Geometrical and combinatorial aspects of APN functions

Yves Edel

Department of Pure Mathematics and Computer Algebra
Ghent University

Contact Forum "Coding Theory and Cryptography III"
Brussels, 25 September 2009

Outline

APN functions and . . .

- Cryptography
- Coding Theory
- Geometry
- Designs and Invariants

Nonlinear Functions

To be secure, cryptographic algorithms need a nonlinear part.

E.g. the "S-boxes" are such nonlinear functions.

There are different concepts of nonlinearity
We focus on the concept that provides optimal security against differential cryptanalysis, i.e. on (almost) perfect nonlinear functions.

Nonlinear Functions

$$F : \mathbb{F}_p^m \mapsto \mathbb{F}_p^m$$

$$m(F) := \max_{a \in \mathbb{F}_p^m - \{0\}} |\{F(x+a) - F(x) | x \in \mathbb{F}_p^m\}|$$

If F is linear, then $m(F) = 1$.

If $m(F) = p^m$ (hence $|\{F(x+a) - F(x)$ is a permutation) we call F perfect nonlinear (PN).

PN functions exist only for p odd, as for $p = 2$, we have that x and $x + a$ yield the same value of $F(x + a) - F(x)$.

Nonlinear Functions

$$F : H \mapsto N$$

$$m(F) := \max_{a \in \mathbb{F}_p^m - \{0\}} |\{F(x+a) - F(x) | x \in \mathbb{F}_p^m\}|$$

If F is linear, then $m(F) = 1$.

If $m(F) = p^m$ (hence $|\{F(x+a) - F(x)$ is a permutation) we call F perfect nonlinear (PN).

PN functions exist only for p odd, as for $p = 2$, we have that x and $x + a$ yield the same value of $F(x + a) - F(x)$.

Nonlinear Functions

$$F : \mathbb{F}_p^m \mapsto \mathbb{F}_p^m, \quad p \text{ prime}$$

$$m(F) := \max_{a \in \mathbb{F}_p^m - \{0\}} |\{F(x+a) - F(x) | x \in \mathbb{F}_p^m\}|$$

If F is linear, then $m(F) = 1$.

If $m(F) = p^m$ (hence $\{F(x+a) - F(x)$ is a permutation$\}$) we call F perfect nonlinear (PN).

PN functions exist only for p odd, as for $p = 2$, we have that x and $x + a$ yield the same value of $F(x + a) - F(x)$.

Nonlinear Functions

$$F : \mathbb{F}_p^m \mapsto \mathbb{F}_p^m, \quad p \text{ prime}$$

$$m(F) := \max_{a \in \mathbb{F}_p^m - \{0\}} |\{F(x+a) - F(x) | x \in \mathbb{F}_p^m\}|$$

If F is linear, then $m(F) = 1$.

If $m(F) = p^m$ (hence if $F(x+a) - F(x)$ is a permutation) we call F perfect nonlinear (PN).

PN functions exist only for p odd, as for $p = 2$, we have that x and $x + a$ yield the same value of $F(x+a) - F(x)$.

For $p = 2$, if $m(F) = 2^{n/2}$ (hence if $F(x+a) - F(x)$ is 2^{n-1} to 1) we call F almost perfect nonlinear (APN).

Nonlinear Functions

$$F : \mathbb{F}_p^m \mapsto \mathbb{F}_p^m, \quad p \text{ prime}$$

$$m(F) := \max_{a \in \mathbb{F}_p^m - \{0\}} |\{F(x+a) - F(x) | x \in \mathbb{F}_p^m\}|$$

If F is linear, then $m(F) = 1$.

If $m(F) = p^m$ (hence if $F(x+a) - F(x)$ is a permutation) we call F perfect nonlinear (PN).

PN functions exist only for p odd, as for $p = 2$, we have that x and $x + a$ yield the same value of $F(x+a) - F(x)$.

For $p = 2$, if $m(F) = 2^m/2$ (hence if $F(x+a) - F(x)$ is "2 to 1") we call F almost perfect nonlinear (APN).

Nonlinear Functions

$$F : \mathbb{F}_p^m \mapsto \mathbb{F}_p^m, \quad p \text{ prime}$$

$$m(F) := \max_{a \in \mathbb{F}_p^m - \{0\}} |\{F(x+a) - F(x) | x \in \mathbb{F}_p^m\}|$$

If F is linear, then $m(F) = 1$.

If $m(F) = p^m$ (hence if $F(x+a) - F(x)$ is a permutation) we call F perfect nonlinear (PN).

PN functions exist only for p odd, as for $p = 2$, we have that x and $x + a$ yield the same value of $F(x+a) - F(x)$.

For $p = 2$, if $m(F) = 2^m/2$ (hence if $F(x+a) - F(x)$ is "2 to 1") we call F almost perfect nonlinear (APN).

APN Functions known before 2006

The known APN functions $F : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ were the power functions $F(x) = x^d$ with:

	Exponents d	Conditions
Gold functions	$2^i + 1$	$gcd(i, m) = 1$, $1 \leq i \leq \frac{m-1}{2}$
Kasami functions	$2^{2i} - 2^i + 1$	$gcd(i, m) = 1$, $1 \leq i \leq \frac{m-1}{2}$
Welch function	$2^t + 3$	$m = 2t + 1$
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$m = 2t + 1$
Inverse function	$2^{2t} - 1$	$m = 2t + 1$
Dobbertin function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$m = 5i$

Extended Affine Equivalence

We call two APN functions $F, F' : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$ extended affine (EA) equivalent if there exist invertible linear maps $L, L' : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$ and an affine map $A : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$ such that

$$F'(x) = L'(F(L(x))) + A(x)$$

If F is a permutation, also its inverse "F^{-1}" is APN.

Error Correcting Codes

A binary linear code $[n, k, d]$ is a k-dimensional subspace of the vectorspace $\mathbb{F}_2^n$, such that any two different $c, c' \in [n, k, d]$ differ in at least d coordinates.

A matrix who's rows generate the code $[n, k, d]$ is called a generator matrix of the code.

APN Functions as (Error Correcting) Codes

$$M_F := \begin{pmatrix} 1 & \dots & 1 & \dots \\ 0 & \dots & x & \dots \\ F(0) & \dots & F(x) & \dots \end{pmatrix}$$

M_F is the generator matrix of a linear binary code C_F of length 2^m.

Carlet, Charpin and Zinoviev (1998)

F is APN if and only if C_F has strength 5 ($C_F^\perp$ has distance 6).
C_F has dimension $2m + 1$.

An APN function is equivalent to a binary linear of length 2^m C which

- has strength 5 (i.e. $C^\perp$ has distance 6) and
- contains the first order Reed-Muller Code.

APN Functions as (Error Correcting) Codes

$$M_F := \begin{pmatrix} 1 & \dots & 1 & \dots \\ 0 & \dots & x & \dots \\ F(0) & \dots & F(x) & \dots \end{pmatrix}$$

M_F is the generator matrix of a linear binary code C_F of length 2^m.

Carlet, Charpin and Zinoviev (1998)

F is APN if and only if C_F has strength 5 ($C_F^\perp$ has distance 6). C_F has dimension $2m + 1$.

An APN function is equivalent to a binary linear of length 2^m C which

- has strength 5 (i.e. $C^\perp$ has distance 6) and
- contains the first order Reed-Muller Code.

CCZ Equivalence (Code Equivalence)

We call two APN functions $F, F' : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$ CCZ equivalent if there exists a invertible linear map $L : \mathbb{F}_2^{2m+1} \mapsto \mathbb{F}_2^{2m+1}$ such that

$$\left\{ \begin{pmatrix} 1 \\ x \\ F'(x) \end{pmatrix} \right\} = \left\{ L \begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix} \right\}$$

EA equivalent functions are also CCZ equivalent.

For APN functions, CCZ equivalence is stronger than EA equivalence.

For PN functions, CCZ equivalent functions are also EA equivalent (Kyureghyan, Pott 2008).

CCZ Equivalence (Code Equivalence)

We call two APN functions $F, F' : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$ CCZ equivalent if there exists a invertible linear map $L : \mathbb{F}_2^{2m+1} \mapsto \mathbb{F}_2^{2m+1}$ such that

$$\left\{ \begin{pmatrix} 1 \\ x \\ F'(x) \end{pmatrix} \right\} = \left\{ L \begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix} \right\}$$

EA equivalent functions are also CCZ equivalent.

For APN functions, CCZ equivalence is stronger than EA equivalence.

For PN functions, CCZ equivalent functions are also EA equivalent (Kyureghyan, Pott 2008).

Bijective APN

Problem

Is there an APN $F : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$, m even, that is a permutation?

Dillon Wolfe (2009)

There is an APN permutation for $m = 6$.

Dillon Wolfe (2009)

An APN permutation is equivalent to a binary linear code of strength 5, ..., containing a complementary pair of simplex codes.

There exists **no** APN permutation, different from the Dillon-Wolfe example, equivalent to any APN (I know) for $m \leq 12$, even!

Bijective APN

Problem

Is there an APN $F : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$, m even, that is a permutation?

Dillon Wolfe (2009)

There is an APN permutation for $m = 6$.

Dillon Wolfe (2009)

An APN permutation is equivalent to a binary linear code of strength 5, ..., containing a complementary pair of simplex codes.

There exists **no** APN permutation, different from the Dillon-Wolfe example, equivalent to any APN (I know) for $m \leq 12$, even!

Bijective APN

Problem

Is there an APN $F : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$, m even, that is a permutation?

Dillon Wolfe (2009)

There is an APN permutation for $m = 6$.

Dillon Wolfe (2009)

An APN permutation is equivalent to a binary linear code of strength 5, ..., containing a complementary pair of simplex codes.

There exists **no** APN permutation, different from the Dillon-Wolfe example, equivalent to any APN (I know) for $m \leq 12$, even!

Bijective APN

Problem

Is there an APN $F : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$, m even, that is a permutation?

Dillon Wolfe (2009)

There is an APN permutation for $m = 6$.

Dillon Wolfe (2009)

An APN permutation is equivalent to a binary linear code of strength 5, ..., containing a complementary pair of simplex codes.

There exists **no** APN permutation, different from the Dillon-Wolfe example, equivalent to any APN (I know) for $m \leq 12$, even!

Bijective APN

The new APN-Permutation Problem

Is there an APN $F : \mathbb{F}_2^m \mapsto \mathbb{F}_2^m$, m even, that is a permutation, different from the Dillon-Wolfe example?

Switching

Problem

Let $F : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a quadratic APN and $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a boolean function.
When is $F + f$ again a quadratic APN?

Dillon (2006) found many new quadratic APN for $m = 6, 7, 8$.

The series: $x^3 + tr(x^9)$ (Budaghyan, Carlet, Leander 2007/2009)

Switching

Problem

Let $F : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ be an APN function, and $f : \mathbb{F}_2^m \longrightarrow U$, U a l-dimensional subspace of $\mathbb{F}_2^m$.

When is $F + f$ again an APN function?

Theorem (1-dimensional) **E., Pott (2009)**

Let $F : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ be APN, $u \in \mathbb{F}_2^m \setminus \mathbf{0}$, and let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ be a boolean function. Then $F(v) + f(v) \cdot u$ is APN if and only if

$$f(x) + f(x + a) + f(y) + f(y + a) = 0$$

for all $x, y, a \in \mathbb{F}_2^m$ with

$$F(x) + F(x + a) + F(y) + F(y + a) = u. \tag{1}$$

Switching

Problem

Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be an APN function, and $f : \mathbb{F}_2^m \to U$, U a l-dimensional subspace of $\mathbb{F}_2^m$.

When is $F + f$ again an APN function?

Theorem (1-dimensional) **E., Pott (2009)**

Let $F : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be APN, $u \in \mathbb{F}_2^m \setminus \mathbf{0}$, and let $f : \mathbb{F}_2^m \to \mathbb{F}_2$ be a boolean function. Then $F(v) + f(v) \cdot u$ is APN if and only if

$$f(x) + f(x + a) + f(y) + f(y + a) = 0$$

for all $x, y, a \in \mathbb{F}_2^m$ with

$$F(x) + F(x + a) + F(y) + F(y + a) = u. \tag{1}$$

Switching

Let $S \subset \mathbb{F}_2^{2^m}$ be the vector space generated by the indicator functions of the 4-tuples $x, y, x + a, y + a$ satisfying condition (**??**).

Theorem: $F(x) + f(x) \cdot u$ is APN if and only if $f \in S^{\perp}$

Write $\mathbb{F}_2^m = u\mathbb{F}_2 \oplus V$

Let $D \subset C_F$ the $2m$-dimensional vector space spanned by the matrix

$$\left((1, x, F(x)|_V)^t : x \in \mathbb{F}_2^m\right)$$

If $f, g \in S^{\perp}$ are in the same coset of D, then $F(x) + f(x)u$ and $F(x) + g(x)u$ are EA equivalent.

In particular: If $S^{\perp}$ has dimension $2m$, then there is no candidate for a non trivial "switching function" $f(x) \cdot u$.

Switching

Let $S \subset \mathbb{F}_2^{2^m}$ be the vector space generated by the indicator functions of the 4-tuples $x, y, x+a, y+a$ satisfying condition (**??**).

Theorem: $F(x) + f(x) \cdot u$ is APN if and only if $f \in S^{\perp}$

Write $\mathbb{F}_2^m = u\mathbb{F}_2 \oplus V$

Let $D \subset C_F$ the $2m$-dimensional vector space spanned by the matrix

$$\left((1, x, F(x)|_V)^t \,:\, x \in \mathbb{F}_2^m\right)$$

If $f, g \in S^{\perp}$ are in the same coset of D, then $F(x) + f(x)u$ and $F(x) + g(x)u$ are EA equivalent.

In particular: If $S^{\perp}$ has dimension $2m$, then there is no candidate for a non trivial "switching function" $f(x) \cdot u$.

Switching

Let $S \subset \mathbb{F}_2^{2^m}$ be the vector space generated by the indicator functions of the 4-tuples $x, y, x+a, y+a$ satisfying condition (**??**).

Theorem: $F(x) + f(x) \cdot u$ is APN if and only if $f \in S^{\perp}$

Write $\mathbb{F}_2^m = u\mathbb{F}_2 \oplus V$

Let $D \subset C_F$ the $2m$-dimensional vector space spanned by the matrix

$$\left((1, x, F(x)|_V)^t \,:\, x \in \mathbb{F}_2^m\right)$$

If $f, g \in S^{\perp}$ are in the same coset of D, then $F(x) + f(x)u$ and $F(x) + g(x)u$ are EA equivalent.

In particular: If $S^{\perp}$ has dimension $2m$, then there is no candidate for a non trivial "switching function" $f(x) \cdot u$.

Switching

Theorem E., Pott (2009)

The function $F : \mathbb{F}_{2^6} \longrightarrow \mathbb{F}_{2^6}$ with

$$\begin{aligned} F(x) &= x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \\ &\quad u^{14}(tr(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + \\ &\quad tr_{8/2}((u^2x)^9) + tr_{4/2}(x^{21})) \end{aligned}$$

is an APN function.
The function cannot be CCZ equivalent to any crooked function.
Moreover, it is CCZ inequivalent to any power mapping.
($tr_{8/2}$ and $tr_{4/2}$ denote the relative trace $\mathbb{F}_8 \longrightarrow \mathbb{F}_2$ and $\mathbb{F}_4 \longrightarrow \mathbb{F}_2$)

Switching produces several further new APN functions for $m = 7, 8, 9$.

Switching

Theorem **E., Pott (2009)**

The function $F : \mathbb{F}_{2^6} \longrightarrow \mathbb{F}_{2^6}$ with

$$\begin{aligned} F(x) &= x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \\ &\quad u^{14}(tr(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + \\ &\quad tr_{8/2}((u^2x)^9) + tr_{4/2}(x^{21})) \end{aligned}$$

is an APN function.
The function cannot be CCZ equivalent to any crooked function.
Moreover, it is CCZ inequivalent to any power mapping.
($tr_{8/2}$ and $tr_{4/2}$ denote the relative trace $\mathbb{F}_8 \longrightarrow \mathbb{F}_2$ and $\mathbb{F}_4 \longrightarrow \mathbb{F}_2$)

Switching produces several further new APN functions for $m = 7, 8, 9$.

Incidence Structures

An incidence structure is an triple $(\mathcal{B}, \mathcal{P}, \mathcal{I})$.

The elements of the set $\mathcal{B}$ are called the blocks (or lines).

The elements of the set $\mathcal{P}$ are called the points.

$\mathcal{I} \subseteq \mathcal{B} \times \mathcal{P}$. A block B an a point P are called incident if $(B, P) \in \mathcal{I}$.

Often we give a block by $B := \{P \in \mathcal{P} | (B, P) \in \mathcal{I}\}$.

$(\mathcal{B}, \mathcal{P}, \mathcal{I})$ and $(\mathcal{B}', \mathcal{P}', \mathcal{I}')$ are called isomorpic if there is a bijection $\mathcal{B} \times \mathcal{P} \to \mathcal{B}' \times \mathcal{P}'$, such that $(B, P) \in \mathcal{I} \Leftrightarrow \pi(B, P) \in \mathcal{I}'$

PN Functions and Projective Planes

The graph of F is:

$$G_F := \{(x, F(x)) | x \in \mathbb{F}_p^m\} \subset \mathbb{F}_p^m \times \mathbb{F}_p^m$$

The incidence structure Γ_F with point set $\mathbb{F}_p^m \times \mathbb{F}_p^m$ and the p^{2m} blocks $\{B_{a,b} | a, b \in \mathbb{F}_p^m\}$ where

$$B_{a,b} := \{(x + a, F(x) + b) | x \in \mathbb{F}_p^m\}, B_{a,\infty} := \{(a, y) | y \in \mathbb{F}_p^m\}.$$

If F is a PN-function then

$$|B_{a,b} \cap B_{a',b'}| = \begin{cases} 0 & \text{if } a = a', b \neq b' \\ 1 & \text{if } a \neq a' \end{cases}$$

In $\Gamma_F \cup \{B_{a,\infty} | a \in \mathbb{F}_p^m\}$ every pair of disjoint points is on a unique block. This is an affine plane of order p^m.

PN Functions and Projective Planes

The graph of F is:

$$G_F := \{(x, F(x)) | x \in \mathbb{F}_p^m\} \subset \mathbb{F}_p^m \times \mathbb{F}_p^m$$

The incidence structure Γ_F with point set $\mathbb{F}_p^m \times \mathbb{F}_p^m$ and the p^{2m} blocks $\{B_{a,b} | a, b \in \mathbb{F}_p^m\}$ where

$$B_{a,b} := \{(x + a, F(x) + b) | x \in \mathbb{F}_p^m\}, B_{a,\infty} := \{(a, y) | y \in \mathbb{F}_p^m\}.$$

If F is a PN-function then

$$|B_{a,b} \cap B_{a',b'}| = \begin{cases} 0 & \text{if} \quad a = a', b \neq b' \\ 1 & \text{if} \quad a \neq a' \end{cases}$$

In $\Gamma_F \cup \{B_{a,\infty} | a \in \mathbb{F}_p^m\}$ every pair of disjoint points is on a unique block. This is an affine plane of order p^m.

APN Functions and Semibiplanes

An incidence structure with v points, v blocks in which each block contains k points, is called a (v, k)-semibiplane if

- any pair of points is joined by 0 or 2 blocks and
- any pair of blocks meet in 0 or 2 points.

Coulter, Henderson (1999)

If F is APN then Γ_F is a $(2^{2m}, 2^m)$-semibiplane.

APN Functions and Semibiplanes

We call a semibiplane divisible if there is a partition of the points in k classes P_i with $|P_i| = n$, such that

$$\#\text{blocks through } p, q = \begin{cases} 0 & \text{if } p, q \text{ are in the same } P_i \\ 0 \text{ or } 2 & \text{if } p, q \text{ are in different } P_i \end{cases}$$

A incidence structure admits a Singergroup if there is a group of automorphisms acting regular on both, blocks and points.

Pott (2007)

There exists an APN function $F : H \to N$ if and only if there exists a divisible semibiplane with a Singergroup $G = N \times H$ where $|N| = |H|$ and where N acts regularly on the point classes P_i.

Yet Another Equivalence

PN-functions are said to be isotopic if the corresponding planes are isomorphic.

Definition E., Pott

We say that two APN functions are isomorphic if the corresponding semibiplanes are isomorphic.

CCZ equivalent APN functions are isomorphic.

DO-PN Functions, Semifields, Spreads

$F \in \mathbb{F}_{p^m}[X]$ is called a Dembowski-Ostrom (DO) polynomial if

$$F(X) = \sum_{i,j} a_{i,j} X^{p^i + p^j}$$

$$x \circ y := F(x+y) - F(x) - F(y) + F(0)$$

Let F be a DO-PN then $(\mathbb{F}_p^m, +, \circ)$ is a commutative pre-semifield.

$$\mathcal{V} := \{V_a | a \in \mathbb{F}_p^m\} \cup V_\infty, \text{ with}$$

$$V_a := \{(x, x \circ a) | x \in \mathbb{F}_p^m\}, V_\infty := \{(0, y) | y \in \mathbb{F}_p^m\}$$

$\mathcal{V}$ is a partition of the space $\mathbb{F}_p^{2m}$ in subspaces, so $\mathcal{V}$ is a spread.

The cosets a spread form the blocks of a translation plane.

Any DO-PN function gives rise to a translation plane.

DO-PN Functions, Semifields, Spreads

$F \in \mathbb{F}_{p^m}[X]$ is called a Dembowski-Ostrom (DO) polynomial if

$$F(X) = \sum_{i,j} a_{i,j} X^{p^i + p^j}$$

$$x \circ y := F(x+y) - F(x) - F(y) + F(0)$$

Let F be a DO-PN then $(\mathbb{F}_p^m, +, \circ)$ is a commutative pre-semifield.

$$\mathcal{V} := \{V_a | a \in \mathbb{F}_p^m\} \cup V_\infty, \text{ with}$$

$$V_a := \{(x, x \circ a) | x \in \mathbb{F}_p^m\}, V_\infty := \{(0, y) | y \in \mathbb{F}_p^m\}$$

$\mathcal{V}$ is a partition of the space $\mathbb{F}_p^{2m}$ in subspaces, so $\mathcal{V}$ is a spread.

The cosets a spread form the blocks of a translation plane.

Any DO-PN function gives rise to a translation plane.

DO-PN Functions, Semifields, Spreads

$F \in \mathbb{F}_{p^m}[X]$ is called a Dembowski-Ostrom (DO) polynomial if

$$F(X) = \sum_{i,j} a_{i,j} X^{p^i + p^j}$$

$$x \circ y := F(x+y) - F(x) - F(y) + F(0)$$

Let F be a DO-PN then $(\mathbb{F}_p^m, +, \circ)$ is a commutative pre-semifield.

$$\mathcal{V} := \{V_a | a \in \mathbb{F}_p^m\} \cup V_\infty, \text{ with}$$

$$V_a := \{(x, x \circ a) | x \in \mathbb{F}_p^m\}, V_\infty := \{(0, y) | y \in \mathbb{F}_p^m\}$$

$\mathcal{V}$ is a partition of the space $\mathbb{F}_p^{2m}$ in subspaces, so $\mathcal{V}$ is a spread.

The cosets a spread form the blocks of a translation plane.

Any DO-PN function gives rise to a translation plane.

Quadratic APN-Functions, Dual Hyperovals

Let F be a APN function.

$$x \circ y := F(x+y) - F(x) - F(y) + F(0)$$

$$\mathcal{V}_F := \{V_a | a \in \mathbb{F}_2^m\} \text{ with } V_a := \{(x, x \circ a) | x \in \mathbb{F}_2^m\}$$

For any $V \neq V' \in \mathcal{V}_F$ is $V \cap V'$ is 1-dimensional.
Any three mutually different $V_i \in \mathcal{V}_F$ intersect only in zero.

The blocks
$B_{a,b} := \{(x, y+b) | (x,y) \in V_a\} = \{(x, x \circ a + b) | x \in \mathbb{F}_2^m\}$
form an semibiplane.

F is quadratic iff

$$F(X) = \sum_{i,j} a_{i,j} X^{2^i+2^j}$$

If F is an quadratic APN $\mathcal{V}_F$ then is a dual hyperoval.

Quadratic APN-Functions, Dual Hyperovals

Let F be a APN function.

$$x \circ y := F(x+y) - F(x) - F(y) + F(0)$$

$$\mathcal{V}_F := \{V_a | a \in \mathbb{F}_2^m\} \text{ with } V_a := \{(x, x \circ a) | x \in \mathbb{F}_2^m\}$$

For any $V \neq V' \in \mathcal{V}_F$ is $V \cap V'$ is 1-dimensional.
Any three mutually different $V_i \in \mathcal{V}_F$ intersect only in zero.

The blocks
$B_{a,b} := \{(x, y+b) | (x,y) \in V_a\} = \{(x, x \circ a + b) | x \in \mathbb{F}_2^m\}$
form an semibiplane.

F is quadratic iff

$$F(X) = \sum_{i,j} a_{i,j} X^{2^i + 2^j}$$

If F is an quadratic APN $\mathcal{V}_F$ then is a dual hyperoval.

Quadratic APN Functions, Dual Hyperovals

Pott 2007

The semibiplane defined via the graph of F and the semibiplane defined via the "dual hyperoval" of F are isomorphic.

Yoshiara 2008

One of the new quadratic APN functions lead to a unknown example of dual hyperovals.

Quadratic APN Functions, Dual Hyperovals

For disj. $V, V', V'' \in \mathcal{V}$ let $l'' = V \cap V'$, $l = V' \cap V''$, $l' = V'' \cap V$.

Define $p(V, V', V'') := \langle l, l', l'' \rangle \setminus (\langle l, l' \rangle \cup \langle l', l'' \rangle \cup \langle l'', l \rangle)$.

E. 2009

- Let $\mathcal{V}$ be a dual hyperoval. There exists a quadratic APN function F such that $\mathcal{V}_F \sim \mathcal{V}$ if and only if the space $\langle p(V, V', V'') | V, V', V'' \in \mathcal{V} \rangle$ is disjoint from any $V \in \mathcal{V}$.
- There is a 1-to-1 correspondence between the EA-equivalence classes of quadratic APN functions and the isomorphy classes of such dual hyperovals.
- Given an dual hyperoval $\mathcal{V}$ fulfilling the above property, we can effectively construct an F such that $\mathcal{V}_F$ is isomorphic to the dual hyperoval $\mathcal{V}$.

Quadratic APN Functions, Dual Hyperovals

For disj. $V, V', V'' \in \mathcal{V}$ let $I'' = V \cap V'$, $I = V' \cap V''$, $I' = V'' \cap V$.

Define $p(V, V', V'') := \langle I, I', I'' \rangle \setminus (\langle I, I' \rangle \cup \langle I', I'' \rangle \cup \langle I'', I \rangle)$.

E. 2009

- Let $\mathcal{V}$ be a dual hyperoval. There exists a quadratic APN function F such that $\mathcal{V}_F \sim \mathcal{V}$ if and only if the space $\langle p(V, V', V'') | V, V', V'' \in \mathcal{V} \rangle$ is disjoint from any $V \in \mathcal{V}$.
- There is a 1-to-1 correspondence between the EA-equivalence classes of quadratic APN functions and the isomorphy classes of such dual hyperovals.
- Given an dual hyperoval $\mathcal{V}$ fulfilling the above property, we can effectively construct an F such that $\mathcal{V}_F$ is isomorphic to the dual hyperoval $\mathcal{V}$.

Quadratic APN Functions, Dual Hyperovals

For disj. $V, V', V'' \in \mathcal{V}$ let $l'' = V \cap V'$, $l = V' \cap V''$, $l' = V'' \cap V$.

Define $p(V, V', V'') := \langle l, l', l'' \rangle \setminus (\langle l, l' \rangle \cup \langle l', l'' \rangle \cup \langle l'', l \rangle)$.

E. 2009

- Let $\mathcal{V}$ be a dual hyperoval. There exists a quadratic APN function F such that $\mathcal{V}_F \sim \mathcal{V}$ if and only if the space $\langle p(V, V', V'') | V, V', V'' \in \mathcal{V} \rangle$ is disjoint from any $V \in \mathcal{V}$.
- There is a 1-to-1 correspondence between the EA-equivalence classes of quadratic APN functions and the isomorphy classes of such dual hyperovals.
- Given an dual hyperoval $\mathcal{V}$ fulfilling the above property, we can effectively construct an F such that $\mathcal{V}_F$ is isomorphic to the dual hyperoval $\mathcal{V}$.

Quadratic APN Functions, Dual Hyperovals

For disj. $V, V', V'' \in \mathcal{V}$ let $I'' = V \cap V'$, $I = V' \cap V''$, $I' = V'' \cap V$.

Define $p(V, V', V'') := \langle I, I', I'' \rangle \setminus (\langle I, I' \rangle \cup \langle I', I'' \rangle \cup \langle I'', I \rangle)$.

E. 2009

- Let $\mathcal{V}$ be a dual hyperoval. There exists a quadratic APN function F such that $\mathcal{V}_F \sim \mathcal{V}$ if and only if the space $\langle p(V, V', V'') | V, V', V'' \in \mathcal{V} \rangle$ is disjoint from any $V \in \mathcal{V}$.
- There is a 1-to-1 correspondence between the EA-equivalence classes of quadratic APN functions and the isomorphy classes of such dual hyperovals.
- Given an dual hyperoval $\mathcal{V}$ fulfilling the above property, we can effectively construct an F such that $\mathcal{V}_F$ is isomorphic to the dual hyperoval $\mathcal{V}$.

Quadratic APN Functions, Dual Hyperovals

Problem: If there are two quadratic APN functions which are CCZ-equivalent, but not EA-equivalent, how does this translate in the geometric approach?

Observation: For all quadratic APN, $m \leq 9$ (I know), this does not happen.

Conjecture: There is only one EA class of quadratic APN in the CCZ-equivalence class of any quadratic APN.
And the CCZ-automorphism group of an quadratic APN equals the EA-automorphism group .

McGuire et al. (2009)

This conjecture is true for the Gold APN-functions.

Quadratic APN Functions, Dual Hyperovals

Problem: If there are two quadratic APN functions which are CCZ-equivalent, but not EA-equivalent, how does this translate in the geometric approach?

Observation: For all quadratic APN, $m \leq 9$ (I know), this does not happen.

Conjecture: There is only one EA class of quadratic APN in the CCZ-equivalence class of any quadratic APN.
And the CCZ-automorphism group of an quadratic APN equals the EA-automorphism group .

McGuire et al. (2009)

This conjecture is true for the Gold APN-functions.

Knuth's Operation

If the PN (APN) function F is DO (quadratic) then
$\circ : \mathbb{F}_p^m \times \mathbb{F}_p^m \to \mathbb{F}_p^m \qquad x \circ y := F(x+y) - F(x) - F(y) - F(0)$

is a bilinear function, hence determined by its values on a basis.

$$e_i \circ e_j := \sum_k K_{i,j,k} e_k$$

Knuth (1965)

- Let F be DO. F is PN if and only if any nontrivial linear combination of the m matrices $K_{i,j,k}$, $j = 1..m$, has full rank.
- If $K_{i,j,k}$ has this property, then any cube arising from it by permuting the indices has also this rank property.
- A cube with this rank property yields a spread. The corresponding planes are in general not isomorphic.

Knuth's Operation

If the PN (APN) function F is DO (quadratic) then
$\circ : \mathbb{F}_p^m \times \mathbb{F}_p^m \to \mathbb{F}_p^m \qquad x \circ y := F(x+y) - F(x) - F(y) - F(0)$

is a bilinear function, hence determined by its values on a basis.

$$e_i \circ e_j := \sum_k K_{i,j,k} e_k$$

Knuth (1965)

- Let F be DO. F is PN if and only if any nontrivial linear combination of the m matrices $K_{i,j,k}$, $j = 1..m$, has full rank.
- If $K_{i,j,k}$ has this property, then any cube arising from it by permuting the indices has also this rank property.
- A cube with this rank property yields a spread. The corresponding planes are in general not isomorphic.

Knuth's Operation

E.

F is a quadratic APN iff

- any nontrivial linear combination of the m matrices $K_{i,j,k}$, $j = 1..m$, has rank $m-1$, and
- the m matrices $K_{i,j,k}$, $k = 1..m$, are symplectic.

A cube with this rank property yields a dual hyperoval.
If the permuted cube fulfills the rank condition, then the corresponding semibiplanes are in general not isomorphic.

Corollary: For even m no permutation of the indices of $K_{i,j,k}$, moving k, eads to a cube of a quadratic APN .

Remark 1: For odd $m \leq 9$ all cubes of a quadratic APN (I know) fulfill the rank condition in every direction.

Remark 2: For odd $m = 5, 7$ all permuted cubes of a quadratic APN, can not be again "quadratic APN cubes".

Knuth's Operation

E.

F is a quadratic APN iff

- any nontrivial linear combination of the m matrices $K_{i,j,k}$, $j = 1..m$, has rank $m-1$, and
- the m matrices $K_{i,j,k}$, $k = 1..m$, are symplectic.

A cube with this rank property yields a dual hyperoval.
If the permuted cube fulfills the rank condition, then the corresponding semibiplanes are in general not isomorphic.

Corollary: For even m no permutation of the indices of $K_{i,j,k}$, moving k, eads to a cube of a quadratic APN .

Remark 1: For odd $m \leq 9$ all cubes of a quadratic APN (I know) fulfill the rank condition in every direction.

Remark 2: For odd $m = 5, 7$ all permuted cubes of a quadratic APN, can not be again "quadratic APN cubes".

Designs and Invariants

The semibiplane Γ_F of an APN function F can also be considered as a design.

An invariant of a design is a property that is in common to all isomorphic designs.

Two APN functions F, F' which disagree in one invariant of their designs $\Gamma_F, \Gamma_{F'}$ are not isomorphic (CZZ-equivalent, ...)

Invariants can give information about the APN, of the type: "There is no F' isomorphic to F having the property..."

Example: There is no quadratic APN F' which is isomorphic to F.

Designs and Invariants

The semibiplane Γ_F of an APN function F can also be considered as a design.

An invariant of a design is a property that is in common to all isomorphic designs.

Two APN functions F, F' which disagree in one invariant of their designs $\Gamma_F, \Gamma_{F'}$ are not isomorphic (CZZ-equivalent, ...)

Invariants can give information about the APN, of the type: "There is no F' isomorphic to F having the property..."

Example: There is no quadratic APN F' which is isomorphic to F.

The Design Δ_F

Let F be an APN function and M be the incidence matrix of Γ_F.

$$M \cdot M^t = 2^m I + 2N$$

Define Δ_F as the design with incidence matrix N.

Invariants of Δ_F are also invariants of Γ_F.

Δ_F is orbit of the block $\{(a, F(x+a) - F(x)) | x, a \in \mathbb{F}_2^m, a \neq 0\}$ under the action of $\mathbb{F}_2^m \times \mathbb{F}_2^m$.

The Design Δ_F

Let F be an APN function and M be the incidence matrix of Γ_F.

$$M \cdot M^t = 2^m I + 2N$$

Define Δ_F as the design with incidence matrix N.

Invariants of Δ_F are also invariants of Γ_F.

Δ_F is orbit of the block $\{(a, F(x+a) - F(x)) | x, a \in \mathbb{F}_2^m, a \neq 0\}$ under the action of $\mathbb{F}_2^m \times \mathbb{F}_2^m$.

The Design Δ_F

E. P.

For all CCZ inequivalent APN functions with $m \leq 9$ (known to us), the designs Δ_F not isomorphic

Hence the CCZ equivalence classes of these APN functions are also their isomorphy classes.

Question: is the APN function already determined by its design Δ_F?

Invariants

Some Design Invariants:

- The rank of the incidence matrix of of the design Γ_F (Δ_F) over various fields.
- The Smith normal form of the Incidence matrix of Γ_F (Δ_F)
- The automorphism group of the design Γ_F (Δ_F)

Some CCZ Invariants:

- The Walsh spectrum.
- The automorphism group of the Code C_F.

An EA Invariant:

- The algebraic degree of F

Invariants

Some Design Invariants:

- The rank of the incidence matrix of of the design Γ_F (Δ_F) over various fields.
- The Smith normal form of the Incidence matrix of Γ_F (Δ_F)
- The automorphism group of the design Γ_F (Δ_F)

Some CCZ Invariants:

- The Walsh spectrum.
- The automorphism group of the Code C_F.

An EA Invariant:

- The algebraic degree of F

Invariants

Some Design Invariants:

- The rank of the incidence matrix of of the design Γ_F (Δ_F) over various fields.
- The Smith normal form of the Incidence matrix of Γ_F (Δ_F)
- The automorphism group of the design Γ_F (Δ_F)

Some CCZ Invariants:

- The Walsh spectrum.
- The automorphism group of the Code C_F.

An EA Invariant:

- The algebraic degree of F

Relations of the Automorphism Groups

$$
\begin{array}{ccc}
\text{EA-Aut} & & \\
\mid\cap & & \\
\text{code group } \mathrm{Aut}(C_F) & & \\
\| & & \\
\text{multiplier group}(\Gamma_F) & \subseteq & \text{multiplier group}(\Delta_F) \\
\cap & & \cap \\
\text{design group } \mathrm{Aut}(\Gamma_F) & \subseteq & \text{design group } \mathrm{Aut}(\Delta_F))
\end{array}
$$

Properties and Invariants

If the CCZ-equivalence class of F contains
- a monomial APN function, then $C_{2^m-1} \subseteq \mathrm{Aut}(C_F)$
- a quadratic APN function, then $E_{2^m} \subseteq \mathrm{Aut}(C_F)$
- an APN function $\in \mathbb{F}_2[X]$, then $C_m \subseteq \mathrm{Aut}(C_F)$

If the isomorphy class of F contains
- a monomial APN function, then $E_{2^{2m}} \times C_{2^m-1} \subseteq \mathrm{Aut}(\Gamma_F)$
- a quadratic APN function, then $E_{2^{3m}} \subseteq \mathrm{Aut}(\Gamma_F)$
- an APN function $\in \mathbb{F}_2[X]$, then $E_{2^{2m}} \times C_m \subseteq \mathrm{Aut}(\Gamma_F)$

Properties and Invariants

An APN function F is called crooked if

$$\mathcal{V}_a = \{x \circ a | x \in \mathbb{F}_{2^m}\} = \{F(x+a) - F(x) - F(a) - F(0) | x \in \mathbb{F}_{2^m}\}$$

is a subspace for all a.

Any quadratic APN is crooked.

E.P.

If the isomorphy class of F contains a crooked APN function then the $\mathbb{F}_2$-rank of the incidence matrix of Δ_F is at most 2^{m+1}.

Properties and Invariants

An APN function F is called crooked if

$$\mathcal{V}_a = \{x \circ a | x \in \mathbb{F}_{2^m}\} = \{F(x+a) - F(x) - F(a) - F(0) | x \in \mathbb{F}_{2^m}\}$$

is a subspace for all a.

Any quadratic APN is crooked.

E.P.

If the isomorphy class of F contains a crooked APN function then the $\mathbb{F}_2$-rank of the incidence matrix of Δ_F is at most 2^{m+1}.

Conclusion

There are different points of view on APN functions.

Not only cryprography profits from progress in APN functions.

Conclusion

There are different points of view on APN functions.

Not only cryprography profits from progress in APN functions.

The end.