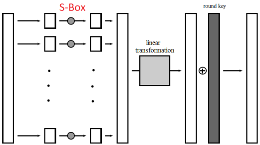
On Some Properties of Quadratic APN Functions of a Special Form

Irene Villa

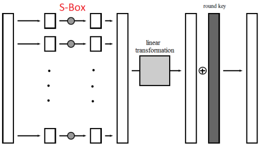
University of Bergen (Norway)

Cryptography

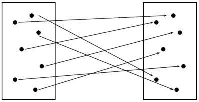
Cryptography	
> Block ciphers	

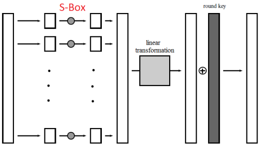
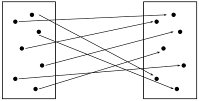
Cryptography

> Block ciphers



≫ S-Boxes



Cryptography	
$>$ Block ciphers	
$\gg$ S-Boxes	
$\ggg$ APN functions	optimal resistance against differential attack

Definitions

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}}$$

Definitions

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}}$$

unique *Univariate Polynomial Representation*

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \ \delta_i \in \mathbb{F}_{2^n}$$

Definitions

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}}$$

unique *Univariate Polynomial Representation*

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \ \delta_i \in \mathbb{F}_{2^n}$$

$$\textit{linear function } L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}$$

Definitions

$$\boxed{F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}}$$

unique *Univariate Polynomial Representation*

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \ \ \delta_i \in \mathbb{F}_{2^n}$$

$$\textit{linear function } L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}$$

$$Tr_n(x) = x + x^2 + x^4 + \cdots + x^{2^{n-1}}$$

Almost Perfect Nonlinear (APN)

$F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is APN if for any $a, b \in \mathbb{F}_{2^n}$ $a \neq 0$,
$F(x + a) - F(x) = b$ has at most 2 solutions

Almost Perfect Nonlinear (APN)

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if for any $a, b \in \mathbb{F}_{2^n}$ $a \neq 0$,
$F(x + a) - F(x) = b$ has at most 2 solutions

CCZ-equivalence relation

$F_1, F_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are CCZ-equivalent ($F_1 \overset{\text{CCZ}}{\sim} F_2$) if
$\mathcal{L}(\Gamma_{F_1}) = \Gamma_{F_2}$, with $\mathcal{L}$ affine permutation of $\mathbb{F}_{2^n}^2$ and
$\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ (*graph* of F)

Almost Perfect Nonlinear (APN)

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if for any $a, b \in \mathbb{F}_{2^n}$ $a \neq 0$, $F(x+a) - F(x) = b$ has at most 2 solutions

CCZ-equivalence relation

$F_1, F_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are CCZ-equivalent ($F_1 \overset{\text{CCZ}}{\sim} F_2$) if $\mathcal{L}(\Gamma_{F_1}) = \Gamma_{F_2}$, with $\mathcal{L}$ affine permutation of $\mathbb{F}_{2^n}^2$ and $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ (*graph* of F)

$$\boxed{F(x) = L_1(x^3) + L_2(x^9)}$$

L_1, L_2 linear functions over $\mathbb{F}_{2^n}$

On $F(x) = L_1(x^3) + L_2(x^9)$

On $F(x) = L_1(x^3) + L_2(x^9)$

(Budaghyan, Carlet and Leander, 2009)

- n even, if $L_1(x) + L_2(x^3)$ is a permutation then $L_1(x^3) + L_2(x^9)$ is APN,
- n odd, a weaker condition leads to APN functions

On $F(x) = L_1(x^3) + L_2(x^9)$

(Budaghyan, Carlet and Leander, 2009)

- n even, if $L_1(x) + L_2(x^3)$ is a permutation then $L_1(x^3) + L_2(x^9)$ is APN,
- n odd, a weaker condition leads to APN functions

• $x^3 + a^{-1} Tr_n(a^3 x^9)$ is APN for any $a \neq 0$, $\quad (x^3 + Tr_n(x^9))$

On $F(x) = L_1(x^3) + L_2(x^9)$

(Budaghyan, Carlet and Leander, 2009)

- n even, if $L_1(x) + L_2(x^3)$ is a permutation then $L_1(x^3) + L_2(x^9)$ is APN,
- n odd, a weaker condition leads to APN functions

• $x^3 + a^{-1}Tr_n(a^3x^9)$ is APN for any $a \neq 0$, $\quad (x^3 + Tr_n(x^9))$
• $x^3 + a^{-1}Tr_3(a^6x^{18} + a^{12}x^{36})$ is APN for any $a \neq 0$ and $3|n$;
• $x^3 + a^{-1}Tr_3(a^3x^9 + a^6x^{18})$ is APN for any $a \neq 0$ and $3|n$.

On $F(x) = L_1(x^3) + L_2(x^9)$

(Budaghyan, Carlet and Leander, 2009)

- n even, if $L_1(x) + L_2(x^3)$ is a permutation then $L_1(x^3) + L_2(x^9)$ is APN,
- n odd, a weaker condition leads to APN functions

• $x^3 + a^{-1}Tr_n(a^3x^9)$ is APN for any $a \neq 0$, $(x^3 + Tr_n(x^9))$
• $x^3 + a^{-1}Tr_3(a^6x^{18} + a^{12}x^{36})$ is APN for any $a \neq 0$ and $3|n$;
• $x^3 + a^{-1}Tr_3(a^3x^9 + a^6x^{18})$ is APN for any $a \neq 0$ and $3|n$.

(Budaghyan, Carlet and Leander, 2009)

$n = 8$, $x^9 + Tr_n(x^3)$ is APN
(CCZ-ineq. to power functions and to $x^3 + Tr_n(x^9)$)

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.
For $n = 8$ listed 23 APN functions:

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.
For $n = 8$ listed 23 APN functions:

- 17 are of the form $L_1(x^3) + L_2(x^9)$ [1-13,15-17,19]:

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.
For $n = 8$ listed 23 APN functions:

- 17 are of the form $L_1(x^3) + L_2(x^9)$ [1-13,15-17,19]:
    - 10 are affine equivalent to $x^3 + L(x^9)$ [1,3,5-9,11-13],
    - 5 are affine equivalent to $x^9 + L(x^3)$ [2,4-6,19].

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.
For $n = 8$ listed 23 APN functions:

- 17 are of the form $L_1(x^3) + L_2(x^9)$ [1-13,15-17,19]:
  - 10 are affine equivalent to $x^3 + L(x^9)$ [1,3,5-9,11-13],
  - 5 are affine equivalent to $x^9 + L(x^3)$ [2,4-6,19].
- 2 are of the form $L_1(x^3) + L_2(x^5) + L_3(x^9)$ [21,22].

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.
For $n = 8$ listed 23 APN functions:

- 17 are of the form $L_1(x^3) + L_2(x^9)$ [1-13,15-17,19]:
  - 10 are affine equivalent to $x^3 + L(x^9)$ [1,3,5-9,11-13],
  - 5 are affine equivalent to $x^9 + L(x^3)$ [2,4-6,19].
- 2 are of the form $L_1(x^3) + L_2(x^5) + L_3(x^9)$ [21,22].
- 3 are of the form $L_1(x^3) + L_2(x^5) + L_3(x^9) + L_4(x^{17})$ [14,18,20].

(Edel and Pott, 2008)
List of APN functions for n=6,7,8.
For $n = 8$ listed 23 APN functions:

- 17 are of the form $L_1(x^3) + L_2(x^9)$ [1-13,15-17,19]:
  - 10 are affine equivalent to $x^3 + L(x^9)$ [1,3,5-9,11-13],
  - 5 are affine equivalent to $x^9 + L(x^3)$ [2,4-6,19].
- 2 are of the form $L_1(x^3) + L_2(x^5) + L_3(x^9)$ [21,22].
- 3 are of the form $L_1(x^3) + L_2(x^5) + L_3(x^9) + L_4(x^{17})$ [14,18,20].
- Last function x^{57} [23] is of algebraic degree 4.

Necessary Conditions

Lemma (1)

For n even, $k = (2^n - 1)/3$ and $\alpha \in \mathbb{F}_{2^n}^*$ primitive element if $F(x) = L_1(x^3) + L_2(x^9)$ is APN then $F(\alpha^j) \neq 0$ for $j = 0, \ldots, k-1$

Necessary Conditions

Lemma (1)

For n even, $k = (2^n - 1)/3$ and $\alpha \in \mathbb{F}_{2^n}^*$ primitive element if $F(x) = L_1(x^3) + L_2(x^9)$ is APN then $F(\alpha^j) \neq 0$ for $j = 0, \dots, k-1$

Lemma (2)

For n multiple of 6, if $L_1(x^3) + L_2(x^9)$ is APN then for any $a, \beta \neq 0$ with $Tr_3(\beta) = 0$ $L_1(a^3\beta) \neq 0$

Necessary Conditions

Lemma (1)

For n even, $k = (2^n - 1)/3$ and $\alpha \in \mathbb{F}_{2^n}^*$ primitive element if $F(x) = L_1(x^3) + L_2(x^9)$ is APN then $F(\alpha^j) \neq 0$ for $j = 0, \dots, k-1$

Lemma (2)

For n multiple of 6, if $L_1(x^3) + L_2(x^9)$ is APN then for any $a, \beta \neq 0$ with $Tr_3(\beta) = 0$ $L_1(a^3\beta) \neq 0$

Proposition

If $L_1(x^3) + L_2(x^9)$ is APN, then the linear function $L_3(x) = L_1(x^2 + x) + L_2(x^8 + x)$ is a 2-to-1 map satisfying $L_3(x) = 0$ if and only if $x = 0, 1$

Necessary and Sufficient Conditions

Lemma (3)

$L_1(x^3) + L_2(x^9)$ is APN if and only if

- *for any $a \neq 0$ and $x \neq 0, 1$*
  $L_1(a^2(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0$

or equivalently

- *for any $a, y \neq 0$ with $Tr_n(y) = 0$*
  $L_1(a^3 y) + L_2(a^9(y^4 + y^2 + y)) \neq 0$

Necessary and Sufficient Conditions

Lemma (3)

$L_1(x^3) + L_2(x^9)$ is APN if and only if

- *for any $a \neq 0$ and $x \neq 0, 1$* $L_1(a^2(x^2 + x)) + L_2(a^9(x^8 + x)) \neq 0$

or equivalently

- *for any $a, y \neq 0$ with $Tr_n(y) = 0$* $L_1(a^3 y) + L_2(a^9(y^4 + y^2 + y)) \neq 0$

Lemma (4)

$L_1(x^3) + L_2(x^9)$ is APN if and only if for any $a \neq 0$ there exists one and only one $\lambda \neq 0$ such that $Tr_n(\lambda L_1(ax^2 + a^2 x) + \lambda L_2(ax^8 + a^8 x)) \equiv 0$

Necessary and Sufficient Conditions

Lemma (5)

$L_1(x^3) + L_2(x^9)$ is APN if and only if for any $a, y \neq 0$ with $Tr_n(y) = 0$, if it exists $t \in \mathbb{F}_{2^n}$ satisfying $Tr_n(t) = 0$ and $L_1(a^3 y) = L_2(a^9 y^3 t)$ then $L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0$

Necessary and Sufficient Conditions

Lemma (5)

$L_1(x^3) + L_2(x^9)$ is APN if and only if for any $a, y \neq 0$ with $Tr_n(y) = 0$, if it exists $t \in \mathbb{F}_{2^n}$ satisfying $Tr_n(t) = 0$ and $L_1(a^3y) = L_2(a^9y^3t)$ then $L_2(a^9(y^4 + ty^3 + y^2 + y)) \neq 0$

Corollary

If for any $a, y \neq 0$ $Tr_n(y) = 0$ the equation $L_1(a^3y) + L_2(a^9y^3t) = 0$ is satisfied only for t with $Tr_n(t) = 1$, then $L_1(x^3) + L_2(x^9)$ is APN

On $x^9 + L(x^3)$

On $x^9 + L(x^3)$

Lemma (6)

If $3|n$ then $x^9 + Tr_n(x^3)$ is not APN

On $x^9 + L(x^3)$

Lemma (6)

If $3|n$ then $x^9 + Tr_n(x^3)$ is not APN

Using Lemma (5) (computational results done with MAGMA)

On $x^9 + L(x^3)$

Lemma (6)

If $3|n$ then $x^9 + Tr_n(x^3)$ is not APN

Using Lemma (5) (computational results done with MAGMA)

$\Rightarrow$ $x^9 + Tr_n(x^3)$ is APN only for $n = 4, 5, 8$ (checked until n=200);

On $x^9 + L(x^3)$

Lemma (6)

If $3|n$ then $x^9 + Tr_n(x^3)$ is not APN

Using Lemma (5) (computational results done with MAGMA)

- $\Rightarrow$ $x^9 + Tr_n(x^3)$ is APN only for $n = 4, 5, 8$ (checked until n=200);
- $\Rightarrow$ list of APN of the form $x^9 + L(x^3)$ (representatives for CCZ-equivalence relation) for $n = 4, \ldots, 10$

On $x^9 + L(x^3)$

CCZ-equivalent classes, with $\alpha \in \mathbb{F}_{2^n}^*$ primitive element

n	$\sharp$	Representative for $L(x)$
4	1	0
5	2	$0, \quad Tr_n(x)$
6	2	$\alpha^{44}x + \alpha x^2, \quad \alpha^{23}x + x^4$
7	1	0
8	8	$0, \quad Tr_n(x), \quad x^2 + x^{16},$ $x^8 + x^{128}, \quad x^4 + \alpha^{85}x^8 + x^{16},$ $\alpha^{60}x + \alpha^{200}x^2 + \alpha^{242}x^4 + \alpha^{190}x^8 + \alpha x^{16},$ $\alpha^{228}x^{64} + \alpha^{107}x^{32} + \alpha^{80}x^8 + \alpha^{137}x^2 + \alpha^{189}x,$ $\alpha^{25}x^{128} + \alpha^{194}x^4 + \alpha^{146}x^2$
9	0	-
10	2	$0, \quad \alpha^{1021}x + \alpha^{1022}x^2 + \alpha x^4$

Fact

If $3 \nmid n$ then $L(x) = 0$ generates the APN function x^9.

Fact

If $3 \nmid n$ then $L(x) = 0$ generates the APN function x^9.

Proposition

If n is even then for any $a \neq 0$ not a cube

$$L(x) = ax^4 + a^{-1}x^2 + a^{-2}x$$

generates an APN function $x^9 + L(x^3)$ linear equivalent to x^3.

Comparison with Edel-Pott list ($n = 6$ and $n = 8$) :

Comparison with Edel-Pott list ($n = 6$ and $n = 8$) :
[$n = 6$]

1. $L(x) = \alpha^{44}x + \alpha x^2$,
   $$x^9 + L(x^3) \overset{CCZ}{\sim} \text{no. } 2\ (x^3 + \alpha^{-1} Tr_n(\alpha^3 x^9)),$$
2. $L(x) = \alpha^{23}x + x^4$,
   $$x^9 + L(x^3) \overset{CCZ}{\sim} \text{no. } 1\ (x^3).$$

$[n = 8]$

1. $L(x) = 0$, no. 2 (x^9),
2. $L(x) = Tr_n(x)$, no. 4 $(x^9 + Tr_n(x^3))$,
3. $L(x) = x^2 + x^{16}$,
   $x^9 + L(x^3) \overset{CCZ}{\sim}$ no. 3 $(x^3 + Tr_n(x^9))$,
4. $L(x) = x^8 + x^{128}$,
   $x^9 + L(x^3) \overset{CCZ}{\sim}$ no. 1 (x^3) ,
5. $L(x) = x^4 + \alpha^{85}x^8 + x^{16}$,
   $x^9 + L(x^3) \overset{CCZ}{\sim}$ no. 6,
6. $L(x) = \alpha^{60}x + \alpha^{200}x^2 + \alpha^{242}x^4 + \alpha^{190}x^8 + \alpha x^{16}$,
   $x^9 + L(x^3) \overset{CCZ}{\sim}$ no. 9,
7. $L(x) = \alpha^{228}x^{64} + \alpha^{107}x^{32} + \alpha^{80}x^8 + \alpha^{137}x^2 + \alpha^{189}x$,
   $x^9 + L(x^3) \overset{CCZ}{\sim}$ no. 5,
8. $L(x) = \alpha^{25}x^{128} + \alpha^{194}x^4 + \alpha^{146}x^2$,
   $x^9 + L(x^3) \overset{CCZ}{\sim}$ no. 19.

Thank you for your attention