Involutions over the Galois field $\mathbb{F}_{2^n}$

Pascale Charpin, Sihem Mesnager, Sumanta Sarkar

***Abstract*—An involution is a permutation such that its inverse is itself (i.e., cycle length ≤ 2). Due to this property involutions have been used in many applications including cryptography and coding theory.**

In this paper we provide a systematic study of involutions that are defined over finite field of characteristic 2. We characterize the involution property of several classes of polynomials and propose several constructions. Further we study the number of fixed points of involutions which is a pertinent question related to permutations with short cycle. In this paper we mostly have used combinatorial techniques.

***Keywords*—Permutation; involution; fixed point; Boolean function; monomial; linear function; switching construction; block-cipher.**

I. Introduction

Permutation polynomials have been extensively studied for their applications in cryptography, coding theory, combinatorial design, etc. Finding new classes of permutations is a challenging task. In many situations, both the permutation polynomial and its compositional inverse are required. For instance, in block ciphers, a permutation is used as an S-box to build the confusion layer during the encryption process. While decrypting the cipher, the compositional inverse of the S-box comes into the picture. Therefore, if both the permutation and its compositional inverse are efficient in terms of implementation, it is advantageous to the designer. This motivates the use of an *involution*, a permutation whose compositional inverse is itself, *i.e.*, the permutation P is such that $P \circ P$ is the identity. For a practical advantage, it is often desired to have permutation polynomials which are easy to implement. One immediate practical advantage of involution is that the implementation of the inverse does not require additional resources, which is particularly useful (as part of a block cipher) in devices with limited resources.

Involutions have been used frequently in block cipher designs, *e.g.*, in AES [1], Khazad, Anubis [2], PRINCE [3]. For instance, in AES the inverse mapping is used as the S-box, which is an involution (see a detailed discussion in [12]). In the block cipher PRINCE [3], an involution was used (denoted by M'). Recently, in [6], behaviour of permutations of an affine equivalent class have been analyzed with respect to some cryptanalytic attacks, and it is shown that involutions are the best candidates against these attacks. It is to be noted that all the discussions in these references are from a cryptographic point of view, and it seems that involutions have rarely been studied in detail as a mathematical object. In [17, Corollary 1] and [9, Lemma 3] (by using [14]), specific types of involutions have been discussed very briefly in the broader context of compositional inverses.

Involutions have been used in coding theory too. For instance, in Gallager's PhD thesis [1], where he proposed LDPC code, used an involution to update check nodes, this way he obtained low-complexity hardware implementation of the sum product algorithm which is used for decoding. This technique is termed as Gallager's involution transform. In another direction there have been some works (for example, [26]) on involution matrices (*i.e.,* on vector space). However, the maximum distance separable (MDS) property of these matrices was the main focus there.

So, a more rigorous study of this important class of permutations (over finite fields) is required. At this point we would like to refer to [10], where we initiated the research on involutions as a combinatorial object in the class of Dickson polynomials. To the best of our knowledge there is no other document in the literature that makes detailed mathematical study of involutions.

In this paper, our purpose is to give basic tools and constructions to use involutions in some context or to develop the study of specific involutions (existence and properties). After preliminaries (Section II), Section III is devoted to monomials and linear involutions. We notably compute the number of monomial involutions over $\mathbb{F}_{2^n}$ (Theorem 3.3) and give some tools to characterize linear involutions. We fully describe the corpus of binary linear involutions (Theorem 3.16). Sections IV and V deal with the construction of new classes of involutions. To exchange outputs two by two by preserving *good* properties is a usual way. The so-called *switching construction* is a more general way. Here we want to preserve the involution property. We give a necessary and sufficient condition to obtain a set of new involutions from one involution using these methods (Theorem 4.1 and 4.11). Applied to the *inverse function*, our results lead to a class of involutions whose properties remain similar to those of the inverse function $x \mapsto x^{-1}$ (Corollary 4.18). Section VI is devoted to the study of the set of fixed points of our proposed constructions.

II. Preliminaries

This paper is on the functions F which are involutions of some finite field of characteristic 2, denoted by $\mathbb{F}_{2^n}$. To any polynomial of $\mathbb{F}_{2^n}[x]$ corresponds a function on $\mathbb{F}_{2^n}$ and we will generally identify this polynomial with its corresponding function.

This work was presented at ISIT 2015 (extended abstract in the proceedings [11]).

P. Charpin is with INRIA-Paris, 2 rue Simone IFF, 75012 Paris (e-mail: Pascale.Charpin@inria.fr).

S. Mesnager is with Department of Mathematics, University of Paris VIII, 2 rue de la liberté, 93526 Saint-Denis Cedex, France and LAGA UMR 7539, CNRS, Télécom ParisTech, France (e-mail: smesnager@univ-paris8.fr).

S. Sarkar is with TCS Innovation Labs, Plot No.1, Software Units Layout, Madhapur, Hyderabad 500 081, India (e-mail: Sumanta.Sarkar@gmail.com).

A. Some background

Let F be a polynomial with coefficients in $\mathbb{F}_{2^k}$, for some nonzero k, We denote by $|E|$ the cardinality of a set E. The trace function from $\mathbb{F}_{2^n}$ onto any subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$ is as follows:

$$Tr_{n/k}(y) = y + y^{2^k} + \cdots + y^{2^{k(n/k-1)}}.$$

The absolute trace function on $\mathbb{F}_{2^n}$ (*i.e.,* $k = 1$) is simply denoted by Tr. For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ the *derivative* of F 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 a property was presented in a more general form in [14]:

Definition 2.1: 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 let b be a fixed element of $\mathbb{F}_{2^k}$. Then γ is a *b-linear translator* of f if

$$f(x) + f(x + u\gamma) = ub \quad \text{for all } x \in \mathbb{F}_{2^n} \text{ and for all } u \in \mathbb{F}_{2^k}.$$

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

$$f(x) + f(x + \gamma) = b \quad \text{for all } x \in \mathbb{F}_{2^n}.$$

B. Involutions, basic properties

Note that an *involution* is a special permutation, but the *involution property* includes the bijectivity as it appears in the classical definition.

Definition 2.2: Let F be any function over $\mathbb{F}_{2^n}$. We say that F is an involution if

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

Example 1: The most known involutions over $\mathbb{F}_{2^n}$ are:

1) The trivial ones: $x \mapsto x + a$, for any constant $a \in \mathbb{F}_{2^n}$;
2) The inverse function $x \mapsto x^{-1}$, for any n;
3) When $n = 2m$ the linear function $x \mapsto x^{2^m}$;
4) The functions $x \mapsto x + \gamma f(x)$ where $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ is any Boolean function with a 0-linear structure γ (see [14, 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 some elements of $\mathbb{F}_{2^n}$ two by two and by fixing the remaining points.

Definition 2.3: Let F be a permutation of $\mathbb{F}_{2^n}$. Let t be a positive integer. A cycle of F is a subset $\{x_1, \cdots, x_t\}$ of pairwise distinct elements of $\mathbb{F}_{2^n}$ such that $F(x_i) = x_{i+1}$ for $1 \leq i \leq t-1$ and $F(x_t) = x_1$. The cardinality of a cycle is called its length.

Remark 2.4: Let $\{x\}$ be a cycle of F of length 1. Then x is a fixed point of F, that is, $F(x) = x$.

Proposition 2.5: An involution has no cycle of length ≥ 3.

Proof: Let x_1, x_2 and x_3 be three elements defined by $x_3 = F(x_2)$ and $x_2 = F(x_1)$. Then $x_3 = F(x_2) = F(F(x_1)) = x_1$ since F is an involution. Therefore, every cycle is of length ≤ 2 as the cardinality of a cycle $\{x_1, \cdots, x_t\}$ must be equal to t. ■

Proposition 2.6: Let F be a permutation of $\mathbb{F}_{2^n}$. Then $\mathbb{F}_{2^n}$ is the union of cycles of F. In particular, if F is an involution then $\mathbb{F}_{2^n}$ is the union of cycles of F with length ≤ 2.

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

$$F^{-1} \circ F(x) = F \circ F(x) = I(x);$$

F is its own *inverse*.

Lemma 2.7: 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 $F \circ G = G \circ F$.

Proof: If F and G are involutions then for all x

$$G \circ F \circ F \circ G(x) = G\left(F \circ F(G(x))\right) = G(G(x)) = x.$$

Now $F \circ G \in \mathcal{V}_n$ if and only if $(F \circ G)^{-1} = F \circ G$. But $(F \circ G)^{-1} = G \circ F$, completing the proof. ■

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 $F \circ G(x) = \left(x^{2^m}\right)^{-1} = \left(x^{-1}\right)^{2^m}$.

Involutions are conserved through some composition.

Lemma 2.8: Let F be an involution on $\mathbb{F}_{2^n}$ and let G be any permutation. Then $G^{-1} \circ F \circ G$ is an involution.

Proof: Simply, $G^{-1} \circ F \circ G$ is its own inverse:

$$\left(G^{-1} \circ F \circ G\right)^{-1} = G^{-1} \circ F^{-1} \circ G = G^{-1} \circ F \circ G.$$

■

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 2.9: 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 $d(F) \geq \lceil 2^{n/2} \rceil$.

Proof: Assume that F is an involution such that $d(F) > 1$. Set $\delta = d(F)$. If $\delta < 2^{n/2}$ then $F \circ F(x)$ has a nonzero term λx^{δ^2} where $\delta^2 \leq (2^{n/2} - 1)^2$. Moreover, any other nonzero term has an exponent less than (and not equal to) δ^2. Thus $F \circ F$ cannot be the identity. ■

Remark 2.10: Now consider the *algebraic degree* of a given involution F, that is the maximal Hamming weight of the 2-adic expansions of exponents:

$$\deg(F) = \max_{i \in I} \{\, wt(i) \,\},\ wt(i) = \sum_{j=0}^{n-1} i_j, \text{ where } i = \sum_{j=0}^{n-1} i_j 2^j.$$

We will see later that there are many involutions with algebraic degree one (linear). Also note that $F = x + Tr(x^{2^k+1})$, is an involution over $\mathbb{F}_{2^n}$ if and only if $Tr(1) = 0$, where $\deg(F) = 2$. Hence the lower bound of $\deg(F)$ for a nonlinear involution F is 2.

Definition 2.11: Let Q be a permutation of $\mathbb{F}_{2^n}$ and let $E \subsetneq \mathbb{F}_{2^n}$. Then E *is stable under* Q if $Q(E) = E$.

III. Some special classes of involutions

A. Monomials

Generally, the compositional inverse of a monomial permutation has a complicated form [15]. In this part we discuss about monomial involutions, which are easily identified.

Proposition 3.1: Let $Q(x) = \lambda x^d$ is a polynomial over $\mathbb{F}_{2^n}$, then $Q(x)$ is an involution if and only if

$$\begin{aligned} \lambda^{d+1} &= 1 \quad \text{and} \\ d^2 &= 1 \pmod{2^n - 1}. \end{aligned} \tag{1}$$

Proof: We have $Q(Q(x)) = \lambda^{d+1} x^{d^2}$. Hence $\lambda^{d+1} x^{d^2} = x$ if and only if $\lambda^{d+1} = 1$ and $x^{d^2} = x \pmod{x^{2^n} + x}$, that is $d^2 = 1 \pmod{2^n - 1}$. ∎

We see that the involutions of the form $x \mapsto x^d$ are fully characterized by (1). First we characterize these monomial involutions when $2^n - 1$ is prime, *i.e.,* is a Mersenne prime.

Proposition 3.2: Let $n > 1$ be a positive integer such that $2^n - 1$ is prime. Then the only monomial involution of the form $x \mapsto x^d$ on $\mathbb{F}_{2^n}$ are the identity $x \mapsto x$ and the inverse function $x \mapsto x^{-1}$.

Proof: As $2^n - 1$ is a prime number, then, equation (1) clearly has two solutions : $d = \pm 1 \pmod{2^n - 1}$. Now assume that $1 < d < 2^n - 2$. We have: $d^2 = 1 \pmod{2^n - 1}$ if and only if $2^n - 1$ divides $(d+1)(d-1)$. Note that the odd prime $2^n - 1$, must be a factor either of $d + 1$ or of $d - 1$, but that is a contradiction. ∎

The next question that strikes in this regard is : what happens when $2^n - 1$ is a composite number. This is equivalent to characterize d such that $d^2 = 1 \pmod{p}$ for all prime factors p of $2^n - 1$. This seems to be hard to characterize, and so is to exhibit all the monomial involutions in that case. Nevertheless, we are able to provide the number of such involutions.

Theorem 3.3: The number of monomial involutions on $\mathbb{F}_{2^n}$ equals 2^s where s is the number of the prime factors in the prime decomposition of $2^n - 1$.

Proof: Given a positive integer p, let us denote by $\rho(p)$, the number of square roots of unity modulo p, that is, the number of solutions of the congruence equation : $x^2 = 1 \pmod{p}$. Let us first show that

$$\rho(pq) = \rho(p)\rho(q), \quad \text{when } p \text{ and } q \text{ are coprime.} \tag{2}$$

To this end, note that according to Chinese's Remainder Theorem, $\mathbb{Z}/(pq)\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ via the isomorphism

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

By construction, in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, $(a, b)^2 = (c, d)$ is equivalent to $a^2 = c$ and $b^2 = d$ so that $\psi(x^2) = (x^2 \pmod{p}, \ x^2 \pmod{q})$, proving (2).

Now, one has $\rho(p^\alpha) = 2$ for any odd prime number p and positive integer α. Indeed, suppose that $x^2 = 1 \pmod{p^\alpha}$. Then

$$x^2 - 1 = (x + 1)(x - 1) = 0 \pmod{p^\alpha}$$

and this is equivalent to

$$x + 1 = 0 \pmod{p^\alpha} \ \text{ or } \ x - 1 = 0 \pmod{p^\alpha},$$

that is $x = \pm 1 \pmod{p^\alpha}$. Since $2^n - 1$ is an odd number, we can write

$$2^n - 1 = \prod_{i=1}^{s} p_i^{\alpha_i}, \quad p_i \in M_n$$

where α_i's are positive integers. Then

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

∎

B. Dickson polynomials

Dickson polynomials $D_k \in \mathbb{F}_2[x]$ are recursively defined by

$$\begin{aligned} &D_0(x) = 0 \text{ and } D_1(x) = x; \\ &D_{k+2}(x) = xD_{k+1}(x) + D_k(x). \end{aligned} \tag{3}$$

We have the following fundamental result concerning Dickson polynomials that are permutations.

Theorem 3.4: [18] The Dickson polynomial $D_k \in \mathbb{F}_2[x]$ is a permutation on $\mathbb{F}_{2^m}$ if and only if $\gcd(k, 2^{2m} - 1) = 1$.

It is shown in [10] that there exist Dickson polynomials that are involutions. The main result is given by the following theorem.

Theorem 3.5: [10] Consider the polynomials D_k, $1 \leq k \leq 2^n - 1$, $n = 2m$ with $m \geq 2$, such that $\gcd(k, 2^n - 1) = 1$. Let S be the set of all square roots of 1 modulo $2^n - 1$ defined by

$$S = \{ \ u \mid 1 \leq u \leq 2^n - 2, \ u^2 = 1 \pmod{2^n - 1} \ \}.$$

Then D_k is an involution on $\mathbb{F}_{2^m}$ if and only if

- $k \in S$, when m is odd;
- $k \in S \cup 2^{m/2} S$ if m is even.

C. Linear involutions

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 propose a detailed study of linear involutions. The following simple lemma is particularly useful for polynomials of $\mathbb{F}_2[x]$, when we try to check the involution property of multinomial linear functions.

Lemma 3.6: 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

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

where $(i, j) \in I \times I$.

Proof: This is directly obtained by expanding $Q \circ Q$:

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

∎

We now give further generalization using a result on the compositional inverse of a linear permutation from [24]. An

explicit form of the compositional inverse of a linear permutation (in general form) is provided there. We state the result for the field $\mathbb{F}_{2^n}$.

Suppose $Q(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ is a linear permutation. It is known that $Q(x)$ is a permutation polynomial if and only if the matrix

$$D_Q \quad = \quad \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^2 & a_0^2 & \dots & a_{n-2}^2 \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{2^{n-1}} & a_2^{2^{n-1}} & \dots & a_0^{2^{n-1}} \end{pmatrix}$$

is nonsingular [19]. The matrix D_Q is called the *associate Dickson matrix* of Q.

Theorem 3.7: [24, Theorem 4.8] Let $Q(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ be a linear permutation over $\mathbb{F}_{2^n}$ and $\overline{a}_i$ denote the $(i,0)$-th cofactor of D_Q, *i.e.,* the determinant of D_Q is

$$det(D_Q) = a_0\overline{a}_0 + \sum_{i=1}^{n-1} a_{n-i}^{2^i}\overline{a}_i.$$

Then the compositional inverse of $Q(x)$ is given by

$$Q^{-1}(x) = \frac{1}{det(D_Q)} \sum_{i=0}^{n-1} \overline{a}_i x^{2^i} \quad . \tag{4}$$

Using Theorem 3.7, we can derive a necessary and sufficient condition on the coefficients of the linear involutions.

Proposition 3.8: The linear polynomial $Q(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ is an involution over $\mathbb{F}_{2^n}$ if and only if

$$\overline{a}_i \quad = \quad det(D_Q) a_i \ , \quad \text{for all } i = 0, \dots, n-1. \tag{5}$$

Proof: Since Q is an involution, then $Q^{-1} = Q$, *i.e.*,

$$\frac{1}{det(D_Q)} \sum_{i=0}^{n-1} \overline{a}_i x^{2^i} \quad = \quad \sum_{i=0}^{n-1} a_i x^{2^i} \quad .$$

Comparing the coefficients of both sides,

$$\overline{a}_i \quad = \quad det(D_Q) a_i \ , \quad \text{for all } i = 0, \dots, n-1.$$

■

Using this result we can derive an interesting necessary condition for involutions which can help identify some classes of linear functions which are not involutions (see Proposition 3.14 later).

Proposition 3.9: Suppose $Q(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ is an involution over $\mathbb{F}_{2^n}$, then

$$a_0^2 + \sum_{i=1}^{n-1} a_i a_{n-i}^{2^i} = 1. \tag{6}$$

Proof: From (5), we have

$$a_0\overline{a}_0 = det(D_Q) a_0^2 \quad \text{for } i = 0,$$

and

$$a_{n-i}^{2^i}\overline{a}_i \quad = \quad det(D_Q) a_i a_{n-i}^{2^i} \quad \text{for all } i = 1, \dots, n-1.$$

Summing all these equations we get

$$a_0\overline{a}_0 + \sum_{i=1}^{n-1} a_{n-i}^{2^i}\overline{a}_i \quad = \quad det(D_Q) \left(a_0^2 + \sum_{i=1}^{n-1} a_i a_{n-i}^{2^i} \right),$$

that is,

$$det(D_Q) \quad = \quad det(D_Q) \left(a_0^2 + \sum_{i=1}^{n-1} a_i a_{n-i}^{2^i} \right).$$

Therefore,

$$a_0^2 + \sum_{i=1}^{n-1} a_i a_{n-i}^{2^i} = 1.$$

■

Example 3: Suppose $Q(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ is a linear polynomial over $\mathbb{F}_{2^n}$, such that $a_i = 0$ for all $i \in \{0\} \cup \{0, 1, \dots, \lceil \frac{n+1}{2} \rceil\}$. Then Q cannot be an involution, since for such a_i's, Condition (6) does not hold.

In the following, we start with the linear monomials and move to more general results afterwards. According to Proposition 3.1, we directly have:

Proposition 3.10: Let $Q(x) = \lambda x^{2^i}$, where $0 < i < n$ and $\lambda \in \mathbb{F}_{2^n}^*$, then

- For even n, Q is an involution if and only if $i = \frac{n}{2}$ and $\lambda^{2^i+1} = 1$.
- For odd n, Q is not an involution.

Next we consider linear binomials.

Proposition 3.11: Let $Q(x) = ax^{2^i} + bx^{2^j}$, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}^*$, where $i < j < n$. Then we have:

- For odd n, Q can never be an involution.
- For even n, $n = 2m$, Q is an involution if and only if $j = i + m$ and either

$$i = 0 \ \text{ and } \ a^2 + b^{2^m+1} = 1.$$

or m is even,

$$i = \frac{m}{2}, \ ab^{2^i} + a^{2^j} b = 1 \ \text{ and } \ a^{2^i+1} + b^{2^j+1} = 0.$$

Proof: Using Lemma 3.6, we obtain:

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

The exponents e of x belong to the set $\{2i, i+j, 2j\}$ (recall that $i \neq j$) satisfying the inequality $0 \leq e < 2n-2$. Hence, to get $Q \circ Q(x) = x$, two of the three exponents have to be removed. We thus study the different cases:

- $2i = 2j \pmod n$ implies $2j = 2i + n$ which is impossible for odd n. On the other hand if $n = 2m$ then $j = i + m$.
- $2j = j + i \pmod n$ implies $2j = n + i + j$, that is $j = n + i$ which is impossible. The case $2i = j + i \pmod n$ implies $i = n + j$ which is impossible too.

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

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

Further, $2i = n$ only when $i = 0$. In this case, $Q \circ Q(x) = x$ for all x if and only if $a^2+b^{2^m+1} = 1$ (which implies $a \in \mathbb{F}_{2^m}$ and then $ab + a^{2^m}b = 0$). Otherwise we must have $i + j = n$, providing $2i = m$ since $j = m + i$. ∎

We deduce directly two classes of binomial linear involutions.

Corollary 3.12: Let $n = 2m$ and $F(x) = ax + bx^{2^m}$. Then F is an involution on $\mathbb{F}_{2^n}$ for all nonzero a, b such that $a^2 = b^{2^m+1} + 1$.

Corollary 3.13: Let $n = 4k$ and $F(x) = ax^{2^k} + bx^{2^{3k}}$. Let $\mathcal{G}$ be the cyclic subgroup of $\mathbb{F}_{2^n}^*$ of order $2^k + 1$. Then F is an involution on $\mathbb{F}_{2^n}$ for all a, b of $\mathcal{G} \setminus \{1\}$ such that $a + b \in \mathcal{G}$.

Proof: Note that $k+n/2 = 3k$. Since $a, b \in \mathcal{G}$ and 2^k+1 divides $2^{3k}+1$, we have $a^{2^k+1}+b^{2^{3k}+1} = 1+1 = 0$. Further, since a and b are in $\mathbb{F}_{2^{2k}}$, we have

$$ab^{2^k} + ba^{2^{3k}} = ab^{2^k} + a^{2^k}b = (a + b)^{2^k+1} = 1.$$

∎

The class of trinomial linear involutions seems a little more complicated than monomials and binomials. We would like to emphasize that our tools are efficient to treat involution property of linear involutions, and here we apply them for a class of trinomial linear involutions.

Proposition 3.14: Let $Q(x) = a_0x + a_ix^{2^i} + a_jx^{2^j}$, where $0 < i < j$ and a_0, a_i and a_j are all in $\mathbb{F}_{2^n}^*$. Then we have:

(i) If Q is an involution and $j \neq n - i$ then $a_0 = 1$.

(ii) Assume that $j = n - i$ and $a_0 = 1$. If $a_ia_{n-i}^{2^i} + a_i^{2^{n-i}}a_{n-i} \neq 0$ then Q is not an involution.

(iii) Suppose $n = 2ki$, and $Q(x) = x + a_ix^{2^i} + a_{n-i}x^{2^{n-i}}$ where both a_i and a_{n-i} belong to the subfield $\mathbb{F}_{2^i}$ of $\mathbb{F}_{2^n}$.Then Q is an involution if and only if $n = 4i$ and $a_i = a_{n-i}$.

Proof: Statements (i) and (ii) are directly obtained from (6).

We are going to prove (iii). As both a_i and a_{n-i} belong to the subfield $\mathbb{F}_{2^i}$, so $a_{n-i}^{2^i} = a_{n-i}$ and $a_i^{2^{n-i}} = a_i$. Also, in the expression of $Q(Q(x))$ given by Lemma 3.6, one may note that the coefficients $a_ia_j^{2^i} + a_i^{2^j}a_j$ equal to 0 whenever $i = 0$ and $a_0 = 1$. So we get

$$\begin{aligned} Q(Q(x)) &= x + a_i^2x^{2^{2i}} \\ &+ a_{n-i}^2x^{2^{2(n-i)}} + (a_ia_{n-i} + a_{n-i}a_i)x^n \\ &= x + a_i^2x^{2^{2i}} + a_{n-i}^2x^{2^{2(n-i)}}, \end{aligned}$$

where we must have $2i = 2n-2i \pmod n$, that is $2i = n-2i$ (assuming $i < n - i$). This implies $a_i^2 + a_{n-i}^2 = 0$, *i.e.,* $a_i = a_{n-i}$, completing the proof. ∎

Now we study binary linear involutions.

Proposition 3.15: Let $Q(x) = \sum_{i\in I} x^{2^i}$ with $|I| > 1$. 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

$$\sum_{i\in I} x^{2^{2i}} = x \pmod{x^{2^n} + x}. \tag{7}$$

Proof: By using the expression given in Lemma 3.6, we get (7), since $a_i = 1$ for all i. Clearly $2j = 2i \pmod n$ is impossible for odd n unless $i = j$. ∎

Thus, for even n it is easy to construct linear involutions having binary coefficients. Actually we are able to give the whole expression of such involutions. Also, Equation (7) allows us to count the number of linear polynomials in $\mathbb{F}_2[x]$ which induce involutions of $\mathbb{F}_{2^n}$.

Theorem 3.16: Let $n = 2m$. Denote by $\mathcal{I}_n$ the number of linear involutions over $\mathbb{F}_{2^n}$ of the following form

$$Q(x) = \sum_{i=0}^{n-1} a_ix^{2^i}, \quad \text{where } a_i \in \mathbb{F}_2.$$

Then

$$\mathcal{I}_n = 2 \times \sum_{\tau=0}^{m-1} \binom{m-1}{\tau}.$$

Moreover any such involution Q is defined by a subset J of $\{1, \ldots, m-1\}$ and its expression is as follows

$$Q(x) = x^{2^e} + \sum_{i\in J} x^{2^i} + \sum_{i\in J} x^{2^{m+i}}, \ e \in \{0, m\}.$$

Proof: Let $I = \{i \in [0, n-1] \mid a_i = 1\}$. Proposition 3.15 tells that

$$Q(x) \ \text{ induces an involution if and only if } \sum_{i\in I} x^{2^{2i}} = x.$$

We assume that Q is an involution. We first observe that the integers of the form $2i$ are pairwise distinct. Thus they have to be removed by pairs in such a way that for any $i \in I$, with $0 < i < m$, there is $j \in I$ such that $2i = 2j \pmod n$, that is $j = i + m$.

Note that for any such pair (i, j) we must have $0 < i < m < j$. Indeed only one $i \in I$ has to satisfy $2i = n \mod n$, *i.e.,* either $i = 0$ or $i = m$.

We consider all involutions Q over $\mathbb{F}_{2^n}$ having a fixed number of terms, say s. Set $|I| = s$ and $\tau = (s-1)/2$ for $s \geq 3$. Clearly s must be odd since $Q(1) \neq 0$. If $s = 1$ then $Q(x) \in \{x, x^{2^m}\}$ and $\tau = 0$ by convention. For $\tau > 0$ fixed, to describe all the involutions we have to choose τ elements, providing all $s - 1 = 2 \times \tau$ elements as follows:

$$0 < i_1 < \cdots < i_\tau < m \ \text{ giving } \ j_k, \ k = 1 \ldots \tau, \ j_k = i_k + m. \tag{8}$$

There are $\binom{m-1}{\tau}$ such choices of τ pairs (i_k, j_k) such that $2i_k = 2j_k$ modulo n. Further, each choice allows to construct two involutions by adding either x or x^{2^m}. This completes the proof on the value of $\mathcal{I}_n$. The exact expression of the involution Q is directly deduced from (8). ∎

We already have seen that linear monomial involutions and linear 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. The simplest case is $x \mapsto x + \gamma Tr(x)$ where $Tr(\gamma) = 0$ (these functions are involutions for any n). We will give a more general result by Corollary 4.7 later; see also Corollary 4.20.

IV. Involution from another involution

A. Exchanging values of a pair of inputs

Recently, Yu, Wang and Li have proposed some new permutations with low differential uniformity [27]. 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 4.1: Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an involution. Let α and β be two nonzero distinct elements of $\mathbb{F}_{2^n}$. Define $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 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.

Proof: Note that obviously G is a permutation whenever F is a permutation. We assume that F is an involution. Let π be the *transposition*[1] of $\mathbb{F}_{2^n}$ that swaps α and β. Note that a transposition is an involution. Now, $G = F \circ \pi$. According to Lemma 2.7, G is an involution over $\mathbb{F}_{2^n}$ if and only if F and π commute over $\mathbb{F}_{2^n}$. Observe that $\pi(x) \neq x$ if and only if $x \in \{\alpha, \beta\}$.

Hence, if G is an involution then $G(x) = F(\pi(x)) = \pi(F(x))$ with

$$\pi(F(x)) \neq F(x) \quad \Longleftrightarrow \quad F(x) \in \{\alpha, \beta\},$$

But, by definition, $G(x) \neq F(x)$ for $x \in \{\alpha, \beta\}$ only. Thus $\{\alpha, \beta\}$ is stable under F.

Conversely, if $\{\alpha, \beta\}$ is stable under F, then $\mathbb{F}_{2^n} \setminus \{\alpha, \beta\}$ is also stable under F. Furthermore, the restriction of F to $\{\alpha, \beta\}$ is either π or the identity map and therefore commutes with π. Next, the restriction of π to $\mathbb{F}_{2^n} \setminus \{\alpha, \beta\}$ being the identity map, it commutes with F over $\mathbb{F}_{2^n} \setminus \{\alpha, \beta\}$. ■

Remark 4.2: One can directly obtain the expression of G from Theorem 4.1. Indeed, set $\gamma = \beta + \alpha$.Then $G(x) = F(x) + \gamma f(x)$, where f is a Boolean function which is 0 everywhere except at α and β.

Remark 4.3: If $\{\alpha, \beta\}$ is stable under F, then only two cases can occur :

(i) $F(\alpha) = \beta$, or equivalently $F(\beta) = \alpha$; in this case α and β are fixed points of G.

(ii) $F(\beta) = \beta$ and $F(\alpha) = \alpha$, *i.e.,* α and β are two fixed points of F but are not fixed points of G.

Remark 4.4: Recently, in a lot of papers, the inverse function has been modified and some cryptographic properties of the derived functions have been studied (see, for instance, [9], [16], [17], [27]). By doing this, the involution property of the inverse function is destroyed in the new function. However, by Theorem 4.1, we exhibit a mapping which preserves the involution property. More precisely, Remark 4.3 shows that we can reduce a pair of fixed points of an involution and hence reduce the total number of fixed points in a new involution.

[1] A transposition is an exchange of two elements of an ordered list with all others staying the same; it is therefore a permutation of two elements.

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

In this subsection 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 [14]. The simplest one is given in Example 1, but a more general definition could give other examples.

We start by giving an instance of a theorem of [14]. Recall that a $\mathbb{F}_{2^k}$-linear function on $\mathbb{F}_{2^n}$ $(n = rk)$ is of the type

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

Also recall *linear translators* from Definition 2.1 in Section II.

Theorem 4.5: [14, 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 $\mathbb{F}_{2^k}$, $h : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, $\gamma \in \mathbb{F}_{2^n}^*$ and let b be a fixed element of $\mathbb{F}_{2^k}$.

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 $\mathbb{F}_{2^k}$. This theorem allows us to construct more involutions, notably linear involutions as we show now.

Corollary 4.6: The hypotheses are those of Theorem 4.5 with $b = 0$. Set $K(x) = x + \gamma h(f(x))$. 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 K is an involution over $\mathbb{F}_{2^n}$; further, if L is an involution which commutes with K then F is an involution too.

Proof: If $b = 0$ then g is the identity in Theorem 4.5 so that F is bijective. And we have

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

as γ is a 0-translator of f. Since L is $\mathbb{F}_{2^k}$-linear, we have: $F = L \circ K$ so that $F^{-1} = K \circ L^{-1}$. According to Lemma 2.7, when L is an involution, F is an involution whenever $K \circ L = L \circ K$. ■

We now give two interesting instances of the previous corollary. We first present a class of linear involutions over $\mathbb{F}_{2^n}$, for any n and later give a specific class (for $n = 2m$).

Corollary 4.7: Let $n = rk$ where $k > 1$ and $r > 1$. Let $\gamma \in \mathbb{F}_{2^n}^*$ and the mapping over $\mathbb{F}_{2^n}$:

$$Q : x \mapsto x + \gamma Tr_{n/k}(x).$$

Then Q is an involution if and only if $Tr_{n/k}(\gamma) = 0$.

Proof: According to Corollary 4.6, Q is an involution if and only if γ is a 0-linear translator of $x \mapsto Tr_{n/k}(x)$. That is

$$Tr_{n/k}(x) + Tr_{n/k}(x + \gamma u) = Tr_{n/k}(\gamma u) = u Tr_{n/k}(\gamma) = 0,$$

for all $u \in \mathbb{F}_{2^k}$, completing the proof. ■

Corollary 4.8: Let $n = 2m$. Let h be any mapping from $\mathbb{F}_{2^m}$ to itself then the mappings F from $\mathbb{F}_{2^n}$ to itself defined by

$$F(x) = h(Tr_{n/m}(x)) + x^e,\ e \in \{1, 2^m\}, \tag{9}$$

are involutions of $\mathbb{F}_{2^n}$.

Proof: One can apply Corollary 4.6 with $L(x) = x^e$ and $\gamma = 1$ to prove that F is an involution. First, observe that 1 is a 0-linear translator of $Tr_{n/m}$ since

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

One then deduces from Corollary 4.6 that F is an involution since L commutes with $K : x \mapsto x + h(Tr_{n/m}(x))$:

$$\begin{aligned} K(x^e) &= x^e + h(Tr_{n/m}(x^e)) = \big(x + h(Tr_{n/m}(x))\big)^e \\ &= (K(x))^e. \end{aligned}$$

■

The bijectivity of functions F, given by (10) in the next example, has been recently discussed in several papers. It is easy to prove that F is a permutation when $\delta \in \mathbb{F}_{2^m}$; we indicate that such F is an involution, since it is an instance of (9). When $\delta \notin \mathbb{F}_{2^m}$ proofs are not so simple [22].

Example 4: Let s be any integer and $\delta \in \mathbb{F}_{2^m}$. Taking $h(y) = (y + \delta)^s$ yields to the involutions

$$F(x) = (x^{2^m} + x + \delta)^s + x^e,\ e \in \{1, 2^m\}. \tag{10}$$

C. Switching constructions

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

$$Q(x) = G(x) + \gamma f(x) \text{ where } \begin{cases} G \text{ is an involution} \\ \gamma \in \mathbb{F}_{2^n}^* \\ f \text{ is any Boolean function.} \end{cases} \tag{11}$$

Such a construction of Q from G is called the *switching construction*. We first recall the conditions for Q to be a permutation.

Theorem 4.9: [7], [8] Let Q be defined by (11), 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,

$$Q^{-1} = G^{-1} \circ H \quad \text{where} \quad H(x) = x + \gamma f(G^{-1}(x)). \tag{12}$$

In the following, one can identify the involutions of the shape (11).

Lemma 4.10: Let Q be defined by (11). If Q is an involution then $f \circ G = f$.

Proof: We use the notation of Theorem 4.9 in the proof. If Q is an involution then $Q^{-1} = Q$. So, from (12) and since G is an involution too

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

If $f(x) = 0$ then $G\big(x + \gamma f(G(x))\big) = G(x)$ yielding that $x + \gamma f(G(x)) = x$, since G is a permutation. Thus $f(G(x)) = 0$. If $f(x) = 1$ then $G(x) + \gamma = G\left(x + \gamma f(G(x))\right)$ and one necessarily has $f(G(x)) \neq 0$. ■

Theorem 4.11: Let Q be defined by (11). Then Q is an 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 an involution. Then, according to Lemma 4.10, $f \circ G = f$. Furthermore, according to Theorem 4.9 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 this $f \circ G^{-1} = f \circ G = f$ in (12), we get $Q = G \circ H$ which equals $H \circ G$ by Lemma 2.7.

Conversely, suppose that (i) to (iii) hold. From the first assertion of Theorem 4.9, we get that Q is a permutation. Note that (ii) implies $Q = H \circ G$. From (12) and (iii), we get that

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

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

Remark 4.12: The conditions, (i) to (iii), of Theorem 4.11 are quite strong. However these conditions are actually held for some f and G and they can be used to construct such involution Q, as we will see later. In accordance with Definition 2.3, condition (i) and (ii) can be explained better. 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. Condition (iii) is the fact that the two involutions H and G are commutative and this is clear from Lemma 2.7.

1) More on the added Boolean function: According to Remark 4.12, the Boolean function f has to satisfy strong properties in order to obtain an involution Q from an involution G. In this subsection, we investigate the *support* of such f, *i.e.,* the set $Supp(f) = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$. More precisely, we try to get explicit description of the support of those f which provides an involution.

Corollary 4.14 (of Theorem 4.11) later leads to a better understanding of the function f when Q is an involution. But we first consider the composition of Q and G.

Corollary 4.13: Let Q be defined by (11). If Q is an involution then Q and G commute. More precisely: $Q \circ G = G \circ Q = H$, with $H(x) = x + \gamma f(x)$.

Proof: We have $Q(x) = G(x) + \gamma f(x)$ where G is an involution. Assuming that Q is an involution, we use Theorem 4.11. Notably, from (iii), we have $H \circ G(x) = G \circ H(x)$, for all $x \in \mathbb{F}_{2^n}$. Thus $Q \circ G = H \circ G \circ G = H$ and $G \circ Q = G \circ G \circ H = H$, proving $Q \circ G = G \circ Q$. ■

Corollary 4.14: Assume that Q, defined by (11), is an involution. Denote by $Supp(f)$ the support of f. Define for any $x \in \mathbb{F}_{2^n}$

$$U_x = \{x,\ G(x),\ x + \gamma,\ G(x + \gamma)\}.$$

Then:

- For any $x \in Supp(f)$, $U_x \subset Supp(f)$ and we have

$$G(x) + G(x + \gamma) = \gamma. \tag{13}$$

Consequently U_x is stable under Q.

- If $x \in Supp(f)$ is a fixed point of G then $x+\gamma$ is a fixed point of G too, *i.e.,* $U_x = \{x,\ x+\gamma\}$. Moreover $Q(x) = x+\gamma$ and $Q(x+\gamma) = x$.

Proof: We assume that $x \in Supp(f)$. Then $x+\gamma \in Supp(f)$ as $f(x) = f(x+\gamma)$ for all x. Since $f \circ G = f$, $G(x)$ and $G(x+\gamma)$ are in $Supp(f)$ too so that U_x is a subset of $Supp(f)$.

Now, $G \circ H = H \circ G$ (from Theorem 4.11), implies

$$Q(x) = H \circ G(x) = G(x) + \gamma = G \circ H(x) = G(x+\gamma).$$

Thus, using (13) and Corollary 4.13, it is easy to check for $x \in Supp(f)$:

$$Q(x) = G(x) + \gamma f(x) = G(x) + \gamma = G(x+\gamma)$$

$$Q(x+\gamma) = G(x+\gamma) + \gamma f(x+\gamma) = G(x) + \gamma + \gamma = G(x)$$

$$Q(G(x)) = G(G(x)) + \gamma f(G(x)) = x + \gamma f(x) = x + \gamma$$

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

We conclude that $Q(U_x) = U_x$ for any $x \in Supp(f)$.

Let $x \in Supp(f)$ such that $G(x) = x$. Thus $Q(x) = x+\gamma$. By using (13) we get directly $G(x+\gamma) = x+\gamma$ and, further,

$$Q(x) = x+\gamma \quad \text{and} \quad Q(x+\gamma) = x+\gamma+\gamma = x.$$

■

Remark 4.15: The set U_x has cardinality 2, when $x \in Supp(f)$ is a fixed point of G. In this case, Q exchanges the two values $G(x) = x$ and $G(x+\gamma) = x+\gamma$ and then removes two fixed points of G. When $x \in Supp(f)$ is not a fixed point of G, it could happen that $G(x) = x+\gamma$, implying that $U_x = \{x, x+\gamma\}$. In this case $Q(x) = x$ and $Q(x+\gamma) = x+\gamma$, *i*.e., Q adds two fixed points to the set of fixed points of G (see Theorem 4.1).

2) Some constructions: Theorem 4.11 has interesting consequences, allowing us to construct new involutions with good properties. In this subsection, we exhibit involutions Q from specific involutions G (as given by (11)). According to Corollary 4.14, we are able to present a general construction.

Theorem 4.16: Let Q be given by (11) where γ and G satisfy:

$$\text{there is an } x \in \mathbb{F}_{2^n} \text{ such that } \ G(x) + G(x+\gamma) = \gamma. \quad (14)$$

Moreover f is such that $Supp(f) = U_x$. Then Q is an involution.

Proof: Recall that $U_x = \{x,\ G(x),\ x+\gamma,\ G(x+\gamma)\}$. Further, according to (14), we have:

$$U_x = \{x,\ G(x),\ x+\gamma,\ G(x)+\gamma\}.$$

Hence, U_x is stable under the transformation $x \in \mathbb{F}_{2^n} \mapsto x+\gamma$. Clearly, $f(x+\gamma) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ proving that the Condition (i) of Theorem 4.11 holds. Now, to prove that Q is an involution, we have to prove that Conditions (ii) and (iii) of Theorem 4.11 are also satisfied.

Since $G(U_x) = U_x$, one has $f(G(y)) = 1$ if $y \in U_x$ and $f(G(y)) = 0$ if $y \notin U_x$ proving (ii). Let $H(y) = y + \gamma f(y)$. Then

$$G(H(y)) = G(y + \gamma f(y)) = G(y) + \gamma f(y)$$

for every $y \in \mathbb{F}_{2^n}$ because of (14). Since $f(y) = f(G(y))$, we have proved (iii), *i.e.,* $G \circ H = H \circ G$. ■

Example 5: Let $n = 9$ and $G(y) = y^d$ with $d = 218$. Since $218 \times 218 = 1$ modulo 511, G is an involution over $\mathbb{F}_{2^9}$. We choose $\gamma \in \mathbb{F}_{2^9}^\star$ in the image of the map $R : y \mapsto y^d + (y+\gamma)^d$. Further we take x such that $R(x) = \gamma$. We get $U_x = \{x, x^d, x+\gamma, (x+\gamma)^d\}$. Let f be defined by $f(y) = 1$ if and only if $y \in U_x$. Then $y \mapsto y^d + \gamma f(y)$ is an involution. Recall that there is a bound on the degree of monomial involutions, which is directly derived from Lemma 2.9: assuming that Q is an involution, with $Q(x) = x^s + \gamma f(x)$ where $x \mapsto x^s$ is an involution. According to Lemma 2.9, $s \geq 2^{n/2}$ for even n and $s \geq 2^{(n+1)/2}$ for odd n.

Proposition 4.17: Let Q be given by (11) where $G(x) = x^s$, $s > 1$, then $s \geq \lceil 2^{n/2} \rceil$.

In the following, we present some specific constructions of involutions. Note that Q is obviously an involution when f is the null function.

Corollary 4.18: Let Q be given by (11) 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 (b.1), (b.2) holds

  (b.1) If n is odd then $f(x) = 0$, $\forall x \in \mathbb{F}_{2^n} \setminus \{0,1\}$ 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)).

Proof: Assume that Q is an involution. We use Corollary 4.14 to determine γ and the support of f. Note that the function $x \mapsto x^{-1}$ has only two fixed points: 0 and 1.

Let $x \in Supp(f)$ providing

$$U_x = \{x, x^{-1}, x+\gamma, (x+\gamma)^{-1}\}.$$

From (13), we get:

$$y^{-1} + (y+\gamma)^{-1} = \gamma \ \text{ where } y \in U_x. \quad (15)$$

Note that if $\gamma = 1$, $y \in \{0,1\}$. Assuming that $\gamma \neq 1$, (15) becomes

$$y^2 + \gamma y + 1 = 0,$$

which has solutions if and only if $Tr(\gamma^{-1}) = 0$.

This means that for such a γ, which is not in $\{0,1\}$, there are only two elements in $Supp(f)$, a pair (y, y^{-1}) with $y^{-1} = y+\gamma$.

Now take $\gamma = 1$. If n is odd then $y^2 + y + 1 = 0$ has no roots in $\mathbb{F}_{2^n}$, since $Tr(1) = 1$, so that $Supp(f) = \{0,1\}$. When n is even, the equation $y^2 + y + 1 = 0$ has two roots,

say y and $y+1=y^{-1}$. Thus either $Supp(f)=\{0,1\}$ or $Supp(f)=\{y,y+1\}$ or $Supp(f)=\{0,1,y,y+1\}$.

Conversely, assume that f satisfies (a) or (b), *i.e.,* (b.1) or (b.2). It is clear that in all cases, the involution G is modified by exchanging the values of some pairs of inputs. Actually we use Theorem 4.1. Only one pair (y,y^{-1}) is concerned in (a):

$$Q(y)=y^{-1}+\gamma=y \quad \text{and} \quad Q(y^{-1})=y+\gamma=y^{-1}$$

and $Q(x)=x^{-1}$ for all $x\neq y$. It is the case (i) of Theorem 4.1 where two fixed points are added. The case (b.1) is when the two fixed points of $x\mapsto x^{-1}$ are removed by doing $Q(0)=1$ and $Q(1)=0$. The case (b.2) is similar to (b.1) and (a) (when two pairs are concerned), respectively. ■

Remark 4.19: The differential uniformity of Q (when $G(x)=x^{-1}$) is known not to be more than 6 (see [9, Section 4.2]). When only two outputs are exchanged, the differential uniformity is studied in [27] for even n.
When G is a linear involution, many constructions are possible.

Corollary 4.20: Let Q be given by (11) with $G(x)$ being a linear involution. Then Q is an involution if and only if

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

Proof: The conditions (i) and (ii) are the same as (i) and (ii) of Theorem 4.11. The condition (iii) becomes, using (13), $G(z)+G(\gamma)+G(z)=\gamma$, which is $G(\gamma)=\gamma$. ■

Remark 4.21: Let $n=2m$. When we apply Corollary 4.20 with $G:x\mapsto x^{2^m}$, condition (iii) becomes $\gamma^{2^m}=\gamma$, that is $\gamma\in\mathbb{F}_{2^m}^*$.

V. Piece by piece construction of involutions

Basically, if E is stable under an involution Q of $\mathbb{F}_{2^n}$ then $Q|_E$ and $Q_{\mathbb{F}_{2^n}\setminus E}$ are involutions of, respectively, E and $\mathbb{F}_{2^n}\setminus E$. That suggests the following way to construct involutions from involutions of 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 let F be an involution of $\mathbb{F}_{2^m}$. Then

$$H(x)=\begin{cases} F(x) & \text{if } x\in\mathbb{F}_{2^m} \\ Q(x) & \text{if } x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}\end{cases} \tag{16}$$

is an involution of $\mathbb{F}_{2^n}$. Simple examples of involutions of $\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$ are the identity function, the inverse function and $x\mapsto x^{2^m}$ when $n=2m$. Another example is given below. This kind of construction allows us to provide an involution with a given number of fixed points.

Proposition 5.1: Let $n=2m$. Let $b\in\mathbb{F}_{2^m}\setminus\{0,1\}$. Let F be an involution of $\mathbb{F}_{2^m}$. 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 $\mathbb{F}_{2^n}$ having the same number of fixed points as F.

Proof: Consider, for $b\notin\{0,1\}$

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

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 Corollary 3.12, it is easy to check that Q is an involution of $\mathbb{F}_{2^n}$, so is 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 $x\in\mathbb{F}_{2^m}$. ■

VI. Fixed points of involutions

The number of fixed points of a permutation (in particular, involution) is an important cryptographic criteria. In this context, one may read [25]: *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.*

A random permutation of $\mathbb{F}_{2^n}$ has **O(1)** of fixed points, while a random involution of $\mathbb{F}_{2^n}$ has $\mathbf{2^{n/2}}$+**O(1)** fixed points [5] (see [13, VIII.42]). Therefore, a permutation (involution) with no fixed points or more than **O(1)** fixed points can be distinguished from the random permutation, and thus can be attacked (see [5]). The so-called "reflection ciphers" depend on involutions, however, these involutions should be chosen carefully, as [4] pointed out that such involutions should have no fixed points. In [21], an attack against such ciphers was presented that exploited the set of fixed points of the involutions.

A. General properties

According to Proposition 2.6, it is clear that an involution over $\mathbb{F}_{2^n}$ has an even number of fixed points. Using this we have the following result.

Proposition 6.1: 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, this contradicts the fact that F has even number of fixed points. ■
Thus, we see that an involution F over $\mathbb{F}_{2^n}$ cannot be a so-called *complete permutation*, *i.e.,* F and $x\mapsto F(x)+x$ are both bijective [20]. A complete mapping is called *orthomorphism* in cryptology and appears in the design of some block ciphers [23].

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

Lemma 6.2: 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 if and only if a is a fixed point of F. ■

To have control of the number of fixed points is important for applications in cryptology. Let $a \in \mathbb{F}_{2^n}^*$ and $P_a : x \mapsto x + a$. Then P_a is an involution over $\mathbb{F}_{2^n}$ which has no fixed point. Moreover, for any permutation P, $P^{-1} \circ P_a \circ P$ is an involution without any fixed point. The more general property is as follows.

Proposition 6.3: Suppose M is an involution over $\mathbb{F}_{2^n}$ having τ fixed point. and P is a permutation over $\mathbb{F}_{2^n}$. Then

$$F = P^{-1} \circ M \circ P,$$

is an involution having τ fixed point.
It is to be noted that the ENIGMA cipher and PRINCE block cipher [3] are of the form of F.

B. Fixed point of some special classes of involutions

We start with monomial involutions.

Proposition 6.4: Suppose that $Q : x \mapsto x^d$ is an involution, then the nonzero fixed points of Q form a cyclic subgroup of $\mathbb{F}_{2^n}^*$ of order τ with $\tau = \gcd(d-1, 2^n-1)$.

Proof: Recall that $d^2 = 1 \pmod{2^n - 1}$, since Q is an involution. From $x^d + x = 0$ we have $x(x^{d-1}+1) = 0$, so the set of nonzero fixed points is the set of x such that $x^{d-1} = 1$. ■

This is an interesting tool which gives us the control of choosing the number of fixed points of involutions.

In particular, if $n = km$ and $\tau = 2^m - 1$, the set of fixed points of Q is $\mathbb{F}_{2^m}$. Consider the function H, constructed by (16), where F is an involution which has ρ fixed points in $\mathbb{F}_{2^m}$, and take $Q(x) = x^d$. Clearly H has ρ fixed points too.

Restricting to the case of linear involutions, the number of fixed points can be easily lower bounded.

Lemma 6.5: [21, Lemma 1] Let Q be a linear involution over $\mathbb{F}_{2^n}$. Then the number of fixed points of Q is greater than or equal to $2^{n/2}$.

According to Theorem 3.16, we are able to construct linear involutions over $\mathbb{F}_{2^n}$, where $n = 2m$, which have exactly 2^m fixed points. We prove below that starting from a linear permutation over $\mathbb{F}_{2^m}$ (with coefficients in $\mathbb{F}_2$) one can construct a linear involution whose set of fixed points is $\mathbb{F}_{2^m}$.

Theorem 6.6: Consider any involution $Q(x) = \sum_{i=0}^{n-1} a_i x^{2^i}$ of $\mathbb{F}_{2^n}$, where a_i's are in $\mathbb{F}_2$. Let J be the subset of $\{1, \ldots, m-1\}$ defining Q (according to Theorem 3.16). Denote by $Fix(Q)$ the set of fixed points of Q. Define two functions over $\mathbb{F}_{2^m}$

$$Q_e(y) = \xi y + \sum_{i \in J} y^{2^i},\ y \in \mathbb{F}_{2^m},\ e \in \{0, m\},$$

where $\xi = 1$ if $e = m$ and $\xi = 0$ if $e = 0$. Thus $Fix(Q) = \mathbb{F}_{2^m} \cup Ker(Q_e)$, where e is either 0 or m. Consequently, $Fix(Q) = \mathbb{F}_{2^m}$ if and only if Q_e permutes $\mathbb{F}_{2^m}$.

Proof: Recall that $x \in Fix(Q)$ if and only if $Q(x) + x = 0$. In Theorem 3.16, we have proved that the expression of such Q is:

$$Q(x) = x^{2^e} + \sum_{i \in J} (x + x^{2^m})^{2^i}, \quad e \in \{0, m\}.$$

Thus $\mathbb{F}_{2^m} \subseteq Fix(Q)$ for each value of e. Now define the function f from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ as $f(x) = x + x^{2^m}$. Thus we get two functions, Q_e with $e \in \{0, m\}$, over $\mathbb{F}_{2^m}$:

$$Q_0(y) = \sum_{i \in J} y^{2^i},\ y \in \mathbb{F}_{2^m},\ Q_0(f(x)) = Q(x) + x \text{ for } e = 0,$$

and

$$Q_m(y) = y + \sum_{i \in J} y^{2^i},\ y \in \mathbb{F}_{2^m},\ Q_m(f(x)) = Q(x) + x,$$

for $e = m$. Thus, $x \notin \mathbb{F}_{2^m}$ is a fixed point of Q if and only if $f(x)$ is in the kernel of Q_0 (respectively. Q_m). Hence $Fix(Q) = \mathbb{F}_{2^m}$ if and only if Q_0 (respectively. Q_m) permutes $\mathbb{F}_{2^m}$. ■

Let $Q = H \circ G$ where G is an involution and $H : x \mapsto x + \gamma f(x)$. Recall that $Q = G \circ H = H \circ G$ and $Q \circ G = G \circ H$ (Corollary 4.13). Then, we have the following obvious result.

Proposition 6.7: An input x is a fixed point of Q if and only if $f(x) = 0$ and $G(x) = x$ or $f(x) = 1$ and $G(x) = x + \gamma$.

Remark 6.8: Proposition 6.7 says that G and Q can have a different fixed point only if $f(x) = 1$. Indeed, when $f(x) = 0$, any fixed point of G is a fixed point of Q. However, when $f(x) = 1$,

- if $G(x) = x$ then x is not a fixed point of Q,
- if $G(x) = x + \gamma$ then x is a fixed point of Q,
- if $G(x) \notin \{x, x + \gamma\}$ then x is not a fixed point of Q.

Therefore, setting $M = \#\{x \in \mathbb{F}_{2^n} \mid Q(x) = x\}$, we have

$$\begin{aligned} M &= \#\Big(\{x \in \mathbb{F}_{2^n} \mid G(x) = x\} \cap Supp(f+1)\Big) \\ &\quad + \#\Big(\{x \in \mathbb{F}_{2^n} \mid G(x) = x + \gamma\} \cap Supp(f\Big). \end{aligned}$$

Proposition 6.9: Let G and Q be two involutions having 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: Suppose that x is a fixed point of G then $Q(x)$ is a fixed point of G too, since $G(Q(x)) = Q(G(x)) = Q(x)$ (Corollary 4.14). Conversely suppose that x is such that $Q(x)$ is a fixed point of G. Then $G(Q(x)) = Q(x)$. Since $G(Q(x)) = Q(G(x))$, $Q(G(x)) = Q(x)$ proving that $G(x) = x$ since Q is bijective. This proves that Q permutes the set of fixed point of G.

To prove the second assertion, it suffices to observe that the roles of G and Q can be exchanged in the previous lines. ■

VII. Conclusions

In this paper, we have presented some general results on involutions over $\mathbb{F}_{2^n}$. We have proposed several constructions providing new involutions, and presented results on the number of fixed points of involutions which has cryptographic interest. All these results give further insight into involutions that can be useful in bringing new constructions of involutions having good cryptographic properties such as high nonlinearity, low differential uniformity, etc. Thus, our work leads to many open problems which will interest a large community.

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] C. Boura, A. Canteaut, L.R. Knudsen and G. Leander, "Reflection ciphers", In Proceedings of the Ninth International *Workshop on Coding and Cryptography* (WCC-2015), Paris, April 13-17, 2015.

[5] 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.

[6] A. Canteaut and J. Roué, "On the behaviors of affine equivalent Sboxes regarding differential and linear attacks", EUROCRYPT 2015, Lecture Notes of Computer Sciences, to appear.

[7] P. Charpin and G. Kyureghyan, "On a class of permutation polynomials over $\mathbb{F}_{2^n}$". SETA 2008, Lecture Notes in Comput. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368-376, 2008.

[8] P. Charpin and G. Kyureghyan, "When does $G(x) + \gamma Tr(H(x))$ permute $\mathbb{F}_{2^n}$?" *Finite Fields Appl.*, 15 (5) pp. 615-632, 2009.

[9] P. Charpin, G. Kyureghyan and V. Suder, "Sparse permutations with low differential uniformity", *Finite Fields Appl.*, 28 pp. 214-243, 2014.

[10] P. Charpin, S. Mesnager and S. Sarkar, "Dickson polynomials that are involutions", *Finite Fields and Applications - Fq12 - Saratoga, USA, July 13-17, 2015. IACR Cryptology ePrint Archive* 2015/434.

[11] P. Charpin, S. Mesnager and S. Sarkar, "On involutions of finite fields", In *Proceedings of the 2015 IEEE International Symposium on Information Theory*, ISIT 2015, Hong-Kong, China, 2015.

[12] R. Elumalai and A.R.Reddy, "Improving diffusion power of AES Rijndael with 8×8 MDS matrix", *International Journal of Scientific & Engineering Research*, Volume 2, Issue 3, March 2011.

[13] 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

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

[15] G. Kyureghyan and V. Suder, On inversion in Z_{2^n-1}, *"Finite Fields and Their Applications"*, Elsevier, 25, pp. 234-254, 2014.

[16] Y. Li and M. Wang, "Permutation polynomials EA-equivalent to the inverse function over $GF(2^n)$", *Cryptogr. Commun.* 3 pp. 175-186, 2011.

[17] Y. Li, M. Wanga and Y. Yu, Constructing differentially 4-uniform permutations over $GF(2^{2k})$ from the inverse function revisited, *Cryptology ePrint Archive*, Report 2013/731.

[18] R. Lidl, G.L. Mullen and G. Turnwald, *"Dickson Polynomials"*, Pitman Monographs in Pure and Applied Mathematics, Vol. 65, Addison-Wesley, Reading, MA, 1993.

[19] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications. vol. 20, second edition, Cambridge University Press, 1997.

[20] H. Niederreiter and K.H. Robinson, "Complete mappings of finite fields", *J. Austral. Math. Soc.* (Series A) 33 pp. 197-212, 1982.

[21] H. Soleimany, C. Blondeau, X. Yu, W. Wu, K. Nyberg, H. Zhang, L. Zhang, and Y. Wang, "Reflection cryptanalysis of PRINCE-like ciphers". *J. Cryptology* 28, no. 3, pp. 718-744, 2015.

[22] Z. Tu, X. Zeng and Y.Jiang, "Two classes of permutation polynomials having the form $(x^{2^m}+x+\delta)^s+x$". *Finite Fields Appl.* 31 pp. 12-24, 2015.

[23] S. Vaudenay, "On the Lai-Massey scheme", Advances in Cryptology - ASIACRYPT'99 Volume 1716 of the series Lecture Notes in Computer Science pp 8-19, 1999.

[24] B. Wu and Z. Liu, "Linearized polynomials over finite fields revisited", *Finite Fields Appl.* 22 , pp. 79-100, 2013.

[25] 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, 1996.

[26] A. M. Youssef, S. Mister and S. E. Tavares, "On the Design of Linear Transformations for Substitution Permutation Encryption Networks", Proceedings of *Selected Areas in Cryptography, SAC-97*, pp. 40-48, 1997.

[27] 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.

Pascale Charpin received the Ph.D. degree and the Doctorate in Sciences (Theorical Computer Science) from the University of Paris VII, France, in 1982 and 1987, respectively. She was with the department of Mathematics at the University of Limoges, France, from 1973 to 1982. From 1982 to 1989, she has worked at the University of Paris VI. She is currently Director of Research (Emeritus) at INRIA, the French National Institute for Research in Computer Science, in Paris. She was the scientific head of the group CODES (coding and cryptography) in this institute from 1995 to 2002. Her research interests include finite algebra, algorithmic and applications to coding (error-correcting coding and cryptology). Dr. Charpin served on the Editorial Board of the *IEEE Transactions on Computers* (from 2000 to 2004) and serves on the Editorial Board of *Designs, Codes and Cryptography* (from 2002) and *Finite Fields and their Applications* (from 2013).

Sihem Mesnager received the Ph.D. degree in Mathematics from the University of Pierre et Marie Curie (Paris VI), Paris, France, in 2002 and the Habilitation to Direct Theses (HDR) in Mathematics from the University of Paris VIII, France, in 2012. Currently, she is an associate Professor in Mathematics at the University of Paris VIII (France) in the laboratory LAGA (Laboratory of Analysis, Geometry and Applications), University of Paris XIII and CNRS. She is also Professor adjoint to Telecom ParisTech (France), research group MIC2 in mathematics of the department INFERES, Telecom ParisTech (ex. National high school of telecommunications). Her research interests include discrete Mathematics, Boolean functions, Cryptology, Coding theory, Commutative Algebra and Computational Algebraic Geometry. She is Editor in Chief of the International Journal of Information and Coding Theory (IJOCT) and an Associate Editor for the international journal IEEE Transactions on information Theory (IEEE-IT). She also serves the editorial board of the international journal Advances in Mathematics of Communications (AMC), the international journal Cryptography and Communications Discrete Structures, Boolean Functions and Sequences (CCDS) and the international journal RAIRO ITA (Theoretical Informatics and Applications). She was a program co-chair for International Workshop on the Arithmetic of Finite Fields (WAIFI) in 2014 and International Conference on coding and Cryptography (ICCC) in 2015 and served on the board of program comitties of several international conferences and workshops (Africacrypt 2009, SETA 2010, SETA 2014, WCC 2011, WCC 2013, WCC 2015, International Workshop Castle Meeting on Coding Theory and Applications in 2014, ICCC 2015, ACA 2015, WAIFI 2016, SETA 2016, ICCA 2016, etc.). She is (co)-author for more than 65 articles, 2 books and gave approx. 65 national and international conferences. Since 2013, she is vice-president of the french Chapter of IEEE in information theory.

Sumanta Sarkar Sumanta Sarkar received his Masters degree in mathematics from the University of North Bengal, India, in 2002. In 2008 he completed his Ph.D. thesis at the Indian Statistical Institute, Kolkata, and obtained his Ph.D. degree from the Jadavpur University, India.

Currently he is a research scientist at TCS Innovation Labs, Hyderabad, India. He was a researcher at INRIA Paris-Rocquencourt from 2008 to 2010, and at University of Calgary from 2011 to 2013. His research interests are in Discrete Mathematics, Information Security, Cryptography, and Coding Theory.