A Generalization of Almost Perfect Nonlinear Functions

Shuhei TSUJIE
(Joint work with Masamichi KURODA)

Hokkaido University

Dec 20, 2016

This presentation is based on arXiv:1612.00580

Derivatives and linearity

Let $F := \mathbb{F}_{p^n} = GF(p^n)$.
For a function $f : F \to F$ and $a \in F$, define the derivative $D_a f$ by

$$D_a f(x) := f(x + a) - f(x).$$

For $a, b \in F$, we consider the set

$$N_f(a, b) := \{ x \in F \mid D_a f(x) = b \}.$$

The number $\max_{a \in F^\times, b \in F} \#N_f(a, b)$ is considered to be the "linearity" of f because we have that

$$f \text{ is linear over } \mathbb{F}_p \Leftrightarrow \max_{a \in F^\times, b \in F} \#N_f(a, b) = p^n.$$

PN and APN functions

If the number $\max_{a \in F^\times, b \in F} \#N_f(a,b)$ is small
then f has high nonlinearity.

Definition

f is perfect nonlinear (PN) $\overset{\text{def}}{\Leftrightarrow} \#N_f(a,b) = 1, (\forall a \in F^\times, b \in F)$.

Unfortunately, there exist no PN functions for $p = 2$
since if x is a solution of

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

then $x + a$ is also a solution, which leads that $N_f(a,b)$ is divisible by 2.

Definition

f is almost perfect nonlinear (APN) $\overset{\text{def}}{\Leftrightarrow} \#N_f(a,b) \leq 2, (\forall a \in F^\times, b \in F)$.

Many researchers have studied APN functions for $p = 2$.
There are applications to differential cryptanalysis and finite geometry.

Some researchers have studied APN functions for odd characteristic.
Their algebraic properties, however, is quite different from the case of characteristic 2.

We consider a generalization of APN functions for odd characteristic as follows:

For a function $F \to F$ and $a \in F$ we define

$$\tilde{D}_a f(x) := \sum_{i \in \mathbb{F}_p} f(x + ia).$$

Note that if $p = 2$ then we have

$$\tilde{D}_a f(x) = f(x) + f(x + a) = f(x + a) - f(x) = D_a f(x).$$

For $a, b \in F$ define

$$\tilde{N}_f(a, b) := \left\{ x \in F \;\middle|\; \tilde{D}_a f(x) = b \right\}.$$

Definition

f is a generalized almost perfect nonlinear (GAPN) function
$\overset{\text{def}}{\Leftrightarrow} \#\tilde{N}_f(a, b) \leq p, \quad (\forall a \in F^\times, b \in F).$

Some generalizations

Proposition (Beth-Ding (1993), Nyberg (1994))

The inverse permutation $f(x) = x^{2^n-2}$ on $\mathbb{F}_{2^n}$ is APN if and only if n is odd.

Proposition

The inverse permutation $f(x) = x^{p^n-2}$ on $\mathbb{F}_{p^n}$ with p odd is a GAPN function.

Some generalizations

Proposition (Gold (1968), Nyberg (1994))

The monomial function $f(x) = x^{2^i+1}$ *with* $\gcd(n, i) = 1$ *on* $\mathbb{F}_{n^n}$
is an APN function of algebraic degree 2.
(These functions are called the Gold functions)

Theorem

The monomial function $f(x) = x^{p^i+p-1}$ *with* $\gcd(n, i) = 1$ *on* $\mathbb{F}_{p^n}$
is a GAPN function of algebraic degree p.

Some generalizations

Definition

A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called a (generalized) almost bent function if

$$W_f(a,b) := \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}(ax)+\mathrm{Tr}(bf(x))} \in \left\{ 0, \pm p^{\frac{n+1}{2}} \right\}, (\forall a, b \in \mathbb{F}_{p^n}, b \neq 0).$$

Theorem (Chabaud-Vaudenay (1995))

When $p = 2$, "AB $\Rightarrow$ APN."

Theorem

Let $p = 3$. Suppose that a function f on $\mathbb{F}_{3^n}$ of algebraic degree 3 satisfies $f(-x) = -f(x)$. If f is a GAB function then f is a GAPN function.

Some generalizations

Theorem (Yoshiara (2008))

When $p = 2$, we can construct dual hyperovals with APN functions of algebraic degree 2.

Theorem

We can construct dual arcs with GAPN functions of algebraic degree p.