Boolean plateaued functions, vectorial functions with plateaued components, and their APNness

Claude Carlet

LAGA, Universities of Paris 8 and Paris 13, CNRS, France

Outline

- Plateaued Boolean functions in cryptography
- Characterizations of plateaued Boolean functions and of componentwise plateaued vectorial functions

- Characterization by means of derivatives
- Characterization by means of autocorrelation functions
- Characterization by means of Walsh power moments

- Characterizations of the APNness of componentwise plateaued vectorial functions

- The case of unbalanced component functions

- Open problems and further work

Plateaued Boolean functions in cryptography

Studying *cryptographic criteria* for Boolean functions

$$f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$$

and vectorial functions ((n, m)-functions)

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

and finding *constructions* are *simpler within some classes of functions*.

Considering *quadratic functions* (Boolean or vectorial) considerably simplifies the calculation of the *Hamming weight* and of the *Walsh transform* and eases the study of several cryptographic criteria.

A function f (Boolean or vectorial) is quadratic if the function $\varphi_f(x, y) = f(0) + f(x) + f(y) + f(x + y)$ is bilinear.

But the low algebraic degree of quadratic functions hardly allows resisting the *Berlekamp-Massey and Rønjom-Helleseth attacks* in the case of Boolean function, and the *higher-order differential attack* in the case of vectorial functions.

Also, the number of equivalence classes of quadratic functions up to EA-equivalence (i.e. under composition by an affine permutation of $\mathbb{F}_2^n$ and addition of an affine Boolean function) equals $\lfloor n/2 \rfloor$ only.

Super-classes of functions having the same advantages as quadratic functions and including many more equivalent classes have then been studied (since 1992).

In the case of **Boolean functions**, these classes have been successively those of :

1. *partially-bent functions* (C.C., CRYPTO'92), which are by definition affinely equivalent to functions of the form :

$$f(x+y) = g(x) + h(y),\ x \in \mathbb{F}_2^r,\ y \in \mathbb{F}_2^{n-r},\ r \text{ even},$$

where g is bent, i.e. has maximal *nonlinearity* (Hamming distance to affine functions), i.e. whose Walsh transform

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x},$$

(where $\cdot$ is an inner product) has constant magnitude $2^{n/2}$, and h is affine. Such function has algebraic degree at most $r/2 \leq n/2$,

2. *plateaued functions* (Zheng, Zhang, ICICS'99), whose Walsh transform takes values 0 and $\pm\mu$ only, where $\mu = 2^k$ for some k such that $n/2 \leq k \leq n$ is called the *amplitude* of f. The algebraic degree is bounded above by $\lceil n/2 \rceil$.

The definition of plateaued functions does not depend on the choice of the inner product.

The class of partially-bent functions includes by definition all bent functions.

Every partially-bent function is plateaued but there exist plateaued functions which are not partially-bent (Zheng-Zhang, ICICS'99).

The class of plateaued functions also includes all semi-bent functions, but not only bent and semi-bent functions.

The cryptographic criteria are easily studied within these two classes, but *the classes themselves are difficult to study* !

For **vectorial** (n, m)**-functions** :

There is no equivalent of partially-bent functions for $m > n/2$ since we know that no bent (n, m)-function exists when $m > n/2$ (Nyberg, EUROCRYPT'91).

The most general equivalent of plateaued Boolean functions for vectorial functions $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is *componentwise plateaued* functions, whose component functions $u \cdot F$, $u \neq 0$, are plateaued.

These functions are important for block ciphers since all *Almost Bent* (AB) (n, n)-functions (achieving maximal nonlinearity $nl(F)$, for n odd) are componentwise plateaued, as well as some APN functions, n even, like the *Kasami functions* (at least for $6 \not| n$).

Notation : $W_F(a,u) = W_{u\cdot F}(a)$.
Recall that AB implies APN ; that

$$nl(F) = \min\{nl(u \cdot F)\,,\, u \in \mathbb{F}_2^n,\, u \neq 0\};$$

that for $m = n$,

$$nl(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}};$$

and that F is APN if

$$|\{x \in \mathbb{F}_2^n\,;\; F(x) + F(x+a) = b\}| \leq 2,\; \forall a, b \in \mathbb{F}_2^n,\; a \neq 0.$$

Moreover, we know that if an (n,n) APN function is componentwise plateaued in odd dimension n, then it is AB.

Little is known on plateaued Boolean functions, except (very partly) for bent and semi-bent functions. Still less is known on componentwise plateaued vectorial functions.

On plateaued Boolean functions are known :

- some direct consequences of the definition,
- a characterization by the second order derivatives (C.C.-Prouff, FSE 2003),
- characterizations by constant ratio of consecutive Walsh power moments of even orders (Mesnager, SETA 2014, to appear).

On componentwise plateaued vectorial functions, no general characterization is known.

Characterizations of plateaued Boolean functions and of componentwise plateaued vectorial functions

I. Characterization by means of derivatives

$D_a f(x) = f(x) + f(x+a)$,

$D_a D_b f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b)$

C.C.-Prouff, FSE 2003 :

Any Boolean function f is plateaued on $\mathbb{F}_2^n$ if and only if the expression $\sum_{a,b\in\mathbb{F}_2^n}(-1)^{D_aD_bf(x)}$ does not depend on $x \in \mathbb{F}_2^n$.
This constant expression equals then the square of the amplitude.

Theorem 1. *Let F be an (n, m)-function. Then are equivalent :*

1. *F is componentwise plateaued,*
2. *for every $v \in \mathbb{F}_2^n$, the size of the set*

$$\{(a, b) \in (\mathbb{F}_2^n)^2 \,;\, D_a D_b F(x) = v\}$$

does not depend on $x \in \mathbb{F}_2^n$.

In other words, the value distribution of $D_a D_b F(x)$ when (a, b) ranges over $(\mathbb{F}_2^n)^2$ is independent of $x \in \mathbb{F}_2^n$.

Moreover, the value distribution of $D_a D_b F(x)$ equals the value distribution of $D_a F(b) + D_a F(x)$ when $(a, b) \in (\mathbb{F}_2^n)^2$.

Examples

1. *Let F be AB* (n odd), it is known that :
– $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = 0\}| = 3 \cdot 2^n - 2$ (i.e. F is APN),
– $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = v \neq 0\}| = 2^n - 2$.

2. *Let n be even and $F(x) = x^{2^i+1}$ be a Gold APN function*, $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = v\}|$ equals :

$$\begin{cases} 3 \cdot 2^n - 2 & \text{for } v = 0, \\ 2^n \pm 2^{\frac{n}{2}+1} - 2 & \text{for } v \text{ a nonzero cube } (\frac{2^n-1}{3} \text{ cases}) \\ 2^n \pm 2^{\frac{n}{2}} - 2 & \text{for } v \text{ a non-cube } (2 \cdot \frac{2^n-1}{3} \text{ cases}). \end{cases}$$

Moreover, among the two "$\pm$" above, one is "$+$" and one is "$-$".

Remark 1. Let F be CCZ-equivalent to a Gold APN function $G(x) = x^{2^i+1}$ (i.e. if its graph corresponds to that of the Gold function by an affine permutation) or to a Kasami APN function $G(x) = x^{4^i-2^i+1}$.

The graph G_F of F satisfies $G_F = \mathcal{L}(G_G)$ and we can consider w.l.o.g. $\mathcal{L}$ linear. Then :

$W_F(a,u) = W_G(\mathcal{L}^*(a,u))$, where $\mathcal{L}^*$ is the adjoint operator of $\mathcal{L}$.

If n is odd, F is AB and then plateaued.

If n is even (and $3 \not| n$ if G is Kasami), then, for every a :

- if u is a nonzero cube, then $W_G(a,u) \in \{0, \pm 2^{\frac{n}{2}+1}\}$,
- if u is not a cube then $W_G(a,u) = \pm 2^{\frac{n}{2}}$.

It is then easily seen that F is componentwise plateaued if and only if it is EA-equivalent to G.

Note that this gives a new proof that the Gold and Kasami APN functions are CCZ-inequivalent.

Remark 2. F is componentwise plateaued if and only if : $\forall x \in \mathbb{F}_2^n$, $\exists \phi_x : (a,b) \mapsto (a',b')$ bijective such that $D_a D_b F(x) = D_{a'} D_{b'} F(0)$.

Corollary 1. *Let F be a componentwise plateaued function. Let :*

$$\phi_x : (a,b) \mapsto (a',b') \text{ be such that } D_a D_b F(x) = D_{a'} D_{b'} F(0).$$

Let Q be a quadratic function such that, for every (a,b) :

$$D_a D_b Q = D_{a'} D_{b'} Q.$$

Then $F + Q$ has plateaued components.

This set of quadratic functions Q is a vector space.
For every componentwise plateaued function F, the set of $F + Q$ is then an *affine space* of componentwise plateaued functions.

Corollary 2. *Let $F(x) = x^d$ be any power function. Then :*

$$\forall v \in \mathbb{F}_{2^n}, \forall x \in \mathbb{F}_{2^n}, \forall \lambda \in \mathbb{F}_{2^n}^*,$$
$$|\{(a,b) \in \mathbb{F}_{2^n}^2 \,;\, D_aF(b) + D_aF(x) = v\}| =$$
$$|\{(a,b) \in \mathbb{F}_{2^n}^2 \,;\, D_aF(b) + D_aF(x/\lambda) = v/\lambda^d\}|.$$

In particular, $|\{(a,b) \in \mathbb{F}_{2^n}^2 \,;\, D_aF(b) + D_aF(0) = v\}|$ is invariant when v is multiplied by any d-th power in $\mathbb{F}_{2^n}^*$.
Then F is componentwise plateaued if and only if, for every $v \in \mathbb{F}_{2^n}$:

$$|\{(a,b) \in \mathbb{F}_{2^n}^2 \,;\, D_aF(b) + D_aF(1) = v\}| =$$

$$|\{(a,b) \in \mathbb{F}_{2^n}^2 \,;\, D_aF(b) + D_aF(0) = v\}|.$$

A necessary condition is then that

$$|\{(a,b) \in \mathbb{F}_{2^n}^2 \,;\, D_a F(b) + D_a F(1) = v\}|$$

is invariant when v is multiplied by any d-th power in $\mathbb{F}_{2^n}^*$.

This condition is necessary and sufficient in the case of APN power permutations.

The case of unbalanced components :

When $u \cdot F$ is unbalanced and plateaued, its amplitude equals $|W_F(0,u)|$.

F is then componentwise plateaued if and only if :

$$\forall u, x, \sum_{a,b \in \mathbb{F}_2^n} (-1)^{u \cdot D_a D_b F(x)} = W_F^2(0, u).$$

By applying the Fourier transform, we obtain :

Theorem 2. *Let F be any (n, m)-function whose component functions are all unbalanced. Then F is componentwise plateaued if and only if, for every $v, x \in \mathbb{F}_2^n$:*

$$\left|\left\{(a, b) \in (\mathbb{F}_2^n)^2 ; D_a D_b F(x) = v\right\}\right| =$$

$$\left|\left\{(a, b) \in (\mathbb{F}_2^n)^2 ; F(a) + F(b) = v\right\}\right|.$$

II. **Characterization by means of autocorrelation functions**

$\Delta_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)}$

Proposition 1. *A Boolean function f is plateaued of amplitude μ if and only if $\sum_{a \in \mathbb{F}_2^n} \Delta_f^2(a) = \mu^2 \Delta_f(0) = \mu^2 2^n$.*
It is plateaued (whatever is its amplitude) if and only if, for every $x \in \mathbb{F}_2^n$, we have

$$2^n \sum_{a \in \mathbb{F}_2^n} \Delta_f(a)\Delta_f(a+x) = [\sum_{a \in \mathbb{F}_2^n} \Delta_f^2(a)]\Delta_f(x).$$

An (n,m)-function F is componentwise plateaued if and only if, for every $x \in \mathbb{F}_2^n$ and every $u \in \mathbb{F}_2^m$, we have

$$2^n \sum_{a \in \mathbb{F}_2^n} \Delta_{u \cdot F}(a) \Delta_{u \cdot F}(a+x) = [\sum_{a \in \mathbb{F}_2^n} \Delta_{u \cdot F}^2(a)] \Delta_{u \cdot F}(x).$$

III. **Characterization by means of Walsh power moments**

Theorem 3. *An n-variable Boolean function f is plateaued if and only if, for every nonzero $\alpha \in \mathbb{F}_2^n$, we have*

$$\sum_{w \in \mathbb{F}_2^n} W_f^3(w) W_f(w+\alpha) = 0.$$

An (n,m)-function F is componentwise plateaued if and only if :

$$\forall u \in \mathbb{F}_2^m, \forall \alpha \in \mathbb{F}_2^n, \alpha \neq 0, \sum_{w \in \mathbb{F}_2^n} W_F^3(w,u) W_F(w+\alpha, u) = 0.$$

Proposition 2. *An n-variable Boolean function f is plateaued if and only if, for every $b \in \mathbb{F}_2^n$:*

$$\sum_{a \in \mathbb{F}_2^n} W_f^4(a) = 2^n (-1)^{f(b)} \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot b} W_f^3(a).$$

An (n,m)-function F is componentwise plateaued if and only if, for every $b \in \mathbb{F}_2^n$ and every $u \in \mathbb{F}_2^m$:

$$\sum_{a \in \mathbb{F}_2^n} W_F^4(a,u) = 2^n (-1)^{u \cdot F(b)} \sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot b} W_F^3(a,u).$$

Theorem 4. *For every n-variable Boolean function f we have :*

$$\left(\sum_{a \in \mathbb{F}_2^n} W_f^4(a) \right)^2 \leq 2^{2n} \left(\sum_{a \in \mathbb{F}_2^n} W_f^6(a) \right),$$

with equality if and only f is plateaued.

For every (n,m)-function F, we have :

$$\sum_{u\in\mathbb{F}_2^m}\left(\sum_{a\in\mathbb{F}_2^n} W_F^4(a,u)\right)^2 \leq 2^{2n}\sum_{u\in\mathbb{F}_2^m}\left(\sum_{a\in\mathbb{F}_2^n} W_F^6(a,u)\right),$$

with equality if and only if F is componentwise plateaued.
For every n-variable Boolean function we have also :

$$\sum_{u\in\mathbb{F}_2^m}\sum_{a\in\mathbb{F}_2^n} W_F^4(a,u) \leq 2^n\sum_{u\in\mathbb{F}_2^m}\sqrt{\sum_{a\in\mathbb{F}_2^n} W_F^6(a,u)}$$

with equality if and only if F is componentwise plateaued.

Characterizations of the APNness of componentwise plateaued vectorial functions

Characterization by the derivatives :

We first extend a well-known result on quadratic functions :

Theorem 5. *Any componentwise plateaued (n,n)-function F is APN if and only if, for every $a \neq 0$ in $\mathbb{F}_2^n$, the equation*

$$F(x) + F(x+a) = F(0) + F(a)$$

has the 2 solutions 0 and a only.

Characterization by the Walsh transform :

Known : $\sum_{a\in\mathbb{F}_2^n, u\in\mathbb{F}_2^n, u\neq 0} W_F^4(a,u) = 2^{3n+1}(2^n-1)$.

Proposition 3. *Let F be any componentwise plateaued (n,n)-function such that $F(0)=0$. Then F is APN if and only if the set $\{(a,b)\in\mathbb{F}_{2^n}^2 \,|\, F(a)+F(b)+F(a+b)=0\}$ has size $3\cdot 2^n-2$. Equivalently :*

$$\sum_{a\in\mathbb{F}_{2^n}, u\in\mathbb{F}_2^n, u\neq 0} W_F^3(a,u) = 2^{2n+1}(2^n-1).$$

This necessary and sufficient condition was known until now only for quadratic functions (and it is necessary for general functions).

Proposition 4. *Let F be a componentwise plateaued (n,n)-function. Let, for every u, 2^{λ_u} be the amplitude of $u \cdot F$. Then F is APN if and only if :*

$$\sum_{u \in \mathbb{F}_2^n, u \neq 0} 2^{2\lambda_u} \leq 2^{n+1}(2^n - 1).$$

There is then equality and the set

$$\{(x,y) \in (\mathbb{F}_2^n)^2 \,|\, F(x) = F(y); x \neq y\}$$

has size at most $2 \cdot (2^n - 1)$.

The case of unbalanced component functions

Theorem 6. *Let F be any componentwise plateaued (n, n)-function having all its component functions unbalanced, then*

$$\left|\{(a, b) \in (\mathbb{F}_2^n)^2, a \neq b\,;\, F(a) = F(b)\}\right| \geq 2 \cdot (2^n - 1),$$

with equality if and only if F is APN.

Corollary 3. *Let n be even and $F(x) = x^d$ be any componentwise plateaued power function. Then F is APN if and only if $gcd(d, 2^n - 1) = 3$.*

This applies to the Kasami functions for n even not divisible by 3.

From Theorem 2, we also obtain :

Corollary 4. *For every componentwise plateaued (n, n)-function, with n even, whose value distribution is the same as for the APN Gold functions, the value distribution of $D_a D_b F(x)$ is the same as for the Gold functions. Consequently, the function is APN and the extended Walsh spectrum is the same as well.*

Dobbertin proved that if F is a power APN function then it is 3-to-1 over $\mathbb{F}_{2^n}^*$. Hence, this corollary applies to every power APN function F.

Open problems and further work

Open problems :

1. Find constructions of numerous plateaued Boolean functions which are neither bent nor semi-bent.

2. Find general constructions of componentwise plateaued (n, n)-functions.

3. Find a proof using the charaterizations above, that the Kasami APN (n, n)-functions are componentwise plateaued for n even not divisible by 3.

4. Determine whether the Kasami APN (n, n)-functions are componentwise plateaued for n even divisible by 3.

5. Find new APN componentwise plateaued functions by using the characterizations above.

6. Determine whether CCZ-equivalence of componentwise plateaued functions reduces to EA-equivalence.

Further work : generalize these results to p-ary functions.