



**On the
Algebraic
Immunity of
Symmetric
Boolean
Functions**

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

*On the Algebraic Immunity of Symmetric
Boolean Functions*

An Braeken Bart Preneel

Katholieke Universiteit Leuven
Dept. Elect. Eng.-ESAT/SCD-COSIC
Belgium

DIAMANT/EIDMA symposium 2005



OUTLINE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

1 INTRODUCTION

- Motivation
- Background

2 ALGORITHM

- Annihilators
- Properties

3 MAXIMUM AI

- Classes
- Properties of classes

4 CONCLUSIONS



OUTLINE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

1 INTRODUCTION

- Motivation
- Background

2 Algorithm

- Annihilators
- Properties

3 Maximum AI

- Classes
- Properties of classes

4 Conclusions



KEY STREAM GENERATOR

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

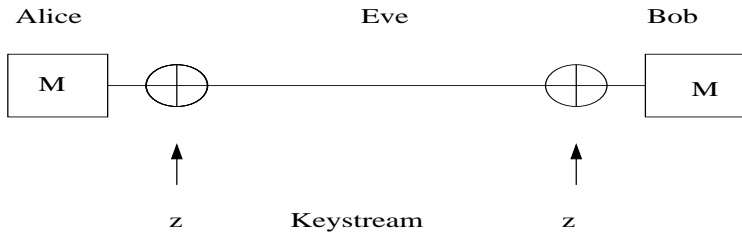
Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions





ONE-TIME PAD

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

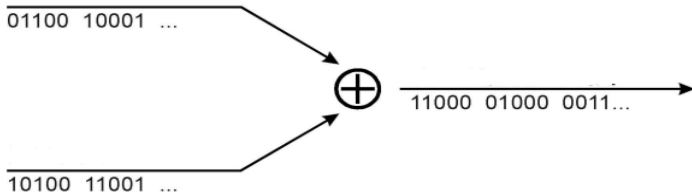
Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions





MOTIVATION

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken, Bart Preneel

Introduction

Motivation
Background

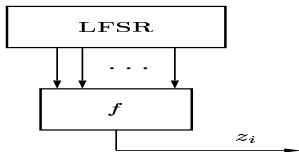
Algorithm

Annihilators
Properties

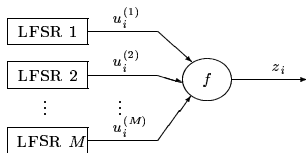
Maximum AI

Classes
Properties of classes

Conclusions



Filter generator



Combination generator



MOTIVATION: ALGEBRAIC ATTACKS

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

System of nonlinear equations in key and output variables.

$$z_i = f(L^i(\bar{k}))$$

- Use low degree functions g : $f \cdot g = \bar{0}$
 $\Rightarrow z_i g(L^i(\bar{k})) = 0$
- Use low degree functions h : $(f \oplus \bar{1}) \cdot h = \bar{0}$
 $\Rightarrow (z_i \oplus 1)h(L^i(\bar{k})) = 0$



BOOLEAN FUNCTION

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

DEFINITION

The lowest degree of function g for which $f \cdot g = \bar{0}$ or $(f \oplus \bar{1}) \cdot g = \bar{0}$ is called the **algebraic immunity (AI)** of f .
The function g for which $f \cdot g = \bar{0}$ is called annihilator of f .

- $AI(f) \leq \lceil \frac{n}{2} \rceil$
- Attack complexity is exponential in AI



SYMMETRIC BOOLEAN FUNCTION

- Function value of all vectors with the same weight is equal
 $\Rightarrow \mathbb{V}\mathbb{V}: v_f = (v_f(0), \dots, v_f(n))$
- ANF in terms of homogeneous polynomials σ_k ,
 $0 \leq k \leq n$

$$\sigma_k(x_0, \dots, x_{n-1}) = \bigoplus_{0 < i_1 < \dots < i_k} x_{i_1} \cdots x_{i_k}$$

\Rightarrow SANF :

$$f(\bar{x}) = \bigoplus_{k=0}^n \lambda_f(k) \sigma_k, \lambda_f(k) = \sum_{i \leq k} v_f(i), \text{ for } 0 \leq k \leq n$$

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

Introduction

Motivation

Background

Algorithm

Annihilators

Properties

Maximum AI

Classes

Properties of
classes

Conclusions



SYMMETRIC BOOLEAN FUNCTION

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation

Background

Algorithm

Annihilators

Properties

Maximum AI

Classes

Properties of classes

Conclusions

Examples:

- $v_{\sigma_0} = (1, 1, 1, 1, \dots)$
 $v_{\sigma_1} = (0, 1, 0, 1, 0, 1, \dots)$
 $v_{\sigma_2} = (0, 0, 1, 1, 0, 0, 1, 1, \dots)$
 $v_{\sigma_4} = (0, 0, 0, 0, 1, 1, 1, 1, \dots)$
- $\sigma_{\bar{a}} = \sigma_{2^{a_0}} \sigma_{2^{a_1}} \cdots \sigma_{2^{a_{n-1}}} \Rightarrow v_{\sigma_a} = v_{\sigma_{2^{a_0}}} \cdots v_{\sigma_{2^{a_{n-1}}}}$
e.g. $v_{\sigma_3} = v_{\sigma_1} v_{\sigma_2} = (0, 0, 0, 1, 0, 0, 0, 1, \dots)$



OUTLINE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

- 1 Introduction
 - Motivation
 - Background
- 2 **ALGORITHM**
 - Annihilators
 - Properties
- 3 Maximum AI
 - Classes
 - Properties of classes
- 4 Conclusions



ALGORITHM FOR AI

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

■ Complexity $\frac{1}{8} \binom{n}{d}^w$

? Is there any structure in annihilators of symmetric function?



ANNIHILATORS

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

Annihilator of f : $f \cdot g = \bar{0}$

- $f(\bar{x}) = 1 \Rightarrow g(\bar{x}) = 0$
- $f(\bar{x}) = 0 \Rightarrow g(\bar{x}) = 0/1$

Annihilator: $\underbrace{\{x_0, \dots, x_{k-1}\}}_{\text{Pol } p} \underbrace{\{x_k, \dots, x_{n-1}\}}_{\text{sym } \sigma}$

- $\text{sup}(\sigma) = \{\bar{v} : \text{wt}(\bar{v}) \in \{i_1, \dots, i_k\}\}$
- $\text{sup}(p) \subseteq \{\bar{v} : \text{wt}(\bar{v}) = l\}$

$\Rightarrow \text{sup}(g) \subseteq \{\bar{v} : \text{wt}(\bar{v}) \in \{i_1 + l, \dots, i_k + l\}\}$



DEFINITIONS

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

- σ_i^j = hom. sym. pol. of degree i in $\{x_{n-j}, \dots, x_{n-1}\}$
- P_l^k = pol. in $\{x_0, \dots, x_{k-1}\}$, product of at most l factors of
 - complement of 1 variable
 - 1 variable
 - sum of 2 variables

Example P_4^6 :

- $(x_1 \oplus x_2)(x_3 \oplus x_4)(x_5 \oplus x_6)$
- $(x_1 \oplus 1)x_2(x_3 \oplus x_4)(x_5 \oplus x_6)$
- $(x_1 \oplus 1)(x_2 \oplus 1)(x_3 \oplus x_4)(x_5 \oplus x_6)$
- $x_1 x_2 (x_3 \oplus x_4)(x_5 \oplus x_6)$



POLYNOMIAL SET AN_S

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

n even:

$$\blacksquare \sigma_0^2 P_{\frac{n}{2}-1}^{n-2}, \sigma_0^3 P_{\frac{n}{2}-1}^{n-3}, \dots, \sigma_0^{n-1} P_{\frac{n}{2}-1}^1, \sigma_0$$

$$\blacksquare \sigma_1^4 P_{\frac{n}{2}-2}^{n-4}, \dots, \sigma_1^{n-1} P_{\frac{n}{2}-2}^1, \sigma_1$$

\vdots

$$\blacksquare \sigma_{\frac{n}{2}-2}^{n-2} P_1^2, \sigma_{\frac{n}{2}-2}^{n-1} P_1^1, \sigma_{\frac{n}{2}-2}$$

$$\blacksquare \sigma_{\frac{n}{2}-1}$$



POLYNOMIAL SET AN_S

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken, Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

n odd:

$$\blacksquare \sigma_0^1 P_{\lfloor \frac{n}{2} \rfloor - 1}^{n-1}, \sigma_0^2 P_{\lfloor \frac{n}{2} \rfloor - 1}^{n-2}, \dots, \sigma_0^{n-1} P_{\lfloor \frac{n}{2} \rfloor - 1}^1, \sigma_0$$

$$\blacksquare \sigma_1^3 P_{\lfloor \frac{n}{2} \rfloor - 2}^{n-3}, \dots, \sigma_1^{n-1} P_{\lfloor \frac{n}{2} \rfloor - 2}^1, \sigma_1 \vdots$$

$$\blacksquare \sigma_{\lfloor \frac{n}{2} \rfloor - 2}^{n-2} P_1^2, \sigma_{\lfloor \frac{n}{2} \rfloor - 2}^{n-1} P_1^1, \sigma_{\lfloor \frac{n}{2} \rfloor - 2}$$

$$\blacksquare \sigma_{\lfloor \frac{n}{2} \rfloor - 1}$$



THEOREM

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken, Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

THEOREM

One of the lowest degree annihilators of a symmetric function can be constructed by means of a linear combination of the polynomials in AN_S .

- Symmetric part: vectors of same weight are zero
- Polynomial part: is equal to one for subset of vectors with exactly same weight



EXAMPLE

f is symmetric function in \mathbb{F}_2^{16}

- $v_f(6) = v_f(7) = v_f(10) = v_f(11) = 0$
 $\Rightarrow g = \sigma_2^9 x_0(x_1 \oplus x_2)(x_3 \oplus x_4)(x_5 \oplus x_6)$ is annihilator of f
 - σ_2^9 is equal to 1: vectors with weight $\in \{2, 3, 6, 7\}$.
 - $x_0(x_1 \oplus x_2)(x_3 \oplus x_4)(x_5 \oplus x_6)$ is equal to 1: subset of vectors with weight 4
- $\Rightarrow g$ is equal to 1: subset of vectors with weight $\in \{6, 7, 10, 11\}$

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions



EXAMPLE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

f is symmetric function in \mathbb{F}_2^{10}

- $v_f(2) = v_f(6) = 0$
 $\Rightarrow (\mathbf{x}_0 \oplus 1)(\sigma_2^9 \oplus \sigma_3^9)$ is annihilator of f
- $v_f(2) = v_f(6) = 1$
 $\Rightarrow (\mathbf{x}_0 \oplus 1)(\sigma_2^9 \oplus \sigma_3^9)$ is annihilator of $f \oplus \bar{1}$



ALGORITHM

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

$$\blacksquare N = 2 \sum_{i=1}^{\lceil \frac{n}{2} \rceil - 1} (2^i - 1) + 2^{\lceil \frac{n}{2} \rceil} - 1$$

\Rightarrow Complexity: $N^{2.81}$

TABLE: Comparison of the size of annihilator-set

n	10	12	14	16	18
$\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$	386	1 586	6 476	26 333	106 762
$ \text{AN}_S $	83	177	376	1 005	2 539

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions



PROPERTY 1

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

THEOREM

Let f be a symmetric Boolean function on \mathbb{F}_2^n with value vector v_f . If $v_f(\lfloor \frac{n}{2} \rfloor - 1) = v_f(\lfloor \frac{n}{2} \rfloor + 1)$ for all n , or in addition for n odd $v_f(\lfloor \frac{n}{2} \rfloor - 2) = v_f(\lfloor \frac{n}{2} \rfloor)$, then f can not have maximum AI.

Example $n = 7$:

- $(x_0 \oplus x_1)(x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6)$
 $\Rightarrow \text{weight} \in \{3, 5\}$
- $(x_0 \oplus x_1)(x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6 \oplus 1)$
 $\Rightarrow \text{weight} \in \{2, 4\}$



PROPERTY 2

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

THEOREM

For $n = 2^{j+1} - 1$ where $j \geq 1$, the value vector of f should be of the form $(\bar{a}|\bar{a}^c)$ where $\bar{a} \in \mathbb{F}_2^j$ in order to reach the maximum AI.

Example: $n = 7$

- $\sigma_3 \Rightarrow \text{weight} \in \{3, 7\}$
- $\sigma_2 \oplus \sigma_3 \Rightarrow \text{weight} \in \{2, 6\}$
- $\sigma_1 \oplus \sigma_3 \Rightarrow \text{weight} \in \{1, 5\}$
- $\sigma_0 \oplus \sigma_1 \oplus \sigma_2 \oplus \sigma_3 \Rightarrow \text{weight} \in \{0, 4\}$



PROPERTY 3

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

THEOREM

Let f be a Boolean function on \mathbb{F}_2^n . If $wt(f) < \sum_{i=0}^d \binom{n}{i}$ or $2^n - wt(f) < \sum_{i=0}^d \binom{n}{i}$, then the AI of f is less or equal than d .

- n odd \Rightarrow only balanced Boolean functions



EXPERIMENTS

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

- n odd ($n \leq 17$):

$$v_f(i) = \begin{cases} 0 & \text{for } i < \lceil \frac{n}{2} \rceil \\ 1 & \text{for } i \geq \lceil \frac{n}{2} \rceil. \end{cases}$$

- n even: different classes



OUTLINE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

- 1 Introduction
 - Motivation
 - Background
- 2 Algorithm
 - Annihilators
 - Properties
- 3 **MAXIMUM AI**
 - Classes
 - Properties of classes
- 4 Conclusions



AFFINE EQUIVALENCE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

- $f(\bar{x})$ and $f(\bar{x}A \oplus \bar{b})$, where A is an $n \times n$ nonsingular matrix and $\bar{b} \in \mathbb{F}_2^n$ will have the same AI.
- $f(\bar{x})$ and $f(\bar{x}A \oplus \bar{b})$ are symmetric if and only if
 - $\bar{b} \in \{\bar{0}, \bar{1}\}$
 - n even: A has property that the sum of the elements in each row and column of A is equal to $n - 1$



CLASS 1

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

THEOREM

The symmetric function f in \mathbb{F}_2^n with value vector

$$v_f(i) = \begin{cases} 0 & \text{for } i < \lceil \frac{n}{2} \rceil \\ 1 & \text{else} \end{cases} \quad (1)$$

has maximum AI.

Example $v_f = (0, 0, 0, 0, 1, 1, 1, 1)$, for $n = 7$

Example $v_f = (0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$, for $n = 8$



CLASS 1

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

- Annihilators of $f \oplus \bar{1}$:

$$\{x_{i_1} \cdots x_{i_{\lceil \frac{n}{2} \rceil}} : \text{with } 0 \leq i_1 < i_2 < \cdots < i_{\lceil \frac{n}{2} \rceil} \leq n-1\}$$

⇒ Number of terms in annihilator?



CLASS 2

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

- $n = 8$: $v_f = (1, 0, 0, 0, 1, 1, 1, 1, 0)$
- $n = 10$: $v_f = (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$
- $n = 12$: $v_f = (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$
- \vdots



PROPERTIES OF MAX AI FUNCTIONS

On the
Algebraic
Immunity of
Symmetric
Boolean
Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

TABLE: Properties of Symmetric function on \mathbb{F}_2^n with Maximum AI for n even

Function	Degree	weight	$\max W_f $
Class 1	$2^{\lceil \log_2 n \rceil}$	$2^{n-1} + \frac{1}{2} \binom{n}{\frac{n}{2}}$	$\binom{n}{\frac{n}{2}}$
Class 2	$2^{\lceil \log_2 n \rceil}$	$2^{n-1} + \frac{1}{2} \binom{n}{\frac{n}{2}}$	$\binom{n}{\frac{n}{2}}$
Class 3	$\geq n - i$	$2^{n-1} + \frac{1}{2} \binom{n}{\frac{n}{2}} - \binom{n}{n-i}$	$\binom{n}{\frac{n}{2}} - 2 \binom{n}{n-i}$



OUTLINE

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of classes

Conclusions

- 1 Introduction
 - Motivation
 - Background
- 2 Algorithm
 - Annihilators
 - Properties
- 3 Maximum AI
 - Classes
 - Properties of classes
- 4 CONCLUSIONS



CONCLUSIONS

On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken,
Bart Preneel

Introduction

Motivation
Background

Algorithm

Annihilators
Properties

Maximum AI

Classes
Properties of
classes

Conclusions

There exist symmetric functions with

- maximum algebraic immunity
- nonlinearity is very small

⇒ In practice: together with secondary construction