On APN permutations

Marco Calderini

University of Trento

Boolean Functions and their Applications
July 3-8, 2017

Cryptographic motivations

Some cryptographic primitives, as block ciphers, have components called S-boxes. Often an S-box is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.

Many block ciphers are a series of "rounds". Each round consists of an S-box, a P-box and the XOR with a round key.

$$x \to \underbrace{S(x) \to P(S(x)) \to P(S(x)) \oplus k}_{oneround} \to \ldots$$

The S-box has to satisfy certain criteria, including in particular

- High nonlinearity provides resistance of the S-box to linear cryptanalysis.
- Low differential uniformity provides resistance of the S-box to differential cryptanalysis.
- Being invertible (it is easier to design the encryption/decryption function).

Cryptographic motivations

Some cryptographic primitives, as block ciphers, have components called S-boxes. Often an S-box is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$.

Many block ciphers are a series of "rounds". Each round consists of an S-box, a P-box and the XOR with a round key.

$$x \to \underbrace{S(x) \to P(S(x)) \to P(S(x)) \oplus k}_{oneround} \to \ldots$$

The S-box has to satisfy certain criteria, including in particular

- High nonlinearity provides resistance of the S-box to linear cryptanalysis.
- Low differential uniformity provides resistance of the S-box to differential cryptanalysis.
- Being invertible (it is easier to design the encryption/decryption function).

Notations

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Vectorial Boolean function.

$F_\lambda(x) := Tr_1^n(\lambda F(x))$, $\lambda \in \mathbb{F}_{2^n}$, are the components of F (Tr_m^n is the trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$).

$\widehat{F}(\alpha, \beta) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha x + \beta F(x))}$, $\alpha, \beta \in \mathbb{F}_{2^n}$, are the Walsh coefficients.

$D_a F(x) = F(x + a) - F(x)$ is the derivative of F in the direction a.

Definitions

Definition

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then F is said δ-differentially uniform iff the equation

$$F(x+a) - F(x) = b$$

has at most δ solutions for all $a \in \mathbb{F}_{2^n}^*$ and for all $b \in \mathbb{F}_{2^n}$

F is called Almost Perfect Nonlinear (APN) iff $\delta = 2$.
APN functions have the smallest possible differential uniformity.
Indeed, if x is a solution to $F(x+a) - F(x) = b$, so it is $x + a$.

Equivalently

Proposition

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN iff $|\{D_a F(x) \mid x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$ for all $a \in \mathbb{F}_{2^n}^*$.

To verify if F is APN it is sufficient to check if $|\{D_a F(x) \mid x \in \mathbb{F}_{2^n}\}| = 2^{n-1}$ for all $a \neq 0$ in any hyperplane $\mathcal{H}$.

APN functions and their components

Proposition (Nyberg (1994), Berger, Canteaut, Charpin, Laigle-Chapuy (2006))

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then, for any non-zero $a \in \mathbb{F}_{2^n}$

$$\sum_{\beta \in \mathbb{F}_{2^n}} \widehat{D_a F}^2(0, \beta) \geq 2^{2n+1}.$$

Moreover F is APN iff $\sum_{\beta \in \mathbb{F}_{2^n}} \widehat{D_a F}^2(0, \beta) = 2^{2n+1}$.

F is a permutation iff $\sum_{\beta \in \mathbb{F}_{2^n}^*} \widehat{D_a F}(0, \beta) = -2^n$ for all non-zero $a \in \mathbb{F}_{2^n}$.

APN permutations are completely characterized by the derivatives of their components.

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is partially-bent if there exist two subspace U and V s.t. $U \oplus V = \mathbb{F}_{2^n}$ and $f_{|_U}$ is bent and $f_{|_V}$ is affine. V is the set of the linear structures of f.

Theorem (Nyberg 1994)

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, with all partially-bent components. If F is APN then:

- *If n is odd, then any component has one nonzero linear structure. Different components have different nonzero linear structure.*
- *If n is even, then at least $\frac{2}{3}(2^n - 1)$ components are bent. In particular, F cannot be a permutation.*

Theorem (Hou 2006)

Let F be a permutation over $\mathbb{F}_{2^n}$, with n even. If F has more than $2^{n-2}-1$ quadratic components, then it is not APN.

Theorem (C.,Sala,Villa 2016)

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, with n even. If F is an APN permutation then F has no partially-bent (quadratic) components.

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is plateaued if

$$\widehat{f}(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\alpha x)+f(x)} \in \{0, \pm\lambda\}.$$

Note: f partially-bent $\Rightarrow$ plateaued.

Theorem (Berger, Canteaut, Charpin, Laigle-Chapuy 2006)

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, with n even. If F has all plateaued components and F is APN, then at least $\frac{2}{3}(2^n - 1)$ are bent. In particular F cannot be a permutation.

Remark

An APN permutation in even dimension can have plateaued components.

Examples

x^3 is APN over $\mathbb{F}_{2^n}$, for all n.

- n odd 1-to-1
- n even 3-to-1

x^{2^n-2} is a permutation over $\mathbb{F}_{2^n}$ for all n.

- n odd APN
- n even 4-differentially uniform

APN monomials and permutations

Family	Monomial	Conditions	Proved by
Gold	x^{2^k+1}	$gcd(k,n)=1$	Gold
Kasami	$x^{2^{2k}-2^k+1}$	$gcd(k,n)=1$	Kasami
Welch	x^{2^k+3}	$n=2k+1$	Dobbertin
Niho	$x^{2^k+2^{\frac{t}{2}}-1}$, k even $x^{2^k+2^{\frac{3t+1}{2}}-1}$, k odd	$n=2k+1$	Dobbertin
Inverse	x^{2^n+2}	n odd	Nyberg
Dobbertin	$x^{2^{4k}+2^{3k}+2^{2k}+2^k+1}$	$n=5k$	Dobbertin

Theorem (Dobbertin 1998)

APN power functions are permutations of $\mathbb{F}_{2^n}^*$ if n is odd, and are three-to-one if n is even.

Non existence results

Theorem (Hou 2006)

Let $F \in \mathbb{F}_{2^n}[x]$ be a permutation polynomial, with $n = 2m$. Then:

- *If $n = 4$ then F is not APN (computational fact).*
- *if $F \in \mathbb{F}_{2^m}[x]$ then F is not APN.*

In his paper, Hou conjectured that APN permutations did not exist in even dimension.
This was a long-standing open problem until, in 2009, Dillon presented an APN permutation in dimension 6.

APN functions and codes

Theorem (Carlet, Charpin, Zinoviev 1998)

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, *with* $F(0) = 0$. *Let* u *be a primitive element of* $\mathbb{F}_{2^n}$. *Then* F *is APN if and only if the binary linear code* C_F *defined by the parity check matrix*

$$H_F = \begin{bmatrix} u & u^2 & \dots & u^{2^n-1} \\ F(u) & F(u^2) & \dots & F(u^{2^n-1}) \end{bmatrix}$$

has minimum distance 5.

APN functions and codes

Let $\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{F}_{2^n}\}$.

Two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are **CCZ-equivalent** if and only if Γ_F and Γ_G are affine-equivalent, i.e. let $\mathcal{L}$ an affine map on $(\mathbb{F}_{2^n})^2$, $\mathcal{L}\Gamma_F = \Gamma_G$

or equivalently

if the extended codes with parity check matrices

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & u & \dots & u^{2^n-1} \\ F(0) & F(u) & \dots & F(u^{2^n-1}) \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & \dots & 1 \\ 0 & u & \dots & u^{2^n-1} \\ G(0) & G(u) & \dots & G(u^{2^n-1}) \end{bmatrix}$$

are equivalent.

APN permutations and codes

Theorem (Browning, Dillon, Kibler, McQuistan 2007)

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN, with $F(0) = 0$. F is CCZ equivalent to an APN permutation iff $C_F^\perp$ is a double simplex code (i.e. $C_F^\perp = C_1 \oplus C_2$ with C_i a $[2^n - 1, n, 2^{n-1}]$-code).

If F is APN and $C_F^\perp = C_1 \oplus C_2 = \langle f_1(x) \rangle \oplus \langle f_2(x) \rangle$ is a double simplex code

$$\left.\begin{array}{l} C_1\{ \\ C_2\{ \end{array}\left[\begin{array}{ccc} \dots & f_1(x) & \dots \\ \dots & f_2(x) & \dots \end{array}\right]\right\} C_F^\perp$$

where $f_i(x) = L_i(x, F(x))$ (L_i linear map from $\mathbb{F}_2^{2n}$ to $\mathbb{F}_2^n$)

f_i's are permutations of $\mathbb{F}_{2^n}$, thus F is CCZ-equivalent to $f_2 \circ f_1^{-1}$ which is an APN permutation.

So to find an APN permutation we want to write $C_F^\perp = C_1 \oplus C_2$

The first APN permutation in even dimension

At the Fq9 conference (Dublin 2009), Dillon presented the construction of an APN permutation on $\mathbb{F}_{2^6}$.

Consider the function

$$F(x) = ux^3 + ux^{10} + u^2x^{24} \text{ , } u \text{ is a primitive element of } \mathbb{F}_{2^6}$$

(F is equivalent to the Kim function $\kappa(x) = x^3 + x^{10} + ux^{24}$)
Denote $L = \mathbb{F}_{2^6}$ and $K = \mathbb{F}_{2^3}$

A codeword of $C_F^\perp$ is

$$(\,Tr(\alpha x + \beta F(x))_{x\in L^*},\ \alpha, \beta \in L$$

Note that $L = K \oplus uK$

Then we can write $C_F^\perp = C_1 \oplus C_2$ with

$$C_1 = \{ Tr(\alpha x + \beta F(x))_{x \in L^*} \mid (\alpha, \beta) \in K \times K \}$$

and

$$C_2 = \{ Tr(\alpha x + \beta F(x))_{x \in L^*} \mid (\alpha, \beta) \in uK \times uK \}.$$

For the Kim function, we have that $Tr(\alpha x + \beta F(x))$ is balanced for all $\alpha, \beta \in K$ $\beta \neq 0$ and the same holds for $\alpha, \beta \in uK$.

Thus C_1 and C_2 are simplex codes.

Theorem (Browning, Dillon, McQuistan, Wolfe 2009)

$\kappa(x)$ is CCZ-equivalent to an APN permutation.
The code $C_\kappa^\perp$ contains 222 simplex subcodes, 32 of which split into two sets of 16, with any pair from different sets being "disjoint". The 256 corresponding inverse pairs of APN permutations are, of course, all CCZ-equivalent to κ.

APN permutations and Walsh spectrum

The set of Walsh zeroes of F is

$$WZ_F = \{(\alpha,\beta) : \widehat{F}(\alpha,\beta) = 0\} \cup \{(0,0)\}$$

APN permutations and Walsh spectrum

An APN function F on $\mathbb{F}_{2^n}$ is CCZ-equivalent to a permutation iff the Walsh zeroes of F contains two subspaces of dimension n intersecting only trivially.

Indeed, there exists a linear permutation, mapping $\mathbb{F}_{2^n} \times \{0\}$ and $\{0\} \times \mathbb{F}_{2^n}$ to these two spaces, respectively. This leads to $\mathcal{L}$ such that the resulting CCZ-equivalent function is a permutation.

Properties of κ

- Walsh zeroes of κ has more structure with respect to some subspaces, i.e.,

$$\{(u_1x, v_1y) : x, y \in \mathbb{F}_{2^3}\}, \{(u_2x, v_2y) : x, y \in \mathbb{F}_{2^3}\} \subseteq WZ_F$$

  for some $u_1, u_2, v_1, v_2 \in \{x \in \mathbb{F}_{2^6} : Tr_3^6(x) = 1\} \cup \{1\}$.
- The function κ satisfies the subspace property, which is defined as

$$F(ax) = a^{2^k+1}F(x), \forall a \in \mathbb{F}_{2^{\frac{n}{2}}} \tag{1}$$

  for some integer k.
- According to Browning-Dillon-McQuistan-Wolfe this explained some of the simplicity of why κ is equivalent to a permutation,

$$\widehat{F}(\alpha, \beta) = \widehat{F}(\alpha y, \beta y^{2^k+1}), \quad y \in \mathbb{F}_{2^{\frac{n}{2}}}$$

APN functions of κ-form

Let $n = 2m$.

Remark

$F = \sum_d a_d x^d$ satisfies the subspace property iff

$$d \equiv 2^k + 1 \mod 2^m - 1.$$

In particular, F quadratic satisfies the subspace property if d in $\{2^k + 1, 2^k + 2^m, 2^{k+m} + 2^m, 2^{k+m} + 1\}$.

Functions with κ-form:

$$F(x) = x^{2^k+1} + Ax^{2^{k+m}+2^m} + Bx^{2^{k+m}+1} + Cx^{2^k+2^m}$$

A family with κ-form

Theorem (Göloğlu 2015)

Let $n = 2m$. $F_k(x) = x^{2^{k+m}+2^m} + x^{2^k+2^m} + x^{2^{k+m}+1}$. Then, F_k is APN iff m is even and $gcd(k, n) = 1$.

However, Göloğlu did not find any F_k which is equivalent to a permutation for $n = 8$ and $n = 12$

Theorem (Göloğlu, Langevin 2015)

Gold functions are not equivalent to any permutation on even extensions.

Theorem (Budaghyan, Helleseth, Li, Sun 2016)

Let $n = 2m = 4t$. F_k is affine equivalent to the Gold function $x^{2^{m-k}+1}$.

$$\Downarrow$$

F_k is not equivalent to a permutation.

APN functions of κ-form

Recently Dáša Krasnayová, in her Master's thesis "Constructions of APN permutations", studied necessary and sufficient conditions for

$$F(x) = x^3 + Ax^{3\cdot 2^m} + Bx^{2^{m+1}+1} + Cx^{2+2^m}$$

with $A, B, C \in \mathbb{F}_{2^m}$ to be APN or equivalent to a permutation $(n = 2m)$.

Theorem (Krasnayová 2016)

Let $n = 2m$, $\Delta = 1 + A + B + C$. *Then* F *is APN iff* A, B, C *satisfy*

<table>
<tr><th>m odd</th><th>m even</th></tr>
<tr><td colspan="2">$\Delta \neq 0$</td></tr>
<tr><td>$Tr_1^m\left(\frac{1+A}{\Delta}\right) = 1$</td><td>$Tr_1^m\left(\frac{1+A}{\Delta}\right) = 0$</td></tr>
<tr><td>$1 + B + A^2 + AC \neq 0$</td><td>$-$</td></tr>
<tr><td>$Tr_1^m\left(\frac{\Delta^2}{1+B+A^2+AC}\right) = 1$</td><td>$-$</td></tr>
<tr><td colspan="2">if $Tr_1^m(\frac{B+AC}{\Delta^2}) = 1$ then $A^2B^2 + C^2 \neq \Delta^2(AC + b)$</td></tr>
<tr><td colspan="2">$Tr_1^m\left(\frac{\Delta(T\Delta+B+C)(T^2\Delta^2+AC+B)}{(T\Delta^2+AB+C)^2}\right) = 1$,
for every T s.t. $Tr_1^m(T) = 1$, $\Delta T + 1 + A \neq 0$,
$(T\Delta^2 + AB + C) \neq 0$ and $T^2\Delta^2 + AC + B \neq 0$</td></tr>
</table>

To check if $F(x) = x^3 + Ax^{3\cdot 2^m} + Bx^{2^{m+1}+1} + Cx^{2+2^m}$ is equivalent to a permutation, Krasnayová determined necessary and sufficient conditions to have $u, v \in \mathcal{T}_1 = \{x \mid Tr_m^n(x) = 1\}$ such that

$$\sum_{\alpha \in u\mathbb{F}_{2^m}} \sum_{\beta \in v\mathbb{F}_{2^m}} \widehat{F}^2(\alpha, \beta) = 2^{4m}.$$

This is equivalent to

$$\{(u\alpha, v\beta) \mid \alpha, \beta \in \mathbb{F}_{2^m}\} \subset WZ_F$$

Krasnayová applied her results for $n = 6$ and $n = 10$ (when m odd it is more easy to check the conditions to be equivalent to a permutation)

- $n = 6$: 112 APN functions, 84 of which equivalent to a permutation.
  (All these functions are CCZ-equivalent to κ)
- $n = 10$: 496 APN functions,
  no one is equivalent to a permutation.

Some computational facts

- Let $n = 8$, if $F(x) = x^{2^k+1} + Ax^{2^{k+m}+2^m} + Bx^{2^{k+m}+1} + Cx^{2^k+2^m}$ is APN then it is equivalent to a Gold function, for all $gcd(k, n) = 1$ and $A, B, C \in \mathbb{F}_{2^8}$.
- Let $n = 10, 12, 14$. If $F(x) = x^{2^k+1} + Ax^{2^{k+m}+2^m} + Bx^{2^{k+m}+1} + Cx^{2^k+2^m}$ is APN then it is equivalent to a Gold function, for all $gcd(k, n) = 1$ and $A, B, C \in \mathbb{F}_{2^m}$

Remark

When m is even we have two classes of function in κ-form: x^{2^k+1} and $x^{2^k+1} + x^{2^{k+m}+1} + x^{2^k+2^m}$ ($\sim x^{2^{m-k}+1}$).
When m is odd we have one class of function in κ-form: x^{2^k+1}.

Theorem (Göloğlu, Krasnayová, Lisoněk 2017)

Let $n = 2m$. *Let* $F(x) = x^3 + Ax^{3\cdot 2^m} + Bx^{2\cdot 2^m+1} + Cx^{2+2^m}$, *with* $A, B, C \in \mathbb{F}_{2^m}$. *If F is APN then one of the following cases occurs:*

- $AC + B + B^2 + C^2 = 0$ *and* F *is equivalent to* x^3.
- $AC + B + A^2 + 1 = 0$, m *even and* F *is equivalent to* $x^{2^{m-1}+1}$.
- $m = 3$ *and* F *is equivalent to* κ.

An approach with hyperelliptic curves[1]

Consider the Kim function $F(x) = ux^3 + ux^{10} + u^2x^{24}$, we have

$$Tr(\alpha x + \beta F(x)) \text{ is balanced}$$

$$\Updownarrow$$

$$C_{\alpha,\beta} : y^2 + y = \alpha x + \beta F(x) \text{ is s.t. } \#C_{\alpha,\beta} = 2^6 + 1$$

$$\Updownarrow$$

$$C'_{\alpha,\beta} : y^2 + y = (\beta u)^{32}x^5 + (\beta u + (\beta u^2)^8)x^3 + \alpha^2 x^2 \text{ is s.t. } \#C'_{\alpha,\beta} = 2^6 + 1$$

[1] Petr Lisoněk, "APN permutations and double simplex codes", Mathematics of Communications: Sequences, Codes and Designs 2015.

The number of points on curves $C : y^2 + y = \sum_i c_i x^{2^i+1}$ can be analyzed using the method given in
G. van der Geer, M. van der Vlugt: Reed-Muller codes and supersingular curves. I. Compositio Math. 84 (1992), no. 3, 333-367.

Let

$$C : y^2 + y = \sum_i c_i x^{2^i+1}$$

Denote $Q(x) = Tr(\sum_i c_i x^{2^i+1})$, then

$$B(u, v) = Q(u + v) - Q(u) - Q(v)$$

is a symmetric bilinear form;
Let

$$W := \{w \in \mathbb{F}_{2^n} \mid B(w, v) = 0, \forall v \in \mathbb{F}_{2^n}\}.$$

Theorem (van der Geer, van der Vlugt 1992)

W is the set of roots in $\mathbb{F}_{2^n}$ of a polynomial $XE_Q^- E_Q^+ \in \mathbb{F}_{2^n}[c_0, \ldots, c_h][X]$. Moreover, $\#C = 2^n + 1$ iff Q does not completely vanish on W.

Lisoněk noted that for the case of the Kim function we have $(K = \mathbb{F}_{2^3})$

- E_Q^- and E_Q^+ are free of α (this happens for all curves of this type).
- Consider $\beta \in K$. Then putting $X = \beta^2 Z$, we obtain $E_Q^- = \beta \cdot G$, with G free of b. There exists z_0 such that $E_Q^-(\beta^2 z_0) = 0$ and $Q(\beta^2 z_0) = 1$ for all $\beta \in K$.
- Similar argument for $\beta \in uK$.

So, to verify if $\#C'_{\alpha,\beta} = 2^6 + 1$ for all $(\alpha, \beta) \in K \times K$ and $(\alpha, \beta) \in uK \times uK$ $((\alpha, \beta) \neq (0,0))$, we need solving just two pairs of equations.

Lisoněk proposed to start with a polynomial $F(x)$ which is sum of pairs having form

$$c_i x^{2^{k_i+m}(2^i+1)} + d_i x^{2^{k_i}(2^i+1)}.$$

There are some compatibility conditions on the different k_i's.

Lisoněk performed some computational searches

- in $n = 6$, he found APN functions equivalent to a permutation (all CCZ-eq. to κ)
- in $n = 10$, he found APN functions but not equivalent to a permutation.

Conclusions

Problem

Find an infinite family of APN functions which includes the Kim function (satisfying subspace property).

Problem

Show that the existing families of APN functions are not equivalent to permutations.

Still The Big APN Problem

Are there APN permutations on $\mathbb{F}_{2^{2m}}$ for $m > 3$?

Thanks for your attention!