A note on invariant linear transformations in multivariate public key cryptography

Andreas Wiemers *

1 Introduction

Imai and Matsumoto [1] introduced a public key cryptosystem based on multivariate quadratic polynomials. In a simplified way, the essence of their cryptosystem can be described in the following way: Start with a central monomial of the form

$$F(x) = x^{q^t+1}$$

The secret key comprises two invertible linear transformations T and L such that

$$T \circ F \circ L$$

is the public key. In order to study equivalent public keys it is natural to ask for the "invariant" secret keys (T, L), i.e.

$$T \circ F \circ L = F$$

Lin, Faugere, Perret and Wang [2, Theorem 8] give a partial answer to this question by considering such L which fulfill

$$F \circ L = F$$

In this paper we will determine all invariant invertible linear transformations (T, L).

2 Preliminaries

Let K be a finite field with q elements. R is an extension field over K of degree n. We write explicitely

$$R = K[S]/ < g(S) >$$

where $g(S)$ is an irreducible polynomial of degree n. We denote by s the image of S in R. R is a n-dimensional vector space over K. We set concretely

$$\phi : K^n \longrightarrow R \qquad (a_0, \dots, a_{n-1}) \mapsto a_0 + a_1 s + \dots + a_{n-1} s^{n-1}$$

*Federal Office for Information Security, Germany

As in [2] we denote by $\mathcal{F}$ the set of all mappings from R to R of the form

$$x \mapsto \sum_{0 \le i \le j \le n-1} \alpha_{i,j} x^{q^i + q^j} \qquad \text{where } \alpha_{i,j} \in R$$

$\mathcal{L}$ denotes the set of all invertible linear mappings from R to R of the form

$$x \mapsto \sum_{0 \le i \le n-1} \beta_i x^{q^i} \qquad \text{where } \beta_i \in R$$

3 The Main Result

We will prove a result which extends Theorem 8 in [2].
Theorem: *Let $F(x) = ax^{q^i+1}$ with $a \in R^*$ and $1 \le i \le n-1$. Assume we have mappings L and T in $\mathcal{L}$ with*

$$T \circ F \circ L = F$$

Then only one of the following cases can occur:

1. *Case:* $4i \equiv 0 \bmod n$ *and* $2i \neq n$:

$$\begin{aligned} L(x) &= cx^{q^r} + dx^{q^{r+2i}} \qquad \textit{where } c, d \in R^*, 0 \le r \le n-1 \\ T^{-1}(x) &= c^{q^i+1}x^{q^r} + cd^{q^i}x^{q^{r+3i}} + c^{q^i}dx^{q^{r+i}} + d^{q^i+1}x^{q^{r+2i}} \end{aligned}$$

2. *Case:* $2i = n$:

$$L(x) = cx^{q^r}, T^{-1}(x) = (c^{q^i+1} - d)x^{q^{r+n/2}} + dx^{q^r} \qquad \textit{where } c \in R^*, d \in R, 0 \le r \le n-1$$

3. *Case:*

$$L(x) = cx^{q^r}, T^{-1}(x) = c^{q^i+1}x^{q^r} \qquad \textit{where } c \in R^*, 0 \le r \le n-1$$

Notes:

1. The result in [2, Theorem 8] is covered by assuming in addition $T^{-1}(x) = x$. This implies in case 2

$$r = 0, d = 0, c^{q^i+1} = 1$$

whereas in case 3 we have

$$r = 0, c^{q^i+1} = 1$$

2. As an example for new cases compared to [2] that can occur, consider

$$F(x) = x^{q+1}, L(x) = cx + dx^{q^2}, n = 4$$

Then we have

$$F(L(x)) = c^{q+1}F(x) + cd^q F(x)^{q^3} + c^q dF(x)^q + d^{q+1}F(x)^{q^2}$$

3. Not every combination of c and d is possible. For instance, the condition "L is invertible" in case 1 is equivalent to the validity of the inequation

$$(-c/d)^{q^{n/2}+1} \neq 1$$

4. In case 1, T must be invertible. This is equivalent to the condition that the linear transformation

$$a_0 Y + a_1 Y^{q^i} + a_2 Y^{q^{2i}} + a_3 Y^{q^{3i}} \in R[Y]$$

in invertible where

$$a_0 = c^{q^i+1}, a_1 = c^{q^i}d, a_2 = d^{q^i+1}, a_3 = d^{q^i}c$$

We set $p = q^{n/4}$. p is the order of the subfield R_4 of index 4 in R.
If $i = n/4$, we can directly apply [3, p. 362] to the linear transformation

$$\begin{aligned} & a_0 Y + a_1 Y^{q^i} + a_2 Y^{q^{2i}} + a_3 Y^{q^{3i}} \\ = \; & a_0 Y + a_1 Y^p + a_2 Y^{p^2} + a_3 Y^{p^3} \end{aligned}$$

Therefore, T is invertible if and only if the determinant of the matrix

$$A = \begin{pmatrix} a_0 & a_3^p & a_2^{p^2} & a_1^{p^3} \\ a_1 & a_0^p & a_3^{p^2} & a_2^{p^3} \\ a_2 & a_1^p & a_0^{p^2} & a_3^{p^3} \\ a_3 & a_2^p & a_1^{p^2} & a_0^{p^3} \end{pmatrix}$$

does not vanish. In case that $c, d \in R_4$, this determinant is in a simple form, since then A is circular. We compute

$$\text{case } i = n/4; c, d \in R_4 : \det(A) \neq 0 \iff c \neq \pm d$$

If $i = 3n/4$, we apply [3, p. 362] to the linear transformation

$$\begin{aligned} & a_0 Y + a_1 Y^{q^i} + a_2 Y^{q^{2i}} + a_3 Y^{q^{3i}} \\ = \; & a_0 Y + a_3 Y^p + a_2 Y^{p^2} + a_1 Y^{p^3} \end{aligned}$$

so that we have a similar condition for the matrix A', where we exchange a_1 and a_3 in A. In case that $c, d \in R_4$, we compute the same result

$$\text{case } i = 3n/4; c, d \in R_4 : \det(A') \neq 0 \iff c \neq \pm d$$

Proof of the main theorem: It suffices to prove the result for $a = 1$. We extend the Frobenius mapping

$$\tau : R \longrightarrow R \qquad x \mapsto x^q$$

trivially to the polynomial ring $R[X_0, \ldots, X_{n-1}]$

$$\tau : R[X_0, \ldots, X_{n-1}] \longrightarrow R[X_0, \ldots, X_{n-1}]$$

τ is an isomorphism of rings which acts only on the coefficients.We set

$$Z = X_0 + X_1 s + \cdots + X_{n-1} s^{n-1}$$

$F = x^{q^i+1}$ induces via ϕ a mapping from K^n to R. As this mapping, F can be written in the form of the polynomial

$$\tau^i(Z)Z \in R[X_0, \ldots, X_{n-1}]$$

In the same way, the mapping

$$L(x) = \sum_{0 \leq j \leq n-1} \beta_j x^{q^j}$$

can be written as mapping from K^n to R in the form of the polynomial

$$\sum_{0 \leq j \leq n-1} \beta_j \tau^j(Z) \in R[X_0, \ldots, X_{n-1}]$$

Similarly, we can write the mapping

$$T^{-1}(x) = \sum_{0 \leq j \leq n-1} \gamma_j x^{q^j}$$

as polynomial

$$\sum_{0 \leq j \leq n-1} \gamma_j \tau^j(Z) \in R[X_0, \ldots, X_{n-1}]$$

The equation

$$F \circ L = T^{-1} \circ F$$

implies that the polynomial

$$\delta = \tau^i\Big(\sum_{0 \leq j \leq n-1} \beta_j \tau^j(Z)\Big) \cdot \sum_{0 \leq j \leq n-1} \beta_j \tau^j(Z) - \sum_{0 \leq j \leq n-1} \gamma_j \tau^j(\tau^i(Z)Z)$$

is - as mapping from K^n to R - identical to 0. It is well known that every $h \in K[X_0, \ldots, X_{n-1}]$ that is identical to 0 as a mapping from K^n to K lies in the ideal

$$< X_0^q - X_0, \ldots X_{n-1}^q - X_{n-1} >$$

over $K[X_0, \ldots, X_{n-1}]$. See for example [3, Lemma 7.40]. This immediately implies that also

$$\delta \in < X_0^q - X_0, \ldots X_{n-1}^q - X_{n-1} >$$

where the right hand side is meant as an ideal over $R[X_0, \ldots, X_{n-1}]$. But δ is homogenous of degree 2. Therefore, $\delta = 0$ as polynomial in $R[X_0, \ldots, X_{n-1}]$ and we have the equation over $R[X_0, \ldots, X_{n-1}]$

$$\tau^i(\sum_{0 \le j \le n-1} \beta_j \tau^j(Z)) \cdot \sum_{0 \le j \le n-1} \beta_j \tau^j(Z) = \sum_{0 \le j \le n-1} \gamma_j \tau^{i+j}(Z) \tau^j(Z)$$

$\tau^j(Z)$ is the image of $(X_0, \ldots, X_{n-1})$ under the Vandermonde matrix with entries

$$\tau^j(s^i)$$

This matrix is invertible since the elements $\tau^j(s)$ are pairwise different. We define a transformation of variables by this matrix, i.e. we set

$$Y_j = \tau^j(Z)$$

in $R[Y_0, \ldots, Y_{n-1}]$. We write the equation above in the new variables

$$(\sum_{0 \le j \le n-1} \tau^i(\beta_j) Y_{i+j}) \cdot \sum_{0 \le j \le n-1} \beta_j Y_j = \sum_{0 \le j \le n-1} \gamma_j Y_{i+j} Y_j$$

(Indices are modulo n.) The rest of the proof follows now from the validity of this equation in an elementary, but rather tedious way: We set

$$\epsilon_t = \tau^i(\beta_{t-i})$$

so that

$$\sum_{0 \le j \le n-1} \epsilon_j Y_j = \sum_{0 \le j \le n-1} \tau^i(\beta_j) Y_{i+j}$$

We fix an index r with coefficient $\beta_r \neq 0$. This implies

$$\epsilon_r = 0$$

since the monomial Y_r^2 does not appear on the right side of the equation. We write the left side of the equation as sum of monomials with certain cofficients. The monomials of the form $Y_r Y_j$ with $j \neq r$, $0 \le j \le n-1$, in this sum have the coefficient

$$\epsilon_j \beta_r$$

Because of the structure of the right side of the equation, we get $\epsilon_j = 0$ unless $j = r + i$ or $j = r - i$. This implies that in the sum

$$\sum_{0 \le j \le n-1} \beta_j Y_j$$

at most two coefficients do not vanish. Therefore, we assume that we have

$$\beta_r \neq 0 \text{ and } \beta_s \neq 0$$

for $r \neq s$. The left side of the equation above now reads

$$\begin{aligned} & (\tau^i(\beta_r)Y_{r+i} + \tau^i(\beta_s)Y_{s+i})(\beta_r Y_r + \beta_s Y_s) \\ = \; & \tau^i(\beta_r)Y_{r+i}\beta_r Y_r + \tau^i(\beta_r)Y_{r+i}\beta_s Y_s + \tau^i(\beta_s)Y_{s+i}\beta_r Y_r + \tau^i(\beta_s)Y_{s+i}\beta_s Y_s \end{aligned}$$

Considering the structure of the right side of the equation, this immediately implies

$$r + i - s \equiv -i \bmod n \text{ and } s + i - r \equiv -i \bmod n$$

This gives the condition

$$4i \equiv 0 \bmod n \text{ and } s \equiv r + 2i \bmod n$$

and in addition $2i \neq n$. The left side of the equation above now reads

$$\tau^i(\beta_r)\beta_r Y_{r+i}Y_r + \tau^i(\beta_r)\beta_s Y_{r+i}Y_{r+2i} + \tau^i(\beta_s)\beta_r Y_{r+3i}Y_r + \tau^i(\beta_s)\beta_s Y_{r+3i}Y_{r+2i}$$

Therefore, the γ_j are uniquely defined and the claim of case 1 follows.
If in the sum

$$\sum_{0 \leq j \leq n-1} \beta_j Y_j$$

exactly one coefficient does not vanish, then the equation above reads

$$\tau^i(\beta_r)\beta_r Y_{r+i}Y_r = \sum_{0 \leq j \leq n-1} \gamma_j Y_{i+j} Y_j$$

Let us assume that $2i \neq n$. Then, all the monomials in the sum on the right side of this equation are different. This implies directly the claim of case 3.
If $i = n/2$, we get the equation

$$\tau^i(\beta_r)\beta_r Y_{r+n/2}Y_r = \sum_{0 \leq j \leq n-1} \gamma_j Y_{n/2+j} Y_j = \gamma_r Y_{r+n/2} Y_r + \gamma_{r+n/2} Y_{r+n/2} Y_r$$

which gives the claim of case 2.

4 References

[1] Matsumoto, Imai: Public quadratic polnomial-tuples for efficient signature-verification and message-encryption, EUROCRYPT 1988, Lecture Notes in Comput. Science, Vol. 330, 1988, pp. 419-453.
[2] Lin, Faugere, Perret, Wang: On enumeration of polynomial equivalence classes and their application to MPKC, Finite Fields and Their Applications 18, 2012, pp. 283-302.
[3] Lidl, Niederreiter: Finite Fields, Vol. 20, Encyclopdia of Math. and its appl., Cambridge University Press, Cambridge 1997