Extending Coggia-Couvreur Attack on Loidreau’s Rank-metric Cryptosystem

Anirban Ghatak

Abstract A recent paper by Coggia and Couvreur presents a polynomial time key-recovery attack on Loidreau’s encryption scheme, based on rank-metric codes, for some parameters. Their attack was formulated for the particular case when the secret matrix in Loidreau’s scheme is restricted to a 2-dimensional subspace. We present an extension of the Coggia-Couvreur attack to deal with secret matrices chosen over subspaces of dimension greater than 2.

Keywords Rank-metric codes · code-based cryptography · cryptanalysis

Mathematics Subject Classification (2010) MSC[2010] 11T71

1 Introduction

One of the directions of current research in code-based cryptography is to formulate a strong variant of the McEliece scheme using codes in the rank-metric. The majority of proposals for rank-metric cryptosystems have been based on the use of Gabidulin codes and their variants or low-rank parity check (LRPC) codes. Of these, most of the Gabidulin-code based cryptosystems have been subjected to successful key-recovery attacks, for instance, R. Overbeck’s attack on the Gabidulin-Paramonov-Tretjakov (GPT) proposal. The basis of Overbeck’s attack is the fact that the application of a Frobenius-type map on a Gabidulin code generator matrix can be used to distinguish it from a random matrix. This principle - referred to in literature as a “distinguisher” - has since been used repeatedly to mount successful key recovery attacks on repair proposals on the GPT and other rank-metric variants; for instance, the attack on Faure-Loidreau’s scheme by Gaborit et al.

It follows that the first design objective of any rank-metric cryptosystem, based on Gabidulin-type codes, is resistance to key recovery attack along the lines of Overbeck’s method. So far, a few recent proposals claim to have achieved that
- for example, the repair of the Faure-Loidreau rank-metric scheme by Wachter-Zeh et al. [12] and Loidreau’s scheme [7]. Loidreau’s scheme uses Gabidulin codes for encryption with the following additional feature. It uses a secret matrix with entries from a strict subspace of the field underlying the Gabidulin code. It is claimed that Overbeck’s Frobenius-map distinguisher fails if the Gabidulin generator matrix is modified with this secret matrix. Coggia and Couvreur have shown (1) that polynomial time key recovery is possible with Loidreau’s scheme, for certain parameter constraints, when the dimension of the secret subspace is precisely $\lambda = 2$. While the dimension constraint appears restrictive, their approach has opened up the possibility for cryptanalysis of rank-metric schemes which have claimed resistance to attacks using Overbeck-type distinguishers. In this article we extend the Coggia-Couvreur key-recovery attack on Loidreau’s cryptosystem to admit secret matrices over subspaces of dimension $\lambda = 3$.

Contributions:
1. A proof of the non-random nature of the public generator matrix (i.e. formulating a “distinguisher” as in (1)) in Loidreau’s scheme for $\lambda \geq 3$.
2. Completing the key-recovery attack for $\lambda = 3$.

Organization of the article: The first section outlines Loidreau’s scheme and describes the steps of the Coggia-Couvreur attack. Section 3 formulates the distinguisher for any dimension of the secret subspace. The next section (Section 4) deals with the computation of certain specific subspaces, which are subsequently used in the extraction of parameters. Finally Section 5 provides the details of extending the key recovery attack to the case of $\lambda = 3$. We conclude with a discussion on the results and future work.

2 Loidreau’s Scheme and Coggia-Couvreur Attack

We first outline Loidreau’s scheme and discuss the reason it is claimed to resist Overbeck’s distinguisher.

2.1 Outline of Loidreau’s scheme:

Loidreau’s scheme (7) is similar to the Gabidulin rank-metric scheme, modified to resist Overbeck’s distinguisher.

- $G$ generator matrix of a Gabidulin code $G_k(a)$ over $\mathbb{F}_{q^m}$; $rk_q(a) = n$.
- $\mathcal{V} \subset \mathbb{F}_{q^m}$, $dim_q(\mathcal{V}) = \lambda \leq m$; $P \in GL_n(q^m)$ is a matrix over $\mathcal{V}$.
- Define $G_p := GP^{-1}$ and $t := \lfloor \frac{n-k}{2} \rfloor$.
- The public key is $K_p := (G_p, t)$ and the secret key, $K_s := (a, P)$.
- Encryption: $c = mG_p + e$; $e \in \mathbb{F}_{q^m}^n$ and $rk_q(e) = t$.
- Decryption: $cP = mG + eP$.

The $\mathbb{F}_q$-dimension of the product space $supp(e)$ over $\mathcal{V}$ is $t\lambda \leq \lfloor \frac{n-k}{2} \rfloor$, and hence, decoding for $G_k(a)$ will extract plaintext $m$.

Overbeck’s attack relies on the “Frobenius map” distinguisher on a Gabidulin code structure of the public generator matrix. Raising elements of $G_p$ to successive $q$-powers and vertically stacking the rows results in an augmented matrix where the
increase of rank is only by unity at each stage. But the rank of such a matrix constructed from a random code matrix would have an increment equal to the rank of the code matrix at every stage with high probability. So the Gabidulin type code matrix will have markedly less rank at some stage of the augmentation. However, in Loidreau’s scheme, \( G = GP^{-1} \), where \( P \) is constrained to some subspace \( V \subset F^{q_m} \). But there is no control over the entries of \( P^{-1} \) and so, the rank increment achieved at each stage via the \( q \)-exponentiation map is no longer exactly unity. Hence Overbeck’s distinguisher is no longer effective.

2.2 Coggia-Couvreur Attack for \( \lambda = 2 \)

Coggia and Couvreur defined a distinguisher for Loidreau’s scheme when the secret subspace \( V \) has dimension \( \lambda = 2 \). In this particular case they showed that key recovery is possible by solving for a triple \((\gamma, g, h)\) over \( F^{q_m} \), where \( \gamma \) specifies the secret subspace and \( g, h \) specify a decomposition of the (dual) public generator matrix \( C^\perp_{pub} \) in terms of the secret matrix \( P \) and the secret generator matrix.

Notation: Henceforth in the article, the notation \( g[i] \), \( i \) an integer, would mean raising all components of \( g \) to the \( q^i \)-th power.

2.2.1 Distinguisher for \( \lambda = 2 \)

– Without loss of generality can specify the secret subspace as:
\[
V = \langle (1, \gamma) \rangle; \gamma \in F^{q_m} \setminus F_q
\]

Then we have the formulation: \( P^T = P_0 + \gamma P_1 \), where \( P_0, P_1 \in GL_n(F_q) \).
– The dual of the secret code has generator matrix: \( C^\perp_{pub} \cong \mathcal{G}_{n-k}(a') \) for some \( a' \in F^{q_m}_n \) with \( \text{rk}_{q}(a') = n \).
– Define \( g := a'P_0 \) and \( h := a'P_1 \).
– \( C^\perp_{pub} = (g + \gamma h, g [1] + \gamma h [1], \ldots, g [r] + \gamma h [r]) \), where \( r := n - k - 1 \).

Theorem 1 ([1])
\[
\text{dim}_{q_m}(C^\perp_{pub} + C^\perp_{pub} [1] + C^\perp_{pub} [2]) \leq 2 \text{dim}_{q_m} C^\perp_{pub} + 2.
\]

It follows that \( C^\perp_{pub} \) will be distinguishable from a random matrix in polynomial time whenever \( 2(n - k) + 2 < n \), i.e. when \( n < 2k - 2 \). Hence, for the distinguisher to work, the rate of the code should satisfy: \( k/n > 1/2 + 1/n \approx 1/2 \).

2.2.2 Recovery of alternate key

– The following iterated intersection is shown to be of \( F^{q_m} \)-dimension 2 and is generated by \( g [r] + \gamma [r] h [r] \) and \( g [r+1] + \gamma [1] h [r+1] \):
\[
(C^\perp_{pub} + C^\perp_{pub} [1]) \cap (C^\perp_{pub} [1] + C^\perp_{pub} [2]) \cap \cdots \cap (C^\perp_{pub} [r] + C^\perp_{pub} [r+1])
\]

– Can extract the subspaces: \( \langle g + \gamma h \rangle, \langle g + \gamma [-1] h \rangle, \ldots, \langle g + \gamma [-r] h \rangle \).
Likewise, define $V$ Assume that $P$ Accordingly we have:

\[ \lambda \]

3.1 Distinguisher for $\lambda \geq 3$

A crucial result (Proposition 5, [1]) shows that, viewed as vectors over $\mathbb{F}_q$, the set of roots of $P_\gamma(X)$ form an orbit under the action of the projective linear group $PGL(2, q)$. The action is sharply transitive and as such, any root of $P_\gamma(X)$ can be chosen as a valid $\gamma$.

With a valid choice for $\gamma$, say $\gamma'$, and using the known quantities $g + \gamma h$ and say, $u_{12}$, set up the equations:

\[ g + \gamma h = g' + \gamma' h'; \quad u_{12} = \frac{\gamma'[-2]}{\gamma[-2]} - \frac{\gamma'}{\gamma'[-1]}(g' + \gamma'[-1] h'). \]

Solving for the triple $(\gamma', g', h')$ provides an alternative secret key.

3 Distinguisher for Loidreau’s Scheme for $\lambda \geq 3$

We attempt to extend Coggia-Courvreur attack to the cases where the secret subspace $V$ has dimension $\lambda > 2$. The first step is to establish the non-randomness of the public matrix, i.e. formulating the so-called “distinguisher”.

3.1 Distinguisher for $\lambda = 3$

Assume that $V = \langle 1, \gamma_1, \gamma_2 \rangle$, where $\gamma_i \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$.

Accordingly we have: $P^T = P_0 + \gamma_1 P_1 + \gamma_2 P_2$; where all $P_i \in GL_n(q)$.

Define $g_0 = aP_0, \quad g_1 = aP_1, \quad g_2 = aP_2$. Then we have, for $r = n - k - 1$,

\[ c_{pub}^{\perp} = \langle (g_0 + \gamma_1 g_1 + \gamma_2 g_2), (g_0^{[1]} + \gamma_1 g_1^{[1]} + \gamma_2 g_2^{[1]}), \ldots, (g_0^{[r]} + \gamma_1 g_1^{[r]} + \gamma_2 g_2^{[r]}) \rangle \]

Likewise $c_{pub}^{\perp}[1]$ is spanned by:

\[ \langle g_0^{[1]} + \gamma_1 g_1^{[1]} + \gamma_2 g_2^{[1]} \rangle, \quad \langle g_0^{[2]} + \gamma_1 g_1^{[2]} + \gamma_2 g_2^{[2]} \rangle, \ldots, \quad \langle g_0^{[r+1]} + \gamma_1 g_1^{[r+1]} + \gamma_2 g_2^{[r+1]} \rangle \]
and $C_{pub}^{\perp}$ is spanned by:

$$(\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2), (\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2 + \gamma_3 \mathbf{b}_3), \ldots, (\mathbf{g}_0 + [r+2] \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2).$$

Hence, akin to the formulation for $\lambda = 2$ presented in [1], we state the following theorem based on the preceding discussion.

**Theorem 2** The dual $C_{pub}^{\perp}$ of the public code in Loidreau’s scheme satisfies:

$$\dim_q(C_{pub}^{\perp} + C_{pub}^{\perp}[1] + C_{pub}^{\perp}[2] + C_{pub}^{\perp}[3]) \leq 3 \dim_q C_{pub}^{\perp} + 3.$$

**Proof** Consider the sum space $C_{pub}^{\perp} + C_{pub}^{\perp}[1] + C_{pub}^{\perp}[2]$. For $i = 2, \ldots, r$, given the choice of $\gamma_1, \gamma_2 \in \mathbb{F}_q \setminus \mathbb{F}_q^3$, the following matrix is invertible:

$$\begin{pmatrix}
1 & \gamma_1 & \gamma_2 \\
1 & [\gamma_1] & [\gamma_2] \\
1 & [\gamma_2] & [\gamma_2]
\end{pmatrix}$$

It follows that one can extract the triples $(\mathbf{g}_0^{[i]}, \mathbf{b}_1^{[i]}, \mathbf{b}_2^{[i]}), i = 2, \ldots, r$, from

$$(\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2), (\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2 + \gamma_3 \mathbf{b}_3)$$

and $(\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2 + \gamma_3 \mathbf{b}_3)$. In addition to these $(n - k - 2)$ triples, $C_{pub}^{\perp} + C_{pub}^{\perp}[1] + C_{pub}^{\perp}[2]$ contains the following 6 vectors:

$$(\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2), (\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2 + \gamma_3 \mathbf{b}_3), (\mathbf{g}_0 + \gamma_1 \mathbf{b}_1 + \gamma_2 \mathbf{b}_2 + \gamma_3 \mathbf{b}_3)$$

$$(\mathbf{g}_0^{[r+1]} + \gamma_1 \mathbf{b}_1^{[r+1]} + \gamma_2 \mathbf{b}_2^{[r+1]}), (\mathbf{g}_0^{[r+1]} + \gamma_1 \mathbf{b}_1^{[r+1]} + \gamma_2 \mathbf{b}_2^{[r+1]} + \gamma_3 \mathbf{b}_3^{[r+1]})$$

and $(\mathbf{g}_0^{[r+2]} + \gamma_1 \mathbf{b}_1^{[r+2]} + \gamma_2 \mathbf{b}_2^{[r+2]} + \gamma_3 \mathbf{b}_3^{[r+2]})$.

Thus we can conclude that the sum space $C_{pub}^{\perp} + C_{pub}^{\perp}[1] + C_{pub}^{\perp}[2]$ is spanned by $3(n - k - 2) + 3 + 3 = 3(n - k)$ vectors as outlined above. Adding $C_{pub}^{\perp}[3]$ to this sum space adds vectors involving terms of $q$-power 3 and above, going up to the term having $(r + 3)$-th power of $q$.

Evidently this allows the extraction of another triple $(\mathbf{g}_0^{[r+1]}, \mathbf{b}_1^{[r+1]}, \mathbf{b}_2^{[r+1]})$, adds two terms with $q$-power $r + 2$ and a last term with $q$-power $r + 3$.

Therefore,

$$\dim_q(C_{pub}^{\perp} + C_{pub}^{\perp}[1] + C_{pub}^{\perp}[2] + C_{pub}^{\perp}[3]) \leq 3(n - k) + 3.$$

From the above theorem, we can infer that for $\lambda = 3$, $C_{pub}^{\perp}$ is distinguishable in polynomial time from a random code matrix when $3(n - k) + 3 < n$, i.e. when $3k - 3 > 2n$. This also implies that this distinguisher is effective if the underlying codes have rate $\frac{k}{n} > \frac{2}{3}$.

---

1 In a recent version of their paper: arxiv.org/abs/1903.02933v2, the authors have indicated the form of the sum space to extend their argument for $\lambda = 2$. We had independently arrived at a similar conclusion based on the original version of their paper and have, moreover, presented the details of the proof for $\lambda \geq 3$. 


3.2 Distinguisher for $\lambda > 3$

Based on the principle outlined for $\lambda \leq 3$, one can propose distinguishers for Loidreau’s scheme, subject to a constraint on the rate $\frac{k}{m}$ of the underlying code.

For $\lambda = m > 3$, it is assumed that the secret subspace $V = \langle 1, \gamma_1, \ldots, \gamma_{m-1} \rangle$, $\gamma_i \in \mathbb{F}_q = \mathbb{F}_q \setminus \mathbb{F}_q$. In the same spirit as before, we first look at the $m$-fold $q$-power sum of $C_{\text{pub}}^\perp$, the dual public code, given by:

$$C_{\text{pub}}^\perp[m] = C_{\text{pub}}^\perp[1] \oplus C_{\text{pub}}^\perp[2] \oplus \cdots \oplus C_{\text{pub}}^\perp[m-1].$$

(1)

Grouping together terms involving the same $q$-powers, we can extract $m$-tuples $(g_0^{[i]}, g_1^{[i]}, \ldots, g_{m-1}^{[i]})$ whenever we can form an invertible $m \times m$ matrix of the following form:

$$
\begin{pmatrix}
1 & \gamma_1 & \cdots & \gamma_{m-1} \\
1 & \gamma_1 & \cdots & \gamma_{m-1}^{[i]} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \gamma_1 & \cdots & \gamma_{m-1}^{[m-1]}
\end{pmatrix}
$$

Thus, we can count the number of terms in the $m$-fold sum, prior to the stage that such an invertible matrix can be formed to extract the first set of $m$-tuples with largest $q$-power $m-1$ as follows:

There are precisely $\frac{m(m-1)}{2}$ terms of the form $(g_0^{[i]} + \gamma_1^{[j]} g_1^{[j]} + \cdots + \gamma_{m-1}^{[j]} g_{m-1}^{[j]})$, with both $i, j$ allowed to assume appropriate values between 0 and $m - 2$.

Next, assuming $m < n - k - 1$, we can continue to collect $m$-tuples of higher $q$-powers till $i = n - k - 1$. Beyond this, we revert back to the sum vectors involving higher $q$-powers all the way up to $i = n - k - 1 + (m - 1) = n - k - m - 2$ and this adds another set of $(m - 1) + (m - 2) + \cdots + 1 = \frac{m(m-1)}{2}$ vectors.

Therefore, we conclude that the $m$-fold sum in (1) has $\mathbb{F}_q^n$-dimension $M$, where

$$M \leq 2 \times \frac{m(m-1)}{2} + m(n - k - 1 - (m - 2)) = m(n - k) = m \dim_q(C_{\text{pub}}^\perp).$$

Adding $C_{\text{pub}}^\perp[m]$ to the sum space in (1) does not change the stage at which the first $m$-tuple can be extracted. But it does alter the stage of extracting the final $m$-tuple: we can obtain an invertible $m \times m$ matrix to extract the tuple $(g_0^{[n-k]}, g_1^{[n-k]}, \ldots, g_{m-1}^{[n-k]})$. Beyond this, there are again a set of $\frac{m(m-1)}{2}$ vectors with terms of increasing $q$-powers till $n - k - 1 + m$. This yields a total of $m(m - 1) + m(n - k - (m - 2)) = m(n - k) + m$ vectors.

Hence we have the following

**Theorem 3** If the secret subspace of Loidreau’s scheme has dimension given by $\lambda = m \geq 2$, the dual of the public code, denoted $C_{\text{pub}}^\perp$, satisfies:

$$\dim_q(C_{\text{pub}}^\perp + C_{\text{pub}}^\perp[1] + C_{\text{pub}}^\perp[2] \oplus \cdots \oplus C_{\text{pub}}^\perp[m]) \leq m \dim_q(C_{\text{pub}}^\perp + m).$$

Evidently this procedure yields a distinguisher when $m(n - k) + m < n$. So the distinguisher is effective when the underlying code has rate $\frac{k}{m} > \frac{m-1}{m}$. This argues in favour of using low or moderate rate codes in conjunction with secret subspaces of large dimensions in order to counter this distinguisher.
4 Computing the extraction subspaces

To extend the Coggia-Couvreur attack to the case $\lambda = 3$, we attempt to obtain an alternative tuple $\{\gamma_i, \gamma_j, \mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2\}$, which can lead to a valid secret key. Following the procedure outlined in Section 2, the first step is to compute the subspace $\langle \mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2 \rangle$, and hence, sum spaces of the form $\langle \mathbf{g}_0 + \gamma_i \mathbf{g}_1 + \gamma_j \mathbf{g}_2 \rangle$, for integers $i > 0$. These subspaces, taken together, are then utilized to extract alternative tuples for a valid secret key - hence we term them extraction subspaces. Further we term the subspaces formed by adjoining successive $q$-powers of subspaces as sumspaces. To obtain the extraction subspaces, we first examine the intersections for the 3-fold sumspaces.

4.1 Intersections of sumspaces

We now establish the dimensions of intersection spaces among the sumspaces with different sequences of $q$-poers of the dual code $C_{pub}^\perp$. For that, we introduce the following notation to denote sumspaces involving several $q$-poers. Define

$$ S_i^j := C_{pub}^\perp + C_{pub}^\perp[j] + \cdots + C_{pub}^\perp[j+i-1] $$

which starts with $q^j$-th power of $C_{pub}^\perp$ and adds $i - 1$ more terms with increasing $q$-poers till $C_{pub}^\perp[j+i-1]$. In this notation, we have:

$$ S_4 \perp := (C_{pub}^\perp + C_{pub}^\perp[1] + C_{pub}^\perp[2] + C_{pub}^\perp[3]). $$

Hence, we have established in Theorem 2 that:

$$ \dim_q(S_4^3) \leq 3 \dim_q C_{pub}^\perp + 3. $$

Looking at the spanning sets for the 3-fold sumspaces $S_0^3$ and $S_1^3$, it is evident that both of them have $\mathbb{F}_q$-dimensions $\leq 3(n-k)$. Assuming both the above sumspaces possess maximum dimension and further, the 4-fold sumspace $S_0^3$ has dimension $3(n-k) + 3$, we have:

$$ \dim_q(S_0^3 \cap S_1^3) = 3(n-k) - 3 \quad (2) $$

A spanning set for $S_3^3$ consists of triples $\{g_0^{[i]}, g_1^{[i]}, g_2^{[i]}\}$ for $i = 4, 5, \cdots, r + 2$, along with the following 6 vectors:

$$ (g_0^{[2]} + \gamma_1 g_1^{[2]} + \gamma_2 g_2^{[2]}), (g_0^{[3]} + \gamma_1 g_1^{[3]} + \gamma_2 g_2^{[3]}), (g_0^{[4]} + \gamma_1 g_1^{[4]} + \gamma_2 g_2^{[4]}), (g_0^{[r+3]} + \gamma_1 g_1^{[r+3]} + \gamma_2 g_2^{[r+3]}), (g_0^{[r+4]} + \gamma_1 g_1^{[r+4]} + \gamma_2 g_2^{[r+4]}), \quad (3) $$

In all, we have $3(r + 2 - 3) = 3(n-k-2)$ vectors from the triples and the 6 vectors apart from them, spanning $S_3^3$. Moreover, we can list the vectors “shared” between $S_2^3$ and $S_0^3$ as follows.

1. All the triples for indices $i = 4, 5, \cdots, r$.
2. The last 3 vectors of $S_0^3$ belong to the span of the last two triples of $S_2^3$.  


3. The first 3 vectors of $S_2^3$ belong to the span of the first two triples of $S_0^3$.

Therefore, the intersection space of the above 3-fold sumspaces has dimension $3(r - 3) + 6$. Thus we have:

$$\dim_q = (S_0^3 \cap S_2^3) = 3(n - k) - 6. \quad (3)$$

**Theorem 4** The dimension of the intersection space $S_0^3 \cap S_3^m$ over $\mathbb{F}_q$ is precisely $3(n - k) - 3m$.

**Proof** We prove the theorem by induction on $m$. For the first $q$-power term of the second sumspace. The preceding discussion, the above holds for $m = 1, 2$. Assuming it holds up to $m - 1$, we have

$$\dim_q = (S_0^3 \cap S_{m-1}^3) = 3(n - k) - 3(m - 1).$$

Raising the first exponent to $m$ from $m - 1$ reduces one shared triple from the intersection space. However, the last three vectors of the first sumspace and the first three vectors of the second sumspace are still shared. Thus, there is a reduction of the dimension of the intersection space by precisely 3 in going from $m - 1$ to $m$. Hence

$$\dim_q = (S_0^3 \cap S_m^3) = 3(n - k) - 3m.$$

\[\square\]

**Corollary 1** Given $r = n - k - 1$, we have:

$$\dim_q = (S_0^3 \cap S_r^3) = 3(n - k) - 3r = 3. \quad (4)$$

4.2 Extraction subspaces from intersection between $C_{pub}^1$ and sumspaces

Building on the previous analysis, we now compute the extraction subspaces from the intersection of $C_{pub}^1$ with recursively obtained subspaces.

From Corollary 1, we expect to identify 3 independent vectors which span the intersection space $S_0^3 \cap S_3^m$. Two obvious choices are the vectors:

$$v_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

The choice of a third vector spanning $S_0^3 \cap S_3^m$, linearly independent with respect to the two above, must be from the intersection of the following subspaces:

$$\langle S_0^3 \cap S_3^m \rangle \cap \langle S_1^3 \rangle = \langle \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle$$

and

$$\langle S_0^3 \cap S_3^m \rangle \cap \langle S_2^3 \rangle = \langle \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle.$$

Thus the third vector can have the following equivalent representations:

$$v_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} m_1 \gamma_1^r + m_2 \gamma_2^r \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$
where \( k_1, k_2, m_1, m_2 \in F_q \). Let

\[
\mathbf{x}_1 := \mathbf{v}_1^{[-r]} = g_0 + \gamma_1 g_1 + \gamma_2 g_2;
\]

\[
\mathbf{x}_2 := \mathbf{v}_2^{[-r]} = g_0[2] + \gamma_1[2] g_1[2] + \gamma_2[2] g_2[2];
\]

\[
\mathbf{x}_3 := \mathbf{v}_3^{[-r]} = g_0[1] + (a_1 \gamma_1 + a_2 \gamma_1[1]) g_1[1] + (a_1 \gamma_2 + a_2 \gamma_2[1]) g_2[1].
\]

Define \( B_1 := \langle \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \rangle \). In a manner similar to that outlined in [1], we proceed to first obtain the subspace \( \langle g_0, g_1, g_2 \rangle \) and then the other extraction subspaces.

- Obtain \( \langle g_0 + \gamma_1 g_1 + \gamma_2 g_2 \rangle \) from the intersection \( C_{\mu B}^\perp \cap B_1 \).

Raising to the \( q \)-th power, we get \( \langle g_0[1] + \gamma_1[1] g_1[1] + \gamma_2[1] g_2[1] \rangle \).

- Consider the following sum of subspaces:

\[
B_2 = B_1 + \langle g_0[1] + \gamma_1[1] g_1[1] + \gamma_2[1] g_2[1] \rangle + \langle g_0[1] + (b_1 \gamma_1[1-r] + b_2 \gamma_1[2-r]) g_1[1] + (a_1 \gamma_1[1-r] + a_2 \gamma_2[2-r]) g_2[1] \rangle
\]

where one of the forms of \( v_3 \) yields the third component.

Evidently \( B_2 = \langle x_1, g_0[1] : g_1[1], g_2[1] : x_2 \rangle \).

- We can thus extract \( \langle g_0[1] + \gamma_1[1-r] g_1[1] + \gamma_2[1-r] g_2[1] \rangle \) from \( B_2 \cap (C_{\mu B}^\perp)[1-r] \). Hence we obtain \( B_3 := \langle g_0 + \gamma_1[1-r] g_1 + \gamma_2[1-r] g_2 \rangle \).

- The following sum of subspaces:

\[
B_3 + \langle x_1 \rangle + \langle g_0 + (c_1 \gamma_1[1-r] + c_2 \gamma_2) g_1 + (c_1 \gamma_1 + c_2 \gamma_2) g_2 \rangle
\]

where the third component is obtained from \( x_3 \), yields \( B = \langle g_0, g_1, g_2 \rangle \). The \( i \)-th extraction subspace \( \langle g_0 + \gamma_1[1-i] g_1 + \gamma_2[1-i] g_2 \rangle \) can be obtained by taking the \( q^{-i} \)-th power of the intersection \( B[i] \cap C_{\mu B}^\perp \).

5 Completing the Attack for \( \lambda = 3 \)

Following Coggia and Couvreur ([1]) for the 2-dimensional case, we can specify the goal of the attack as follows.

**Objective:**

To extract an alternative tuple \( \{g_0, g_1', g_2', \gamma_1', \gamma_2'\} \) such that it satisfies:

\[
C_{\mu B} = \langle g_0[i] + \gamma_1 g_1[i] + \gamma_2 g_2[i] | i = 0, 1, \cdots, n-k-1 \rangle
\]

(5)

The analogous result was ingeniously achieved in the two-dimensional case by performing a semilinear transformation on the single parameter \( \gamma \) and setting up an equation to obtain the \( g \)-parameters (\( \langle g, h \rangle \) in [1]). We now show that the same trick works in the 3-dimensional case as well.

**Proposition 1** Define \( \gamma_1, \gamma_2 \in F_q = \langle g, h \rangle \) as follows:

\[
\gamma_1 = \frac{a_{11} \gamma_1' + a_{12} \gamma_2' + a_{13}}{a_{31} \gamma_1' + a_{32} \gamma_2' + a_{33}}; \quad \gamma_2 = \frac{a_{21} \gamma_1' + a_{22} \gamma_2' + a_{23}}{a_{31} \gamma_1' + a_{32} \gamma_2' + a_{33}}.
\]

where \( a_{ij} \) are the entries of a matrix \( A \in GL_3(F_q) \).

Then the tuple \( \{g_0, g_1', g_2', \gamma_1', \gamma_2'\} \) satisfies Equation (5) for the following choices:

\[
g_0' = a_{33} g_0 + a_{13} g_1 + a_{23} g_2; \quad g_1' = a_{31} g_0 + a_{11} g_1 + a_{21} g_2; \quad g_2' = a_{32} g_0 + a_{12} g_1 + a_{22} g_2.
\]
Proof Substituting the values of $\gamma_1, \gamma_2$ in $g_0^{[i]} + \gamma_1 g_1^{[i]} + \gamma_2 g_2^{[i]}$ and rearranging in the form $\ldots^{[i]} + \gamma_1^{[i]} \ldots^{[i]} + \gamma_2^{[i]} \ldots^{[i]}$ leads to the assertion.

\[ \Box \]

It was further shown in [11] that the secret subspace parameter $\gamma$ was the root of a polynomial with constituent factors of the form: $X^{[i]} - X^{[j]}$. They established that performing a standard semilinear transformation on any root yielded another root - the projective linear group $PGL(2, q)$ acts sharply transitively on the set of roots. In this section, we produce a bivariate polynomial of which each root pair is a tuple $\{\gamma_1, \gamma_2\}$ that can similarly lead to a valid secret key.

5.1 The Polynomial Equation for $\{\gamma_1, \gamma_2\}$

We now use the extraction subspaces to set up a polynomial equation for the tuple $\{\gamma_1, \gamma_2\}$. Owing to the structure of the underlying Gabidulin codes, we can choose any element in $\langle g_0 + \gamma_1 g_1 + \gamma_2 g_2 \rangle$ as a candidate for $g_0 + \gamma_1 g_1 + \gamma_2 g_2$. Moreover, for distinct integers $i, j, k$ in the range $[1, n-k-1]$, we can show that (cf. Lemma 5 in [11]) $\langle g_0, g_1, g_2 \rangle$ can be expressed as a direct sum as follows:

\[ \langle g_0 + \gamma_1^{[i]}, g_1 + \gamma_2^{[i]} g_2 \rangle \oplus \langle g_0 + \gamma_1^{[j]}, g_1 + \gamma_2^{[j]} g_2 \rangle \oplus \langle g_0 + \gamma_1^{[k]}, g_1 + \gamma_2^{[k]} g_2 \rangle. \]

This implies that, given a choice of $(i, j, k)$ there exists a unique triple $(u, v, w)$ such that: $u + v = g_0 + \gamma_1 g_1 + \gamma_2 g_2$, where $u = k_1 g_0 + \gamma_1^{[i]} g_1 + \gamma_2^{[i]} g_2$, $v = k_2 g_0 + \gamma_1^{[j]} g_1 + \gamma_2^{[j]} g_2$ and $w = k_3 g_0 + \gamma_1^{[k]} g_1 + \gamma_2^{[k]} g_2$, for $k_1 \in \mathbb{F}_q^m$. Thus we have:

\[ k_1 + k_2 + k_3 = 1; \]
\[ k_1 \gamma_1^{[i]} + k_2 \gamma_1^{[j]} + k_3 \gamma_1^{[k]} = \gamma_1; \]
\[ k_1 \gamma_2^{[i]} + k_2 \gamma_2^{[j]} + k_3 \gamma_2^{[k]} = \gamma_2. \]

Solving the system of equations (6), we obtain:

\[ k_1 = \frac{1}{\Delta} (\gamma_1^{[i]} - \gamma_2^{[i]} - \gamma_1^{[j]} - \gamma_2^{[j]} - \gamma_1^{[k]} - \gamma_2^{[k]}); \]
\[ k_2 = \frac{1}{\Delta} (\gamma_1^{[i]} - \gamma_2^{[i]} - \gamma_1^{[j]} - \gamma_2^{[j]} - \gamma_1^{[k]} - \gamma_2^{[k]}); \]
\[ k_3 = \frac{1}{\Delta} (\gamma_1^{[i]} - \gamma_2^{[i]} - \gamma_1^{[j]} - \gamma_2^{[j]} - \gamma_1^{[k]} - \gamma_2^{[k]}); \]

where

\[ \Delta = (\gamma_1^{[i]} - \gamma_2^{[i]} - \gamma_1^{[j]} - \gamma_2^{[j]} - \gamma_1^{[k]} - \gamma_2^{[k]}). \]

Denote the vector $u$ obtained for the index set $(i, j, k)$ as $u_{ijk}$. It is obvious that any pair $(u_{ijk}, u_{ij'k'})$ satisfies: $u_{ijk} = \alpha u_{ij'k'}$, for some $\alpha \in \mathbb{F}_q^m$, since $u_{ijk}, u_{ij'k'} \in \langle (g_0 + \gamma_1^{[i]} g_1 + \gamma_2^{[i]} g_2) \rangle_{\mathbb{F}_q^m}$. As the coefficients $k_i$ in (9) are dependent on $i, j, k$, as well, we denote:

\[ u_{ijk} = k_{ij}^{[i]} (g_0 + \gamma_1^{[i]} g_1 + \gamma_2^{[i]} g_2). \]
This leads to an equation in terms of the coefficients used to describe the vector $u$ as follows: $k_{ij}^{k} = \alpha k_{ij}^{k'}$. Substituting the values of $k_1$ for both sets of indices, using Equations (7) and (8), we obtain a polynomial equation in $\gamma_1, \gamma_2$ over $\mathbb{F}_q^m$.

As an illustration, the corresponding equation for $u_{123}$ and $u_{145}$ is:

\[
\frac{1}{\Delta_{123}}[(\gamma_1 \gamma_2^{-1} - \gamma_2 \gamma_1^{-1}) + (\gamma_2 \gamma_1^{-1} - \gamma_1 \gamma_2^{-1}) + (\gamma_1 \gamma_2^{-1} - \gamma_1 \gamma_2^{-1})] = \alpha \frac{1}{\Delta_{145}}[(\gamma_1 \gamma_2^{-1} - \gamma_2 \gamma_1^{-1}) + (\gamma_2 \gamma_1^{-1} - \gamma_1 \gamma_2^{-1}) + (\gamma_1 \gamma_2^{-1} - \gamma_1 \gamma_2^{-1})]
\]

where $\Delta_{1jkh}'s$ are obtained by similar substitutions in (8) and $\alpha \in \mathbb{F}_q^m$.

Raising both sides of (9) to $q^5$ and rearranging the factors, we have a polynomial equation in $\gamma_1, \gamma_2$. If we assign the pair of indeterminates $X, Y$ to $\gamma_1, \gamma_2$ respectively, the resulting bi-variate equation has the form (for $\alpha \in \mathbb{F}_q^m$):

\[
\left[ (X^{[3]} Y^{[3]} - X^{[2]} Y^{[2]}) + (X^{[2]} Y^{[5]} - X^{[5]} Y^{[2]}) \right] \times \left[ (X^{[4]} Y^{[4]} - X^{[4]} Y^{[2]}) + (X^{[4]} Y^{[4]} - X^{[4]} Y^{[2]}) \right] = \alpha \left[ (X^{[3]} Y^{[2]} - X^{[2]} Y^{[3]} + (X^{[1]} Y - X Y^{[1]}) + (X^{[1]} Y - X Y^{[1]}) \right]
\]

To obtain alternative candidates for the original pair $(\gamma_1, \gamma_2)$, therefore, we will examine the set of roots of a modified version of the above equation.

5.2 Linear group action on the set of roots

Recall that in [1], the parameter $\gamma \in \mathbb{F}_q^m \setminus \mathbb{F}_q$, which spans the secret subspace $V = \{(1, \gamma)\}$, is a root of a polynomial $P_{\gamma}(X) = \sum_{\lambda = 2} \frac{1}{X^{\lambda}} Q_{\gamma}(X)$, where $Q_{\gamma}(X)$ has terms which are products of the form: $A(X) = X^{q^k} - X^{q^k}$. We term $P_{\gamma}(X)$ as the reduced polynomial for the case $\lambda = 2$, as this was obtained by removing all the linear factors over $\mathbb{F}_q$, with multiplicities, from $Q_{\gamma}(X)$. As formulated in [1], a valid alternative $\gamma'$ is obtained by the following map:

\[
PGL(2, q) \times \mathbb{P}(1, q) \rightarrow \mathbb{P}(1, q); \left( \begin{pmatrix} a & c \\ b & d \end{pmatrix}, [\gamma : 1] \right) \mapsto \left[ \frac{a \gamma + b}{c \gamma + d} \right] (11)
\]

where $ad - bc \neq 0$. As shown in [1], this map can be interpreted as the action of the projective linear group $PGL(2, q)$ on the projective space $\mathbb{P}(1, q)$, and any $\gamma' = \frac{a \gamma + b}{c \gamma + d}$ may be chosen for $\gamma$. Further, (cf. Lemma 6 and Proposition 5 in [1]) the transformation $\gamma \mapsto \frac{a \gamma + b}{c \gamma + d}$ fixes the roots of $A(X) = 0$. As $\gamma \in \mathbb{F}_q = \mathbb{F}_q$, this implies that the set of roots of $P_{\gamma}(X) = 0$ is fixed as well. This leads to the conclusion that any root of $P_{\gamma}(X)$ is a valid choice for the parameter $\gamma$. 
It is evident that the above action is a collineation in two variables \( x_1, x_2 \), representing the general basis elements of a 2-dimensional \( \mathcal{V} \), which leads to a linear fractional transformation of the ratio \( \gamma = \frac{x_2}{x_1} \). In the 3-dimensional case, we consider a collineation in three variables \( x_1, x_2, x_3 \), leading to a linear fractional transformation on the 2 ratios: \( \gamma_1 = \frac{x_2}{x_1} \) and \( \gamma_2 = \frac{x_3}{x_2} \) given by:

\[
\gamma_1' = \frac{a_{11}\gamma_1 + a_{12}\gamma_2 + a_{13}}{a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}}; \quad \gamma_2' = \frac{a_{21}\gamma_1 + a_{22}\gamma_2 + a_{23}}{a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}}.
\]

(12)

Similar to the defining map in (11), the coefficients in (12) form a \( 3 \times 3 \) matrix \( A = (a_{ij}) \) over \( \mathbb{F}_q \), with non-zero determinant.

One observes that the polynomial equation in (10), having \((\gamma_1, \gamma_2)\) as a root pair, is constituted of factors of the following form:

\[
f^{(i|j|k)}(X, Y) := (X^{[i]} - X^{[j]}Y^{[i]}) + (X^{[k]} - X^{[i]}Y^{[k]}) + (X^{[j]} - X^{[k]}Y^{[j]})
\]

(13)

It is required that the action induced by the ‘collineation matrix’ \( A \) should fix the set of roots of the polynomial of the form given in (10): a way to achieve that is to fix the set of roots of any term having the form given in (13). To that end we have the following lemma.

**Lemma 2** Under the transformations

\[
X \mapsto \frac{a_{11}X + a_{12}Y + a_{13}}{a_{31}X + a_{32}Y + a_{33}}; \quad Y \mapsto \frac{a_{21}X + a_{22}Y + a_{23}}{a_{31}X + a_{32}Y + a_{33}}; \quad a_{ij} \in \mathbb{F}_q,
\]

a polynomial \( f^{(i|j|k)}(X, Y) \) as given in Equation (13) is transformed to:

\[
\frac{\Delta_A}{(a_{31}X + a_{32}Y + a_{33})^{[i]+[j]+[k]}} f^{(i|j|k)}(X, Y)
\]

(14)

where \( \Delta_A \) is the determinant of \( A = (a_{ij}) \), a \( 3 \times 3 \) matrix over \( \mathbb{F}_q \).

**Proof** Under the transformations, all the terms of the following forms have zero coefficient.

1. \( X^{[i]+[j]+[k]} \), \( Y^{[i]+[j]+[k]} \);
2. \( X^{[a]+[b]}Y^{[c]}, Y^{[a]+[b]}X^{[c]} \), where \((a, b, c)\) are permutations of \((i, j, k)\);
3. \( X^{[a]}, Y^{[b]} \), where \( a \) and \( b \) run over \( i, j, k \).

The non-zero terms may be grouped as:

\( (X^{[i]} - X^{[j]}Y^{[i]}), (X^{[k]} - X^{[i]}Y^{[k]}), (X^{[j]} - X^{[k]}Y^{[j]}), (X^{[i]}Y^{[k]} - X^{[k]}Y^{[i]}), \) and \( (X^{[j]}Y^{[k]} - X^{[k]}Y^{[j]}), \)

each with coefficient:

\[
\frac{\Delta_A}{(a_{31}X + a_{32}Y + a_{33})^{[i]+[j]+[k]}}.
\]

It is evident from (10) that the polynomial equation \( \mathcal{F}(X, Y) \) satisfied by \((\gamma_1, \gamma_2)\) is of the following form:

\[
\mathcal{F}(X, Y) = f^{(i_1:j_1:k_1)}(X, Y)f^{(i_2:j_2:k_2)}(X, Y) - \alpha f^{(i_1:j_2:k_2)}(X, Y)f^{(i_2:j_1:k_1)}(X, Y)
\]

(15)
where \( i_l > j_l > k_l; \ l = 1, 2, \) with \( i_1 \geq i_2, \) the two sets of \((i, j, k)\)-indices being distinct, and \( \alpha \in \mathbb{F}_q^* \).

From Lemma [2] it follows that, under the stated transformations,

\[
\mathcal{F}(X, Y) \longmapsto \frac{\Delta_3^2}{(a_{31}X + a_{32}Y + a_{33})^2} \mathcal{F}(X, Y)
\]

(16)

where \( \Sigma := [i_1] + [j_1] + [k_1] + [i_2] + [j_2] + [k_2] \).

For any pair \((\gamma_1, \gamma_2)\) of \(V = (1, \gamma_1, \gamma_2)\) such that \(V \neq (1, \gamma_1, \gamma_2)\) is a 3-dimensional vector space over \(\mathbb{F}_q\), we have: \((a_{31} \gamma_1 + a_{32} \gamma_2 + a_{33}) \neq 0\) when the \(a_{ij}\)’s from \(\mathbb{F}_q\) are not all zero.

As any root pair of \(\mathcal{F}(X, Y)\) sends \([\Delta_3^2/(a_{31}X + a_{32}Y + a_{33})] \mathcal{F}(X, Y)\) to zero, the semilinear transformation on the two original basis elements \(\{\gamma_1, \gamma_2\}\) produces another pair of basis elements which satisfies the same equation \(\mathcal{F}(X, Y)\). In the 2-dimensional case, the action of \(PGL(2, q)\) is sharply transitive on the points of \(PG(1, q)\). Hence one could conclude that all the roots of the reduced polynomial \(P_\gamma(X)\) for the single parameter \(\gamma\) belonged to the single orbit of the action. In the 3-dimensional case, we have established that the action of \(PGL(3, q)\) on the points of \(PG(2, q)\) indeed maps one root of the initial polynomial \(\mathcal{F}(X, Y)\) to another. We next construct a counterpart of the reduced polynomial \(P_\lambda(X)\) that is analogously obtained from \(\mathcal{F}(X, Y)\).

5.3 The reduced polynomial for \(\lambda = 3\)

We first analyze the construction of the reduced polynomial \(P_\lambda(X)\) in the 2-dimensional case. To that end we have the following proposition.

**Proposition 2** Denote the polynomial \(Q_\gamma(X)\) as \(Q_\gamma(X) = f_1(X) - \alpha q^2 f_2(X)\) where \(f_1(X) := (X^{q^3} - X^q)(X^{q^2} - X)\) and \(f_2(X) := (X^{q^3} - X)(X^{q^2} - X^q)\) and \(\alpha \in \mathbb{F}_q^*\). Then

\[
P_\gamma(X) = \frac{Q_\gamma(X)}{\gcd(f_1(X), f_2(X))}
\]

**Proof** As \((X^{q^3} - X^q) = (X^{q^3} - X)^q\), the roots of \(f_1\) are the elements of \(\mathbb{F}_{q^2}\), each counted with multiplicity \(q + 1\).

Further, \((X^{q^3} - X)\) is the defining equation of \(\mathbb{F}_{q^3}\) and \((X^{q^3} - X^q) = (X^q - X)^q\). Thus the roots of \(f_2\) are the elements of \(\mathbb{F}_{q^3}\) and the elements of \(\mathbb{F}_{q^2}\), the latter counted with multiplicity \(q\). As \(\mathbb{F}_{q^3} \cap \mathbb{F}_{q^2} = \mathbb{F}_q\), it follows that

\[
\gcd(f_1(X), f_2(X)) = (X^q - X)^{q+1}.
\]

We next attempt a similar reduction of the initial polynomial \(\mathcal{F}(X, Y)\), by first identifying the constituent polynomials as follows.

\[
\mathcal{F}(X, Y) = f_1(X, Y) f_2(X, Y) - \alpha f_3(X, Y) f_4(X, Y)
\]
where

\[ f_1(X, Y) = [(X^{[5]}Y^{[3]} - X^{[3]}Y^{[5]}) + (X^{[3]}Y^{[2]} - X^{[2]}Y^{[3]}) + (X^{[2]}Y^{[5]} - X^{[5]}Y^{[2]})] \]

\[ f_2(X, Y) = [(X^{[4]}Y^{[1]} - X^{[1]}Y^{[4]}) + (X^{[1]}Y - XY^{[1]}) + (XY^{[4]} - X^{[4]}Y)] \]

\[ f_3(X, Y) = [(X^{[0]}Y^{[1]} - X^{[1]}Y^{[5]}) + (X^{[1]}Y - XY^{[1]}) + (X^{[5]}Y - X^{[5]}Y)] \]

\[ f_4(X, Y) = [(X^{[4]}Y^{[3]} - X^{[3]}Y^{[4]}) + (X^{[3]}Y^{[2]} - X^{[2]}Y^{[3]}) + (X^{[2]}Y^{[4]} - X^{[4]}Y^{[2]})] \].

(18)

In order to reduce the initial polynomial, we will prove the following theorem on the existence of a common factor based on subsequent lemmas.

**Theorem 5** The initial polynomial \( F(X, Y) \) has a factor of the following form:

\[
\left[ \prod_{a \in \mathbb{F}_q} (X + a) \prod_{b, c \in \mathbb{F}_q} (bX + Y + c) \right]^{q^2+1}
\]

(19)

The first lemma towards proving the theorem deals with the polynomials \( f_2(X, Y) \) and \( f_3(X, Y) \).

**Lemma 3** The polynomials \( f_2(X, Y) \) and \( f_3(X, Y) \) are divisible by

\[ f_0(X, Y) = \prod_{a \in \mathbb{F}_q} (X + a) \prod_{b, c \in \mathbb{F}_q} (bX + Y + c) \]

*Proof* Examining the zeroes of the linear polynomials, it is readily established that every factor of the form \( X + a, a \in \mathbb{F}_q \), or \( bX + Y + c, b, c \in \mathbb{F}_q \), divides each of the polynomials: \( f_2(X, Y) \) and \( f_3(X, Y) \). Both the \( X \)-degree and \( Y \)-degree of \( f_0(X, Y) \) equal \( q^2 \), while those for \( f_2 \) and \( f_3 \) are \( q^4 \) and \( q^5 \), respectively. The total degree of \( f_0 \) is \( q + q(q - 1) + q = q^2 + q \), which is again less than \( q^4 + q \) for \( f_2 \) and \( q^5 + q \) for \( f_3 \). Hence the lemma.

\( \square \)

Next we examine the polynomial \( f_4(X, Y) \) and prove that it divides \( f_5(X, Y) \).

**Lemma 4** The polynomial \( f_4(X, Y) = -[f_0(X, Y)]^{q^2} \) where \( f_0(X, Y) \) is the product of linear factors as defined in Lemma 3.

**Lemma** 4 The polynomial \( f_4(X, Y) = -[f_0(X, Y)]^{q^2} \) where \( f_0(X, Y) \) is the product of linear factors as defined in Lemma 3.
Proof Clearly $\prod_{a \in \mathbb{F}_q} (X + a) = X^q - X$.

We further have:

$$
\prod_{b,c \in \mathbb{F}_q} (bX + Y + c) = \prod_{b \in \mathbb{F}_q} \prod_{c \in \mathbb{F}_q} ((bX + Y) + c)
= \prod_{b \in \mathbb{F}_q} ((bX + Y)^q - (bX + Y))
= \prod_{b \in \mathbb{F}_q} ((Y^q - Y) + b(X^q - X))
= (X^q - X)^q \prod_{b \in \mathbb{F}_q} (Z + b), Z := \frac{Y^q - Y}{X^q - X}
= (X^q - X)^q (Z^q - Z)
= ((Y^q - Y)^q - (X^q - X)^q - 1 (Y^q - Y))
= ((Y^{q^2} - Y^q) - (X^q - X)^{q - 1} (Y^q - Y)).
$$

Thus it follows that:

$$
f_0(X, Y) = (X^q - X)((Y^{q^2} - Y^q) - (X^q - X)^q - 1 (Y^q - Y))
= ((Y^{q^2} - Y^q)(X^q - X) - (X^q - X)^q (Y^q - Y)).
$$

Therefore, raising to the $q^2$-th power, we obtain:

$$
[f_0(X, Y)]^{q^2} = [(Y^{q^2} - Y^q)(X^q - X) - (X^q - X)^q (Y^q - Y)]^{q^2}
= [Y^{q^2}X^q - X^q Y^q + Y^q X - X^q Y + Y X^q - Y^q X]^{q^2}
= -[X^{[4]} Y^{[3]} - X^{[3]} Y^{[4]} + X^{[3]} Y^{[2]} - X^{[2]} Y^{[3]} + X^{[2]} Y^{[4]} - X^{[4]} Y^{[2]}] .
\]$$

Lemma 5 The polynomial $f_4(X, Y)$ divides $f_1(X, Y)$; consequently $f_1$ contains all the factors of $f_0(X, Y)$ with multiplicity at least $q^2$.

Proof The polynomial $f_1(X, Y)$ can be rewritten in the following form:

$$
f_1(X, Y) = -[(Y^{q^2} - Y^q)(X^q - X) - (X^q - X)^q (Y^q - Y)]^{q^2}
$$

Clearly $\prod_{a \in \mathbb{F}_q} (X + a) = X^q - X$ is a factor of the polynomial within the brackets on the r.h.s.

It can be shown that any pair $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$, which is a zero of any linear factor of the form $bX + Y + c, b, c \in \mathbb{F}_q$, is a zero of the bracketed polynomial as well. Taking into account the degree of the bracketed polynomial, one can conclude that $[f_0(X, Y)]^{q^2}$ divides $f_1(X, Y)$.

The assertions then follow from Lemma 4.

\[\square\]
Proof of Theorem 5
It follows from the preceding lemmas that both the terms $f_1(X,Y)f_2(X,Y)$ and $f_3(X,Y)f_4(X,Y)$ contain $[f_0(X,Y)]^{q^2+1}$ as a factor where

$$f_0(X,Y) = \prod_{a \in \mathbb{F}_q} (X + a) \prod_{b,c \in \mathbb{F}_q} (bX + Y + c)$$

This proves the theorem.

In view of Theorem 5, we define the reduced polynomial $P_r(X,Y)$ for our case as follows.

Definition 1 The reduced polynomial for $\lambda = 3$ is defined by:

$$P_r(X,Y) = \frac{F(X,Y)}{\prod_{a \in \mathbb{F}_q} (X + a) \prod_{b,c \in \mathbb{F}_q} (bX + Y + c)}^{q^2+1}$$

Before moving on to the final steps of key-recovery for $\lambda = 3$, we present a brief comparison of the reduced polynomials $P_r(X)$ and $P_r(X,Y)$ in the form of a few observations as follows.

1. The reduced polynomial $P_r(X)$, for the case $\lambda = 2$, was obtained in [1] from the initial polynomial $Q_\gamma(X)$ by dividing out the factor $(X^q - X)^{q+1}$. This is equivalent to factoring out all distinct linear polynomials over $\mathbb{F}_q$, each with multiplicity $q + 1$. The polynomial $P_r(X,Y)$ is obtained as the result of an analogous reduction on the initial polynomial $F(X,Y)$ by factoring out all the distinct linear polynomials in $X, Y$ over $\mathbb{F}_q$, each with multiplicity $q^2 + 1$ (cf. Theorem 5).

2. The degree of $P_r(X)$ matches exactly with the cardinality of $PGL(2,q)$. However, for $\lambda = 3$, the total degree of $F(X,Y)$ is $q^5 + q^4 + q^3 + q$, which is reduced by $(q^2 + q)(q^2 + 1) = q^4 + q^3 + q^2 + q$ to yield $q^5 - q^2$. In this case, the total degree of the reduced polynomial does not equal but divides $|PGL(3,q)| = q^8 - q^6 - q^5 + q^3$.

3. The reduction factor in the case $\lambda = 2$ was precisely the gcd of the two additive components of the initial polynomial $Q_\gamma(X)$. In dealing with $F(X,Y)$, one possible way of reduction would have been to use a Gröbner basis of the ideal generated by the additive components $f_1(X,Y)f_2(X,Y)$ and $f_3(X,Y)f_4(X,Y)$. Instead we have extracted a common factor and proceeded to reduce $F(X,Y)$ with it. But our simulations for small field sizes using Sage ([11]) suggest that this factor is indeed the greatest common divisor over $\mathbb{F}_q$ of the additive components in the sense of polynomial factorization (cf. for instance, [6]). So we have the following Conjecture:

Conjecture: The polynomials $f_1(X,Y)f_2(X,Y)$ and $f_3(X,Y)f_4(X,Y)$ in $\mathbb{F}_q[X,Y]$ have a greatest common factor given by $[f_0(X,Y)]^{q^2+1}$. 
5.4 Completion of Key-recovery

We begin outlining the final steps of the key-recovery by first examining the action of \( PGL(3, q) \) on the roots of the reduced polynomial \( P_r(X, Y) \) defined in (20).

In particular, we consider the action on the defining root pair \((\gamma_1, \gamma_2)\) such that \(\gamma_1, \gamma_2 \in \mathbb{F}_q^m \setminus \mathbb{F}_q\), with \(\dim_{\mathbb{F}_q} \langle 1, \gamma_1, \gamma_2 \rangle = 3\), are used to define the initial polynomial \( F(X, Y) \) (cf. Subsection 5.2).

**Proposition 3** Let \((\gamma_1, \gamma_2)\) be the defining root pair of \( P_r(X, Y) \). Then the following action of \( PGL(3, q) \) as defined in Lemma 3 specified by the matrix \( A = (a_{ij}) \in GL_3(\mathbb{F}_q)\), maps \((\gamma_1, \gamma_2)\) to another root of \( P_r(X, Y) \):

\[
\gamma_1 \mapsto \frac{a_{11}\gamma_1 + a_{12}\gamma_2 + a_{13}}{a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}}; \quad \gamma_2 \mapsto \frac{a_{21}\gamma_1 + a_{22}\gamma_2 + a_{23}}{a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}}.
\]

**Proof** Enough to prove that the pair \((\gamma'_1, \gamma'_2)\), defined as follows, is a root.

\[
\gamma'_1 = \frac{a_{11}\gamma_1 + a_{12}\gamma_2 + a_{13}}{a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}}; \quad \gamma'_2 = \frac{a_{21}\gamma_1 + a_{22}\gamma_2 + a_{23}}{a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}}.
\]

We have: \( P_r(X, Y) = F(X, Y)/G(X, Y) \), with (cf. Lemma 4)

\[
G(X, Y) = [f_0(X, Y)]^{2^{s+1}} = f(X, Y)f_4(X, Y)
\]

where

\[
f(X, Y) = [X^{q^2}Y^q - X^qY^{q^2} + X^{q^2}Y - XY^{q^2} - X^{q^2}Y];
\]

\[
f_4(X, Y) = [X^{[4]}Y^{[3]} - X^{[3]}Y^{[4]} + X^{[3]}Y^{[2]} - X^{[2]}Y^{[3]} + X^{[2]}Y^{[4]} - X^{[4]}Y^{[2]}].
\]

If we perform the given transformations substituting \(X\) for \(\gamma_1\) and \(Y\) for \(\gamma_2\), then the application of Lemma 2 yields:

\[
F(X, Y) \mapsto \frac{\Delta_A}{(a_{31}X + a_{32}Y + a_{33})^{q^s+q^{s+1}}} f(X, Y);
\]

\[
f_4(X, Y) \mapsto \frac{\Delta_A}{(a_{31}X + a_{32}Y + a_{33})^{q^s+q^{s+1}+q^2}} f_4(X, Y);
\]

\[
F(X, Y) \mapsto \frac{\Delta_A}{(a_{31}X + a_{32}Y + a_{33})^{q^s+q^{s+1}+q^2+q+1}} F(X, Y)
\]

Hence, under the transformations,

\[
\frac{1}{(a_{31}X + a_{32}Y + a_{33})^{q^s+q^{s+1}}} F(X, Y) f_4(X, Y)
\]

\[
= \frac{1}{(a_{31}X + a_{32}Y + a_{33})^{q^s+q^{s+1}}} P_r(X, Y).
\]

Reverting to \(\gamma_1, \gamma_2\) we, therefore, have:

\[
P_r(\gamma'_1, \gamma'_2) = \frac{1}{(a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33})^{q^s+q^{s+1}}} P_r(\gamma_1, \gamma_2).
\]

Given that \((a_{31}\gamma_1 + a_{32}\gamma_2 + a_{33}) \neq 0\) from the definition of \(\gamma_1, \gamma_2\), the proposition follows.
The above result indicates that we could proceed with a root pair, say \((γ'_1, γ'_2)\), of the polynomial \(P_r(X, Y)\) to extract the tuple \(\{g'_0, g'_1, g'_2, γ'_1, γ'_2\}\) for key-recovery. For the sake of completeness, we briefly outline the key steps in the Coggia-Couvreur attack for \(λ = 3\) as follows.

1. Relating \(g'_0, g'_1, g'_2\) to known parameters: Let

\[
γ_1 = \frac{b_{11}γ'_1 + b_{12}γ'_2 + b_{13}}{b_{31}γ'_1 + b_{32}γ'_2 + b_{33}}; \quad γ_2 = \frac{b_{21}γ'_1 + b_{22}γ'_2 + b_{23}}{b_{31}γ'_1 + b_{32}γ'_2 + b_{33}}
\]

for some \(B = (b_{ij}) \in GL_3(\mathbb{F}_q)\).

Then we can obtain expressions for \(g'_0, g'_1, g'_2\) in terms of \(g_0, g_1, g_2\) and \(γ'_1, γ'_2\) in the manner of Proposition 1, from the equation:

\[
g'_0 + γ'_1g'_1 + γ'_2g'_2 = g_0 + γ_1g_1 + γ_2g_2.
\]

2. Solving for \(g'_0, g'_1, g'_2\): The quantities \(u_{123}, v_{123}\) defined in Subsection 5.1 are used to compute \((g'_0 + γ'_1\cdot g'_1 + γ'_2\cdot g'_2)\) and \((g'_0 + γ'_1\cdot g'_1 + γ'_2\cdot g'_2)\) (vide Lemma [2]). Using, in addition, the known vector \(g'_0 + γ'_1g'_1 + γ'_2g'_2\), we can extract \(g'_0, g'_1, g'_2\).

3. The previous steps outline the recovery of an alternate key in the form of the tuple \(\{g'_0, g'_1, g'_2, γ'_1, γ'_2\}\). Using this alternate key in the formulation of Subsection 3.1, we can compute the dual \(C_{pub}^\perp\) in a similar manner as presented in [1], and hence, decrypt the ciphertext.

6 Conclusion

We have extended the key-recovery attack on Loidreau’s rank-metric scheme, which was proposed by Coggia and Couvreur and proven for dimension parameter \(λ = 2\), to cases with \(λ > 2\). Specifically, we have detailed the steps to identify the non-random structure (the so-called “distinguisher”) of the dual of the public code, denoted \(C_{pub}^\perp\) for all values of \(λ ≥ 3\). Further, we have extended the key-recovery attack to \(λ = 3\).

This expands a successful attack on Loidreau’s scheme when the underlying code rate is \(≥ 1 - \frac{1}{λ}\). It will be worthwhile to attempt a modification of the attack to work for lower rate codes as well, especially for increasing values of \(λ\). In another direction, Loidreau’s rank-metric scheme claims resistance to Overbeck-type attacks, among a few other proposals. It is certainly of interest to revisit the formulation of “distinguishers” and key-recovery attacks on the other Overbeck-resistant rank-metric schemes in the light of this success against Loidreau’s scheme.

Acknowledgements The author would like to thank Arnab Chakraborty and Mridul Nandi for several helpful discussions.

References

1. Coggia, D., Couvreur, A.: On the security of a loidreau rank metric code based encryption scheme. arXiv preprint arXiv:1903.02933v1, v2 (2019, 2020)
2. Faure, C., Loidreau, P.: A new public-key cryptosystem based on the problem of reconstructing \( p \)-polynomials. In: International Workshop on Coding and Cryptography, pp. 304–315. Springer (2005)

3. Gabidulin, E.M., Paramonov, A., Tretjakov, O.: Ideals over a non-commutative ring and their application in cryptography. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 482–489. Springer (1991)

4. Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography WCC, vol. 2013 (2013)

5. Gaborit, P., Otmani, A., Kalachi, H.T.: Polynomial-time key recovery attack on the faure-loidreau scheme based on gabidulin codes. Designs, Codes and Cryptography 86(7), 1391–1403 (2018)

6. von zur Gathen, J., Gerhard, J.: Modern computer algebra. Cambridge university press (2013)

7. Loidreau, P.: A new rank metric codes based encryption scheme. In: International Workshop on Post-Quantum Cryptography, pp. 3–17. Springer (2017)

8. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. DSN Progress Report pp. 42–44 (1978)

9. Overbeck, R.: Structural attacks for public key cryptosystems based on gabidulin codes. Journal of cryptology 21(2), 280–301 (2008)

10. Puchinger, S., Renner, J., Wachter-Zeh, A.: Twisted gabidulin codes in the gpt cryptosystem. arXiv preprint arXiv:1806.10055 (2018)

11. Stein, W., et al.: Sage Mathematics Software (Version 7.5.1). The Sage Development Team (2017). http://www.sagemath.org

12. Wachter-Zeh, A., Puchinger, S., Renner, J.: Repairing the faure-loidreau public-key cryptosystem. In: 2018 IEEE International Symposium on Information Theory (ISIT), pp. 2426–2430. IEEE (2018)