EFLASH: A New Multivariate Encryption Scheme

Ryann Cartor[1] and Daniel Smith-Tone[1,2]

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

ryann.cartor@louisville.edu, daniel.smith@nist.gov

Abstract. Multivariate Public Key Cryptography is a leading option for security in a post quantum society. In this paper we propose a new encryption scheme, EFLASH, and analyze its efficiency and security.

Key words: Multivariate Cryptography, HFE, PFLASH, Discrete Differential, MinRank

1 Introduction

In the 1990's, Peter Shor developed a polynomial time algorithm to factor and compute discrete logarithms using a quantum computer. This discovery has changed the focus of the future of cryptography. With large scale quantum computing increasingly being viewed as an inevitability, as opposed to a mere possibility, research in the field of post-quantum cryptography is more important than ever. In response to this need, the National Institute of Standards and Technology (NIST) is actively searching for ways to refine security standards to keep critical data confidential in a world with large scale quantum computing.

The NIST call for proposals for post-quantum standards, see [1], highlights the attributes required of any solution to the post-quantum predicament. A plethora of possible post-quantum cryptosystems have been proposed at this time, including (but not limited to) lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, and hash-based signatures. Each of these areas rely on mathematical problems for which there is no obvious quantum advantage. In this article, we focus on the application of multivariate cryptography to secure encryption.

1.1 Recent History of Multivariate Encryption

Multivariate encryption has had a complicated history, with an increase in activity in the recent past. These schemes are composed of systems of multivariate quadratic polynomials over a finite field $\mathbb{F}$. The security of these schemes is based on the MQ-problem, the problem of solving systems of quadratic equations over a field, which is known to be NP-hard. Thus, we can be assured the problem is difficult even for quantum computers.

Recently we have seen new candidates and strategies emerge for multivariate encryption. Previously, multivariate schemes centered around bijective functions that map from vector spaces of size n back into a vector space of size n. The problem with this strategy is that there are not many bijective quadratic maps. Furthermore, of the maps that do exist, many of these functions were either too hard to invert, or too easy to invert. The common practice to try to overcome this downfall was to try to hide an easily invertible function by composing the bijective function with affine maps.

In 2013, Tao et al. proposed relaxing the *bijective* condition for the central function and replacing it with an *injective* map with a much larger codomain in [2]. In theory, this would make hiding the structure of the map while maintaining efficient inversion easier to accomplish. The recent resurgence of multivariate encryption is due primarily to this change in philosophy. Many schemes have been proposed along these apparently promising lines.

Some notable schemes that increase the codomain size of the central mappings include the ABC Simple Matrix scheme, see [2], which utilizes a large matrix algebra structure; ZHFE, see [3],which is similar to a high degree version of HFE with a single variable over the extension; and SRP, see [4], which combines the Square encryption scheme, Rainbow signature scheme, and Plus method. Although these schemes appear promising, many of these schemes have subsequently been the victims of surprising (if not disabling) cryptanalysis. The attacks on ABC from [5–7] work well if the base field is small, and both ZHFE and SRP were broken in [8] and [9], respectively.

1.2 Our Contribution

We propose a new encryption system, EFLASH, based on a primitive with strong security results. The scheme is a projected C^{*-} scheme with a parameterization effective for encryption. This scheme also follows the philosophy of increasing the size of the codomain to avoid ciphertext collision. We accomplish this increase in codomain size by replacing the traditional projection with an embedding into a larger space. Interestingly, we are able to essentially eliminate decryption failures with a much smaller blow-up factor than most recent proposals for multivariate encryption.

This construction introduces challenges that a projected C^{*-} signature scheme does not have to address. Since valid decryption requires a unique preimage, it is a requirement that there is a single assignment of the missing coordinates of the output of the central map corresponding to a valid input. Thus, for constant time implementations, every such assignment of coordinates must be computed. We introduce a new method of decryption satisfying these constraints in realistic amounts of time.

1.3 Organization of Paper

The paper is organized as follows. The section following the introduction introduces the idea of big field schemes and describes relevant big field schemes, namely C^*, PFLASH and HFE. Then the subsequent section outlines the cryptanalytic techniques that have had the most success attacking big field schemes. After that, we introduce the algebraic structure of our scheme in Section 4 where we discuss the algebraic aspects of EFLASH and methods for encryption and decryption. Finally, we discuss the resistance to relevant attacks and parameter selection for EFLASH.

2 Big Field Schemes

EFLASH belongs to a family of multivariate cryptosystems known as "big field" schemes. These schemes rely on the multiplicative structure of a degree d extension $\mathbb{F}_{q^d}$ of the finite field $\mathbb{F}_q$. Let $\phi : \mathbb{F}_q^d \to \mathbb{F}_{q^d}$ be a vector space isomorphism (we will also denote $\mathbb{F}_{d^d}$ as $\mathbb{K}$). Notice that univariate monomials of the form $X^{q^i+q^j}$ in $\mathbb{F}_{q^d}[X]$ are the product of two Frobenius automorphisms over $\mathbb{F}_q$, and hence are the product of two $\mathbb{F}_q$-linear functions. Thus $\phi \circ X^{q^i+q^j} \circ \phi^{-1}$ (expressed here and throughout the paper with left-to-right function composition) is coordinate-wise quadratic when expressed over $\mathbb{F}_q$. Thus functions of the form

$$\sum_{0 \le i,j < d} \alpha_{ij} X^{q^i+q^j}$$

are said to be $\mathbb{F}_q$-quadratic.

To disguise the structure of the central map of such schemes one applies an morphism of polynomials, essentially choosing random linear maps mixing the input and output spaces of the central map. Formally, we define these morphisms as follows.

Definition 1 *A* polynomial morphism *is a map between two systems of polynomials, $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ and $G : \mathbb{F}_q^r \to \mathbb{F}_q^s$ defined by a pair of affine maps $T : \mathbb{F}_q^m \to \mathbb{F}_q^s$ and $U : \mathbb{F}_q^r \to \mathbb{F}_q^n$ such that $G = U \circ F \circ T$. If both T and U are invertible, then the morphism is said to be an isomorphism and F and G are said to be isomorphic.*

The following diagram illustrates the entire construction utilizing the big field.

$$\begin{tikzcd}
& \mathbb{K} \arrow[r, "f"] & \mathbb{K} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^n \arrow[r, "U"] \arrow[rrr, bend right, "P"'] & \mathbb{F}_q^d \arrow[u, "\phi"] \arrow[r, "F"] & \mathbb{F}_q^d \arrow[r, "T"] & \mathbb{F}_q^m
\end{tikzcd}$$

2.1 C^*

Matsumoto and Imai introduced the C^* scheme at Eurocrypt '88, effectively introducing the world to massively multivariate cryptography. The scheme uses a big field construction where the quadratic monomial map $f : \mathbb{K} \rightarrow \mathbb{K}$ is defined by $(x)f = x^{q^\theta+1}$ and is hidden by a polynomial isomorphism. The public key for the scheme is given by $P = U \circ \phi \circ f \circ \phi^{-1} \circ T$.

Encryption of a plaintext is accomplished by evaluating the public polynomials P at an encoding of the plaintext x, and is thus very efficient. Decryption is accomplished by inverting each of the three component maps individually. The inversion of $v = (u)f$ is performed by solving $h(q^\theta + 1) = 1(\mod q^n - 1)$, and calculating $u = v^h$. This process can be cumbersome, depending on the degree of extension and the exponent θ.

2.2 PFLASH

Following the break of C^*, efforts to modify the scheme to add security lead to the discovery of PFLASH. The PFLASH scheme is a specific parametrization of a projected C^{*-} scheme. Both the projection and minus modifiers were initially proposed in in relation to C^* in [10]. The purpose of the projection modifier is to change the simplicity of the central map by fixing the value of d input variables. The composition of the projection and an affine map U create a projection onto a codimension d hyperplane. The minus modifier eliminates r equations from the public key. Note the composition of the minus projection with the affine map T has corank r. The public key of PFLASH(q, n, r, d) is given by $(\overline{x})P = (\overline{x})\pi_d \circ U \circ \phi \circ f \circ \phi^{-1} \circ T \circ \pi_r$

The scheme works as a digital signature primitive. To verify a signature, an individual evaluates the public polynomials at the given signature. To create a signature, the signer finds a preimage of each of the private maps. In order to find a preimage of $\phi^{-1} \circ T \circ \pi_r$, randomly append r values to the message, then apply T^{-1} and ϕ. After inverting f, an element that is in the preimage of $U \circ \phi$ and in the image of π_d is selected as the signature.

PFLASH has strong security arguments, including a proof of security against differential attacks that can be found in [11]. Due to the modifications of the scheme, the public key is not isomorphic to the private monomial function, but rather only a polynomial morphism exists between the central map and the public key. As shown in [12], the morphism of polynomials problem is NP-hard, which gives hope that the information lost to the public key may secure the scheme.

2.3 HFE

Another decendent of the C^* scheme is the Hidden Field Equation (HFE) scheme of [13]. HFE replaces the monomial map of the C^* scheme with a more general polynomial with a degree bound D.

Given $\mathbb{K}$, the degree n extension of $\mathbb{F}$, a quadratic polynomial $f : \mathbb{K} \to \mathbb{K}$ with degree bound D is chosen. The function f has the following form:

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

where $\alpha_{i,j}, \beta_i, \gamma \in \mathbb{K}$. The public key is then constructed via the isomorphism:

$$P = U \circ \phi \circ f \circ \phi^{-1} \circ T.$$

Inversion for this scheme is achieved by taking a ciphertext $\overline{y} = (\overline{x})P$ and computing $v = (\overline{y})T^{-1} \circ \phi$. The next step is to solve $v = (u)f$ for u via the Berlekamp algorithm, see [14], and finally recovering $\overline{x} = (u)\phi^{-1} \circ U^{-1}$.

3 Cryptanalyses of Big Field Schemes

There are three main cryptanalytic techniques that are applicable to big field multivariate cryptosystems. In a sense, all of these techniques are related to Q-rank. The MinRank key recovery attack has a complexity directly dependent on the Q-rank of the central map. The differential symmetry attack is relevant when the Q-rank of the central map is minimal in the relevant algebra. The direct algebraic attack has a complexity dependent on the degree of regularity of the public key which is usually a linear function of the Q-rank. We review each of these techniques.

3.1 MinRank

The first effective attack on HFE was presented in [15] and is now commonly called the Kipnis-Shamir (KS) attack. Their idea is to express the central polynomial as a single quadratic form on an a large representation of the extension field. Specifically, choose a representation $\psi : \mathbb{K} \to \mathbb{A}$ of the form $\psi(X) = (X, X^q, \ldots, X^d)$. Then one can choose a matrix representation $\mathbf{F}$ of the central map f such that

$$(X)f = \left[X \; X^q \; \cdots \; X^{q^{d-1}}\right] \mathbf{F} \left[X \; X^q \; \cdots \; X^{q^{d-1}}\right]^\top .$$

As the reader easily notices, the degree bound on f implies that $\mathbf{F}$ has only a small block of nonzero values and thus has low rank. We call the rank of this quadratic form the Q-rank of f.

The attack in [15] exploits this low Q-rank property by using interpolation to find a formula for the public key over the extension field, computing the matrix forms of all of the Frobenius powers of this map, and then finding a low rank linear combination of these matrices with coefficients chosen from $\mathbb{K}$. The attack can be effective, but all of the algebra takes place in $\mathbb{K}$ which can be cumbersome.

The KS attack was significantly improved for determined or slightly overdetermined schemes in [16], where the authors intoduce minors modeling. Whereas the modeling of the low rank property in the KS attack requires structures defined over $\mathbb{K}$, the authors of [16] noticed that a $\mathbb{K}$-linear combination of the *public* quadratic forms defined over $\mathbb{F}_q$ has low rank. Thus one may construct a system of equations over the small field, resolve this system via Gröbner bases over the small field, and finally recover the variety over the big field. Requiring the most intensive calculations to be performed over the base field provided a significant advantage.

PFLASH is algebraically equivalent to an HFE- scheme (with a more efficient inversion process), and though the MinRank problem is less over-defined, the technique can, in principle, still be applied. To see this equivalence, note that the removal of equations can be modeled as a projection whose minimal polynomial, see [17, Definition 1], has low degree. Thus, there is a basis in which one can compose a low degree linear map with the low Q-rank central map of PFLASH producing a low Q-rank composition. As shown in [18, 11], the Q-rank of the PFLASH public key is too large for this attack to be effective.

3.2 Differential Techniques

A second class of attacks that has proven effective against big field schemes is the family of differential attacks involving the recovery of a symmetric relation to remove the minus modifier, or as a tool for accessing a low Q-rank. The discrete differential of a function $f : \mathbb{K} \to \mathbb{K}$ is the bivariate function

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

The differential operation D is linear and acts in many ways like a derivative; e.g. the differential of a $\mathbb{F}_q$-quadratic map is $\mathbb{F}_q$-bilinear, the differential of a $\mathbb{F}_q$-cubic function is $\mathbb{F}_q$-bi-quadratic, etc. The operators D^2, D_x, and so on all work analogously as do $\frac{d^2}{dx^2}$, $\frac{\partial}{\partial x}$, etc.

Differential attacks have been the basis of several cryptanalyses, see [19, 20, 5, 6, 9, 7]. The two basic techniques are linear differential symmetry attacks and differential invariant attacks.

Linear differential symmetry attacks attempt to find linear maps L that "factor through" the differential of the central map in an interesting way. Specifically, the goal is to find maps L satisfying

$$Df(La, x) + Df(a, Lx) = \Lambda_L Df(a, x).$$

If such a map can be found, it allows one to "remove" the minus modifier by discovering new linear combinations of the central maps that are linearly independent of the public key.

Such an attack is what broke SFLASH in [20]. If L represents multiplication by an element $\sigma \in \mathbb{K}$, then one can factor out σ from the differential due to the fact that the central map f is multiplicative. This vulnerability is provably removed via projection as shown in [11]. Thus PFLASH is invulnerable to this attack.

The other differential attack model, the invariant attacks, use the low rank structure on a large subspace of the public key to enhance the linear algebra search version of MinRank. Specifically, if a large subspace of the public key have the property that the matrices representing the functions as quadratic form map a particular subspace V simultaneously into another subspace W of the same dimension, then any projection producing two full rank differentials Df_1 and Df_2 allow one an advantage in recovering V, since V is left invariant by $Df_1 Df_2^{-1}$. This attack has been applied to undermine some of the proposed parameters for ABC and cubic ABC in [5–7] and was used to break the balanced oil-vinegar scheme in [21]. This attack was shown to be useless against PFLASH in [18].

3.3 Algebraic Attacks

The most straightforward attack is to try to directly invert the public key via Gröbner bases. The complexity of solving such systems relies on the degree of regularity of the system, which can be defined as the smallest degree at which a nontrivial syzygy producing a degree fall is generated in the Gröbner basis algorithm.

As shown in [22], the degree of regularity for HFE- systems satisfies the bound

$$d_{reg} \leq (q-1)\left\lfloor \frac{\lceil log_q(D) \rceil + a}{2} \right\rfloor + 2.$$

This upper bound is fairly tight for small fields and provides a fair estimate of the complexity of the direct algebraic attack on HFE-.

4 Description of EFLASH

Our scheme will be a new parameterization of a projected C^{*-}. A major difference between our scheme and the previously studied PFLASH, is the size of the projection. The size of our projection π will be much larger.

4.1 Algebraic Structure

We will let n be the number of variables and $d > n$ be the degree of the extension field over $\mathbb{F}_q$. We will let $m \geq n$ be the number of equations $(m < d)$ and denote the number of equations removed by $a = d - m$. We will compose our central map $(x)f = x^{q^\theta + 1}$ with affine maps S and T from $(\mathbb{F}_q)^d$ to $(\mathbb{F}_q)^d$. We let ϕ be a vector space isomorphism from $(\mathbb{F}_q)^d$ to $\mathbb{F}_{q^d}$, π be a linear embedding from $(\mathbb{F}_q)^n$ to $(\mathbb{F}_q)^d$, and τ be a linear projection from $(\mathbb{F}_q)^d$ to $(\mathbb{F}_q)^m$.

$$\begin{tikzcd}
& & \mathbb{F}_{q^d} \arrow[r, "f"] & \mathbb{F}_{q^d} \arrow[d, "\phi^{-1}"] & & \\
& (\mathbb{F}_q)^d \arrow[r, "S"] & (\mathbb{F}_q)^d \arrow[u, "\phi"] & (\mathbb{F}_q)^d \arrow[r, "T"] & (\mathbb{F}_q)^d \arrow[dr, "\tau"] & \\
& & & & & (\mathbb{F}_q)^m \\
(\mathbb{F}_q)^n \arrow[uur, "\pi"] & & & & &
\end{tikzcd}$$

Our public equations P can be found by computing $P = \pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T \circ \tau$, where $(x)f = x^{q^\theta+1}$ (recall that we are using left to right composition notation).

4.2 Encryption and Decryption

To encrypt a message $\overline{x}$, the sender would just compute $(\overline{x})P = (\overline{x})\pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T \circ \tau = \overline{y}$ to get cipher text $\overline{y}$. To decrypt the message we will take advantage of some of the weaknesses that an unmodified C^* scheme possesses.

To decrypt, we exploit the more efficient method of inversion Patarin developed in his linearization equations attack from [23]. Specifically, if $\overline{v} = (\overline{u})(\phi \circ f \circ \phi^{-1})$ then there is a system of d polynomials of the form

$$\sum_{0 \le i,j < d} \alpha_{i,j,\ell} u_i v_j + \sum_{0 \le i < d} \beta_{i,\ell} u_i + \sum_{0 \le i < d} \gamma_{i,\ell} v_i + \delta_\ell$$

in the coefficients of $\overline{u}$ and $\overline{v}$ which are simultaneously zero. Composing the right inverse of $\pi \circ S$ and T with $\overline{u}$ and $\overline{v}$, respectively, we obtain a bilinear relation between the plaintext $\overline{x}$ and $\overline{y}' = (\overline{x})\pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T$. Given access to the private key the calculation of this bilinear relation is immediate.

Inversion, given the ciphertext $\overline{y}$, is then accomplished by concatenating every possible suffix $\overline{y}_a$ to discover $\overline{y}' = \overline{y}||\overline{y}_a$. Success is determined by solving the affine system in $\overline{x}$ induced from the linearization equations upon input $\overline{y}'$. If the affine system has a solution, $\overline{x}$, we can be assured that $(\overline{x})P = \overline{y}$.

It is statistically unlikely that there are multiple preimages. Under the simplifying heuristic that outputs of f are independent and uniformly distributed, which is certainly not the case but seems statistically close, there are q^n distinct, randomly disributed outputs of $\pi \circ \phi \circ f \circ \phi^{-1} \circ T$. The probability that any two lie in any fixed particular coset of $\ker(\tau)$ is $1-(1-q^{-m})^{q^n} - q^{n-m}(1-q^{-m})^{q^n-1}$, which for $m \approx 2n$ is approximately $q^{-2n} \approx q^{-m}$. Thus, although summing these estimates over all of the q^m cosets of $\ker(\tau)$ indicates that it is likely that the public key is not injective, the probability of decryption failure is negligible.

5 Resistance to Known Attacks

The security analysis of EFLASH is quite related to that of PFLASH because of the similar algebraic structure. There are three attack methods that must be considered. Since the scheme requires more equations than variables to ensure a low probability of decryption failure, we require a careful analysis of the direct algebraic attack to ensure that the degree of regularity of the scheme is not too low. Second, in light of the attack on HFE- schemes, see [24], we require a MinRank analysis. Finally, given the history of the lineage of the C^* family, we require an analysis of symmetric differential methods.

5.1 Algebraic Attack

The first relevant attack for EFLASH is the direct algebraic attack. Algebraically, EFLASH is a high degree projected HFE- scheme, in the sense that EFLASH has a low Q-rank like HFE. Applying a projection to the input variables cannot increase the Q-rank, so we analyze the Q-rank of the central map composed with the minus modifier.

The key observation is that, unlike the case of HFE in which removing one equation in general increases the Q-rank by one, since the quadratic form associated with the central map is so sparse, the removal of one equation in general increases the rank by *two*. To see this, note that the coefficients of the quadratic form associated with HFE are restricted to a square submatrix whose size is typically the Q-rank of the map. A codimension one projection allows these coefficients to bleed into another row and column, which increases the size of the square by one. In contrast, the size of the smallest square containing the nonzero values in the quadratic form of the EFLASH central map is usually much larger than the Q-rank of EFLASH; in fact, the codimension one projection can produce two elements in original rows and columns, see Figure 1.

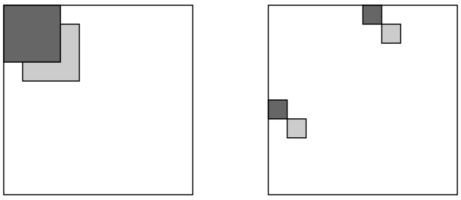

Fig. 1. The shape of the matrices representing the central maps of HFE- and C^{*-}. The darkly shaded regions represent nonzero values of the central map without the minus modifier, the lightly shaded regions represent new nonzero values introduced by the removal of one equation. Unshaded areas have coefficients of zero.

Thus, the central map of EFLASH has Q-rank $2+2a$. By the formula provided in [22], we compute an upper bound on the degree of regularity,

$$d_{reg} \leq (q-1)(a+1)+2. \tag{1}$$

When q is small this bound is known to be fairly tight. The complexity of the algebraic attack on EFLASH is therefore estimated to be $\mathcal{O}\left(\binom{n+d_{reg}}{d_{reg}}^{\omega}\right)$, where $2 \leq \omega \leq 3$ is the linear algebra constant.

We conducted experiments on some small scale instances of EFLASH to study the behavior of the degree of regularity for values of n and $m = d - a$ of a similar ratio to a full sized scheme with a low decryption failure rate. The results are shown in Table 1.

n	d	a	m	d_{reg}	d_{reg} (RANDOM)
16	28	9	19	4	4
24	37	9	28	4	5
32	47	9	38	5	6
40	56	9	47	≥ 6	7

Table 1. The degree of regularity of small scale EFLASH parameters in comparison to that of random systems of the same size.

The data show that the degree of regularity grows with the size of the system when a is fixed. Until the our resource permissions were limited on the machine, each sufficiently large system exhibited a degree of regularity at most one less than that of a random system. We do not have a solid theoretical argument for why the degree of regularity should be bounded thusly; however, for the sizes of schemes necessary to achieve security, the upper bound provided by (1) is already strictly less than the degree of regularity of random systems of the same size. We therefore conclude that for small q the bound provided by (1) is tight.

5.2 MinRank Attack

We can denote the calculations used to find our public equations P as matrix multiplications. Let $\mathbf{F^{*i}}$ be the matrix representation of the i^{th} Frobenius power of the central map f. Then the matrix $\mathbf{F^{*0}}$ represents our central map f, and is the $d \times d$ matrix with 1's in the $(0, \theta)$ and $(\theta, 0)$ coordinates and zeros elsewhere. Matrices $\mathbf{S}$ and $\mathbf{T}$ are $d \times d$ affine maps. We can also consider π as a linear embedding from $(\mathbb{F}_q)^n$ to $(\mathbb{F}_q)^d$, and τ as a linear projection from $(\mathbb{F}_q)^d$ to $(\mathbb{F}_q)^m$. Let σ be a primitive element of the extension, and thus $\{1, \sigma, \sigma^2, \ldots, \sigma^{d-1}\}$ is a basis vector over $\mathbb{F}_q$. Then mappings of ϕ and ϕ^{-1} can be represented as multiplication of M_d and M_d^{-1}, respectively, where

$$M_d = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \sigma & \sigma^q & \ldots & \sigma^{q^{d-1}} \\ \vdots & \vdots & \ldots & \vdots \\ \sigma^{d-1} & \sigma^{(d-1)q} & \ldots & \sigma^{(d-1)q^{d-1}} \end{pmatrix}$$

We can express the actions of τ by the following $d \times d$ matrix,

$$\tau^* = \begin{bmatrix} I_m & 0_{m\times a} \\ 0_{a\times m} & 0_{a\times a} \end{bmatrix}$$

.

Notice that $\tau^* : (\mathbb{F}_q)^d \to (\mathbb{F}_q)^d$. We will call $P^* := \pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T \circ \tau^*$. P and P^* will be comprised of the same m public equations, but P^* will then have a rows of 0 appended to it.

Consider $R = \phi^{-1} \circ T \circ \tau^* \circ \phi$. Then $R : \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ is linear. If we let $(x)\widetilde{\tau} = \mathit{\Pi}_{r\in\ker(R)}(x-r)$, then we know by proposition 2 in [11], there exists a nonsingular linear map $\widetilde{R}$ from $\mathbb{F}_{q^d}$ to $\mathbb{F}_{q^d}$ such that $xR = x\widetilde{\tau}\widetilde{R}$. Let $\widetilde{T} = \phi \circ \widetilde{\tau} \circ \widetilde{R} \circ \phi^{-1}$. This brings us to the following claim.

Claim 1 $(x)P^* = x\pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T \circ \tau^* = x\pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ \widetilde{T}$

Proof.

$$\begin{aligned} \pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ \widetilde{T} &= \pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ \phi \circ \widetilde{\tau} \circ \widetilde{R} \circ \phi^{-1} \\ &= \pi \circ S \circ \phi \circ f \circ \widetilde{\tau} \circ \widetilde{R} \circ \phi^{-1} \quad (*) \\ &= \pi \circ S \circ \phi \circ f \circ R \circ \phi^{-1} \\ &= \pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T \circ \tau^* \circ \phi \circ \phi^{-1} \\ &= \pi \circ S \circ \phi \circ f \circ \phi^{-1} \circ T \circ \tau^* \\ &= P^* \end{aligned}$$

□

Now, let us reconsider $(*)$. We know that our public key is equivalent to $(*)$, so we see that

$$\begin{aligned} P^* &= \pi \circ S \circ \phi \circ f \circ \widetilde{\tau} \circ \widetilde{R} \circ \phi^{-1} \\ &= \pi \circ S \circ \phi \circ f \circ \widetilde{\tau} \circ \phi^{-1} \circ \phi \circ \widetilde{R} \circ \phi^{-1} \\ &= \pi \circ S \circ \phi \circ \hat{f} \circ \phi^{-1} \circ \widehat{T} \end{aligned}$$

Where $\hat{f}$ is our new central map and $\hat{f} = f \circ \widetilde{\tau}$ and $\widehat{T} = \phi \circ \widetilde{R} \circ \phi^{-1}$. We now consider $\widehat{\mathbf{F}}^{*\mathbf{i}}$ to be the i^{th} Frobenius power of the new central map $\hat{f} = f \circ \widetilde{\tau}$. If we denote $h = \phi \circ \hat{f} \circ \phi^{-1}$, then we can find symmetric matrices $(\mathbf{H}_1, \ldots, \mathbf{H_d}) \in (\mathbb{F}_q)^d$ such that $h_i = \overline{x}\mathbf{H_i}\overline{x}^\top$. As shown in [16] we see,

$$(\mathbf{H_1}, \ldots, \mathbf{H_d}) = (\mathbf{M_d}\widehat{\mathbf{F}}^{*\mathbf{0}}\mathbf{M_d^\top}, \ldots, \mathbf{M_d}\widehat{\mathbf{F}}^{*\mathbf{(d-1)}}\mathbf{M_d^\top})\mathbf{M_d^{-1}}. \qquad (2)$$

If we denote the public key by $P = (g_1, g_2, \ldots, g_m)^\top$, then we can consider the symmetric matrices $(\mathbf{G_1}, \mathbf{G_2}, \ldots, \mathbf{G_m})$ that correspond to the public polynomials, such that $g_i = \overline{x}\mathbf{G_i}\overline{x}$. By analysis in [16] we find,

$$(\mathbf{G_1},\dots,\mathbf{G_m}) = (\pi\mathbf{S}\mathbf{M_d}\widetilde{\mathbf{F}}^{*\mathbf{0}}\mathbf{M_d^\top}\mathbf{S}^\top\pi^\top,\dots,\pi\mathbf{S}\mathbf{M_d}\widetilde{\mathbf{F}}^{*\mathbf{(d-1)}}\mathbf{M_d^\top}\mathbf{S}^\top\pi^\top)\mathbf{M_d^{-1}}\widetilde{\mathbf{T}} \tag{3}$$

When we consider our original central map, we saw that $\mathbf{F}^{*\mathbf{0}}$ has rank 2. Looking at our new central map $\hat{f}$, we see that $\widetilde{\tau}$ increases the rank. If we insist that θ is between $a+1$ and $d-a-1$, then $\widehat{\mathbf{F}}^{*0}$ has rank $2(a+1)$, as discussed in Section 5.1.

Notice that the embedding $\pi : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^d$, and the affine map S will not *increase* the rank of the right hand side of (3), so it will not affect our MinRank attack. Applying $\widehat{T}$ normally does increase the rank, but it does not increase the min-Q-rank because it just produces new linear combinations of these matrices.

Using these facts and the analysis from [16] we find that we are solving the MinRank problem:

$$\text{rank}\big(\sum_{k=0}^{m-1}\lambda_i\mathbf{G_i}\big) \le 2(a+1)$$

By the analysis in [25] and [26], the complexity of solving MinRank with the given parameters is $\mathcal{O}\big(\binom{m+d_{reg}}{d_{reg}}^{\omega}\big)$, where d_{reg} is the degree of regularity of the minors system and ω is the linear algebra constant. Treating EFLASH as a special case of HFE-, we may derive the degree of regularity of the minors system from [24, Conjecture 2] by using the Q-rank in place of the sum of the logarithm of the degree bound and the number of equations removed . Then we may estimate that the degree of regularity of the minors system is $d_{reg} = 2a+3$.

5.3 Discrete Differential Attack

In [11], it is shown that almost all parameters of PFLASH are secure against differential adversaries. The proof relies on the fact that the corank of the projection is relatively small. Since EFLASH uses a corank $d-n$ projection, the security proof does not apply and so we must use other arguments.

By the symmetric argument to that of [24, Lemma 2], we can express our projection π under the appropriate basis as a polynomial in $\mathbb{K}$ of degree q^{d-n}. Thus, the central quadratic form can be considered a quadratic form in the $d-n$ "variables" $\pi(x)^{q^i}$, for $0 \le i \le d-n$. In characteristic two, there are at least as many linearly independent quadratic monomials as in GF(2); thus, there are at least $\binom{d-n+1}{2}$ linearly independent quadratic monomials in $\pi(x)^{q^i}$, for $0 \le i \le d-n$ over $\mathbb{K}$.

We expect that the locus of stabilizing pairs of matrices is zero-dimensional over $\mathbb{K}$, though it is necessarily positive dimensional over $\mathbb{F}_q$ since scalar multiples induce symmetry for any map. We performed experiments and found that the solution space was zero-dimensional over $\mathbb{K}$ in all cases. We conclude that the space of linear maps inducing symmetry on EFLASH is too small to be exploited like in the attack on SFLASH of [20].

6 Parameter Selection

In choosing parameters for EFLASH, we need to consider security against the direct algebraic attack, the MinRank attack, and fault attacks exploiting decryption failure. We address the constraints each of these attacks places on parameters, as well as efficiency concerns.

The complexity of both the direct attack and the MinRank attack is directly related to the Q-rank of the public key. In the case of very small fields, such as GF(2), the degree of regularity is little larger than the Q-rank, $2a+2$; thus, several equations must be removed to achieve security. Over GF(2), each increase in a doubles decryption time while making the direct attack approximately n times harder and the MinRank attack approximately $2m$ times harder.

To address decryption failures, we note that the probability estimate of Section 4 is approximately q^{2n-2m}. We set an reasonable bound 2^{-B} on the probability of decryption failure and may set $m = n + \frac{B}{2lg(q)}$ to achieve this bound.

For larger q, the MinRank attack seems to be the most concerning. For efficiency reasons, it is impractical to have a large a; therefore, an instance with large q is vulnerable to MinRank. For this reason, we recommend the choice $q = 2$ with a and n sufficiently large to resist the algebraic attack. Our specific parameter selections for classical security levels are summarized in Table 2.

Scheme	Security	Public Key B	Enc. (ms)	Dec. (ms)	Dec. Failure
EFLASH$(2, 80, 101, 5)$	80-bit	38892	0.7	194	2^{-32}
EFLASH$(2, 134, 159, 9)$	128-bit	169613	1.3	12758	2^{-32}

Table 2. Parameters and performance of EFLASH(q, n, d, a) at the 80-bit and 128-bit classical security levels.

In principle, Grover search should affect the security of these schemes, but at this time we are not aware of a result that indicates a Grover search would be feasible for such large parameters. It is possible that Grover search could halve the dimension of the preimage search space. Thus, we may have to roughly double the size of the plaintext. To protect against the possible threat of Grover search we consider the parameter selections shown in Table 3.

On the other hand, we may consider the possibility of the cryptosystem being implemented on a quantum device so that the search step in decryption may be Groverized. Therefore Grover's algorithm may, in fact, improve efficiency.

Scheme	Security	Public Key B	Enc. (ms)	Dec. (ms)	Dec. Failure
EFLASH$(2, 160, 181, 5)$	80-bit	141691	1.9	1140	2^{-32}
EFLASH$(2, 256, 279, 7)$	128-bit	559249	5.3	16177	2^{-32}

Table 3. Parameters and performance of EFLASH(q, n, d, a) at the 80-bit and 128-bit quantum security levels.

7 Conclusion

In this paper we propose a new multivariate encryption scheme, EFLASH, derived from the lineage of PFLASH. One can view EFLASH as a parameterized projected C^{*-} scheme, where the projection π may be viewed as an embedding that maps from a smaller field to a much larger field. Thus, EFLASH follows the recent trend of achieving encryption with injective expansion maps.

EFLASH inherits some of the solid security justification from it digital signature forebear, PFLASH, though some of the security arguments are weakened by the massive cokernel of the projection. Still, the analysis of the security of EFLASH against each of the primary modes of attack on big field schemes is straightforward and encouraging. In this sense, it makes sense to consider the scheme as a sort of "standard candle" for the advancement of big field multivariate cryptanalysis. If EFLASH is to be broken, it seems that new a new technique will need to be discovered.

References

1. Cryptographic Technology Group: 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.
2. 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
3. Porras, J., Baena, J., Ding, J.: Zhfe, a new multivariate public key encryption scheme. [27] 229–245
4. Yasuda, T., Sakurai, K. In: A Multivariate Encryption Scheme with Rainbow. Springer International Publishing, Cham (2016) 236–251
5. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. [27] 180–196
6. Moody, D., Perlner, R.A., Smith-Tone, D. In: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme. Springer (2017)
7. Moody, D., Perlner, R.A., Smith-Tone, D.: Improved attacks for characteristic-2 parameters of the cubic ABC simple matrix encryption scheme. [28] 255–271
8. Cabarcas, D., Smith-Tone, D., Verbel, J.A.: Key recovery attack for ZHFE. [28] 289–308
9. Perlner, R.A., Petzoldt, A., Smith-Tone, D. In: Total Break of the SRP Encryption Scheme. Springer, In press. (2017)
10. 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.: Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China, October 18-22, 1998, Proceedings. Volume 1514 of Lecture Notes in Computer Science., Springer (1998) 35–49
11. Cartor, R., Smith-Tone, D.: An updated security analysis of PFLASH. [28] 241–254

12. Patarin, J., Goubin, L., Courtois, N.: Improved algorithms for isomorphisms of polynomials. In Nyberg, K., ed.: Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding. Volume 1403 of Lecture Notes in Computer Science., Springer (1998) 184–200

13. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: EUROCRYPT. (1996) 33–48

14. Berlekamp, E.R.: Factoring polynomials over large finite fields. Mathematics of Computation **24** (1970) pp. 713–735

15. Kipnis, A., Shamir, A.: Cryptanalysis of the hfe public key cryptosystem by relinearization. Advances in Cryptology - CRYPTO 1999, Springer **1666** (1999) 788

16. 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

17. Daniels, T., Smith-Tone, D.: Differential properties of the HFE cryptosystem. [27] 59–75

18. Chen, M.S., Yang, B.Y., Smith-Tone, D.: Pflash - secure asymmetric signatures on smart cards. Lightweight Cryptography Workshop 2015 (2015) http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-smith-tone-paper.pdf.

19. Hashimoto, Y.: Cryptanalysis of multi-hfe. IACR Cryptology ePrint Archive **2015** (2015) 1160

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. Shamir, A., Kipnis, A.: Cryptanalysis of the oil & vinegar signature scheme. CRYPTO 1998. LNCS **1462** (1998) 257–266

22. Ding, J., Kleinjung, T.: Degree of regularity for HFE-. IACR Cryptology ePrint Archive **2011** (2011) 570

23. Patarin, J.: Cryptoanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In Coppersmith, D., ed.: CRYPTO. Volume 963 of Lecture Notes in Computer Science., Springer (1995) 248–261

24. Vates, J., Smith-Tone, D.: Key recovery attack for all parameters of HFE-. [28] 272–288

25. Bardet, M., Faugere, J.C., Salvy, B.: On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving. (2004)

26. Bardet, M., Faugére, J., Salvy, B., Yang, B.: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. Proc. of MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry (2005)

27. 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)

28. 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

We illustrate our scheme by presenting a toy example. We generate public and private keys and perform a decryption. For simplicity, we consider linear, as opposed to affine, transformations.

A.1 Public and Private Key Generation

Let $q = 2$, $n = 4$, $d = 8$ and $a = 2$. We construct the degree d extension field $\mathbb{K} = \mathbb{F}_2[x]/\left\langle x^8 + x^4 + x^3 + x^2 + 1\right\rangle$. We randomly select the C^* monomial $f(x) = x^{2^5+1}$. We next randomly select the invertible transformation T and embedding U:

$$T = \begin{bmatrix} 1\,0\,1\,1\,1\,0\,1\,0 \\ 0\,1\,0\,1\,0\,1\,1\,1 \\ 1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,1\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,0\,1\,0\,1 \\ 1\,0\,0\,0\,0\,1\,1\,1 \\ 0\,1\,0\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1 \end{bmatrix}, \text{ and } U = \begin{bmatrix} 0\,1\,1\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 1\,0\,1\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,0\,0\,0\,0 \end{bmatrix}.$$

We fix $\mathit{\Pi} : \mathbb{F}_q^8 \rightarrow \mathbb{F}_q^6$, the projection onto the first 6 coordinates. Then the public key $P = \mathit{\Pi} \circ T \circ \phi^{-1} \circ f \circ \phi \circ U$ in symmetric matrix form over $\mathbb{F}_q$ is given by:

$$\mathbf{P_1} = \begin{bmatrix} 0\,0\,0\,1 \\ 0\,0\,0\,0 \\ 0\,0\,0\,1 \\ 1\,0\,1\,0 \end{bmatrix}, \mathbf{P_2} = \begin{bmatrix} 1\,0\,1\,1 \\ 0\,1\,0\,0 \\ 1\,0\,0\,1 \\ 1\,0\,1\,0 \end{bmatrix}, \mathbf{P_3} = \begin{bmatrix} 0\,1\,0\,1 \\ 1\,0\,1\,0 \\ 0\,1\,1\,0 \\ 1\,0\,0\,1 \end{bmatrix},$$

$$\mathbf{P_4} = \begin{bmatrix} 0\,1\,1\,1 \\ 1\,0\,0\,1 \\ 1\,0\,0\,0 \\ 1\,1\,0\,0 \end{bmatrix}, \mathbf{P_5} = \begin{bmatrix} 0\,0\,1\,1 \\ 0\,1\,0\,1 \\ 1\,0\,0\,1 \\ 1\,1\,1\,0 \end{bmatrix}, \mathbf{P_6} = \begin{bmatrix} 0\,0\,1\,1 \\ 0\,0\,1\,0 \\ 1\,1\,0\,0 \\ 1\,0\,0\,0 \end{bmatrix}.$$

We note that P has some linear terms that can be found on the diagonals of the public matrices.

The plaintext $\overline{x}$ and the output, $\overline{v}$, of $\phi^{-1} \circ f \circ \phi \circ U$ are related by linearization equations due to the relation

$$uv^{2^5} + u^{2^{10}}v = 0,$$

where $u = \phi(U\overline{x})$ and $v = \phi(\overline{v})$. Given our choice of basis we generate these linearization equations, written here in matrix form:

$$\mathbf{L_1} = \begin{bmatrix} 1&1&1&1&1&1&0&1 \\ 0&0&0&0&1&0&1&0 \\ 1&0&1&1&0&1&1&0 \\ 1&1&0&0&0&0&1&0 \end{bmatrix}, \mathbf{L_2} = \begin{bmatrix} 1&1&1&1&0&0&1&1 \\ 1&0&1&0&0&0&0&0 \\ 1&1&1&0&0&0&1&1 \\ 0&1&1&1&1&1&1&0 \end{bmatrix}, \mathbf{L_3} = \begin{bmatrix} 1&0&0&1&0&0&1&1 \\ 1&0&0&1&0&0&1&0 \\ 1&0&0&0&0&0&1&1 \\ 0&0&1&0&1&1&0&1 \end{bmatrix},$$

$$\mathbf{L_4} = \begin{bmatrix} 1&1&0&0&0&1&1&1 \\ 1&1&1&0&1&1&0&1 \\ 1&1&0&1&1&1&1&0 \\ 1&1&1&1&0&1&0&1 \end{bmatrix}, \mathbf{L_5} = \begin{bmatrix} 0&0&0&0&1&1&0&1 \\ 0&0&1&0&1&0&0&0 \\ 0&1&1&1&0&1&0&1 \\ 1&0&0&1&1&1&0&1 \end{bmatrix}, \mathbf{L_6} = \begin{bmatrix} 0&0&0&0&0&1&1&1 \\ 0&1&1&1&1&1&0&1 \\ 0&0&1&0&1&1&1&1 \\ 0&1&0&1&1&1&1&1 \end{bmatrix},$$

$$\mathbf{L_7} = \begin{bmatrix} 1&1&0&0&1&0&0&0 \\ 1&1&0&0&1&0&0&1 \\ 1&1&1&1&0&0&1&1 \\ 0&1&1&1&1&1&1&1 \end{bmatrix}, \mathbf{L_8} = \begin{bmatrix} 1&1&1&1&1&0&0&0 \\ 1&0&0&0&1&0&0&0 \\ 0&1&0&1&1&1&1&1 \\ 0&1&0&0&0&1&1&1 \end{bmatrix}.$$

A.2 Encryption and Decryption

Encryption is accomplished by evaluating the public key at the ciphertext. We randomly choose a plaintext

$$\overline{x} = \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}.$$

Computing $(\overline{x})P$ we obtain the ciphertext

$$\overline{y} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Decryption is accomplished by first appending a random suffix on $\overline{y}$ to form $\overline{y_0}$, applying T^{-1}, and then solving the linear system defined by the linearization equations. Our first attempt appends the zero vector to $\overline{y}$. Thus

$$\overline{y}_0 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

We then solve the system $\mathbf{0} = \overline{x}\mathbf{L}_i\overline{y}_0^\top$, where $1 \leq i \leq 8$, for $\overline{x}$. We immediately obtain the valid plaintext $\begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}$. We subsequently append all remaining possible suffixes on $\overline{y}$ and attempt to invert. Each of these linear systems is inconsistent, however; thus $\overline{x}$ is the unique preimage and so the valid plaintext.