An analysis of Coggia-Couvreur Attack on Loidreau’s Rank-metric public-key encryption scheme in the general case
Pierre Loidreau, Ba-Duc Pham

To cite this version:
Pierre Loidreau, Ba-Duc Pham. An analysis of Coggia-Couvreur Attack on Loidreau’s Rank-metric public-key encryption scheme in the general case. 2022. hal-03514106

HAL Id: hal-03514106
https://hal.science/hal-03514106
Preprint submitted on 20 Jan 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
An analysis of Coggia-Couvreur Attack on Loidreau’s Rank-metric public-key encryption scheme in the general case

Pierre Loidreau\textsuperscript{1} and Ba-Duc Pham\textsuperscript{2}

\textsuperscript{1} Univ Rennes, DGA MI, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
pierre.loidreau@univ-rennes1.fr
\textsuperscript{2} Univ Rennes, IRMAR - UMR 6625, F-35000 Rennes, France
ba-duc.pham@univ-rennes1.fr

Abstract. In this paper we show that in the case where the public-key can be distinguished from a random code in Loidreau’s encryption scheme, then Coggia-Couvreur attack can be extended to recover an equivalent secret key. This attack can be conducted in polynomial-time if the masking vector space has dimension 3, thus recovering the results of Ghatak.

Keywords: Rank metric codes, Gabidulin codes, code based cryptography, cryptanalysis

Introduction

Since the use of $\mathbb{F}_q^m$-linear rank metric permits to design a short public key encryption scheme, one of the directions of code based cryptography consists in instantiating McEliece encryption scheme \cite{1} with codes in rank metric, \cite{2,3}.

Because of the structure of Gabidulin codes, any cryptosystem instantiated with codes containing Gabidulin codes not sufficiently scrambled was attacked \cite{1}. In 2017, Loidreau proposed a scheme based on Gabidulin codes masked with a small dimensional vector space \cite{5}. If the dimension of the vector space is too small, then there exists a very simple polynomial-time distinguishing algorithm.

The question was to know if distinguishing is enough to break. Coggia and Couvreur \cite{6} showed that in the case where the dimension of the masking space is 2, a decryption procedure can be recovered in polynomial-time. More recently, Ghatak \cite{7} claimed that this approach could be extended to a masking space of dimension 3.

In this work we show that this can be extended to any dimension. The attack is not necessary polynomial, but we include the previous results. Moreover we are able to prove rigorously under some assumptions the efficiency of the attack.
Contribution

1. Completing the key-recovery attack for any \( \lambda \)
2. In \([7]\), the author uses one reduced polynomial to determine \( \gamma = \{\gamma_1, \gamma_2\} \) where \( \gamma \) specifies the secret subspace but their assumption is not clear in practice when we implement in MAGMA. In this paper, the use of system of polynomial equation gives a proof for the equivalent between the set of roots and the orbit of one root under the action of \( \text{PGL}(3, \mathbb{F}_q) \). It completes the polynomial time key recovery attack.

Organization of the article The first section outlines Loidreau’s scheme. In the beginning of the next section, we formulate the distinguisher for any dimension of the secret subspace. Afterwards, we describe the attack for any \( \lambda \) in 4 steps. In the end of this section, we analyse the complexity of the attack in case \( \lambda = 3 \). We conclude with a discussion on the results and future works.

1 The encryption scheme

1.1 Generalities

Let \( G \) a random generator matrix of a Gabidulin code \( G_k(g) \). Fix an integer \( \lambda \leq m \) and an \( \mathbb{F}_q \)-vector subspace \( V \) of \( \mathbb{F}_q^m \) of dimension \( \lambda \). Let \( P \in \text{GL}(n, \mathbb{F}_q^m) \) whose entries are all in \( V \). Then, let

\[
G_{\text{pub}} = GP^{-1}
\]

- KeyGen: Public key \((G_{\text{pub}}, t)\) where \( t = \lfloor \frac{n-k}{2\lambda} \rfloor \)
- Secret key \((g, P)\)
- Encryption: Given a plaintext \( m \in \mathbb{F}_q^k \), choose \( e \in \mathbb{F}_q^m \) of rank weight \( t \). The ciphertext is:

\[
c = mG_{\text{pub}} + e
\]

- Decryption:
  - Compute \( cP = mG + eP \).
  - Decode in \( G_k(g) \) and \( \text{rk}(eP) \leq t\lambda \leq \frac{n-k}{2} \)

Let us denote by \( C_{\text{pub}} \) the code generated by \( G_{\text{pub}} \) and by \( C_{\text{pub}}^\perp \), the dual code. Let \( H_{\text{pub}} \) be a generator matrix of \( C_{\text{pub}}^\perp \). It is immediate that

\[
H_{\text{pub}} = H_{\text{sec}}P^T
\]

where \( H_{\text{sec}} \) is a parity-check matrix of \( G_k(g) \).
1.2 Goal of a reconstructing attack and solution set

Our main goal is to design a reconstructing attack from the knowledge of $C_{\perp \text{pub}}$ and under some particular sets of parameters.

W.l.o.g. one can suppose that $1 \in V$. Suppose that $V = \langle 1, \beta_1, \ldots, \beta_{\lambda-1} \rangle_{F_q}$ for some $\{\beta_i\}_{i=1}^{\lambda-1} \in F_{q^m} \setminus F_q$. Therefore, $P^T$ can be decomposed into

$$P^T = P_0 + \sum_{i=1}^{\lambda-1} \beta_i P_i$$

where $P_i$ are $n \times n$ matrices with entries in $F_q$ not necessarily invertible.

Let $C_{\perp \text{sec}}^\perp$ the dual code of $G_k(g)$. Thus, $C_{\perp \text{sec}}^\perp = G_n - k(a)$ for some $a \in F_{nq^m}$ with $\text{rk}(a) = n$. We define

$$h_0 = aP_0, h_1 = aP_1, \ldots, h_{\lambda-1} = aP_{\lambda-1}$$

Lemma 1. The code $C_{\perp \text{pub}}^\perp$ is spanned by $h_0^{[i]} + \sum_{j=1}^{\lambda-1} \beta_j h_j^{[i]}$ for $i = 0, \ldots, n - k - 1$

Proof. For any $c \in C_{\perp \text{pub}}^\perp$, there exists $P \in F_{q^m}[X; \theta]$ of degree smaller than $n - k$ such that

$$c = P(\alpha)P^T = P(\alpha)P_0 + \sum_{i=1}^{\lambda-1} \beta_i P(\alpha)P_i = P(h_0) + \sum_{i=1}^{\lambda-1} \beta_i P(h_i)$$

Let us define the so-called solution set of the encryption scheme

Definition 1 (Solution set). The set $S$ of all $(h, \vec{\beta}) \in (F_{nq^m})^\lambda \times F_{q^m}^{\lambda-1}$ such that

$$C_{\perp \text{pub}}^\perp = \left\{ h_0^{[i]} + \sum_{j=1}^{\lambda-1} \beta_j h_j^{[i]}, \ i = 0, \ldots, n - k - 1 \right\}$$

where $\forall j = 0, \ldots, \lambda, h_j$ has rank $n$ and $\langle 1, \beta_1, \ldots, \beta_{\lambda-1} \rangle_{F_q}$ has dimension $\lambda$ is called solution set of the encryption scheme.

It is obvious that finding an element of the solution set $S$ implies the ability to design a polynomial-time decryption algorithm. What we call a reconstructing attack corresponds to finding an element in $S$. The solution set $S$ has the following properties.

Proposition 1. Let $(h, \vec{\beta}) \in (F_{nq^m})^\lambda \times F_{q^m}^{\lambda-1}$. Let $A = (a_{ij})_{i,j=0}^{\lambda-1} \in GL_{\lambda}(F_q)$. Let us define the following group action on $(F_{nq^m})^\lambda \times F_{q^m}^{\lambda-1}$ by $A \cdot (h, \vec{\beta}) = (h', \vec{\beta}')$
where

\[
\begin{align*}
    h_j &= \frac{a_{j,0}h_0' + \sum_{i=1}^{\lambda-1} a_{j,i}h_i'}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i}, \quad j = 0, \ldots, \lambda - 1 \\
    \beta_j' &= \frac{a_{j,0} + \sum_{i=1}^{\lambda-1} a_{i,j} \beta_i}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i}, \quad j = 1, \ldots, \lambda - 1
\end{align*}
\]

1. Then if \((h, \bar{\beta}) \in S\) we have \(A \cdot (h, \bar{\beta}) \in S\).
2. Moreover let \(\bar{A} = \{B \in GL_\lambda(F_q) | \exists c \in F_q^\times, B = cA\}\). Then, for any \(B \in \bar{A}\), and for any \((h, \bar{\beta}) \in (F_q^n)^\lambda \times F_q^{\lambda-1}\) we have

\[
    A \cdot (h, \bar{\beta}) = B \cdot (h, \bar{\beta})
\]

Proof. Let \((h, \bar{\beta}) \in S\). Since from the definition of \(S\) the elements \(1, \beta_1, \ldots, \beta_{\lambda-1}\) are \(F_q\)-linearly independent, and since \(A\) is non-singular, \((a_{0,0}, \ldots, a_{0,\lambda-1}) \neq 0\) this implies that \(a_{0,0} + \sum_{i=1}^{\lambda-1} a_{0,i} \beta_i \neq 0\). Therefore, the elements \(\beta_1', \ldots, \beta_{\lambda-1}'\) are well defined and for all \(0 \leq \ell \leq n - k - 1\),

\[
\begin{align*}
    h_0^{[\ell]} + \sum_{j=1}^{\lambda-1} \beta_j' h_j^{[\ell]} \\
    &= \frac{1}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i} \left( a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i \right) h_0^{[\ell]} + \sum_{j=1}^{\lambda-1} \left( a_{0,j} + \sum_{i=1}^{\lambda-1} a_{i,j} \beta_i \right) h_j^{[\ell]} \\
    &= \frac{1}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i} \left( a_{0,0}h_0' + \sum_{j=1}^{\lambda-1} a_{0,j} h_j^{[\ell]} \right) + \sum_{i=1}^{\lambda-1} \beta_i \left( a_{i,0}h_0' + \sum_{j=1}^{\lambda-1} a_{i,j} h_j^{[\ell]} \right) \\
    &= \left( a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i \right)^{\ell-1} \left( h_0^{[\ell]} + \sum_{i=1}^{\lambda-1} \beta_i h_i^{[\ell]} \right)
\end{align*}
\]

Therefore

\[
    C_{\text{pub}} \stackrel{def}{=} \left( h_0^{[\ell]} + \sum_{i=1}^{\lambda-1} \beta_i h_i^{[\ell]}, \ 0 \leq \ell \leq n - k - 1 \right) = \left( h_0^{[\ell]} + \sum_{i=1}^{\lambda-1} \beta_i h_i^{[\ell]}, \ 0 \leq \ell \leq n - k - 1 \right)
\]

Thus, \((h', \bar{\beta}') \in S\).

For the second point of the proposition: Let \(B \in \bar{A}\). It means that there exists \(c \in F_q^\times\) such that \(BA^{-1} = cI\) or equivalently \(B = cA\).
Let \((h''', \vec{\beta}''') \equiv B \cdot (h', \vec{\beta}')\), where \((h', \vec{\beta}') = A \cdot (h, \vec{\beta}) \in (\mathbb{F}_q^n)^\lambda \times \mathbb{F}_q^\lambda-1\). It means that

\[
\begin{cases}
    h'_j = \frac{b_{j,0}h''_0 + \sum_{i=1}^{\lambda-1} b_{j,i}h''_i}{b_{0,0} + \sum_{i=1}^{\lambda-1} b_{i,0} \beta''_i}, & j = 0, \ldots, \lambda - 1 \\
    \beta''_i = \frac{b_{0,i} + \sum_{j=1}^{\lambda-1} b_{i,j} \beta''_j}{b_{0,0} + \sum_{j=1}^{\lambda-1} b_{0,j} \beta''_j}, & j = 1, \ldots, \lambda - 1 
\end{cases}
\]

It is obvious that the actions of 2 matrix \(A, B\) give us same image, which is \((h''', \vec{\beta}''') = (h', \vec{\beta}').\)

\[\square\]

## 2 Attacks on the system

Now the section is organised as follows: In a first part we make a brief summary of the attack. Since it is technical, this section highlights the different principles. In first subsection, we introduce the distinguisher between the dual of the public code and the random codes. Afterwards, we make some assumptions in the beginning and under these assumptions, we exploit the attack based on the distinguisher introduced in 2.1. We also consider the special case of \(\lambda = 3\) and analyze its complexity in Section 2.3.

We will also need to introduce a special setting to simplify the technicalities of the proofs. For any \((h, \vec{\beta}) \in S\), we denote

\[y_{(h, \vec{\beta})}^{[u,j]} = h^{[u]}_0 + \sum_{i=1}^{\lambda-1} \beta_i^{[u]} h^{[u]}_i\]

for any integers \((u, j)\). For a given \((h, \vec{\beta})\), to simplify, we denote it by \(y^{[u,j]}\). Moreover, we can denote \(y^{[M]} = \{y^{[u,j]}\}_{(u,j) \in M \subset \mathbb{Z} \times \mathbb{Z}}\). The codes that we will consider will be generated by the \(y^{[u,j]}\), where \((u, j) \in \mathbb{Z} \times \mathbb{Z}\). Let \(I \subset \mathbb{Z} \times \mathbb{Z}\). We denote by

\[C_{I} \equiv \{y^{[u,j]} \mid (u, j) \in I\},\]

if \(I\) is non-empty and \(C_{\emptyset} \equiv \{0\}\). From the expression of \(C_{\text{pub}}^\perp\) in Definition 1, we have

\[C_{\text{pub}}^\perp = C_{(0) \times [0, \ldots, n-k-1]}\]

Now we introduce a very fundamental theorem which will support all of our future proofs
Theorem 1 (CodeSet theorem). We have
\[ \forall I, J \subset \mathbb{Z} \times \mathbb{Z}, \begin{cases} C_{I \cup J} = C_I + C_J \\ C_{I \cap J} \subset C_I \cap C_J \end{cases} \]
If moreover \( M \subset \mathbb{Z} \times \mathbb{Z} \), where \( y^{[u,j]} \), \((u,j) \in M\) are \( \mathbb{F}_q^m \) linearly independent, then
- for all \( I \subset M \), \( \dim(C_I) = |I| \)
- \( \forall I, J \subset M, C_I \cap C_J = C_{I \cap J} \)
- \( \forall I, J \subset M, C_{I \cup J} = C_I \oplus C_J \), where \( \cup \) means that the sets do not intersect.

Proof. The code generating set for \( C_I + C_J \) is the union of generating sets for \( C_I \) and \( C_J \), since \( y^{[u,j]} \) and \( y^{[j]} \) are generating sets respectively for \( C_I \) and \( C_J \) then \( y^{[u,j]} \) is a generating set for \( C_I + C_J \). Hence \( C_{I \cup J} = C_I + C_J \). Now the generating set \( y^{[I \cap J]} \) of \( C_{I \cap J} \) is included in the generating set of \( C_I \) and of \( C_J \). Therefore \( C_{I \cap J} \subset C_I \cap C_J \).

Let us consider now \( M \) such that \( y^{[M]} \) is formed with linearly independent vectors. It is immediate that for any \( I \subset M \), a basis of \( C_I \) is \( y^{[I]} \), therefore the dimension of \( C_I \) is exactly equal to \( |I| \). Let \( c \in C_I \cap C_J \). We have
\[
c = \sum_{(u,j) \in I} c_{u,j} y^{[u,j]} = \sum_{(u,j) \in I \setminus J} c_{u,j} y^{[u,j]} + \sum_{(u,j) \in I \cap J} c_{u,j} y^{[u,j]}\]
and similarly
\[
c = \sum_{(u,j) \in J} c'_{u,j} y^{[u,j]} = \sum_{(u,j) \in J \setminus I} c'_{u,j} y^{[u,j]} + \sum_{(u,j) \in I \cap J} c'_{u,j} y^{[u,j]}\]
Since by hypotheses on \( M \), the \( y^{[M]} \) are linearly independent, this implies the equality of the coefficients on this bases and thus that \( c_{u,j} = 0 \), for \( (u,j) \in I \setminus J \). Therefore, \( c \in C_{I \cap J} \).

The last item comes from the fact that is \( I \) and \( J \) do not intersect then \( I \cap J = \emptyset \), thus \( C_I \cap C_J = \{0\} \).

2.1 A distinguishing attack in the general case

We show that if \( n, k, \lambda \) satisfy \( k > \frac{(\lambda-1)n}{\lambda} + 1 \), then one can distinguish the public-code from a random code in polynomial time. First we prove the following theorem.

Theorem 2. \( \dim_{\mathbb{F}_q^m} \left( C_{pub}^{\perp} + C_{pub}^{\perp}[1] + \cdots + C_{pub}^{\perp}[\lambda] \right) \leq \lambda(n - k) + \lambda \)
Proof. Let $\mathcal{S}_0 \overset{\text{def}}{=} \sum_{i=0}^{\lambda-1} C_{\text{pub}}^{\perp}[i]$. We want to show that $\dim\left(\mathcal{S}_0 + C_{\text{pub}}^{\perp}[\lambda]\right) \leq \lambda(n-k) + \lambda$. For any $(\mathbf{h}, \beta) \in \mathcal{S}$ from the expression of $C_{\text{pub}}^{\perp}$ under the form (2) and from the CodeSet theorem we obtain

$$S_0 = C_{S_0}, \quad \text{where } S_0 = \bigcup_{u=0}^{\lambda-1} \{u\} \times [u, n-k+u-1]$$

and

$$C_{\text{pub}}^{\perp}[\lambda] = C_{(\lambda) \times [\lambda, n-k+\lambda-1]}$$

Let

$$I = \bigcup_{u=0}^{\lambda-1} \{u\} \times [\lambda-1, n-k-1] = [0, \lambda-1] \times [\lambda-1, n-k-1]$$

We have clearly $I \subset S_0$, implying $C_I \subset S_0$.

By the hypotheses on $\mathcal{S}$ the $(1, \beta_1, \ldots, \beta_{\lambda-1})$ are linearly independent over $\mathbb{F}_q$. Thus,

$$\det \begin{bmatrix} 1 & \beta_1 & \ldots & \beta_{\lambda-1} \\ 1 & \beta_1 & \ldots & \beta_{\lambda-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_1^{[\lambda-1]} & \ldots & \beta_{\lambda-1}^{[\lambda-1]} \end{bmatrix} \neq 0,$$

it implies that for any $j \in \lambda-1, \ldots, n-k-1$, $C_{[0, \lambda-1] \times \{j\}} = \langle h_i^{[j]} \rangle, \ 0 \leq i \leq \lambda-1$. Hence,

$$C_I = \left( h_i^{[j]}, \ 0 \leq i \leq \lambda-1 \right)$$

In particular from the structure of $y^{[u,j]}$ for any $J \subset \star \times [\lambda-1, n-k-1]$, we have $C_J \subset C_I \subset S_0$.

Thus, $C_{(\lambda) \times [\lambda, n-k-1]} \subset S_0 \cap C_{\text{pub}}^{\perp}[\lambda]$. From its construction, $C_{\text{pub}}^{\perp}[\lambda]$ has dimension $n-k$. The vectors $y^{[\lambda,j]}$, $j \in [\lambda, n-k+\lambda-1]$ are linearly independent and from the CodeSet theorem, $C_{(\lambda) \times [\lambda, n-k-1]}$ has dimension $n-k-\lambda$. Therefore,

$$\dim(S_0 \cap C_{\text{pub}}^{\perp}[\lambda]) \geq n-k-\lambda.$$ Conversely,

$$\dim\left(\mathcal{S}_0 + C_{\text{pub}}^{\perp}[\lambda]\right) = \dim(S_0) + \dim(C_{\text{pub}}^{\perp}[\lambda]) - \dim(S_0 \cap C_{\text{pub}}^{\perp}[\lambda])$$

$$\leq \lambda(n-k) + (n-k) - (n-k-\lambda) = \lambda(n-k) + \lambda$$

Now the distinguishing attack comes from this proposition.
Proposition 2 (\cite{6} Proposition 2). If $C_{\text{rand}}$ is a random code of length $n$ and dimension $k$, then for a non-negative integer $a$ and a positive $\lambda < k$, we have 

$$\mathbb{P} \left( \dim_{F_q^m} \left( C_{\text{rand}} + C_{\text{rand}}^{[1]} + \cdots + C_{\text{rand}}^{[\lambda]} \right) \leq \min(n, (\lambda + 1)k) - a \right) = O(q^{-ma}).$$

Now whenever $k > \frac{(\lambda-1)n}{\lambda} + 1$, the dimension of $C_{\text{rand}} + C_{\text{rand}}^{[1]} + \cdots + C_{\text{rand}}^{[\lambda]}$ is very probably equal to $(\lambda + 1)(n - k)$ whereas the dimension of $C_{\text{pub}}^\perp + C_{\text{pub}}^{[1]} + \cdots + C_{\text{pub}}^{[\lambda]}$ is probably equal to $\lambda(n - k + 1)$ (since $\lambda(n - k + 1) < n$), which is strictly less than $(\lambda + 1)(n - k)$.

2.2 Reconstructing attack

We suppose that the public code has rate larger than $(\lambda - 1)/\lambda$, so that the distinguisher introduced in Section 2.1 works on it.

Although the attack we describe should work heuristically, to have rigorous proofs of work we need the following assumptions, which are not very constraining

(1) There exists an element $(\vec{h}, \vec{\beta}) \in S$ such that $\forall i_1, \ldots, i_\lambda \in \{1, \ldots, n - k - 1\}$ distinct, 

$$\det \begin{bmatrix} 1 & \beta_1^{[i_1]} & \beta_2^{[i_1]} & \cdots & \beta_\lambda^{[i_1]} \\ 1 & \beta_1^{[i_2]} & \beta_2^{[i_2]} & \cdots & \beta_\lambda^{[i_2]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_1^{[i_\lambda]} & \beta_2^{[i_\lambda]} & \cdots & \beta_\lambda^{[i_\lambda]} \end{bmatrix} \neq 0,$$

(2) $\dim_{F_q^m} C_{\text{pub}}^\perp + C_{\text{pub}}^{[1]} + C_{\text{pub}}^{[2]} + \cdots + C_{\text{pub}}^{[\lambda]} = \lambda(n - k) + \lambda$

(3) There is no $\vec{A} \in \text{PGL}(\lambda, F_q^m) \backslash \text{PGL}(\lambda, F_q)$ and $A = (a_{ij})_{i,j=1}^\lambda$ that satisfies 

$$\beta_j = \frac{a_{0,j} + \sum_{i=1}^{\lambda-1} a_{i,j} \beta_i}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i}, \quad \forall j = 1, \ldots, \lambda - 1$$

The first step of the attack is dedicated to finding one dimensional vector-spaces $A_i$ for $i = 1, \ldots, n - k - 1$, such that any element $(\vec{h}, \vec{\beta}) \in S$ satisfies:

$$A_i = \left\langle h_0 + \sum_{j=1}^{\lambda-1} \beta_j^{[-1]} h_j \right\rangle$$

From the $A_i$’s, one obtains a system of $\lambda - 1$ multivariate polynomials which are of degree $q^{\lambda+1} - q^i$ for $i = 1, \ldots, \lambda - 1$ satisfied by all the vectors $\vec{\beta}$ such that $(\vec{h}, \vec{\beta}) \in S$. Under the above assumptions, we can also prove the stabilization of the set of solution $S$ under the action of $\text{PGL}(\lambda, F_q)$ in the end of 3.2.2.

The complexities of the steps (by operations over $F_{q^m}$):
Step 1. It costs $O(n^3 \log q)$ operations for computing $C_{\text{pub}}^{\perp [i]}$ and $O(n^{\omega+1})$ for taking the intersection.

Step 2. The principal complexity of this is finding the roots of the system of polynomials. In case of $\lambda = 3$, it can be done in polynomial time where the complexity is $\tilde{O}(\tilde{d}^2 n \log q)$ for $\tilde{d} = (q^4 - q)(q^4 - q^2)$.

Once such a root is found, the remaining of step 2 needs a finite number of linear systems solving which costs $O(n^\omega)$.

**First step: Recovering one-dimensional vector spaces** We now suppose that the three assumptions in section 1.2 are true we have the following theorem:

**Theorem 3.** Let $d := n - k - \lambda + 1$. Under Assumptions [1] [2] [3] we have the following theorem:

**Algorithm 1:** Recovering 1-dimensional vector spaces

Input: $C_{\text{pub}}^{\perp}, \lambda \leq \frac{n}{n^3 \log q}$

Output: $A_i$ for $i = 0, \ldots, n - k - 1$

1. $S_0 \leftarrow C_{\text{pub}}^{\perp [0]} + C_{\text{pub}}^{\perp [1]} + \cdots + C_{\text{pub}}^{\perp [\lambda - 1]}$

2. $A \leftarrow \left(\cap_{i=0}^{d} S_0^{[i]}\right)$

3. $D_{\lambda - 1} \leftarrow A^{[\lambda - 2]} \cap C_{\text{pub}}^{\perp [\lambda - 1 - d]}$ and $B_0 \leftarrow A + D_{\lambda - 1}^{[1 - \lambda]}$

4. $D_0 \leftarrow B_0 \cap C_{\text{pub}}^{\perp [-1]}$

5. for $\ell \in 1, \ldots, \lambda - 2$ do

6.  $B_\ell \leftarrow A + \sum_{j=0}^{\ell - 1} D_j^{[\ell - j]}$

7.  $D_\ell \leftarrow B_\ell \cap C_{\text{pub}}^{\perp [-1]}$

8.  $H \leftarrow \sum_{j=0}^{\lambda - 1} C_j^{[2 - j - \lambda]}$

9. for $i \in 0, \ldots, n - k - 1$ do

10. Return $A_i \leftarrow H \cap C_{\text{pub}}^{\perp [-1]}

Algorithm [7] returns the 1-dimensional vector spaces

$$A_i = \left( h_0 + \sum_{j=1}^{\lambda - 1} \beta_j^{[2 - j - \lambda]} h_j \right), \quad i = 0, \ldots, n - k - 1$$

for any $(h, \tilde{\beta}) \in S$.

**Proof.** For the proof we will thus make intensive use of the CodeSet theorem. First from assumption (2) and theorem [2] the set

$$M = \bigcup_{u=0}^{\lambda} \{u\} \times [u, n - k + u - 1] = S_0 \cup \{\lambda\} \times [\lambda, n - k + \lambda - 1]$$
with cardinality $\lambda(n-k) + \lambda$, is such that $y^{[M]}$ is formed of linearly independent vectors and $C_M = \sum_{i=0}^{\lambda} C_{pub}^{[i]}$. This point is very important since this is the crucial point of the proof of the theorem.

**Line 1.** From theorem 2 we have

$$S_0 = C_{S_0}, \text{ where } S_0 = \bigcup_{u=0}^{\lambda-1} \{u\} \times [u, n-k + u - 1]$$

We can write $S_0$ under the form

$$S_0 = \left( \bigcup_{u=0}^{\lambda-2} \{u\} \times [u, \lambda - 2] \right) \cup [0, \lambda - 1] \times [\lambda - 1, n-k - 1] \cup \left( \bigcup_{u=0}^{\lambda-1} \{u\} \times [n-k, n-k + u - 1] \right)$$

Let $I_4 = I_3 \cup \{\lambda\} \times [n-k, n-k + \lambda - 1]$. With these notations, we have $S_0 = I_1 \cup I_2 \cup I_3 \cup I_4 = M$. Since their cardinalities satisfy $|I_1| = \frac{\lambda(\lambda-1)}{2}$, $|I_2| = \lambda(n-k - \lambda + 1)$, $|I_3| = \frac{\lambda(\lambda-1)}{2}$ and $|I_4| = \lambda$. From theorem 2 the dimension of $S_0$ and $C_M$ is exactly $\lambda(n-k)$ and $\lambda(n-k) + \lambda$ respectively, and additionally under the CodeSet theorem,

$$S_0 = C_{I_1} \oplus C_{I_2} \oplus C_{I_3}$$

$$C_M = C_{I_1} \oplus C_{I_2} \oplus C_{I_4}$$

The set $I_2$ corresponds to the set denoted by $I$ in the proof of theorem 2. We have

$$C_{I_2} = \left\{ h_i^{[j]} | 0 \leq i \leq \lambda - 1, \lambda - 1 \leq j \leq n-k - 1 \right\}$$

This property gives us the flexibility for the modification of the set $M$ to obtain several sets of indexes $M'$ such that $y^{[M']}$ is formed of linearly independent vectors. It can be done by the replacement of the set $[0, \lambda - 1]$ by the set $A_j$ of $\lambda$ elements corresponding to any $j$. We can see it precisely as the following lemma:

**Lemma 2.** For every set $I'_2 = \bigcup_{j=\lambda-1}^{n-k-1} A_j \times \{j\}$ where $|A_j| = \lambda$, then $M' = I_1 \cup I'_2 \cup I_4$ satisfies

$- C_{M'} = C_{M'}$.

$- y^{[M']}$ is formed of linearly independent vectors.

**Proof.** $C_{I'_2} = \left\{ h_i^{[j]} | 0 \leq i \leq \lambda - 1, \lambda - 1 \leq j \leq n-k - 1 \right\} = C_{I_2}$ (Assumption [1]). Moreover,

$|I'_2| = |I_2| = \lambda(n-k - \lambda + 1)$. Hence $C_{M'} = C_{I_1} \oplus C_{I'_2} \oplus C_{I_4} = C_{M}$ and $y^{[M']}$ is formed of linearly independent vectors.

$\square$
Through this section, to apply the CodeSet theorem, in the beginning of each step, we will define its set of indexes $M'$ such that $y^{[M']}$ are linearly independent vectors and it contains the set of indexes of subspace that we want to compute the intersection. To be convenient, we will use some images where the red dot • are indexes of some transformation of $I_1$, the blue square • are indexes of some transformation of $I_4$, the green $\times$ are indexes of some transformation of $I_2$ and the black diamond • are indexes of $C_{pub}$. On the other hand, the integer points which are inside the blue figures are indexes of linearly independent vectors. The left triangular covers all the points of the set of indexes $I_1$ the right triangular covers all the points of the set of indexes $I_4$ and the rectangular covers all the points of the set of indexes which is flexible modification of $I_2$.

To be convenient, for $I \subset \mathbb{Z} \times \mathbb{Z}$ and $a \in \mathbb{Z}$, we denote 
\[
I + a = \{(u + a, j + a), \ (u, j) \in I\}.
\]
In the figures, we can consider $I + a$ as the translation of $I$ by the vector $(a, a)$. For example, in the figure 1, the set of red points shows $I_1$ in the first image and $I_1 + d + 1$ in the second ones.

**Line 2.** We show that 
\[
A = C_{I_1 \cup I_3 + \{(\lambda - (n-k)-1)\}}.
\]

**Lemma 3.** Let $S_i \overset{\text{def}}{=} C_{pub}^{[i]} + C_{pub}^{[i+1]} + \cdots + C_{pub}^{[i+\lambda-1]}$. For any set $\ast$ of $\lambda$ distinct integers modulo $m$ we have 
\[
\forall 0 \leq d \leq n - k - \lambda + 1, \ C_{S_0} \cap C_{(I_1 + d) \cup \ast \times [\lambda - 1 + d, n - k - 1] \cup I_3} = C_{S_0} \cap C_{(I_1 + d+1) \cup \ast \times [\lambda + d - 1, n - k] \cup (I_3 + 1) \subset M_1}.
\]

**Proof.** We prove the theorem by induction. This lemma is true for $d = 0$. We suppose that it is true until $0 \leq d \leq n - k - \lambda$, then we need to prove that it must be true for $d + 1$.

Indeed, 
\[
\bigcap_{i=0}^{d+1} S_i = C_{S_0} \cap \bigcap_{i=0}^{d} S_i = C_{S_0} \cap C_{(I_1 + d+1) \cup \ast \times [\lambda + d, n - k] \cup (I_3 + 1) \subset M_1}
\]

Let $M_1 = I_1 \cup I_4 \cup [d + 1, \lambda + d] \times [\lambda - 1, n - k - 1]$ 

Concerning $S_0 \subset M_1$ and $J \overset{\text{def}}{=} (I_1 + d+1) \cup \ast \times [\lambda + d, n - k] \cup (I_3 + 1) \subset M_1$.

We can apply the CodeSet theorem
\[
C_{S_0} \cap C_{J} = C_{S_0 \cap J}
\]

And by a slightly fastidious computation on the sets intersections, we see that 
\[
S_0 \cap J = (I_1 + d+1) \cup \ast \times [\lambda + d, n - k - 1] \cup I_3
\]

It is not very difficult to check that the sets do not intersect which gives the result.
In the rest of the proof we will suppose that $d = n - k - \lambda + 1$. If we instantiate the lemma with $d$ and elevate to the power $[-d]$ we obtain the following corollary:

**Corollary 1.** $A = C_{I_1 \cup I_3 - d}$

**Proof.** We have $\bigcap_{i=0}^{d} \mathcal{S}_i = C_{(I_1 + d) \cup I_3}$, with $I_1$ and $I_3$ subsets of $M$. Thus, from CodeSet theorem we have

$$A^{[d]} = C_{I_1 + d} \otimes C_{I_3}$$

Implying that $A = C_{I_1} \oplus C_{I_3 - d}$.

---

**Line 3.** Since $C_{\text{pub}}^{\perp} = C_{(0) \times [0,n-k-1]}$, we have

$$A^{[d-1]} \cap C_{\text{pub}}^{\perp} = C_{(I_1 + (d-1)) \cup (I_3 - 1)} \cap C_{(0) \times [0,n-k-1]}$$

with

$$I_1 + (d - 1) = \{ (u, j) : d - 1 \leq u \leq j \leq n - k - 2 \}$$

$$I_3 - 1 = \{ (u, j) : 0 \leq u \leq \lambda - 2, \ n - k - 1 \leq j \leq n - k + u - 1 \}$$

Let

$$I'_1 = (\{(0) \cup [n - k - \lambda, n - k - 2]) \times [\lambda - 1, n - k - 2] \} \cup [0, \lambda - 1] \times \{n - k - 1\}$$

and $M_2 = I_1 \cup I_4 \cup I'_2$
Since the intersecting sets are all subsets of the set \( \operatorname{operator} \), we also have

\[ \lambda \leq (n-k)/2 \]

Note that elevating to the power \( (n-k)/2 \), we obtain

\[ (I_1 + (d-1) \cup (I_3 - 1)) \cap \{0\} \times [0, n-k-1] = \{(0, n-k-1)\} \]

Since the intersecting sets are all subsets of the set \( M_2 \), we can apply the CodeSet theorem, and we obtain

\[ \mathcal{A}^{[d-1]} \cap \mathcal{C}_{\text{pub}}^+ = \mathcal{C}_{\{(0,n-k-1)\}} \]

which by elevating to the power \( [\lambda - d - 1] \) gives

\[ \mathcal{D}_{\lambda-1} = \mathcal{A}^{[\lambda-2]} \cap \mathcal{C}_{\text{pub}}^{[\lambda-d-1]} = \mathcal{C}_{\{\lambda-d-1,2\lambda-3\}} \]

Note that elevating to the power \( \lfloor m \rfloor \) the scalars corresponds to the identity operator, we also have \( \mathcal{D}_{\lambda-1} = \mathcal{C}_{\{m+\lambda-d-1,2\lambda-3\}} \). This will be of use in the proof of the algorithm. Now since \( \mathcal{B}_0 = \mathcal{A} + \mathcal{D}_{\lambda-1}^{[1+\lambda]} \), we deduce that

\[ \mathcal{B}_0 = \mathcal{C}_{I_1 \cup I_3 - d} + \mathcal{C}_{\{\lambda,d-2\}} \]

**Line 4.** Compute \( \mathcal{D}_0 = \mathcal{B}_0 \cap \mathcal{C}_{\text{pub}}^{[-1]} \)

We compute

\[ \mathcal{D}_0^{[1]} = \mathcal{B}_0^{[1]} \cap \mathcal{C}_{\text{pub}}^{[-1]} \]

\[ = (C_{(I_1+1) \cup I_3-(d-1)} + C_{\{d+1,\lambda-1\}}) \cap C_{\{0,(n-k)-1\}} \]

\[ = (C_{(I_1+1) \setminus (1,\lambda-1) \times \lambda} \oplus C_{\{0,(n-k)-1\}} \oplus C_{I_3-(d-1)}) \cap C_{\{0,(n-k)-1\}} \]

where \( * \) is instantiated for the set \( [0, \lambda-2] \cup \{-d+1\} \) which contains \( \lambda \) different integers.

Let \( I_2 = ([0,\lambda-1] \cup \{\lambda-1\}) \cup ([2-d, \lambda-d] \times [\lambda, n-k-1]) \) and \( M_3 = I_1 \cup I_4 \cup I_2 \). Now \( (I_1 + 1) \cup I_3 - (d-1) \cup \{-d+1, \lambda-1\} \subseteq M_3 \). Moreover,

\[ (\{(I_1 + 1) \cup I_3 - (d-1)\} \cap \{0\} \times [0, (n-k) - 1]) = \emptyset \]
Fig. 3. Points of \(((I_1 + 1)\setminus[1, \lambda - 1] \times (\lambda - 1)) \cup \mathcal{I} \times \{(\lambda - 1) \cup I_3 - (d - 1)\} \cup \{0\} \times [0, (n - k) - 1]\)

and \(* \times \{(\lambda - 1) \cap \{0\} \times [0, n - k - 1]\} = \{(0, \lambda - 1)\}

Hence, by the CodeSet theorem,

\[
B_0^1 \cap C_{\text{pub}}^\perp = C_{(0, \lambda-1)}
\]

\[
B_0 \cap C_{\text{pub}}^\perp[-1] = C_{(m-1, \lambda-2)}
\]

Line 5,6,7 For \(1 \leq i \leq \lambda - 2\), we compute

\[
B_i = A + \sum_{j=0}^{i-1} C_j^{(i-j)}
\]

\[
D_i = B_i \cap C_{\text{pub}}^\perp[-1] = C_{(m-1, \lambda+i-2)}
\]

We prove by induction, suppose that \(D_i = C_{(m-1, \lambda+i-2)}\) for all \(1 \leq i \leq \ell \leq \lambda - 2\). we prove this for \(i = \ell + 1\)

\[
B_{\ell+1} = A + \sum_{j=0}^{\ell} C_j^{(\ell+1-j)}
\]

\[
D_{\ell+1} = B_{\ell+1} \cap C_{\text{pub}}^\perp[-1] = C_{(m-1, \lambda+\ell-1)}
\]

Indeed,

\[
B_{\ell+1} = A + \sum_{j=0}^{\ell} \left(C_{(m-1, \lambda+j-2)}\right)^{(\ell+1-j)}
\]

\[
= A + \sum_{j=0}^{\ell} C_{(\ell-j, \lambda+\ell-1)}
\]

\[
= C_{I_1 \cup I_3 - d + \tilde{C}_{[0, \ell] \times \{(\lambda+\ell-1)\}}}
\]

\[
= C_{I_1 \cup (I_3 - d)[\ell - d + 1, \lambda - d - 1] \times (\lambda + \ell - 1)} + C_\mathcal{I} \times (\lambda + \ell - 1)
\]
Fig. 4. Points of $I_3 \cup (I_3 - d[\ell - d + 1, \lambda - d - 1] \times \{\lambda + \ell - 1\}) \cup \{0\} \times [0, (n - k) - 1]$

where $\ast$ is instantiated for the set $[\ell - d + 1, \lambda - d - 1] \cup [0, d]$ of $\lambda$ distinct integers.

We compute $D_{\ell+1}^{[1]} = B_{\ell+1}^{[1]} \cap C_{\parallel pub}^{\perp}$. Let

$$I_2' = ([0, \lambda - 1] \times \{\lambda - 1\}) \cup \{(0) \cup [2 - d, \lambda - d]\} \times [\lambda, n - k - 1]$$

and $M_4 = I_1 \cup I_4 \cup I_2'$. Then, $I_1 + 1, I_3 - d + 1$ and $\ast \times \{\lambda + \ell + 1\} \subset M_4$. Moreover,

$$I_3 - d + 1 \cap \{0\} \times [0, n - k - 1] = \emptyset$$

$$I_1 + 1 \cap \{0\} \times [0, n - k - 1] = \emptyset$$

Hence, by CodeSet theorem,

$$B_{\ell+1}^{[1]} \cap C_{\parallel pub}^{\perp} = C_{\ast \times \{\lambda + \ell - 1\}}$$

Therefore, $D_{\ell+1} = B_{\ell+1} \cap C_{\parallel pub}^{\perp} = C_{\ast \times \{(m - 1, \lambda + \ell - 1)\}}$

Line 8. Compute $\mathcal{H} = \sum_{j=0}^{\lambda-1} C_j^{[2-j-\lambda]}$.

We consider the sum of subspace:

$$\sum_{j=0}^{\lambda-1} C_j^{[2-j-\lambda]} = \sum_{j=0}^{\lambda-2} C_{[(m+1-\lambda-j,0)]} + C_{[(m+1-(n-k),0)]}$$

$$= C_{[(m+3-2\lambda,m+1-\lambda)\cup(m+1-(n-k))]\times(0)} = C_{\ast \times (0)} =: \mathcal{H}$$

where $\ast$ is instantiated for the set $[m + 2 - 2\lambda, m + 1 - \lambda] \cup \{m + 1 - (n - k)\}$ of $\lambda$ distinct integers.

Line 9-10 Next, for any $i \in \{0, \ldots, n - k - 1\}$, one can compute

$$C_{\parallel pub}^{\perp \ast} \cap \mathcal{H} = \langle h_0 + \sum_{i=1}^{\lambda-1} \beta_i^{[-i]} h_i \rangle$$
– For $\lambda - 1 \leq i \leq n - k - 1$, $\ast \times \{i\} \subset M$

$$\{(0, i)\} = \{(0) \times [0, n - k - 1]\} \cap (\ast \times \{i\})$$

Hence, by the CodeSet theorem, $C_{(0,0)} = C_{\text{pub}}^\perp \cap H^{[i]}$

– For $0 \leq i \leq \lambda - 2$, $C_{\text{pub}}^\perp \cap H^{[\lambda - 1]} = C_{\{(\lambda - 1) \times [\lambda - 1, n-k+\lambda-2]\}}$ and $H^{[\lambda + i - 1]} = C_{\ast \times (\lambda + i - 1)}$.

Moreover, $\ast \times \{\lambda + i - 1\} \subset \ast \times [\lambda - 1, 2\lambda - 3] \subset M$ and

$$\{(\lambda - 1, \lambda + i - 1)\} = \{(\lambda - 1) \times [\lambda - 1, n - k + \lambda - 2]\} \cap (\ast \times \{\lambda + i - 1\})$$

Hence, by the CodeSet theorem,

$$C_{\text{pub}}^\perp \cap H^{[\lambda - 1]} = C_{\{(\lambda - 1) \times (\lambda + i - 1)\}}$$

Therefore, for any $i \in \{0, \ldots, n - k - 1\}$, one can compute

$$C_{\text{pub}}^\perp \cap H = C_{\{(-i,0)\}} = \langle h_0 + \sum_{i=1}^{\lambda-1} \beta_j^{[-t]} h_i \rangle$$

Note that this specialization of one element of $S$ should be true for any element in $S$. Indeed, for 2 elements $(h', \beta)$ and $(h, \beta)$, if there exists $A \in GL(\lambda, \mathbb{F}_q)$ such that $(h', \beta') = A \cdot (h, \beta)$, then

$$\langle h_0 + \sum_{j=1}^{\lambda-1} \beta_j^{[-t]} h_j \rangle = \langle h_0 + \sum_{j=1}^{\lambda-1} \beta_j^{[-t]} h_j' \rangle$$

since $h_0' + \sum_{j=1}^{\lambda-1} \beta_j^{[-t]} h_j' = \left( a_{0,0} + \sum_{i=1}^{\lambda-1} a_i \beta_i \right) \left( h_0 + \sum_{i=1}^{\lambda-1} \beta_i h_i \right)$

Second step: Recovering the vector space

From step 1, we recovered the 1-dimensional vector-spaces

$$\forall i = 0, \ldots, n - k - 1, \ A_i = \left( h_0 + \sum_{j=1}^{\lambda-1} \beta_j^{[-t]} h_j \right)$$

The vector spaces $A_i$ do not depend on $(h, \beta) \in S$. We introduce the following lemma.

Lemma 4. For any $u_0 \in A_0$, and for any set $I = \{i_1, \ldots, i_\lambda\} \subset \{1, \ldots, n-k-1\}$ of $\lambda$ distinct elements, there exists a unique $\lambda$-tuple $u_\Sigma^{def} = (u_{i_1}, u_{i_2}, \ldots, u_{i_\lambda}) \in \bigotimes_{j=1}^{\lambda} A_i$ such that

$$\sum_{i,j \in I} u_{i_j} = u_0$$
Proof. We observe that, from assumption (1) we have
\[ A_i \oplus \cdots \oplus A_i = \langle h_0, \ldots, h_{\lambda-1} \rangle. \]
Since \( A_0 \subset \langle h_0, \ldots, h_{\lambda-1} \rangle \), this completes the proof. \( \square \)

We denote \( k_{i_\ell} \in F_q \) such that \( \forall i_\ell \in I, u_{i_\ell} = k_{i_\ell} \left( h_0 + \sum_{j=1}^{\lambda-1} \beta_j h_j \right) \). A vector \( u_0 \in A_0 \) can be written under the form
\[ u_0 = \alpha h_0 + \sum_{j=1}^{\lambda-1} \beta_j h_j \]
From the structure of the solution space \( S \), there exists an \( (h, \beta) \in S \) such that \( \alpha h_0 = 1 \). It means that we can fix \( u_0 := h_0 + \sum_{j=1}^{\lambda-1} \beta_j h_j \) as a known vector. For this element and for any \( I = \{ i_1, \ldots, i_\lambda \} \) from Lemma 4 we have
\[ \sum_{i_\ell \in I} k_{i_\ell} \left( h_0 + \sum_{j=1}^{\lambda-1} \beta_j h_j \right) = \left( \sum_{i_\ell \in I} k_{i_\ell} \right) h_0 + \sum_{j=1}^{\lambda-1} \left( \sum_{i_\ell \in I} k_{i_\ell} \beta_j h_j \right) h_j = h_0 + \sum_{j=1}^{\lambda-1} \beta_j h_j \]
Since the \( h_j \) are linearly independent we obtain the following system
\[ \begin{pmatrix} k_1^{I} \\ k_2^{I} \\ \vdots \\ k_\lambda^{I} \end{pmatrix} \begin{pmatrix} 1 & \beta_1^{[-i_1]} & \cdots & \beta_1^{[-i_\lambda]} \\ 1 & \beta_2^{[-i_2]} & \cdots & \beta_2^{[-i_\lambda]} \\ \vdots & \vdots & & \vdots \\ 1 & \beta_\lambda^{[-i_\lambda]} & \cdots & \beta_\lambda^{[-i_\lambda]} \end{pmatrix} = (1, \beta_1, \beta_2, \ldots, \beta_\lambda) \]
in the unknowns \( k_i^{I} \) and \( \beta_j \). From assumption (1) knowing the \( \beta_j \)'s, the solution is unique. To solve the system, let us consider the associate matrix
\[ Mat^I(\bar{X}) := \begin{pmatrix} 1 X_1^{[i_1]} X_2^{[i_1]} \cdots X_{\lambda-1}^{[i_1]} \\ 1 X_1^{[i_2]} X_2^{[i_2]} \cdots X_{\lambda-1}^{[i_2]} \\ \vdots \\ 1 X_1^{[i_\lambda]} X_2^{[i_\lambda]} \cdots X_{\lambda-1}^{[i_\lambda]} \end{pmatrix} \]
where \( \bar{X} = (X_1, X_2, \ldots, X_{\lambda-1}) \) is formed with the unknowns. We define the multivariate polynomial
\[ f^I(\bar{X}) \triangleq \det(Mat^I(\bar{X})) \]
Since \( f^I \in \mathbb{F}_q[\bar{X}] \) we have
Lemma 5. \( f^2 \) has degree \( \sum_{j \in \mathbb{Z}} [j] \) and for all \( u \in \mathbb{Z} \), \( f^{2+u}(\vec{X}) = f^2(\vec{X})^{[u]} \).

By Cramer’s rule, for any \( j = 1, \ldots, \lambda \) we have

\[
k^2_{ij} = \frac{f^{-((\mathcal{J} \setminus \{i\}) \cup \{0\})}(\vec{\beta})}{f^{-\mathcal{J} \cup \{0\}}(\vec{\beta})},
\]

where \( \vec{\beta} = (\beta_1, \ldots, \beta_\lambda) \). Let us define \( \mathcal{J}_s = (\{1, \ldots, \lambda + 1\} \setminus \{s + 1\}) \) for all \( s = 1, \ldots, \lambda \). From (3), we have

\[
\forall s \in \{1, \ldots, \lambda\}, \quad k^2_{1s} = \frac{f^{-(\mathcal{J}_s \setminus \{1\} \cup \{0\})}(\vec{\beta})}{f^{-\mathcal{J}_s}(\vec{\beta})}
\]

By elevating the equation to the power \( [\lambda + 1] \), from Lemma 5 we have

\[
\forall s \in \{1, \ldots, \lambda\}, \quad (k^2_{1s})^{[\lambda + 1]} = \frac{f^{(\lambda + 1) - (\mathcal{J}_s \setminus \{1\} \cup \{0\})}(\vec{\beta})}{f^{(\lambda + 1) - \mathcal{J}_s}(\vec{\beta})}
\]

Now since we know only the vector space \( \mathcal{A}_1 \) and not the exact vectors \( \vec{h}_0 + \sum_{j=1}^{\lambda - 1} \vec{h}_j \), we do not know \( k^{\mathcal{J}_s}_{1s} \). However, we can compute the quantity \( \frac{k^{\mathcal{J}_s}_{1s}}{k^{\mathcal{J}_s}_{1s}} \) for \( s \in \{1, \ldots, \lambda - 1\} \) thank to Algorithm 2 and Lemma 4.

\[\textbf{Algorithm 2:} \text{ Determining quotient } \frac{k^{\mathcal{J}_s}_{1s}}{k^{\mathcal{J}_s}_{1s}}\]

\begin{itemize}
  \item \textbf{Input:} \((A_i)_{i=1}^{n-k-1}, (\mathcal{J}_s)_{s=1}^\lambda \) and the vector \( \vec{u}_0 \in \mathcal{A}_0 \)
  \item \textbf{Output:} \( \alpha_s = \frac{k^{\mathcal{J}_s}_{1s}}{k^{\mathcal{J}_s}_{1s}} \) for \( s \in \{1, \ldots, \lambda - 1\} \)
  \item 1. For \( i = 1, \ldots, n - k - 1 \), fix \( \vec{u}_i \) arbitrarily in \( \mathcal{A}_i \)
  \item 2. For \( s = 1, \ldots, \lambda \), find \( a^{\mathcal{J}_s}_{J_s} \) such that \( \sum_{J_s \in \mathcal{J}_s} a^{\mathcal{J}_s}_{J_s} \vec{u}_j = \vec{u}_0 \)
  \item 3. Return \( \frac{a^{\mathcal{J}_s}_{1s}}{a^{\mathcal{J}_s}_{1s}} \) for \( s = 1, \ldots, \lambda - 1 \)
\end{itemize}

Now let us define by \( \alpha_s = (k^{\mathcal{J}_s}_{1s}/k^{\mathcal{J}_s}_{1s})^{[\lambda + 1]} \) for \( s = 1, \ldots, \lambda - 1 \). To simplify notations, we also define

\[
\forall s \in \{1, \ldots, \lambda\} \quad \begin{cases} L_s = (\lambda + 1) - (\mathcal{J}_s \setminus \{1\} \cup \{0\}) \\ M_s = (\lambda + 1) - \mathcal{J}_s \end{cases}
\]

We obtain the set of equations

\[
\forall s \in \{1, \ldots, \lambda - 1\}, \quad f^{L_s}(\vec{\beta}) f^{M_s}(\vec{\beta}) - \alpha_s f^{M_s}(\vec{\beta}) f^{L_s}(\vec{\beta}) = 0
\]

Let

\[
\mathcal{F}_s(\vec{X}) \overset{\text{def}}{=} f^{L_s}(\vec{X}) f^{M_s}(\vec{X}) - \alpha_s f^{M_s}(\vec{X}) f^{L_s}(\vec{X}) \in \mathbb{F}_q[\vec{X}].
\]
The polynomial $F_s$ has degree $q^{\lambda+1} + q^{\lambda} + 2 \sum_{j=1}^{\lambda-1} q^j + 1 -q^{\lambda-s}$

This gives us a multivariate polynomial system over $\mathbb{F}_q$ for which $\vec{\beta}$ is a solution. However, from our hypotheses we can do better and even reduce the degrees of the polynomials.

Since $\beta_1, \ldots, \beta_{\lambda}$ are linearly independent they cannot be roots of linear factors over $\mathbb{F}_q$ of $F_s$. Therefore we can reduce for all $s$ the polynomial $F_s(\vec{X})$ by its $\mathbb{F}_q$-linear factors.

**Lemma 6.** Let us define

$$f_0(\vec{X}) = \prod_{a \in \mathbb{F}_q} (X_1 + a)^{\lambda-1} \left( \prod_{i=2}^{\lambda} \prod_{a_1, \ldots, a_i \in \mathbb{F}_q} (X_i + \sum_{j=1}^{i-1} a_j X_j + a_0) \right)$$

For any set $\mathcal{I}$ of cardinality $\lambda$, $f^\mathcal{I}(\vec{X})$ is divisible by $f_0(\vec{X})$

**Proof.** Let $\vec{\beta}$ be a root of $X_i + \sum_{j=1}^{i-1} a_j X_j + a_0$ then they are $\mathbb{F}_q$-linear. Hence, for all set of cardinality $\lambda$, $\mathcal{I}$, the corresponding columns of $\text{Mat}^\mathcal{I}(\vec{\beta})$ are co-linear. Therefore, $f^\mathcal{I}(\vec{\beta}) = \det(\text{Mat}^\mathcal{I}(\vec{\beta})) = 0$

We have the following two corollaries

**Corollary 2.** We have $f^{\mathcal{J}_{\lambda-1}}(\vec{X}) = f_0(\vec{X})$

**Proof.** Both polynomials are monic. Since $\mathcal{J}_\lambda - 1 = \{0, \ldots, \lambda - 1\}$, they also have the same degree $\sum_{i=0}^{\lambda-1} q^i$

**Corollary 3.** For all $\mathcal{I} = \{i_1, \ldots, i_{\lambda}\}$, we have $(f_0(\vec{X}))^{[i_1]} | f^\mathcal{I}(\vec{X})$

We have

- From the lemma: $f_0(\vec{X})$ divides $f^{\mathcal{J}_s}(\vec{X})$ and $f^{\mathcal{I}_s}(\vec{X})$ for all $s \in \{1, \ldots, \lambda - 1\}$.
- From corollary $3$: $f_0(\vec{X})^{[1]}$ divides $f^{\mathcal{J}_1}(\vec{X})$ and $f^{\mathcal{I}_1}(\vec{X})$, since the minimum index of the sets is equal to 1.

Therefore, for all $s \in \{1, \ldots, \lambda - 1\}$, $F_s(\vec{X})$ can be divided by $f_0(\vec{X})^{q+1}$. We now consider the reduced polynomials

$$\forall s \in \{1, \ldots, \lambda - 1\}, \quad \mathcal{P}_s(\vec{X}) \overset{\text{def}}{=} \frac{F_s(\vec{X})}{(f_0(\vec{X}))^{q+1}} = \frac{F_0(\vec{X})}{f^{\mathcal{J}_{\lambda-1}}(\vec{X}) f^{\mathcal{I}_{\lambda}}(\vec{X})}$$

This gives us a new polynomial system for which $\vec{\tilde{\beta}}$ is also a solution, but the degree is reduced.
Lemma 7. Let \( \tilde{A} = (a_{i,j})_{i=0, j=0}^{\lambda-1, \lambda-1} \in PGL(\lambda; \mathbb{F}_q) \). Consider the transformation on \( f^T(\vec{X}) \) defined on \( \vec{X} = (X_1, \ldots, X_{\lambda-1}) \) by

\[
\forall j \in \{1, \ldots, \lambda - 1\}, \quad X_j \mapsto \frac{a_{0,j} + \sum_{i=1}^{\lambda-1} a_{i,j} X_i}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} X_i}
\]

then the polynomial \( f^T(\vec{X}) \) is transformed into

\[
f^T(\vec{X}) \mapsto \tilde{A}.f^T(\vec{X}) \overset{def}{=} \frac{\Delta_A}{(a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} X_i)^{\deg(f^T)}} f^T(\vec{X})
\]

where \( \Delta_A \) is the determinant of \( A \).

Proof. Let \( D = a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} X_i \). Thus, for \( j = 1, \ldots, \lambda \), the \( j \)th row of \( \text{Mat}^T(\vec{X}) \) denoted by \( \text{Row}_j(\text{Mat}^T(\vec{X})) \) becomes

\[
\text{Row}_j(\text{Mat}^T(\vec{X})) \mapsto \frac{\text{Row}_j(\text{Mat}^T(\vec{X}) \cdot A)}{D^{[i,j]}}.
\]

Therefore, since \( \deg(f^T) = \sum_{j \in \mathbb{Z} \setminus [j]} \), from lemma 5 we obtain

\[
\det(\text{Mat}^T(\vec{X})) \mapsto \frac{\det \tilde{A}}{D^{\deg(f^T)}} \det(\text{Mat}^T(\vec{X}))
\]

\[
f^T(\vec{X}) \mapsto \frac{\Delta_A}{D^{\deg(f^T)}} f^T(\vec{X})
\]

Apply the lemma, we have

\[
\mathcal{F}_s(\vec{X}) \mapsto \frac{\Delta_A^2}{D^{q^{\lambda+1} + q^{\lambda+2} \sum_{j=1}^{\lambda-1} q^j + 1 - q^{\lambda-1}}} \mathcal{F}_s(\vec{X})
\]

\[
f^{\mathcal{J}_s^1}(\vec{X}) \mapsto \frac{\Delta_A}{D^{\sum_{j=1}^{\lambda-1} q^j}} f^{\mathcal{J}_s^1}(\vec{X})
\]

\[
f^{\mathcal{J}_s^s}(\vec{X}) \mapsto \frac{\Delta_A}{D^{\sum_{j=1}^{\lambda-1} q^j}} f^{\mathcal{J}_s^s}(\vec{X})
\]

20
Hence,
\[ P_s(\vec{X}) \mapsto \frac{1}{D^{q^{\lambda+1}-q^2}} P_s(\vec{X}) \]

We therefore have

**Proposition 3.** If there isn’t any common factor between the polynomials \( P_s(X) \), then the set of root of the polynomial system

\[ \forall i = 1, \ldots, \lambda - 1, \quad P_i(\vec{X}) = 0 \tag{4} \]

equals the orbit of any root under the group action of \( \text{PGL}(\lambda, \mathbb{F}_q) \)

**Proof.** If there isn’t any common factor between the polynomials \( P_s(X) \) then the number of roots is at bounded by \( \prod_{j=1}^{\lambda-1} (q^{\lambda+1} - q^j) = |\text{PGL}(\lambda, q)| \) (Bezout bound [8]). Moreover, any element in the orbit of a solution \( \beta \) under the group action of \( \text{PGL}(\lambda, \mathbb{F}_q) \) is again root of the system. From Assumption [3] the orbit of \( \beta \) under \( \text{PGL}(\lambda, \mathbb{F}_q) \) has cardinality \( |\text{PGL}(\lambda, \mathbb{F}_q)| \) which means that the stabilization of \( \beta \) with respect to this group action is trivial. In that case any root of the system \( \beta \) corresponds to an element of \( S \).

For instance, when \( q = 2 \) and \( \lambda = 3 \) the system of equation below taking \((\beta_1, \beta_2)\) as solution:

\[ \begin{cases} P_{r1}(X,Y) = 0 \\ P_{r2}(X,Y) = 0 \end{cases} \]

This is a system of 2 polynomial equation in 2 variables. In practice, by using MAGMA, we can see that there isn’t any common factor between \( P_{r1}(X) \) and \( P_{r2}(X) \). Therefore, the number of roots has Bezout’s upper bound by the product of the degrees of \( P_{r1}(X,Y) \) and \( P_{r2}(X,Y) \).

Therefore, the number of roots are at most \((q^4 - q)(q^4 - q^2) = |\text{PGL}(3, q)|\). Thus, all the roots are in the orbit of a root under an action of \( \text{PGL}(3, q) \).

The remaining problem is finding a root of the system of equation above. It can be done by the following steps:

1. Calculating \( \text{Res}(Pr_1, Pr_2, Y) \) the resultant of \( Pr_1 \) and \( Pr_2 \) in the variable \( Y \). We obtain a univariate polynomial of degree 168 in variable \( X \). Finding one root \( x_0 \) of this polynomial.
2. Calculating \( \gcd(Pr_1(x_0, Y), Pr_2(x_0, Y)) \) which is a polynomial of degree 4 in variable \( Y \). Taking one root \( y_0 \) and verify it is a root of the system of equation.

In general, the problem of finding one root of a system of polynomial equation is a hard question as well as finding all roots of a system of polynomial equation.

21
**Polynomial System Solving over Finite Fields** Let $\mathbb{F}$ be a finite field.

**Input:** $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$.

**Goal:** Find a vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$ s.t: $f_1(\alpha) = \cdots = f_m(\alpha) = 0$.

Theoretically it is a NP-hard problem (problem AN9 p.251 in Appendix: A list of NP-complete problem [9]). For the special cases $\lambda = 2$ and $\lambda = 3$ finding a solution can be done in polynomial-time (by using properties of resultants for $\lambda = 3$).

However, in the case of no common factor, the number of roots is bounded by Bezout bound. To check that $\text{Pr}_i(X)^{\lambda-1}$ don’t have common factor, we can check whether $\text{Res}(\text{Pr}_i(X), \text{Pr}_j(X), X_1) \neq 0$, $\forall 1 \leq i < j \leq \lambda - 1$. (Prop. 1, Ch. 3, [10]). It costs $O(d^3)$ where $d = \prod_{j=1}^{\lambda-1} (q^\lambda + 1 - q^j)$ arithmetic operations over $\mathbb{F}_{q^m}[X_2, \ldots, X_{\lambda-1}]$.

We can see the importance of the Assumption(3) in the Proposition 3. In the case where this assumption does not satisfy, i.e there exists $A \in \text{PGL}(\lambda, \mathbb{F}_q)\backslash\mathcal{I}_\lambda$ and $A = (a_{ij})_{i,j=1}^\lambda$ such that

$$
\beta_j = \frac{a_{0,j} + \sum_{i=1}^{\lambda-1} a_{i,j} \beta_i}{a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} \beta_i}
$$

Thus, $\beta$ is a root of a system of $\lambda - 1$ polynomial equations of degree 2:

$$(a_{0,0} + \sum_{i=1}^{\lambda-1} a_{i,0} X_i) X_j - (a_{0,j} + \sum_{i=1}^{\lambda-1} a_{i,j} X_i) = 0, \ j = 1, \ldots, \lambda - 1$$

This polynomial is different from 0. Indeed, if it was, $a_{0,0} = a_{j,j}$ for $j = 1, \ldots, \lambda - 1$ and $a_{i,j} = 0$ for $i \neq j$, which means $A \in \mathcal{I}_\lambda$.

This system is multivariate quadratic (MQ)-system, the associated problem to decide if this system is solvable or not, also known as MQ-problem, is proven to be NP-complete [9]. Some algorithms used to solve this system is reviewed in the paper [11]. In case of $\lambda = 3$, this can be solved easily by Resultant. Therefore, when the Assumption [3] does not satisfy, we can exploit some information about $\beta$ by solving a multivariate quadratic system.

**Final step:** Now from a solution $\vec{\beta}$ to [4], we aim at finding the corresponding vector $\vec{h} \in (\mathbb{F}_{q^m})^\lambda$ such that $(\vec{h}, \vec{\beta}) \in S$.

We point out the key steps in the Coggia-Couvreur attack for $\lambda$ as follows. To be convenient, we denote known elements by blue color and unknown elements by red color. Given $\beta_1^{\lambda}, \ldots, \beta_{\lambda-1}, \beta_{\lambda}^{\lambda}$, recover $(\vec{h}_0, \ldots, \vec{h}_{\lambda-1}, \beta_1^{\lambda}, \ldots, \beta_{\lambda-1})$ corresponding.
1. For $\mathcal{I} = \{1, \ldots, \lambda\}$, since $\tilde{\beta}$ is known, $k_i = \frac{f^{- (\mathcal{I} \setminus \{i\}) \cup \{0\}}(\tilde{\beta})}{f^{- \mathcal{I}}(\tilde{\beta})}$, $i = 1, \ldots, \lambda$ can be computed. Moreover, from the Lemma 4 there exists a unique $\lambda$-tuple $\mathbf{u}_\mathcal{I} = (u_1, \ldots, u_\lambda) \in \bigtimes_{j=1}^\lambda \mathcal{A}_j$ such that $\sum_{i=1}^\lambda u_i = u_0$, so we can compute

$$h_0^i + \sum_{j=1}^\lambda \beta_j [-1] h_j^i = \frac{u_i}{k_i^i}, i = 1, \ldots, \lambda.$$

It implies to a linear system of $\lambda$ equations and $\lambda$ unknowns which are vectors $h_0^i, \ldots, h_{\lambda-1}^i$ and the determinant of the matrix of coefficients is non-zero.

2. After recovering an alternate key of the form $(h_0^i, \ldots, h_{\lambda-1}^i, \beta_1, \ldots, \beta_{\lambda-1})$, we can compute the dual code $C_{pub}^\perp$ and hence decrypt the ciphertext.

### 2.3 Complexity of the case $\lambda = 3$

This part shows the complexity of the attack by giving the number of operation in $\mathbb{F}_{q^m}$. Let $\omega$ be the exponent of the complexity of linear algebra operations. The Frobenius map costs $O(\log q)$ operations.

**Step 1.**

- Computation of dual code $C_{pub}^\perp$ costs $O(n^\omega)$ operations.
- Computation of $C_{pub}^\perp [i]$, $\forall i = 1, \ldots, n - k + 1$ costs $O(n^2 \log q)$ operations.
- Computation $S_j = \sum_{i=j}^{j+k-1} C_{pub}^\perp [i]$ uses Gaussian elimination, so it costs $O(n^\omega)$.

Thus, computation $\int_{i=0}^{n-k-\lambda+1} S_j$ costs $O(n^{\omega+1})$.

Overall step 1 costs $O(n^3 \log q + n^{\omega+1})$ operations.

**Step 2.**

- Computation $(\mathcal{I}^1, \ldots, \mathcal{I}^\lambda)$ represents the resolution of a linear system $\lambda$ unknowns and $n$ equations costs $O(n)$ operations. This computation performed $O(n)$ times, so it costs $O(n^2)$ operations.
- Complexity of finding a root of a polynomial of degree $\tilde{d}$ by Cantor–Zassenhaus algorithm (12) costs $O(d^2 m \log q)$ operations in $\mathbb{F}_{q^m}$ for $d = (q^4 - q)(q^4 - q^2)$.
- Computation of resultant of bivariate polynomials $\text{Res}(P_1, P_2, X)$ which $P_1, P_2$ of degree $d, e$ by Lickteig–Roy subresultant algorithm costs $O(d^2 e)$ (13).
- A finite number of linear systems solving costs $O(n^\omega)$

**Summary.** For $m = O(n)$, overall cost of $O(n^3 \log q + n^{\omega+1}) + \tilde{O}(d^2 n \log q)$ for $d = (q^4 - q)(q^4 - q^2)$. 

23
Conclusion We provided a distinguisher for the Loidreau’s scheme for any $\lambda$ and the public code has rate $R_{pub} \geq 1 - 1/\lambda$. From this distinguisher, we are able to complete a polynomial time key recovery with the assumption of finding one root of a system of polynomial equation. Moreover, we have extended the key recovery attack for $\lambda = 3$.

The parameters of $(k, n)$, which $R_{pub} \geq 1 - 1/\lambda$ should be avoided in Loidreau’s scheme. In the future, it will be worthwhile to attempt a modification of the attack to work for lower rate codes $R_{pub} < 1 - 1/\lambda$ as well.

References