Solving Some Affine Equations over Finite Fields

Sihem Mesnager\(^1\), Kwang Ho Kim\(^2,3\), Jong Hyok Choe\(^2\), and Dok Nam Lee\(^2\)

\(^1\) Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, University of Paris XIII, CNRS, LAGA UMR 7539, Sorbonne Paris Cité, 93430 Villetaneuse, France, and Telecom ParisTech 75013 Paris. Email: smesnager@univ-paris8.fr

\(^2\) Institute of Mathematics, State Academy of Sciences, Pyongyang, Democratic People’s Republic of Korea. Email: khk.cryptech@gmail.com

\(^3\) PGItech Corp., Pyongyang, Democratic People’s Republic of Korea.

Abstract. Let \(l\) and \(k\) be two integers such that \(l|k\). Define \(T_k^l(X) := X + X^{p^l} + \cdots + X^{p^{l(k/l - 2)}} + X^{p^{l(k/l - 1)}}\) and \(S_k^l(X) := X - X^{p^l} + \cdots + (-1)^{l(k/l - 1)}X^{p^{l(k/l - 1)}}\), where \(p\) is any prime.

This paper gives explicit representations of all solutions in \(\mathbb{F}_{p^n}\) to the affine equations \(T_k^l(X) = a\) and \(S_k^l(X) = a\), \(a \in \mathbb{F}_{p^n}\). For the case \(p = 2\) that was solved very recently in [7], the result of this paper reveals another solution.

Keywords: Affine equation · Finite field · Zeros of a polynomial · Linearized polynomial.

Mathematics Subject Classification. 11D04, 12E05, 12E12.

1 Introduction

Let \(\mathbb{F}_{p^n}\) be the finite field of \(p^n\) elements where \(p\) is a prime and \(n \geq 1\) is a positive integer. A polynomial \(L(X) \in \mathbb{F}_{p^n}[X]\) of shape

\[L(X) = \sum_{i=0}^{t} a_i X^{p^i}, a_i \in \mathbb{F}_{p^n}\]

is called a linearized polynomial over \(\mathbb{F}_{p^n}\). An affine equation over \(\mathbb{F}_{p^n}\) is an equation of type

\[L(X) = a, \tag{1}\]

where \(L\) is a linearized polynomial and \(a \in \mathbb{F}_{p^n}\).

Affine equations arise in many several different problems and contexts such as rank metric codes and linear sets. In particular, those involving the trace functions are crucial in many contexts of cryptography and error-correcting codes [1–3]. Recent research on linearized polynomials and related topics can be found
in [4, 5, 7, 8, 10]. However, to explicit the solutions of affine equations is often challenging as the ultimate goal of such study.

In this paper, we study the following two affine equations

\[ T^k_l(X) := \sum_{i=0}^{\frac{k}{l}-1} X^{ip^i} = a, \quad (2) \]

\[ S^k_l(X) := \sum_{i=0}^{\frac{k}{l}-1} (-1)^i X^{ip^i} = a, \quad (3) \]

where \( a \in \mathbb{F}_{p^n} \), \( k \) and \( l \) are positive integers such that \( l \mid k \).

It is well-known that a linearized polynomial induce a linear transformation of \( \mathbb{F}_{p^n} \) over \( \mathbb{F}_p \). In particular, if \( x_1 \) and \( x_2 \) are two solutions in \( \mathbb{F}_{p^n} \) to Equation (1), then their difference \( x_1 - x_2 \) is a zero of \( L \) in \( \mathbb{F}_{p^n} \), that is, their difference lies in the set \( \{ x \in \mathbb{F}_{p^n} \mid L(x) = 0 \} \), that we call the kernel of \( L \) restricted to \( \mathbb{F}_{p^n} \).

Determination of the \( \mathbb{F}_{p^n} \) -solutions to Equation (1) can therefore be divided into two problems: determining the kernel of \( L \) restricted to \( \mathbb{F}_{p^n} \) and explicit a particular solution \( x_0 \) in \( \mathbb{F}_{p^n} \). Indeed, if those two problems are solved then the set of all \( \mathbb{F}_{p^n} \)-solutions to Equation (1) is \( x_0 + \{ x \in \mathbb{F}_{p^n} \mid L(x) = 0 \} \).

In this paper, we solve these two problems for the linearized polynomials \( T^k_l \) and \( S^k_l \). We firstly determine the kernels of \( T^k_l \) and \( S^k_l \) in Section 3. Next, we give explicit representations of particular solutions to Equation (2) and Equation (3) in Section 4. As by-product of those results, we also characterize the elements \( a \) in \( \mathbb{F}_{p^n} \) for which Equation (2) and Equation (3) has at least one solution in \( \mathbb{F}_{p^n} \) in Section 4.

Remark 1. In [7], we considered the particular case of \( p = 2 \) for which \( T^k_l(X) = S^k_l(X) \). Interestingly, Theorem 1 and Theorem 4 in this paper provides another solution for this particular case.

2 Preliminaries

Throughout this paper, we maintain the following notations (otherwise, we will point out it at the appropriate place).

- \( p \) is any prime and \( n \) is a positive integer.
- \( a \) is any element of the finite field \( \mathbb{F}_{p^n} \).
- \( k \) and \( l \) are positive integers such that \( l \mid k \).
- We denote the greatest common divisor and the smallest common multiple of two positive integers \( u \) and \( v \) by \( (u, v) \) and \( [u, v] \), respectively.
- \( d := (n, k) \), \( e := (n, l) \) and \( L := [d, l] \).

We now present a lemma that will be frequently used throughout this paper.

Lemma 1. For any positive integers \( k, l \) and \( m \) with \( m \mid l \mid k \).
Lemma 2. The third items are similarly proved by using Item 2 of Lemma 1. 

Proof. The first three items are obtained by easy straightforward calculations. Hence, we give proofs only for the last two items. 

Since $nk = [n, k][d]$, one has $\frac{n}{d} = [\frac{n}{k}]$ and $\{jd \mid 0 \leq j \leq \frac{n}{d} - 1\} = \{ik \mod n \mid 0 \leq i \leq [\frac{n}{k}] - 1\}$ because $n$ divides $ik$ if and only if $i$ is a multiple of $\frac{n}{d} = [\frac{n}{k}]$. Therefore $T^{n,k}_{d}(x) = T^{n}_{d}(x)$. 

Furthermore, if $\frac{n}{d} = \frac{n}{k}$ is even, then $\frac{k}{k}$ is odd since it is prime to $\frac{n}{d}$. Thus, when two integers $i$ and $j$ are such that $jd = ik \mod n$, they have the same parity. This proves $S^{n,k}_{d}(x) = S^{n}_{d}(x)$ if $\frac{n}{d} = [\frac{n}{k}]$ is even. 

Finally, the last item is proved as follows: By Item 1, we have $S^{k}_{1}(x) = S^{2l}_{2l}(X)$. Let $x \in \mathbb{F}_{p}$. Then $y := T^{k}_{2l}(x) \in \mathbb{F}_{p^{2l}}$. Hence $S^{k}_{1}(x) + S^{k}_{1}(x)^{p^{l}} = S^{2l}_{2l}(y) + S^{2l}_{2l}(y)^{p^{l}} = (y - y^{p^{l}}) + (y - y^{p^{l}})^{p^{l}} = 0$. 

\[\Box\]

3 On the Kernels of $T^{k}_{l}$ and $S^{l}_{1}$

To determine the kernels of $T^{k}_{l}$ and $S^{l}_{1}$ in $\mathbb{F}_{p^{n}}$, we begin with determining the zeros of $T^{k}_{l}$ and $S^{l}_{1}$ in the algebraic closure $\overline{\mathbb{F}}_{p}$.

Lemma 2. It holds:

1. \[\{x \in \overline{\mathbb{F}}_{p} \mid T^{k}_{l}(x) = 0\} = S^{2l}_{2l}(\overline{\mathbb{F}}_{p^{2l}}) = \{x - x^{p^{l}} \mid x \in \mathbb{F}_{p^{2l}}\}.\]

2. When $\frac{k}{l}$ is even, 

\[\{x \in \overline{\mathbb{F}}_{p} \mid S^{l}_{1}(x) = 0\} = T^{2l}_{2l}(\overline{\mathbb{F}}_{p^{2l}}) = \{x + x^{p^{l}} \mid x \in \mathbb{F}_{p^{2l}}\}.\]

3. When $\frac{k}{l}$ is odd, 

\[\{x \in \overline{\mathbb{F}}_{p} \mid S^{l}_{1}(x) = 0\} = S^{2l}_{2l} \circ T^{2l}_{2l}(\overline{\mathbb{F}}_{p^{2l}}) = \{(x + x^{p^{l}}) - (x + x^{p^{l}})^{p^{l}} \mid x \in \mathbb{F}_{p^{2l}}\}.\]

Proof. For $x \in \mathbb{F}_{p^{n}}$, by Item 3 of Lemma 1, $T^{k}_{l} \circ S^{2l}_{2l}(x) = x = x^{p^{l}} = 0$ proving the inclusion of $S^{2l}_{2l}(\overline{\mathbb{F}}_{p^{2l}})$ in $\{x \in \overline{\mathbb{F}}_{p} \mid T^{k}_{l}(x) = 0\}$. Then we conclude the equality from the fact that the two sets have the same cardinality $p^{k-l}$. The second and third items are similarly proved by using Item 2 of Lemma 1. 

\[\Box\]
Based on the above lemma, we then deduce the kernels of $T^k$ and $S^k$ restricted to $F_{p^n}$. For the reader’s convenience, we present our results by three statements each corresponding to an item of Lemma 2.

**Theorem 1.** The following holds true:

\[ \{ x \in F_{p^n} \mid T^k(x) = 0 \} = \begin{cases} F_{p^d}, & \text{if } p \mid \frac{k}{T} \\ S^{2e}_c(F_{p^d}), & \text{otherwise.} \end{cases} \]

Consequently,

\[ \# \{ x \in F_{p^n} \mid T^k(x) = 0 \} = \begin{cases} p^d, & \text{if } p \mid \frac{k}{T} \\ p^{d-e}, & \text{otherwise.} \end{cases} \]

**Proof.** By Item 1 of Lemma 2,

\[ \{ x \in F_{p^n} \mid T^k(x) = 0 \} = S^2_t(F_{p^d}) \cap F_{p^n} \subset F_{p^{(a,k)}} = F_{p^d} \]

Therefore, by Item 1 of Lemma 1

\[ \{ x \in F_{p^n} \mid T^k(x) = 0 \} = \{ x \in F_{p^d} \mid T^k_T(x) = 0 \} \]

Thus, if $p \mid \frac{k}{T}$, then

\[ \{ x \in F_{p^d} \mid T^k_T(x) = 0 \} = F_{p^d}, \]

and if $p \nmid \frac{k}{T}$, then

\[ \{ x \in F_{p^d} \mid T^k_T(x) = 0 \} = S^{2e}_c(F_{p^d}) \]

(by Item 1 of Lemma 2).

\[ \square \]

**Theorem 2.** Suppose that $\frac{k}{T}$ is even.

1. If $\frac{d}{e}$ is even, then

\[ \{ x \in F_{p^n} \mid S^k_t(x) = 0 \} = \begin{cases} F_{p^d}, & \text{if } p \mid \frac{k}{T} \\ T^{2e}_c(F_{p^d}), & \text{otherwise.} \end{cases} \]

and consequently

\[ \# \{ x \in F_{p^n} \mid S^k_t(x) = 0 \} = \begin{cases} p^d, & \text{if } p \mid \frac{k}{T} \\ p^{d-e}, & \text{otherwise.} \end{cases} \]

2. If $\frac{d}{e}$ is odd, then

\[ \{ x \in F_{p^n} \mid S^k_t(x) = 0 \} = F_{p^d} \]

and consequently

\[ \# \{ x \in F_{p^n} \mid S^k_t(x) = 0 \} = p^d. \]
Proof. By Item 2 of Lemma 2, when \( k \) is even, we know that \( \{ x \in \mathbb{F}_{p^n} | S_k^k(x) = 0 \} = T^2_\ell(F_{p^n}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^d} \) and thus
\[
\{ x \in \mathbb{F}_{p^n} | S_k^k(x) = 0 \} = \{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \}.
\]

Now, suppose that \( \frac{d}{c} = \frac{d}{(d,l)} = \frac{L}{T} \) is even. Then, by Item 1 of Lemma 1
\[
\{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \{ x \in \mathbb{F}_{p^d} | T_L^L \circ S_L^L(x) = 0 \}
\]
\[
= \{ x \in \mathbb{F}_{p^d} | \frac{k}{L} T_L^L(x) = 0 \}.
\]

Therefore, if \( p \nmid \frac{k}{L} \), then
\[
\{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \mathbb{F}_{p^d},
\]
and if \( p \mid \frac{k}{L} \), then
\[
\{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \}
\]
\[
= \{ x \in \mathbb{F}_{p^d} | T_L^L \circ S_L^L(x) = 0 \} \quad \text{(by Item 4 of Lemma 1)}
\]
\[
= \{ x \in \mathbb{F}_{p^d} | S_d^d(x) = 0 \} \quad \text{(by Item 2 of Lemma 2)}.
\]

Suppose now that \( \frac{d}{c} = \frac{L}{T} \) is odd. In this case, \( \frac{k}{L} \) is even as \( \frac{k}{L} = \frac{k}{T} \cdot \frac{T}{L} \) is even by the assumption. Thus, we have
\[
\{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \}
\]
\[
= \{ x \in \mathbb{F}_{p^d} | T_L^L \circ S_L^L(x) = 0 \} \quad \text{(by Item 1 of Lemma 1)}
\]
\[
= \{ x \in \mathbb{F}_{p^d} | S_d^d(x) = 0 \} \quad \text{because } S_d^d(x) \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^d} \] for \( x \in \mathbb{F}_{p^d} \). \(\square\)

**Theorem 3.** Suppose that \( \frac{k}{T} \) is odd.

1. When \( \frac{k}{T} \) is odd,
\[
\{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \{ 0 \}
\]
and consequently
\[
\# \{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = 1.
\]

2. When \( \frac{k}{T} \) is even,
\[
\{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \begin{cases} 
S_d^d(F_{p^d}), & \text{if } p \mid \frac{k}{T} \\
S_d^d \circ T_{2c}^c(F_{p^d}), & \text{otherwise}
\end{cases}
\]
and consequently
\[
\# \{ x \in \mathbb{F}_{p^d} | S_k^k(x) = 0 \} = \begin{cases} 
p^d, & \text{if } p \mid \frac{k}{T} \\
p^d - c, & \text{otherwise}.
\end{cases}
\]
Proof. First of all, note that $\frac{d}{n}$ and $\frac{d}{l}$ are odd being divisors of odd $\frac{k}{n}$ and by Item 3 of Lemma 2 one has

$$\{x \in \mathbb{F}_{p^n} | S_1^k(x) = 0\} = S_1^{2k} \circ T_1^{2l}(\mathbb{F}_{p^{n+2k}}) \cap \mathbb{F}_{p^n} = \{x \in \mathbb{F}_{p^{n+2k}} | S_1^k(x) = 0\}.$$ 

Suppose that $\frac{n}{n}$ is odd. Then, $(n, 2k) = d$ and we have

$$\{x \in \mathbb{F}_{p^n} | S_1^k(x) = 0\} = \{x \in \mathbb{F}_{p^n} | S_1^k(x) = 0\} = \{x \in \mathbb{F}_{p^n} | S_1^k(x) = 0\} \text{ (by Item 1 of Lemma 1)}$$

$$(S_1^{2L} \circ T_1^{2l}(\beta)) = \{S_1^{2L} \circ T_1^{2l}(\beta) = 0\} \text{ (by Item 3 of Lemma 2)}.$$ 

Now, suppose that $\frac{n}{n}$ is odd. Then, $(n, 2k) = 2d$ and

$$\{x \in \mathbb{F}_{p^n} | S_1^k(x) = 0\} = \{x \in \mathbb{F}_{p^{n+2d}} | S_1^k(x) = 0\}.$$ 

Since $\frac{k}{n}$ is odd, from Item 5 of Lemma 1 it follows

$$S_1^{2L}(x) + S_1^{2L}(x)^{p^d} = 0 \quad \text{(4)}$$

for every $x \in \mathbb{F}_{p^{n+2d}}$. And, $\frac{k}{n}$ and $\frac{d}{l}$ (being a divisor of $\frac{k}{n}$) are odd since $\frac{n}{n}$ is even and $(\frac{n}{n}, \frac{k}{n}) = 1$. Therefore, for every $x \in \mathbb{F}_{p^{n+2d}}$, it holds

$$x^{p^L} = (x^{p^{L+d}})^{p^d} = x^{p^d},$$

$$x^{p^k} = (x^{p^{k+d}})^{p^d} = x^{p^d}$$

and hence

$$S_1^{2L}(x) = S_1^{2d}(x) \text{ and } T_k^{2d}(x) = T_d^{2d}(x). \quad \text{(5)}$$

Moreover, since $\frac{k}{n} = \frac{d}{l}$ is odd, one has $(2d, l) = (d, l) = e$ and $[2d, l] = \frac{2d}{(2d, l)} = 2$. Therefore, by Item 4 of Lemma 1, for every $x \in \mathbb{F}_{p^{n+2k}}$ we have

$$S_1^{2L}(x) = S_1^{2d}(x) = S_1^{2d}(x) = S_1^{2d}(x) = S_1^{2d}(x) = S_1^{2d}(x),$$

that is,

$$S_1^{2L}(x) = S_1^{2d}(x). \quad \text{(6)}$$

6
Then, for every $x \in \mathbb{F}_{p^2}$ one has
\[
S_d^2 \circ S_L^k(x) = S^L_L \circ S_L^k(x) \quad \text{(by (5))}
\]
\[
= S^L_L \circ S_L^k \circ S_L^k(x) \quad \text{(by Item 1 of Lemma 1)}
\]
\[
= S^k_L \circ S^L_L \circ S_L^k(x) \quad \text{(again by Item 1 of Lemma 1)}
\]
\[
= \frac{k}{L} S^L_L(x) \quad \text{(by (4))}
\]
\[
= \frac{k}{L} S^{2d}_L(x) \quad \text{(by (6))},
\]
that is,
\[
S^k_L(S^d_d(x)) = \begin{cases} 0, & \text{if } p \mid \frac{k}{L} S^d_d(x), \\ S^d_d(x), & \text{otherwise.} \end{cases} \tag{7}
\]
Thus, when $p \mid \frac{k}{L}$, it holds
\[
\{ x \in \mathbb{F}_{p^2} \mid S^k_L(x) = 0 \} \supset S^d_d(\mathbb{F}_{p^2}) = \ker(T^d_d),
\]
where the equality is from Item 1 of Lemma 2. By the way, by (5) and Item 2 of Lemma 1, $T^d_d(x) = T^d_d(x) = T^d_d \circ S^k_L(x)$ for every $x \in \mathbb{F}_{p^2}$ and therefore
\[
\{ x \in \mathbb{F}_{p^2} \mid S^k_L(x) = 0 \} \subset \ker(T^d_d). \quad \text{Hence, when } p \mid \frac{k}{L}, \text{ we get}
\]
\[
\{ x \in \mathbb{F}_{p^2} \mid S^k_L(x) = 0 \} = S^d_d(\mathbb{F}_{p^2}).
\]
On the other hand, if $p \nmid \frac{k}{L}$, then by (7)
\[
\{ x \in \mathbb{F}_{p^2} \mid S^k_L(x) = 0 \} \supset \{ S^d_d(x) \mid S^d_d(x) = 0, x \in \mathbb{F}_{p^2} \}
\]
\[
= \{ S^d_d \circ T^d_e(\beta) \mid \beta \in \mathbb{F}_{p^2} \} \quad \text{(by Item 2 of Lemma 2)}
\]
\[
= \ker(T^d_e) \quad \text{(by Item 3 of Lemma 2 since } \frac{d}{e} = \frac{L}{l} \text{ is odd).}
\]
By the way, when $x \in \mathbb{F}_{p^2}$, we can write
\[
S^k_L(x) = \frac{k - L}{2L} S^L_L(x) + S^L_L(x)
\]
because $\frac{k}{L}$ is odd, and therefore if $S^k_L(x) = 0$ for $x \in \mathbb{F}_{p^2}$, then $S^L_L(x) = 0$ (since $S^L_L(x) = 0$ by (6) and (7)) when $S^k_L(x) = 0$, that is, one has
\[
\{ x \in \mathbb{F}_{p^2} \mid S^k_L(x) = 0 \} \subset \ker(S^L_L) \cap \mathbb{F}_{p^2}.
\]
Thus, to conclude the theorem it is sufficient to show:
\[
\ker(S^d_d) = \ker(S^L_L) \cap \mathbb{F}_{p^2}. \tag{8}
\]
To begin with, let us show
\[
\ker(S^d_d) \subset \ker(S^L_L) \cap \mathbb{F}_{p^2}.
\]
In fact, if \( y \in \ker(S^d_e) \) or equivalently \( y = S^2d_e \circ T^2e_i(\beta) \) for some \( \beta \in F_{p^d} \), then

\[
S^L(y) = S^L \circ S^d_e \circ T^2e_i(\beta) \\
= S^L \circ S^2L \circ T^2e_i(\beta) \text{ (by (5))} \\
= S^2L \circ T^2e_i(\beta) \text{ (by Item 1 of Lemma 1)} \\
= S^d_e \circ T^2e_i(\beta) \text{ (by (6))} \\
= S^4d_e(\beta) \text{ (by Item 2 of Lemma 1)} \\
= 0 \text{ (since } \beta \in F_{p^d}).
\]

Next, we prove

\[ \# \ker(S^d_e) = \# \{ \ker(S^L) \cap F_{p^d} \} \]

which will conclude (8). Let \( A := \ker(S^2d_e) = T^2e_i(F_{p^d}) \). Then, by (6), \( A = \ker(S^2L) \cap F_{p^d} \), and since \( S^2L = S^2L \circ S^L \) by Item 1 of Lemma 1,

\[ \ker(S^L) \cap F_{p^d} \subset A. \]

Hence, now we determine \( S^L(A) \) which will make us possible to compute \( \# \{ \ker(S^L) \cap F_{p^d} \} \). First, since \( S^2d_e(S^L(A)) = S^2L(S^L(A)) = S^2L(A) = \{0\} \), it holds

\[ S^L(A) \subset F_{p^d}. \]

Then, since \( d = \frac{p^d}{4} \) is odd, by Item 2 of Lemma 1, \( S^d_e(A) = (S^2L \circ T^2e_i(F_{p^d}) = T^2d(F_{p^d}) = F_{p^d} \) and so

\[ F_{p^d} \subset A. \]

Now, let us prove that \( S^L \) is a permutation on \( F_{p^d} \). In fact, if \( y \in F_{p^d} \) is an element in \( \ker(S^L) \), then by Item 3 of Lemma 2 we can write \( y = S^2L \circ T^2e_i(\beta) \) for some \( \beta \in F_{p^d} \), and one has \( y = y^{p^d} = (S^L \circ T^2e_i(\beta))^{p^d} = S^2L \circ T^2e_i(\beta) = -y \), i.e. \( y = 0 \). Therefore, \( \ker(S^L) \cap F_{p^d} = \emptyset \) and \( S^L \) is a permutation on \( F_{p^d} \) and subsequently on \( F_{p^d} \). By acting \( S^L \) on both sides of (10) we get

\[ F_{p^d} \subset S^L(A). \]

Combined (9) and (11) proves

\[ S^L(A) = F_{p^d}. \]

From here it follows

\[ \# \{ \ker(S^L) \cap F_{p^d} \} = \# A / p^d = p^{(2d-e) - d} = p^{d-e} = \# \ker(S^L). \]
4 On particular solutions of (2) and (3)

In this section, we give particular solutions for each of the two equations (2) and (3) as well as characterizations of the \( a \)'s in \( \mathbb{F}^*_{p^n} \) for which the equations (2) and (3) have at least one solution in \( \mathbb{F}^*_{p^n} \). We present these results by three statements as in Section 3 each of them corresponding again to the three cases defined in Lemma 2.

**Theorem 4.** Let \( \delta \in \mathbb{F}^*_{p^n} \) and \( \delta_1 \in \mathbb{F}^*_{p^d} \) be any elements such that \( T^k_{d}(\delta) = 1 \) and \( T^d_{d}(\delta_1) = 1 \).

1. When \( p \mid k \), there exists a solution in \( \mathbb{F}^*_{p^n} \) to the equation \( T^k_{d}(X) = a \) if and only if \( T^d_{n}(a) = 0 \). In that case,

\[
x_0 = S^2_{d}(x_0) = \left( \sum_{i=0}^{\frac{p-2}{k}} \sum_{j=0}^{\frac{p-1}{d}} \delta^{p^{\delta_i}} a^{p^{\delta_j}} \right)
\]

is a particular \( \mathbb{F}_{p^n} \)-solution to the equation \( T^k_{d}(X) = a \).

2. When \( p \nmid k \), there exists a solution in \( \mathbb{F}^*_{p^n} \) to the equation \( T^k_{d}(X) = a \) if and only if \( S^2_{e} \circ T^d_{n}(a) = 0 \). In that case,

\[
x_0 = y_0 + \frac{L}{k} (a - T^k_{l}(y_0)) \delta_1,
\]

where

\[
y_0 = \sum_{i=0}^{\frac{p-2}{k}} \sum_{j=0}^{\frac{p-1}{d}} \delta^{p^{\delta_i}} S^2_{l}(a) \delta^{p^{\delta_j}},
\]

is a particular \( \mathbb{F}_{p^n} \)-solution to the equation \( T^k_{l}(X) = a \).

**Proof.** Let \( a = T^k_{l}(x_0) \) for some \( x_0 \in \mathbb{F}_{p^n} \). Then

\[
T^d_{n}(a) = T^d_{n} \circ T^k_{l}(x_0)
\]

\[
= T^d_{n} \circ T^L_{j} \circ T^k_{l}(x_0) \quad \text{(by Item 1 of Lemma 1)}
\]

\[
= T^L_{j} \circ T^d_{n} \circ T^k_{l}(x_0)
\]

\[
= T^L_{j} \circ T^d_{n} \circ T^k_{l}(x_0) \quad \text{(by Item 4 of Lemma 1)}
\]

\[
= T^L_{j} \circ T^d_{n}(x_0) \quad \text{(by Item 1 of Lemma 1)}
\]

\[
= \frac{k}{L} T^d_{n}(x_0) \quad \text{(since \( T^d_{n}(x_0) \in \mathbb{F}_{p^n} \subset \mathbb{F}_{p^n} \)).}
\]

Thus, if \( p \mid k \), then \( T^d_{n}(a) = 0 \), and if \( p \nmid k \), then \( S^2_{e} \circ T^d_{n}(a) = S^2_{e} \circ T^d_{n}(x_0) = S^2_{e}(x_0) = 0 \) where we applied Item 3 of Lemma 1. In other words, if \( p \mid k \), then

\[
T^k_{l}(\mathbb{F}_{p^n}) \subset \{ a \in \mathbb{F}_{p^n} \mid T^d_{n}(a) = 0 \},
\]

(12)
and if \( p \mid k \), then
\[
T^k_{\ell}(\mathbb{F}_{p^n}) = \{ a \in \mathbb{F}_{p^n} \mid S^{2e}_{\epsilon} \circ T^m_d(a) = 0 \}. \tag{13}
\]

By the way, by Theorem 1 we have:
\[
\# T^k_{\ell}(\mathbb{F}_{p^n}) = p^n / \# \{ \ker(T^k_{\ell}) \cap \mathbb{F}_{p^n} \} = \begin{cases} p^{n-d}, & \text{if } p \not| k \\ p^{n-(d-c)}, & \text{otherwise.} \end{cases}
\]

On the other hand, by the well-known nature of the trace mapping one knows
\[
\# \{ a \in \mathbb{F}_{p^n} \mid T^m_d(a) = 0 \} = p^{n-d}
\]
and
\[
\# \{ a \in \mathbb{F}_{p^n} \mid S^{2e}_{\epsilon} \circ T^m_d(a) = 0 \} = \# \{ a \in \mathbb{F}_{p^n} \mid T^m_d(a) \in \mathbb{F}_{p^n} \} = p^{n-(d-c)}. \tag{12}
\]

Thus, we conclude that the inclusions (12) and (13) are indeed equalities. That is, the if and only if conditions for \( T^k_{\ell}(X) = a \) to have an \( \mathbb{F}_{p^n} \) solution are justified.

Let us check the validity of the given particular solutions. If \( T^m_d(a) = 0 \), we have
\[
T^k_{\ell} \left( S^{2l}_{\ell} \left( \sum_{i=0}^{\frac{n-2}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} a^{b_{ki}} \right) \right) = T^k_{\ell} \circ S^{2l}_{\ell} \left( \sum_{i=0}^{\frac{n-2}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} a^{b_{ki}} \right)
= S^{2k}_{\ell} \left( \sum_{i=0}^{\frac{n-2}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} a^{b_{ki}} \right) \quad \text{(by Item 3 of Lemma 1)}
= \sum_{i=0}^{\frac{n-2}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} a^{b_{ki}} - \sum_{j=0}^{\frac{n-2}{2}} \sum_{i=j+1}^{\frac{n-1}{2}} \delta^{b_{kj}} a^{b_{ki}}
= a - \delta T^m_d(a) = a.
\]

Now, suppose that \( S^{2e}_{\epsilon} \circ T^m_d(a) = 0 \) i.e. \( T^m_d(a) \in \mathbb{F}_{p^n} \). Then, \( S^{2l}_{\ell}(T^m_d(a)) = T^m_d(a) - \delta T^m_d(a) \mid p^l = 0 \), and for \( y_0 = \sum_{i=0}^{\frac{n-2}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} S^{2l}_{\ell}(a)^{b_{ki}} \), it holds
\[
S^{2k}_{\ell}(y_0) = \sum_{i=0}^{\frac{n-2}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} S^{2l}_{\ell}(a)^{b_{ki}} - \sum_{i=0}^{\frac{n-1}{2}} \sum_{j=i+1}^{\frac{n-1}{2}} \delta^{b_{kj}} S^{2l}_{\ell}(a)^{b_{ki}}
= S^{2l}_{\ell}(a) - \delta T^m_d(S^{2l}_{\ell}(a)) = S^{2l}_{\ell}(a) - \delta S^{2l}_{\ell}(T^m_d(a))
= S^{2l}_{\ell}(a).
\]

Since \( S^{2k}_{\ell}(y_0) = S^{2l}_{\ell}(T^k_{\ell}(y_0)) \) (Item 3 of Lemma 1), we get
\[
\beta := a - T^k_{\ell}(y_0) \in \ker(S^{2l}_{\ell}) \cap \mathbb{F}_{p^n} \subset \mathbb{F}_{p^l} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^l}.
\]
Now, $\beta \delta_1 \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^d}$ and therefore

$$T_k^d(\beta \delta_1) = T_k^d \circ T_l^d(\beta \delta_1) \quad \text{(by Item 1 of Lemma 1)}$$

$$= \frac{k}{L} T_k^d(\beta \delta_1) \quad \text{(since $T_l^d(\beta \delta_1) \in \mathbb{F}_{p^d}$)}$$

$$= \frac{k}{L} T_L^d(\beta \delta_1) \quad \text{(by Item 4 of Lemma 1)}$$

$$= \frac{k}{L} T_L^d(\delta_1) \quad \text{(since $\beta \in \mathbb{F}_{p^d}$)}$$

$$= k L \beta.$$

That is, we get $T_k^d(L_k(L_k(a - T_k^d(y_0))\delta_1)) = a - T_k^d(y_0)$, or equivalently,

$$T_k^d(y_0 + \frac{L}{k}(a - T_k^d(y_0))\delta_1) = a.$$

\[\Box\]

**Theorem 5.** Let $p \neq 2$, $\frac{k}{L}$ even, $\delta \in \mathbb{F}_{p^n}$ and $\delta_1 \in \mathbb{F}_{p^d}$ be any elements such that $T_n^d(\delta) = 1$ and $T_e^d(\delta_1) = 1$.

1. When $\frac{d}{e}$ is odd, or, when $\frac{d}{e}$ is even and $p \mid \frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S_k^d(X) = a$ if and only if $T_n^d(a) = 0$. In that case,

$$x_0 = T_k^d(\sum_{i=0}^{\frac{d}{e}-2} \sum_{j=i+1}^{\frac{d}{e}-1} \delta^{p^k} a^{p^k})$$

is a particular $\mathbb{F}_{p^n}$-solution to the equation $S_k^d(X) = a$.

2. When $\frac{d}{e}$ is even and $p \nmid \frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S_k^d(X) = a$ if and only if $T_{k/e}^d \circ T_n^d(a) = 0$. In that case,

$$x_0 = y_0 + \frac{L}{k}(a - S_k^d(y_0))\delta_1,$$

where

$$y_0 = \sum_{i=0}^{\frac{d}{e}-2} \sum_{j=i+1}^{\frac{d}{e}-1} \delta^{p^k} T_k^d(a)^{p^k},$$

is a particular $\mathbb{F}_{p^n}$-solution to the equation $S_k^d(X) = a$.

**Proof.** Suppose that $S_k^d(x_0) = a$ for some $x_0 \in \mathbb{F}_{p^n}$. When $\frac{d}{e} = \frac{L}{k}$ is odd, $\frac{k}{L}$ is even since $\frac{k}{L} = \frac{k}{L} \cdot \frac{k}{L}$ was assumed to be even. Then, we have

$$T_n^d(a) = T_n^d \circ S_k^d(x_0)$$

$$= T_n^d \circ S_k^d \circ S_L^d(x_0) \quad \text{(by Item 1 of Lemma 1)}$$

$$= S_L^d(S_k^d \circ T_n^d(x_0))$$

$$= 0 \quad \text{(since $S_k^d \circ T_n^d(x_0) \in \mathbb{F}_{p^{d'}} \subset \mathbb{F}_{p^{d'}}$ and $\frac{k}{L}$ is even)}$$
and thus
\[ S^k(S_{p^n}) \subset \{ a \in \mathbb{F}_{p^n} | T^a_d (a) = 0 \}. \]  
(15)

On the other hand, when \( \frac{d}{e} = \frac{k}{L} \) is even, one has
\[
T^a_d (a) = T^a_d \circ S^k(x_0)
= T^a_d \circ T^k_L \circ S^L_I(x_0) \quad \text{(by Item 1 of Lemma 1)}
= T^k_L \circ S^L_I \circ T^a_d(x_0)
= T^k_L \circ S^d_c \circ T^a_d(x_0) \quad \text{(by Item 4 of Lemma 1)}
= \frac{k}{L} \circ S^d_c \circ T^a_d(x_0) \quad \text{(since \( S^d_c \circ T^a_d(x_0) \in \mathbb{F}_{p^d} \subset \mathbb{F}_{p^L} \)).}
\]

Therefore, if \( p \mid \frac{k}{L} \), then (15) still holds true, and if \( p \nmid \frac{k}{L} \), then it holds
\[
T^{2e}_c \circ T^a_d (a) = T^{2e}_c \circ S^d_c \circ T^a_d(x_0)
= S^{2d}_d \circ T^a_d(x_0) \quad \text{(by Item 2 of Lemma 1)}
= 0 \quad \text{(since \( T^a_d(x_0) \in \mathbb{F}_{p^e} \))}
\]
and thus
\[ S^k(S_{p^n}) \subset \{ a \in \mathbb{F}_{p^n} | T^{2e}_c \circ T^a_d (a) = 0 \}. \]  
(16)

By the way, by Theorem 2 we have:
\[
\#S^k(S_{p^n}) = \frac{p^n}{\# \ker(S^k) \cap \mathbb{F}_{p^n}} = \begin{cases} 
p^{n-d}, & \text{if } \frac{d}{e} \text{ is odd}, \text{ or, } \frac{d}{e} \text{ is even and } p \nmid \frac{k}{L}, \\np^{n-(d-e)}, & \text{otherwise}. \end{cases}
\]

On the other hand, by the well-known nature of the trace mapping one knows
\[
\# \{ a \in \mathbb{F}_{p^n} | T^a_d (a) = 0 \} = p^{n-d}
\]
and
\[
\# \{ a \in \mathbb{F}_{p^n} | T^{2e}_c \circ T^a_d (a) = 0 \} = p^{n-(d-e)}.
\]

Therefore the inclusions (15) and (16) are indeed equalities. That is, the if and only if conditions for \( S^k(X) = a \) to have a \( \mathbb{F}_{p^n} \)-solution are justified.

Since \( S^k \circ T^{2L}_L = S^{2k}_L \) (Item 2 of Lemma 1), it can be checked by the same computation as in the proof of Item 1 of Theorem 4 that under the condition \( T^a_d (a) = 0 \),
\[
x_0 = T^{2L}_L \left( \sum_{i=0}^{2-2} \sum_{j=1+1}^{2-1} \delta^{3^{k_j}} a^{3^{k_i}} \right)
\]
is a particular \( \mathbb{F}_{p^n} \)-solution to the equation \( S^k(X) = a \).

Now, assuming that \( \frac{d}{e} = \frac{k}{L} \) is even, let us suppose that \( T^{2e}_c \circ T^a_d (a) = 0 \) i.e. \( T^a_d(a)^{p^e} = -T^a_d(a) \). Then, \( \frac{k}{L} \) is odd since it is prime to \( \frac{d}{e} = \frac{d}{e} \cdot \frac{k}{L} \) which is even.
Hence, $T^{2l}(T^n_d(a)) = T^n_d(a) + T^n_d(a)^p = 0$, and for $y_0 = \sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \delta^{p^j} T^{2l}_l(a)^{p^j}$, it holds

$$S^k_k(y_0) = \sum_{i=0}^{l-2} \sum_{j=i+1}^{l-1} \delta^{p^j} T^{2l}_l(a)^{p^j} - \sum_{i=0}^{l-1} \sum_{j=i+1}^{l} \delta^{p^j} T^{2l}_l(a)^{p^j}$$

$$= T^{2l}_l(a) - \delta T^{2l}_l(T^{2l}_l(a)) = T^{2l}_l(a) - \delta T^{2l}_l(T^n_d(a))$$

$$= T^{2l}_l(a).$$

Since $S^k_k(y_0) = T^{2l}_l(S^k_k(y_0))$ (Item 2 of Lemma 1), letting $\beta := a - S^k_k(y_0)$, we have

$$\beta \in \ker(T^{2l}_d) \cap F_p \cap F_{p^e} \cap F_{p^{2e}}$$

and

$$S^k_k(\beta \delta_1) = \frac{k}{L} S^k_k(\beta \delta_1) \text{ (since } L \text{ is even)}$$

$$= \frac{k}{L} S^d_k(\beta \delta_1) \text{ (by Item 4 of Lemma 1)}$$

$$= \frac{k}{L} S^d_k(T^{2d}_d(\beta \delta_1)) \text{ (by Item 1 of Lemma 1)}$$

$$= \frac{k}{L} S^d_k(\beta T^{2d}_d(\delta_1)) \text{ (since } \beta \in F_{p^e})$$

$$= \frac{k}{L} S^d_k(\beta) = \frac{k}{L} (\beta - \beta p) \text{.}$$

On the other hand, since $\ker(T^{2l}_d) \cap F_{p^e} = S^c_e(F_{p^e})$ (see Theorem 1), $\beta \in \ker(T^{2l}_d) \cap F_{p^e}$ means that $\beta = \alpha - \alpha p$ for some $\alpha \in F_{p^e}$, and therefore we get $\beta + \beta p = (\alpha - \alpha p) + (\alpha - \alpha p) p = 0$ and hence

$$S^k_k(\beta \delta_1) = \frac{2k}{L} \beta,$$

or equivalently,

$$S^k_k \left( y_0 + \frac{L}{2k} (a - S^k_k(y_0)) \delta_1 \right) = a.$$

\[\Box\]

**Theorem 6.** Let $p \neq 2$, $\frac{L}{k}$ odd, $\delta \in F_{p^e}$ and $\delta_1 \in F_{p^e}$ be any elements such that $T^n_d(\delta) = 1$ and $T^{2d}_d(\delta_1) = 1$.

1. When $\frac{n}{2}$ is even and $p | \frac{k}{2}$, there exists a solution in $F_{p^e}$ to the equation $S^k_k(X) = a$ if and only if $S^k_k(a) = 0$. In that case,

$$x_0 = T^{2l}_l(\sum_{i=0}^{n-2} \sum_{j=i+1}^{n-1} \delta^{p^j} a^{p^j} (-1)^j)$$

is a particular $F_{p^e}$-solution to the equation $S^k_k(X) = a$.  

13
2. When $\frac{n}{2}$ is even and $p \nmid \frac{k}{L}$, there exists a solution in $\mathbb{F}_{p^n}$ to the equation $S^k_d(X) = a$ if and only if $T_{2e}^c \circ S^n_d(a) = 0$. In that case,

$$x_0 = y_0 + \frac{L}{2k} S_2^{2d} ((a - S^k_l(y_0)) \delta_1),$$

where

$$y_0 = \sum_{i=0}^{\frac{n}{2}-2} \sum_{j=1}^{\frac{n}{2}-1} a^{p^k j} T_{2l}^{(a)} p^{k_i} (-1)^i,$$

is a particular $\mathbb{F}_{p^n}$-solution to the equation $S^k_d(X) = a$.

3. When $\frac{n}{2}$ is odd, the equation $S^k_d(X) = a$ has a unique $\mathbb{F}_{p^n}$-solution:

$$x_0 = \frac{T_{2l} \circ S^{[n,k]}_l(a)}{2}.$$

**Proof.** Suppose $a \in S^k_d(\mathbb{F}_{p^n})$ i.e. $a = S^k_d(x_0)$ for some $x_0 \in \mathbb{F}_{p^n}$.

Let us assume that $\frac{n}{2}$ is even. In this case, $\frac{k}{L}$ and its divisor $\frac{L}{2}$ are odd since $(\frac{n}{2}, \frac{k}{L}) = 1$. One has

$$S^n_d(a) = S^n_d \circ S^k_l(x_0)$$

$$= S^n_d \circ S^k_l \circ S^k_l(x_0) \text{ (by Item 1 of Lemma 1)}$$

$$= S^n_d \circ T_{2d}^n \circ S^k_l \circ S^k_l(x_0) \text{ (again by Item 1 of Lemma 1)}$$

$$= S^k_L \circ T_{2d}^n \circ S^k_L \circ S^k_l(x_0) \text{ (by (5))}$$

$$= S^k_L \circ S^{2L}_L \circ S^k_l \circ T_{2d}^n(x_0)$$

$$= S^k_L \circ S^{2L}_L \circ T_{2d}^n(x_0) \text{ (by Item 1 of Lemma 1)}$$

$$= \frac{k}{L} S^{2L}_L \circ T_{2d}^n(x_0) \text{ (by (4))}$$

$$= \frac{k}{L} S^{2d}_L \circ T_{2d}^n(x_0) \text{ (by (6))}$$

$$= \frac{k}{L} S_e^o(x_0) = \frac{k}{L} S^{2e}_e \circ T_{2e}^n(x_0) \text{ (once again by Item 1 of Lemma 1).}$$

Therefore, if $p \nmid \frac{k}{L}$, then it holds

$$S^k_d(\mathbb{F}_{p^n}) \subset \{ a \in \mathbb{F}_{p^n} | S^n_d(a) = 0 \}, \quad (17)$$

and if $p \nmid \frac{k}{L}$, then it holds

$$S^k_d(\mathbb{F}_{p^n}) \subset \{ a \in \mathbb{F}_{p^n} | T_{2e}^c \circ S^n_d(a) = 0 \} \quad (18)$$

since $T_{2e}^c \circ S^n_d(S^k_l(x_0)) = T_{2e}^c \circ S^{2e}_e \circ T_{2e}^n(x_0) = 0$ by Lemma 2. Comparisons of set cardinalities regarding Item 2 of Theorem 3 make us conclude that the inclusions (17) and (18) are indeed equalities. That is, the if and only if conditions for $S^k_d(X) = a$ to have a $\mathbb{F}_{p^n}$-solution are justified.
If \( S^0_d(a) = 0 \), then for \( x_0 = T^{2l}_I(\sum_{i=0}^{\ell-2} \sum_{j=i+1}^{\ell-1} \delta^{p^k_j} a^{p^k_i} (-1)^i) \),

\[
S^k_I(x_0) = T^{2k}_k(\sum_{i=0}^{\ell-2} \sum_{j=i+1}^{\ell-1} \delta^{p^k_j} a^{p^k_i} (-1)^i) \quad \text{(by Item 2 of Lemma 1)}
\]

\[
= \sum_{i=0}^{\ell-2} \sum_{j=i+1}^{\ell-1} \delta^{p^k_j} a^{p^k_i} (-1)^i + \sum_{i=1}^{\ell} \sum_{j=i+1}^{\ell} \delta^{p^k_j} a^{p^k_i} (-1)^{i-1}
\]

\[
= a - \delta S^0_d(a) = a.
\]

Now, suppose that \( \frac{d}{\ell} = \frac{\ln \ell}{\kappa} \) is even and \( T^{2e}_e \circ S^0_d(a) = 0 \) (i.e. \( S^0_d(a)^{p^r} = -S^0_d(a) \)). Then, \( \frac{d}{\ell} \) is odd since it is prime to \( \frac{d}{\ell} \), which is even, and hence \( T^{2l}_I(S^0_d(a)) = S^0_d(a) + S^0_d(a)^{p^r} = 0 \). Thus, for \( y_0 = \sum_{i=0}^{\ell-2} \sum_{j=i+1}^{\ell-1} \delta^{p^k_j} T^{2l}_I(a)^{p^k_i} (-1)^i \), one has

\[
T^{2k}_k(y_0) = \sum_{i=0}^{\ell-2} \sum_{j=i+1}^{\ell-1} \delta^{p^k_j} T^{2l}_I(a)^{p^k_i} (-1)^i + \sum_{i=1}^{\ell} \sum_{j=i+1}^{\ell} \delta^{p^k_j} T^{2l}_I(a)^{p^k_i} (-1)^{i-1}
\]

\[
= T^{2l}_I(a) - \delta S^0_d(T^{2l}_I(a)) = T^{2l}_I(a).
\]

Since \( T^{2k}_k(y_0) = T^{2l}_I \circ S^k_I(y_0) \) (by Item 2 of Lemma 1), we have

\[
\beta := a - S^k_I(y_0) \in \ker(T^{2l}_I) \cap F_{p^r} \subset F_{p^{2r}} \subset F_{p^{2e}}.
\]

Now,

\[
S^k_I(S^{2d}_d(\beta \delta_1)) = S^k_I(S^{2L}_d(\beta \delta_1)) \quad \text{(by (5))}
\]

\[
= S^k_I \circ S^k_I(S^{2L}_d(\beta \delta_1)) \quad \text{(by Item 1 of Lemma 1)}
\]

\[
= S^k_I \circ (S^k_I \circ S^{2L}_d(\beta \delta_1)) = S^k_I \circ (S^{2L}_d(\beta \delta_1)) \quad \text{(by Item 1 of Lemma 1)}
\]

\[
= \frac{k}{L} S^{2L}_d(\beta \delta_1) \quad \text{(by (4))}
\]

\[
= \frac{k}{L} S^{2d}_d(\beta \delta_1) \quad \text{(by (6))}
\]

\[
= \frac{k}{L} S^{2e}(\beta T^{2d}_2(\delta_1)) \quad \text{(by Item 1 of Lemma 1)}
\]

\[
= \frac{k}{L} S^{2e}(\beta T^{2d}_2(\delta_1)) = \frac{k}{L} S^{2e}(\beta) = \frac{k}{L} (\beta + \beta^{p^r})
\]

By the way, since \( \beta \in \ker(T^{2l}_I) \cap F_{p^{2e}} = S^{2e}(F_{p^{2e}}) \) (Theorem 1), it holds \( \beta + \beta^{p^r} = 0 \) and thus we get

\[
S^k_I(S^{2d}_d(\beta \delta_1)) = \frac{2k}{L} \beta.
\]

That is,

\[
S^k_I(y_0 + \frac{L}{2k} S^{2d}_d((a - S^k_I(y_0))\delta_1)) = a.
\]

15
If \( \frac{n}{d} = \frac{\ln n}{k} \) is odd, then by Theorem 3, \( S_k^t \) is a permutation on \( \mathbb{F}_{p^n} \) and the equation \( S_k^t(X) = a \) has a unique \( \mathbb{F}_{p^n} \)-solution. In fact, by successive applications of Item 2 of Lemma 1 we have

\[
S_k^t(T_{2}^{[n,k]}(a/2)) = T_{k}^{2k} \circ S_k^{[n,k]}(a/2) = T_{[n,k]}^{2[n,k]}(a/2) = a.
\]

\[\square\]

5 Conclusion

We explicitly determined the sets of preimages of linearized polynomials

\[
T_k^t(X) := \sum_{i=0}^{\frac{d}{2}-1} X^{p^{i}},
\]

\[
S_k^t(X) := \sum_{i=0}^{\frac{d}{2}-1} (-1)^i X^{p^{i}},
\]

over \( \mathbb{F}_p \) and over the finite field \( \mathbb{F}_{p^n} \) for any characteristic \( p \) and any integer \( n \geq 1 \). In particular, another solution for the case \( p = 2 \) that was solved very recently in [7] was obtained by Theorem 1 and Theorem 4.

References


7. S. Mesnager, K.H. Kim, J.H. Choe, D.N. Lee and D.S. Go. Solving \( x + x^{2} + \cdots + x^{2^{m-1}} = a \) over \( \mathbb{F}_{2^n} \). Cryptography and Communications. To appear. https://doi.org/10.1007/s12095-020-00425-3