2F - A New Method for Constructing Efficient Multivariate Encryption Schemes

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

daniel.smith@nist.gov

Abstract. The Support Minors method of solving the MinRank problem has contributed to several new cryptanalyses of post-quantum cryptosystems including some of the most efficient multivariate cryptosystems. While there are a few viable multivariate schemes that are secure against rank methods, the most prominent schemes, particularly for encryption, are not particularly efficient.
In this article we present a new generic construction for building efficient multivariate encryption schemes. Such schemes can be built from maps having rank properties that would otherwise be damaging, but are immune to traditional rank attack. We then construct one such efficient multivariate encryption scheme and show it to be about 100 times faster than other secure multivariate encryption schemes in the literature.

Key words: Multivariate Cryptography, MinRank, encryption

1 Introduction

In the past two years there have been several new advances in cryptanalysis that have significantly impacted the efficiency of various post-quantum cryptosystems. In particular, there has been a dramatic change in the power and variety of attacks exploiting rank properties of cryptosystems.

These new attacks rely on creative instances or more efficient modeling of the MinRank problem. The MinRank problem is the generic problem of finding a low rank linear combination of a collection of matrices.

In the rank-metric code-based regime, the basic problem of rank syndrome decoding is exactly an instance of MinRank. While it was previously assumed that the asymptotically most efficient attack on such schemes is the so-called support-trapping method, see [1], the new support minors technique of [2] not

This work was partially supported by a grant from the Simons Foundation (712530, DCST).

only significantly outperforms support-trapping asymptotically, but greatly reduces the efficiency of secure instances of these schemes. Schemes such as ROLLO [3] suffered a roughly square root security reduction.

In the multivariate arena, new MinRank instances have been found that have significantly changed the security level of prominent schemes. The rectangular MinRank attack of [4] reduces the security of Rainbow and is made possible by the efficiency of support minors modeling. Even in conjunction with the new "simple attack" of [5], the support minors technique supporting the rectangular MinRank attack is required for the cryptanalysis of larger parameters. While the new MinRank instances found in GeMSS, see [6], reduce the security level even with the minors technique, see [7], MinRank attacks powered by the support minors modeling make the HFEv- framework infeasible for practical use, see [8].

These results along with numerous other rank-based attacks on encryption and signature schemes, see [9–12], show that MinRank methods are a major obstacle to overcome in the construction of secure and efficient schemes. Thus we are in need of a method to side-step MinRank attacks.

Our Contributions We offer a new method for generating multivariate encryption schemes that are immune from rank attacks. The technique exploits the fact that modulus switching induces a nonlinear action over finite fields. We find that we can take essentially any multivariate encryption primitive and apply a modulus switching hack that we call 2F (since two fields of differing characteristic are used) to mask rank properties and construct an efficient encryption scheme. As an exercise, we construct from a primitive that is insecure against four different attacks (two rank-based, one differential and one algebraic) a new multivariate encryption scheme and show that the new 2F version is secure against these attacks.

The paper is organized as follows. In Section 2, we present some historical schemes that have relevance to our construction. Next, in Section 3, we introduce the generic 2F construction and verify its correctness. Then in Section 4, we introduce a prototype 2F scheme chosen to illustrate the effects on security the 2F construction has. Section 5 then provides a detailed security analysis highlighting the impact of the construction on every known attack surface. We then suggest parameters for the 128-bit and 143-bit security levels in Section 6, drawing performance comparisons with other secure multivariate encryption schemes in the literature. Finally, we conclude, reflecting on the changes we have seen in the design approach to multivariate cryptography and noting directions for future work.

2 Multivariate Encryption Schemes

In this section we describe the relevant historical schemes that motivate and power our new construction as well as schemes to which we want to draw comparison. We introduce them in order of their development and mention the known results on these schemes in the literature.

2.1 HFE

The HFE cryptosystem presented in [13] is a "big field" scheme in the lineage of C^*, see [14]. Such schemes rely on the vector space structure of finite extension fields to create vector-valued maps whose nonlinear component is derived from multiplication in the extension field.

Let $\mathbb{F}_q$ be a finite field with q elements, let $\mathbb{K}$ be a degree n extension of $\mathbb{F}_q$, and let $\phi : \mathbb{F}_q^n \to \mathbb{K}$ be an $\mathbb{F}_q$-vector space isomorphism. An HFE polynomial of degree bound D is a polynomial $f : \mathbb{K} \to \mathbb{K}$ of the form

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

where $\alpha_{ij}, \beta_i, \gamma \in \mathbb{K}$. We note that since the ith and jth Frobenius powers are $\mathbb{F}_q$-linear, f is $\mathbb{F}_q$-quadratic. The HFE public key is then given by

$$P(\mathbf{x}) = T \circ \phi^{-1} \circ f \circ \phi \circ U(\mathbf{x}),$$

where U and T are $\mathbb{F}_q$-linear or $\mathbb{F}_q$-affine maps, see Figure 1.

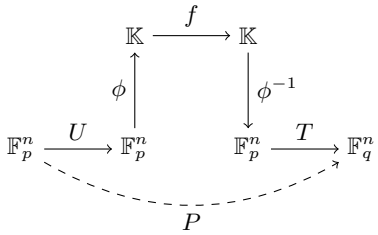

Fig. 1. The HFE scheme. Given the $\mathbb{F}_q$-quadratic map f, the $\mathbb{F}_q$-vector space isomorphism ϕ, and $\mathbb{F}_q$-linear maps U, and T, we construct the vector-valued function $P : \mathbb{F}_q^n \to \mathbb{F}_q^n$.

One may use the plain HFE as a public key encryption scheme. Encryption is accomplished by evaluating the public key at an encoding of the plaintext while decryption is performed by inverting each of the private maps sequentially. The inversion of the central map can be performed efficiently by using Berlekamp's algorithm, see [15], as long as D is fairly small.

There are a few attacks that make HFE inefficient. The first attack on HFE was [16]. An improvement on this technique in [9] modeled a MinRank instance with matrices over the small field with solutions in the large field and solved that instance with the minors modeling technique. The same MinRank instance was later found to be more efficiently solvable by once again returning to the Kipnis-Shamir method with variables defined over the extension field in [17]. The new attack on GeMSS, see [7], exploits a new MinRank instance associated with the structure of the HFE public key, but for naked HFE instances has the

same complexity as the above attack. Finally, the new method for using support minors for MinRank instances with solutions in extension fields of [8] significantly reduces the complexity of attacking HFE and renders it too inefficient for use.

2.2 SQUARE

The SQUARE multivariate encryption scheme, see [18], is a big field scheme using a simple monomial map that is two-to-one and that employs the projection modifier, the idea of fixing certain variables before the publication of the key to alter its algebraic properties. The SQUARE central map can be seen as an odd field HFE map but with degree bound 2 and no affine component.

Specifically, choose an odd characteristic field $\mathbb{F}_q$ and let $\mathbb{K}$ be a degree $n+p$ extension of $\mathbb{F}_q$. Let $f : \mathbb{K} \to \mathbb{K}$ be defined by $f(X) = X^2$. Let $T : \mathbb{F}_q^{n+p} \to \mathbb{F}_q^{n+p}$ be an invertible linear map and let $U : \mathbb{F}_q^n \to \mathbb{F}_q^{n+p}$ be an injection. We then generate a public key $P = T \circ \phi^{-1} \circ f \circ \phi \circ U$, where $\phi : \mathbb{F}_q^{n+p} \to \mathbb{K}$ is a $\mathbb{F}_q$-vector space isomorphism.

We note that unlike the case of HFE where most elements in the range of the central map have a unique preimage, the map f above is a 2-to-1 map. Thus, some sort of padding of the plaintext is necessary to ensure uniqueness of preimages.

SQUARE was broken in [19] with a differential attack similar to that of [20]. We note also that attacks in the style of [9, 17, 7, 8] also break SQUARE due to the very low Q-rank of the central map.

2.3 ABC Simple Matrix

The ABC Simple Matrix Encryption scheme of [21] uses the structure of a matrix algebra instead of an extension field to obtain its nonlinear central map. A modified version of this scheme was published in [22] to repair a high decryption failure rate of the original that leaked information about the secret key. Another version with a cubic public key was introduced in [23].

Fix parameters $s \leq r$ and set $n = rs$. Let $\mathbf{A}$ be an $r \times s$ matrix of random linear forms in n variables and let $\mathbf{B}$ and $\mathbf{C}$ be $s \times u$ and $s \times v$ matrices of random linear forms, respectively, where u and v are additional parameters of the system. We construct the quadratic map $F : \mathbb{F}_q^{rs} \to \mathbb{F}_q^{r(u+v)}$ by vectorizing the matrix product $\mathbf{A}\left[\mathbf{B}\ \mathbf{C}\right]$. The public key P is then computed by composing with linear transformations U and T.

As before, encryption is achieved by simply evaluating the public key at an encoding of the plaintext. To invert the central map, one parses the preimage of the ciphertext under T into an $r \times (u+v)$ matrix $\mathbf{V}$, sets $\mathbf{W}$ to be a formal left inverse of $\mathbf{A}$ consisting of rs unknowns w_{ij} and computes the product $\mathbf{WV}$. Since $\mathbf{W}$ is a left inverse of $\mathbf{A}$, this product must produce $\left[\mathbf{B}\ \mathbf{C}\right]$ evaluated at $U(\mathbf{x})$. This equality produces a system of $s(u+v)$ equations that are linear in $2rs$ unknowns, the values w_{ij} and the values x_i. Via Gaussian elimination, all of the variables w_{ij} can be eliminated to produce $s(u+v) - rs$ linear equations

in the rs unknown values x_i. Since this system has a small dimensional solution space, these relations can be used to transform the public key into a system with very few unknowns that can be solved directly to reveal the preimage.

Several attacks are known to affect the security of the ABC scheme. The first attack that broke security claims was [24]. The attack revealed that there exist rank $2s$ maps in the span of the public quadratic forms and outlined an algebraic/combinatorial attack that was more efficient than the designers anticipated. Subsequently, in [25] it was shown that the cubic scheme was vulnerable to a similar attack and is less efficient than the quadratic scheme. These attacks on the cubic version were further improved in [26]. Most recently, it was shown in [11] that increasing r relative to s decreases security against rank attacks at the same rate that it decreases the decryption failure rate, thus showing that there are fundamental limits to the efficiency of any such scheme.

2.4 PCBM

The PCBM multivariate encryption scheme, see [27] is a relatively new encryption scheme with similar algebraic structure to HFERP, see [28], but with a wildly different approach to parametrization. PCBM is currently the fastest published multivariate encryption scheme targeting CCA security that remains secure at the 128-bit level.

Fix q and n and let C be a random k-dimensional subspace of $\mathbb{F}_q^n$. Let $\mathbf{H}$ be an $(n-k) \times n$ matrix whose right kernel is C. Given k random $n \times (n-k)$ matrices $\mathbf{A}_i$, we form the products $\mathbf{B}_i = \mathbf{A}_i\mathbf{H}$. Then define the polynomial

$$f_i(\mathbf{x}) = \mathbf{x}\mathbf{B}_i\mathbf{x}^\top + \mathbf{x}\mathbf{L}_i,$$

where $\mathbf{L}_i$ is a random $n \times 1$ matrix.

Note that for any $\mathbf{x} \in \mathbb{F}_q^n$, the value $\mathbf{H}\mathbf{x}^\top$ uniquely identifies the coset of C in $\mathbb{F}_q^n$ containing $\mathbf{x}$. This value is encoded in extra polynomials g_i via a small instance of EFLASH or PFLASH, see [29, 30]. Finally, a large number of random quadratic equations h_i are included. The public key is then given by

$$P(\mathbf{x}) = T \circ (F \| G \| H) \circ U,$$

where T is affine, U is an affine embedding not intersecting C, $F = \left[f_i\right]$, $G = \left[g_i\right]$ and $H = \left[h_i\right]$.

Inversion is accomplished sequentially with the most interesting step being the inversion of F. Once the coset to which $\mathbf{x}$ belongs is extracted from G, it is easy to derive $\mathbf{x}$ by solving a linear system. Specifically, if $\mathbf{x} = \mathbf{x}' + \widehat{\mathbf{x}}$, where $\widehat{\mathbf{x}} \in C$ and $\mathbf{x}'$ is a coset representative derived from G we have that

$$f_i(\mathbf{x}) = (\mathbf{x}' + \widehat{\mathbf{x}})\,\mathbf{B}_i\left(\mathbf{x}'^\top + \widehat{\mathbf{x}}^\top\right) + (\mathbf{x}' + \widehat{\mathbf{x}})\mathbf{L}_i^\top = \mathbf{x}'\mathbf{B}_i\mathbf{x}'^\top + \widehat{\mathbf{x}}\mathbf{B}_i\mathbf{x}'^\top + (\mathbf{x}' + \widehat{\mathbf{x}})\mathbf{L}_i^\top,$$

for all i and thus we can solve linearly for $\widehat{\mathbf{x}}$ and $\mathbf{x}$.

The natural ways to attack this structure relate to searching for the large subspace C and MinRank methods attacking either the low rank, in general

$2(n-k)$, maps of F or by attacking the low Q-rank map G. The very large number of random maps H added mitigates these risks though, and the check equations that H provides makes PCBM have a very low decryption failure rate.

3 2F Modulus Switching

The first post-quantum cryptosystem to employ modulus switching was NTRU, see [31]. There, independent reduction modulo two coprime integers was used to mix and unmix operations in two polynomial rings.

While the original NTRU proposal was probabilistic in nature, with appropriate restrictions on the parameters, perfect correctness can be assured, such as is the case for the NIST Round 3 finalist NTRU, see [32]. The same analogy will hold with the 2F construction as well. In the following, we present a perfectly correct version of 2F but comment that we may select parameters to construct a probabilistic version as well.

Let p and q be primes with q much larger than p. Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be an efficiently invertible and computationally injective quadratic function. In particular, we may consider F to be any public key of a multivariate encryption scheme over a prime field. Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an invertible linear map and let ι be the map that casts a function on $\mathbb{F}_p^n$ as a function on $\mathbb{F}_q^n$ with the same coefficients considered as least absolute residues lying in $\mathbb{F}_q$. The 2F version of the map F is then $\widetilde{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ (with domain restricted to $(-\frac{p}{2}, \frac{p}{2})^n$) defined by

$$\widetilde{F} = T \circ \iota(F).$$

The reason this simple modulus-switching transformation changes the algebraic properties of the function is that ι is neither $\mathbb{F}_p$-linear nor $\mathbb{F}_q$-linear. A key observation is that even ι modulo p is not $\mathbb{F}_p$-linear since reduction is first computed modulo q and then modulo p. Thus, in general, $\widetilde{F} \neq T' \circ F$ for any $\mathbb{F}_p$-linear function T'.

First, we must show that the inversion process succeeds; that is, we must show that finding a preimage under T, reducing modulo p, and, finally computing a preimage under F produces a preimage of $\widetilde{F}$. This discussion establishes the necessary relationship between the sizes of p and q for the inversion of $\widetilde{F}$ to depend only on the ability to invert F.

Theorem 1. *Let p and q be odd primes, let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a homogeneous quadratic map and let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an invertible $\mathbb{F}_q$-linear transformation. If*

$$q > \frac{(p-1)^3}{4}\binom{n+1}{2},$$

then $\mathbf{y} = T \circ \iota(F)(\mathbf{x})$ if and only if $T^{-1}(\mathbf{y}) \pmod p = F(\mathbf{x})$

Proof. Clearly, $T^{-1}(\mathbf{y}) = \iota(F)(\mathbf{x})$. It remains to be shown that $\iota(F)(\mathbf{x}) \pmod p$ is the same as $F(\mathbf{x})$.

To accomplish the above task, we first consider computing the value of a coordinate function F_i over the integers. Since the least residue value of each coordinate of $\mathbf{x}$ is bounded in absolute value by $\frac{p-1}{2}$, as are the coefficients of F_i, each monomial has a least residue bounded in absolute value by $\frac{(p-1)^3}{8}$. As there are $\binom{n+1}{2}$ such monomials in F_i, the value calculated as an integer is bounded in absolute value by $\frac{(p-1)^3}{8}\binom{n+1}{2}$. Since this quantity is less than $\frac{q}{2}$, no reduction modulo q occurs in the computation of F_i. Therefore $\iota(F)(\mathbf{x})$ equals $F(\mathbf{x})$ over the integers, and thus reduced modulo p has the same value as $F(\mathbf{x})$.

Recall that valid decryption for any encryption scheme requires that a ciphertext has a unique preimage. Injective functions satisfy this property with probability 1; however, many encryption schemes are based on functions that are not injective, but satisfy some weaker property. We describe two such properties below.

Definition 1 *A finite family $\mathcal{F}$ of functions $F : A \to B$ on the finite sets A and B is* statistically injective *with bound p if given $G \xleftarrow{\mathcal{U}} \mathcal{F}$,*

$$\mathcal{P}\left(\exists a \neq a_0 \in A \text{ with } G(a) = G(a_0)\right) \leq p.$$

The family $\mathcal{F}$ is computationally injective *with bound p if given $G \xleftarrow{\mathcal{U}} \mathcal{F}$ and $a_0 \xleftarrow{\mathcal{U}} A$,*

$$\mathcal{P}\left(\exists a \in A \setminus \{a_0\} \text{ with } G(a) = G(a_0)\right) \leq p.$$

A good example of a statistically injective family of functions is the collection of public keys for the PCBM encryption scheme, see [27]. It is estimated in [27] that the probability that a uniformly sampled PCBM$(148, 149, 113, 37, 12, 414)$ public key is an injective function is approximately $1 - 2^{-200}$; thus, since decryption failure can only occur when a ciphertext has multiple preimages, PCBM may be used to target CCA security.

For an example of a computationally injective family of functions, consider the collection of public keys with parameters $(q, n, m) = (3, 140, 226)$ of the HFERP encryption scheme, see [28, Section 7]. There the bound for computational injectivity (and therefore a bound on the probability that a randomly generated ciphertext has multiple preimages) is about 2^{-136}, though the probability that a given public key is an injective function is quite low. Due to Theorem 1, we have that injectivity as well as computational and statistical injectivity are preserved by the 2F construction.

Corollary 1. *Let p and q be primes, let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a homogeneous quadratic map and let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an invertible $\mathbb{F}_q$-linear transformation. If*

$$q > \frac{(p-1)^3}{4}\binom{n+1}{2},$$

then $P = T \circ \iota(F)$ is injective if and only if F is injective. Under the same condition, P is computationally (or statistically) injective if and only if F is computationally (or statistically) injective.

We note here that it may be desirable for efficiency to choose a smaller value of q than the one mentioned above. There are two clear motivations for such a choice.

First, the output distributions for fixed quadratic forms are typically far narrower than the theoretical limit given by the bound above. Thus it is possible to pick a far smaller q that still has a very low, or even zero, decryption failure rate.

Second, it is not necessary to have the plaintext space be all of $\mathbb{F}_p^n$. For example, we could insist that valid plaintexts lie in $\{-1, 0, 1\}^n$, in which case we can use a much larger p and still utilize a smaller q for which the natural analogue of Theorem 1 still holds. In this latter case, the output distribution of a fixed quadratic form is even narrower, so there is room for further optimization of q if we allow a small decryption failure rate from the 2F construction.

4 An Instance of 2F Multivariate Encryption

As an exercise, we construct and demonstrate 2FSQUARE, the 2F version of the SQUARE encryption scheme, see [18], without projection. Since SQUARE can be broken by numerous methods, see [8, 9, 33], this choice offers the best chance for future cryptanalysis and advancement in this line of research.

Let p be an odd prime and fix a positive integer n. Let q be a prime larger than $\frac{(p-1)^3}{4}\binom{n+1}{2}$. Let $\mathbb{K}$ be a degree n extension of $\mathbb{F}_p$ and let $\phi : \mathbb{F}_p^n \to \mathbb{K}$ be an $\mathbb{F}_p$-vector space isomorphism. Select an invertible linear transformation $U : \mathbb{F}_p^n \to \mathbb{F}_p^n$ and define $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ by

$$F(\mathbf{x}) = \phi^{-1}(\phi(U(\mathbf{x}))^2).$$

Select another invertible linear transformation $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and define

$$P(\mathbf{x}) = T \circ \iota(F)(\mathbf{x}),$$

where ι be the map that casts a function on $\mathbb{F}_p^n$ as a function on $\mathbb{F}_q^n$ with the same coefficients considered as least absolute residues lying in $\mathbb{F}_q$. See Figure 2 for a visual description of P.

Encryption is accomplished by evaluating the public key P at the plaintext $\mathbf{x}$. Decryption is accomplished by inverting T, reducing the result modulo p and inverting F. For the latter step, some redundancy must be built into the domain of F to produce unique preimages as was already the case for SQUARE.

5 Security Analysis

The 2F construction adds a nonlinear modification to a multivariate cryptosystem, so we expect it to change the algebraic properties such as rank that we normally use to cryptanalyze multivariate cryptosystems. We verify the security of 2FSQUARE against the typical attacks we use on multivariate schemes in this section. In addition to analyzing what structure is taken away by the 2F construction, we analyze the structure added by 2F at the end of the section.

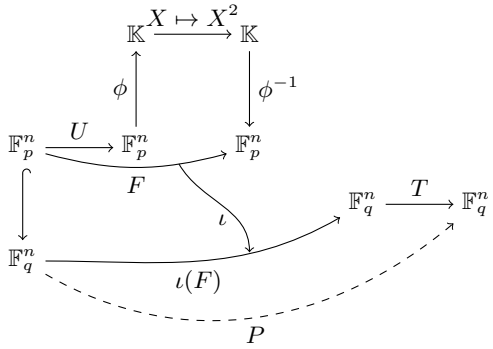

Fig. 2. The 2FSQUARE scheme. Given the $\mathbb{F}_p$-vector space isomorphism ϕ, $\mathbb{F}_p$-linear map U, $\mathbb{F}_q$-linear map T and the modulus switching map ι, we construct the vector-valued function $P : \mathbb{F}_p^n \to \mathbb{F}_q^n$. The inclusion of $\mathbb{F}_p^n$ into $\mathbb{F}_q^n$ is understood to coordinate-wise map the least absolute residue $a \in \mathbb{F}_p$ to least absolute residue $a \in \mathbb{F}_q$.

5.1 MinRank Attacks

The SQUARE cryptosystem is vulnerable to two different types of rank attacks. The historically first such attack originated in the work of Kipnis and Shamir, see [16], and was improved in [9].

Note that we may represent elements of $\mathbb{K}$ as n-dimensional vectors over $\mathbb{F}_p$. Then the $\mathbb{F}_p$-vector space isomorphism ϕ can be expressed as a matrix over $\mathbb{F}_p$. In particular, if θ is a primitive element for $\mathbb{K}$ over $\mathbb{F}_p$, then we can represent ϕ via right multiplication by the matrix

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta & \theta^p & \cdots & \theta^{p^{n-1}} \\ \theta^2 & \theta^{2p} & \cdots & \theta^{2p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \theta^{(n-1)} & \theta^{(n-1)p} & \cdots & \theta^{(n-1)p^{n-1}} \end{bmatrix},$$

given that the vector representations of elements in $\mathbb{K}$ is relative to the same basis, $\{1, \theta, \theta^2, \ldots, \theta^{(n-1)}\}$.

Letting $G(X) = X^2$, and setting $\mathbf{G}^{*i}$ to be the matrix representation of the ith Frobenius power of G, we have that

$$G(X)^{p^i} = \begin{bmatrix} X & X^p & \cdots & X^{p^{(n-1)}} \end{bmatrix} \mathbf{G}^{*i} \begin{bmatrix} X \\ X^p \\ \vdots \\ X^{p^{(n-1)}} \end{bmatrix}.$$

The matrix $\mathbf{G}^{*i}$ has only one nonzero value, a 1 in the ith row and column.

Let $\mathbf{U}$ be the matrix representation of U and set $\mathbf{S} = \mathbf{UM}$. We may then note that if $\mathbf{H}_i$ is the ith quadratic form in $H = \phi^{-1} \circ G \circ \phi \circ U$, we have

$$\left[\mathbf{H}_0 \, \mathbf{H}_1 \, \cdots \, \mathbf{H}_{n-1}\right] (\mathbf{M} \otimes \mathbf{I}_n) = \left[\mathbf{S}\mathbf{G}^{*0}\mathbf{S}^\top \, \cdots \, \mathbf{S}\mathbf{G}^{*(n-1)}\mathbf{S}^\top\right]. \tag{1}$$

Since $\mathbf{G}^{*0}$, for example, has rank 1, there is thus a $\mathbb{K}$-linear combination of the matrices $\mathbf{H}_i$ of rank 1.

Notice that the public key of 2FSQUARE is given in matrix form by

$$\left[\mathbf{P}_0 \, \mathbf{P}_1 \, \cdots \, \mathbf{P}_{n-1}\right] = \left[\widetilde{\mathbf{H}}_0 \, \widetilde{\mathbf{H}}_1 \, \cdots \, \widetilde{\mathbf{H}}_{n-1}\right] (\mathbf{T} \otimes \mathbf{I}_n), \tag{2}$$

where $\mathbf{T}$ is the matrix representation of T and $\mathbf{P}_i$ are the matrix representations of the public quadratic forms. Critically, T is $\mathbb{F}_q$-linear, and so not $\mathbb{F}_p$-linear. Thus there is a $\mathbb{K}$-linear combination of $\mathbb{F}_q$-linear combinations of the $\mathbf{P}_i$ that has low rank as a $\mathbb{K}$-valued matrix. This combination does not correspond to a linear combination over any ring, and so the rank property is broken. We verified experimentally for small instances that the smallest rank in the span of the public matrices is high over $\mathbb{F}_p$, $\mathbb{F}_q$ and $\mathbb{K}$.

The second kind of rank attack affecting SQUARE is that of [7]. This rank attack is also based on Equation (1). The attack works by finding a row of $\mathbf{S}^{-1}$ and reconstructing $\mathbf{S}$ by Frobenius relations. Specifically, if $\mathbf{s} = \left[s_0 \; s_1 \; \ldots \; s_{n-1}\right]$ is the first row of $\mathbf{S}^{-1}$, then the matrix $\mathbf{Z}$ whose ith row is given by $\mathbf{s}\mathbf{H}_i$ has rank 1. This rank condition induces a system of equations on the unknown coefficients of $\mathbf{s}$ which can be solved at low degree, in fact, at degree 2 in this case.

Again, the $\mathbb{F}_q$-linear map T present in Equation (2) halts the attack. Since the relationship between the public matrices $\mathbf{P}_i$ and $\mathbf{G}^{*i}$ is not linear with respect to any ring, the rank condition present in the $\mathbf{H}_i$ is not echoed by the public matrices. Once again, we have verified this property experimentally.

5.2 Differential

Another class of attack against which SQUARE is vulnerable is the attack based on differential symmetry. This attack is the one that first broke SQUARE, see [19].

Recall that the discrete differential of any function $F(x)$ is merely the associated bilinear function $DF(a, x) = F(a + x) - F(a) - F(x) + F(0)$. We may examine the differential over the small field where the function of interest is vector-valued, or over the large field in which our function is the monomial map $G(X) = X^2$. In the latter case, the differential is $DG(A, X) = 2AX$.

Given any element β of the extension field $\mathbb{K}$, we see that the differential satisfies a symmetric multiplicative symmetry

$$DG(\beta A, X) + DG(A, \beta X) = 2\beta DG(A, X).$$

Passing this relation to the small field and incorporating U we obtain the linear differential symmetry

$$DH(\mathbf{M}_\beta \mathbf{Ua}, \mathbf{Ux}) + DH(\mathbf{Ua}, \mathbf{M}_\beta \mathbf{Ux}) = 2\mathbf{M}_\beta DH(\mathbf{Ua}, \mathbf{Ux}),$$

where $H = \phi^{-1} \circ G \circ \phi$.

For the original SQUARE cryptosystem the linear transformation T was $\mathbb{F}_p$-linear, and then there is an easy way to translate the above relation into a relation on the public key. This relation can then be used to complete an attack on SQUARE by the same technique as [33]. Due to the fact that T is not $\mathbb{F}_p$-linear, however, the symmetric application of an $\mathbb{F}_p$-linear map corresponding to multiplication by an element of $\mathbb{K}$ in the correct basis is not equivalent to the composition of a linear map with the public differential over any ring. Thus, 2FSQUARE is immune from differential attack as well.

5.3 Direct

In [34], the authors present evidence that the analysis of EFLASH, see [29], against direct message recovery attacks is incomplete. Specifically, they show that low Q-rank relations in the extension field correspond to low degree syzygies in the direct attack. This observation offers another method of cryptanalysis against SQUARE as an instance of EFLASH with special parameters.

Note, however, that the observation of [34] relies on relations induced by the Frobenius automorphisms of $\mathbb{K}$ "passing through" the output transformation in the sense that there exists an $\mathbb{F}_p$ linear map L such that L composed with T is equal to T composed with the Frobenius automorphism. As before, since T is not $\mathbb{F}_p$-linear in 2FSQUARE, this property fails to hold, thus, 2FSQUARE does not have the anomalous low degree syzygies observed in [34]. We have experimentally verified for small instances that the first fall degree matches the semi-regular degree.

The best method for effecting a direct attack on a balanced multivariate system is called the hybrid approach. First the attacker guesses the values of k variables. Then some polynomial system solver is used to solve the resulting system.

The type of polynomial system solver that is optimal depends on many parameters including the density of the equations, the number of variables and the solving degree. Typically denser systems for which the solving degree is lower benefit from Gröbner basis solvers powered by F4, see [35]. Systems with a larger number of variables or less dense systems or that require a higher operating degree do not benefit as greatly from the normalization step in F4 and can therefore benefit from the lower memory costs, see [8], of the XL algorithm [36]. For parameters of cryptographic interest, we expect that XL variants will be the most effective.

Notice that the system must be solved over $\mathbb{F}_q$, and so we are not able to add the normal field equations. Still, we may add equations of the form

$$g_i(x_i) = \prod_{j=\frac{1-p}{2}}^{\frac{p-1}{2}} (x_i - j),$$

which perform the same role as $\mathbb{F}_p$ field equations when solving over $\mathbb{F}_q$.

Thus, under the standard semi-regular assumption, the complexity of the hybrid direct attack with k guesses will then be

$$\text{Complexity}_{\text{direct}} = 3p^k \binom{n+1}{2} \binom{n+d}{d}^2 \tag{3}$$

$\mathbb{F}_q$ operations, where d is the smallest degree with a nonpositive coefficient in the series expansion of

$$\mathcal{H}(t) = \frac{(1-t^2)^n (1-t^p)^{n-k}}{(1-t)^{n-k}}.$$

Note that each such field operation will cost $2(\log_2 q^2 + \log_2 q)$ bit operations.

5.4 Lattice Attacks

While it seems that all of the standard multivariate attacks are made less efficient by the 2F construction, some structure is added to the public key. Notice that there exist $\mathbb{F}_q$-linear combinations of the public key that are polynomials with small coefficients, bounded in size by $\frac{p-1}{2}$. This observation is the basis for an attack based on lattices.

Notice that, analogous to the NTRU lattice, we may construct the lattice given by the rowspace of

$$\begin{bmatrix} \frac{p}{q}\mathbf{I}_n & \mathbf{P} \\ \mathbf{0} & q\mathbf{I}_{\binom{n+1}{2}} \end{bmatrix},$$

where $\mathbf{P}$ is the matrix whose ith row is the ordered list of monomial coefficients of the ith public equation P_i. Notice that there exists a vector $\mathbf{w}$ with entries in $\mathbb{F}_q$ such that $\mathbf{t}_i \| \mathbf{w}$ multiplied by the above matrix is $\frac{p}{q}\mathbf{t}_i$ concatenated with the list of monomial coefficients of $H_i \circ U$, where $\mathbf{t}_i$ is the ith row of T^{-1}. Thus, we expect that the shortest vector in this dimension $d = \binom{n+1}{2} + n$ lattice to be among these vectors.

All coordinates of this short vector lie in the interval $(-p/2, p/2)$ with at least $\binom{n+1}{2}$ of them taking integral values, and so the expected length is well-approximated by $s = \sqrt{(p^2-1)d/12}$. In contrast the expected length of the shortest vector in a random lattice of dimension d and volume $V = p^n q^{d-2n}$ is approximately $np^{n/d}q^{1-2n/d}/2\sqrt{\pi e}$.

We may follow the core-SVP methodology of [37] to estimate the complexity of solving this SVP instance conservatively ignoring some polynomial overhead. Following the geometric series assumption, we suppose that the length of the ith Gram-Schmidt basis vector is given by $\|\mathbf{b}_i^*\| = \delta^{d-2i-1}V^{1/d}$, where $\delta = ((\pi b)^{1/b} b/2\pi e)^{1/2(b-1)}$. The BKZ block size is then the smallest b for which the projected length $s\sqrt{b/d}$ is bounded by $\|\mathbf{b}_{d-b}^*\|$. The classical core-SVP hardness of this problem instance is then computed as

$$\text{Complexity}_{\text{core-SVP}} = 2^{0.292b}. \tag{4}$$

Of course, we may change the disparity in the length of the shortest vector in the above lattice and the value suggested by the Gaussian heuristic by bringing the values of p and q closer, either by introducing a nonzero decryption failure rate, by restricting the plaintext space or both, as discussed in Section 3. Thus, the 2F construction has the strength to address any vulnerability arising from some future lattice attack by adjusting these parameters in such a way as to make the vectors associated with the secret key not be among the shortest vectors in the lattice. The optimization of these strategies as well as other lattice attacks is an interesting direction to further study.

6 Parameters and Performance

As discussed in Section 5, the best known attacks on 2FSQUARE are the direct attack and the lattice attack. We find that for $p = 3$ the disparity in the length between the shortest vector in the lattice of Subsection 5.4 and the Gaussian heuristic is sufficiently small and the dimension sufficiently large that the limiting attack is the direct attack. In contrast, for $p = 7$ the shortest vector is much smaller than would be implied by the Gaussian heuristic and the lattice attack then offers an advantage. Thus, we may select parameters based on the formula (3) for $p = 3$ and based on formula (4) for $p = 7$. To be careful, we assume that one bit of information is leaked in the form of the parity of some coordinate of the plaintext. We do this because the central map of SQUARE is a two-to-one function and 1-bit of redundant information is necessary to specify a unique preimage. For 128-bit security, we may select $p = 3$, $q = 6653$ and $n = 81$ or $p = 7$, $q = 344,749$ and $n = 54$. Targeting NIST level I security, see [38], we may select $p = 3$, $q = 8377$ and $n = 91$ or $p = 7$, $q = 449,287$ and $n = 64$. We summarize the complexity of attacks at these security levels in Table 1.

Table 1. Complexity of known attacks at the 128-bit and 143-bit (corresponding to NIST level I) security levels.

Scheme	Sec.	k	Direct	b	core-SVP
2FSQUARE$(3, 6653, 81)$	128	43	128	463	135
2FSQUARE$(3, 8377, 91)$	143	46	143	700	204
2FSQUARE$(7, 130411, 69)$	128	18	169	360	105
2FSQUARE$(7, 145861, 73)$	143	20	176	412	120

We made a proof-of-concept implementation on the Magma Computer Algebra System,[1] see [39], to make a comparison to other secure multivariate encryption schemes, see [21, 27]. We find that our simple implementation is dramatically faster at the same security level, even when compared with optimized code. Still,

[1] Any mention of commercial products does not indicate endorsement by NIST.

Magma's implementation of the `Sqrt` command for finite fields is extremely efficient, so we suspect that an optimized implementation will not significantly outperform this one. The results of these experiments are recorded in Table 2.

Table 2. Public key, message and ciphertext sizes, decryption failure rate and encryption and decryption performance of multivariate encryption schemes at the best available comparison to the 128-bit security level.

Scheme	Sec.	PK	pt	ct	Enc.(ms)	Dec.(ms)	DFR
ABC(2^8,384,760)	128	54863KB	384B	760B	502	545	2^{-32}
PCBM(149,414)	128	743KB	149b	414b	13	743	2^{-350}
2FSQ$(3, 6653, 81)$	128	417KB	162b	129B	1.5	0.4	0
2FSQ$(3, 8377, 91)$	143	606KB	182b	148B	1.2	0.5	0
2FSQ$(7, 130411, 69)$	128	346KB	207b	147B	1.0	2.6	0
2FSQ$(7, 145861, 73)$	143	413KB	219b	157B	1.1	2.8	0

7 Conclusion

In the aftermath of several significant advances in cryptanalysis, there are several new directions to explore to find secure post-quantum schemes. These new schemes have motivations coming from avoiding rank attacks as well as importing ideas from other areas in cryptography.

In the area of multivariate digital signatures the new Mayo scheme of [40] introduces a method of creating oil-vinegar style maps, see [41], that can have more balance between the number of variables and number of equations. The Q modifier of [42] introduces a new method inspired by the relinearization algorithm of [16] to construct structured instances of UOV that have a more efficient inversion. While the recent result [43] shows that the latter scheme has limits on how long the keys can be used statically, both schemes appear to be secure for now.

The PCBM multivariate encryption scheme, inspired by linear codes, see [27], establishes a new way of parameterizing a multivariate encryption scheme similar to HFERP, see [28], but far more efficient. Now the 2F construction provides a new way, inspired by the modulus switching of NTRU, to build secure and very efficient multivariate encryption schemes.

While the above digital signature schemes take inspiration from established knowledge in multivariate cryptography, the encryption schemes mentioned are derived from examining code-based and lattice-based ideas. In all cases, however, there is a motivation to build a more efficient scheme that does not have exploitable rank properties.

In particular, both the Q-modifier and the 2F construction are generic and attempt to nonlinearly modify a given multivariate primitive. This genericity

means that there is a multitude of possible schemes that may be derived from these constructions that may have disparate security properties. This fact suggests that there may be an enticing direction in which this work can progress aside from advancing new targets for cryptanalysis; namely, we may work in the attempt to build new multivariate schemes based on the 2F construction with other profitable modifications.

References

1. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. CoRR **abs/1301.1026** (2013)
2. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A.: Improvements of algebraic attacks for solving the rank decoding and minrank problems. In Moriai, S., Wang, H., eds.: Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I. Volume 12491 of Lecture Notes in Computer Science., Springer (2020) 507–536
3. Melchor, C.A., Aragon, N., Bardet, M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.C., Gaborit, P., Hauteville, A., Otmani, A., Ruatta, O., Tillich, J.P., Zémor, G.: ROLLO - Rank-Ouroboros, Lake & LOcker. Submission to the NIST's post-quantum cryptography standardization process (2019)
4. Beullens, W.: Improved cryptanalysis of UOV and rainbow. In Canteaut, A., Standaert, F., eds.: Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I. Volume 12696 of Lecture Notes in Computer Science., Springer (2021) 348–373
5. Beullens, W.: Breaking rainbow takes a weekend on a laptop. IACR Cryptol. ePrint Arch. (2022) 214
6. Casanova, A., Faugere, J.C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: G*e*MSS - A Gr*e*at Multivariate Short Signature. Submission to the NIST's post-quantum cryptography standardization process (2020)
7. Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all HFE signature variants. In Malkin, T., Peikert, C., eds.: Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Volume 12825 of Lecture Notes in Computer Science., Springer (2021) 70–93
8. Baena, J., Briaud, P., Cabarcas, D., Perlner, R.A., Smith-Tone, D., Verbel, J.A.: Improving support-minors rank attacks: applications to gemss and rainbow. IACR Cryptol. ePrint Arch. (2021) 1677
9. 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
10. Vates, J., Smith-Tone, D.: Key recovery attack for all parameters of HFE-. In 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) 272–288
11. Apon, D., Moody, D., Perlner, R.A., Smith-Tone, D., Verbel, J.A.: Combinatorial rank attacks against the rectangular simple matrix encryption scheme. In Ding, J., Tillich, J., eds.: Post-Quantum Cryptography - 11th International Conference,

PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings. Volume 12100 of Lecture Notes in Computer Science., Springer (2020) 307–322
12. Ding, J., Perlner, R.A., Petzoldt, A., Smith-Tone, D.: Improved cryptanalysis of hfev- via projection. In Lange, T., Steinwandt, R., eds.: Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. Volume 10786 of Lecture Notes in Computer Science., Springer (2018) 375–395
13. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: EUROCRYPT. (1996) 33–48
14. Matsumoto, T., Imai, H.: Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption. In: EUROCRYPT. (1988) 419–453
15. Berlekamp, E.R.: Factoring polynomials over large finite fields. Mathematics of Computation **24** (1970) pp. 713–735
16. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. Advances in Cryptology - CRYPTO 1999, Springer **1666** (1999) 788
17. Verbel, J.A., Baena, J., Cabarcas, D., Perlner, R.A., Smith-Tone, D.: On the complexity of "superdetermined" minrank instances. In Ding, J., Steinwandt, R., eds.: Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers. Volume 11505 of Lecture Notes in Computer Science., Springer (2019) 167–186
18. 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
19. Billet, O., Macario-Rat, G.: Cryptanalysis of the square cryptosystems. In Matsui, M., ed.: Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. Volume 5912 of Lecture Notes in Computer Science., Springer (2009) 451–468
20. 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
21. 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
22. Tao, C., Xiang, H., Petzoldt, A., Ding, J.: Simple matrix - A multivariate public key cryptosystem (MPKC) for encryption. Finite Fields Their Appl. **35** (2015) 352–368
23. Ding, J., Petzoldt, A., Wang, L.: The cubic simple matrix encryption scheme. In 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) 76–87
24. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In 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) 180–196

25. 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)
26. Moody, D., Perlner, R.A., Smith-Tone, D.: Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme. In 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) 255–271
27. Smith-Tone, D., Tone, C.: A multivariate cryptosystem inspired by random linear codes. Finite Fields Their Appl. **69** (2021) 101778
28. Ikematsu, Y., Perlner, R.A., Smith-Tone, D., Takagi, T., Vates, J.: HFERP - A new multivariate encryption scheme. In Lange, T., Steinwandt, R., eds.: Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings. Volume 10786 of Lecture Notes in Computer Science., Springer (2018) 396–416
29. Cartor, R., Smith-Tone, D.: EFLASH: A new multivariate encryption scheme. In Cid, C., Jr., M.J.J., eds.: Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers. Volume 11349 of Lecture Notes in Computer Science., Springer (2018) 281–299
30. Ding, J., Dubois, V., Yang, B.Y., Chen, C.H.O., Cheng, C.M.: Could SFLASH be Repaired? In Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I., eds.: ICALP (2). Volume 5126 of Lecture Notes in Computer Science., Springer (2008) 691–701
31. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In Buhler, J.P., ed.: Algorithmic Number Theory, Berlin, Heidelberg, Springer Berlin Heidelberg (1998) 267–288
32. Chen, C., Danba, O., Hoffstein, J., H ulsing, A., Rijneneld, J., Schanck, J.M., Saito, T., Schwabe, P., Whyte, W., Xagawa, K., Yamakawa, T., Zhang, Z.: NTRU. Submission to the NIST's post-quantum cryptography standardization process (2020)
33. Smith-Tone, D.: Practical cryptanalysis of k-ary c^*. In Ding, J., Tillich, J., eds.: Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings. Volume 12100 of Lecture Notes in Computer Science., Springer (2020) 360–380
34. Øygarden, M., Felke, P., Raddum, H., Cid, C.: Cryptanalysis of the multivariate encryption scheme EFLASH. In Jarecki, S., ed.: Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24-28, 2020, Proceedings. Volume 12006 of Lecture Notes in Computer Science., Springer (2020) 85–105
35. Faugere, J.C.: A new efficient algorithm for computing grobner bases (f4). Journal of Pure and Applied Algebra **139** (1999) 61–88
36. Courtois, N., Klimov, A., Patarin, J., A.Shamir: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. EUROCRYPT 2000, LNCS **1807** (2000) 392–407
37. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - A new hope. In Holz, T., Savage, S., eds.: 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016, USENIX Association (2016) 327–343

38. 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.
39. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system i: The user language. J. Symb. Comput. **24** (1997) 235–265
40. Beullens, W.: MAYO: practical post-quantum signatures from oil-and-vinegar maps. In AlTawy, R., Hülsing, A., eds.: Selected Areas in Cryptography - 28th International Conference, SAC 2021, Virtual Event, September 29 - October 1, 2021, Revised Selected Papers. Volume 13203 of Lecture Notes in Computer Science., Springer (2021) 355–376
41. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. EUROCRYPT 1999. LNCS **1592** (1999) 206–222
42. Smith-Tone, D.: New practical multivariate signatures from a nonlinear modifier. In Cheon, J.H., Tillich, J., eds.: Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings. Volume 12841 of Lecture Notes in Computer Science., Springer (2021) 79–97
43. Hashimoto, Y.: On the modifier Q for multivariate signature schemes. IACR Cryptol. ePrint Arch. (2021) 1046