Open problem in boolean functions

Finding Dahus

Yann Rotella

Université de Versailles Saint Quentin en Yvelines

Frisiacrypt 2022, Terschelling, The Netherlands

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

Resiliency

A function f is said k-resilient if and only if for any g with less than k variables,

$$f(x_0, x_1, \dots, x_{n-1}) + g(x_{i_0}, x_{i_1}, \dots, x_{i_{k-1}})$$

is balanced.

RESILIENCY

A function f is said k-resilient if and only if for any g with less than k variables,

$$f(x_0, x_1, \ldots, x_{n-1}) + g(x_{i_0}, x_{i_1}, \ldots, x_{i_{k-1}})$$

is balanced. This is equivalent to say that

$$W_f(a) = 0$$

for all a of Hamming weight smaller than or equal to k [Car21].

Resiliency

A function f is said k-resilient if and only if for any g with less than k variables,

$$f(x_0, x_1, \ldots, x_{n-1}) + g(x_{i_0}, x_{i_1}, \ldots, x_{i_{k-1}})$$

is balanced. This is equivalent to say that

$$W_f(a) = 0$$

for all a of Hamming weight smaller than or equal to k [Car21].

Example :

$$f = x_0 x_1 x_2 + x_3 + x_4$$

Algebraic Immunity

The algebraic immunity of a Boolean function f is

$$\mathrm{AI}(f) = \min_{g \neq 0} \{\deg(g) | fg = 0 \text{ or } g(f+1) = 0\}$$

Algebraic Immunity

The algebraic immunity of a Boolean function f is

$$\mathrm{AI}(f) = \min_{g \neq 0} \{\deg(g) | fg = 0 \text{ or } g(f+1) = 0\}$$

Example :

$$f = x_0 x_1 x_2 + x_3 + x_4$$

Degree and Resiliency [Sieg84]

Let f be an n-variable Boolean function, then when $\deg(f) > 1$,

$$\deg(f) + \mathrm{res}(f) \leq n - 1$$

Degree and Resiliency [Sieg84]

Let f be an n-variable Boolean function, then when $\deg(f) > 1$,

$$\deg(f) + \mathrm{res}(f) \leq n - 1$$

Example :

$$f = x_0 x_1 x_2 + x_3 + x_4$$

Bound on algebraic immunity

For any f with n variables,

$$\mathrm{AI}(f) \leq \lceil n/2 \rceil$$

BOUND ON ALGEBRAIC IMMUNITY

For any f with n variables,

$$\mathrm{AI}(f) \leq \lceil n/2 \rceil$$

Example :

$$f = x_0 x_1 x_2 + x_3 + x_4$$

GOLDREICH'S PRNG [G00]

- Seed is $x_1, x_2, \ldots, x_n$
- For any output bit $y_i = f(x_{i_1}, x_{i_2}, \ldots, x_{i_c})$

Goldreich's PRNG [G00]

- Seed is $x_1, x_2, \ldots, x_n$
- For any output bit $y_i = f(x_{i_1}, x_{i_2}, \ldots, x_{i_c})$

Question : How much can you output with $f = x_0 x_1 x_2 + x_3 + x_4$?

GOLDREICH'S PRNG [G00]

- Seed is $x_1, x_2, \ldots, x_n$
- For any output bit $y_i = f(x_{i_1}, x_{i_2}, \ldots, x_{i_c})$

Question : How much can you output with $f = x_0 x_1 x_2 + x_3 + x_4$?

resiliency and algebraic immunity

Open problem

On the algebraic immunity - Resiliency trade-off, implications for Goldreich's Pseudorandom Generator - A. Dupin, P. Méaux and M. Rossi - eprint 2021/649

Open problem

On the algebraic immunity - Resiliency trade-off, implications for Goldreich's Pseudorandom Generator - A. Dupin, P. Méaux and M. Rossi - eprint 2021/649

Conjecture

For all $0 \leq k \leq \ell$, for all $n > k+1$, there exists an n-variable function such that

$$\mathrm{res}(f) = k \text{ and } \mathrm{AI}(f) = \min(\lceil n/2 \rceil, n-k-1)$$

Why is it interesting ?

- The two criteria are used differently

Why is it interesting ?

- The two criteria are used differently
- Previous constructions do not work

Why is it interesting?

- The two criteria are used differently
- Previous constructions do not work
- Exhaustively checked up to 6 variables

Why is it interesting?

- The two criteria are used differently
- Previous constructions do not work
- Exhaustively checked up to 6 variables
- Goal is more precise