On the Effect of Projection on Rank Attacks in Multivariate Cryptography

Morten Øygarden, Daniel Smith–Tone and Javier Verbel

July 2021

Introduction

The *Big–Field Schemes* form a class of multivariate signature and encryption schemes. The most prominent example is the HFEv- signature scheme, which G*e*MSS is based on.

In late 2020, Tao, Petzoldt and Ding proposed a new rank attack, which breaks the current parameters of HFEv- (and G*e*MSS).

There are other combinations of central maps and modifiers among the Big–Field Schemes. How does this new attack affect them?

In particular, we will focus on pHFEv- and PFLASH.

Multivariate Signature Schemes

- **Public Key:** system of n quadratic polynomial equations in $\mathbb{F}_q[x_1, \dots, x_n]$.

- **Signing**: For a document $(d_1, \dots, d_n)$, solve the system

$$\begin{array}{rcl} p_1(x_1, \dots, x_n) & = & d_1 \\ \dots & & \\ p_d(x_1, \dots, x_n) & = & d_n \end{array}$$

  to recover a valid signature $(c_1, \dots, c_n)$.

- **Verification**: evaluate the polynomials $p_1(x_1, \dots, x_n), \dots, p_n(x_1, \dots, x_n)$ on the signature $(c_1, \dots, c_n)$ and verify that it equals $(d_1, \dots, d_n)$.

The HFE- Signature Scheme

Let $\mathbf{S} \in \mathbb{F}_q^{n \times n}$ and $\mathbf{T} \in \mathbb{F}_q^{n \times (n-a)}$ be secret matrices of maximal rank.
$\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ an isomorphism.

$$\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[rr, "f(X)"] & & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^n \arrow[r, "\mathbf{S}"] \arrow[rrrr, dashed, bend right, "p_1, \ldots, p_{n-a} \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]"'] & \mathbb{F}_q^n \arrow[u, "\phi"] & & \mathbb{F}_q^n \arrow[r, "\mathbf{T}"] & \mathbb{F}_q^{(n-a)}
\end{tikzcd}$$

The HFE- Signature Scheme

Let $\mathbf{S} \in \mathbb{F}_q^{n\times n}$ and $\mathbf{T} \in \mathbb{F}_q^{n\times(n-a)}$ be secret matrices of maximal rank.
$\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ an isomorphism.

$$\begin{tikzcd}
& \mathbb{F}_{q^n} \arrow[r, "\color{blue}{f(X)}"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^n \arrow[r, "\mathbf{S}"] \arrow[rrr, dashed, "p_1,\dots,p_{n-a} \in \mathbb{F}_q[x_1,x_2,\dots,x_n]"'] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "\mathbf{T}"] & \mathbb{F}_q^{(n-a)}
\end{tikzcd}$$

$$\color{blue}{f(X)} \color{black} = f_{hfe}(X) = \sum_{\substack{i,j\in\mathbb{N} \\ q^i+q^j\le D}} \alpha_{i,j} X^{q^i+q^j} + \sum_{\substack{i\in\mathbb{N} \\ q^i\le D}} \beta_i X^{q^i} + \gamma,$$

where $\alpha_{i,j}, \beta_i, \gamma \in \mathbb{F}_{q^n}[X]$. D is (relatively) small for signing to be efficient.

The MinRank Problem

MinRank Problem

For a target rank r, and k matrices $M_i \in \mathbb{F}_q^{m \times n}$, find a nontrivial set of constants $(u_0 \ldots, u_{k-1}) \in \mathbb{F}_q^k$ such that

$$\text{Rank}\left(\sum_{i=0}^{k-1} k_i M_i\right) \leq r.$$

The problem is NP–complete in general, but can be solved in practice for small r.

Solving a certain instance of the MinRank problem is typically the hardest step in a rank attack.

Polynomials and Matrices

Any (homogeneous) quadratic polynomial can be written using a symmetric matrix.

If $\mathrm{Char}(\mathbb{F}_q) > 2$, then this is the $(n \times n)$ matrix $\mathbf{P}_i$ such that

$$p_i(x_1, \ldots, x_n) = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \mathbf{P}_i \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Polynomials and Matrices

Any (homogeneous) quadratic polynomial can be written using a symmetric matrix.

If $\mathrm{Char}(\mathbb{F}_q) > 2$, then this is the $(n \times n)$ matrix $\mathbf{P}_i$ such that

$$p_i(x_1, \ldots, x_n) = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \mathbf{P}_i \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Over the ring $\mathbb{F}_{q^n}[X]$, we use:

$$f^{q^i}(X) = \begin{bmatrix} X & X^q & \ldots & X^{q^{n-1}} \end{bmatrix} \mathbf{F}^{*i} \begin{bmatrix} X \\ \vdots \\ X^{q^{n-1}} \end{bmatrix}.$$

Bettale–Faugère–Perret (2013)

There is an invertible matrix $\mathbf{M} \in \mathbb{F}_{q^n}^{n\times n}$, such that the public key can be written as:

$$(\mathbf{P}_1|\cdots|\mathbf{P}_{n-a}) = \left(\mathbf{SMF}^{*0}(\mathbf{SM})^\top|\cdots|\mathbf{SMF}^{*(n-1)}(\mathbf{SM})^\top\right)\left(\mathbf{M}^{-1}\mathbf{T}\otimes\mathbf{I}_n\right).$$

Bettale–Faugère–Perret (2013)

There is an invertible matrix $\mathbf{M} \in \mathbb{F}_{q^n}^{n \times n}$, such that the public key can be written as:

$$(\mathbf{P}_1 | \cdots | \mathbf{P}_{n-a}) = \left(\mathbf{SMF}^{*0} (\mathbf{SM})^\top | \cdots | \mathbf{SMF}^{*(n-1)} (\mathbf{SM})^\top \right) \left(\mathbf{M}^{-1} \mathbf{T} \otimes \mathbf{I}_n \right).$$

Tao–Petzoldt–Ding suggest to solve a MinRank problem for the indeterminate vector $\mathbf{u} = (u_0, \ldots, u_{n-1})$ in:

$$\mathbf{uP}^* := \begin{bmatrix} \mathbf{uP}_1 \\ \vdots \\ \mathbf{uP}_{n-a} \end{bmatrix} \in \mathbb{F}_{q^n}^{(n-a) \times n}$$

Bettale–Faugère–Perret (2013)

There is an invertible matrix $\mathbf{M} \in \mathbb{F}_{q^n}^{n\times n}$, such that the public key can be written as:

$$(\mathbf{P}_1|\cdots|\mathbf{P}_{n-a}) = \left(\mathbf{SMF}^{*0}(\mathbf{SM})^\top|\cdots|\mathbf{SMF}^{*(n-1)}(\mathbf{SM})^\top\right)\left(\mathbf{M}^{-1}\mathbf{T}\otimes\mathbf{I}_n\right).$$

Tao–Petzoldt–Ding suggest to solve a MinRank problem for the indeterminate vector $\mathbf{u} = (u_0, \ldots, u_{n-1})$ in:

$$\mathbf{uP}^* := \begin{bmatrix} \mathbf{uP}_1 \\ \vdots \\ \mathbf{uP}_{n-a} \end{bmatrix} \in \mathbb{F}_{q^n}^{(n-a)\times n}$$

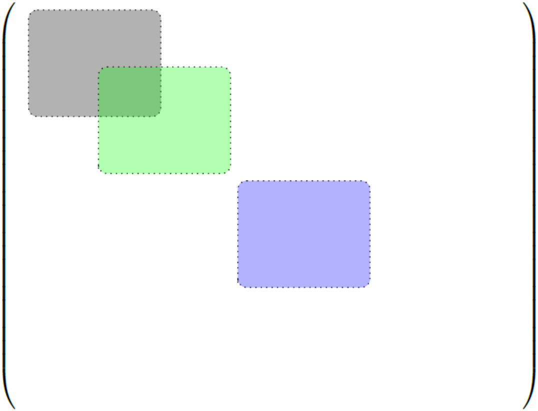
To see why this works, let $\mathbf{v} = (1, 0, \ldots, 0)$, and inspect:

$$\mathbf{vF}^* := \begin{bmatrix} \mathbf{vF}^{*0} \\ \vdots \\ \mathbf{vF}^{*n-1} \end{bmatrix}$$

Sketch of $\mathbf{F}^{*0}$ ($d = \lceil log_q D \rceil$)

$$\begin{pmatrix} \boxed{\begin{matrix} * & * \\ \\ * & * \end{matrix}} & \begin{matrix} 0 & 0 & \cdots \\ \\ \vdots & \vdots & \ddots \end{matrix} & & \\ & & & \\ & & & \\ & & & \end{pmatrix}$$

Three Superimposed $\mathbf{F}^{*i}$ Matrices



Attack Against HFE-

At most $d = \log_q D$ of the $\mathbf{F}^{*i}$ matrices have a nonzero first row.

$\Rightarrow$ There is a nonzero vector $\mathbf{u} \in \mathbb{F}_{q^n}^n$ such that

$$\mathbf{uP}^* := \begin{bmatrix} \mathbf{uP}_1 \\ \vdots \\ \mathbf{uP}_{n-a} \end{bmatrix} \in \mathbb{F}_{q^n}^{(n-a)\times n}$$

has rank at most d. $\mathbf{u}$ can be found by solving a MinRank problem.

This observation relies on the input matrix, $\mathbf{S}$, being invertible. What happens if this is not the case?

pHFE- and PFLASH

Let $\mathbf{S} \in \mathbb{F}_q^{(n-p)\times n}$ and $\mathbf{T} \in \mathbb{F}_q^{n\times(n-a)}$ be secret matrices of maximal rank.
$\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ an isomorphism.

$$\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[r, "{\color{blue} f(X)}"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^{(n-p)} \arrow[r, "\mathbf{S}"] \arrow[rrr, dashed, bend right, "{p_1, \ldots, p_{n-a} \in \mathbb{F}_q[x_1, x_2, \ldots, x_{n-p}]}"'] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "\mathbf{T}"] & \mathbb{F}_q^{(n-a)}
\end{tikzcd}$$

pHFE- and PFLASH

Let $\mathbf{S} \in \mathbb{F}_q^{(n-p)\times n}$ and $\mathbf{T} \in \mathbb{F}_q^{n\times(n-a)}$ be secret matrices of maximal rank.
$\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ an isomorphism.

$$
\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[r, "{\color{blue}f(X)}"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^{(n-p)} \arrow[r, "\mathbf{S}"] \arrow[rrr, dashed, "{p_1, \ldots, p_{n-a} \in \mathbb{F}_q[x_1, x_2, \ldots, x_{n-p}]}"'] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "\mathbf{T}"] & \mathbb{F}_q^{(n-a)}
\end{tikzcd}
$$

$$
\textbf{pHFE-:}\ {\color{blue}f(X)} = f_{hfe}(X) = \sum_{\substack{i,j\in\mathbb{N}\\ q^i+q^j\leq D}} \alpha_{i,j} X^{q^i+q^j} + \sum_{\substack{i\in\mathbb{N}\\ q^i\leq D}} \beta_i X^{q^i} + \gamma
$$

pHFE- and PFLASH

Let $\mathbf{S} \in \mathbb{F}_q^{(n-p)\times n}$ and $\mathbf{T} \in \mathbb{F}_q^{n\times(n-a)}$ be secret matrices of maximal rank.
$\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ an isomorphism.

$$\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[r, "f(X)"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^{(n-p)} \arrow[r, "\mathbf{S}"] \arrow[rrr, dashed, bend right, "{p_1, \ldots, p_{n-a} \in \mathbb{F}_q[x_1, x_2, \ldots, x_{n-p}]}"'] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "\mathbf{T}"] & \mathbb{F}_q^{(n-a)}
\end{tikzcd}$$

$$\textbf{pHFE-:}\ f(X) = f_{hfe}(X) = \sum_{\substack{i,j\in\mathbb{N} \\ q^i+q^j \le D}} \alpha_{i,j} X^{q^i+q^j} + \sum_{\substack{i\in\mathbb{N} \\ q^i \le D}} \beta_i X^{q^i} + \gamma$$

$$\textbf{PFLASH:}\ f(X) = f_{C^*}(X) = X^{q^\theta+1}$$

pHFE- and PFLASH

Let $\mathbf{S} \in \mathbb{F}_q^{(n-p)\times n}$ and $\mathbf{T} \in \mathbb{F}_q^{n\times(n-a)}$ be secret matrices of maximal rank.
$\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ an isomorphism.

$$
\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[r, "{\color{blue}f(X)}"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^{(n-p)} \arrow[r, "\mathbf{S}"] \arrow[rrr, dashed, bend right, "{p_1, \dots, p_{n-a} \in \mathbb{F}_q[x_1, x_2, \dots, x_{n-p}]}"'] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "\mathbf{T}"] & \mathbb{F}_q^{(n-a)}
\end{tikzcd}
$$

$$\textbf{pHFE-:}\ {\color{blue}f(X)} = f_{hfe}(X) = \sum_{\substack{i,j\in\mathbb{N} \\ q^i+q^j \le D}} \alpha_{i,j} X^{q^i+q^j} + \sum_{\substack{i\in\mathbb{N} \\ q^i \le D}} \beta_i X^{q^i} + \gamma$$

$$\textbf{PFLASH:}\ {\color{blue}f(X)} = f_{C^*}(X) = X^{q^\theta+1}$$

For signature schemes, projection typically adds a factor q^p to signing time.

Sketch: Bounding the Degree for pHFE-

Lemma

A linear map $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$, where $|\mathrm{Ker}(S)| = q^p$, can be written as

$$S = \phi^{-1} \circ \pi \circ \phi \circ S',$$

where S' is an invertible linear map, and $\pi \in \mathbb{F}_{q^n}[X]$ a q–linear polynomial of degree q^p.

Sketch: Bounding the Degree for pHFE-

Lemma

A linear map $S : \mathbb{F}_q^n \to \mathbb{F}_q^n$, where $|\mathrm{Ker}(S)| = q^p$, can be written as

$$S = \phi^{-1} \circ \pi \circ \phi \circ S',$$

where S' is an invertible linear map, and $\pi \in \mathbb{F}_{q^n}[X]$ a q–linear polynomial of degree q^p.

The public key can then be written as:

$$T \circ \phi^{-1} \circ f \circ \phi \circ S = T \circ \phi^{-1} \circ f \circ \pi \circ \phi \circ S'.$$

How does the “new” central map $f \circ \pi$ behave?

p $= 0$, $d \times d$–Block. $p > 0$, $(d + p) \times (d + p)$–Block

Sketch: Bounding the Degree for pHFE-

Proposition

Let $(\mathbf{P}_1, \ldots, \mathbf{P}_{n-a})$ be the public key of an instance of pHFEv-. Then there is a nonzero tuple $\mathbf{u} \in \mathbb{F}_{q^n}^{n-p}$ such that $\mathbf{uP}^*$ has rank at most $p + d$.

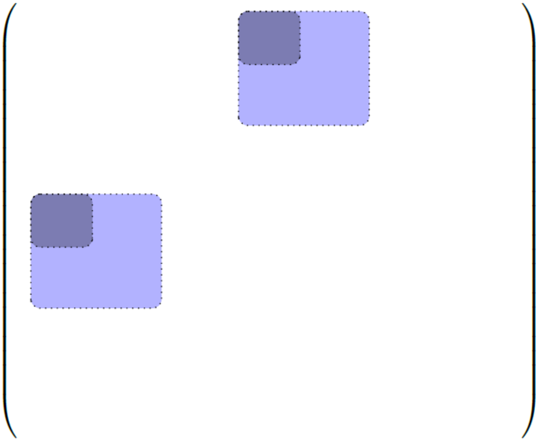
Sketch: Bounding the Degree for pHFE-

Proposition

Let $(\mathbf{P}_1, \ldots, \mathbf{P}_{n-a})$ be the public key of an instance of pHFEv-. Then there is a nonzero tuple $\mathbf{u} \in \mathbb{F}_{q^n}^{n-p}$ such that $\mathbf{u}\mathbf{P}^*$ has rank at most $p + d$.

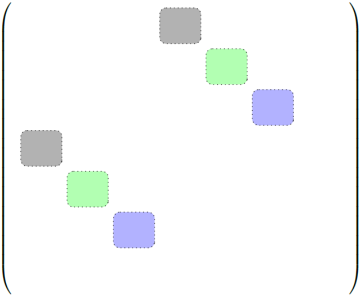
We can use a similar line of argument for the C^* central map (PFLASH), but the resulting bound will not be tight.

$$\begin{pmatrix} & \boxed{1} & \\ \boxed{1} & & \\ & & \end{pmatrix}$$



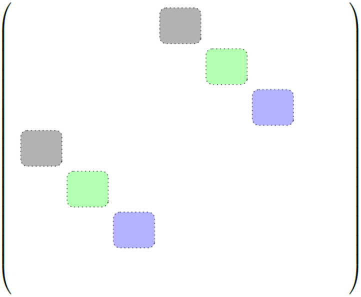
Sketch for $p = 1$

Consider a vector of weight 2: $\mathbf{v} = (1, 0, \ldots, 0, 1, 0, \ldots, 0)$, and multiply it with the matrices:



Sketch for $p = 1$

Consider a vector of weight 2: $\mathbf{v} = (1, 0, \ldots, 0, 1, 0, \ldots, 0)$, and multiply it with the matrices:



The resulting matrix $\mathbf{vF}^*_{C^*}$ will have weight 4.

Small Example: $n = 7$, $\theta = 2$, $p = 1$

We choose the vector $\mathbf{v} = (1, 0, 1, 0, 0, 0, 0)$. The first matrix of the central map is:

$$\mathbf{F}^{*0}_{C^*} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Small Example: $n = 7$, $\theta = 2$, $p = 1$

We choose the vector $\mathbf{v} = (1, 0, 1, 0, 0, 0, 0)$. The first matrix of the central map is:

$$\mathbf{F}^{*0}_{C^*} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The matrix constructed from the various vector–matrix products will be

$$\mathbf{v}\mathbf{F}^{*}_{C^*} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Sketch: Bounding the Degree for PFLASH

Step I: Construct vectors of weight $1 + p$ that minimizes the rank (depends on θ).

Sketch: Bounding the Degree for PFLASH

Step I: Construct vectors of weight $1 + p$ that minimizes the rank (depends on θ).

Step II: Show that this vector lies in the image of **SM**.

Sketch: Bounding the Degree for PFLASH

Proposition

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

Sketch: Bounding the Degree for PFLASH

Proposition

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

We also discuss the number solutions $\mathbf{u}$ for the MinRank problem, and identify weak choices of θ. See the paper for more details.

Experiments: pHFE- (Top) and PFLASH (Bottom)

q	n	a	p	D	Upper Bound	Rank of 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 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

Effects on variants of HFE

For the new rank attack, including a projection p is comparable to increasing the HFE–degree to $q^p D$.

Effects on variants of HFE

For the new rank attack, including a projection p is comparable to increasing the HFE–degree to $q^p D$.

In terms of signing time, projection is more efficient. Over $\mathbb{F}_2$, it is faster by a factor

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

Effects on variants of HFE

For the new rank attack, including a projection p is comparable to increasing the HFE–degree to $q^p D$.

In terms of signing time, projection is more efficient. Over $\mathbb{F}_2$, it is faster by a factor

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

Scheme	p_1 [a]	p_2 [b]
GeMSS128	2	0
RedGeMSS128	6	4
GeMSS256	14	10
RedGeMSS256	18	14

[a] Using $\omega = 2.37$

[b] Using $\omega = 2.81$

Effects on variants of C^* (PFLASH)

The suggested projection used in PFLASH ($p = 1$) is not sufficient to achieve security.

More work needed to find good parameters for PFLASH.

Conclusions

- The new rank attack by Tao, Petzoldt and Ding can also be used against PFLASH.
- Adding (or increasing the size of the) projection can be used to counter this attack.
- Projection increases the singing time for signature schemes (often cheap for encryption schemes).