Foundations of cryptanalysis: on Boolean functions

Anne Canteaut

Anne.Canteaut@inria.fr

http://www-rocq.inria.fr/secret/Anne.Canteaut/

Ice Break 2013

Outline

- Basic properties of Boolean functions
- Linear approximations of a Boolean function and Walsh transform
- Resistance to differential attacks
- Finding good Sboxes

Basic properties of Boolean functions

Boolean functions

Definition. A Boolean function of n variables is a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2$.

Truth table of a Boolean function.

x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
$f(x_1, x_2, x_3)$	0	1	0	0	0	1	1	1

Value vector of f: word of 2^n bits corresponding to all $f(x), x \in \mathbf{F}_2^n$.

Vectorial Boolean functions

Definition. A vectorial Boolean function with n inputs and m outputs is a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$:

$$\begin{array}{rccc} S: & \mathbf{F}_2^n & \longrightarrow & \mathbf{F}_2^m \\ & (x_1, \ldots, x_n) & \longmapsto & (y_1, \ldots, y_m) \end{array}$$

Each function

$$S_i : (x_1, \ldots, x_n) \longmapsto y_i$$

is called a coordinate of S.

Example.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5
$S_1(x)$	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1
$S_2(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0
$S_3(x)$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1
$S_4(x)$	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0

Hamming weight of a Boolean function.

The Hamming weight of a Boolean function f, $wt(f)$, is the Hamming weight of its value vector.

A function of n variables is balanced if and only if $wt(f) = 2^{n-1}$.

Proposition. A vectorial function S with n inputs and n outputs is a permutation if and only if any nonzero linear combination of its coordinates

$$x \longmapsto \bigoplus_{i=1}^{n} \lambda_i S_i(x), \quad \lambda = (\lambda_1, \ldots, \lambda_n) \neq 0$$

is a balanced Boolean function.

Algebraic normal form (ANF)

Monomials in $x_1, \ldots, x_n$:

$$\{x^u,\ \ u \in \mathbf{F}_2^n\} \text{ where } x^u = \prod_{i=1}^{n} x_i^{u_i}.$$

Example: $x_1^1 x_2^0 x_3^1 x_4^1 = x_1 x_3 x_4 = x^{1011}$.

Proposition.

Any Boolean function of n variables has a unique polynomial representation:

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbf{F}_2^n} a_u x^u,\ \ a_u \in \mathbf{F}_2.$$

Moreover, the coefficients of the ANF and the values of f satisfy:

$$a_u = \bigoplus_{x \preceq u} f(x) \text{ and } f(u) = \bigoplus_{x \preceq u} a_x,$$

where $x \preceq u$ if and only if $x_i \le u_i$ for all $1 \le i \le n$.

Example

x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
$f(x_1, x_2, x_3)$	0	1	0	0	0	1	1	1

$$a_{000} = f(000) = 0$$
$$a_{100} = f(100) \oplus f(000) = 1$$
$$a_{010} = f(010) \oplus f(000) = 0$$
$$a_{110} = f(110) \oplus f(010) \oplus f(100) \oplus f(000) = 1$$
$$a_{001} = f(001) \oplus f(000) = 0$$
$$a_{101} = f(101) \oplus f(001) \oplus f(100) \oplus f(000) = 0$$
$$a_{011} = f(011) \oplus f(001) \oplus f(010) \oplus f(000) = 1$$
$$a_{111} = \bigoplus_{x \in \mathbf{F}_2^3} f(x) = wt(f) \bmod 2 = 0$$

$$f = x_1 \oplus x_1 x_2 \oplus x_2 x_3.$$

Computing the ANF

$n = 3$:

0	1	2	3	4	5	6	7
$f(0)$	$f(1)$	$f(2)$	$f(3)$	$f(4)$	$f(5)$	$f(6)$	$f(7)$
$f(0)$	$f(0) \oplus f(1)$	$f(2)$	$f(2) \oplus f(3)$	$f(4)$	$f(4) \oplus f(5)$	$f(6)$	$f(6) \oplus f(7)$
$f(0)$	$f(0) \oplus f(1)$	$f(0) \oplus f(2)$	$f(0) \oplus f(1)$ $\oplus f(2) \oplus f(3)$	$f(4)$	$f(4) \oplus f(5)$	$f(4) \oplus f(6)$	$f(4) \oplus f(5)$ $\oplus f(6) \oplus f(7)$
$f(0)$	$f(0) \oplus f(1)$	$f(0) \oplus f(2)$	$f(0) \oplus f(1)$ $\oplus f(2) \oplus f(3)$	$f(0) \oplus f(4)$	$f(0) \oplus f(1)$ $f(4) \oplus f(5)$	$f(0) \oplus f(2)$ $\oplus f(4) \oplus f(6)$	$f(0) \oplus f(1)$ $\oplus f(2) \oplus f(3)$ $\oplus f(4) \oplus f(5)$ $\oplus f(6) \oplus f(7)$

first step:

$$f(2i+1) \leftarrow f(2i+1) \oplus f(2i)$$

second step:

$$f(4i+j+2) \leftarrow f(4i+j+2) \oplus f(4i+j), \ \forall 0 \leq j < 2$$

third step:

$$f(8i+j+4) \leftarrow f(8i+j+4) \oplus f(8i+j), \ \forall 0 \leq j < 4$$

Computing the ANF

When the value vector is stored as a $\mathbf{32}$-bit integer `x`:

```
x ^= (x & 0x55555555) << 1;
x ^= (x & 0x33333333) << 2;
x ^= (x & 0x0f0f0f0f) << 4;
x ^= (x & 0x00ff00ff) << 8;
x ^= x << 16;
```

Degree of a Boolean function

Definition.
The degree of a Boolean function is the degree of the largest monomial in its ANF.

Proposition.
The weight of an n-variable function f is odd if and only if $\deg f = n$.

Definition.
The degree of a vectorial function S with n inputs and m outputs is the maximal degree of its coordinates.

Example

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5
$S_1(x)$	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1
$S_2(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0
$S_3(x)$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1
$S_4(x)$	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0

$$\begin{aligned}
S_1 &= 1 + x_1 + x_3 + x_2x_3 + x_4 + x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4 \\
S_2 &= 1 + x_1x_2 + x_1x_3 + x_1x_2x_3 + x_4 + x_1x_4 + x_1x_2x_4 + x_1x_3x_4 \\
S_3 &= 1 + x_2 + x_1x_2 + x_2x_3 + x_4 + x_2x_4 + x_1x_2x_4 + x_3x_4 + x_1x_3x_4 \\
S_4 &= 1 + x_3 + x_1x_3 + x_4 + x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4
\end{aligned}$$

Identifying $\mathbf{F}_2^n$ with a finite field

$\mathbf{F}_2^n$ is identified with the finite field with 2^n elements.

$$\mathbf{F}_{2^n} = \{0\} \cup \{\alpha^i,\ 0 \leq i \leq 2^n - 2\}$$

where α is a root of a primitive polynomial of degree n.

$$\Rightarrow \text{for any } i, \quad \alpha^i = \sum_{j=0}^{n-1} \lambda_j \alpha^j$$

Example for $n = 4$:

primitive polynomial: $1 + x + x^4$, α a root of this polynomial.

$\mathbf{F}_{2^4}$	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7
	0	1	α	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^3+\alpha+1$
$\mathbf{F}_2^4$	0000	0001	0010	0100	1000	0011	0110	1100	1011

α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
α^2+1	$\alpha^3+\alpha$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	α^3+1
0101	1010	0111	1110	1111	1101	1001

The univariate representation of Sboxes

Any vectorial function with n inputs and n outputs can be seen as

$$S : \mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}$$

Then,

$$S(X) = \sum_{i=0}^{2^n-1} c_i X^i \,, c_i \in \mathbf{F}_{2^n}.$$

Example:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	f	e	b	c	6	d	7	8	0	3	9	a	4	2	1	5

$$\begin{aligned} S(X) \;=\; & \alpha^{12} + \alpha^2 X + \alpha^{13} X^2 + \alpha^6 X^3 + \alpha^{10} X^4 + \alpha X^5 + \alpha^{10} X^6 + \alpha^2 X^7 \\ & + \alpha^9 X^8 + \alpha^4 X^9 + \alpha^7 X^{10} + \alpha^7 X^{11} + \alpha^5 X^{12} + X^{13} + \alpha^6 X^{14} \end{aligned}$$

Remark. The (multivariate) degree of X^i is exactly the number of ones in the binary expansion of i.

Linear approximations of a function

and Walsh transform

Idea

Algebraic attacks (and variants):

use relations between the input and output bits of the cipher which hold with probability 1.

but the degree is usually too high!

Linear (or correlation) attacks [Siegenthaler 85][Matsui 93]:

use linear relations between the input and output bits of the cipher which hold with probability less than 1.

Example

Compute

$$\boldsymbol{f(x_1, x_2, x_3, x_4) = 1 \oplus x_1 \oplus x_4 \oplus S_2(x)}$$

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
$S_1(x)$	1	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1	0xc665
$S_2(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0	0x2a57
$S_3(x)$	1	1	0	1	1	1	1	0	0	0	0	0	1	0	0	1	0x907b
$S_4(x)$	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	0	0x0caf

$$\begin{aligned} 1 \oplus x_1 \oplus x_4 &= \texttt{0xffff} + \texttt{0xaaaa} + \texttt{0xff00} = \texttt{0xaa55} \\ S_2(x) &= \texttt{0x2a57} \\ f(x) &= \texttt{0x8002} \end{aligned}$$

The relation $\boldsymbol{f(x) = 0}$ holds for $\mathbf{14}$ of the $\mathbf{16}$ values of $\boldsymbol{x} \in \mathbf{F}_2^4$, i.e., with probability $\frac{14}{16} = \frac{7}{8}$.

Computing the probabilities of all linear relations

Bias of a Boolean function

For any Boolean function f of n variables

$$\mathcal{E}(f) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)} = 2^n - 2wt(f).$$

Equivalently,

$$\Pr[f(x) = 1] = \frac{wt(f)}{2^n} = \frac{1}{2}\left(1 - \frac{\mathcal{E}(f)}{2^n}\right).$$

$\longrightarrow$ we need to compute the biases of all Boolean functions

$$x \longmapsto b \cdot S(x) \oplus a \cdot x \;.$$

Linear approximations of an Sbox

$a \setminus b$	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	-4	.	4	.	-4	8	-4	4	8	4	.	-4	.	4	.
2	4	-4	.	-4	.	.	4	4	8	.	4	8	-4	-4	.
3	8	4	4	-4	4	.	.	.	.	4	-4	-4	-4	.	8
4	.	-4	4	4	-4	.	.	-8	.	4	4	4	4	.	8
5	-4	4	.	4	8	.	4	-4	8	.	-4	.	4	-4	.
6	-4	.	4	.	4	8	4	4	-8	4	.	4	.	-4	.
7	.	.	.	8	.	-8	.	.	.	.	8	.	8	.	.
8	.	-4	4	-8	.	4	4	-8	.	-4	-4	.	.	4	-4
9	-4	-12	.	.	4	-4	.	4	.	.	-4	-4	.	.	4
a	-4	.	-12	-4	.	4	.	-4	.	4	.	.	-4	.	4
b	.	.	.	4	-4	4	-4	.	.	-8	-8	4	-4	-4	4
c	.	.	.	-4	-4	-4	-4	.	.	8	-8	4	4	-4	-4
d	-4	.	4	4	.	-4	.	-4	.	4	.	.	-12	.	-4
e	4	-4	.	.	4	4	-8	-4	.	.	4	-4	.	-8	-4
f	-8	4	4	-8	.	-4	-4	.	.	-4	4	.	.	-4	4

$$\Pr_{x}[a \cdot x \cdot b \cdot S(x) = 1] = \frac{1}{2}\left(1 - \frac{\mathcal{E}[a,b]}{2^n}\right)$$

For instance, for $a = \texttt{0x9}$ and $b = \texttt{0x2}$, we have $p = \frac{1}{2}(1 + \frac{12}{16}) = \frac{7}{8}$.

Walsh transform of a Boolean function

Walsh transform of a Boolean function f of n variables

$$\begin{array}{lcl} \mathbf{F}_2^n & \longrightarrow & \mathbb{Z} \\ a & \longmapsto & \mathcal{E}(f + \varphi_a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x) + a \cdot x} \end{array}$$

where $\varphi_a : x \longmapsto a \cdot x$

Walsh transform of a vectorial function S:

$$\begin{array}{lcl} \mathbf{F}_2^n \times \mathbf{F}_2^n & \longrightarrow & \mathbb{Z} \\ (a, b) & \longmapsto & \mathcal{E}(b \cdot S + \varphi_a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{b \cdot S(x) + a \cdot x} \end{array}$$

Computing the Walsh transform

$f(x)$	0	1	0	0	0	1	1	1
$(-1)^{f(x)}$	1	-1	1	1	1	-1	-1	-1
step 1	0	2	2	0	0	2	-2	0
step 2	2	2	-2	2	-2	2	2	2
$\mathcal{E}(f+\varphi_a)$	0	4	0	4	4	0	-4	0

first step:

$$S(2i) \leftarrow S(2i) + S(2i+1)$$
$$S(2i+1) \leftarrow S(2i) - S(2i+1)$$

second step:

$$S(4i+j) \leftarrow S(4i+j) + S(4i+j+2),\ \forall 0 \le j < 2$$
$$S(4i+j+2) \leftarrow S(4i+j) - S(4i+j+2),\ \forall 0 \le j < 2$$

third step:

$$S(8i+j) \leftarrow S(8i+j) + S(8i+j+4),\ \forall 0 \le j < 4$$
$$S(8i+j+4) \leftarrow S(8i+j) - S(8i+j+4),\ \forall 0 \le j < 4$$

Complexity : $n2^n$ operations.

Lemma:

$$\mathcal{E}(\varphi_a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{a \cdot x} = \begin{cases} 2^n & \text{if } a = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Proposition. The Walsh transform is an involution (up to a multiplicative constant): for any $x \in \mathbf{F}_2^n$,

$$\begin{aligned} \sum_{a \in \mathbf{F}_2^n} \mathcal{E}(f + \varphi_a)(-1)^{a \cdot x} &= \sum_{u \in \mathbf{F}_2^n} \sum_{a \in \mathbf{F}_2^n} (-1)^{f(u) + a \cdot u + a \cdot x} \\ &= \sum_{u \in \mathbf{F}_2^n} (-1)^{f(u)} \sum_{a \in \mathbf{F}_2^n} (-1)^{a \cdot (x+u)} \\ &= 2^n (-1)^{f(x)} \end{aligned}$$

Some basic properties of the Walsh transform

Parseval equality.

$$\sum_{a \in \mathbf{F}_2^n} \mathcal{E}^2(f + \varphi_a) = 2^{2n}.$$

Proof.

$$\begin{aligned}
\sum_{a \in \mathbf{F}_2^n} \mathcal{E}^2(f + \varphi_a) &= \sum_{a \in \mathbf{F}_2^n} \left(\sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+a \cdot x} \right) \left(\sum_{y \in \mathbf{F}_2^n} (-1)^{f(y)+a \cdot y} \right) \\
&= \sum_{x \in \mathbf{F}_2^n} \sum_{y \in \mathbf{F}_2^n} (-1)^{f(x)+f(y)} \sum_{a \in \mathbf{F}_2^n} (-1)^{a \cdot (x+y)} \\
&= 2^n \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+f(x)} \\
&= 2^{2n} .
\end{aligned}$$

[Check it on each column of the table on Slide 18]

Linearity of a Boolean function

Definition. For any Boolean function f of n variables,

$$\mathcal{L}(f) = \max_a |\mathcal{E}(f + \varphi_a)|$$

is called the linearity of f (highest bias for an affine approximation).

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2}\mathcal{L}(f)$$

is called the nonlinearity of f (distance of f to the affine functions).

Can we say something about $\mathcal{L}(f)$?

$$\mathcal{L}(f) = \max_a |\mathcal{E}(f + \varphi_a)|$$

Theorem. [Rothaus 76] For any Boolean function of n variables,

$$\mathcal{L}(f) \geq 2^{\frac{n}{2}} ,$$

with equality for even n only. The functions achieving this bound are called bent functions. They are not balanced.

Proof. From Parseval equality:

$$2^{2n} = \sum_{a \in \mathbf{F}_2^n} \mathcal{E}^2(f + \varphi_a) \leq \max_{a \in \mathbf{F}_2^n} \mathcal{E}^2(f + \varphi_a) \times 2^n = 2^n \mathcal{L}^2(f)$$

with equality if and only if all $\mathcal{E}^2(f + \varphi_a)$ are equal.

Then, $\mathcal{L}(f) \geq 2^{\frac{n}{2}}$ with equality if and only if

$$\mathcal{E}(f + \varphi_a) = \pm 2^{\frac{n}{2}}, \ \forall a \in \mathbf{F}_2^n .$$

In particular, none of the $f + \varphi_a$ is balanced.

Can we say something about $\mathcal{L}(f)$?

What is the lowest possible value for $\mathcal{L}(f)$ when n is odd?
When f is balanced?

Functions of degree 2.

For n odd, $n = 2t + 1$

$$x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2t-1}x_{2t} \oplus x_{2t+1}$$

satisfies $\mathcal{L}(f) = 2^{\frac{n+1}{2}}$. Moreover, f is balanced and

$$\forall a \in \mathbf{F}_2^n, \;\; \mathcal{E}(f + \varphi_a) \in \{0, \pm 2^{\frac{n+1}{2}}\}.$$

Theorem.

$$2^{\frac{n}{2}} \leq \min_{f \in \mathcal{B}ool_n} \mathcal{L}(f) \leq 2^{\frac{n+1}{2}}$$

Boolean functions with a low linearity

n	$\min_{f \in \mathcal{B}ool_n} \mathcal{L}(f)$	
5	8	[Berlekamp-Welch 72]
7	16	[Mykkelveit 80]
9	24, 26, 28, 30	[Kavut-Maitra-Yücel 06]
11	46-60	
13	92-120	
15	182-216	[Paterson-Wiedemann 83]

Open problem. Find the lowest possible linearity for a Boolean function of n variables, where n is odd and $n \geq 9$.

Balanced Boolean functions with a low linearity

n	$\min_{f \in \mathcal{B}al_n} \mathcal{L}(f)$
4	8
5	8
6	12
7	16
8	20, 24
9	24, 28, 32
10	36, 40

Open problem. Find the lowest possible linearity for a balanced Boolean function of n variables, when $n \geq 8$.

Proposition. [Katz 71] If f is balanced, all values $\mathcal{E}(f + \varphi_a)$ are divisible by $2^{\lceil \frac{n-1}{\deg f} \rceil + 1}$, i.e., at least by 4 (and by 8 if $\deg f < n - 1$).

Linearity of an Sbox

Criterion on the Sbox.

All linear approximations of S should have a small bias, *i.e.*,

$$\mathcal{L}(S) = \max_{a \in \mathbf{F}_2^n,\, b \in \mathbf{F}_2^n, b \neq 0} |\mathcal{E}\left(b \cdot S + \varphi_a\right)| = \max_{b \neq 0} \mathcal{L}(b \cdot S)$$

must be as small as possible.

$$\mathcal{NL}(S) = 2^{n-1} - \frac{1}{2}\mathcal{L}(S)$$

is called the nonlinearity of S.

Sboxes with a low linearity

What is the lowest possible value for $\mathcal{L}(S)$ when S is a vectorial function with n inputs and n outputs?

Theorem. [Chabaud-Vaudenay94] For any function S with n inputs and n ouputs,

$$\mathcal{L}(S) \geq 2^{\frac{n+1}{2}} ,$$

with equality for odd n only. The functions achieving this bound are called almost bent functions.

For n even.

There exist Sboxes with

$$\mathcal{L}(S) = 2^{\frac{n+2}{2}}$$

but we do not known if this value is minimal.

Resistance to differential attacks

Difference table of an Sbox

$a \setminus b$	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	2	0	4	2	0	2	2	0	0	0	2	0	0	0	2
2	2	2	0	2	4	0	2	0	4	0	0	0	0	0	0
3	2	0	4	0	2	0	0	0	0	6	0	0	0	2	0
4	2	0	2	4	0	0	0	2	2	0	0	2	0	0	2
5	0	4	2	0	0	0	2	2	0	0	4	2	0	0	0
6	4	0	0	0	0	4	0	4	0	0	0	0	4	0	0
7	0	2	0	0	2	2	2	0	2	2	2	0	0	2	0
8	0	4	0	0	0	4	0	0	0	0	0	0	4	0	4
9	2	2	0	2	2	0	0	0	4	0	0	2	0	2	0
a	0	0	2	2	0	2	2	2	0	2	2	0	0	0	2
b	0	0	2	0	4	0	2	2	0	0	0	6	0	0	0
c	0	2	0	0	0	2	0	0	2	2	2	2	0	4	0
d	2	0	0	0	2	0	0	0	0	2	0	0	8	2	0
e	0	0	0	0	0	0	4	0	0	0	4	0	0	4	4
f	0	0	0	4	0	0	0	4	2	2	0	2	0	0	2

$$\delta_S(a,b) = \#\{X \in \mathbf{F}_2^n, \ \ S(X \oplus a) \oplus S(X) = b\}$$

Resistance to differential attacks

Criterion on the Sbox. [Nyberg-Knudsen 92] All entries in the difference table of S should be small.

$$\delta(S) = \max_{a,b \neq 0} \#\{X \in \mathbb{F}_2^n,\ \ S(X \oplus a) \oplus S(X) = b\}$$

must be as small as possible.

$\delta(S)$ is called the differential uniformity of S (always even).

Theorem. For any Sbox S with n inputs and n outputs,

$$\delta(S) \geq 2\ .$$

The functions achieving this bound are called almost perfect nonlinear functions (APN).

Finding good Sboxes

Affine equivalence between Sboxes

S_1 and S_2 are affinely equivalent if there exist two affine permutations A_1 and A_2, such that

$$S_2 = A_2 \circ S_1 \circ A_1$$

Then,

$$\delta(S_2) = \delta(S_1) \text{ and } \mathcal{L}(S_2) = \mathcal{L}(S_1)$$

Permutations of $\mathbb{F}_2^4$

$\delta(S) \geq 4$ and $\mathcal{L}(S) \geq 8$

16 classes of optimal Sboxes [Leander-Poschmann 07]

8 of them have all $x \mapsto b \cdot S(x)$ of degree 3.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
G_0	0	1	2	13	4	7	15	6	8	11	12	9	3	14	10	5
G_1	0	1	2	13	4	7	15	6	8	11	14	3	5	9	10	12
G_2	0	1	2	13	4	7	15	6	8	11	14	3	10	12	5	9
G_3	0	1	2	13	4	7	15	6	8	12	5	3	10	14	11	9
G_4	0	1	2	13	4	7	15	6	8	12	9	11	10	14	5	3
G_5	0	1	2	13	4	7	15	6	8	12	11	9	10	14	3	5
G_6	0	1	2	13	4	7	15	6	8	12	11	9	10	14	5	3
G_7	0	1	2	13	4	7	15	6	8	12	14	11	10	9	3	5
G_8	0	1	2	13	4	7	15	6	8	14	9	5	10	11	3	12
G_9	0	1	2	13	4	7	15	6	8	14	11	3	5	9	10	12
G_{10}	0	1	2	13	4	7	15	6	8	14	11	5	10	9	3	12
G_{11}	0	1	2	13	4	7	15	6	8	14	11	10	5	9	12	3
G_{12}	0	1	2	13	4	7	15	6	8	14	11	10	9	3	12	5
G_{13}	0	1	2	13	4	7	15	6	8	14	12	9	5	11	10	3
G_{14}	0	1	2	13	4	7	15	6	8	14	12	11	3	9	5	10
G_{15}	0	1	2	13	4	7	15	6	8	14	12	11	9	3	10	5

Permutations of $\mathbf{F}_2^n$, n odd

$$\mathcal{L}(S) \geq 2^{\frac{n+1}{2}} \text{ and } \delta(S) \geq 2$$

- Any AB Sbox (i.e., with $\mathcal{L}(S) = 2^{\frac{n+1}{2}}$) is APN [Chabaud-Vaudenay 94].
- The converse holds for some cases only, including quadratic APN Sboxes [Carlet-Charpin-Zinoviev 98].
- AB Sboxes over $\mathbf{F}_2^n$ have degree at most $\frac{n+1}{2}$.

Known AB permutations of $\mathbb{F}_2^n$, n odd

Monomials permutations $S(x) = x^s$ over $\mathbb{F}_{2^n}$.

quadratic	$2^i + 1$ with $\gcd(i,n) = 1$, $1 \leq i \leq (n-1)/2$	[Gold 68],[Nyberg 93]
Kasami	$2^{2i} - 2^i + 1$ with $\gcd(i,n) = 1$ $2 \leq i \leq (n-1)/2$	[Kasami 71]
Welch	$2^{\frac{n-1}{2}} + 3$	[Dobbertin 98] [C.-Charpin-Dobbertin 00]
Niho	$2^{\frac{n-1}{2}} + 2^{\frac{n-1}{4}} - 1$ if $n \equiv 1 \bmod 4$ $2^{\frac{n-1}{2}} + 2^{\frac{3n-1}{4}} - 1$ if $n \equiv 3 \bmod 4$	[Dobbertin 98] [Xiang-Hollmann 01]

Non-monomial permutations [Budaghyan-Carlet-Leander08]

For n odd, divisible by 3 and not by 9.

$$S(x) = x^{2^i+1} + ux^{2^{j\frac{n}{3}}+2^{(3-j)\frac{n}{3}+i}} \text{ with } \gcd(i,n) = 1 \text{ and } j = i\frac{n}{3} \bmod 3$$

Known APN permutations of $\mathbb{F}_2^n$, n even

For $n = 6$.

$$\delta(S) \geq 2 \text{ and } \mathcal{L}(S) \geq 12$$

S= {0, 54, 48, 13, 15, 18, 53, 35, 25, 63, 45, 52, 3, 20, 41, 33, 59, 36, 2, 34, 10, 8, 57, 37, 60, 19, 42, 14, 50, 26, 58, 24, 39, 27, 21, 17, 16, 29, 1, 62, 47, 40, 51, 56, 7, 43, 44, 38, 31, 11, 4, 28, 61, 46, 5, 49, 9, 6, 23, 32, 30, 12, 55, 22};

satisfies

$$\delta(S) = 2 \ , \ \deg S = 4 \text{ and } \mathcal{L}(S) = 16 \text{ [Dillon 09]}$$

The corresponding univariate polynomial over $\mathbf{F}_{2^6}$ contains 52 nonzero monomials (out of the 56 possible monomials of degree at most 4).

This is the only known APN permutation with an even number of variables.

Good permutations of $\mathbf{F}_2^n$, n even

Usually, we search for permutations S with

$$\delta(S) = 4 \text{ and } \mathcal{L}(S) = 2^{\frac{n+2}{2}} .$$

Monomials permutations $S(x) = x^s$ over $\mathbf{F}_{2^n}$.

$2^i + 1,\ \gcd(i, n) = 2$	$n \equiv 2 \bmod 4$	[Gold 68]
$2^{2i} - 2^i + 1,\ \gcd(i, n) = 2$	$n \equiv 2 \bmod 4$	[Kasami 71]
$2^{\frac{n}{2}} + 2^{\frac{n}{4}} + 1$	$n \equiv 4 \bmod 8$	[Bracken-Leander 10]
$2^n - 2$		[Lachaud-Wolfmann 90]

The last one is affinely equivalent to the AES Sbox.

Some conclusions

- Many other properties of Sboxes can be exploited by an attacker;
- A strong algebraic structure may introduce weaknesses.
- Don't forget implementation!!!

Some useful links:

- *Boolean functions* (and related entries), in *Encyclopedia of Cryptography and Security*, Springer, 2011.
- *Handbook of Finite Fields* (G. Mullen and D. Panario, eds.), CRC Press, 2013.