On involutions of finite fields

Pascale CHARPIN
INRIA Paris-Rocquencourt,
Le Chesnay, France,
Pascale.Charpin@inria.fr

Sihem MESNAGER
University of Paris VIII, Dept. Mathematics
LAGA, CNRS and Telecom ParisTech, France,
smesnager@univ-paris8.fr

Sumanta SARKAR
Centre of Excellence in Cryptology,
Indian Stat. Inst., Kolkata, India,
Sumanta.Sarkar@gmail.com.

***Abstract*—In this paper we study involutions over a finite field of order 2^n. We present some classes, several constructions of involutions and we study the set of their fixed points.**

I. INTRODUCTION

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n. Every polynomial of $\mathbb{F}_{2^n}[x]$ identifies a mapping from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Permutations of $\mathbb{F}_{2^n}$ have been extensively studied for its applications in cryptography, coding theory, combinatorial design, etc. Any permutation P has a *compositional inverse* G such that $P \circ G = G \circ P = \mathcal{I}$, where $\mathcal{I}$ is the identity. It is often desired to have permutations which are easy to implement. On the other hand, in many situations, both the permutation and its compositional inverse are required. For instance, in block ciphers an S-box is used as a permutation to build the confusion layer during the encryption process. While decrypting the cipher, the compositional inverse of the S-box is used. This motivates the use of an *involution*, a permutation whose compositional inverse is itself. One immediate practical advantage of involution is that implementation of the inverse does not require additional resources, which is particularly useful for its implementation (as part of a block cipher) in devices with limited resources.

Involutions have been used frequently in block cipher designs (as S-Boxes), e.g., in AES [1], Khazad, Anubis [2], PRINCE [3]. However, in these references involutions have been observed from a cryptographic point of view, and it seems that as a mathematical object involution has rarely been studied. Our purpose is to study this mathematical object systematically. We present several constructions of this kind of polynomials. Since involutions have on the average a high number of fixed points, our aim is to identify involutions that have low number of fixed points. This paper is an extended abstract of a forthcoming full paper [5].

II. INVOLUTIONS, BASIC PROPERTIES

The trace function from $\mathbb{F}_{2^n}$ onto any subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$ is as follows:

$$Tr_{n/k}(y) = \sum_{i=0}^{\frac{n}{k}-1} y^{2^{ki}}.$$

The *absolute trace* on $\mathbb{F}_{2^n}$ ($k = 1$) is simply denoted by Tr. For any function $F(x), x \in \mathbb{F}_{2^n}$, its *derivative* at point $a \in \mathbb{F}_{2^n}^*$ is the function $x \mapsto F(x) + F(x + a)$. This function can be constant for some a; such property was generalized in [8]:

Definition 1: Let $n = rk$, $1 \leq k \leq n$. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, $\gamma \in \mathbb{F}_{2^n}^*$ and b be a constant of $\mathbb{F}_{2^k}$. Then γ is a *b-linear translator* of f if $f(x) + f(x + u\gamma) = ub$ for all $x \in \mathbb{F}_{2^n}$ and for all $u \in \mathbb{F}_{2^k}$. In particular, when $k = 1$, γ is usually said to be a *b-linear structure* of the Boolean function f (where $b \in \mathbb{F}_2$), that is $f(x)+f(x+\gamma) = b$ for all $x \in \mathbb{F}_{2^n}$.

Note that an *involution* is a special permutation, but the *involution property* includes the bijectivity.

Definition 2: Let F be any function over $\mathbb{F}_{2^n}$. We say that F is an involution when it satisfies

$$F \circ F(x) = x, \quad \text{for all } x \in \mathbb{F}_{2^n}.$$

Example 1: The most known involutions over $\mathbb{F}_{2^n}$ are:
– The trivial one's: $x \mapsto x + a$, for any $a \in \mathbb{F}_{2^n}$;
– The inverse function $x \mapsto x^{-1}$, for any n;
– When $n = 2m$ the linear function $x \mapsto x^{2^m}$;
– The functions $x \mapsto x + \gamma f(x)$ where f is any Boolean function with a 0-linear structure γ (see [8, Theorem 3]).

It is important to see that an involution F on $\mathbb{F}_{2^n}$ is a sequence of pairs. More precisely, F acts by exchanging a pair of elements of $\mathbb{F}_{2^n}$ and by fixing the remaining points.

Proposition 1: Let F be an involution over $\mathbb{F}_{2^n}$ and denote by U the set of fixed-points of F. Set $E = \mathbb{F}_{2^n} \setminus U$. Then F is the identity on U and acts on a sequence of pairs of E as follows, where $|E|$ is the cardinality of E,

$$E = \{(x_0, x_1), \ldots, (x_i, x_{i+1}), \ldots, (x_{N-1}, x_N)\},\ N = \frac{|E|}{2}.$$

where $x_{i+1} = F(x_i)$ and $F(x_{i+1}) = x_i$.

Let $\mathcal{V}_n$ be the set of involutions on $\mathbb{F}_{2^n}$; $\mathcal{V}_n$ is not a group for the composition operator (see the next lemma). But, $\mathcal{V}_n$ contains the *identity*, which is the *identity element* for the operation $\circ$. If F is an involution then $F^{-1} = F$ so that F is its own *inverse*.

Lemma 1: Let F, G be both in $\mathcal{V}_n$. Then the inverse of $F \circ G$ is $G \circ F$. Consequently $F \circ G \in \mathcal{V}_n$ if and only if F and G commute.

Example 2: Let $G(x) = x^{2^m}$, where $m = 2n$. It is easy to check that for any involution $F \in \mathbb{F}_{2^m}[x]$, $F \circ G$ is an involution. For instance, if $F(x) = x^{-1}$ then $F \circ G(x) = x^{-2^m} = \left(x^{-1}\right)^{2^m}$.

Involution are conserved through some compositions. In fact it is easy to check that for any $F \in \mathcal{V}_n$, and for any permutation G, the function $G^{-1} \circ F \circ G$ is an involution.

Let $F(x) = \sum_{i \in I} \lambda_i x^i$ be any polynomial of $\mathbb{F}_{2^n}[x]$, where I denotes the set of nonzero terms of F. The *degree* of F is the maximal integer value in I.

Lemma 2: Let $F \in \mathbb{F}_{2^n}[x]$. Denote by $d(F)$ the degree of F. If F is an involution, which is not the identity, then its degree satisfies $d(F) \geq \lceil 2^{n/2} \rceil$.

III. Involutions with special forms

A. Monomials

We are interested in this section in monomial involutions, that is, involutions of the form x^s. According to Lemma 2, one has necessarily $s \geq \lceil 2^{n/2} \rceil$.

Proposition 2: Let $Q(x) = \lambda x^d$ is a polynomial over $\mathbb{F}_{2^n}$, then $Q(x)$ is involution if and only if $\lambda^{d+1} = 1$ and

$$d^2 = 1 \pmod{2^n - 1}. \tag{1}$$

In Proposition 3 below we treat the case where $2^n - 1$ is a Mersenne prime. In this case, $d^2 = 1 \pmod{2^n - 1}$ if and only if $2^n - 1$ divides $(d+1)(d-1)$. But this is impossible for $1 < d < 2^n - 2$.

Proposition 3: Let n be a positive integer such that $2^n - 1$ is prime. Then the only monomial involutions on $\mathbb{F}_{2^n}$ are the identity $x \mapsto x$ and the inverse function $x \mapsto x^{-1}$.

Thus a quite natural question arises: what happens when $2^n - 1$ is a composite number? It is clear that

$$d^2 = 1 \pmod{2^n - 1} \quad \Leftrightarrow \quad \forall p \in M_n, \ \ d^2 = 1 \pmod{p}$$

where M_n denotes the set of prime factors of $2^n - 1$. It seems to be hard to exhibit all the monomial involutions in that case. However, the number of such involutions can be computed.

Theorem 1: The number of monomial involutions $x \mapsto x^d$ on $\mathbb{F}_{2^n}$ equals 2^τ where τ is the number of prime factors in the prime decomposition of $2^n - 1$.

Sketch of proof: Given a positive integer p, let us denote $\rho(p)$ the number of square roots of unity modulo p. Let us first show that $\rho(pq) = \rho(p)\rho(q)$, when p and q are coprime. To this end, note that according to Chinese's Theorem, $\mathbb{Z}/(pq)\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ via the isomorphism

$$\psi \ : \ x \in \mathbb{Z}/(pq)\mathbb{Z} \ \mapsto \ (x \pmod{p}, \ x \pmod{q}).$$

Now, one has $\rho(p^\alpha) = 2$ for any odd prime number p and positive integer α. We write

$$2^n - 1 = \prod_{i=1}^{\tau} p_i^{\alpha_i}, \quad p_i \in M_n, \ \alpha_i > 0.$$

Then $\rho(2^n - 1) = \prod_{i=1}^{\tau} \rho(p_i^{\alpha_i}) = 2^\tau$. ∎

B. Linear involution

First of all, note that linear involutions exist, one trivial example would be the function $x \mapsto x^{2^m}$ on $\mathbb{F}_{2^n}$, for $n = 2m$. In this section we make a study of linear involutions. First we start with the linear monomials and move to more general results afterwards.

Proposition 4: Let $Q(x) = \lambda x^{2^i}$, where $0 < i < n$ and $\lambda \in \mathbb{F}_{2^n}^*$. Then Q is an involution if and only if n is even, $\lambda^{2^i+1} = 1$ and $i = \frac{n}{2}$.

Next we consider linear binomials.

Proposition 5: Let $Q(x) = ax^{2^i} + bx^{2^j}$, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}^*$, where $i < j$. Then

- For even n, $n = 2m$, Q is an involution if and only if $j = i + m$ and either
$$i = 0, \ ab^{2^i} + a^{2^j} b = 0 \ \text{ and } \ a^{2^i+1} + b^{2^j+1} = 1$$
or m is even and
$$i = \frac{m}{2}, \ ab^{2^i} + a^{2^j} b = 1 \ \text{ and } \ a^{2^i+1} + b^{2^j+1} = 0.$$
- For odd n, Q is not an involution, for all a, b.

Proof: We compute $Q \circ Q$:

$$\begin{aligned} Q \circ Q(x) &= a\left(ax^{2^i} + bx^{2^j}\right)^{2^i} + b\left(ax^{2^i} + bx^{2^j}\right)^{2^j} \\ &= a^{2^i+1}x^{2^{2i}} + x^{2^{i+j}}\left(ab^{2^i} + a^{2^j}b\right) + b^{2^j+1}x^{2^{2j}}. \end{aligned}$$

Note that the exponents of x, $e \in \{2i, i+j, 2j\}$, all satisfy $0 \leq e < 2n - 2$ and recall $i \neq j$. To get $Q \circ Q(x) = x$, two of the three exponents have to be removed. We consider the following cases:

- $2i \equiv 2j \pmod{n}$ implies $2j = 2i + n$ which is impossible for odd n; if $n = 2m$ then $j = i + m$.
- $2j \equiv j + i \pmod{n}$ implies $2j = n + i + j$, that is $j = n + i$ which is impossible. The case $2i \equiv j + i \pmod{n}$ implies $i = n + j$ which is impossible too.

Thus Q is an involution only when $j = i + m$ (n even) and in this case

$$Q \circ Q(x) = x^{2^{2i}}\left(a^{2^i+1} + b^{2^j+1}\right) + x^{2^{i+j}}\left(ab^{2^i} + a^{2^j}b\right).$$

Note that $2i \equiv n \pmod{n}$ only when $i = 0$. Otherwise we must have $i + j = n$, providing $2i = m$ since $j = m + i$. ∎

Now we look at linear involutions with any number of terms. The following obvious lemma is particularly useful for polynomials of $\mathbb{F}_2[x]$.

Lemma 3: Let I be any subset of $\{0, 1, \ldots, n-1\}$ and $Q(x) = \sum_{i \in I} a_i x^{2^i}$ where $a_i \in \mathbb{F}_{2^n}^*$. Then

$$Q \circ Q(x) = \sum_{i \in I} a_i^{2^i+1} x^{2^{2i}} + \sum_{i<j, (i,j) \in I^2} (a_i a_j^{2^i} + a_i^{2^j} a_j) x^{2^{i+j}}.$$

Proposition 6: Let $Q(x) = \sum_{i \in I} x^{2^i}$, where the cardinality $|I|$ of I is such that $|I| > 1$. Then Q cannot be an involution on $\mathbb{F}_{2^n}$ when n is odd. When n is even, Q is an involution on $\mathbb{F}_{2^n}$ if and only if

$$\sum_{i \in I} x^{2^{2i}} = x \pmod{x^{2^n} + x}. \tag{2}$$

Proof: involution By using the expression given in Lemma 3, we get (2) since $a_i = 1$ for all i. Clearly $2j \equiv 2i \pmod{n}$ is impossible for odd n unless $i = j$. ∎

Thus, for even n it is easy to construct linear involutions having coefficients from the set $\{0, 1\}$. For instance, it is easy to describe a large set of trinomials which are involutions of $\mathbb{F}_{2^n}$ (where $n = 2m$):

$$x + x^{2^i} + x^{2^{m+i}}, \ i = 1, 2, \ldots, m-1.$$

We already have seen that linear monomial and binomial involutions do not exist over $\mathbb{F}_{2^n}$, when n is odd. However, linear involutions with higher number of terms for odd n do exist, as it is shown below, where one may note that γ cannot be 1 as n is odd, which makes it distinct from Proposition 6.

Proposition 7: The function $x \mapsto x + \gamma Tr(x)$ is an involution if and only if $Tr(\gamma) = 0$, where $\gamma \in \mathbb{F}_{2^n}^*$.

IV. Involution from another involution

A. Exchanging values of a pair of inputs

Recently, Yu, Wang and Li proposed some new permutations with low differential uniformity [9]. These are obtained by exchanging two values of a given permutation. We first show that it is easy to construct an involution from another involution, by using this method.

Theorem 2: Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ be an involution. Let α and β be two nonzero distinct elements of $\mathbb{F}_{2^n}$. Define $G : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ as follows:

$$G(x) = \begin{cases} F(x) & \text{for all } x \notin \{\alpha, \beta\} \\ F(\alpha) & \text{if } x = \beta \\ F(\beta) & \text{if } x = \alpha. \end{cases}$$

Then G is an involution if and only if $\{\alpha, \beta\}$ is stable under F, that is

$$\forall x \in \{\alpha, \beta\}, \quad F(x) \in \{\alpha, \beta\} \tag{3}$$

Proof: Clearly, $G(G(x)) = F(F(x))$ if $x \notin \{\alpha, \beta\}$. Thus, if $x \notin \{\alpha, \beta\}$, $G(G(x)) = x$, that is, the restriction of G to the complement set of $\{\alpha, \beta\}$ is an involution. Suppose now that (3) holds. Recall that any permutation of a set of cardinality 2 is an involution. Hence, the restriction of G to $\{\alpha, \beta\}$ is an involution too proving that G is an involution of $\mathbb{F}_{2^n}$. Conversely, suppose that G is an involution, that is $G(G(x)) = x = F(F(x))$ for every $x \in \mathbb{F}_{2^n}$. Let x be such that $F(x) = \alpha$. If $x \notin \{\alpha, \beta\}$ then

$$G(G(x)) = G(F(x)) = G(\alpha) = F(\beta) = x = F(\alpha),$$

which is impossible since F is bijective. Hence $x \in \{\alpha, \beta\}$. If $F(x) = \beta$, similar argument follows, thus completing the proof. ∎

Remark 1: Recently, in a lot of papers, the authors modify the inverse function and look at some cryptographic properties of the derived function (for instance, [6], [9]). Actually, doing this, we often lose the involution property.

B. Using subfields of $\mathbb{F}_{2^n}$

In this section we study involutions of the form

$$x \mapsto G(x) + \gamma f(x), \ \gamma \in \mathbb{F}_{2^n}^*$$

where G is an involution and f is a function from $\mathbb{F}_{2^n}$ to a subfield of $\mathbb{F}_{2^n}$. We begin by recalling those involutions introduced in [8]. The simplest one is in Example 1; we are interested here in more general classes of involutions.

We begin by giving an instance of a theorem of [8]. Recall that a $\mathbb{F}_{2^k}$-linear function on $\mathbb{F}_{2^n}$ $(n = rk)$ is of the form

$$L : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}, \ L(x) = \sum_{i=0}^{r-1} \lambda_i x^{2^{ki}}, \ \lambda_i \in \mathbb{F}_{2^n}.$$

Theorem 3: [8, Theorem 1] Let $n = rk$, $k > 1$. Let L be a $\mathbb{F}_{2^k}$-linear permutation on $\mathbb{F}_{2^n}$. Let f be a function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^k}$, $h : \mathbb{F}_{2^k} \mapsto \mathbb{F}_{2^k}$, $\gamma \in \mathbb{F}_{2^n}^*$ and b be fixed in $\mathbb{F}_{2^k}$. Assume that f is surjective. Assume that γ is a b-linear translator of f. Then

$$F(x) = L(x) + L(\gamma)h(f(x))$$

permutes $\mathbb{F}_{2^n}$ if and only if $g : u \mapsto u + bh(u)$ permutes $\mathbb{F}_{2^k}$.

Corollary 1: Hypotheses are those of Theorem 3 with $b = 0$. Set $G(x) = x + \gamma h(f(x))$. Then the function

$$F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}, \ F(x) = L(x) + L(\gamma)h(f(x))$$

is a permutation on $\mathbb{F}_{2^n}$. Moreover G is an involution over $\mathbb{F}_{2^n}$; further, if L is an involution which commutes with G then F is an involution too.

Proof: If $b = 0$ then g is the identity in Theorem 3 so that F is bijective. And we have

$$\begin{aligned} G \circ G(x) &= G(x + \gamma h(f(x))) \\ &= x + \gamma h(f(x)) + \gamma h(f(x + \gamma h(f(x)))) \\ &= x + \gamma h(f(x)) + \gamma h(f(x)) = x, \end{aligned}$$

since γ is a 0-translator of f. Since L is $\mathbb{F}_{2^k}$-linear, we have: $F = L \circ G$ so that $F^{-1} = G \circ L^{-1}$. According to Lemma 1, when L is involution, F is an involution whenever G and L commute. ∎

Example 3: Let $n = 2m$. Let ϕ be any mapping from $\mathbb{F}_{2^m}$ to itself then the mapping ψ from $\mathbb{F}_{2^n}$ to itself given by

$$\psi(x) = \phi(Tr_{n/m}(x)) + x^{2^m} \tag{4}$$

is an involution on $\mathbb{F}_{2^n}$. For this, one can apply Corollary 1. First note that $\gamma = 1$ is a 0-linear translator of $Tr_{n/m}$ since

$$Tr_{n/m}(x) + Tr_{n/m}(x + u) = 0, \text{ for all } u \in \mathbb{F}_{2^m}.$$

So, ψ is a permutation (taking $L(x) = x^{2^m}$). But L is an involution which commutes with $G : x \mapsto x + \phi(Tr_{n/m}(x))$.

C. Adding a Boolean function

Here we consider the functions over $\mathbb{F}_{2^n}$ of the form

$$Q(x) = G(x) + \gamma f(x) \tag{5}$$

where G is an involution, $\gamma \in \mathbb{F}_{2^n}^*$ and f is any Boolean function. We first recall the conditions for Q to be a permutation.

Theorem 4: [6] Let Q be defined by (5), where G is a permutation only. Then Q is a permutation over $\mathbb{F}_{2^n}$ if and only if γ is a 0-linear structure of $f \circ G^{-1}$, where G^{-1} denotes the compositional inverse function of G. Moreover, in this case,

$$Q^{-1} = G^{-1} \circ H \quad \text{where} \quad H(x) = x + \gamma f(G^{-1}(x)). \tag{6}$$

Next we identify when permutations defined by (5) are involutions.

Theorem 5: Let Q be defined by (5). Then Q is involution if and only if

(i) γ is a 0-linear structure of f,
(ii) $f \circ G = f$ and
(iii) $H \circ G = G \circ H$ where $H(x) = x + \gamma f(x)$.

Proof: Suppose that Q is involution. We first show that one has necessarily $f \circ G = f$. If Q is involution then $Q^{-1} = Q$. So, from (6) and since G is involution too

$$\begin{aligned} Q(x) &= G(x) + \gamma f(x) = G \circ H(x) = Q^{-1}(x) \\ &= G\left(x + \gamma f(G(x))\right). \end{aligned}$$

If x is such that $f(x) = 0$ then $G\big(x + \gamma f(G(x))\big) = G(x)$ yielding that $x + \gamma f(G(x)) = x$ since $G \circ G(x) = x$. Thus $f(G(x)) = 0$. If $f(x) = 1$ then

$$G(x) + \gamma = G\left(x + \gamma f(G(x))\right)$$

and one has necessarily $f(G(x)) \neq 0$. Furthermore, according to Theorem 4 and since $G^{-1} = G$, γ is a 0-linear structure of $f \circ G^{-1}$ which is equal to f. The third assertion follows from $Q^{-1} = Q$ and $G^{-1} = G$. Replacing $f \circ G^{-1} = f \circ G = f$ in (6), we get $Q = G \circ H$ which equals $H \circ G$, due to Lemma 1. Conversely, suppose that (i) to (iii) hold. From the first assertion of Theorem 4, we get that Q is a permutation. Note that (ii) implies $Q = H \circ G$. From (6) and (iii), we get that

$$Q^{-1} = G^{-1} \circ H = G \circ H = Q = H \circ G,$$

proving that H is involution, which completes the proof. ■

Remark 2: The conditions, (i) to (iii), of Theorem 5 are quite strong. However it is possible to construct such involutions Q, as we show by the corollary below. In accordance with Definition 1, one can explain a little more about these conditions. Condition (ii) means that f is constant on any pair $(x, G(x))$. Moreover (i) means that $f(x) = f(x + \gamma)$ for all x. This implies that any pair $(x, x+\gamma)$ is either in the support of f or outside this support. We will illustrate this in the next section. Condition (iii) is the fact that the involutions H and G commute and this is clear from Lemma 1.

Corollary 2: Let Q be given by (5) with $G(x) = x^{-1}$ and f is not the null function. Then Q is an involution if and only if either of the following conditions holds:

- (a) $\gamma \neq 1$, with $Tr(\gamma^{-1}) = 0$, and f is 0 everywhere except at the roots of equation $x^2 + \gamma x + 1 = 0$.
- (b) $\gamma = 1$ and one of the following conditions holds:
  - (b.1) If n is odd then $f(x) = 0$ for all $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ and $f(0) = f(1) = 1$;
  - (b.2) If n is even then $f(x) = 0$ unless either $x \in \{0, 1\}$ or $x \in \{y, y + 1\}$ where $y^2 + y + 1 = 0$ or $x \in \{0, 1, y, y + 1\}$.

In the case (a), Q has 4 fixed points. In the case (b), Q has 0 fixed point (case (b.1) and, respectively, $0, 4, 2$ fixed points (case (b.2).

Sketch of proof: Following Theorem 5, Q is an involution if and only if (i)–(iii) hold. Note that (i) means that $H : x \mapsto x + \gamma f(x)$ is a permutation and we have for all $x \in \mathbb{F}_{2^n}$:

$$\begin{aligned} (i) &\iff f(x) = f(x + \gamma) \\ (ii) &\iff f(x^{-1}) = f(x) \\ (iii) &\iff x^{-1} + \gamma f(x^{-1}) = \frac{1}{x + \gamma f(x)}. \end{aligned}$$

Assume that (i)–(iii) hold. Thus (ii) and (iii) imply

$$\left(1 + x\gamma f(x)\right)\left(x + \gamma f(x)\right) = x, \ x \neq 0, \ x + \gamma f(x) \neq 0. \quad (7)$$

If $x = 0$, then (iii) becomes $\gamma f(0) = (\gamma f(0))^{-1}$. This is satisfied if and only if either $f(0) = 0$ or $f(0) = \gamma = 1$. Now assume that $x + \gamma f(x) = 0$ where $f(x) = 1$. Then (iii) becomes $\gamma^{-1} + \gamma = 0$ which leads to $\gamma = 1$, since $\gamma \neq 0$; further $x = 1$. From (i), $f(0) = f(1)$ when $\gamma = 1$.

Assuming that $\gamma \neq 1$, and (7) holds which is, equivalent to

$$f(x) = 0 \text{ or } x^2 + \gamma x + 1 = 0$$

where $Tr(\gamma^{-1}) = 0$, since f is not the null function.

Now $\gamma = 1$. If n is odd then $x^2 + x + 1 = 0$ has no root so that $f(x) = 0$ for $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$. When n is even there are two roots, say y and $y + 1 = y^{-1}$. Thus f can be equal to 1 either at one of the pairs $(0, 1)$ and $(y, y + 1)$ or at both the pairs. On other points f equals 0.

Conversely, assume that f satisfies (a) or (b), *i.e.*, (b.1) or (b.2). Clearly, the involution G is modified by exchanging the values of some pairs of inputs. So we use Theorem 2. ■

V. Involutions piece by piece

We present the following way to construct involutions from involutions in lower dimensions. Let n be a positive integer and $m|n$. Let Q be an involution of $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and F be an involution of $\mathbb{F}_{2^m}$. Then

$$H(x) = \begin{cases} F(x) & \text{if } x \in \mathbb{F}_{2^m} \\ Q(x) & \text{if } x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m} \end{cases} \quad (8)$$

is an involution of $\mathbb{F}_{2^n}$. To illustrate our purpose we present two such constructions of involutions without fixed points.

Proposition 8: Let $n = 2m$. Let $b \in \mathbb{F}_{2^m}^\star$. Let F be an involution of $\mathbb{F}_{2^m}$ with no fixed points. Define

$$H(x) = \begin{cases} F(x) & \text{if } x \in \mathbb{F}_{2^m} \\ \frac{\left(x + bx^{2^m}\right)}{b+1} & \text{if } x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}. \end{cases}$$

Then H is an involution of $\mathbb{F}_{2^n}$ with no fixed points.

Proof: Consider, for any $b \in \mathbb{F}_{2^m}^\star$,

$$Q(x) = \frac{\left(x + bx^{2^m}\right)}{b+1}, x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}.$$

Note that $Q(x) \in \mathbb{F}_{2^m}$ if and only if $x + bx^{2^m} = x^{2^m} + bx$, that is $x \in \mathbb{F}_{2^m}$. Next, using Proposition 5, it is easy to check that Q is an involution of $\mathbb{F}_{2^n}$, then of $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Furthermore, Q has no fixed points in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ since $Q(x) = x$ if and only if either $x = 0$ or $x + bx^{2^m} = x + bx$, that is $x \in \mathbb{F}_{2^m}$. ■

Now let $Q(x) = x^d$, $d^2 \equiv 1 \pmod{2^n - 1}$. Thus the set of fixed points of Q has cardinality $\tau = \gcd(d - 1, 2^n - 1) + 1$; x is a fixed point of Q if $x = 0$ or $x^\tau = 1$. In particular, if $n = km$ and $\tau = 2^m$ this set is $\mathbb{F}_{2^m}$. We construct H by using (8), where F is an involution which has no fixed point in $\mathbb{F}_{2^m}$ and $Q = x^d$. Clearly H has no fixed point.

VI. Fixed points of involutions

The need of involutions in symmetric cryptosystems is clear, as explained in Introduction. In this context, One can read in [10]: "*The graphs obtained by some experimental results indicate a strong correlation between the cryptographic properties and the number of fixed points and suggest that the S-boxes should be chosen to contain few fixed points.*"

But a random permutation of $\mathbb{F}_{2^n}$ has **one** fixed point in average, while a random involution of $\mathbb{F}_{2^n}$ has $\mathbf{2^{n/2}+O(1)}$ fixed points [4] (see [7, VIII.42]). On the other hand a permutation (or involution) which has no fixed point is also subject to some attacks [4].

A. General properties

According to Proposition 1, it is clear that an involution has an even number of fixed points. Thus, it cannot be a so-called *complete permutation*, *i.e.,* say the mappings F and $x \mapsto F(x)+x$, both are bijective. It is because the number of fixed points of F is the number of solutions of the equation $F(x)+x=0$.

Proposition 9: Let F be an involution of $\mathbb{F}_{2^n}$. Then the function $x \mapsto F(x)+x$ cannot be a permutation.

Proof: Set $G(x)=F(x)+x$ and assume that G is a permutation. Thus, there is only one y such that $G(y)=0$. So y is a fixed point of F and it is the only one fixed point. ■

The construction of involutions by adding a constant to a given involution is also linked with its fixed points.

Lemma 4: Let F be a permutation over $\mathbb{F}_{2^n}$ such that $F(0)=0$; consider the permutations defined by $G_a(x)=F(x)+a$ where $a \in \mathbb{F}_{2^n}$. If G_a is an involution then a is a fixed point of F. When F is a linear involution, the number of involutions G_a is exactly the number of fixed points of F.

Proof: First, we have for any a and for all $x \in \mathbb{F}_{2^n}$

$$G_a(G_a(x)) = G_a\left(F(x)+a\right) = F\left(F(x)+a\right)+a.$$

If G_a is an involution then $G_a(G_a(a))=a$ which means $F(a)=a$. Now suppose that F is a linear involution. Then

$$G_a(G_a(x)) = F\left(F(x)\right)+F(a)+a = x+F(a)+a,$$

proving that G_a is an involution whenever a is a fixed point of F. ■

B. Involutions of the form (5)

Let Q be defined by (5) and $H(x)=x+\gamma f(x)$. We begin with the following remark.

Remark 3: Observe that if Theorem 5 holds then

$$Q(x)=G(x)+\gamma f(x)=G(x)+\gamma f(G(x))=H(G(x)). \quad (9)$$

Thus $f \circ Q = f \circ H \circ G = f \circ G \circ H = f \circ H = f$, because $H \circ G = G \circ H$ and γ is a 0-linear structure of f. From (9), one deduces that $G \circ Q = H = Q \circ G$, that is, G and Q commute.

Lemma 5: A point x is a fixed point of Q if and only if $f(x)=0$ and $G(x)=x$ or $f(x)=1$ and $G(x)=x+\gamma$.

Proposition 10: Let G and Q be two involutions linked by the relation $Q(x)=G(x)+\gamma f(x)$. Then, x is a fixed point of G if and only if $Q(x)$ is a fixed point of G. Similarly, x is a fixed point of Q if and only if $G(x)$ is a fixed point of Q.

Proof: Since Q and G commute (Remark 3) we have $G(Q(x))=Q(G(x))$. So $G(x)=x$ implies $G(Q(x))=Q(x)$. Conversely, $G(Q(x))=Q(x)$ implies $Q(G(x))=Q(x)$. Further, $G(x)=x$ since Q is bijective. This proves that Q permutes the set of fixed points of G. The second assertion is similarly proved by exchanging the roles of G and Q in the preceding lines. ■

C. Constructions of involutions without fixed points

We start by observing that $P_a : x \mapsto x+a$ is an involution of $\mathbb{F}_{2^n}$ without fixed point, for any $a \in \mathbb{F}_{2^n}^*$. Our previous results allow us to construct involutions without fixed points which are not so simple. We have proposed a general method in Section V as illustrated by Proposition 8. By Theorem 2, one can reduce the number of fixed points of a given involution as shown in Corollary 2. Proposition 10 shows how the set of fixed points of G is modified by composition. Involutions which have a few fixed points have cryptographic interest.

Proposition 11: Suppose M is an involution and P is a permutation over $\mathbb{F}_{2^n}$, where M does not have any fixed point. Then $F=P^{-1} \circ M \circ P$ is also an involution having no fixed point. More generally, the number of fixed points of M is preserved.

It is to be noted that the ENIGMA cipher and PRINCE block cipher [3] are of the form of F. To find other transformations which preserve or decrease the number of fixed points in any permutation is an interesting research problem.

References

[1] Advanced Encryption Standard. http://en.wikipedia.org/wiki/Rijndael_S-box

[2] A. Biryukov, Analysis of Involutional Ciphers: Khazad and Anubis, *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 2887, pp. 45-53, 2003.

[3] J. Borghoff, A. Canteaut, T. Güneysu, E. Bilge Kavun, M. Knezevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S.S. Thomsen, and T. Yalçın. PRINCE - a low-latency block cipher for pervasive computing applications. In X. Wang and K. Sako (Eds.): *ASIACRYPT 2012*, LNCS 7658,pp. 208-225, 2012.

[4] A. Canteaut, Similarities between Encryption and Decryption: How far can we go?, Stafford Tavares lecture, *Selected Areas in Cryptography* - SAC 2013, Vancouver, Canada, August 2013.

[5] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $GF(2^n)$ for cryptographic purpose. Preprint.

[6] P. Charpin, G.M. Kyureghyan and V. Suder, Sparse permutations with low differential uniformity, *Finite Fields Appl.*, 28 (2014) 214-243.

[7] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press 2009, ISBN 978-0-521-89806-5, pp. I-XIII, 1-810. http://algo.inria.fr/flajolet/Publications/book.pdf

[8] G.M. Kyureghyan, Constructing permutations of finite fields via linear translators, *Journal of Combinatorial Theory*, Series A 118 (2011), 1052-1061.

[9] Y. Yu, M. Wang and Y. Li, Constructing differentially 4 uniform permutations from known ones, Chinese Journal of Electronics Vol.22, No.3, July 2013.

[10] A.M. Youssef, S.E. Tavares and H.M. Heys, A new class of substitution-permutation networks, Proceedings of *selected Areas in Cryptography, SAC-96*, pp 132-147.