \begin{bmatrix} \mathbf{M}_d \\ \mathbf{0}_{o\times d} \end{bmatrix} \in \mathcal{M}_{(d+o)\times d}(\mathbb{E})$$

Finally, define $\mathbf{F}^{*i}$ be the matrix representation of the quadratic form over $\mathbb{A}$ of the i^{th} Frobenius power of the chosen HFE core map. Now we have all the necessary notation to view the public key as a matrix equation.

Denote the m-dimensional vector of $(d+o)\times(d+o)$ symmetric matrices associated by the private key as follows:

$$(\mathbf{F}_{(HFE,0)}, \ldots, \mathbf{F}_{(HFE,d-1)}, \mathbf{F}_{(R,0)}, \ldots, \mathbf{F}_{(R,o+r-1)}\mathbf{F}_{(P,0)}, \ldots, \mathbf{F}_{(P,s-1)}). \quad (2)$$

Note that the function corresponding to the application of each coordinate of a vector of the quadratic forms followed by the application of a linear map represented by a matrix is denoted as a right product of the vector and a matrix representation of the linear map.

Next, observe

$$(\mathbf{F}_{(HFE,0)}, \ldots, \mathbf{F}_{(HFE,d-1)})\mathbf{M}_d = (\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top, \ldots, \widehat{\mathbf{M}}_d\mathbf{F}^{*(d-1)}\widehat{\mathbf{M}}_d^\top),$$

which yields

$$(\bar{x}\mathbf{F}_{(HFE,0)}\bar{x}^\top, \ldots, \bar{x}\mathbf{F}_{(HFE,d-1)}\bar{x}^\top)\mathbf{M}_d = \\ (\bar{x}\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top\bar{x}^\top, \ldots, \bar{x}\widehat{\mathbf{M}}_d\mathbf{F}^{*(d-1)}\widehat{\mathbf{M}}_d^\top\bar{x}^\top),$$

as a function of $\bar{x}$. This gives the following equation:

$$(\mathbf{F}_{(HFE,0)}, \ldots, \mathbf{F}_{(HFE,d-1)}, \mathbf{F}_{(R,0)}, \ldots, \mathbf{F}_{(P,s-1)})\widetilde{\mathbf{M}}_d = \\ (\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top, \ldots, \widehat{\mathbf{M}}_d\mathbf{F}^{*(d-1)}\widehat{\mathbf{M}}_d^\top, \mathbf{F}_{(R,0)}, \ldots, \mathbf{F}_{(P,s-1)}) \tag{3}$$

Now, look to the relation between the public key and its corresponding private key central maps:

$$(\mathbf{P}_0, \ldots, \mathbf{P}_{m-1})\mathbf{T}^{-1} = (\mathbf{U}\mathbf{F}_{(HFE,0)}\mathbf{U}^\top, \ldots, \mathbf{U}\mathbf{F}_{(P,s-1)}\mathbf{U}^\top). \tag{4}$$

By combining equations 3 and 4, we have the following:

$$(\mathbf{P}_0, \ldots, \mathbf{P}_{m-1})\mathbf{T}^{-1}\widetilde{\mathbf{M}}_d = \\ (\mathbf{U}\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top\mathbf{U}^\top, \ldots, \mathbf{U}\widehat{\mathbf{M}}_d\mathbf{F}^{*(d-1)}\widehat{\mathbf{M}}_d^\top\mathbf{U}^\top, \mathbf{U}\mathbf{F}_{(R,0)}\mathbf{U}^\top, \ldots, \mathbf{U}\mathbf{F}_{(P,s-1)}\mathbf{U}^\top)$$

As in [16], let $\widehat{\mathbf{T}} = \mathbf{T}^{-1}\widetilde{\mathbf{M}}_d = [t_{i,j}] \in \mathcal{M}_{m\times m}(\mathbb{E})$ and $\mathbf{W} = \mathbf{U}\widehat{\mathbf{M}}_d$. This identification produces

$$\sum_{i=0}^{m-1} t_{i,0}\mathbf{P}_i = \mathbf{W}\mathbf{F}^{*0}\mathbf{W}^\top. \tag{5}$$

Since the rank of $\mathbf{F}^{*i}$ is equal to the Q-rank of the quadratic form of the HFE core map for all i, the rank of this $\mathbb{E}$-linear combination of the public matrices is bounded by the minimum of the rank of $\mathbf{U}\widehat{\mathbf{M}}_d$ and the rank of $\mathbf{F}^{*0}$, *id est* the Q-rank of our HFE core map. This statement forms the following theorem:

Theorem 2 *The min-Q-rank of the public key P of HFERP(q,d,o,r,s,l) is given by:*

$$\textit{min-Q-rank(P)} \leq \textit{min}\{\textit{Rank}(\mathbf{U}\widehat{\mathbf{M}}_d), \textit{Rank}(\mathbf{F}^{*0})\}$$

Proof. The proof in [16] describes the parameters in which the min-Q-rank(P) can be equal to zero. So, we move forward with the assumption that $\mathbf{U}\widehat{\mathbf{M}}_d \neq 0$, which occurs with high probability when $d > l$. In (5) we have a linear combination of the public key equations equal to the following:

$$\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^\top = \mathbf{U}\widehat{\mathbf{M}}_d\mathbf{F}^{*0}\widehat{\mathbf{M}}_d^\top\mathbf{U}^\top. \tag{6}$$

This proves our result.

It should be noted that $\mathbf{U}$, $\widehat{\mathbf{M}}_d$, and $\mathbf{F}^{*0}$ are chosen by the user. They can easily be chosen in such a way such that

$$\text{min-Q-rank(P)} = \min\{\textit{Rank}(\mathbf{U}\widehat{\mathbf{M}}_d), \textit{Rank}(\mathbf{F}^{*0})\}.$$

This would also occur with high probability if $\mathbf{U}$, $\widehat{\mathbf{M}}_d$, and $\mathbf{F}^{*0}$ were randomly generated. Directly from [15], we also have the following complexity for the MinRank attack on HFERP:

Corollary 1 *The complexity of the MinRank attack with minors modeling on HFERP is given by*

$$Comp._{Minors} = \mathcal{O}\left(\binom{m + \lfloor \log_q(D) \rfloor}{\lceil \log_q(D) \rceil}^2 \binom{m}{2}\right) = \mathcal{O}\left(m^{2\lceil \log_q(D) \rceil + 2}\right).$$

6.3 Base-Field Rank and Invariant Attacks

Variants of several attacks applicable to other versions of the Rainbow cryptosystem are applicable to HFERP. These include the linear-algebra-search version of MinRank [29], the HighRank attack [29] and the UOV invariant attack [4].

The MinRank attack works by randomly choosing one or more vectors $\mathbf{w}_j$ in the plaintext space and solving for a linear combination $t_i \in \mathbb{F}$ of the plaintext equations satisfying:

$$\sum_{i=1}^{m} t_i Df_i(\mathbf{w}_j) = 0$$

The attack succeeds when $\mathbf{w}_j$ is in the kernel of a low rank linear combination of differentials of the public polynomials. In the case of HFERP, the HFE component equations form a d-dimensional subspace of the public equations having rank d over $\mathbb{F}$. Note that the attacker can remove up to $d-1$ equations while preserving at least a one dimensional subspace of low rank maps. Thus, the attack can succeed with a one dimensional solution space for t_i and only a single $\mathbf{w}_j$ as long as $m \leq n + d$.

If $m > n + d$, the adversary may still use a single vector $\mathbf{w}_j$ to constrain the t_i's rather than attempting to find two vectors in the kernel of the HFE equations. In this case, the attacker must search through an $m - n - d + 1$ dimensional space of spurious solutions to find the useful 1 dimensional space of t_is. This method is still less expensive than searching for two vectors in the kernel of the HFE equations when $m < n + 2d$.

It should be further noted that, since the differentials of the oil maps will map any vector in the kernel of the HFE equations to the d-dimensional HFE input space, we expect an $o_1 + r_1 - d$ dimensional subspace of the oil equations to also have such a vector in the kernel of their differentials, see Figure 1. Thus, when $m < n + \max(d, o_1 + r_1)$, vectors in the HFE kernel can be recognized, because they are in the kernel of an unusually large subspace of the public equations, and when $2d < n$ the linear combinations of the public equations from the HFE and oil spaces can be recognized due to their low rank.

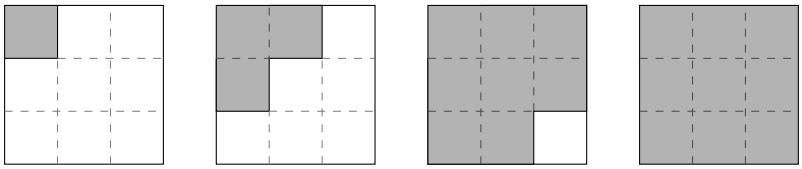


Fig. 1. The shape of the matrix representations of the central maps of HFERP. The shaded regions represent possibly nonzero values while unshaded areas have coefficients of zero.

Thus the complexity of MinRank (for plausible choices of m) is

$$Comp._{MinRank} = \begin{cases} \mathcal{O}\left(q^d m^\omega\right) & m < n + \max(d, o_1 + r_1) \\ \mathcal{O}\left(q^{d+m-n-\max(d,o_1+r_1)} n^\omega\right) & m \geq n + \max(d, o_1 + r_1) \\ & m < n + d + \max(d, o_1 + r_1) \\ & n > 2d \\ \mathcal{O}\left(q^{m-n} n^\omega\right) & m \geq n + \max(d, o_1 + r_1) \\ & m < n + 2d \\ & n \leq 2d \\ \mathcal{O}\left(q^{2d} m^\omega\right) & m < 2n + \max(d, o_1 + r_1 - d) \\ & \text{No better attack.} \end{cases}$$

In the HighRank attack, the attacker randomly selects linear combinations of the public polynomials with the hope of selecting a polynomial with significantly less than full rank. This attack takes advantage of the $d + o_1 + r_1$-dimensional subspace of the public polynomials generated by the HFE maps and either the Rainbow-1 maps of Figure 1 or for UOV of the d-dimensional HFE subspace. The complexity of the attack is then:

$$Comp._{HighRank} = \mathcal{O}\left(q^{m-d-o_1-r_1} n^\omega\right).$$

It should also be noted that linear combinations of HFE and Rainbow-1 polynomials form an $m - s$ dimensional subspace of the public polynomials, that act linearly on the $o_2 - l$ dimensional preimage under $\mathcal{U}$ of the oil subspace. This bounds their rank to be at most $2d$. Noting that the probability that a random square matrix has corank a is approximately q^{-a^2}, we see that, the high rank attack can be straightforwardly applied if $2d < n - \sqrt{m - d - o_1 - r_1}$.

Additionally, the HighRank attack can be combined with the oil and vinegar invariant attack to distinguish linear combinations of the HFE and Rainbow

maps from other linear combinations of the public maps. Here, a pair of maps from the HFE and Rainbow subspace can be identified by restricting their differentials to a subspace of the plaintext space in which both maps are full rank, and checking to see if $(Dp_1)^{-1}Dp_2$ has a large invariant subspace (which will be the intersection of the preimage of the oil subspace under $\mathcal{U}$ and the subspace used to restrict the differentials). This allows the high rank attack to be applied with similar complexity as long as $2d < n - \sqrt{\frac{m-d-o_1-r_1}{2}}$: Applying the attack will involve testing no more than $\left(q^{\frac{m-d-o_1-r_1}{2}}\right)^2 = q^{m-d-o_1-r_1}$ pairs of rank $n-2d$ maps, and therefore this step will not dominate the complexity of the approximately $q^{m-d-o_1-r_1}$ rank computations involved in the HighRank step.

If $2d \geq \zeta$, where $\zeta_1 = n - \sqrt{\frac{m-d-o_1-r_1}{2}}$, the complexity of HighRank is given by:

$$Comp._{HighRank} = \begin{cases} Comp._{HighRank} = \mathcal{O}\left(q^{m-d}n^{\omega}\right) & 2d \geq \zeta_1 \\ Comp._{HighRank} = \mathcal{O}\left(q^{m-d-o_1-r_1}n^{\omega}\right) & 2d < \zeta_1. \end{cases}$$

Finally, when $2d \geq n - \sqrt{\frac{m-d-o_1-r_1}{2}}$, as in the UOV attack, the previous steps must be combined with a projection, aimed at removing enough vinegar variables that the restriction of the differentials of linear combinations of HFE and Rainbow maps to the projected plaintext space is less than full rank. This yields a complexity for hybrid HighRank/UOV invariant type attacks of:

$$Comp._{UOV} = \begin{cases} \mathcal{O}\left(q^{m-d-o_1-r_1}n^{\omega}\right) & n > \zeta_2 \\ \mathcal{O}\left(q^{m-d-o_1-r_1+\sqrt{\frac{m-d-o_1-r_1}{2}}+2d-n}(o_1+o_2-l)^4\right) & n \leq \zeta_2. \end{cases}$$

where $\zeta_2 = 2d + \sqrt{\frac{m-d-o_1-r_1}{2}}$. This attack may also be applied to the Rainbow-2 maps of Figure 1 in which case the complexity is:

$$Comp._{UOV2} = \begin{cases} \mathcal{O}\left(q^s n^{\omega}\right) & n > 2d + 2o_1 + \sqrt{\frac{s}{2}} \\ \mathcal{O}\left(q^{s+\sqrt{\frac{s}{2}}+2d+2o_1-n}(o_2-l)^4\right) & n \leq 2d + 2o_1 + \sqrt{\frac{s}{2}}. \end{cases}$$

7 Parameter Selection and Experimental Results

We propose single-layer parameters (A) and (B) for 80-bit security and multi-layer parameters (C) and (D) for 128-bit security :

(A) $(q = 3, d = 42, o = 21, r = 15, s = 17, l = 0, D = 3^7 + 1)$

(B) $(q = 3, d = 63, o = 21, r = 11, s = 10, l = 0, D = 3^7 + 1)$

(C) $(q = 3, d = 85, o_1 = o_2 = 70, r_1 = r_2 = 89, s = 61, l = 0, D = 3^7 + 1)$

(D) $(q = 3, d = 60, o_1 = o_2 = 40, r_1 = r_2 = 23, s = 40, l = 0, D = 3^9 + 1)$

Then we have the following values for (n, m): $(63, 95)$ for (A), $(84, 105)$ for (B), $(225, 464)$ for (C), and $(140, 226)$ for (D). The security level for suggested parameters is estimated by all the attack in §6. Here, we assume that the degree of regularity for direct attack is 10 by Conjecture 1 for (A),(B), and (C) while it is 12 for (D).

To draw a direct comparison with HFE, note that to achieve the same security level as HFERP, an HFE scheme requires m equations, and hence $n = m$ variables. Therefore secure HFE public keys are far larger while offering slower decryption due to the use of the Berlekamp algorithm in a far larger field.

We ran a series of experiments with Magma, see [30], on a 2.6 GHz Intel® Xeon$^{\mathrm{R}}$ CPU[1]. These are not optimized implementations.

	(A)	(B)	(C)	(D)
Key Generation	0.299 s	0.572 s	20.498 s	3.43 s
Encryption	0.001 s	0.001 s	0.006 s	0.001 s
Decryption	3.977 s	8.671 s	49.182 s	124.27 s
Secret Key Size	19.8KB	31.7KB	1344.0KB	226.0KB
Public Key Size	48.2KB	93.6KB	2905.7KB	552.3KB

Table 1. Experimental results for HFERP.

We also investigated the growth of the first fall degree (d_{reg}) as well as the solving degree with five experiments performed at each of eight different parameters sets. We directly compared these data with randomly generated systems, see Table 2.

For comparison, we include the semi-regular degree for systems of m equations in n variables. This quantity was calculated by computing the first non-positive coefficient in the series

$$S_{n,m}(t) = \frac{(1 - t^q)^n (1 - t^2)^m}{(1 - t)^n (1 - t^{2q})^m}.$$

[1] Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

Noting that the degree of regularity of the zero-dimensional ideal is the same as the first fall degree of the ideal generated by the homogeneous components of the generators of highest degree. We derive the above formula as the fusion of the techniques in [31] and [32].

It is clear that the degree of regularity of the small scale instances of HFERP grows in relation to that of random schemes. By the data in the tables, we can estimate that the degree of regularity for direct attack on (A) and (B) is greater than 9 at least.

Table 2. Direct attack experiment data for various values of d, o, r, s. (s.r.d. stands for semi- regular degree)

			HFERP		Random		
(q, d, o, r, s, l, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(3, 8, 4, 3, 3, 0, 2188)$	12	18	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	4
$(3, 10, 5, 4, 3, 0, 2188)$	15	22	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	5
$(3, 12, 6, 5, 4, 0, 2188)$	18	27	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	5
$(3, 14, 7, 5, 5, 0, 2188)$	21	31	$6, 5, 5, 5, 5$	$6, 6, 6, 6, 6$	$5, 5, 5, 5, 5$	$6, 6, 6, 6, 6$	6

Table 2.A. Direct Attack, $d = 2o, d + o \fallingdotseq 2(r + s), o = 4, 5, 6, 7$

			HFERP		Random		
(q, d, o, r, s, l, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(3, 9, 3, 2, 2, 0, 2188)$	12	16	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	5
$(3, 12, 4, 2, 2, 0, 2188)$	16	20	$5, 6, 6, 5, 5,$	$5, 6, 6, 6, 5$	$6, 5, 6, 6, 5$	$6, 6, 6, 6, 6$	6
$(3, 15, 5, 3, 3, 0, 2188)$	20	26	$6, 5, 5, 5, 5$	$6, 6, 6, 6, 6$	$5, 5, 5, 6, 5$	$6, 6, 6, 6, 6$	6
$(3, 18, 6, 3, 3, 0, 2188)$	24	30	$5, 5, 5, 5, 5$	$7, 7, 7, 7, 7$	$5, 5, 5, 5, 7$	$7, 7, 7, 7, 7$	7

Table 2.B. Direct Attack, $d = 3o, r + s \fallingdotseq o, o = 3, 4, 5, 6$

			HFERP		Random		
(d, o, r, s, l, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(3, (3, 3), (4, 4), 2, 0, 2188)$	9	19	$3, 3, 3, 3, 3$	$3, 3, 2, 3, 2$	$3, 3, 3, 3, 3$	$2, 3, 3, 2, 2$	3
$(7, (6, 6), (7, 7), 5, 0, 2188)$	19	38	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	5
$(10, (8, 8), (11, 11), 7, 0, 2188)$	26	55	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	5
$(14, (11, 11), (14, 14), 10, 0, 2188)$	36	74	5		5		6

Table 2.C. Direct Attack,
$d \fallingdotseq 3.4a, o \fallingdotseq (2.8a, 2.8a), r \fallingdotseq (3.56a, 3.56a), s \fallingdotseq 2.44a, a = 1, 2, 3, 4$

			HFERP		Random		
(d, o, r, s, l, D)	n	m	d_{reg}	sol. deg	d_{reg}	sol. deg	s.r.d.
$(5, (3, 3), (2, 2), 3, 0, 3^9 + 1)$	11	18	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	$4, 4, 4, 3, 4$	4
$(7, (5, 5), (3, 3), 5, 0, 3^9 + 1)$	17	28	$4, 4, 4, 4, 4$	$4, 4, 4, 4, 4$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	5
$(10, (6, 6), (4, 4), 6, 0, 3^9 + 1)$	22	36	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$5, 5, 5, 5, 5$	$6, 6, 6, 6, 6$	6
$(12, (8, 8), (5, 5), 8, 0, 3^9 + 1)$	28	46	$5, 5$	$6, 6$	$5, 5$	6	6

Table 2.D. Direct Attack,
$d \fallingdotseq 2.4a, o \fallingdotseq (1.6a, 1.6a), r \fallingdotseq (0.92a, 0.92a), s \fallingdotseq 1.6a, a = 2, 3, 4, 5$

8 Conclusion

SRP was an ambitious encryption scheme attempting to combine the efficiency of the inversion of Square with the security of Rainbow to achieve security with a small blow-up factor between the plaintext and ciphertext. Unfortunately, this technique was a bit too ambitious.

Interestingly, the idea of replacing Square with a more general and higher Q-rank HFE primitive seems to solve this problem. Even more interestingly, the resulting scheme, HFERP, though in principle assailable via essentially every major cryptanalytic technique available in multivariate cryptography, appears to be out of range of these myriad attacks.

The parameter ℓ in SRP was introduced for efficiency, attempting to reduce the public key size while maintaining the algebraic structure of the scheme. We have found that this quantity adds nothing to security and have set it equal to zero for our suggested parameters. An interesting possible future problem is to determine whether ℓ can be securely set to a value larger than zero and thereby reduce public key size. For now, we err on the side of caution, and conservatively use all of the entropy we can get.

9 Acknowledgments

The first and fourth authors were supported by JST CREST (Grant Number JPMJCR14D6).

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. Mosca, M.: Cybersecurity in a quantum world: will we be ready? Workshop on Cybersecurity in a Post-Quantum World, Invited Presentation (2015) https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf.
3. Yasuda, T., Sakurai, K. In: A Multivariate Encryption Scheme with Rainbow. Springer International Publishing, Cham (2016) 236–251
4. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. EUROCRYPT 1999. LNCS **1592** (1999) 206–222
5. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. ACNS 2005, LNCS **3531** (2005) 164–175
6. Petzoldt, A., Chen, M.S., Yang, B.Y., Tao, C., Ding, J. In: Design Principles for HFEv- Based Multivariate Signature Schemes. Springer Berlin Heidelberg, Berlin, Heidelberg (2015) 311–334
7. Patarin, J.: Hidden Field Equations (HFE) and Isomorphisms of Polynomials: two new Families of Asymmetric Algorithms. Eurocrypt '96, Springer **1070** (1996) 33–48
8. 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

9. Ding, J., Petzoldt, A., Wang, L.: The cubic simple matrix encryption scheme. [33] 76–87
10. Porras, J., Baena, J., Ding, J.: ZHFE, A new multivariate public key encryption scheme. [33] 229–245
11. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. [33] 180–196
12. 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)
13. Moody, D., Perlner, R.A., Smith-Tone, D.: Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme. [34] 255–271
14. Cabarcas, D., Smith-Tone, D., Verbel, J.A.: Key recovery attack for ZHFE. [34] 289–308
15. Vates, J., Smith-Tone, D.: Key recovery attack for all parameters of HFE-. [34] 272–288
16. Perlner, R.A., Petzoldt, A., Smith-Tone, D. In: Total Break of the SRP Encryption Scheme. Springer, In press. (2017)
17. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: EUROCRYPT. (1996) 33–48
18. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature verification and message-encryption. Eurocrypt '88, Springer **330** (1988) 419–545
19. Berlekamp, E.R.: Factoring polynomials over large finite fields. Mathematics of Computation **24** (1970) pp. 713–735
20. Clough, C., Baena, J., Ding, J., Yang, B.Y., Chen, M.S.: Square, a New Multivariate Encryption Scheme. In Fischlin, M., ed.: CT-RSA. Volume 5473 of Lecture Notes in Computer Science., Springer (2009) 252–264
21. Patarin, J.: The oil and vinegar algorithm for signatures. Presented at the Dagsthul Workshop on Cryptography (1997)
22. Patarin, J., Goubin, L., Courtois, N.: C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai. In Ohta, K., Pei, D., eds.: ASIACRYPT. Volume 1514 of Lecture Notes in Computer Science., Springer (1998) 35–49
23. Shamir, A., Kipnis, A.: Cryptanalysis of the oil & vinegar signature scheme. CRYPTO 1998. LNCS **1462** (1998) 257–266
24. Moody, D., Perlner, R.A., Smith-Tone, D.: Key recovery attack on the cubic ABC simple matrix multivariate encryption scheme. In Avanzi, R., Heys, H.M., eds.: Selected Areas in Cryptography - SAC 2016 - 23rd International Conference, St. John's, NL, Canada, August 10-12, 2016, Revised Selected Papers. Volume 10532 of Lecture Notes in Computer Science., Springer (2016) 543–558
25. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. Advances in Cryptology - CRYPTO 1999, Springer **1666** (1999) 788
26. 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
27. 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

28. Ding, J., Hodges, T.J.: Inverting HFE systems is quasi-polynomial for all fields. In Rogaway, P., ed.: Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. Volume 6841 of Lecture Notes in Computer Science., Springer (2011) 724–742
29. Goubin, L., Courtois, N.: Cryptanalysis of the ttm cryptosystem. In Okamoto, T., ed.: ASIACRYPT. Volume 1976 of Lecture Notes in Computer Science., Springer (2000) 44–57
30. 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).
31. Yang, B., Chen, J.: Theoretical analysis of XL over small fields. In Wang, H., Pieprzyk, J., Varadharajan, V., eds.: Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004. Proceedings. Volume 3108 of Lecture Notes in Computer Science., Springer (2004) 277–288
32. Bardet, M., Faugre, J., Salvy, B., Yang, B.: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In MEGA '05, 2005. Eighth International Symposium On Effective Methods In Algebraic Geometry (2005)
33. 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)
34. Lange, T., Takagi, T., eds.: Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings. Volume 10346 of Lecture Notes in Computer Science., Springer (2017)

A Toy Example

The purpose of the following toy example is to help the reader understand the process of generating a public key for an instance of HFERP as well as an example of encryption and decryption. The parameters used are by no means secure and are soley for instructional purposes.

Parameters of this toy example are as follows: $q = 7,\ d = o = r = 2,\ s = 1,$ and $l = 0$. Then, construct $\mathbb{E}$ a degree 2 extension field over $\mathbb{F}_7$. The chosen HFE core map is $f = \xi^{12}X^{14} + \xi^6 X^8 + \xi^{29}X^2$ where $\xi \in \mathbb{E}$. Let $\mathcal{T}$ and $\mathcal{U}$ be the following affine maps:

$$\mathcal{T} = \begin{bmatrix} 2\,1\,2\,4\,5\,0\,3 \\ 1\,1\,3\,3\,4\,4\,4 \\ 4\,2\,1\,3\,1\,0\,6 \\ 0\,1\,0\,1\,5\,5\,5 \\ 5\,5\,3\,6\,4\,2\,4 \\ 2\,5\,1\,6\,5\,6\,0 \\ 1\,1\,2\,2\,6\,4\,3 \end{bmatrix}, \mathcal{U} = \begin{bmatrix} 4\,6\,6\,4 \\ 3\,2\,0\,2 \\ 1\,1\,6\,5 \\ 3\,6\,6\,6 \end{bmatrix}$$

With the parameters described above, $\mathcal{F}$ can be represented as the follwing matrices over $\mathbb{F}_7$

$$F_1 = \begin{bmatrix} 0\,1\,0\,0 \\ 4\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \end{bmatrix}, F_2 = \begin{bmatrix} 0\,3\,0\,0 \\ 1\,6\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \end{bmatrix}, F_3 = \begin{bmatrix} 3\,1\,6\,1 \\ 3\,1\,4\,5 \\ 3\,4\,0\,0 \\ 3\,2\,0\,0 \end{bmatrix},$$

$$F_4 = \begin{bmatrix} 5\,1\,0\,3 \\ 0\,5\,0\,3 \\ 0\,4\,0\,0 \\ 6\,1\,0\,0 \end{bmatrix}, F_5 = \begin{bmatrix} 6\,0\,3\,4 \\ 6\,2\,4\,2 \\ 6\,3\,0\,0 \\ 0\,3\,0\,0 \end{bmatrix}, F_6 = \begin{bmatrix} 4\,4\,1\,1 \\ 3\,0\,0\,3 \\ 3\,6\,0\,0 \\ 1\,2\,0\,0 \end{bmatrix}, F_7 = \begin{bmatrix} 6\,3\,2\,3 \\ 4\,4\,0\,6 \\ 2\,3\,1\,3 \\ 6\,4\,0\,6 \end{bmatrix}$$

P_1 and P_2 represent the HFE component, $P_3 \to P_6$ represent the rainbow component, and P_7 represents the plus component. With the public key generated by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{U}$, its matrix form over $\mathbb{F}_7$ is:

$$P_1 = \begin{bmatrix} 1\,1\,2\,5 \\ 1\,2\,3\,2 \\ 3\,2\,4\,4 \\ 3\,3\,0\,3 \end{bmatrix}, P_2 = \begin{bmatrix} 0\,2\,0\,6 \\ 4\,5\,2\,0 \\ 6\,3\,3\,4 \\ 3\,1\,2\,2 \end{bmatrix}, P_3 = \begin{bmatrix} 2\,3\,1\,4 \\ 4\,5\,4\,5 \\ 3\,5\,5\,1 \\ 5\,1\,0\,6 \end{bmatrix},$$

$$P_4 = \begin{bmatrix} 0\,6\,0\,2 \\ 1\,3\,0\,2 \\ 5\,1\,5\,1 \\ 5\,3\,0\,5 \end{bmatrix}, P_5 = \begin{bmatrix} 4\,3\,2\,3 \\ 6\,5\,2\,4 \\ 4\,3\,1\,5 \\ 5\,2\,4\,5 \end{bmatrix}, P_6 = \begin{bmatrix} 1\,4\,2\,2 \\ 3\,3\,6\,2 \\ 5\,4\,0\,0 \\ 3\,5\,5\,4 \end{bmatrix}, P_7 = \begin{bmatrix} 1\,3\,6\,0 \\ 0\,3\,4\,0 \\ 1\,2\,4\,2 \\ 2\,1\,6\,4 \end{bmatrix}$$

Given the following plaintext, $(2, 6, 1, 5)$, the resulting ciphertext is $(0, 0, 1, 3, 0, 4, 0)$.

Decryption: Given a ciphertext $(0, 0, 1, 3, 0, 4, 0)$, the following process is how you would obtain its corresponding plaintext.
Part of the secrect key:

$$\mathcal{T}^{-1} = \begin{bmatrix} 1\,6\,4\,2\,2\,2\,5 \\ 5\,4\,4\,6\,0\,5\,2 \\ 5\,3\,5\,2\,3\,2\,4 \\ 5\,6\,5\,5\,2\,1\,1 \\ 2\,5\,4\,2\,1\,5\,2 \\ 2\,5\,6\,6\,3\,5\,5 \\ 1\,2\,5\,4\,4\,0\,5 \end{bmatrix}, \mathcal{U}^{-1} = \begin{bmatrix} 4\,5\,2\,1 \\ 3\,1\,3\,1 \\ 4\,1\,2\,0 \\ 5\,6\,1\,1 \end{bmatrix}$$

Feed the ciphertext through $\mathcal{T}^{-1}$ to get

$$(0, 6, 2, 6, 0, 4, 6) \tag{7}$$

The first $d = 2$ elements are the corresponsing HFE outputs. Take these elements and adjust the HFE core map as follows:

$$f := f - 0\xi^{1-1} - 6\xi^{2-1} = \xi^{12}X^{14} + \xi^{6}X^{8} + \xi^{29}X^{2} + \xi$$

Perform the Berlekamp algorithm to find the preimage of f. In doing so in this toy example, you get $(0, 6)$. Next, construct the vector:

$$\overline{u} = [0, 6, u_1, u_2]\,.$$

Construct equations of the form $\overline{u}F_1\overline{u}^\top = x_i$ where x_i refers to the i^{th} element of (7), for $i \in \{3, 4, 5, 6\}$. This will result with the following equations:

$$\begin{bmatrix} 6u_1 + 1 \\ 3u_1 + 3u_2 + 5 \\ 2u_2 + 2 \\ u_1 + 2u_2 \end{bmatrix} = \begin{bmatrix} 2 \\ 6 \\ 0 \\ 4 \end{bmatrix}$$

Solving this system of equations gives us $u_1 = 6$ and $u_2 = 6$. Thus,

$$\overline{u} = [0, 6, 6, 6]\,.$$

Finally, feed this through $\mathcal{U}^{-1}$ to get the plaintext, $[2, 6, 1, 5]$.