Cryptographic Sboxes

Anne Canteaut

Anne.Canteaut@inria.fr

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

Summer School, Šibenik, June 2014

Vectorial Boolean functions

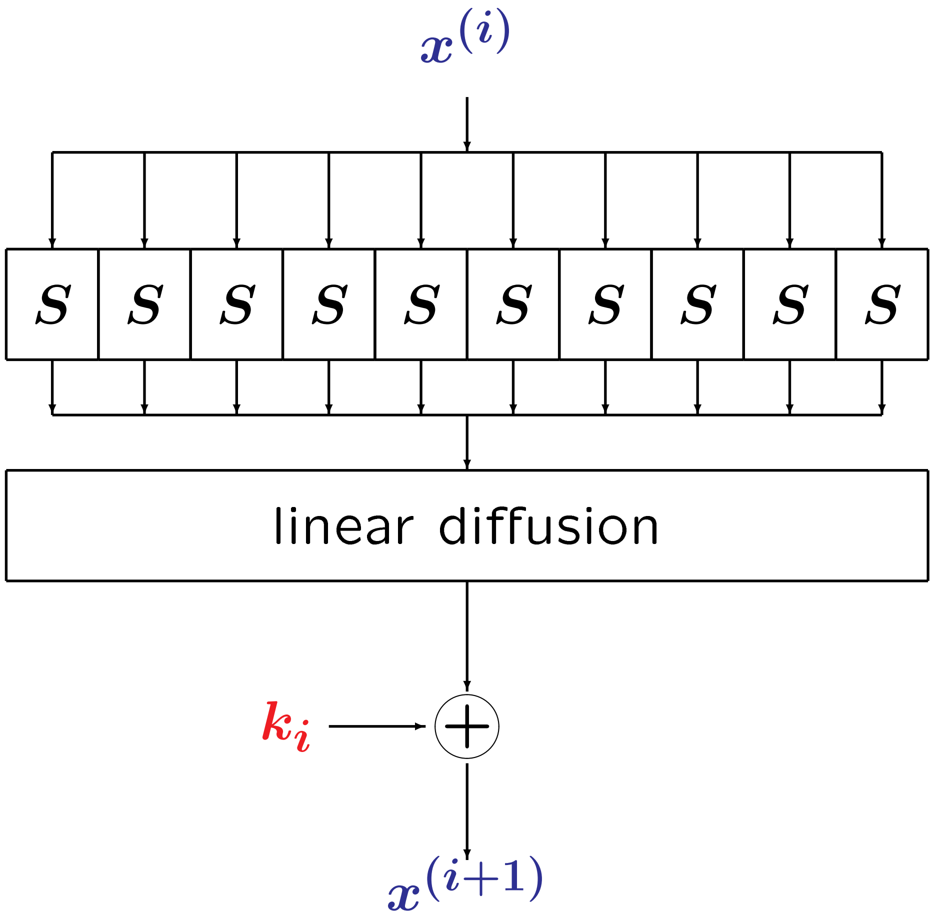
A vectorial Boolean function with n inputs and m outputs is a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$:

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

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

Round function in a substitution-permutation network



Outline

- Algebraic degree
- Differential uniformity
- Nonlinearity
- Finding good Sboxes

Degree of an Sbox

$$f(x_1,\ldots,x_n) = \sum_{u\in\mathbf{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}, \quad a_u \in \mathbf{F}_2.$$

Definition.

The degree of a Boolean function is the degree of the largest monomial in its algebraic normal form.

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

Proposition.

If S is a permutation of $\mathbf{F}_2^n$, then $\deg S \le n-1$.

Example

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
$S_2(x)$	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

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

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

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

Resistance to differential attacks [Nyberg Knudsen 92],[Nyberg 93]

Criterion on the Sbox. All entries in the difference table of S should be small.

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

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).

For SPN using S

Expected probability of a 2-round characteristic

$$\leq \left(\frac{\delta(S)}{2^n}\right)^d$$

where d is the branch number of the linear layer.

Expected probability of a 2-round differential [Daemen Rijmen 02]

$$\mathrm{MEDP}_2 \leq \left(\frac{\delta(S)}{2^n}\right)^{d-1}$$

E.g., for the 4-round AES,

$$\mathrm{MEDP}_4 \leq \left(2^{-6}\right)^{16}$$

Refinements involving the whole difference table [Park et al. 03].

Resistance to linear attacks

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

$$\mathbf{Pr}[a \cdot x + b \cdot S(x) = 0] = \frac{1}{2}\left(1 + \frac{\mathcal{W}[a,b]}{2^n}\right)$$

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

Walsh transform of an Sbox

Walsh transform of a Boolean function f of n variables

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

Walsh transform of an Sbox S:

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

Linearity of an Sbox

Criterion on the Sbox.

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

$$\mathcal{L}(S) = \max_{a \in \mathbf{F}_2^n,\ b \in \mathbf{F}_2^n, b \neq 0} |\mathcal{W}_S(a,b)|$$

must be as small as possible.

Parseval's equality:

for any output mask b,

$$\sum_{a \in \mathbf{F}_2^n} \mathcal{W}_S^2(a,b) = 2^{2n}\ .$$

For SPN using S

Expected square correlation of a 2-round linear trail

$$\leq \left(\frac{\mathcal{L}(S)}{2^n}\right)^{2d'}$$

where d' is the linear branch number of the linear layer.

Expected square correlation of a 2-round linear mask

[Daemen Rijmen 02]

$$\mathrm{MELP}_2 \leq \left(\frac{\mathcal{L}(S)}{2^n}\right)^{2(d'-1)}$$

Refinements involving the whole square correlation table [Park et al. 03].

Link between the difference and square correlation tables

Theorem. [Chabaud Vaudenay 94][Blondeau Nyberg 13]
There is a one-to-one correspondence between the difference table

$$\delta(a,b),\ a \in \mathbf{F}_2^n, b \in \mathbf{F}_2^n$$

and the square correlation table

$$\mathcal{W}^2(a,b),\ a,b \in \mathbf{F}_2^n, b \in \mathbf{F}_2^n$$

$$\begin{aligned}
\mathcal{W}^2(u,v) &= \sum_{a,b\in\mathbf{F}_2^n} (-1)^{a\cdot u+b\cdot v}\delta(a,b) \\
\delta(a,b) &= 2^{-2n} \sum_{u,v\in\mathbf{F}_2^n} (-1)^{a\cdot u+b\cdot v}\mathcal{W}^2(u,v)
\end{aligned}$$

There is a one-to-one correspondence between the Sbox and the correlation table.
But several Sboxes may have the same square correlation table.

Finding good Sboxes

w.r.t. the previous criteria

Equivalence between Sboxes

Affine equivalence

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

where A_1 and A_2 are two affine permutations of $\mathbf{F}_2^n$.

CCZ equivalence [Carlet Charpin Zinoviev 98]

$$(x', S_2(x')) = A\,(x, S_1(x))$$

where A is an affine permutation of $\mathbf{F}_2^{2n}$.

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

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

$\mathbf{16}$ classes of optimal Sboxes [Leander-Poschmann 07]
$\mathbf{8}$ of them have all $\boldsymbol{x \mapsto b \cdot S(x)}$ of degree $\mathbf{3}$.

	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

Theorem. [Chabaud Vaudenay 94]
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.

- Any AB function is APN.

$$\mathcal{L}(S) = 2^{\frac{n+1}{2}} \Longrightarrow \delta(S) = 2$$

- The converse holds for some cases only, for instance for APN Sboxes of degree 2 [Carlet Charpin Zinoviev 98]

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

Monomials permutations $S(x) = x^s$ over $\mathbf{F}_{2^n}, n = 2t+1$.

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

Non-monomial permutations. [Budaghyan-Carlet-Leander08]

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

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

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

There exist Sboxes with

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

but we do not known if this value is minimal.

APN power functions over $\mathbf{F}_2^n$, n even, are not permutations.

Do there exist APN permutations for n even?

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

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

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

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

Good permutations of $\mathbb{F}_2^n$, 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 $\mathbb{F}_{2^n}$.

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

The last one is affine 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!!!