Shanghai Jiao Tong University
School of Electronic Information and Electrical Engineering

APN functions

Zhaole Li

Workshop of APN function, 2022

Differential attack

The differential attack, introduced by Biham and Shamir, is a chosen plaintext attack for block ciphers in general.
Define the block m of plaintext and c and c' being the ciphertexts related to m and $m+\alpha$, the bitwise difference $c+c'$ has a larger probability to equal β than if c and c' are randomly chosen binary sequences.

Differential uniformity is specific for S-boxes in block ciphers and is as important as nonlinearity of Boolean functions.

Definition (Differential uniformity)

Let n, m, δ be positive integers. An (n, m) function F is called differentially δ-uniform if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x + a) = b$ has at most δ solutions. The minimum of those values δ having such property, that is, the maximum number of solutions of such equations, is denoted by δ_F and called the differential uniformity of F.

$$\delta_F = \max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^m} \left| \{x \in \mathbb{F}_2^n \mid D_a F(x) = F(x) + F(x + a) = b\} \right| .$$

Differential uniformity of some S-boxes

Example

S-box of AES: 4
S-box of PRESENT: 4
S-box5 of DES: 16

- The differential uniformity δ_F is even since the solutions of equation $F(x) + F(x+a) = b$ come out by pairs: if x is the solution, then $x + a$ is also a solution.
- Lower differential uniformity means better resistance to the differential attack
- The low bound of differential uniformity δ_F of any (n, m) function F is 2^{n-m}
- The differential uniformity equals 2^{n-m} if and only if every derivative $D_aF, a \neq 0$, is balanced, and we say F is perfect nonlinear

When n is odd or $m > n/2$, the (n, m) function f has differential uniformity strict larger than 2^{n-m}.

Definition (Almost Perfect Nonlinear functions)

An (n, n) function F is called almost perfect nonlinear (APN) if it is differentially 2-uniform, implies that for all $a \in \mathbb{F}_2^{n*}$ and $b \in \mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ has 0 or 2 solutions.

- An (n,m) function is bent if and only if all its derivatives $D_aF(x), a \in \mathbb{F}_2^{n*}$ are balanced which means bent and perfect nonlinear conincide.
- Almost Bent functions exist only for odd n but APN functions exist for all integers.
- if $n=m$ and F is a permutation, then F and its inverse F^{-1} have the same differential uniformity.

1. affine equivalent
2. extended affine(EA) equivalent
3. Carlet–Charpin–Zinoviev(CCZ) equivalent

Affine equivalent

Definition (Affine automorphism)

We call L is an $\mathbb{F}_2$ linear automorphism of $\mathbb{F}_2^n$ if

$$L : \mathbb{F}_2^n \to \mathbb{F}_2^m$$
$$(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, \ldots, x_n) \times M.$$

M being a nonsingular $n \times n$ binary matrix.

Affine equivalent

Definition

Two (n, m) functions F and $L' \circ F \circ L$, where

$$L : \mathbb{F}_2^n \to \mathbb{F}_2^m$$
$$(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, ..., x_n) \times M + (a_1, a_2, \ldots, a_n).$$

is an affine automorphism of $\mathbb{F}_2^n$ and L' is an affine automorphism of $\mathbb{F}_2^m$ are called affine equivalent, where M is a nonsingular $n \times n$ matrix over $\mathbb{F}_2$ and L' is an $\mathbb{F}_2$-linear automorphism of F_2^m.

EA equivalent

Definition

Two (n, m) functions F and $L' \circ F \circ L + L''$, where L is an affine automorphism of $\mathbb{F}_2^n$, L' is an affine automorphism of $\mathbb{F}_2^m$, and

$$\begin{aligned} L'' : \mathbb{F}_2^n &\to \mathbb{F}_2^m \\ (x_1, x_2, \ldots, x_n) &\mapsto (x_1, x_2, \ldots, x_n) \times M + (a_1, a_2, \ldots, a_m). \end{aligned}$$

is an affine (n, m)-function, M being an $n \times m$ binary matrix, are called (extended affine) EA equivalent.

CCZ equivalent

Definition

Two (n, m) functions F and G whose graphs $\mathcal{G}_F = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m \mid y = F(x)\}$ and $\mathcal{G}_G = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m \mid y = G(x)\}$ are affinely equivalent, are called Carlet–Charpin–Zinoviev (CCZ) equivalent.

The facts are that EA equivalence implies CCZ equivalence which is not obvious and the converse is not true.

CCZ equivalent

Proof.

If $G = \phi_2 \circ F \circ \phi_1$ and ϕ_1 and ϕ_2 are are affine automorphisms of $\mathbb{F}_2^n, \mathbb{F}_2^m$, then $L = (L_1, L_2)$ is an affine automorphism of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ that maps $\mathcal{G}_F$ onto $\mathcal{G}_G$, where $L_1(x, y) = \phi_1^{-1}(x)$ and $L_2(x, y) = \phi_2^(y)$ since $G(\phi_1^{-1}(x)) = \phi_2(F(x))$. If $\phi(x)$ is an affine function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ and $G(x) = F(x) + \phi(x)$, then $L(x, y) = (x, y + \phi(x))$ is an affine automorphism that maps $\mathcal{G}_F$ onto $\mathcal{G}_G$, and F and G are CCZ equivalent. But EA equivalence holds algebraic degree and CCZ equivalence does not: x^3 is CCZ equivalent to $(x + Trace(x^3))^3$ where $x \in \mathbb{F}_{2^8}$, and the former is 2, the latter is 3. □

- CCZ equivalence preserves the differential uniformity of functions: In the graph $\mathcal{G}_F = \{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m \mid y = F(x)\}$ of the function F, the differential uniformity is the maxmial number of the solutions $(X,Y) \in \mathcal{G}_F \times \mathcal{G}_F$ such that $X + Y = (a,b)$ where $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^m$.
- CCZ equivalence preserves the nonlinearity of functions: Since $W_F(u,v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{uF(x)+vx}$ is the Fourier transform of $\mathcal{G}_F = \{(x,y) \in \mathbb{F}_2^n \times \mathbb{F}_2^m \mid y = F(x)\}$ and

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^{n*}, v \in \mathbb{F}_2^n} |W_F(u,v)|.$$

Note that $\max_{u \in \mathbb{F}_2^{n*}, v \in \mathbb{F}_2^n} |W_F(u,v)|$ is invariant under affine transformation.

CCZ inequivalent

Proving the CCZ inequivalence between two functions is extremely difficult, unless some CCZ invariants can be proved (and calculated) different for the two functions.

- The extended Walsh spectrum.
- The equivalence class of the code
- The Γ-rank
- The Δ-rank

Maybe a little amazing, APN functions often have high nonlinearity as well.

- AB functions are APN functions. But converse is not true.
- For n even, Gold, Kasami and inverse functions have the nonlinearity $2^{n-1} - 2^{n/2}$ while the best nonlinearity is $2^{n-1} - 2^{n/2-1}$.
- For n odd, Gold and Kasami are AB functions, inverse function also achieves the maximal even number bel $2^{n-1} - 2^{n/2}$.
- Dobbertin functions have low nonlinearity.

Several infinite families of APN functions

Shanghai Jiao Tong University

Denote a power function as a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto x^d$. It's mathmatically easy to study.

functions	Exponents d	Conditions	$w_2(d)$
Gold	$2^i + 1$	$\gcd(i, m) = 1$	2
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, m) = 1$	$i + 1$
Welch	$2^t + 3$	$m = 2t + 1$	3
Niho(odd)	$2^t + 2^{3t+1/2} - 1$	$m = 2t + 1$	$t + 1$
Niho(even)	$2^t + 2^{t/2} - 1$	$m = 2t + 1$	$(t + 2)/2$
Inverse	$2^{2t} - 1$	$m = 2t + 1$	$m - 1$
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$m = 5i$	$i + 3$

Table: Known APN power functions x^d on $\mathbb{F}_2^m$

Several infinite families of APN functions

- All APN monomials are bijective for odd n and non-bijective for even n.
- The inverse function $x \mapsto x^{2n-2}$ has been chosen for the S-boxes of the AES with $n = 8$ since its bijectivity, good nonlinearity, good differential uniformity, highest possible algebraic degree $n-1$ and simplicity for design.

APN function

- There exists no APN function CCZ inequivalent to power functions on $\mathbb{F}_2^n$ for $n \leq 5$.
- There exists APN functions EA inequivalent to power functions on $\mathbb{F}_2^n$.

By the minimum distance of related codes of the APN functions we have:
Let F be any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ such that $F(0)=0$. Let H be the matrix $\begin{bmatrix} 1 & \alpha & \cdots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & \cdots & F(\alpha^{2^n-2}) \end{bmatrix}$, where α is a primitive element of $\mathbb{F}_2^n$, Let C_F be the linear code admitting H for parity check matrix. Then F is APN if and only if C_F has minimum distance 5.

Code isomorphim

- Two (n,n) functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are CCZ equivalent if the extended codes with parity check matrices $\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & u & \cdots & u^{2^n-2} \\ F(0) & F(u) & \cdots & F(u^{2^n-2}) \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & u & \cdots & u^{2^n-2} \\ G(0) & G(u) & \cdots & G(u^{2^n-2}) \end{bmatrix}$ are equivalent.
- Thus we can transform the CCZ equivalent to the code isomorphim.

Find quadratic APN functions

Theorem

Let F and G be quadratic APN functions on $\mathbb{F}_2^n$ with $n \geq 2$. Then F is CCZ-equivalent to G if and only if F is EA-equivalent to G.

A Recursive Tree Search for Quadratic APN Functions

- Sbox is initialized to be undefined ($\perp$) at each entry, corresponding to the look-up table of the APN function F.
- If sbox has been completely defined, then it has found a APN function.
- If not, selects the next undefined entry x and sets $F(x)$ to a value y that is randomly selected from among a predefined list of possible choices.
- After adding a value y, checks whether F can be both APN and quadratic. If not, the current branch of the search tree is skipped and $F(x)$ is set to the next possible value y.
- Maybe it's long time in cases where no quadratic APN function is found, so we abort and restart after a predetermined time.

APN check

After setting $F(x)$ to a new value y, it need to check whether the APN property of F has been violated:
Recall that the DDT of a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as the $2n \times 2n$ integer matrix containing $|\{x \in \mathbb{F}_2^n \mid F(x) + F(x + \alpha) = \beta\}|$ at the position in row α and column β. After each entry of F is fixed, update the partial DDT according to the newly fixed entry and check whether, for any $\alpha \neq 0$, it contains values larger than 2.

Each time after setting $F(x)$ to a new value y, check whether we can deduce the existence of a monomial of algebraic degree higher than 2 in the algebraic normal form of F:
Looking for the sum for all a_u with $wt(u) \geq 3$, i.e.

$$a_I = \sum_{x \in \mathbb{F}_2^n \ x \leq u} F(x)$$

After finding a APN function, we need to check whether it is EA-equivalent to a known function. Note that for two quadratic APN functions, EA-equivalence coincides with CCZ-equivalence.

Ortho-Derivative

Definition (Ortho-Derivative)

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function. We say that $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an ortho-derivative for F if, $\forall x \in \mathbb{F}_2^n$

$$\pi_F(a) \cdot (F(x) + F(x+a) + F(0) + F(a)) = 0.$$

- if F is quadratic then $F(x) + F(x+a) + F(0) + F(a)$ is linear,
- $\pi_F(a)$ is orthogonal to the linear part of the hyperplane $Im(D_a F)$.
- $\pi_F(0)$ can take any value.

Since a quadratic function F is APN if and only if the sets $\{F(x) + F(x+a) + F(0) + F(a), x \in \mathbb{F}_2^n\}$ are hyperplanes for all nonzero $a \in \mathbb{F}_2^n$.

Lemma

F is APN if and only if $\pi_F(a)$ is uniquely defined for all $a \in \mathbb{F}_2^{n*}$ with $\pi_F(0) = 0$.

Lemma

For two EA-equivalent quadratic APN functions $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the ortho-derivatives π_F and π_G are linear-equivalent.

Testing two quadratic APN functions for EA-inequivalence (which is the same as CCZ-inequivalence in this case) is simple. One simply computes the corresponding ortho-derivatives and evaluates their extended Walsh spectra and differential spectra. This method is much more efficient than checking the code equivalence with Magma.

Shanghai Jiao Tong University

Thank You

Zhaole Li · APN functions