On the APNness and differential uniformity of some classes of (n, n)-functions over $\mathbb{F}_2^n$

Claude Carlet

(1) University of Bergen, Norway

(2) LAGA, Universities of Paris 8 and Paris 13, CNRS, France

Outline

- Differentially uniform and APN (n, n)-functions
- Symmetric functions and their generalizations
- Monotone functions and their generalizations

Differentially uniform and APN (n, n)-functions

The differential uniformity of a vectorial function:

$$F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m,$$

(called *an* (n, m)*-function*), equals:

$$\delta_F = \max_{\substack{a \in \mathbb{F}_2^n, a \neq 0 \\ b \in \mathbb{F}_2^m}} |\{x \in \mathbb{F}_2^n;\ D_a F(x) := F(x) + F(x + a) = b\}|.$$

($D_a F(x)$ is called a derivative of F).

Such function F is called *differentially* δ_F*-uniform*.

This parameter plays a central role in cryptography, since it quantifies the resistance to the differential attack of those cryptosystems using F as a substitution box (S-box).

The choice of the S-box in the AES (the NIST standard for civil cryptography) is based on the work of Kaisa Nyberg on such notion in the early 90's.

Vectorial functions, when they are used as S-boxes in block ciphers, should have low differential uniformity.

In this talk, we shall focus on $m = n$, which is the situation in the so-called *Substitution-Permutation Network* model of block ciphers.

For $m = n$, the best (i.e. smallest) possible value of δ_F equals 2.

The function is then called *almost perfect nonlinear* (APN).

APNness: $\sum_{x \in A} F(x) \neq 0$ for every affine plane (2-dimensional affine space) A of $\mathbb{F}_2^n$, that is, $F(A)$ is not an affine plane.

The algebraic degree of a vectorial (n, n)-function equals the degree of its algebraic normal form (ANF):

$$F(x) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i; \quad a_I \in \mathbb{F}_2^n.$$

Vectorial functions are better non-quadratic (i.e. with an algebraic degree larger than 2), because of the higher order differential attack.

Very few infinite classes of APN functions are known, all the more if we avoid quadratic functions.

In the model of substitution-permutation networks, the S-boxes must be bijective.

No APN permutation is known in even dimension n larger than 6, while for implementation reasons, n is preferred to be even (and is still better a power of 2).

Equivalences and invariance:

Two vectorial functions F and G are called *EA equivalent* if there exist two affine permutations L, L' over $\mathbb{F}_2^n$ and an affine function $L'' : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ such that $G = L \circ F \circ L' + L''$.

Differential uniformity is EA invariant.

No infinite class of non-quadratic APN functions that are new up to EA equivalence has been found since 2005.

Two vectorial functions F and G are called *CCZ equivalent* if there exists an affine permutations $L : (\mathbb{F}_2^n)^2 \mapsto (\mathbb{F}_2^n)^2$ which maps the graph $\{(x, y) \in (\mathbb{F}_2^n)^2; y = F(x)\}$ of F to the graph of G.

EA equivalence is a particular case of CCZ equivalence.

Differential uniformity is CCZ invariant.

The last class of non-quadratic APN functions found that is new up to CCZ equivalence dates back to 2000.

The vector space $\mathbb{F}_2^n$ can be endowed with the field structure of $\mathbb{F}_{2^n}$ through the choice of a basis of this n-dimensional vector space over $\mathbb{F}_2$.

All the known infinite classes of non-quadratic APN functions are CCZ equivalent to power functions $F(x) = x^d$, $x \in \mathbb{F}_{2^n}$, and live then in a very narrow family of functions.

Table 1: Known APN exponents up to equivalence (any n) and up to inversion (n odd).

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$
Inverse	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

New approaches for studying APN functions seem then necessary.

When an APN function is found, it can be considered new only if it is EA inequivalent to all known APN functions. If it is also CCZ inequivalent, it is still better.

All the known studies of APN (and differentially uniform) S-boxes for block ciphers consider functions over the finite field $\mathbb{F}_{2^n}$. No known infinite class of APN functions, or differentially uniform functions of a low order, is given by the algebraic normal form (ANF).

A way to avoid falling in already known functions (up to equivalence) when searching for APN functions is to work on $\mathbb{F}_2^n$ without using the structure of $\mathbb{F}_{2^n}$.

We need to find features of (n, n)-functions, that are specific to the representation in $\mathbb{F}_2^n$, and would ease the study of APNness.

- When the properties are too restrictive, we can try to find a proof of non-existence.

- Then the properties need to be gradually weakened, enlarging significantly the corresponding corpus and also making that the proof of non-existence of APN functions does not work in this wider context.

- Once such functions are found, infinite classes should be searched for.

Symmetric functions and their generalizations

Definition. We call *symmetric* any (n, n)-function $F(x) = (f_1(x), \ldots, f_n(x))$ such that, for every $x \in \mathbb{F}_2^n$ and every permutation σ of $\{1, \ldots, n\}$:

$$F(\sigma(x)) = \sigma(F(x)),$$

that is:

$$f_i(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f_{\sigma(i)}(x_1, \ldots, x_n), \forall i = 1, \ldots, n.$$

Note that the coordinate functions of symmetric (n, n)-functions are in general not symmetric Boolean functions.

In fact, we have $F(x) = x\,f(x) + 1_n\,g(x)$ where f and g are symmetric Boolean functions.

Proposition. No symmetric (n, n)-function can be APN for $n \geq 4$.

Sketch of proof: F being symmetric, we have:

$$\begin{aligned} F(x) + F(x+a) = b &\Leftrightarrow \sigma(F(x) + F(x+a)) = \sigma(b) \\ &\Leftrightarrow \sigma(F(x)) + \sigma(F(x+a)) = \sigma(b) \\ &\Leftrightarrow F(\sigma(x)) + F(\sigma(x) + \sigma(a)) = \sigma(b). \end{aligned}$$

Then, for F APN, if $\sigma(a) = a$ and $\sigma(b) = b$, and if $F(x)+F(x+a) = b$, the pair $\{x, x+a\}$ is globally invariant under σ.

If $w_H(x+a) \neq w_H(x)$ then $\sigma(x) = x$ and $\sigma(x+a) = x+a$.

The rest of the proof is more technical.

Definition. We call *rotation symmetric* (in brief, RS) any (n,n)-function F such that, for every $x \in \mathbb{F}_2^n$, and every cyclic shift over $\{1,\ldots,n\}$, e.g. $s(x_1,\ldots,x_n) = (x_n, x_1, \ldots, x_{n-1})$:

$$F(s(x)) = s(F(x)),$$

that is:

$$F = (f, f \circ s^{n-1}, f \circ s^{n-2} \ldots, f \circ s^2, f \circ s).$$

Note that the coordinate functions of RS (n,n)-functions are in general not RS Boolean functions.

Every power function transformed into a function over $\mathbb{F}_2^n$ through the choice of a normal basis $(\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}})$ is RS.

Open problem: find RS APN functions which are not equivalent to power functions.

Monotone functions and their generalizations

We write $x \preceq y$ if $supp(x) \subseteq supp(y)$.

Definition. An (n, n)-function F is monotone if

$$x \preceq y \Longrightarrow F(x) \preceq F(y).$$

Equivalently, each coordinate function f of F is a monotone Boolean function, that is, satisfies $x \preceq y \Longrightarrow f(x) \leq f(y)$.

Monotone functions have bad nonlinearity [C.C. Cryptography and Communications, 2018].

The number $M(n)$ of monotone n-variable Boolean functions is called the *Dedekind number* and is unknown for $n \geq 9$.

Asymptotically, we have $\log_2(M(n)) \sim \binom{n}{\lfloor n/2 \rfloor}$.

The number $(M(n))^n \sim (2^{2^n})\sqrt{\frac{2n}{\pi}}$ of monotone (n,n)-functions is then huge.

The number of functions EA equivalent to monotone functions is still larger.

Lemma. For every positive integers n and δ such that $2 \leq \delta \leq n$ and every monotone differentially δ-uniform (n, n)-function F, we have:

$$\forall a \in \mathbb{F}_2^n,\ w_H(F(a)) \leq w_H(a) + \log_2(\delta).$$

Applying this to the monotone differentially δ-uniform function $x \mapsto 1_n + F(x + 1_n)$, we obtain:

$$\forall a \in \mathbb{F}_2^n,\ w_H(F(a)) \geq w_H(a) - \log_2(\delta).$$

Proposition. For every positive integers n and δ such that $2 \leq \delta \leq n$ and every monotone differentially δ-uniform (n, n)-function, we have:

$$\delta \left(1 + n + \binom{n}{2} + \cdots + \binom{n}{\lfloor 1 + 2\log_2(\delta) \rfloor} \right) \geq 2^n.$$

In particular, no monotone APN (n, n)-function exists for $n \geq 8$.

We propose to call *weakly monotone* the functions F such that $x \preceq y$ implies $w_H(F(x)) \leq w_H(F(y))$, that is, such that the pseudo-Boolean function $w_H \circ F$ is monotone.

Our proof of non-existence of APN functions is then no more valid.

Open problem: find weakly monotone APN functions.