Shanghai Jiao Tong University | School of Electronic Information and Electrical Engineering

APN functions

Zhaole Li

Workshop of APN function, 2022

Section 1

Introduction

Vectorial Boolean functions

Given two positive integers n and m, a vectorial Boolean (n, m)-function, or simply (n, m)-function, is any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. When $m = 1$, we often call it n-variable Boolean function.

One can identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$.

For a given n-variable pseudo-Boolean function φ, which is a function from $\mathbb{F}_2^n$ to $\mathbb{R}$, the Fourier-Hadamard transform of φ defined on $\mathbb{F}_2^n$ by:

$$\hat{\varphi}(u) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{u \cdot x}, u \in \mathbb{F}_2^n,$$

where "$\cdot$" is the inner product in $\mathbb{F}_2^n$ such as $u \cdot x = \sum_{i=1}^n u_i x_i$.
For a given n-variable Boolean function f, set $\varphi = (-1)^f$, then we obtain the Walsh transform of f:

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + u \cdot x}, u \in \mathbb{F}_2^n.$$

The two transforms are related by $W_f(u) = 2^n \delta_0(u) - 2\hat{(f)}(u)$, where δ_0 is the Dirac symbol.

Parseval relation:

$$\sum_{u \in \mathbb{F}_2^n} W_f^2(u) = 2^{2n}.$$

Titsworth relation:

$$\sum_{u \in \mathbb{F}_2^n} W_f(u) W_f(u+v) = 0, v \neq 0.$$

The nonlinearity of a Boolean function f equals its minimal Hamming distance to affine Boolean functions $u \cdot x + \epsilon$, where $u \in \mathbb{F}_2^n, \epsilon \in \mathbb{F}_2$:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |W_f(u)|.$$

The nonlinearity of an (n, m)-function F equals the minimal nonlinearity of its component functions $v \cdot F$, where $v \in \mathbb{F}_2^m \setminus \{0_m\}$:

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{\substack{u \in \mathbb{F}_2^n \\ v \in \mathbb{F}_2^m, v \neq 0_m}} |W_F(u, v)|^1.$$

[1] The Walsh transform of an (n, m)-function is defined in terms of the Walsh transform of its component functions: $W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x}, v \neq 0$.

The differential attack, introduced by Biham and Shamir[2], is a chosen plaintext attack for block ciphers in general.

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. We denote the minimum of these integers δ by δ_F and call it the differential uniformity of F. For every (n,m)-function F, we have $\delta_F \geq \max(2, 2^{n-m})$.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4 (1), pp. 3–72, 1991.

We can have $\delta_F = 2$ only when $n \geq m$, and this case is specially defined for $n = m$:

Definition (APN functions)

An (n, n)-function F is called almost perfect nonlinear (APN) if it is differentially 2-uniform, i.e. if for every $a \in \mathbb{F}_2^n \setminus \{0_n\}$ and every $b \in \mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ has 0 or 2 solutions (i.e. the derivative $D_aF(x) = F(x) + F(x + a)$ is 2-to-1). Equivalently, $|D_aF(x), x \in \mathbb{F}_2^n| = 2^{n-1}$. In other words, for distinct elements $x, y, z, t \in \mathbb{F}_2^n$, the equality $x + y + z + t = 0_n$ implies $F(x) + F(y) + F(z) + F(t) \neq 0_n$.

Section 2

The distance between APN functions[3]

[3] Budaghyan L, Carlet C, Helleseth T, et al. On the distance between APN functions[J]. IEEE Transactions on Information Theory, 2020, 66(9): 5742-5753.

Given two functions $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the Hamming distance $d(F, G)$ is defined as the number of points $x \in \mathbb{F}_2^n$ which the values of $F(x)$ and $G(x)$ differ, i.e.

$$d(F, G) = |\{x \in \mathbb{F}_2^n : F(x) \neq G(x)\}|.$$

Hence, we consider the case of arbitrarily changing the values of K points, obviously the Hamming distance $d(F, G) = K$. In fact, given a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, K distinct elements $u_1, u_2, \ldots, u_K \in \mathbb{F}_2^n$ and the corresponding K elements $v_1, v_2, \ldots, v_K \in \mathbb{F}_2^n \setminus \{0_n\}$, we define G as

$$G(x) = \begin{cases} F(u_i) + v_i, x = u_i \\ F(x), x \notin \{u_1, u_2, \ldots, u_K\}. \end{cases}$$

The derivative of function G

We define the indicator function of a set S: $1_S(x) = \begin{cases} 1, & if\ x \in S \\ 0, & otherwise. \end{cases}$

Therefore the function G defining over F can be written as

$$G(x) = F(x) + \sum_{i=1}^{K} 1_{u_i}(x) v_i = F(x) + \sum_{i=1}^{K} (1 + (x + u_i)^{2^n - 1}) v_i.$$

So we can observe that for any $a \in \mathbb{F}_2^n \setminus \{0_n\}$, the derivative $D_a G$ takes the form

$$D_a G(x) = D_a F(x) + \sum_{i=1}^{K} 1_{u_i}(x) v_i = D_a F(x) + \sum_{i=1}^{K} 1_{u_i, a+u_i}(x) v_i.$$

The derivative of function G

Denote $U = \{u_1, u_2, \ldots, u_K\}$ is the set of points which values of function F will change. Denote $a + U$ by the set $\{a + u \mid u \in U\}$. It's possibe that there exist $1 \leq i, j \leq K$ such as $u_j = a + u_i$, leading to the two v_i, v_j appearing in the $D_a G(u_i)$. Thus denote U_a by the set $\{u \in U \mid u \in a + U\}$, $\overline{U_a} = U \setminus U_a$. For convenient, we define a function p_a on the index of of U by $p_a(i) = j$ where j satisfies $u_j = a + u_i$. So the equation $D_a G$ can be written more easily in the form

$$D_a G(x) = D_a F(x) + \sum_{u_i \in U_a, i < p_a(i)} 1_{u_i, u_{p_a(i)}}(v_i + v_{p_a(i)}) + \sum_{u_i \in \overline{U_a}} 1_{u_i, a+u_i}(x) v_i.$$

When G is an APN function

G is an APN function iff D_aG is 2-to-1, which means for $a \in \mathbb{F}_{2^n}^*$, $D_aG(x) = D_aG(y)$ occurs for $x = y$ or $x = y + a$.

Theorem

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, let $u_1, u_2, \ldots, u_K$ be K distinct points from $\mathbb{F}_{2^n}$ and let $v_1, v_2, \ldots, v_K$ be K arbitrary elements from $\mathbb{F}_{2^n}^*$. Then function G is APN if all of the following conditions are satisfied for all $a \in \mathbb{F}_{2^n}^*$:

(i) D_aF *is* 2-*to*-1 *on* $\mathbb{F}_{2^n} \setminus (U \cup a + U)$;

(ii) $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j + v_{p_a(i)} + v_{p_a(j)}$ *for* $u_i, u_j \in U_a$ *unless* $u_i = u_j$ *or* $u_i + u_j = a$;

(iii) $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j + v_{p_a(i)}$ *for* $u_i \in U_a, u_j \in \overline{U_a}$;

(iv) $D_aF(u_i) + D_aF(u_j) \neq v_i + v_j$ *for* $u_i, u_j \in \overline{U_a}$ *unless* $u_i = u_j$;

(v) $D_aF(u_i) + D_aF(x) \neq v_i + v_{p_a(i)}$ *for* $u_i \in U_a, x \notin (U \cup a + U)$;

(vi) $\boxed{D_aF(u_i) + D_aF(x) \neq v_i \text{ for } u_i \in \overline{U_a}, x \notin (U \cup a + U).}$

Proof by contrapositive

We prove it by contrapositive: assume there is a tuple $(a, x, y) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^2$ with $x \neq y, x \neq a + y$ satisfying $D_aG(x) = D_aG(y)$. Since $D_aG(x)$ has three cases for x in $\overline{U_a}, U_a$ or $\mathbb{F}_{2^n} \setminus (U \cup a + U)$, we must run over all possible cases for (a, x, y).

$$\begin{cases} x, y \in (U \cup a + U) \\ x, y \notin (U \cup a + U) \begin{cases} x, y \in U_a \\ \text{one of } \; x, y \in U_a \\ x, y \notin U_a \end{cases} \\ \text{one of } \; x, y \in (U \cup a + U) \begin{cases} x \in U_a \\ x \in \overline{U_a} \end{cases} \end{cases}$$

- Consider the first case, when $x, y \notin (U \cup a + U)$, we have $D_aF(x) = D_aF(y)$, so we confirm that D_aF cannot be 2-to-1 over $\mathbb{F}_{2^n} \setminus (U \cup a + U)$ since $x \neq y, x \neq a + y$. Conversely, if D_aF is 2-to-1 over $\mathbb{F}_{2^n} \setminus (U \cup a + U)$, it's easy to see that there exists no tuple (a, x, y) satisfying the
- Consider the last case, assume $D_aG(u_i) = D_aG(y)$ for $u_i = x \in \overline{U_a}$ and $y \notin (U \cup a + U)$, we have $D_aF(u_i) + v_i = D_aF(y)$. So we arrive at (vi).

Fixed points $u_1, u_2, ..., u_K$

By fixing the function F with K points $u_1, u_2, \ldots, u_K$, we can reduce the number of potential values for the values $v_1, v_2, \ldots, v_K$.

Algorithm 1: Reducing the domains of v_i

Input : The set of K distinct points $U = \{u_1, u_2, \ldots, u_K\} \subseteq \mathbb{F}_{2^n}$ with a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Output: A domain $D_i \subseteq \mathbb{F}_{2^n}$ for all v_i s.t. if G is APN, then $v_i \in D_i$ for all i.

for $i \leftarrow 1$ **to** K **do**

    set $D_i \leftarrow \mathbb{F}_{2^n}$;

    compute $A \leftarrow \{D_a F(x) + D_a F(u_i) : x, a \in \mathbb{F}_{2^n}, a \neq 0, u_i \in \overline{U_a}, x \notin (U \cup a + U)\}$;

    update $D_i \leftarrow D_i \setminus A$;

end

Example


```
//K:=6; U being generated by {1, β , β^4, β^21},
//which means the exponents are in {0,4,1,21,56,35,42,14,58,43,16,25,37,22,46}
n:=6;
F<v>:=FiniteField(2,n);
Fstar:={v^i:i in [0..2^n-2]};
F:={f:f in F};
zero:=F diff Fstar;
P<x>:=PolynomialRing(GF(2));
Z:=IntegerRing();
f:=func<x|x^3>;
U:={v^i:i in {0,4,1,21,56,35,42,14,58,43,16,25,37,22,46}};
U:=U join zero;
for u in U do
D:=Fstar;
for a in Fstar do
audomain:=F diff U;
xnotdomain:=U join {a+u:u in U};
xdomain:=F diff xnotdomain;
if a+u in audomain then
A:={f(u)+f(u+a)+f(x)+f(x+a):x in xdomain};
D:=D diff A;
end if;
end for;
D;
end for;
```

Take $F(x) = x^3$ over $\mathbb{F}_{2^6}$ with U generated by $\{1, \beta, \beta^4, \beta^{21}\}$ in the sense of additive closure with β is primitive in $\mathbb{F}_{2^6}$. We get the result

```
for> end for;
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
{ v^56, v^35, v^14, v^49, v^28, v^7 }
```

In above situation (when the set of points U can be transformed into an APN function), the filtering procedure may leave rather large domains for the candidates, which still needs long computations: the 6^{16} potential candidates are left to be examined, and actually there are only 6 possible candidates that lead to an APN function, which are all the same values for the 16 points. So there are still many things to impose on the values v_i.
But in some cases (when the set of points U cannot be transformed into an APN function), no values are left for some v_i, which implies no APN functions can be obtained by changing the values in the points U of F.

When both F and G are APNness, we can get the following property for the distance between F and G:

Corollary

Let F and G be as in the statement of Theorem 1 with $v_i \neq 0$ for $1 \leq i \leq K$, and assume, in addition, that F is APN; consider some fixed i, then no more than $3(K-1)$ derivatives of the form $D_a F(x) + F(u_i + a)$ map to $G(u_i)$.

Proof

In theorem 1 (vi), if G is an APN, then $D_aF(u_i) + D_aF(x) \neq v_i$ for $u_i \in \overline{U_a}, x \notin (U \cup a + U)$, i.e. $F(u_i + a) + D_aF(x) \neq F(u_i) + v_i = G(u_i)$ for $u_i \in \overline{U_a}, x \notin (U \cup a + U)$. This equation gives some insight of the property between G and F:

- when $x \in (U \cup a + U)$, there are chances that $F(u_i + a) + D_aF(x) = G(u_i)$ for $u_i \in \overline{U_a}$, and the number of solution is at most $2(K - 1)$ since $U \cap a + U \neq \emptyset$;
- when $x \in (U \cup a + U)$ and $u_i \in U_a$, we confirm that there are at most K such direction a, but note that $a \neq 0$, so there are at most $K - 1$ direction a.

Corollary

Let F be an APN function over $\mathbb{F}_{2^n}$ and let m_F be the number

$$m_F = \min_{b,\beta \in \mathbb{F}_{2^n}} |\Pi_F^{\beta}(b)|^4.$$

Then for any APN function $G \neq F$ over $\mathbb{F}_{2^n}$, the Hamming distance $d(F,G)$ between F and G satisfies

$$d(F,G) \geq \lceil \frac{m_F}{3} \rceil + 1.$$

[4] we define $\Pi_F^{\beta}(b)$ to be the set of derivative directions a for which $D_a F(x) + F(\beta + a)$ maps to b, i.e.

$$\Pi_F^{\beta}(b) = \{a \in \mathbb{F}_{2^n} : D_a F(x) + F(\beta + a) = b \text{ has solutions}\}.$$

Proof of the Corollary

From above we conclude if two APN functions F, G have distance K, then we can compute all possible values $D_aF(x) + F(u_i + a)$ for u_i and $G(u_i)$. Therefore when b, β run over $\mathbb{F}_{2^n}$, we compute a series of $\Pi_F^\beta(b)$, whose cardinalities must have the minimal value, which is m_F. Of course $m_F \leq 3(K-1)$, so we arrive at the corollary.

Section 3

The lower bound of nonlinearity for known APN functions[5]

[5] Carlet C. On the properties of the Boolean functions associated to the differential spectrum of general APN functions and their consequences[J]. IEEE Transactions on Information Theory, 2021, 67(10): 6926-6939.

We can define $\gamma_F(a,b)$ as below: $\forall a,b \in \mathbb{F}_2^n, \gamma_F(a,b) =$

$$\begin{cases} 1, & \text{if } a \neq 0_n \text{ and } F(x)+F(x+a)=b \text{ has solutions} \\ 0, & \text{otherwise.} \end{cases}$$

Thus, for every APN (n,n)-function F, we view it as a Boolean function $\frac{|(D_aF)^{-1}(b)|}{2} - 2^{n-1}\delta_0(a,b)$, then we have

$$\widehat{\gamma_F(u,v)} = \frac{1}{2}W_F^2(u,v) - 2^{n-1}.$$

So we confirm that for every u,v:

$$W_{\gamma_F}(u,v) = \begin{cases} 2^n, & \text{if } v = 0_n \\ 2^n - W_F^2(u,v), & \text{if } v \neq 0_n. \end{cases}$$

The Walsh transform of the APN function

The fourth moment of the Walsh transform of an APN function F:

$$\sum_{u,v\in\mathbb{F}_2^n} W_F^4(u,v) = 3\cdot 2^{4n} - 2^{3n+1}.$$

When apply the Titsworth relation on the γ_F, we have for all $(u_0,v_0)\neq(0_n,0_n)$,

$$\sum_{u,v\in\mathbb{F}_2^n} W_{\gamma_F}(u,v)W_{\gamma_F}(u+u_0,v+v_0) = 0.$$

Then we have the following theorem:

Theorem

Any APN (n,n)-function F satisfies that for all (u_0, v_0),

$$\sum_{\substack{u,v\in\mathbb{F}_2^n \\ v\neq 0_n, v\neq v_0}} W_F^2(u,v)W_F^2(u+u_0, v+v_0) = 2^{4n} - 2^{3n+1} + 2^{4n}\delta_0(u_0,v_0).$$

Corollary

If there exists $(u_0, v_0) \neq (0_n, 0_n)$ such that $|W_F(u,v)|$ and $|W_F(u+u_0, v+v_0)|$ both achieve the maximun value of $\{|W_F(u,v)| : u, v \in \mathbb{F}_2^n; v \neq 0_n\}$, then we have

$$nl(F) \geq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{4n-1} - 2^{3n}}.$$

Shanghai Jiao Tong University

Thank You

Zhaole Li · APN functions