Secure building-blocks against differential and linear attacks

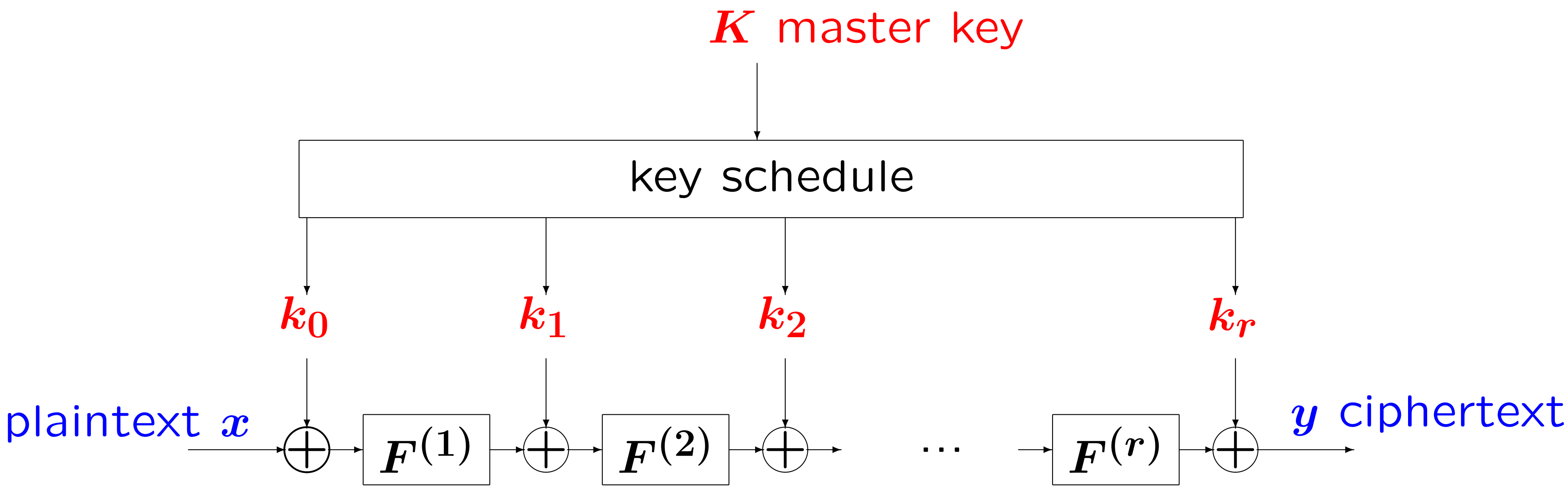
Anne Canteaut

Anne.Canteaut@inria.fr

https://www.paris.inria.fr/secret/Anne.Canteaut/

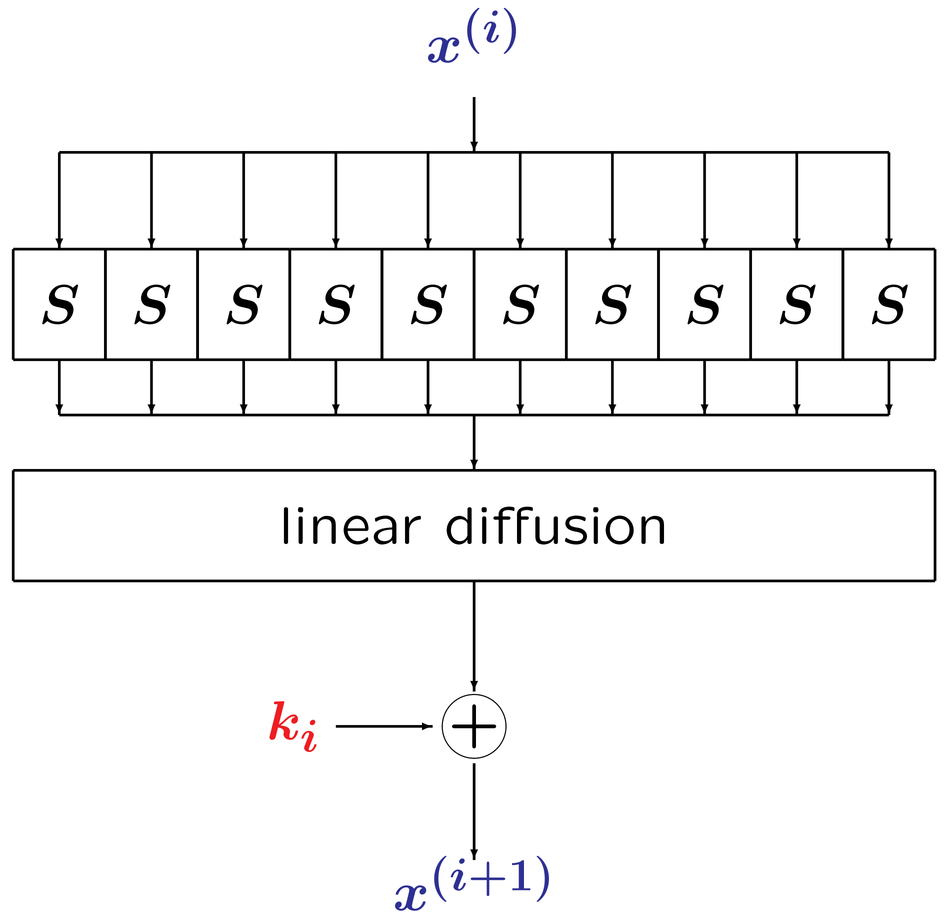
COST Training School, Torremolinos, February 2018

Key-alternating block ciphers



where each $F^{(i)}$ is a permutation of $\mathbf{F}_2^n$.

Round function in a substitution-permutation network



Outline

- Representations of Sboxes
- Linear approximations of a Boolean function and Walsh transform
- Resistance to differential attacks
- Finding good Sboxes
- Security criteria for the linear layer

Representations of Sboxes

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 $\mathbf{F}_2^m$:

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

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 $\mathbf{F}_2[x_1,\ldots,x_n]/(x_1^2+x_1,\ldots,x_n^2+x_n)$:

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

Example: $x^{1011}=x_1^1x_2^0x_3^1x_4^1=x_1x_3x_4.$

Proposition.

Any Boolean function of n variables has a unique polynomial representation in $\mathbf{F}_2[x_1,\ldots,x_n]/(x_1^2+x_1,\ldots,x_n^2+x_n)$:

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

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 $x\preceq y$ if and only if $x_i\leq y_i$ for all $1\leq i\leq n$.

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

$a_{000} = f(000) = 0$

$a_{100} = f(100) \oplus f(000) = 1$

$a_{010} = f(010) \oplus f(000) = 0$

$a_{110} = f(110) \oplus f(010) \oplus f(100) \oplus f(000) = 1$

$a_{001} = f(001) \oplus f(000) = 0$

$a_{101} = f(101) \oplus f(001) \oplus f(100) \oplus f(000) = 0$

$a_{011} = f(011) \oplus f(001) \oplus f(010) \oplus f(000) = 1$

$a_{111} = \bigoplus_{x \in \mathbb{F}_2^3} f(x) = wt(f) \bmod 2 = 0$

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

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

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

Linear approximations of a function and Walsh transform

Linear attacks [Matsui 93]

Idea.

Use linear relations between the input and output bits of the cipher which hold with probability significantly greater or significantly less than $1/2$.

$a \in \mathbf{F}_2^n$: input mask
$b \in \mathbf{F}_2^n$: output mask

$$\left| \mathbf{Pr}_x \left[a \cdot x \oplus b \cdot E_k(x) = 0 \right] - \frac{1}{2} \right|$$

For our 4-bit Sbox.

$$x_1 \oplus x_4 \oplus S_2(x) = \text{0x9} \cdot x \oplus \text{0x2} \cdot S(x)$$

equals 0 with probability $\frac{1}{8}$.

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,

$$\Pr[f(x) = 0] = \frac{wt(f)}{2^n} = \frac{1}{2}\left(1 - \frac{\mathcal{E}(f)}{2^n}\right).$$

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

$$x \longmapsto b \cdot S(x) + a \cdot x \ .$$

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

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

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

Walsh transform of a Boolean function

Walsh transform of a Boolean function f of n variables

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

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

Walsh transform of a vectorial function S:

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

Computing the Walsh transform

$f(x)$	0	1	0	0	0	1	1	1
$T(x) = (-1)^{f(x)}$	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
$\mathcal{E}(f + \ell_a)$	0	4	0	4	4	0	-4	0

first step:

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

second step:

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

third step:

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

Complexity : $n2^n$ operations.

Lemma:

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

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

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

Some basic properties of the Walsh transform

Parseval equality.

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

Proof.

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

[Check it on each column of the table on Slide 19]

Linearity of a Boolean function

Definition. For any Boolean function f of n variables,

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

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 $\mathcal{L}(f)$?

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

Theorem. [Rothaus 76] For any Boolean function with 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:

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

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

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

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

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

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

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

Open problem. Find the highest possible nonlinearity for a balanced Boolean function of n variables, where n is even and $n \geq 8$.

Proposition. [Katz 71] If f is balanced, all values $\mathcal{E}(f + \ell_a)$ 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.*,

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

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-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.

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 distribution 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

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

Resistance to differential attacks

Criterion on the Sbox. [Nyberg-Knudsen 92]

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

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

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).

Link between the difference and square correlation tables

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

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

and the squared LAT

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

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

There is a one-to-one correspondence between the Sbox and the LAT.
But several Sboxes may have the same squared LAT.

Finding good Sboxes

Affine equivalence between Sboxes

S_1 and S_2 are affinely equivalent if there exist two affine permutations of $\mathbf{F}_2^n$, 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 $\mathbf{F}_2^n$, 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 specific cases only, e.g for quadratic APN Sboxes [Carlet-Charpin-Zinoviev 98]
- AB functions 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 $\gcd(i, n) = 1$, $1 \le i \le t$	[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 $\mathbf{F}_2^4$

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

16 classes of optimal Sboxes [Leander-Poschmann 07]

	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 $\mathbf{F}_2^6$

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

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

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

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

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

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

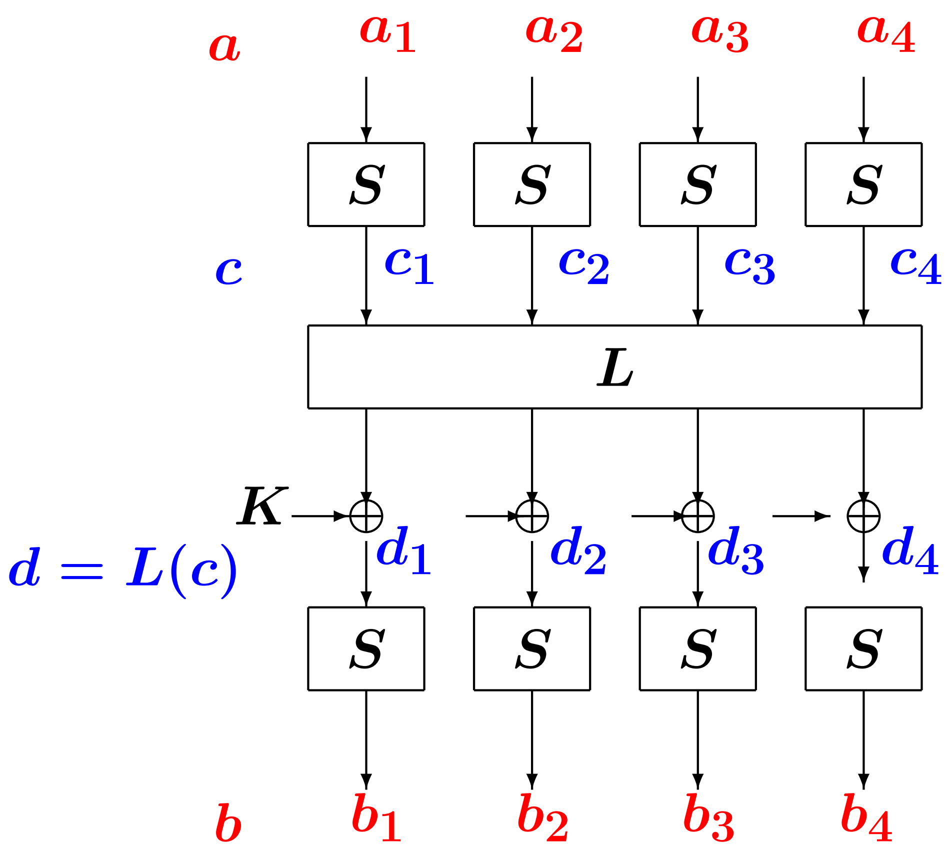
Monomials permutations $S(x) = x^s$ over $\mathbf{F}_{2^n}$.

$2^i + 1,\ \gcd(i, n) = 2$	$n \equiv 2 \bmod 4$	[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.

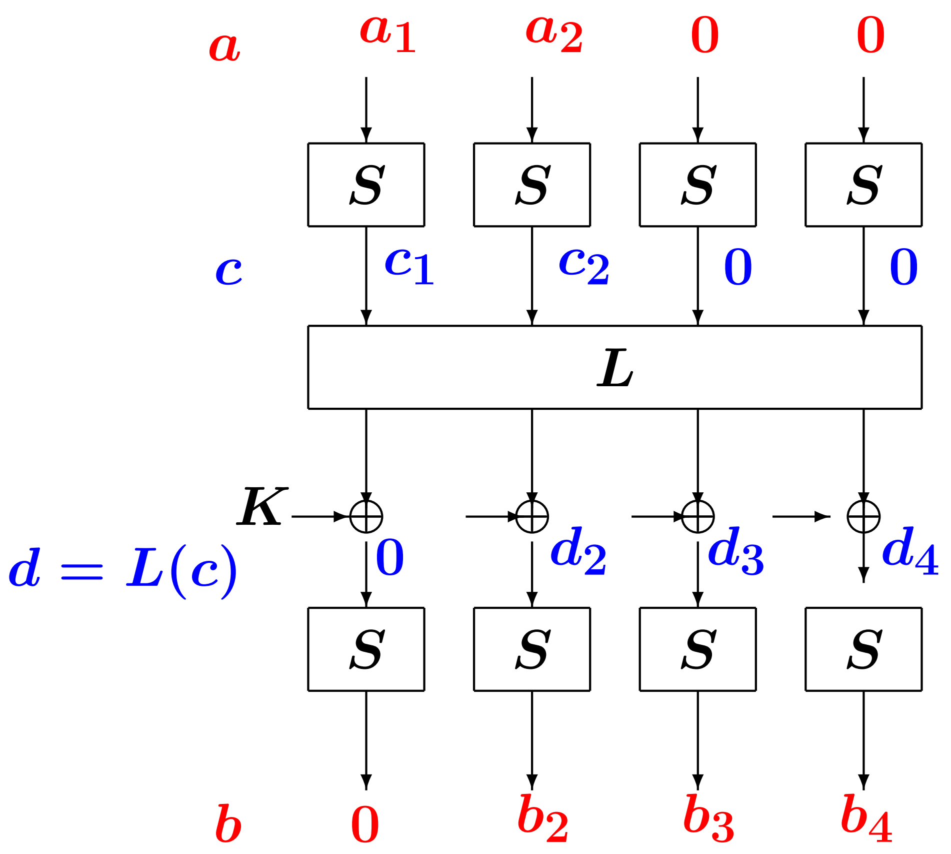
Security criteria for the linear layer

A two-round characteristic



$$\mathrm{EDP}((a, c, L(c), b)) = \prod_{i=1}^{t} \frac{\delta_S(a_i, c_i)}{2^m} \prod_{j=1}^{t} \frac{\delta_S(L(c)_j, b_j)}{2^m}$$

A two-round characteristic



$$\mathrm{EDP}((a, c, L(c), b)) \leq \left(2^{-m}\delta(S)\right)^{wt(c)+wt(L(c))} \leq \left(2^{-m}\delta(S)\right)^{d}$$

Differential branch number of L over $\mathbf{F}_2^m$

minimal number of active Sboxes within a 2-round characteristic

$$d = d_{\min}(\mathcal{C}_L) \text{ where } \mathcal{C}_L = \{(x, L(x)), x \in (\mathbf{F}_2^m)^t\}$$

$\mathcal{C}_L$ is a code over $\mathbf{F}_2^m$ of length $2t$ and size $(2^m)^t$.

Maximizing the differential branch number.

From Singleton's bound,

$$d_{\min}(\mathcal{C}_L) \leq t + 1$$

with equality for MDS codes.

MEDP of a two-round differential

A differential may aggregate many differential characteristics.

Bound on the 2-round MEDP [Hong et al00][Daemen-Rijmen02]:

$$\mathbf{MEDP_2} \leq \left(2^{-m}\delta(S)\right)^{d-1}$$

where d is the differential branch number of L over $\mathbf{F}_2^m$.

AES [Daemen-Rijmen 98][FIPS PUB 197]

In the AES:

- $S(x) = A(x^{254})$ over $\mathbf{F}_{2^8}$ where A is an affine permutation of $\mathbf{F}_2^8$. Then, $\delta(S) = 4$.

- $L =$ `MixColumns` is such that $\mathcal{C}_L$ is an $[8, 4, 5]$ MDS code over $\mathbf{F}_{2^8}$

For any 2-round characteristic Ω,

$$\mathrm{EDP}(\Omega) \leq \left(\frac{\delta(S)}{2^m}\right)^d = 2^{-30}$$

For any 2-round differential (a, b),

$$\mathrm{EDP}(a, b) \leq \left(\frac{\delta(S)}{2^m}\right)^{d-1} = 2^{-24}$$

For linear cryptanalysis

Expected squared correlation (linear potential) of a mask (u, v):

$$\mathrm{ELP}(u,v) = 2^{-2n-\kappa} \sum_{k \in \mathbb{F}_2^\kappa} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot E_k(x)} \right)^2$$

Expected squared correlation of a 2-round linear trail $(a, L^T(c), c, b)$:

$$\mathrm{ELP}((a, L^T(c), c, b)) \le \left(2^{-2m} \mathcal{L}(S)^2\right)^{wt(L^T(c)) + wt(c)} \le \left(2^{-m} \mathcal{L}(S)\right)^{2d'}$$

Linear branch number of L over $\mathbf{F}_2^m$

$$d' = d_{\min}(\mathcal{C}'_L) \text{ where } \mathcal{C}'_L = \{(L^T(x), x), x \in (\mathbf{F}_2^m)^t\}$$

$\mathcal{C}'_L$ is the dual (orthogonal) of $\mathcal{C}_L$:

$$\forall x, y : (L^T(x), x) \cdot (y, L(y)) = L^T(x) \cdot y \oplus x \cdot L(y) = 0$$

Then, $\mathcal{C}'_L$ is MDS if and only if $\mathcal{C}_L$ is MDS.

AES [Daemen-Rijmen 98][FIPS PUB 197]

In the AES:

- $S(x) = A(x^{254})$ over $\mathbf{F}_{2^8}$ where A is an affine permutation of $\mathbf{F}_2^8$.
  Then, $\mathcal{L}(S) = 2^5$.

- $L =$ `MixColumns` is such that $\mathcal{C}_L$ is an $[8, 4, 5]$ MDS code over $\mathbf{F}_{2^8}$

For any 2-round linear trail Ω,

$$\mathrm{ELP}(\Omega) \leq \left(\frac{\mathcal{L}(S)}{2^m}\right)^{2d'} = 2^{-30}$$

For any 2-round linear approximation (a, b),

$$\mathrm{ELP}(a, b) \leq \left(\frac{\mathcal{L}(S)}{2^m}\right)^{2(d'-1)} = 2^{-24}$$

More detailed lecture notes

`https://www.paris.inria.fr/secret/Anne.Canteaut/poly.pdf`