Permutations with small differential uniformity

Pascale Charpin*

* French National Institute for Research
in Computer Science (INRIA, France).

Antalya Algebra Days XII - Antalya, May 2010

Content

1. - A cryptographic context

Differential cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers.

Numerous works which investigate the security offered by different types of functions with respect to differential attacks.

2. - The power functions.

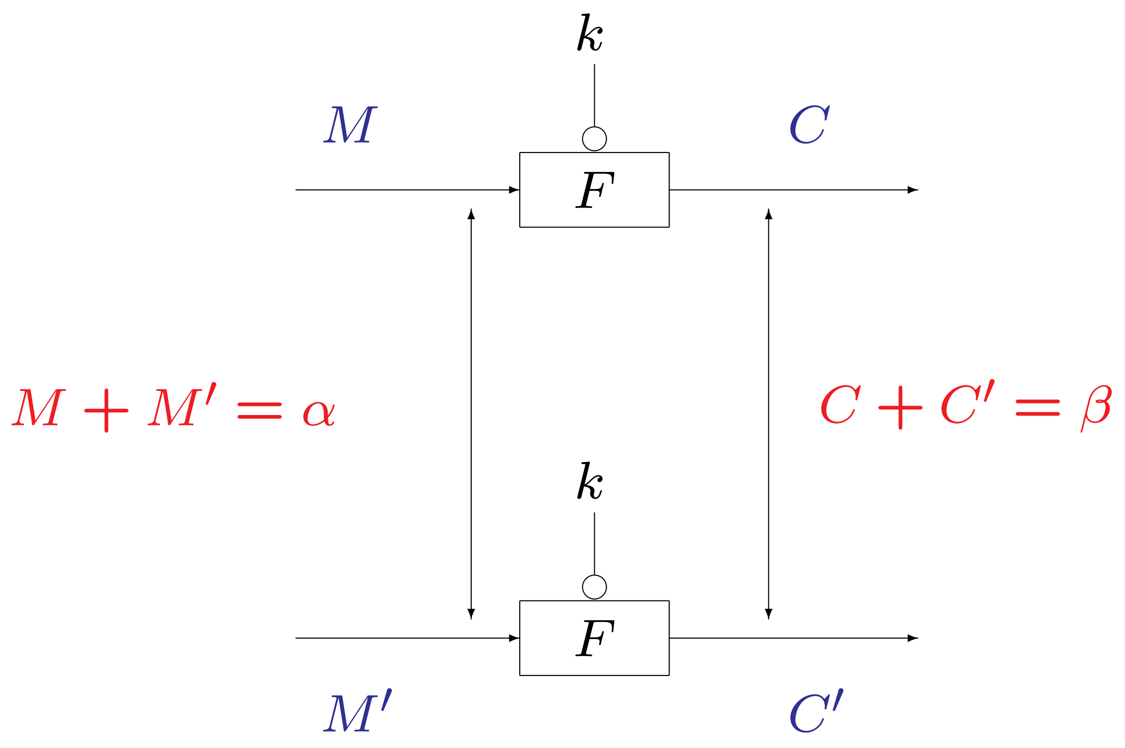
Their properties are related with cyclic codes with two zeroes.

3. - Other sparse functions

Permutations of the shape $G(x) + \lambda\ Tr(H(x))$

Joint works with C. Blondeau, A. Canteaut, G. Kyureghan and
E. Pasalic

Differential cryptanalysis [Biham-Shamir, 1991]



A block cipher - plaintexts M, M' *and ciphertexts* C, C' *-.*

A statistical study of the differences : differential cryptanalysis exploits the existence of $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ such that

$$\boldsymbol{F}(\boldsymbol{M} + \boldsymbol{\alpha}) + \boldsymbol{F}(\boldsymbol{M}) = \boldsymbol{\beta} \text{ for many values of } \boldsymbol{M}.$$

Elements for the design of functions F over $\mathbb{F}_{2^n}$

The image set.

$x \mapsto F(x)$ is a permutation of $\mathbb{F}_{2^n}$.

Differential uniformity.

$$\# \{ x \mid F(x) + F(x + \alpha) = \beta \}$$

must be small for any β (for any fixed α).

Sparse functions.

F has a low implementation complexity
with properties relatively easy to describe.

Starting from applications, appear some directions of research such as the structure of the image set, the behaviour of derivatives, to find sparse functions with interesting properties

The monomial functions

Functions $F : x \mapsto x^d$ over $\mathbb{F}_{2^n}$, $d \in [1, 2^n - 2]$.

$$d = \sum_{i=0}^{n-1} d_i 2^i, d_i \in \{0,1\}, \; wt(d) = \sum_i d_i$$

- The algebraic degree of $\mathbb{F}_{2^n}$ equals $wt(d)$.
- $\mathbb{F}_{2^n}$ is a permutation if and only if $\gcd(d, 2^n - 1) = 1$.
- To compute the derivatives

$$(x+\alpha)^d + x^d = \alpha^d \left(\left(\frac{x}{\alpha} + 1 \right)^d + \left(\frac{x}{\alpha} \right)^d \right).$$

is to compute the derivative in point 1.

To study differential properties is easier ; all elements of the differential spectrum are interesting

The differential spectrum of $F : x \mapsto x^d$

(Joint work with Celine Blondeau and Anne Canteaut, 2010)

$$\delta(b) = \#\{x \in \mathbb{F}_{2^n},\ (x+1)^d + x^d = b\},\ \textit{any } d.$$

The differential uniformity of F is

$$\delta(F) = \max_{b \in \mathbb{F}_{2^n}} \delta(b).$$

The differential spectrum of $F(x) = x^d$ is

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\} \text{ with } \omega_i = \#\{b \in \mathbb{F}_{2^n} | \delta(b) = i\}.$$

It appears that very often

$$\delta(F) = \delta(b) \text{ where } b \in \mathbb{F}_2.$$

To compute $\delta(b)$, $b \in \mathbb{F}_2$, is to study the irreducible factors in $\mathbb{F}_2[x]$ of the polynomial

$$(x+1)^d + x^d + b.$$

The inverse function

Let

$$\boldsymbol{F} \;:\; \boldsymbol{x} \mapsto \boldsymbol{x}^{-1} \quad \text{over} \quad \mathbb{F}_{2^n}.$$

- $\boldsymbol{n}$ odd : $\boldsymbol{\delta(F) = 2}$ and $\boldsymbol{\omega_0 = 2^{n-1}, \omega_2 = 2^{n-1}}$.
- $\boldsymbol{n}$ even : $\boldsymbol{\delta(F) = \delta(0) = 4}$ and $\boldsymbol{\omega_0 = 2^{n-1} + 1}$, $\boldsymbol{\omega_2 = 2^{n-1} - 2}$, $\boldsymbol{\omega_4 = 1}$.

Definition. A new design. Let $F(x) = x^s$ over $\mathbb{F}_{2^n}$.

Then $\boldsymbol{F}$ is said to be quasi-APN if and only if

$$\boldsymbol{\delta(F) \in \{\delta(0), \delta(1)\}} \text{ and } \boldsymbol{\delta(b) \leq 2} \text{ for all } \boldsymbol{b \notin \mathbb{F}_2}.$$

Infinite classes of such functions exist ; for instance for $n = 2t$ $x \mapsto x^d$ with $d = 2^t - 1$. [Blondeau-Canteaut-Charpin, 2010].

To compute $\delta(0)$ and $\delta(1)$

α is a primitive root of $\mathbb{F}_{2^n}$, $\delta(b) = \#R_b$ with

$$R_b = \{\ x \mid (x+1)^d + x^d + b = 0\ \}, \quad b \in \mathbb{F}_2$$

Lemma. $\delta(0) = s - 1$ where $s = \gcd(d, 2^n - 1)$.

Lemma. Consider the trinomials over $\mathbb{F}_2$

$$P(x) = x^{2^k} + x + 1,\ \ k \geq 1.$$

Then any irreducible factors of $P(x)$ has degree $2s$ with

$s = \gcd(2s, k)$ and $2s$ divides $2k$

$\Rightarrow x^{2^s} + x + 1$ divides $P(x)$ for all such s.

Theorem. $\boldsymbol{b \in \mathbb{F}_2}$. Assume that, for $\boldsymbol{i > 0}$,

$$\boldsymbol{\alpha^i \in R_b} \quad \Longrightarrow \quad \boldsymbol{P(\alpha^i) \neq 0}, \text{ for any } \boldsymbol{k \geq 1}.$$

Then, $\boldsymbol{R_b \setminus \mathbb{F}_2}$ is a set of $\boldsymbol{\alpha^i}$ where $\boldsymbol{i}$ describes an even number of cyclotomic cosets modulo $(2^n - 1)$.

The hypothesis of the Theorem is satisfied in the following cases.

(i) When n is odd, for $R_1 \setminus \mathbb{F}_2$ and R_0.

(ii) When $n = 2m$ and m is prime: if 3 divides d then for $R_1 \setminus \mathbb{F}_2$ otherwise for R_o.

Example: n prime $\Rightarrow \delta(1) = 2$ or $\delta(1) \geq 2 + 2n$.

Corollary. Any $\boldsymbol{F(x) = x^d}$ such that $\boldsymbol{\delta(F) \leq 6}$.

(i) Assume that $\boldsymbol{n}$ is odd. Then $\boldsymbol{F}$ is a permutation when

- $\boldsymbol{\delta(F)} \leq 4$
- $\boldsymbol{\delta(F) = 6}$ with $\gcd(3, n) = 1$.

(ii) Let $\boldsymbol{n = 2m}$ with m odd, and $\boldsymbol{\gcd(3, d) = 1}$. Then

- if $\boldsymbol{\delta(F) = 4}$ then $\boldsymbol{F}$ is a permutation;
- if $\boldsymbol{\delta(F) = 6}$ and $\boldsymbol{\gcd(3, n) = 1}$ then $\boldsymbol{F}$ is a permutation.

(iii) When $\boldsymbol{\gcd(3, n) = 3}$ and $\boldsymbol{\delta(F) = 6}$ either $\boldsymbol{7}$ divides $\boldsymbol{d}$ or $\boldsymbol{F}$ is a permutation.

Other properties are derived which, together with numerical results, lead to this question : Does it exist a large class of such permutations F ?

Monomial permutations with $\delta = 4$

n	$number$	$known$	n	$number$	$known$
6	4	yes	7	2	no
8	1	yes	9	2	no
10	13	$6 \times no$	11	8	no
12	3	yes	13	2	no
14	13	yes	15	0	$--$
16	1	yes	17	0	$--$
18	13	yes	19	0	$--$
20	3	yes	21	0	$--$

Known means inverse, quadratic and Kasami exponents. Also [Bracken-Leander, 2009] for $n = 4k$, k odd.

Conjecture. There is no monomial function which is differentially 4-uniform for n odd, $n \geq 15$. For even n, to find a new class of such function is an open problem.

Other sparse functions

To find bijective* sparse functions with a low differential uniformity: The main idea which is currently developed consists in adding any function to an APN function.

For instance: [Pasalic et al., Wang et al., 2009].

$$\boldsymbol{F(x) + L(x)}, F \text{ is APN and } L \text{ is linear.}$$

[Leander-Rodier, 2009]. Study the corpus of functions

$$\boldsymbol{x^{-1} + G(x)} \quad \text{where} \quad G \text{ is any non-affine function.}$$

They proved that these functions are APN on at most a finite number of fields. They cannot be APN if the degree of G is less than 7.

* Open problem: To find an APN permutation on $\mathbb{F}_{\boldsymbol{2^n}}$ for $\boldsymbol{n}$ even. Only one example is known for $\boldsymbol{n = 6}$; such function has a dense polynomial expression [Dillon, Fq9, 2009].

Let, the trace-function on $\mathbb{F}_{2^n}$

$$Tr(x) = x + x^2 + \ldots + x^{2^{n-1}}$$

and consider the polynomials of the shape

$$F(X) = G(X) + \gamma\, Tr(\, H(X)\,),$$

where $G(X),\ H(X) \in \mathbb{F}_{2^n}[X]$ and $\gamma \in \mathbb{F}_{2^n}$.

The function defined by $F(X)$:

$$F(x) = \begin{cases} G(x) & \text{if } Tr(H(x)) = 0 \\ G(x) + \gamma & \text{if } Tr(H(x)) = 1 \end{cases}$$

Problem -1 : Characterize or find such permutation polynomials. [Charpin-Kyureghan, 2008-09] studied the general problem, *i.e.*, over finite fields of any characteristic.

Boolean mappings with a linear structure

Let $c \in \mathbb{F}_2$. An element $\gamma \in \mathbb{F}_{2^n}{}^*$ is said to be a c-linear structure of a Boolean mapping $Tr(R(x))$ if

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

The linear structures of any Boolean function form (by adding 0) a linear subspace of $\mathbb{F}_{2^n}$.

Or equivalently, using the Walsh transforms, it must hold

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(R(x)+\lambda x)} = 0$$

for all $\lambda \in \mathbb{F}_{2^n}$ with $Tr(\gamma\lambda) = c + 1$.

[Yashchenko 1997, Dubuc 2001]

Functions $F(x) = G(x) + \gamma\, Tr(\, H(x)$

Theorem. $G(x)$ is a permutation $\Rightarrow$

$$F(x) = G(x) + \gamma\, Tr(\, H(x)\,)$$

is a permutation over $\mathbb{F}_{2^n}$, if and only if $H(x) = R(G(x))$, and

$$\gamma \quad \text{is a 0-linear structure of } \; Tr(\, R(x)\,).$$

If γ is a 1-linear structure of $Tr(\, R(x)\,)$ then F is $2 - to - 1$.

Proof. $F(x)$ is a permutation **iff** for any $\lambda \in \mathbb{F}_{2^n}{}^*$ it holds

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x))} = 0 \;\; \text{if} \;\; Tr(\gamma\lambda) = 0 \qquad (1)$$

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda G(x) + H(x))} = 0 \;\; \text{if} \;\; Tr(\gamma\lambda) = 1. \qquad (2)$$

(2) means that $Tr(\, R(x) + R(x+\gamma)\,) = u$ for all x with $u = 0$.

If $u = 1$ then $F(x) = y$ for $x \in G^{-1}(y + \gamma u),\; u \in \mathbb{F}_2$. $\diamond$

F is a permutation $\Rightarrow$

for any $a \in \mathbb{F}_{2^n}$ the equation $G(x) = a$ for at most two x.

Theorem. Let $G(x)$ be a linear $2 - to - 1$ function with kernel $\{0, \alpha\}$ and $H : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$. Then

$$G(x) + \gamma Tr(H(x)), \;\; \gamma \in \mathbb{F}_{2^n}$$

is a permutation of $\mathbb{F}_{2^n}$ if and only if

- γ does not belong to the image set of G
- α is a 1-linear structure for $Tr(H(x))$.

Related problems. To find other suitable functions G to construct permutation of this shape. Recall that an APN function is such that all its derivatives are $2 - to - 1$ functions .

Theorem. Let $\gamma \in \mathbb{F}_{2^n}{}^*$, $\boldsymbol{s, t}$ any integer and

$$\boldsymbol{F}(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{s}} + \gamma\, \boldsymbol{Tr}(\, \boldsymbol{x}^{\boldsymbol{t}}\,).$$

Then $\boldsymbol{F}$ is a permutation over $\mathbb{F}_{2^n}$ if and only if

$$\gcd(\boldsymbol{s}, \mathbf{2}^{\boldsymbol{n}} - \mathbf{1}) = \mathbf{1} \quad \text{and} \quad \boldsymbol{t} \equiv \mathbf{2}^{\boldsymbol{j}}(\mathbf{2}^{\boldsymbol{i}} + \mathbf{1})\boldsymbol{s} \pmod{\mathbf{2}^{\boldsymbol{n}} - \mathbf{1}}$$

for some $0 \le i, j \le n-1$, $i \ne n/2$, and either (a) or (b) holds:

(a) $\boldsymbol{i} = \mathbf{0}$ and $\boldsymbol{Tr}(\gamma) = \mathbf{0}$.

(b) $\boldsymbol{i} > \mathbf{0}$ and $\gamma \in \mathbb{F}_{\mathbf{2}^{\boldsymbol{k}}}$ with $\boldsymbol{Tr}(\gamma^{\mathbf{2}^{\boldsymbol{i}}+\mathbf{1}}) = \mathbf{0}$, where $\boldsymbol{k} = \gcd(\mathbf{2}\boldsymbol{i}, \boldsymbol{n})$.

Moreover, if $\boldsymbol{Tr}(\gamma) = \mathbf{1}$ (case (a)), or $\boldsymbol{Tr}(\gamma^{\mathbf{2}^{\boldsymbol{i}}+\mathbf{1}}) = \mathbf{1}$ (case (b)), then $\boldsymbol{F}$ is a $\mathbf{2} - \boldsymbol{to} - \mathbf{1}$ mapping.

The proof uses the complete characterization of the monomial Boolean functions $\boldsymbol{Tr}(\boldsymbol{\lambda x}^{\boldsymbol{t}})$ having a linear structure. The functions $\boldsymbol{x} \mapsto \boldsymbol{Tr}(\boldsymbol{\lambda x}^{\boldsymbol{t}})$ which are neither linear not quadratic have no linear structure [Charpin-Kyureghan, 2009].

Differential uniformity of $F(x) = x^s + \gamma\, Tr(\, x^t\,)$

$$\boldsymbol{\delta(F) = \max_{a,b \in \mathbb{F}_{2^n},\ a \neq 0} \#\{x \in \mathbb{F}_{2^n},\ F(x) + F(x+a) = b\}.}$$

Lemma. Assume that $\boldsymbol{\delta(G) = \rho}$. Then for any $\gamma \neq 0$.

$\boldsymbol{F(x) = G(x) + \gamma Tr(H(x))}$ satisfies $\boldsymbol{\delta(F) \leq 2\rho}$.

Theorem. Assume $\boldsymbol{\gcd(s, 2^n - 1) = 1}$ and $\boldsymbol{\delta(x^s) = \rho}$.

Further, let $1 \leq i < n/2$ and $\boldsymbol{k = \gcd(2i, n)}$. Then:

for any $\gamma \in \mathbb{F}_{2^k}$ such that $\boldsymbol{Tr(\gamma^{2^i+1}) = 0}$

$$\boldsymbol{F(x) = x^s + \gamma\, Tr\left(x^{s(2^i+1)}\right)}$$

is a permutation on $\mathbb{F}_{2^n}$ satisfying $\boldsymbol{\delta(F) \leq 2\rho}$.

Problem - 2 : To study the corpus of these permutations.
Can we have $\boldsymbol{\delta(F) < 2\rho}$ for ρ small ?

Permutations $F(x) = x^s + \gamma\, Tr(\, x^t\,)$

There is no permutation of the shape $x^s + \gamma\, Tr(x^t)$ *with* n *even and* $x \mapsto x^s$ *is APN.*

There is no permutation of the shape $x^s + \gamma\, Tr(x^{s(2^i+1)})$ *with* n *odd and* $\gcd(i,n) = 1$*.*

In particular, the function over $\mathbb{F}_{2^n}$

$$x \mapsto x^3 + \gamma Tr(x^9)^*$$

is not a permutation, for any n and for any γ.

*For $\gamma = 1$, this function is APN for any n [Bracken et al., Budaghyan et al., 2007-2009].

A class of sparse permutations with a low differential uniformity

Proposition. Let

$$\gamma \in \mathbb{F}_{2^n},\ \gamma \neq 0,\ 0 \leq i < n,\ i \neq n/2,\ k = \text{gcd}(2i, n).$$

$$F(x) = x^{-1} + \gamma\ Tr(x^{2^{n-1}-2^{i-1}-1})$$

Then $F(x)$ is a permutation if either **(i)** or **(ii)** holds:

(i) $i = 0$ and $Tr(\gamma) = 0$ (a trivial case).

(ii) $0 < i$ and $\gamma \in \mathbb{F}_{2^k}$ with $Tr(\gamma^{2^i+1}) = 0$.

Moreover: $\delta(F) \leq 4$ for odd n

$\delta(F) \leq 8$ for even n.

A number of Open problems

- More on the non-existence of monomials F such that $\delta(F) = 4$ for n odd.

- The differential spectra of monomials.
  Recent results on $x \mapsto x^{2^t-1}$ [BCC, 2010].

- The number of codewords of weight 3 of cyclic codes with two zeroes.

- Permutations $G(x) + \gamma Tr(H(x))$, where G is $2 - to - 1$ and of degree > 1.

- Differential uniformity of $G(x) + \gamma Tr(H(x))$.

- Find APN permutations over $\mathbb{F}_{2^n}$ when n is even.