Doubly Perfect Nonlinear Boolean Permutations

Laurent Poinsot

Doubly Perfect Nonlinear Boolean Permutations

Laurent Poinsot

LIPN CNRS UMR 7030, Institut Galilée - Université Paris-Nord, 99, avenue Jean-Baptiste Clément, 93430 Villetaneuse, France

Abstract. Due to implementation constraints the XOR operation is widely used in order to combine plaintext and key bit-strings in secret-key block ciphers. This choice directly induces the classical version of the differential attack by the use of XOR-kind differences. While very natural, there are many alternatives to the XOR. Each of them inducing a new form for its corresponding differential attack (using the appropriate notion of difference) and therefore block-ciphers need to use S-boxes that are resistant against these nonstandard differential cryptanalysis. In this contribution we study the functions that offer the best resistance against a differential attack based on a finite field multiplication. We also show that in some particular cases, there are robust permutations which offers the best resistant against **both** multiplication and exponentiation based differential attacks. We call them *doubly perfect nonlinear permutations*.

Keywords: finite field, perfect nonlinear function, group action.

1 Introduction

Shannon has introduced in [13] the notions of *diffusion* and *confusion* which have been mainly accepted and successfully used by cryptologists as guidelines in their work to design secret-key ciphers. These notions accurately set up a category of "nice" cryptographic objects namely the iterative block-ciphers such as the Data and Advanced Encryption Standards (see [3, 4]). Such an algorithm works as an iteration of a certain procedure called the round function. This functions is made in two pieces, a linear and a nonlinear parts, whose roles are to satisfy Shannon's diffusion and confusion. Diffusion refers to a sensitivity to the initial conditions: a small deviation in the input should cause a large change at the output. The linear part of the round-function is devoted to provide a good level of diffusion. The goal of confusion is to hide the algebraic relations between the plaintext and the secret-key in order to make harder the statistical attacks. This is exactly the role assumed by the nonlinear part, also called *S-boxes*. One of the major attacks for which the S-boxes should be highly resistant is the *differential cryptanalysis* [1] or its "dual" counter-part the *linear attack* [5]. The differential cryptanalysis is intrinsically related to the fashion the plaintexts and the round-keys are combined at each step. As to interlock plaintexts with keys, the XOR or component-wise modulo-two sum (or the addition in characteristic 2) is usually chosen because of its implementation efficient nature. A block-cipher is

then vulnerable to the differential attack if there is a nonzero XOR difference of two plaintexts such that the difference in output is statistically distinguishable from a random variable that follows a (discrete) uniform law. The S-boxes that offer the best resistance against such an attack are the *perfect nonlinear functions* [7]. As very particular combinatorial objects, perfect nonlinear functions do not exist in every configurations. For instance if one works in finite elementary Abelian 2-groups, which in practice is usually the case, precisely because of the involutive nature of the addition, perfect nonlinear permutations can not exist. Since, yet in practice the plaintexts and ciphertexts have the same length, we can not use perfect nonlinear permutations as S-boxes. So in many cases block-ciphers exploit suboptimally differentially resistant functions, such as *almost perfect nonlinear* [6] or even *differentially* 4*-uniform* [8] functions.
We make two simple observations. We have seen above that by nature, the XOR prohibits the existence of perfect nonlinear permutations. Moreover apart from the XOR operation, the combination law of plaintexts and keys can take many forms. While really efficient by nature the XOR is a very specific case of group action and it could be interesting to use another one. Roughly speaking (more details are given in subsection 2.2) a group action is nothing but a particular external operation of a group on a set (as the scalar multiplication of vectors). The set in question is the collection of all the possible plaintexts. The set of (round) keys is endowed with a group structure and operates on the messages. Such a very general block-cipher could be vulnerable to a modified differential attack which should be no more related to the XOR differences but to the appropriate group action differences. In [12] is presented the algorithm of a such an attack. Therefore the determination of the best resistant S-boxes or in other terms the adapted concept of perfect nonlinear functions, is needed. The theoretic description of such functions covers the following contributions [9, 10, 11] and the most important definitions and relevant results upon them are recalled in section 2.
We earlier say that altough natural, the XOR is not the only way to combine bit-strings. In the finite field setting the multiplication also may be used. The S-boxes that maximally resist against a differential attack based on the multiplication rather than the addition are called *multiplicatively perfect nonlinear functions* and in this paper we prove the existence of permutations with such a cryptographic property in many situations (and in most cases than classical perfect nonlinear functions). In addition, in some very particular cases, the multiplicative group $\mathbb{K}^*$ of a finite field $\mathbb{K}$ in characteristic two can be equipped with another multiplication, which is distributive on the classical one. With this second multiplication (which is merely an exponentiation), $\mathbb{K}^*$ turns to be a finite field itself (but no more of characteristic two). This paper has as its major goal the construction of Boolean permutations over $\mathbb{K}$ which are perfect nonlinear with respect to **both** multiplications of the new field. They are called *doubly perfect nonlinear Boolean permutations* and can be seen as relevant alternatives to the use of almost perfect nonlinear permutations.

2 Classical and generalized situations

2.1 Notations and conventions

In this contribution the term *function* has the same meaning as the expression *total function*. If X is a finite set then $|X|$ is its cardinality and Id_X its identity map. For $f : X \to Y$ and $y \in Y$ we define as usually the fibre $f^{-1}(\{y\}) = \{x \in X | f(x) = y\}$. For a additive group $(G, +, 0)$ (resp. a multiplicative group $(G, ., 1)$) we define $G^* = G \setminus \{0\}$ (resp. $G^* = G \setminus \{1\}$). For a unitary ring $(R, +, 0, ., 1)$ we have $R^* = R \setminus \{0\}$ and $R^{**} = R^* \setminus \{1\} = R \setminus \{0, 1\}$. Moreover the group of units of R (*i.e.* the group of invertible elements of the ring) is denoted $U(R)$ and obviously $U(R)^* = U(R) \setminus \{1\}$. In order to simplify the notations we sometimes identify a group (or a ring) with its underlying set. The ring of integers modulo n is denoted $(\mathbb{Z}_n, +, 0, ., 1)$ and its underlying set is identified with the particular system of representatives of residue classes $\{0, 1, \ldots, n-1\}$. The finite field of characterisitic p with p^m elements is denoted $\mathsf{GF}(p^m)$. A prime field $\mathsf{GF}(p)$ is identified with $\mathbb{Z}_p$ and therefore with $\{0, 1, \ldots, p-1\}$. Finally $Aut(G)$ denotes the set of all group automorphisms of a group G.

2.2 Group actions

Essential to everything that we shall discuss in this paper is the notion of group actions.
Let G be a group and X a nonempty set. We say that G *acts on* X if there is a group homomorphism $\phi : G \to S(X)$, where $S(X)$ is the group of permutations over X. Usually for $(g, x) \in G \times X$, we use the following convenient notation

$$g.x := \phi(g)(x) \tag{1}$$

and so we hide any explicit reference to the morphism ϕ. An action is called *faithful* if the corresponding homomorphism ϕ is one-to-one. It is called *regular* if for each $(x, y) \in X^2$ there is one and only one $g \in G$ such that $g.x = y$. A regular action is also faithful.

Example 1.

- A group G acts on itself by (left) translation: $g.x := gx$ for $(g, x) \in G^2$ (G is here written multiplicatively). This action is regular;
- A subgroup H of a group G also acts on G by translation: $h.x := hx$ for $(h, x) \in H \times G$. This action is faithful and if H is a proper subgroup, then the action is not regular;
- The multiplicative group $\mathbb{K}^*$ of a field $\mathbb{K}$ acts on $\mathbb{K}$ by the multiplication law of the group. This action is faithful but not regular since 0 is fixed by every elements of $\mathbb{K}^*$. More generally the action of $\mathbb{K}^*$ on a $\mathbb{K}$-vector space by scalar multiplication is also a faithful action (in this case the null vector is fixed by any scalar multiplication).

2.3 Group action perfect nonlinearity

Let X and Y be two finite nonempty sets. A function f is called *balanced* if for each $y \in Y$,

$$|\{x \in X | f(x) = y\}| = \frac{|X|}{|Y|} \ . \tag{2}$$

With the concept of group actions we now have all the ingredients to recall the notion of group action perfect nonlinearity (see [10]).

Definition 1. Let G be a finite group that acts faithfully on a finite nonempty set X. Let H be a finite group (written additively). A function $f : X \to H$ is called *perfect nonlinear* (by respect to the action of G on X) or *G-perfect nonlinear* if for each $\alpha \in G^*$, the *derivative of f in direction α*

$$\begin{aligned} d_\alpha f : X &\to H \\ x &\mapsto f(\alpha.x) - f(x) \end{aligned} \tag{3}$$

is balanced or in other words for each $\alpha \in G^*$ and each $\beta \in H$,

$$|\{x \in X | d_\alpha f(x) = \beta\}| = \frac{|X|}{|H|} \ . \tag{4}$$

As we can see our definition coincides with the classical one (see [2]) in the classical situations (G acts on itself by left translation).

3 Doubly perfect nonlinear Boolean permutations

In the finite fields settings there are two main natural group actions, namely additive and multiplicative translations. The first one is the standard used as plaintext and key combination process and has been widely studied in terms of (classical) perfect nonlinearity and/or bentness. In this contribution we focus on the second one: we construct perfect nonlinear functions by respect to multiplication rather than addition called *multiplicatively perfect nonlinear functions*. Moreover in very particular cases, multiplication can be seen as an addition of a new finite field. In this paper we exhibit some perfect nonlinear functions by respect to both original and new multiplications called *doubly perfect nonlinear functions*.

3.1 Multiplicatively perfect nonlinear functions

Let us begin with a lemma whose proof is a triviality.

Lemma 2. *Let G and H be two finite groups (written multiplicatively). Let λ be a group homomorphism from G to H. For each $\beta \in \lambda(G)$,*

$$|\lambda^{-1}(\{\beta\})| = |\ker \lambda| \ . \tag{5}$$

Let d and m be two nonzero integers. We denote by $V(p,m,d)$ any d dimensional vector space over the finite field $\mathsf{GF}(p^m)$. We use the same symbols "$+$" (resp. "$-$") to denote both additions (resp. substractions) of $V(p,m,d)$ and $\mathsf{GF}(p^m)$ and $\alpha.v$ is the scalar multiplication of $v \in V(p,m,d)$ by $\alpha \in \mathsf{GF}(p^m)$.

Lemma 3. *Let $d,\ e,\ m,\ n > 0$ be any integers. Let λ be a group homomorphism from $(V(p,m,d),+)$ to $(V(p,n,e),+)$. Let G be a subgroup of the group $\mathsf{GF}(p^m)^*$. Then for each $\beta \in \lambda(V(p,m,d))$ and for each $\alpha \in G^*$,*

$$|\{v \in V(p,m,d) | d_\alpha \lambda(v) = \beta\}| = |\lambda^{-1}(\{\beta\})| = |\ker \lambda| \ . \tag{6}$$

The proof of the previous lemma is not difficult and thus is not given here.

Theorem 4. *Let $d,\ e,\ m,\ n > 0$ be any integers such that $d^m \geq e^n$. Let λ be a group epimorphism*[1] *from $(V(p,m,d),+)$ onto $(V(p,n,e),+)$. Then λ is $\mathsf{GF}(p^m)^*$-perfect nonlinear.*

Proof. Since λ is onto, every $\beta \in V(p,n,e)$ belong to $\lambda(V(p,m,d))$. According to lemma 3 with $G = \mathsf{GF}(p^m)^*$, for each $\beta \in V(p,n,e)$ and for each $\alpha \in \mathsf{GF}(p^m)^{**} = \mathsf{GF}(p^m) \setminus \{0,1\}$, $|\{v \in V(p,m,d) | d_\alpha \lambda(v) = \beta\}| = |\lambda^{-1}(\{\beta\})| = |\ker \lambda|$. But $\{\lambda^{-1}(\{\beta\})\}_{\beta \in V(p,n,e)}$ is a partition of $V(p,m,d)$. Therefore we have $|V(p,m,d)| = \sum_{\beta \in V(p,n,e)} |\lambda^{-1}(\{\beta\})| = |\ker \lambda| |V(p,n,e)|$. So $|\ker \lambda| = \frac{|V(p,m,d)|}{|V(p,n,e)|} = p^{md-ne}$. □

In classical situations it is well-known that if a function $f : V(2,m,d) \to V(2,n,e)$ is bent then md is an even integer and $md \geq 2ne$. Replacing addition by multiplication allows us to find "bent" function even if md is an odd integer and/or $2ne > md \geq ne$. When $md = ne$ (and $p = 2$), almost perfect nonlinear (APN) functions are relevant for cryptographic purposes. They are defined (see [6]) by the fact that the equation $d_\alpha f(x) = \beta$ with x as an unknown has at most two solutions for each $\alpha \neq 0$ and each β. The only known examples of APN permutations need md to be an odd integer. In our case by construction any $\mathsf{GF}(p^m)$-linear isomorphism of $V(p,m,d)$ is a $\mathsf{GF}(p^m)^*$-perfect nonlinear; so it is also the case for $p = 2$ and md an even integer.

3.2 Doubly perfect nonlinear Boolean permutations

The group of units $\mathsf{GF}(p^m)^*$ of the finite field $\mathsf{GF}(p^m)$ can be equipped with another multiplication that turns it into a unitary commutative ring. Indeed let γ be a primitive root of $\mathsf{GF}(p^m)$. The *exponential*

$$\begin{array}{rccc} e_\gamma : & (\mathbb{Z}_{p^m-1},+) & \to & \mathsf{GF}(p^m)^* \\ & i & \mapsto & \gamma^i \end{array} \tag{7}$$

is a group isomorphism (in the remainder we always suppose that such a primitive root γ is fixed). We can use it to turn $\mathsf{GF}(p^m)^*$ into a commutative unitary

[1] A **group epimorphism** is a group homomorphism which is onto.

ring, isomorphic to the ring of modulo $p^m - 1$ integers, by[2] $\gamma^i \times \gamma^j = \gamma^{ij}$. We call such a structure $(\mathsf{GF}(p^m), +, 0, ., 1, \times, \gamma)$ a *characteristic* $(p, p^m - 1)$ *field-ring* (which means that $(\mathsf{GF}(p^m), +, 0, ., 1)$ is a characteristic 2 field and $(\mathsf{GF}(p^m)^*, ., 1, \times, \gamma)$ is a characteristic $p^m - 1$ ring *i.e.* $\gamma^{p^m-1} = 1$, $\gamma^i \neq 1$ for all $0 < i < p^m - 1$) or *double-field* when $(\mathsf{GF}(p^m)^*, ., 1, \times, \gamma)$ is also a field. The multiplicative identity of the ring $(\mathsf{GF}(p^m)^*, ., 1, \times, \gamma)$ is $\gamma^1 = \gamma$ and the classical rules of distributivity, absorption and associativity take the following forms $\gamma^i \times (\gamma^j \gamma^k) = (\gamma^i \times \gamma^j)(\gamma^i \times \gamma^k)$, $1 \times \gamma^i = 1$, $\gamma^i \times (\gamma^j \times \gamma^k) = (\gamma^i \times \gamma^j) \times \gamma^k$. The group of units of this ring, $U(\mathsf{GF}(p^m)^*)$, is equal to $\{\gamma^i | i \in U(\mathbb{Z}_{p^m-1})\} = \{\gamma^i | (i, p^m - 1) = 1\}$ (where (i, j) is the greatest common divisor of i and j) and if γ^i is invertible with respect to $\times$ (*i.e.* γ^i is a unit), $(\gamma^i)^{-1} = \gamma^{\frac{1}{i}}$. If $i \neq 0$ is not congruent with 1 modulo $p^m - 1$, then it is a zero divisor in $\mathbb{Z}_{p^m-1}$: it exists $j \in \mathbb{Z}^*_{p^m-1}$ such that $ij = 0$, therefore γ^i is itself a zero divisor[3] in $\mathsf{GF}(p^m)^*$ because $\gamma^i \times \gamma^j = \gamma^{ij} = \gamma^0 = 1$. This ring is an integral domain if and only if $(\mathbb{Z}_{p^m-1}, +, 0, ., 1)$ is itself an integral domain or equivalently a (finite) field. So $(\mathsf{GF}(p^m)^*, ., 1, \times, \gamma)$ is a finite field if and only if $p^m - 1$ is a prime integer. If p is an odd prime number then the only possible choice is $p = 3$ and $m = 1$ (since $3^1 - 1 = 2$) because in the other case $p^m - 1 > 2$ and is even. The following lemma gives a constraint on m when $p = 2$.

Lemma 5. *Let $k \in \mathbb{N}^*$, $k > 1$. Let $m \in \mathbb{N}^*$. If m is not a prime integer then so is $k^m - 1$.*

Proof. Suppose that $m = rs$ where both r and s are integers greater or equal to 2. We will prove that $k^{rs} - 1 = (k^r - 1) \sum_{i=1}^{s} k^{r(s-i)}$ by induction on the integer s.
If $s = 2$ then $k^{2r} - 1 = (k^r - 1)(k^r + 1)$.
Let $s \in \mathbb{N}^*$ such that $s \geq 2$. Suppose that for all integer l such that $1 < l \leq s$, $k^{rl} - 1 = (k^r - 1) \sum_{i=1}^{l} k^{r(l-i)}$. Let us prove that $k^{r(s+1)} - 1 = (k^r - 1) \sum_{i=1}^{s+1} k^{r(s+1-i)}$.
We have

$$\begin{aligned} k^{r(s+1)} - 1 &= k^{r(s+1)} - k^r + k^r - 1 \\ &= k^r(k^{rs} - 1) + (k^r - 1) \\ &= k^r(k^r - 1) \sum_{i=1}^{s} k^{r(s-i)} + (k^r - 1) \text{ (by induction hypothesis)} \end{aligned} \tag{8}$$

$$\begin{aligned} &= (k^r - 1) \left(\sum_{i=1}^{s} k^{r(s+1-i)} + 1 \right) \\ &= (k^r - 1) \sum_{i=1}^{s+1} k^{r(s+1-i)} \ . \end{aligned} \tag{9}$$

[2] More rigorously $\gamma^i \times \gamma^j = e_\gamma(e_\gamma^{-1}(\gamma^i) e_\gamma^{-1}(\gamma^j)) = e_\gamma(ij)$. In fact any calculation in the exponent should be understood modulo $p^m - 1$.
[3] More formally we should say a $\times$-divisor of 1.

□

An integer of the form 2^q-1 where q is a prime number is called a *Mersenne number*. When a Mersenne number is itself a prime integer, it is called a *Mersenne prime*[4]. So given a Mersenne prime $p = 2^q - 1$, $(\mathsf{GF}(2^q)^*, ., 1, \times, \gamma)$ is isomorphic to the prime field $(\mathsf{GF}(p), +, 0, ., 1)$ (which is identified with $(\mathbb{Z}_p, +, 0, ., 1)$) and $(\mathsf{GF}(2^q), +, 0, ., 1, \times, \gamma)$ is a characteristic $(2, p)$ double-field (*i.e.* $(\mathsf{GF}(2^q), +, 0, ., 1)$ is a characteristic 2 field and $(\mathsf{GF}(2^q)^*, ., 1, \times, \gamma)$ is a characteristic p field).

We now characterize the existence of some subgroups of units in rings which will be useful in the sequel.

Lemma 6. *Let R be a non-trivial unitary ring*[5]*. Then -1 is invertible in R.*

Proof. It is obvious since $(-1)(-1) = 1$. □

Lemma 7. *Let $n > 1$. The group of units $U(\mathbb{Z}_n)$ contains at least one subgroup G such that for every $i \in G^*$ (i.e. $i \neq 1$ and $i \in G$), $i - 1 \in U(\mathbb{Z}_n)$ if and only if n is equal to 2 or is an odd integer.*

Proof. If $n = 2$ then $G = U(\mathbb{Z}_2) = \{1\}$ is a group with the good properties. Let suppose that $n > 2$ is an even integer. Then i belongs to $U(\mathbb{Z}_n)$ if and only if $(i, n) = 1$. Therefore i is an odd integer. Then $i-1$ is equal to zero or is an even integer and it is invertible in none of the two cases. Now let suppose that n is an odd integer. Then 2 is invertible modulo n. Since according to lemma 6 (since $n > 1$, $\mathbb{Z}_n$ is non-trivial), -1 is a unit, $-2 = 2(-1) = -1 - 1$ is also invertible. The group $G = \langle -1 \rangle = \{\pm 1\}$ satisfies the assumptions of the lemma. □

We should note that in the particular case where n is a prime number p, $\mathbb{Z}_p^* = U(\mathbb{Z}_p)$ is such a group G. If $n = 2^m - 1$ then n is odd so there is at least one subgroup G of $\mathbb{Z}_{2^m-1}$ such that $\forall i \in G^*$, $i-1 \in U(\mathbb{Z}_{2^m-1})$. If p is an odd prime then $p^m - 1$ is an even number. So unless the trivial case $p = 3$ and $m = 1$, $U(\mathbb{Z}_{p^m-1})$ does not contain any such group G.

Lemma 8. *Let $\gamma^i \in U((\mathsf{GF}(p^m)^*, ., 1, \times, \gamma))$. Then the map*

$$\begin{array}{rccc} \lambda^{\times}_{\gamma^i} : & \mathsf{GF}(p^m)^* & \to & \mathsf{GF}(p^m)^* \\ & \gamma^j & \mapsto & \gamma^i \times \gamma^j \ . \end{array} \tag{10}$$

is a group automorphism of $(\mathsf{GF}(p^m)^*, ., 1)$.

Proof. Since $\times$ is distributive on $.$, $\lambda^{\times}_{\gamma^i}$ is a group endomorphism of $(\mathsf{GF}(p^m)^*, ., 1))$. Let γ^j such that $\gamma^{ij} = 1$. This is equivalent to $ij = 0$. But $\gamma^i \in U(\mathsf{GF}(p^m)^*)$ so $i \in U(\mathbb{Z}_{p^m-1})$ and then $ij = 0$ if and only if $j = 0$. So $\gamma^j = \gamma^0 = 1$ and $\lambda^{\times}_{\gamma^i}$ is one-to-one also is onto. It is thus an element of $Aut((\mathsf{GF}(p^m)^*, ., 1))$. □

[4] For instance $3 = 2^2 - 1$, $5 = 2^3 - 1$, $31 = 2^5 - 1$ and $127 = 2^7 - 1$ are Mersenne prime numbers.

[5] R is not reduced to 0.

Lemma 9. *Let G be a subgroup of $(U(\mathsf{GF}(p^m)^*), \times, \gamma)$. Then G acts faithfully (by group automorphism) on $(\mathsf{GF}(p^m)^*, ., 1)$ by $\rho(\gamma^i) : \gamma^j \mapsto \gamma^i \times \gamma^j$.*

Proof. We define

$$\begin{array}{l} \rho : G \to Aut((\mathsf{GF}(p^m)^*, ., 1)) \\ \quad \gamma^i \mapsto \lambda^{\times}_{\gamma^i} : (\gamma^j \mapsto \gamma^i \times \gamma^j) \ . \end{array} \tag{11}$$

(By lemma 8 we already know that for each $\gamma^i \in G$, we have $\rho(\gamma^i) = \lambda^{\times}_{\gamma^i} \in Aut((\mathsf{GF}(p^m)^*, ., 1))$.) Let's prove that is a group action on $\mathsf{GF}(p^m)^*$. Let γ^i and γ^j be elements of G. Let $\gamma^k \in \mathsf{GF}(p^m)^*$. $\rho(\gamma^i \times \gamma^j)(\gamma^k) = \rho(\gamma^{ij})(\gamma^k) = \gamma^{ij} \times \gamma^k = \gamma^{ijk} = \gamma^i \times (\gamma^j \times \gamma^k) = (\rho(\gamma^i) \circ \rho(\gamma^j))(\gamma^k)$. Then ρ is a group homomorphism from G to $Aut(\mathsf{GF}(p^m)^*, ., 1))$. Finally let $\gamma^i \in G$ such that $\rho(\gamma^i) = Id_{\mathsf{GF}(p^m)^*}$. For any $k \in \mathbb{Z}_{p^m-1}$, $\gamma^{ik} = \gamma^k$. So $ik = k$ and in particular $i1 = 1$, therefore $i = 1$ and $\gamma^i = \gamma^1 = \gamma$. We deduce that ρ is one-to-one and the action is thus faithful. □

Definition 10. Let G be a group and X be any (nonempty) set. The restriction to G^* of a map $f : G \to X$ is denoted f^*.

Theorem 11. *Let $m \in \mathbb{N}^*$ such that $m > 1$. Let G be a subgroup of $U(\mathbb{Z}_{2^m-1})$ such that for each $i \in G^*$, $i - 1 \in U(\mathbb{Z}_{2^m-1})$ (such a group exists according to lemma 7 since $2^m - 1 > 1$ by assumption and is an odd number). Let λ be a field automorphism from $\mathsf{GF}(2^m)$ to itself. Then we have*

1. *λ is $(\mathsf{GF}(2^m)^*, ., 1)$-perfect nonlinear from $\mathsf{GF}(2^m)$ to $\mathsf{GF}(2^m)$;*
2. *λ^* is $(\gamma^G, \times, \gamma)$-perfect nonlinear from $\mathsf{GF}(2^m)^*$ to $\mathsf{GF}(2^m)^*$ where $\gamma^G = e_\gamma(G)$.*

Proof. 1. This result is clear by applying theorem 4 with $\mathsf{GF}(2^m)$ considered as a one-dimensional vectors space over itself;

2. Since $\gamma^G = e_\gamma(G)$, γ^G is a subgroup of the group of units of $\mathsf{GF}(2^m)^*$. By lemma 9, γ^G acts faithfully on $\mathsf{GF}(2^m)^*$ by group automorphism. Because λ is a field homomorphism, $\lambda(\mathsf{GF}(2^m)^*) \subseteq \mathsf{GF}(2^m)^*$ and therefore $\lambda^* : \mathsf{GF}(2^m)^* \to \mathsf{GF}(2^m)^*$ is a group homomorphism. Moreover λ^* is onto. Indeed for $y \in \mathsf{GF}(2^m)^*$ there is $x \in \mathsf{GF}(2^m)$ such that $\lambda(x) = y$. Since $y \neq 0$, $x \neq 0$ and therefore $\lambda^*(x) = y$. So λ^* is a group epimorphism (and then a group automorphism). Let $\beta \in \mathsf{GF}(2^m)^* = \lambda(\mathsf{GF}(2^m)^*)$. Let $\gamma^i \in (\gamma^G)^*$ (so $i \neq 1$). Let's prove that $\{\gamma^j \in \mathsf{GF}(2^m)^* | d_{\gamma^i}\lambda^*(\gamma^j) = \beta\} = \gamma^{\frac{1}{j}} \times \lambda^{-1}(\{\beta\})$. We have

$$\begin{array}{ll} & d_{\gamma^i}\lambda^*(\gamma^j) = \beta \\ \Leftrightarrow & \dfrac{\lambda^*(\gamma^i \times \gamma^j)}{\lambda^*(\gamma^j)} = \beta \\ \Leftrightarrow & \lambda(\dfrac{(\gamma^i \times \gamma^j)}{\gamma^j}) = \beta \text{ (because } \lambda \text{ is a field homomorphism)} \\ \Leftrightarrow & \lambda((\gamma^i \times \gamma^j)(\gamma^{-j})) = \beta \\ \Leftrightarrow & \lambda((\gamma^i \times \gamma^j)(\gamma^{-1} \times \gamma^j)) = \beta \\ \Leftrightarrow & \lambda((\gamma^i\gamma^{-1}) \times \gamma^j) = \beta \text{ (by distributivity)} \\ \Leftrightarrow & \lambda(\gamma^{i-1} \times \gamma^j) = \beta \\ \Leftrightarrow & \gamma^{i-1} \times \gamma^j \in \lambda^{-1}(\{\beta\}) \ . \end{array} \tag{12}$$

Since $\gamma^i \in (\gamma^G)^* \Leftrightarrow i \in G^*$ and by assumption on G, $i-1$ is invertible modulo 2^m-1. Then $\gamma^{i-1} \in U(\mathsf{GF}(2^m)^*)$. According to lemma 8, $\lambda^{\times}_{\gamma^{i-1}} \in Aut((\mathsf{GF}(2^m)^*,.,1))$. Therefore $\gamma^{i-1} \times \gamma^j \in \lambda^{-1}(\{\beta\}) \Leftrightarrow \gamma^j \in (\lambda^{\times}_{\gamma^{i-1}})^{-1}\left(\lambda^{-1}(\{\beta\})\right) = \gamma^{\frac{1}{i-1}} \times \lambda^{-1}(\{\beta\})$. Since $\lambda^{\times}_{\gamma^{\frac{1}{i-1}}}$ is a permutation we have $|\lambda^{-1}(\{\beta\})| = |\gamma^{\frac{1}{i-1}} \times \lambda^{-1}(\{\beta\})|$. Because $\beta \in \mathsf{GF}(p^m)^*$, we have $\lambda^{-1}(\{\beta\}) = (\lambda^*)^{-1}(\{\beta\})$ and by lemma 2, we deduce that $|\gamma^{\frac{1}{i-1}} \times \lambda^{-1}(\{\beta\})| = |(\lambda^*)^{-1}(\{\beta\})| = |\ker \lambda^*|$ with $\ker \lambda^* = \{x \in \mathsf{GF}(2^m)^* | \lambda^*(x) = 1\} = \{x \in \mathsf{GF}(2^m)^* | \lambda(x) = 1\}$. In addition $\{\lambda^{-1}(\{\beta\})\}_{\beta \in \mathsf{GF}(p^m)^*}$ is a partition of $\mathsf{GF}(2^m)^*$. Therefore we have

$$|\mathsf{GF}(2^m)^*| = \sum_{\beta \in \mathsf{GF}(2^m)^*} |\lambda^{-1}(\beta)| = |\ker \lambda^*||\mathsf{GF}(2^m)^*| \ . \tag{13}$$

Then for each $\gamma^i \in (\gamma^G)^*$ (or equivalently for each $i \in G^*$) and for each $\beta \in \mathsf{GF}(2^m)^*$, $|\{\gamma^j \in \mathsf{GF}(2^m)^* | d_{\gamma^i}\lambda^*(\gamma^j) = \beta\}| = |\ker \lambda^*| = 1$.

□

Definition 12. Let $p = 2^q - 1$ be a Mersenne prime number. A function $f : \mathsf{GF}(2^q) \to \mathsf{GF}(2^q)$ such that $f(\alpha) \neq 0$ for all invertible $\alpha \in \mathsf{GF}(2^q)$ is called *doubly perfect nonlinear* if

1. f is $(\mathsf{GF}(2^q)^*, ., 1)$-perfect nonlinear from $\mathsf{GF}(2^q)$ to itself;
2. f^* is $(\mathsf{GF}(2^q)^{**}, \times, \gamma)$-perfect nonlinear from $\mathsf{GF}(2^q)^*$ to itself.

Since the group of field automorphisms of a finite field $\mathsf{GF}(p^m)$ is identical to the Galois group of the degree m extension $\mathsf{GF}(p^m)$ over its prime field which is a cyclic group generated by the Frobenius automorphism

$$\begin{array}{rccc} \mathcal{F}_p : & \mathsf{GF}(p^m) & \to & \mathsf{GF}(p^m) \\ & x & \mapsto & x^p \end{array} \tag{14}$$

every field automorphism λ can be written as $\mathcal{F}_p^r$ for one r such that $0 \leq r \leq m-1$. We now give a nice result that asserts the existence of a Boolean permutation over $\mathsf{GF}(2^q)$, where $p = 2^q - 1$ is a Mersenne prime, which is merely both $(\mathsf{GF}(2^q)^*, ., 1)$ and $(\mathsf{GF}(2^q)^{**}, \times, \gamma)$-perfect nonlinear *i.e.* doubly perfect nonlinear.

Theorem 13. *Let $p = 2^q - 1$ be a Mersenne prime number. Let $\lambda = \mathcal{F}_2^r$ (for any $0 \leq r \leq q-1$) be a field automorphism of $\mathsf{GF}(2^q)$. Then λ is a doubly perfect nonlinear permutation.*

Proof. Because $p = 2^q - 1$ is a prime number, $\mathsf{GF}(2^q)^*$ is isomorphic to the field $\mathsf{GF}(p) = \mathbb{Z}_p$. Therefore we can choose $G = \mathbb{Z}_p^*$ as a group such that for each $i \in G^*$, $i-1$ is invertible modulo p. Then $\gamma^G = U(\mathsf{GF}(2^q)^*) = \mathsf{GF}(2^q)^{**} = \mathsf{GF}(2^q) \setminus \{0, 1\}$. According to theorem 11, λ is $(\mathsf{GF}(2^q)^*, ., 1)$-perfect nonlinear and λ^* is $(\mathsf{GF}(2^q)^{**}, \times, \gamma)$-perfect nonlinear. □

References

[1] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3-72, 1991.

[2] C. Carlet and C. Ding. Highly nonlinear mappings. *Journal of Complexity*, 20(2):205-244, 2004.

[3] FIPS 46-3, Data encryption standard, Federal Information Processing Standards Publication 46-3 (1999), U.S. Department of Commerce/N.I.S.T.

[4] FIPS 197, Advanced encryption standard, Federal Information Processing Standards Publication 197 (2001), U.S. Department of Commerce/N.I.S.T.

[5] M. Matsui. Linear cryptanalysis for DES cipher. In *Advances in Cryptology - Eurocrypt'93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 386-397, 1994.

[6] K. Nyberg and L. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - Crypto'92*, vol. 740 of *Lecture Notes in Computer Science*, pp. 566-574, 1993.

[7] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - Eurocrypt'92*, vol. 547 of *Lecture Notes in Computer Science*, pp. 378-386, 1992.

[8] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - Eurocrypt'93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 55-64, 1994.

[9] L. Poinsot and S. Harari. Generalized Boolean bent functions. In *Progress in Cryptology - Indocrypt 2004*, vol. 3348 of *Lecture Notes in Computer Science*, pp. 107-119, 2004.

[10] L. Poinsot and S. Harari. Group actions based perfect nonlinearity. *GESTS International Transactions on Computer Science and Engineering*, 12(1):1-14, 2005.

[11] L. Poinsot. Non linéarité parfaite généralisée au sens des actions de groupe, contribution aux fondements de la solidité cryptographique. PhD thesis, University of South Toulon-Var, 2005.

[12] L. Poinsot. Boolean bent functions in impossible cases: odd and plane dimensions. *International Journal of Computer Science and Network Security*, 6(8):18-26, 2006.

[13] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656-715, 1949.

This article was processed using the LaTeX macro package with LLNCS style