On the Effect of Projection on Rank Attacks in Multivariate Cryptography

Morten Øygarden[1], Daniel Smith-Tone[2,3], and Javier Verbel[4]

[1] Simula UiB, Norway
morten.oygarden@simula.no
[2] National Institute of Standards and Technology, USA
daniel.smith@nist.gov
[3] University of Louisville, USA
[4] Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE
javier.verbel@tii.ae

Abstract. The multivariate scheme HFEv- used to be considered a promising candidate for a post-quantum signature system. First suggested in the early 2000s, a version of the scheme made it to the third round of the ongoing NIST post-quantum standardization process. In late 2020, the system suffered from an efficient rank attack due to Tao, Petzoldt, and Ding. In this paper, we inspect how this recent rank attack is affected by the projection modification. This modification was introduced to secure the signature scheme PFLASH against its predecessor's attacks. We prove upper bounds for the rank of projected HFEv- (pHFEv-) and PFLASH under the new attack, which are tight for the experiments we have performed. We conclude that projection could be a useful tool in protecting against this recent cryptanalysis.

Keywords: post-quantum cryptography, multivariate cryptography, min-rank

1 Introduction

Multivariate cryptography has received increased attention over the last years, due to its potential of providing quantum–safe public key cryptosystems. Signature schemes based on these ideas seemed particularly promising, with one finalist, Rainbow [12], and one alternate candidate, G*e*MSS [8], reaching the third and current round of the NIST post–quantum standardization process. Recently, new attacks have been presented against both of these candidates [3, 24]. The rank attack against G*e*MSS seems particularly effective, breaking all the suggested parameters for this scheme.

A similar story took place over a decade ago, when the signature scheme SFLASH was broken [14]. In the aftermath, it was discovered that this attack can be avoided by projecting the input space [13], and the amended scheme, PFLASH [9], has withstood cryptanalysis up until this point. In this article, we study the effect of projection on the new rank attack from [24], with a particular interest in the setting of HFEv- (the core of the G*e*MSS scheme), and PFLASH. After briefly describing the schemes and the attack, we prove that the attack also applies to PFLASH, breaking all of the proposed parameters. We then provide upper bounds for the rank in both the setting of HFEv- and PFLASH. We test the validity of these results through experiments, before concluding with a discussion on possible secure parameters and the impact these changes have on signing time.

Notation. For readability, we use the following notational conventions throughout the article. $\mathbb{F}_q^{n_1\times n_2}$ will denote the space of matrices of size $n_1 \times n_2$ over $\mathbb{F}_q$, and matrices will be written in **bold**. Row (resp. column) entries in matrices will be written as an integer modulo n_1 (resp. n_2). For two matrices $\mathbf{A}$ and $\mathbf{B}$, we let $\mathbf{A}|\mathbf{B}$ denote their horizontal concatenation, and $\mathbf{A} \oplus \mathbf{B} = \begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{bmatrix}$ is the direct sum. Maps over $\mathbb{F}_q$ will be written using capital letters, while maps over extension fields, $\mathbb{F}_{q^n}$, will be written with lowercase letters.

2 Big Field Cryptosystems

We start by describing a general big field cryptosystem, with the vinegar, minus and projection modifiers. Let q be the power of a prime, n a positive integer, and fix an isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$. Define $\psi = \phi \times \mathrm{id}_v : \mathbb{F}_q^{n+v} \to \mathbb{F}_{q^n} \times \mathbb{F}_q^v$, where $\psi = \phi$ if $v = 0$. A quadratic central map is chosen of the form $F = \phi^{-1} \circ f \circ \psi : \mathbb{F}_q^{n+v} \to \mathbb{F}_q^n$, where f is specifically chosen in a way such that it is efficient to find preimages of it. Choose a linear map $U = (S \oplus \mathrm{id}_v) \circ U' : \mathbb{F}_q^{n+v-p} \to \mathbb{F}_q^{n+v}$, where both $S : \mathbb{F}_q^{n-p} \to \mathbb{F}_q^n$ and $U' : \mathbb{F}_q^{n+v-p} \to \mathbb{F}_q^{n+v-p}$ are linear maps of full rank. Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^{n-a}$ be a linear map of full rank. Then the public key is created as the composition $P = T \circ F \circ U : \mathbb{F}_q^{n+v-p} \to \mathbb{F}_q^{n-a}$. Figure 1 gives an overview of the construction. We will say that the scheme uses the minus modification if $a > 0$, the vinegar modification if $v > 0$, and the projection modification if $p > 0$.

$$\begin{tikzcd}
 & \mathbb{F}_{q^n} \times \mathbb{F}_q^v \arrow[r, "f"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^{n+v-p} \arrow[r, "U"] & \mathbb{F}_q^{n+v} \arrow[u, "\psi"] \arrow[r, "F"] & \mathbb{F}_q^n \arrow[r, "T"] & \mathbb{F}_q^{n-a}
\end{tikzcd}$$

Fig. 1: Diagram of a general big field scheme with minus, vinegar and projection modifiers.

HFEv-. The signature scheme HFEv- is based on the HFE central map proposed in [21]. It inspired two submissions to the NIST post–quantum standardization process: GeMSS [8] and Gui [11], where the former advanced to the third round as an alternate candidate. Fix a positive integer D, and denote the vinegar variables by $\mathbf{x_v} = (x_{n+1}, \ldots, x_{n+v})$. The central map is constructed from a polynomial f of the form

$$f_{hfe}(X, \mathbf{x_v}) = \sum_{\substack{i,j \in \mathbb{N} \\ q^i + q^j \leq D}} \alpha_{i,j} X^{q^i + q^j} + \sum_{\substack{i \in \mathbb{N} \\ q^i \leq D}} \beta_i(\mathbf{x_v}) X^{q^i} + \gamma(\mathbf{x_v}),$$

where $\alpha_{i,j} \in \mathbb{F}_{q^n}$, the β_i's are linear maps $\mathbb{F}_q^v \to \mathbb{F}_{q^n}$, and γ is a quadratic map $\mathbb{F}_q^v \to \mathbb{F}_{q^n}$. The rank attack introduced in [24], which we will recall in the next section, breaks GeMSS with the proposed parameters for the third round of the NIST Standardization process [8].

PFLASH. The signature scheme PFLASH [13, 9] is based on the C^* cryptosystem [18], and it uses the projection and minus modifiers. Since there are no vinegar modifiers, we will simply write $U = S$ for the input map. For an integer $0 < \theta < n - 1$, the central map is based on the monomial $f_{C^*} = X^{1+q^\theta}$, which is a bijection when $\gcd(q^\theta + 1, q^n - 1) = 1$. In this case, f_{C^*} can be inverted by exponentiation. With the secret key, one can also compute bilinear relations of inputs and outputs of the central map [20], which can be used to find preimages of the public key, as used in [7]. We also refer to [6] for more information on the security of PFLASH.

3 New Rank Attack

In this section, we briefly recall the new rank attack against HFEv-, that was introduced in [24]. More information about the underlying constructions can also be found in [2]. For simplicity, we consider $\mathbb{F}_q$ to be a field of odd characteristic in this section, but note that the results generalize to even fields as well (see e.g., Section 6.3 in [2]). In particular, the results in later sections will also hold in the binary case. Recall that $\mathbf{x_v} = (x_{n+1}, \ldots, x_{n+v})$ denotes the vinegar variables, and that all matrix entries are counted modulo n. For $X \in \mathbb{F}_{q^n}[X]$ we will write $\underline{X} = (X, X^q, \ldots, X^{q^{n-1}})$.

Proposition 1 ([24]). *Let f_{hfe} be an HFEv- polynomial over $\mathbb{F}_{q^n}$. Then,*

$$f_{hfe}(\underline{X}, \mathbf{x_v}) = (\underline{X}, \mathbf{x_v}) \begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B}^\top & \mathbf{D} \end{bmatrix} (\underline{X}, \mathbf{x_v})^\top,$$

where $\mathbf{A} = [\alpha_{i,j}] \in \mathbb{F}_{q^n}^{n \times n}$, $\mathbf{B} = [\beta_{i,j}] \in \mathbb{F}_{q^n}^{n \times v}$ and $\mathbf{D} = [\delta_{i,j}] \in \mathbb{F}_{q^n}^{v \times v}$. Also, for each $0 \leq k < n$

$$(f_{hfe}(\underline{X}, \mathbf{x_v}))^{q^k} = (\underline{X}, \mathbf{x_v}) \mathbf{F}^{*k} (\underline{X}, \mathbf{x_v})^\top,$$

where $\mathbf{F}^{*k} \in \mathbb{F}_{q^n}^{(n+v)\times(n+v)}$ *and its* (i,j)*-coordinate is given by*

$$\begin{cases} \alpha_{i-k,j-k}^{q^k} & \text{if } 0 \leq i,j < n-1 \\ \beta_{i-n,j-k}^{q^k} & \text{if } n \leq i < n+v \text{ and } 0 \leq j < n \\ \beta_{i-k,j-n}^{q^k} & \text{if } n \leq j < n+v \text{ and } 0 \leq i < n \\ \delta_{i-n,j-n}^{q^k} & \text{otherwise.} \end{cases}$$

Let $\mathbf{M} \in \mathbb{F}_{q^n}^{n\times n}$ be an invertible matrix associated with a vector basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (see Proposition 2 [2]), and let us consider an HFEv- public key $(P_1,\ldots,P_{n-a}) = T \circ F \circ U$. If $\mathbf{P}_i$ is the symmetric matrix such that $P_i(\mathbf{x}) = \mathbf{x}\mathbf{P}_i\mathbf{x}^\top$, then we have

$$(\mathbf{x}\mathbf{P}_1\mathbf{x}^\top,\ldots,\mathbf{x}\mathbf{P}_{n-a}\mathbf{x}^\top) = (\mathbf{x}\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^\top\mathbf{x}^\top,\ldots,\mathbf{x}\mathbf{W}\mathbf{F}^{*(n-1)}\mathbf{W}^\top\mathbf{x}^\top)\mathbf{M}^{-1}\mathbf{T},$$

where $\mathbf{W} = \mathbf{U}\tilde{\mathbf{M}}$ and $\tilde{\mathbf{M}} = \mathbf{M} \oplus \mathbf{I}_v$. By symmetry we have the following matrix equation

$$(\mathbf{P}_1|\cdots|\mathbf{P}_{n-a}) = \left(\mathbf{W}\mathbf{F}^{*0}\mathbf{W}^\top|\cdots|\mathbf{W}\mathbf{F}^{*(n-1)}\mathbf{W}^\top\right)\left(\mathbf{M}^{-1}\mathbf{T} \otimes \mathbf{I}_{n+v}\right). \qquad (1)$$

For any vector $\mathbf{u} \in \mathbb{F}_{q^n}^{n+v}$, we define

$$\mathbf{u}\mathbf{F}^* := \begin{bmatrix} \mathbf{u}\mathbf{F}^{*0} \\ \vdots \\ \mathbf{u}\mathbf{F}^{*(n-1)} \end{bmatrix} \in \mathbb{F}_{q^n}^{n\times(n+v)}, \text{ and } \mathbf{u}\mathbf{P}^* := \begin{bmatrix} \mathbf{u}\mathbf{P}_1 \\ \vdots \\ \mathbf{u}\mathbf{P}_{n-a} \end{bmatrix} \in \mathbb{F}_{q^n}^{(n-a)\times(n+v)}.$$

Notice that if the central map of the given public key $(P_1,\ldots,P_{n-a})$ has univariate degree at most D, then

$$\operatorname{rank}(\mathbf{e}\mathbf{F}^*) \leq \lceil \log_q(D) \rceil,$$

where $\mathbf{e} \in \mathbb{F}_{q^n}^{n+v}$ is any vector of weight one. Since $p = 0$, $\mathbf{W}$ is nonsingular, and by equation (1), we have

$$\operatorname{rank}(\mathbf{u}\mathbf{P}^*) \leq \lceil \log_q(D) \rceil,$$

where $\mathbf{u} = \mathbf{e}\mathbf{W}^{-1}$. In [24] the authors find such a vector $\mathbf{u}$ by solving an instance of the MinRank problem with $n+v$ matrices in $\mathbb{F}_q^{(n-a)\times(n+v)}$ and target rank $\lceil \log_q(D) \rceil$. Furthermore, [24] shows how this vector $\mathbf{u}$ can be used to recover an equivalent key for $(P_1,\ldots,P_{n-a})$. That is, to find linear maps T', U' and a HFEv- central map F' of degree at most D, such that

$$(P_1,\ldots,P_{n-a}) = T' \circ F' \circ U'.$$

The complexity of this attack is dominated by performing the MinRank step to recover $\mathbf{u}$. This computation in turn relies heavily on the rank of $\mathbf{u}\mathbf{P}^*$, which will be our primary focus in the next sections.

4 Effect of Projection on the New Rank Attack

We now turn our attention to how the projection modification affects the recently introduced rank attack that was described in the previous section. The first thing to notice is that the invertibility of the input transformation S is required to justify the rank bound. Thus, one may wonder whether the projection modifier masks the rank property just as it was shown to protect PFLASH from the attack on SFLASH, see [14, 22].

Despite the similarities between the HFE and C^* central maps, we find that there are subtle differences in how projection affects the different schemes. As a result, we consider the two settings separately in the following subsections.

4.1 Projection and the HFE Central Map

We adopt an approach dual to that of [25], where removing equations was shown to be equivalent to increasing the degree of the central map. Specifically, we prove that projection is equivalent to increasing the degree of the central map. Thus pHFEv- with degree bound D and projection p is an instance of HFEv- with degree bound q^pD.

For any $\mathbb{F}_q$-subspace K of $\mathbb{F}_{q^n}$ there exists a linear polynomial of the form

$$\min_K(X) = \prod_{\alpha \in K} (X - \alpha),$$

having K as its kernel. This polynomial is also known as the minimal polynomial of K, see [10]. We start by showing the following result.

Lemma 1. *There is a bijective correspondence between k-dimensional subspaces of $\mathbb{F}_{q^n}$ and $(n-k)$-dimensional subspaces of $\mathbb{F}_{q^n}$ given by*

$$W \mapsto Im(min_W(X)).$$

Proof. Let $\mathcal{V}_k$ be the collection of k-dimensional subspaces of $\mathbb{F}_{q^n}$. Define the map $\psi_k : \mathcal{V}_k \to \mathcal{V}_{n-k}$ by $\psi(W) = \mathrm{Im}(\min_W(X)) = W'$. Note that since $\min_W(X)$ has kernel of dimension k, and is $\mathbb{F}_q$–linear, the space W' will have dimension $n-k$, and ψ_k is thus well–defined. Moreover, $\min_{W'}(\min_W(X)) = 0$, and by degree considerations we have, more exactly, $\min_{W'}(\min_W(X)) = X^{q^n} - X$.

Suppose that

$$\min_W(X) = \sum_{i=0}^{k} \alpha_i X^{q^i} \quad \text{and} \quad \min_{W'}(X) = \sum_{i=0}^{n-k} \beta_i X^{q^i}.$$

Then we observe that the composition is

$$\begin{aligned} \min_{W'} \circ \min_W(X) &= \sum_{i=0}^{n-k} \sum_{j=0}^{k} \alpha_j^{q^i} \beta_i X^{q^{i+j}} \\ &= \sum_{r=0}^{n} \left(\sum_{\substack{0 \le i \le n-k \\ 0 \le j \le k,\ j+i=r}} \alpha_j^{q^i} \beta_i \right) X^{q^r} = X^{q^n} - X. \end{aligned} \tag{2}$$

Recalling that $\alpha_k = \beta_{n-k} = 1$, we find that this relation produces a system of n bilinear equations in the $k-1$ coefficients α_j and the $n-k-1$ coefficients β_i. Now fix a space W' in the image of ψ_k, and let β_i be the fixed, associated constants of $\min_{W'}(X)$. Ordering the equations from $r = n-1$ to $r = 0$, we may sequentially solve for α_j. In fact, other than the Frobenius powers applied to the α_j values, the system is triangular, and hence uniquely solvable (see Appendix A for a small toy example of this). Thus, ψ_k is injective. Since the action of taking the orthogonal complement twice yields the original space, the number of subspaces of dimension k and of dimension $n-k$ are equal. It follows that ψ_k is also surjective, and hence a bijection.

Now let S be a linear map[5] $\mathbb{F}_q^n \to \mathbb{F}_q^n$ with kernel of dimension p. Using Lemma 1, we choose π to be the unique minimal polynomial such that $\phi^{-1}(Im(\pi)) = Im(S)$. Note that π has degree q^p. Then we have an exact sequence

$$\mathbb{F}_q^n \xrightarrow{\phi^{-1} \circ \pi \circ \phi} Im(S) \to 0.$$

Since $\mathbb{F}_q$-vector spaces are free (and therefore projective) $\mathbb{F}_q$-modules, there exists an S' such that the following diagram commutes:

$$\begin{tikzcd}
 & \mathbb{F}_q^n \arrow[ld, dashed, "S'"'] \arrow[d, "S"] & \\
\mathbb{F}_q^n \arrow[r, "\phi^{-1}(\pi(\phi))"] & Im(S) \arrow[r] & 0
\end{tikzcd}$$

If S' is singular, then its rank is at least $n-p$, and its kernel is then contained in the kernel of S. If necessary, we can replace S' with a nonsingular linear map by redefining its value on $ker(S')$ to map into $ker(\phi^{-1} \circ \pi \circ \phi)$. We may then without loss of generality choose S' to be of full rank. Thus, we obtain the matrix equation $\mathbf{S} = \mathbf{S'Q}$, where $\mathbf{xQ} = \phi^{-1} \circ \pi \circ \phi(\mathbf{x})$.

[5] This is a slight abuse of notation from the S defined in Section 2, which had $\mathbb{F}_q^{n-p}$ as its domain. This is easily remedied by composing with a projection along the $n-p$ first coordinates.

We may now apply this result in the case of an HFEv- scheme. In this case, we have the public key

$$\left[\mathbf{P}_1 | \cdots | \mathbf{P}_{n-a}\right] = \left[\mathbf{U}\widetilde{\mathbf{M}}\mathbf{F}^{*0}\widetilde{\mathbf{M}}^\top\mathbf{U}^\top | \cdots | \mathbf{U}\widetilde{\mathbf{M}}\mathbf{F}^{*(n-1)}\widetilde{\mathbf{M}}^\top\mathbf{U}^\top\right] \left(\mathbf{M}^{-1}\mathbf{T} \otimes \mathbf{I}_n\right),$$

where $\widetilde{\mathbf{M}} = \mathbf{M} \oplus \mathbf{I}_v$ and $\mathbf{U} = \mathbf{U}'(\mathbf{S} \oplus \mathbf{I}_v)$[6]. We observe that

$$\begin{aligned}
\widetilde{\mathbf{U}}\widetilde{\mathbf{M}}\mathbf{F}^{*i}\widetilde{\mathbf{M}}^\top\widetilde{\mathbf{U}}^\top &= \mathbf{U}'(\mathbf{S} \oplus \mathbf{I}_v)\widetilde{\mathbf{M}}\mathbf{F}^{*i}\widetilde{\mathbf{M}}^\top(\mathbf{S}^\top \oplus \mathbf{I}_v)\mathbf{U}'^\top \\
&= \mathbf{U}'(\mathbf{S}'\mathbf{Q} \oplus \mathbf{I}_v)\widetilde{\mathbf{M}}\mathbf{F}^{*i}\widetilde{\mathbf{M}}^\top(\mathbf{Q}^\top\mathbf{S}'^\top \oplus \mathbf{I}_v)\mathbf{U}'^\top \\
&= \mathbf{U}'(\mathbf{S}'\mathbf{Q}\mathbf{M} \oplus \mathbf{I}_v)\mathbf{F}^{*i}(\mathbf{M}^\top\mathbf{Q}^\top\mathbf{S}'^\top \oplus \mathbf{I}_v)\mathbf{U}'^\top
\end{aligned}$$

We may further rewrite the last expression to obtain

$$\mathbf{U}'(\mathbf{S}'\mathbf{M} \oplus \mathbf{I}_v)(\mathbf{M}^{-1}\mathbf{Q}\mathbf{M} \oplus \mathbf{I}_v)\mathbf{F}^{*i}(\mathbf{M}^\top\mathbf{Q}^\top\mathbf{M}^{-\top} \oplus \mathbf{I}_v)(\mathbf{M}^\top\mathbf{S}'^\top \oplus \mathbf{I}_v)\mathbf{U}'^\top$$

We finally note that

$$\mathbf{X}(\mathbf{M}^{-1}\mathbf{Q}\mathbf{M} \oplus \mathbf{I}_v)\mathbf{F}^{*i}(\mathbf{M}^\top\mathbf{Q}^\top\mathbf{M}^{-\top} \oplus \mathbf{I}_v)\mathbf{X}^\top = \mathbf{X}\mathbf{G}^{*i}\mathbf{X}^\top,$$

where $\mathbf{X} = \left[X \; X^q \cdots X^{q^{n-1}} \; x_1 \cdots x_v\right]$ and where

$$G(X, x_1, \ldots, x_v) = F(\pi(X), x_1, \ldots, x_v).$$

Thus the public key can also be expressed as

$$\left[\mathbf{P}_1 | \cdots | \mathbf{P}_{n-a}\right] = \left[\mathbf{U}''\widetilde{\mathbf{M}}\mathbf{G}^{*0}\widetilde{\mathbf{M}}^\top\mathbf{U}''^\top | \cdots | \mathbf{U}''\widetilde{\mathbf{M}}\mathbf{G}^{*(n-1)}\widetilde{\mathbf{M}}^\top\mathbf{U}''^\top\right] \left(\mathbf{M}^{-1}\mathbf{T} \otimes \mathbf{I}_n\right),$$

where $\mathbf{U}''$ is the nonsingular map $\mathbf{U}'(\mathbf{S}' \oplus \mathbf{I}_v)$. Thus, the pHFEv-$(n, D, a, v, p)$ public key is also an HFEv-(n, q^pD, a, v) public key.

This allows us to follow the same reasoning used in the attack of HFEv- with degree $D = q^{p+d}$, and we have proved the following upper bound.

Proposition 2. *Let $(\mathbf{P}_1, \ldots, \mathbf{P}_{n-a})$ be the symmetric matrices of the public key of an instance of pHFEv-(n, D, a, v, p), where p is the projection corank. Then there is a non–zero tuple $\mathbf{u} \in \mathbb{F}_{q^n}^{n-p}$ such that $\mathbf{u}\mathbf{P}^*$ has rank at most $p + d$, where $d = \lceil \log_q D \rceil$.*

We will test the tightness of this upper bound in Section 5.

4.2 Projection and the C^* Central Map

Define the symmetric matrix $\mathbf{F}_{C^*}^{*i}$, associated with $f_{C^*}^{q^i}$, in a manner similar to Proposition 1. Describing $\mathbf{F}_{C^*}^{*i}$ is simpler than what was done in Proposition 1, seeing that it is 1 at the entries $(i, \theta + i)$ and $(\theta + i, i)$, and 0 elsewhere (recall that

[6] Following our slight abuse of notation when compared with Section 2: U' will now be an invertible linear map $\mathbb{F}_q^{n+v} \to \mathbb{F}_q^{n+v}$

entries are counted modulo n). While we may apply the theory from Section 4.1, the problem is that we no longer have a bound D on the non–zero part of $\mathbf{F}_{C^*}^{*0}$. Following the same reasoning as before would have yielded an upper bound of $2 + 2p$ for the rank, but it is possible to do better.

We define $\mathbf{v} = (v_0, \ldots, v_{n-1}) = \mathbf{uSM} \in \mathbb{F}_{q^n}^n$, and examine what rank the matrix $\mathbf{vF}_{C^*}^*$ can take. Note that the entry v_i, for $i \in \mathbb{Z}_n$, will contribute to the two entries in positions

$$e_1(i) = (i, i + \theta) \qquad \text{and} \qquad e_2(i) = (i - \theta, i - \theta)\,, \tag{3}$$

in the matrix $\mathbf{vF}_{C^*}^*$. Fix an integer i_0, and consider the pair v_{i_0} and $v_{i_0+\theta}$. They will now contribute to four entries in $\mathbf{vF}_{C^*}^*$, but two of them, $e_1(i_0) = (i_0, i_0 + \theta)$ and $e_2(i_0 + \theta) = (i_0, i_0)$, appear in the same row. It follows that the pair v_{i_0} and $v_{i_0+\theta}$ can only make a contribution of at most three to the rank of $\mathbf{vF}^*$. This is the key observation for the following result.

Lemma 2. *Let $I = \{i_0, \ldots, i_{k-1}\}$ be a set of k integers in $\mathbb{Z}_n$, such that $i_{j+1} = i_j + \theta$, for $0 \leq j < k - 1$. Consider the vector $\mathbf{v}_I = (v_0, \ldots, v_{n-1})$, where $v_j \in \mathbb{F}_{q^n} \setminus \{0\}$ if $j \in I$, and $v_j = 0$ otherwise. Then $\mathbf{v}_I\mathbf{F}_{C^*}^*$ has rank at most $k + 1$.*

Proof. For $l = 1, 2$, let $E_l(x)$ be the $n \times n$ matrix that is 1 at entry $e_l(x)$ (as defined in (3)), and 0 elsewhere. Then we can write $\mathbf{v}_I\mathbf{F}_{C^*}^*$ as the sum

$$\mathbf{v}_I\mathbf{F}_{C^*}^* = \sum_{j=0}^{k-1} \big(E_1(i_j) + E_2(i_j)\big).$$

From the discussion prior to the lemma, we know that $E_1(i_{j_0}) + E_2(i_{j_0+1})$ has rank 1, for $0 \leq j_0 < k-1$. Hence, $\mathbf{v}_I\mathbf{F}_{C^*}^*$ can be written as the sum of $2k-(k-1)$ matrices of rank 1, which proves the upper bound.

The next step is to look at which of these vectors $\mathbf{v}_I$ we can find in the image of $\mathbf{SM}$. This leads to the following upper bound.

Proposition 3. *Let $(\mathbf{P}_1, \ldots, \mathbf{P}_{n-a})$ be the symmetric matrices of the public key of an instance of PFLASH with projection p. Then there is a non–zero tuple $\mathbf{u} \in \mathbb{F}_{q^n}^{n-p}$ such that $\mathbf{uP}^*$ has rank at most $2 + p$.*

Proof. Let I be as defined in Lemma 2, and consider an associated vector $\mathbf{v}_I$, with the difference that $v_j \in \mathbb{F}_{q^n}$ if $j \in I$ (i.e., allowing 0 in these entries as well). $\mathbf{SM}$ has cokernel of dimension p, so choosing I of order $p + 1$ will guarantee that there is a non–trivial way to choose the entries in $\mathbf{v}_I$ such that it lies in the image of $\mathbf{SM}$. This can seen by performing Gaussian elimination on $\mathbf{SM}$, where the entries corresponding to I are being eliminated last. If all v_j for $j \in I$ are non–zero, we are done by Lemma 2. Otherwise, suppose one of them is zero, say $v_{i_l} = 0$. Then we may split I into the two (potentially empty) sets $I_1 = \{i_0, \ldots, i_{l-1}\}$, and $I_2 = \{i_{l+1}, \ldots, i_p\}$. Upon considering the two associated vectors $\mathbf{v}_{I_1}$ and $\mathbf{v}_{I_2}$, we may write $\mathbf{v}_I\mathbf{F}_{C^*}^* = \mathbf{v}_{I_1}\mathbf{F}_{C^*}^* + \mathbf{v}_{I_2}\mathbf{F}_{C^*}^*$. Using Lemma 2 on $\mathbf{v}_{I_1}\mathbf{F}^*_{C^*}$ and $\mathbf{v}_{I_2}\mathbf{F}^*_{C^*}$, along with the fact that $|I_1| + |I_2| = p$ ensures that the rank of $\mathbf{v}_I\mathbf{F}^*_{C^*}$ sums up to at most $p + 2$.

Finally, the cases where several entries v_j, $j \in I$ are zero, are dealt with by induction on this argument.

This upper bound is tight for the experiments we have run for PFLASH; more information can be found in Section 5. For now, we note that the integer set I used in the proof of Proposition 3 is not unique, and we can even consider a more general class of sets, than what was discussed in Lemma 2. Indeed, from the entries in (3), we note that the pair v_{i_0} and $v_{i_0+2\theta}$ will in particular contribute to the entries $e_1(i_0) = (i_0, i_0 + \theta)$ and $e_2(i_0 + 2\theta) = (i_0 + \theta, i_0 + \theta)$, each of which lies in the same column. Note that Lemma 2, and the proof of Proposition 3, could easily have been adopted to sets I where the consecutive indices have relative distance 2θ, as opposed to θ. Furthermore, we can use combinations of θ and 2θ for distance, as shown in the following result, which is a direct generalization of Lemma 2. The proof is identical to that of the aforementioned lemma.

Lemma 3. *Let $I = \{i_0, \ldots, i_{k-1}\}$ be a set of k integers in $\mathbb{Z}_n$, such that for $0 \leq j < k - 1$, the difference $i_{j+1} - i_j$ is congruent to either θ or 2θ mod n. Consider the vector $\mathbf{v}_I = (v_0, \ldots, v_{n-1})$, where $v_j \in \mathbb{F}_{q^n} \setminus 0$ if $j \in I$, and $v_j = 0$ otherwise. Then $\mathbf{v}_I\mathbf{F}^*_{C^*}$ has rank at most $k + 1$.*

Number of Solutions for the MinRank Step. Recall that [24] suggests setting $u_0 = 1$, in order to avoid finding multiples of the same solution to the MinRank–step of the attack. Let I a set of the form described in Lemma 3. Note that any such I of order $p + 1$ could have been used to prove Proposition 3. Hence, we expect each choice of I to, in general, correspond to a unique solution u of the MinRank problem of rank $p + 2$. If $\gcd(n, \theta) = 1$, and $2(p + 1) < n$, there are $n2^p$ ways to construct I (2^p combinations of distances θ and 2θ, with n rotations).

We ran a few toy examples to test this theory, by running the MinRank–step for the parameters $q = 2$, $n = 13$, $\theta = 3$, and $p = 1, 2$ and 3. In each test we found all possible solutions $\mathbf{u}$, and inspected the corresponding $\mathbf{v} = \mathbf{uSM}$. In each test the number of solutions were indeed $n2^p$, and the $\mathbf{v}$-vectors corresponded to all the different choices for I.

Weak Choices of $\boldsymbol{n}$ and $\boldsymbol{\theta}$. In special cases, it would be possible to derive a lower upper bound than what was presented in Proposition 3. This can, for instance, happen if the set I from Lemma 3 of order $k \geq 1$ is a loop, in the sense that $i_{k-1} - i_0 \equiv \theta$ or 2θ mod n. This is possible if the following equation has a solution:

$$x\theta + y2\theta \equiv 0 \mod n, \;\; x, y \in \mathbb{Z}_{\geq 0}, \text{ and } x + y = k - 1. \tag{4}$$

Solutions for this condition, with low values of k, can be found when the least common multiple of n and θ is small, or equivalently, when $\gcd(n, \theta)$ is large.

Indeed, we can observe this effect in the last two rows of the right side of Table 1: in both tests we have $n = 14$ and $p = 4$, but they differ by $\theta = 5$ and 6. In the first case, we have $\gcd(14, 5) = 1$, and we find no solutions $\mathbf{u}$ such that $\mathbf{uP}^*$ has rank 5. In the second case we have $\gcd(14, 6) = 2$, and $x = 1$, $y = 3$ is a solution of (4), with $k = 5$. The resulting effect is that we are able to find solutions of $\mathbf{u}$ such that $\mathbf{uP}^*$ is of rank 5. We include the condition $\gcd(n, \theta) = 1$ in our other PFLASH experiments in order to exclude weak cases like these.

5 Experiments

In the previous section we proved an upper bound on the rank of $\mathbf{uP}^*$, for both pHFEv-, and PFLASH; we will now examine this bound through experiments.

All tests have been performed as follows. After creating the public key P, we construct $\mathbf{uP}^*$ with the indeterminate vector $\mathbf{u}$, where $u_0 = 1$. For rank r, we follow the minors modelling [17], by computing the $(r + 1) \times (r + 1)$ minors of $\mathbf{uP}^*$, and solving the associated polynomial system using the implementation of F_4 [15] in the Magma Computer Algebra System[7], see [4]. For efficiency, we did not always include all the minors when computing the Gröbner basis. We chose the rank r to be one less than, or equal, to the upper bound determined in Propositions 2 and 3 for pHFE- and PFLASH, respectively. Red marks that the polynomial system from the minors modelling at this rank was inconsistent, whereas blue indicates that we were able to find solutions. The results are presented in Table 1.

Table 1: Experimentally found rank of $\mathbf{uP}^*$ for various parameters of pHFE- (left) and PFLASH (right). The number X indicates that there are no $\mathbf{u}$ such that $\mathbf{uP}^*$ has rank $\leq X$. The number X means that we were able to find a solution $\mathbf{u}$ yielding $\mathbf{uP}^*$ of rank $\leq X$. See Section 4.2 for a discussion on †.

q	**n**	**a**	**p**	**D**	**Upper Bound**	**Rank of $\mathbf{uP}^*$**
2	13	0	1	5	4	3, 4
2	13	0	2	5	5	4, 5
2	13	0	3	5	6	5
2	15	0	4	5	7	6
2	13	0	0	9	4	3, 4
2	13	4	1	9	5	4, 5
2	13	4	2	9	6	5, 6
2	17	6	1	9	5	4, 5
2	13	4	0	17	5	4, 5
2	13	4	1	17	6	5, 6
2	13	0	2	17	7	6

q	**n**	**a**	**p**	θ	**Upper Bound**	**Rank of $\mathbf{uP}^*$**
2	21	0	1	13	3	2, 3
2	21	0	2	13	4	3, 4
4	31	0	1	7	3	2
4	13	0	3	5	5	4, 5
4	25	8	0	11	2	1, 2
4	25	8	1	11	3	2, 3
4	17	5	3	7	5	4, 5
2	15	1	4	7	6	5, 6
2	15	0	5	7	7	6
4	14	4	4	5	6	5
4	14	4	4	6	$6^{\dagger}$	5

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

We note that in all our experiments, the upper bound seems to be tight. The notable exception is the last row on the right side of Table 1, where $\gcd(n,\theta) \neq 1$, as discussed in Section 4.2. The tests include cases where f_{C^*} is not a permutation, i.e., $\gcd(q^n - 1, q^\theta + 1) \neq 1$, and this does not seem to have an effect on this attack. Finally, the target r and the dimension of $\mathbf{uP}^*$ cannot be too close, in order to ensure that the solutions we find are truly a result of the extension field structure of the scheme. We have chosen to keep $(n-a) > r+3$ in our experiments. Indeed, in an earlier experiment with pHFE- of parameters $q=2$, $n=13$, $a=4$, $p=2$ and $D=17$, we found a unique solution to u at $r=6$, even though our upper bound is seven here. Upon further inspection, this solution was in the subfield $\mathbb{F}_q$ (as opposed to being in $\mathbb{F}_{q^n}$ proper, which is the case for the other tests), and we have not been able to find such solutions when rerunning the case. Hence, we conclude that this was a "false positive" caused by the small parameters of the test.

6 Complexity

In this section we compute the complexity of signing for pHFEv- and PFLASH. The inversion methods are quite disparate, so, again, we separate the exposition.

6.1 pHFEv- Signing

For this subsection we consider the base field $q=2$. This is what was used in the G*e*MSS submission, which is what we will use as a baseline for comparing pHFEv-. The most complex step of the inversion of an HFEv- public key lies in the application of the Berlekamp algorithm, see [1], for inverting the central map. In the case of pHFEv-, there is a tension between the complexity of inverting the degree D polynomial and the number, 2^p, of times that the polynomial must be inverted.

As shown in Section 4, an instance of pHFEv-(n, D, a, v, p) is also an instance of HFEv-$(n, 2^pD, a, v)$. Thus, we may always invert pHFEv-(n, D, a, v, p) by using the inversion procedure for HFEv-$(n, 2^pD, a, v)$. On the other hand, we may invert the instance of pHFEv- by inverting the central map of degree D, until the preimage lies in the image of the input projection. For each preimage, the probability that it lies in the image of a corank p projection is 2^{-p}. To see which is the better of the two methods, we begin by making the analysis in [8] for the complexity of inversion more tight.

As noted in [8, Theorem 1], the complexity of Berlekamp applied to a polynomial of degree D is $\mathcal{O}\left(M_{2^n}(D)(n + \log_2 D)\log_2 D\right)$, where $M_{2^n}(D)$ is the number of operations in the field $\mathbb{F}_{2^n}$ required to multiply two polynomials of degree D. The well-known formula, see [5], for this quantity

$$M_{2^n}(D) = \mathcal{O}\left(D \log_2 D \log_2 \log_2 D\right)$$

produces a complexity of

$$\mathcal{O}\left(D(\log_2 D)^2(n + \log_2 D)\log_2\log_2 D\right).$$

The above quantity only provides the algebraic complexity of polynomial inversion over $\mathbb{F}_{2^n}$. Since each multiplication in $\mathbb{F}_{2^n}$ requires $2n^2+n$ bit operations, we have that inverting the central map has a bit complexity of

$$\mathcal{O}\left((2n^2+n)D\log_2(D)^2(n+\log_2 D)\log_2\log_2 D\right).$$

Since we are considering values of $\log_2 D$ that are far less than n, we may further simplify to obtain the approximate bit complexity

$$Cn^3 D\log_2(D)^2\log_2\log_2 D,$$

for some constant C. We note that $\log_2\log_2 D$ may be as large as three or four, for the values of D needed to secure against [24]. It is thus a nontrivial factor in this expression.

Since the complexity of inverting pHFEv-(n, D, a, v, p) is 2^p times the complexity of inverting HFEv-(n, D, a, v), it is a factor of

$$\frac{(p+\log_2 D)^2\log_2(p+\log_2 D)}{\log_2(D)^2\log_2\log_2 D}$$

faster than inverting the scheme as an instance of HFEv-$(n, 2^pD, a, v)$.

Thus, securing the parameters of GeMSS while maintaining the array of parameters merely requires applying the projection modifier with a sufficiently large corank p to secure the scheme from the attack of [24]. We should note that projection does have the negative effect of increasing the signature failure rate by a factor of approximately e^{2^p}, but the rate is still $\exp(2^p-2^{a+v})$ which is negligible for any realistic parameters.

Parameters for pHFEv-. Let $d=\lceil\log_2 D\rceil$. Similar to [24], we use the support minors equations to derive a bilinear system in n_x+n_y variables, where $n_x=n+v$ and $n_y=\binom{n'}{d+p}$, and $n'=\left\lceil\frac{(n+v)(d+p+1)}{n-a}\right\rceil+d+p+1$. Such a bilinear system is expected to be solved at degree 3. The overall complexity of solving this system is then given by $\mathcal{O}\left((n_xn_y^2+n_x^2n_y)^\omega\right)$, where ω is the linear algebra constant.

In Appendix B, Table 2, we consider the third round parameters of GeMSS, and compute the size of the projection that is needed to achieve the required security level.

6.2 PFLASH Signing

For PFLASH, we recommend using the private key to derive the linearization equations proven to exist by Patarin in [20]. With these equations the legitimate user can find a preimage of the public key in one step instead of inverting the input and output transformations and using exponentiation to invert the central map.

As shown in Section 4, the rank of $\mathbf{uP}^*$ is $p+2$. The parameters suggested in [9] had $p=1$, which makes them vulnerable to the rank attack we have studied.

It is, once again, possible to protect against this by increasing the projection. However, the signing time will now be multiplied by a factor q^p, which favours the use of a small ground field, maybe even $q = 2$. In this setting, direct methods may also become an issue. Particularly a generalized version of the analysis presented in [19], perhaps using some of the notions from [26] should be considered. This is, however, beyond the scope of this article, and we leave it as an open question to determine if and how secure and efficient parameters for PFLASH may be chosen.

7 Conclusion

We have studied how projection affects the new rank attack from [24]. For the pHFEv- and PFLASH systems we have derived an upper bound on how the rank grows with the projection p, which in turn can be used to estimate the complexity of the attack as a whole. These bounds were furthermore observed to be tight in experiments.

While projection is a cheap modification for encryption systems, it does increase the signing time for signature schemes, typically by a factor of q for each dimension. Nevertheless, in the HFEv- setting, we note that projecting is a useful alternative to simply increasing the degree D. PFLASH can also be made secure against rank attacks by increasing p, but we believe more analysis on direct attacks are needed before we can suggest potential parameters.

References

1. E. R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):pp. 713–735, 1970.
2. L. Bettale, J.-C. Faugère, and L. Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.
3. W. Beullens. Improved Cryptanalysis of UOV and Rainbow. Cryptology ePrint Archive, Report 2020/1343, 2020. `https://eprint.iacr.org/2020/1343`.
4. W. Bosma, J. Cannon, and C. Playoust. The magma algebra system i: The user language. *J. Symb. Comput.*, 24(3–4):235–265, Oct. 1997.
5. D. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28:693–701, July 1991.
6. R. Cartor and D. Smith-Tone. An updated security analysis of PFLASH. In *International Workshop on Post-Quantum Cryptography*, pages 241–254. Springer, 2017.
7. R. Cartor and D. Smith-Tone. EFLASH: a new multivariate encryption scheme. In *International Conference on Selected Areas in Cryptography*, pages 281–299. Springer, 2018.
8. A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. GeMSS: A Great Multivariate Short Signature (Round 3 submission). Technical report, National Institute of Standards and Technology, 2020. `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.

9. M.-S. Chen, B.-Y. Yang, and D. Smith-Tone. PFLASH-secure asymmetric signatures on smart cards. In *Lightweight Cryptography Workshop*, 2015.
10. T. Daniels and D. Smith-Tone. Differential properties of the HFE cryptosystem. In M. Mosca, editor, *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, volume 8772 of *Lecture Notes in Computer Science*, pages 59–75. Springer, 2014.
11. J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, and B.-Y. Yang. GUI. Technical report, National Institute of Standards and Technology, 2017. `https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissions`.
12. J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, M. Kannwischer, and J. Patarin. Rainbow (round 3 submission). Technical report, National Institute of Standards and Technology, 2020. `https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions`.
13. J. Ding, V. Dubois, B.-Y. Yang, O. C.-H. Chen, and C.-M. Cheng. Could SFLASH be repaired? In *International Colloquium on Automata, Languages, and Programming*, pages 691–701. Springer, 2008.
14. V. Dubois, P.-A. Fouque, A. Shamir, and J. Stern. Practical Cryptanalysis of SFLASH. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.
15. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.
16. F. Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303, 2014.
17. F. Levy-dit Vehel, J.-C. Faugère, and L. Perret. Cryptanalysis of MinRank. In *Annual International Cryptology Conference*, pages 280–296. Springer, 2008.
18. T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.
19. M. Øygarden, P. Felke, H. Raddum, and C. Cid. Cryptanalysis of the multivariate encryption scheme EFLASH. In *Cryptographers' Track at the RSA Conference*, pages 85–105. Springer, 2020.
20. J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *Annual International Cryptology Conference*, pages 248–261. Springer, 1995.
21. J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer, 1996.
22. D. Smith-Tone. Properties of the discrete differential with cryptographic applications. In N. Sendrier, editor, *PQCrypto*, volume 6061 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2010.
23. V. Strassen. Gaussian elimination is not optimal. *Numerische mathematik*, 13(4):354–356, 1969.
24. C. Tao, A. Petzoldt, and J. Ding. Improved Key Recovery of the HFEv- Signature Scheme. Cryptology ePrint Archive, Report 2020/1424, 2020. `https://eprint.iacr.org/2020/1424`.
25. J. Vates and D. Smith-Tone. Key recovery attack for all parameters of HFE-. In T. Lange and T. Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*, volume 10346 of *Lecture Notes in Computer Science*, pages 272–288. Springer, 2017.

26. M. Øygarden, P. Felke, and H. Raddum. Analysis of Multivariate Encryption Schemes: Application to Dob. Cryptology ePrint Archive, Report 2020/1442, 2020. https://eprint.iacr.org/2020/1442.

A Toy Example of Composing Minimal Polynomials

We provide a small toy example of the bilinear system from the proof of Lemma 1. Consider $n = 5$ and $k = 2$. Then, by Equation (2), and recalling $\alpha_2 = \beta_3 = 1$, we have

$$\begin{aligned}\min_{W'} \circ \min_W(X) &= X^{q^5} - X \\ &= \alpha_0\beta_0 X + (\beta_0\alpha_1 + \beta_1\alpha_0^q)X^q + (\beta_0 + \beta_1\alpha_1^q + \beta_2\alpha_0^{q^2})X^{q^2} \\ &+ (\beta_1 + \beta_2\alpha_1^{q^2} + \alpha_0^{q^3})X^{q^3} + (\alpha_1^{q^3} + \beta_2)X^{q^4} + X^{q^5}.\end{aligned}$$

If the β_j's are known constants, we note that α_1 is uniquely determined by the equation $\alpha_1^{q^3} + \beta_2 = 0$. Subsequently, α_0 will be uniquely determined by $\alpha_0^{q^3} + \beta_2\alpha_1^{q^2} + \beta_1 = 0$.

B G*e*MSS Minrank Complexity

In Table 2, we consider the third round parameters of G*e*MSS, and compute the size of the projection that is needed to achieve the required security level. We do this for two values of ω: $\omega_1 = 2.37$ is the best known asymptotic bound [16], and $\omega_2 = 2.81$ is the more realistic value from Strassen's algorithm [23].

Table 2: Complexity of the MinRank attack from [24] against the GeMSS parameters with projection. The value p_1 (resp. p_2) is the minimum projection needed to achieve security with ω_1 (resp. ω_2), and C_{ω_1} (resp. C_{ω_2}) denotes $\log_2$ of the resulting complexity.

Scheme	(n, v, D, a)	p_1	C_{ω_1}	p_2	C_{ω_2}
GeMSS128	(174, 12, 513, 12)	2	136	0	139
BlueGeMSS128	(175, 14, 129, 13)	4	140	1	128
RedGeMSS128	(177, 15, 17, 15)	6	131	4	128
WhiteGeMSS128	(175, 12, 513, 12)	2	136	0	139
CyanGeMSS128	(177, 13, 129, 14)	4	140	1	128
MagentaGeMSS128	(178, 15, 17, 15)	6	131	4	128
GeMSS192	(265, 20, 513, 22)	7	192	5	201
BlueGeMSS192	(265, 23, 129, 22)	9	192	7	201
RedGeMSS192	(266, 25, 17, 23)	12	192	10	205
WhiteGeMSS192	(268, 21, 513, 21)	7	192	5	201
CyanGeMSS192	(270, 22, 129, 23)	9	192	7	201
MagentaGeMSS192	(271, 24, 17, 24)	12	192	10	205
GeMSS256	(354, 33, 513, 30)	14	263	10	267
BlueGeMSS256	(358, 32, 129, 34)	16	267	11	256
RedGeMSS256	(358, 35, 17, 34)	18	258	14	256
WhiteGeMSS256	(364, 29, 513, 31)	14	263	10	263
CyanGeMSS256	(364, 32, 129, 31)	16	263	12	263
MagentaGeMSS256	(366, 33, 17, 33)	19	263	15	267