Towards APN permutations

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada
some parts are joint work with Benjamin Chase (SFU)

The 5th International Workshop on
Boolean Functions and their Applications (BFA)
Loen, Norway

15 September 2020

Outline

1. APN permutations
2. Walsh zero spaces of APN functions
3. Kim-type APN functions

APN functions

Definition

We say that a function $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ is *almost perfect nonlinear (APN)* if for all $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, the equation

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

has at most two solutions $x \in \mathbb{F}_{2^n}$.

More generally such f is called a *differentially 2-uniform function.*

We can use $\mathbb{F}_2^n$ instead of $\mathbb{F}_{2^n}$ in the definition, or other groups can be used as well.

APN functions

Differentially uniform functions are important in symmetric cryptography (block ciphers, hash functions) where they protect against differential cryptanalysis and linear cryptanalysis attacks.

In block ciphers, APN functions find applications in the construction of *S-boxes* (substitution boxes) which are the only non-linear components of the cipher.

In the design of block ciphers it is beneficial if the S-boxes are *invertible,* that is, if they are *permutations* of $\mathbb{F}_{2^n}$.

APN functions: examples

$f(x) = x^3$ is APN for all n (but it is a permutation of $\mathbb{F}_{2^n}$ only when n is odd)

$f(x) = 1/x$ (with $f(0) = 0$) is APN iff n is odd (it is a permutation of $\mathbb{F}_{2^n}$ for all n). This function is used in the S-box of the *Advanced Encryption Standard (AES)* with $n = 8$; it is differentially 4-uniform when n is even.

Infinite families of APN *monomial* functions have been classified, and also several infinite families of *multinomial* APN functions are known.

The question about existence of APN permutations of $\mathbb{F}_{2^n}$ for even n is the Big APN Problem.

Walsh zero space

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. For $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ we define the Walsh transform of f at (a, b) as $\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax+bf(x))}$. We say that (a, b) is a *Walsh zero* of f if $\mathcal{W}_f(a, b) = 0$.

Definition

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Suppose that S is an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $\dim_{\mathbb{F}_2} S = n$ and each element of S except $(0, 0)$ is a Walsh zero of f. We say that S is a *WZ space of f*.

We say that two WZ spaces S, T of the same function *intersect trivially* if $S \cap T = \{(0, 0)\}$.

Functions CCZ-equivalent to a permutation

Proposition

Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that $f(0) = 0$. Then f is CCZ-equivalent to a permutation of $\mathbb{F}_{2^n}$ if and only if there exist two WZ spaces of f that intersect trivially.

This was used to construct the APN permutation of $\mathbb{F}_{2^6}$ by Dillon et al. in 2009, using the *Kim function* for f. More details on *Kim-type functions* will follow in the second part of the talk.

Characterizing Walsh zeros of quadratic functions

Squaring method computes $(\mathcal{W}_f(a,b))^2$. It associates a certain linear form $\mathcal{L}_b$ to f and (a,b). Then (a,b) is a Walsh zero of f if $\mathrm{Tr}(f(x))$ does not vanish completely on the kernel of $\mathcal{L}_b$.

In this way Walsh spectra were determined for some classes of quadratic functions, most recently for functions of the form $f(x) = x^3 + a^{-1}\mathrm{Tr}(a^3x^9)$ and two other similar families (Budaghyan, Helleseth, Li, Sun 2017). Walsh zeros were not determined explicitly. In order to upper bound the cardinality of the kernel of $\mathcal{L}_b$, an ad-hoc method developed earlier by Dobbertin was used.

For investigations of such kernels one can apply a more systematic theory developed by van der Geer and van der Vlugt (1992).

Characterizing Walsh zeros of quadratic functions

Proposition

Let n be even, $\gcd(k,n)=1$, and $a,b \in \mathbb{F}_{2^n}$. If $b \neq 0$, then (a,b) is a Walsh zero of the Gold function $f(x)=x^{2^k+1}$ if and only if b is a (2^k+1)th power in $\mathbb{F}_{2^n}$ (equivalently, b is a cube in $\mathbb{F}_{2^n}$) and $\mathrm{Tr}_2^n(az) \neq 0$ for each $z \in \mathbb{F}_{2^n}$ such that $bz^{2^k+1}+1=0$.

Proposition

Let n be even and $a,b \in \mathbb{F}_{2^n}$.
(i) If $b \neq 0$ and $\mathrm{Tr}(b)=0$ then (a,b) is a Walsh zero of $f(x)=x^3+\mathrm{Tr}(x^9)$ if and only if it is a Walsh zero of $f(x)=x^3$.
(ii) If $\mathrm{Tr}(b)=1$, let x^* be the unique solution of $x^9+x^3+bx+1=0$ in $\mathbb{F}_{2^n}$. Then (a,b) is a Walsh zero of $f(x)=x^3+\mathrm{Tr}(x^9)$ if and only if x^* is a cube in $\mathbb{F}_{2^n}$ and $\mathrm{Tr}_2^n(az) \neq 0$ for each $z \in \mathbb{F}_{2^n}$ such that $z^3=x^*$.

Examples of WZ spaces

Proposition

Let n be even and $\gcd(k, n) = 1$. *Let* $u \in \mathbb{F}_{2^n}^*$. *The set*

$$G_{k,u} = \{(a, 0) : a \in \mathbb{F}_{2^n} | \mathrm{Tr}(ua) = 0\} \cup \{(a, u^{-(2^k+1)}) : a \in \mathbb{F}_{2^n} | \mathrm{Tr}(ua) = 1\}$$

is a WZ space of the Gold function $f(x) = x^{2^k+1}$ *on* $\mathbb{F}_{2^n}$.

Examples of WZ spaces

Proposition

Let n be even and $f(x) = x^3 + \mathrm{Tr}(x^9)$. Let $b \in \mathbb{F}_{2^n}^*$.
(i) If $\mathrm{Tr}(b) = 0$ and b is a cube in $\mathbb{F}_{2^n}$, then $G_{1,u}$ is a WZ space of f where u is any of the cube roots of $1/b$.
(ii) If $\mathrm{Tr}(b) = 1$ then let x^* be the unique solution of $x^9 + x^3 + bx + 1 = 0$ in $\mathbb{F}_{2^n}$. If x^* is a cube in $\mathbb{F}_{2^n}$ and u is any of the cube roots of x^*, then the set

$$S_u = \{(a, 0) \,:\, a \in \mathbb{F}_{2^n} \,|\, \mathrm{Tr}(ua) = 0\} \cup \{(a, b) \,:\, a \in \mathbb{F}_{2^n} \,|\, \mathrm{Tr}(ua) = 1\}$$

is a WZ space of f.

Outlook

We hope that this approach can lead to an alternative and possibly simpler proof of CCZ-inequivalence of APN Gold functions with permutations in even dimensions.

We have some further results on the WZ spaces but we would like to devote the second half of the talk to some very recent and interesting developments on Kim-type APN functions.

APN permutation of $\mathbb{F}_{2^6}$

An APN permutation of $\mathbb{F}_{2^6}$ was announced at the Fq9 conference in 2009 by Dillon et al. Its construction is based on the APN function

$$\kappa(x) = x^3 + x^{10} + ux^{24}$$

where u is a suitable primitive element of $\mathbb{F}_{2^6}$. The function κ is known as *Kim function.* APN permutations of $\mathbb{F}_{2^6}$ are then constructed by applying a suitable CCZ equivalence transformation to the Kim function; all examples constructed are mutually CCZ equivalent.

Big APN Problem

The question of existence of APN permutations of $\mathbb{F}_{2^n}$ for even $n > 6$ was posed as the *Big APN Problem.*

By generalizing the form of the Kim function, Carlet in 2014 posed the following open problem:

Find more APN functions or, better, infinite classes of APN functions of the form $X^3 + aX^{2+q} + bX^{2q+1} + cX^{3q}$ *where* $q = 2^{n/2}$ *with* n *even, or more generally of the form* $X^{2^k+1} + aX^{2^k+q} + bX^{2^k q+1} + cX^{2^k q+q}$, *where* $\gcd(k, n) = 1$*.*

Kim-type functions

There have been several lines of attack to approach Carlet's problem and similar problems.

Most recently, Li, Li, Helleseth and Qu (arXiv:2007.03996, July 2020) completely characterized APN functions on $\mathbb{F}_{2^n}$ of the form $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$, where $q = 2^m$ and $m = n/2$, $m \geq 4$. We will call functions of this form *Kim-type functions.*

Characterization of Kim-type APN functions

Li, Li, Helleseth and Qu (arXiv:2007.03996, July 2020)

Let

$$\begin{aligned}\theta_1 &= 1 + a_1^2 + a_2\bar{a}_2 + a_3\bar{a}_3\\ \theta_2 &= a_1 + \bar{a}_2 a_3\\ \theta_3 &= \bar{a}_2 + a_1\bar{a}_3\\ \theta_4 &= a_1^2 + a_2\bar{a}_2.\end{aligned}$$

where $\bar{z} = z^q$ for $z \in \mathbb{F}_{q^2}$.

Characterization of Kim-type APN functions

Li, Li, Helleseth and Qu (arXiv:2007.03996, July 2020)

Theorem

Let $n = 2m$ with $m \geq 4$ and $f(x) = \bar{x}^3 + a_1\bar{x}^2 x + a_2\bar{x}x^2 + a_3 x^3$, where $a_1 \in \mathbb{F}_{2^m}, a_2, a_3 \in \mathbb{F}_{2^n}$. Let θ_i's be defined as on the previous slide and define

$$\begin{aligned}\Gamma_1 \quad &= \quad \left\{(a_1, a_2, a_3) \mid \theta_1 \neq 0,\ \mathrm{Tr}_m\left(\frac{\theta_2\bar{\theta}_2}{\theta_1^2}\right) = 0,\right.\\ &\qquad \left.\theta_1^2\theta_4 + \theta_1\theta_2\bar{\theta}_2 + \theta_2^2\theta_3 + \bar{\theta}_2^2\bar{\theta}_3 = 0\right\} \quad \textit{and}\\ \Gamma_2 \quad &= \quad \left\{(a_1, a_2, a_3) \mid \theta_1 \neq 0,\ \mathrm{Tr}_m\left(\frac{\theta_2\bar{\theta}_2}{\theta_1^2}\right) = 0,\right.\\ &\qquad \left.\theta_1^2\theta_3 + \theta_1\bar{\theta}_2^2 + \theta_2^2\theta_3 + \bar{\theta}_2^2\bar{\theta}_3 = 0\right\}.\end{aligned}$$

Characterization of Kim-type APN functions

Li, Li, Helleseth and Qu (arXiv:2007.03996, July 2020)

Theorem (continued)

Then f is APN over $\mathbb{F}_{2^n}$ if and only if

(1) *m is even, $(a_1, a_2, a_3) \in \Gamma_1 \cup \Gamma_2$; or*

(2) *m is odd, $(a_1, a_2, a_3) \in \Gamma_1$.*

Characterization of Kim-type APN functions

A characterization of the Kim-type APN functions for the special case when the coefficients a_i lie in the subfield $\mathbb{F}_q$ was given earlier by Krasnayová (2016) and the following result on affine equivalence of these functions with Gold functions was proved by Göloğlu, Krasnayová and Lisoněk (2020).

Theorem

Suppose that $m \geq 4$ is an integer and let $q = 2^m$. Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1, a_2, a_3 \in \mathbb{F}_q$. If f is APN, then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.

Kim-type APN functions are equivalent to Gold functions

We extend the result of Li, Li, Helleseth and Qu (arXiv:2007.03996, July 2020) and of Göloğlu, Krasnayová and Lisoněk (2020).

Theorem (Chase, L. 2020)

Suppose that $m \geq 4$ is an integer and let $q = 2^m$. Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. If f is APN, then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.

Proof

Proposition

Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}_{q^2}^*$ and $a_3 \in \mathbb{F}_{q^2}$. If $a_1/a_2 \notin U$ and $a_1/a_2 \neq a_3^q$, then f is affine equivalent to $h(x) = x^{3q} + a_1' x^{2q+1} + a_3' x^3$ where $a_1' \in \mathbb{F}_q$ and $a_3' \in \mathbb{F}_{q^2}$.

The affine transformation for restricting a_1 from $a_1 \in \mathbb{F}_{q^2}$ to $a_1 \in \mathbb{F}_q$ is given in Li, Li, Helleseth and Qu (arXiv:2007.03996, July 2020).

Proof

Proposition

Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ *be given by* $f(x) = x^{3q} + a_1 x^{2q+1} + a_3 x^3$ *where* $a_1, a_3 \in \mathbb{F}_{q^2}$ *and* $a_1 = 0$ *or* $a_3 = 0$*. If* f *is APN, then* f *is affine equivalent to* $G_1(x) = x^3$*.*

Proof

Proposition

Let $f : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ *be given by* $f(x) = x^{3q} + a_1 x^{2q+1} + a_3 x^3$ *where* $a_1 \in \mathbb{F}_q$ *and* $a_3 \in \mathbb{F}_{q^2}$*. If* $(a_1, 0, a_3) \in \Gamma_1$ *then* f *is affine equivalent to* $G_1(x) = x^3$ *or* f *is affine equivalent to* $G_2(x) = x^{2^{m-1}+1}$*.*

Proposition

Let $f : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ *be given by* $f(x) = x^{3q} + a_1 x^{2q+1} + a_3 x^3$ *where* $a_1 \in \mathbb{F}_q$ *and* $a_3 \in \mathbb{F}_{q^2}$*. If* $(a_1, 0, a_3) \in \Gamma_2$ *then* f *is affine equivalent to* $G_1(x) = x^3$ *or* f *is affine equivalent to* $G_2(x) = x^{2^{m-1}+1}$*.*

Proof

Proposition

Let $f : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}^*_{q^2}$ and $a_3 \in \mathbb{F}_{q^2}$, and assume that $a_1/a_2 \in U$. If f is APN, then m is even, and furthermore $a_1, a_2, a_3 \in \mathbb{F}_q$ or there exist $u, z \in U$ such that

$$\begin{aligned} a_1 &= \frac{(u^3+z)^2}{u(u^2+z)^2} \\ a_2 &= \frac{(u^3+z)^2}{(u^2+z)^2} \\ a_3 &= \frac{uz^2(u+1)^2}{(u^2+z)^2}. \end{aligned}$$

Proof

Proposition

Let $f : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ be given by
$f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ *where*

$$
\begin{aligned}
a_1 &= \frac{(u^3+z)^2}{u(u^2+z)^2} \\
a_2 &= \frac{(u^3+z)^2}{(u^2+z)^2} \\
a_3 &= \frac{uz^2(u+1)^2}{(u^2+z)^2}
\end{aligned}
$$

for some $u, z \in U$ such that $u^2 \neq z$, and m is even. If f is APN, then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.

Proof

Proposition

Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ *be given by* $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ *where* $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}_{q^2}^*$ *and* $a_3 \in \mathbb{F}_{q^2}$, *and assume that* $a_1/a_2 = a_3^q$. *If* f *is APN, then* f *is affine equivalent to* $G_1(x) = x^3$.

Combination of these results provides the proof of our main theorem.

Reference

B. Chase, P. Lisoněk,
Kim-type APN functions are affine equivalent to Gold functions.
arXiv:2009.05937 [cs.IT]