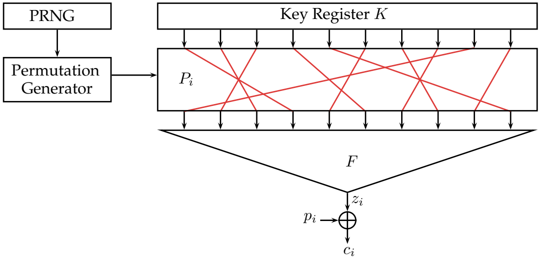
Boolean functions with restricted input and their robustness; application to the FLIP cipher

Claude Carlet, Pierrick Méaux, **Yann Rotella**

Laga, Paris 8 and 13, CNRS, France
ENS Paris, France
Inria - SECRET, Paris, France

FSE 2018

Context: FLIP [Méaux et al., Eurocrypt 2016]



$$\begin{aligned} F(x) &= x_1 + x_2 + \cdots + x_{i_1} \\ &+ x_{i_1+1}x_{i_1+2} + x_{i_1+3}x_{i_1+4} + \cdots x_{i_2-1}x_{i_2} \\ &+ x_{i_2+1} + x_{i_2+2}x_{i_2+3} + x_{i_2+4}x_{i_2+5}x_{i_2+6} + \cdots + x_{n-k}x_{n-k+1}\ldots x_n \end{aligned}$$

Warning

The input of F has always the same Hamming weight.

Example

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$$

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
f	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0

Example

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4$$

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
f	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0

$w_H(x) =$ 0 1 2 3 4

Definitions

Definition (Weightwise Perfectly Balanced Functions)

$$f \text{ is WPB } \Leftrightarrow w_H(f)_k = \frac{\binom{n}{k}}{2}, \ \forall\, 0 < k < n$$

$$\Rightarrow \text{ only if } n = 2^\ell$$

Definitions

Definition (Weightwise Perfectly Balanced Functions)

$$f \text{ is WPB } \Leftrightarrow w_H(f)_k = \frac{\binom{n}{k}}{2}, \ \forall\, 0 < k < n$$

$$\Rightarrow \text{ only if } n = 2^\ell$$

$$f(0,\dots,0) = 0; \quad f(1,\dots,1) = 1.$$

Definitions

Definition (Weightwise Perfectly Balanced Functions)

$$f \text{ is WPB } \Leftrightarrow w_H(f)_k = \frac{\binom{n}{k}}{2}, \ \forall\, 0 < k < n$$

$$\Rightarrow \text{ only if } n = 2^\ell$$

$$f(0,\ldots,0) = 0; \quad f(1,\ldots,1) = 1.$$

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
f	0	1	0	1	0	0	1	1	1	0	1	1	0	0	0	1

Definitions

Definition (Weightwise Almost Perfectly Balanced Functions)

$$f \text{ is WAPB } \Leftrightarrow w_H(f)_k \in \left\{ \frac{\binom{n}{k}}{2}, \frac{\binom{n}{k} \pm 1}{2} \right\}, \forall\, 0 < k < n$$

ANF of weightwise perfectly balanced functions

If f is WPB Boolean function of n variables, then its ANF has

- exactly $n/2$ monomials of degree 1;
- at least $n/4$ monomials of degree 2;
- at least one monomial of degree $n/2$.

ANF of weightwise almost perfectly balanced functions

If f is a WAPB Boolean function of n variables, then its ANF has

- exactly $n/2$ monomials of degree 1 if n is even;
- $(n-1)/2$ or $(n+1)/2$ monomials of degree 1 if n is odd;
- at least $\lfloor n/4 \rfloor$ monomials of degree 2.

Constructions

Let $n = 2^\ell$ and f, g WPB functions with $2^{\ell-1}$ variables, then

$$F(x,y) = f(x) + g(y)$$

is not WPB.

Constructions

Let $n = 2^\ell$,
f, f', g: WPB functions of $2^{\ell-1}$ variables
g': any function of $2^{\ell-1}$ variables, then

$$F(x,y) = f(x) + g(y) + (f(x) + f'(x))g'(y) + \prod_{i=1}^{n} x_i$$

is a WPB function with 2^ℓ variables.

Constructions

Let $n = 2^\ell$,
f, f', g: WPB functions of $2^{\ell-1}$ variables
g': any function of $2^{\ell-1}$ variables, then

$$F(x, y) = f(x) + g(y) + (f(x) + f'(x))g'(y) + \prod_{i=1}^{n} x_i$$

is a WPB function with 2^ℓ variables.

Proof.

Fix y. Then $F(x, y) = f(x) + g(y)$ or $f'(x) + g(y)$.
Problem: when $w_H(x) = 0$ or $n \Rightarrow$ add $\prod_{i=1}^{n} x_i$ □

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

$\Rightarrow f_4(x_1, x_2, x_3, x_4) = f_2(x_1, x_2) + f_2(x_3, x_4) + x_1 x_2 = x_1 + x_3 + x_1 x_2$

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

$\Rightarrow f_4(x_1, x_2, x_3, x_4) = f_2(x_1, x_2) + f_2(x_3, x_4) + x_1 x_2 = x_1 + x_3 + x_1 x_2$

$\Rightarrow f_8(x_1, \ldots, x_8) = f_4(x_1, \ldots, x_4) + f_4(x_5, \ldots, x_8) + x_1 x_2 x_3 x_4$

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

$\Rightarrow f_4(x_1, x_2, x_3, x_4) = f_2(x_1, x_2) + f_2(x_3, x_4) + x_1 x_2 = x_1 + x_3 + x_1 x_2$

$\Rightarrow f_8(x_1, \ldots, x_8) = f_4(x_1, \ldots, x_4) + f_4(x_5, \ldots, x_8) + x_1 x_2 x_3 x_4$

$\Rightarrow f_8(x_1, \ldots, x_8) = x_1 + x_3 + x_5 + x_7 + x_1 x_2 + x_5 x_6 + x_1 x_2 x_3 x_4$

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

$\Rightarrow f_4(x_1, x_2, x_3, x_4) = f_2(x_1, x_2) + f_2(x_3, x_4) + x_1 x_2 = x_1 + x_3 + x_1 x_2$

$\Rightarrow f_8(x_1, \dots, x_8) = f_4(x_1, \dots, x_4) + f_4(x_5, \dots, x_8) + x_1 x_2 x_3 x_4$

$\Rightarrow f_8(x_1, \dots, x_8) = x_1 + x_3 + x_5 + x_7 + x_1 x_2 + x_5 x_6 + x_1 x_2 x_3 x_4$

$\Rightarrow f_{16}(x_1, \dots, x_{16}) = f_8(x_1, \dots, x_8) + f_8(x_9, \dots, x_{16}) + x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8$

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

$\Rightarrow f_4(x_1, x_2, x_3, x_4) = f_2(x_1, x_2) + f_2(x_3, x_4) + x_1 x_2 = x_1 + x_3 + x_1 x_2$

$\Rightarrow f_8(x_1, \dots, x_8) = f_4(x_1, \dots, x_4) + f_4(x_5, \dots, x_8) + x_1 x_2 x_3 x_4$

$\Rightarrow f_8(x_1, \dots, x_8) = x_1 + x_3 + x_5 + x_7 + x_1 x_2 + x_5 x_6 + x_1 x_2 x_3 x_4$

$\Rightarrow f_{16}(x_1, \dots, x_{16}) = f_8(x_1, \dots, x_8) + f_8(x_9, \dots, x_{16}) + x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8$

$$\begin{aligned} f_{16}(x) \quad = \quad & x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13} + x_{15} \\ & + x_1 x_2 + x_5 x_6 + x_9 x_{10} + x_{13} x_{14} \\ & + x_1 x_2 x_3 x_4 + x_9 x_{10} x_{11} x_{12} \\ & + x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 \end{aligned}$$

One particular family of WPB function

For $n = 16$:

$f_2(x_1, x_2) = x_1$ is WPB

$\Rightarrow f_4(x_1, x_2, x_3, x_4) = f_2(x_1, x_2) + f_2(x_3, x_4) + x_1 x_2 = x_1 + x_3 + x_1 x_2$

$\Rightarrow f_8(x_1, \dots, x_8) = f_4(x_1, \dots, x_4) + f_4(x_5, \dots, x_8) + x_1 x_2 x_3 x_4$

$\Rightarrow f_8(x_1, \dots, x_8) = x_1 + x_3 + x_5 + x_7 + x_1 x_2 + x_5 x_6 + x_1 x_2 x_3 x_4$

$\Rightarrow f_{16}(x_1, \dots, x_{16}) = f_8(x_1, \dots, x_8) + f_8(x_9, \dots, x_{16}) + x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8$

$$\begin{aligned} f_{16}(x) &= x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13} + x_{15} \\ &\quad + x_1 x_2 + x_5 x_6 + x_9 x_{10} + x_{13} x_{14} \\ &\quad + x_1 x_2 x_3 x_4 + x_9 x_{10} x_{11} x_{12} \\ &\quad + x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 \end{aligned}$$

$\Rightarrow$ 8 monomials of degree 1, 4 monomials of degree 2, 1 monomial of degree 8.

Definition

Definition

$$\mathrm{NL}(f) = \min_{\deg \ell \leq 1} w_H(f + \ell)$$

Definition

Definition

$$\mathrm{NL}(f) = \min_{\deg \ell \leq 1} w_H(f + \ell)$$

Definition

For any $\mathcal{S} \subseteq \mathbb{F}_2^n$,

$$\mathrm{NL}_{\mathcal{S}}(f) = \min_{\deg \ell \leq 1} w_H(f + \ell)_{\mathcal{S}}$$

Degradation with restricted input

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4$$

Degradation with restricted input

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4$$

σ_2 is a bent function ($\mathrm{NL}(\sigma_2) = 6$)

Degradation with restricted input

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

σ_2 is a bent function ($\mathrm{NL}(\sigma_2) = 6$)

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
σ_2	0	0	0	1	0	1	1	1	0	1	1	1	1	1	1	0

Degradation with restricted input

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

σ_2 is a bent function ($NL(\sigma_2) = 6$)

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
σ_2	0	0	0	1	0	1	1	1	0	1	1	1	1	1	1	0

Degradation with restricted input

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

σ_2 is a bent function ($\mathrm{NL}(\sigma_2) = 6$)

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
σ_2	0	0	0	1	0	1	1	1	0	1	1	1	1	1	1	0

$\mathrm{NL}_2(\sigma_2) = 0$

Non-linearity over fixed Hamming weight

$$\mathcal{S}_{n,k} = \{x \in \mathbb{F}_2^n, w_H(x) = k\}$$

Proposition

For $(n,k) \neq (50,3)$ *nor* $(50,47)$*, we have:*

$$\mathrm{NL}_{\mathcal{S}_{n,k}}(f) < \frac{\binom{n}{k}}{2} - \frac{1}{2}\sqrt{\binom{n}{k}}$$

Non-linearity over fixed Hamming weight

$$\mathcal{S}_{n,k} = \{x \in \mathbb{F}_2^n, w_H(x) = k\}$$

Proposition

For $(n,k) \neq (50,3)$ nor $(50,47)$, we have:

$$\mathrm{NL}_{\mathcal{S}_{n,k}}(f) < \frac{\binom{n}{k}}{2} - \frac{1}{2}\sqrt{\binom{n}{k}}$$

- Improved in [S. Mesnager, 2017].
- Related to the study of punctured Reed and Muller codes [Dumer, Kapralova, 2017].

Definition

Algebraic Immunity over $\mathcal{S}$

Let f be defined over a set $\mathcal{S}$:

$$\mathrm{AI}_{\mathcal{S}}(f) = \min\{\deg(g), g \neq 0 \ \text{over } \mathcal{S} | gf = 0 \text{ or } g(f+1) = 0 \text{ over } \mathcal{S}\}$$

Definition

Algebraic Immunity over $\mathcal{S}$

Let f be defined over a set $\mathcal{S}$:

$$\mathrm{AI}_{\mathcal{S}}(f) = \min\{\deg(g), g \neq 0 \text{ over } \mathcal{S} | gf = 0 \text{ or } g(f+1) = 0 \text{ over } \mathcal{S}\}$$

$$f(x_1, x_2, x_3, x_4) = 1 + x_1 + x_2x_3, \ \mathrm{AI}(f) = 2$$

Definition

Algebraic Immunity over $\mathcal{S}$

Let f be defined over a set $\mathcal{S}$:

$$\mathsf{AI}_{\mathcal{S}}(f) = \min\{\deg(g), g \neq 0 \text{ over } \mathcal{S} | gf = 0 \text{ or } g(f+1) = 0 \text{ over } \mathcal{S}\}$$

$$f(x_1, x_2, x_3, x_4) = 1 + x_1 + x_2x_3, \ \mathsf{AI}(f) = 2$$

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
f	1	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1

$$\mathsf{AI}_2(f) = 1$$

Degradation on restricted input

Let f be a function of n variables.
Let g be a function of m variables.
Let $F(x, y) = f(x) + g(y)$, then for any $k \geq n$ and $k \leq m$,

Degradation on restricted input

Let f be a function of n variables.
Let g be a function of m variables.
Let $F(x,y) = f(x) + g(y)$, then for any $k \geq n$ and $k \leq m$,

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

while

Degradation on restricted input

Let f be a function of n variables.
Let g be a function of m variables.
Let $F(x,y) = f(x) + g(y)$, then for any $k \geq n$ and $k \leq m$,

$$\mathsf{AI}_k(F) \geq \mathsf{AI}(f) - \deg(g)$$

while

$$\mathsf{AI}(F) \geq \max(\mathsf{AI}(f), \mathsf{AI}(g))$$

Degradation on restricted input

Let f be a function of n variables.
Let g be a function of m variables.
Let $F(x, y) = f(x) + g(y)$, then for any $k \geq n$ and $k \leq m$,

$$\mathrm{AI}_k(F) \geq \mathrm{AI}(f) - \deg(g)$$

while

$$\mathrm{AI}(F) \geq \max(\mathrm{AI}(f), \mathrm{AI}(g))$$

Upper bounds

We proved upper bounds on $\mathrm{AI}_k(f)$ (see Paper).

Bias of FLIP?

Range of Hamming weights of the key such that the bias is undetectable for the recommended security level.

Instances	k_{min}	k_{max}
FLIP-530	78	482
FLIP-662	102	621
FLIP-1394	207	1325
FLIP-1704	257	1643

Non-linearity in FLIP.

Proposition

Let $F(x,y) = f(x) + g(y)$, *then*

$$\mathrm{NL}_k(F) \geq \sum_{i=0}^{k} \binom{n}{i} \mathrm{NL}_{k-i}(g) + \sum_{i=0}^{k} \mathrm{NL}_i(f) \left(\binom{m}{k-i} - 2\mathrm{NL}_{k-i}(g) \right)$$

Range of Hamming weights of the key such that the bias is smaller than 2^{-10}:

Instances	k_{min}	k_{max}
FLIP-530	107	464
FLIP-662	136	556
FLIP-1394	221	1239
FLIP-1704	266	1492

Algebraic Immunity in FLIP

We obtain a lower bound on the algebraic immunity of the function used in FLIP (only when k is close to $n/2$):

Instances	$\mathrm{AI}(f)$	Bound of $\mathrm{AI}_k(f)$
FLIP-530	9	≥ 4
FLIP-662	15	≥ 6
FLIP-1394	16	≥ 6
FLIP-1704	23	≥ 8

Those bounds are not tight, but they guarantee resistance against algebraic attacks.

Conclusion

- We defined weightwise (almost) perfectly balanced Boolean functions and provided constructions.
- We defined and gave bounds on AI_k and NL_k.
- We gave properties on direct sums.
- We eventually gave bounds on the exact cryptographic parameters of the 4 FLIP instances.

Conclusion

- We defined weightwise (almost) perfectly balanced Boolean functions and provided constructions.
- We defined and gave bounds on AI_k and NL_k.
- We gave properties on direct sums.
- We eventually gave bounds on the exact cryptographic parameters of the 4 FLIP instances.

But... be careful!

Conclusion

- We defined weightwise (almost) perfectly balanced Boolean functions and provided constructions.
- We defined and gave bounds on AI_k and NL_k.
- We gave properties on direct sums.
- We eventually gave bounds on the exact cryptographic parameters of the 4 FLIP instances.

But... be careful!

Thank you !