Classification of All t-Resilient Boolean Functions with $t + 4$ Variables

CASA
Cyber Security in the Age of Large-Scale Adversaries

FSE 2024, Leuven, Belgium, March 29, 2024.

Shahram Rasoolzadeh
Ruhr University Bochum

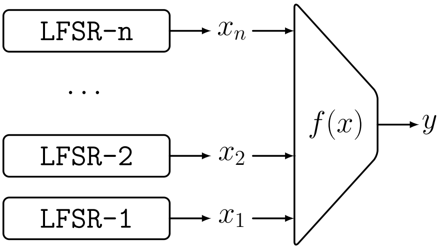
RUHR UNIVERSITÄT BOCHUM RUB

Gefördert durch DFG Deutsche Forschungsgemeinschaft

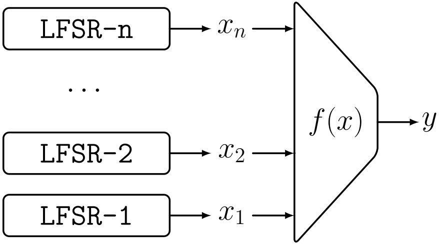
Horst Görtz Institut

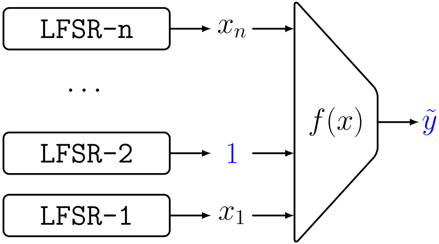
Preliminaries

Resilient Functions

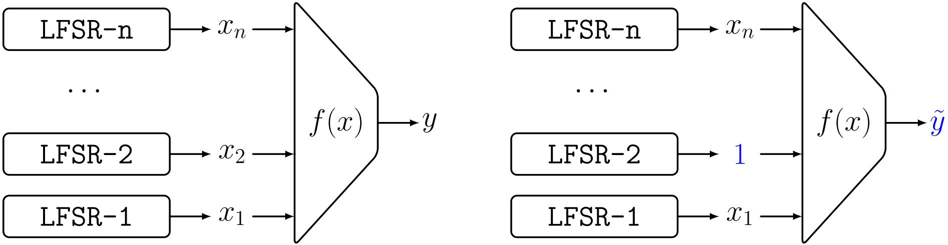


Resilient Functions





Resilient Functions

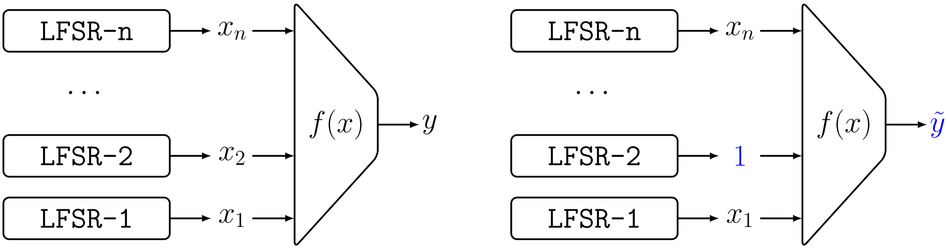


Definition 1: Resilient Boolean Function [Sie84]

Let f to be a **balanced** Boolean function:

$$f \text{ is } t\text{-resilient} \quad \Leftrightarrow \quad \widehat{f}(u) = 0 \;\; \forall u \text{ with } \mathrm{hw}(u) \leq t\,.$$

Resilient Functions



Definition 1: Resilient Boolean Function [Sie84]

Let f to be a **balanced** Boolean function:

$$f \text{ is } t\text{-resilient} \quad \Leftrightarrow \quad \widehat{f}(u) = 0 \;\; \forall u \text{ with } \operatorname{hw}(u) \leq t\,.$$

Walsh Transform: $\widehat{f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, u \rangle}$

Equivalence Relation

CASA
Cyber Security in the Age of Large-Scale Adversaries

Definition 2: Extended Variable-Permutation Equivalence

Let f and g to be two Boolean functions:

$$f \sim g \qquad \Leftrightarrow \qquad \forall x \in \mathbb{F}_2^n, \quad g(x) = f \circ P(x \oplus a) \oplus b$$

with P, a mapping corresponding to a permutation of n variables, and $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$.

Equivalence Relation

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Definition 2: Extended Variable-Permutation Equivalence

Let f and g to be two Boolean functions:

$$f \sim g \qquad \Leftrightarrow \qquad \forall x \in \mathbb{F}_2^n, \quad g(x) = f \circ P(x \oplus a) \oplus b$$

with P, a mapping corresponding to a permutation of n variables, and $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$.

Definition 3: Representative Function

For each class of equivalence relation, it is **the lexicographically smallest** one.

Equivalence Relation

CASA — Cyber Security in the Age of Large-Scale Adversaries

Definition 2: Extended Variable-Permutation Equivalence

Let f and g to be two Boolean functions:

$$f \sim g \qquad \Leftrightarrow \qquad \forall x \in \mathbb{F}_2^n, \quad g(x) = f \circ P(x \oplus a) \oplus b$$

with P, a mapping corresponding to a permutation of n variables, and $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$.

Definition 3: Representative Function

For each class of equivalence relation, it is **the lexicographically smallest** one.

Lemma 1:

$$f \text{ is } t\text{-resilient and } f \sim g \quad \Rightarrow \quad g \text{ is } t\text{-resilient}$$

Algebraic Degree

Algebraic Degree

Lemma 2 [Sie84]:

$$f \text{ is } t\text{-resilient} \;\Rightarrow\; \deg(f) = \begin{cases} n - t - 1 & \text{if } t < n - 1\,, \\ 1 & \text{if } t = n - 1\,. \end{cases}$$

Algebraic Degree

CASA
Cyber Security in the Age of Large-Scale Adversaries

Lemma 2 [Sie84]:

$$f \text{ is } t\text{-resilient} \quad \Rightarrow \quad \deg(f) = \begin{cases} n-t-1 & \text{if } t < n-1\,, \\ 1 & \text{if } t = n-1\,. \end{cases}$$

$(n-1)$-Resilient Function:

$$f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$$

Algebraic Degree

Lemma 2 [Sie84]:

$$f \text{ is } t\text{-resilient} \quad \Rightarrow \quad \deg(f) = \begin{cases} n-t-1 & \text{if } t < n-1\,, \\ 1 & \text{if } t = n-1\,. \end{cases}$$

$(n-1)$-Resilient Function:

$$f(x_1, \ldots, x_n) = x_1 \oplus \ldots \oplus x_n$$

$(n-2)$-Resilient Function:

$$f(x_1, \ldots, x_n) = x_2 \oplus \ldots \oplus x_n$$

Siegenthaler's Construction [Sie84]

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 1

Let f to be a balanced Boolean function with $n+1$ variables:

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 \,.$$

Siegenthaler's Construction [Sie84]

CASA
Cyber Security in the Age of Large-Scale Adversaries

Theorem 1

Let f to be a balanced Boolean function with $n+1$ variables:

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2\,.$$

f is a $(t+1)$-resilient if and only if

- *both f_0 and f_1 are t-resilient functions, and*
- *for any $\alpha \in \mathbb{F}_2^n$ with $\mathrm{hw}(\alpha) = t+1$, $\widehat{f_1}(\alpha) = -\widehat{f_0}(\alpha)$.*

Siegenthaler's Construction [Sie84]

CASA
Cyber Security in the Age of Large-Scale Adversaries

Theorem 1

Let f to be a balanced Boolean function with $n+1$ variables:

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 .$$

f is a $(t+1)$-resilient if and only if

- *both f_0 and f_1 are t-resilient functions, and*
- *for any $\alpha \in \mathbb{F}_2^n$ with $\mathrm{hw}(\alpha) = t+1$, $\widehat{f_1}(\alpha) = -\widehat{f_0}(\alpha)$.*

Definition 4: Type-1 Extension

$$f_1(x) = f_0(x) \oplus 1 \quad \Rightarrow \quad f(x, x_{n+1}) = f_0(x) \oplus x_{n+1}$$

$(n-3)$-Resilient Functions [CCCS91]

- $f(x_1, \ldots, x_n) = x_3 \oplus \ldots \oplus x_n \qquad (n \geq 3)\,,$
- $f(x_1, \ldots, x_n) = x_1x_2 \oplus x_3 \oplus \ldots \oplus x_n \qquad (n \geq 3)\,,$
- $f(x_1, \ldots, x_n) = x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus \ldots \oplus x_n \qquad (n \geq 3)\,,$
- $f(x_1, \ldots, x_n) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus \ldots \oplus x_n \qquad (n \geq 3)\,,$
- $f(x_1, \ldots, x_n) = x_1x_2 \oplus x_1x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_3 \oplus \ldots \oplus x_n \qquad (n \geq 4)\,.$

$(n-4)$-Resilient Functions

$(n-4)$-Resilient Functions

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 2 (Tarannikov and Kirienko [TK00])

Any $(n-m)$-resilient n-variable representative function is in the form of

$$g(x_1, \ldots, x_q) \oplus x_{q+1} \oplus \ldots \oplus x_n \quad \textit{with} \quad q \leq p(m).$$

$(n-4)$-Resilient Functions

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 2 (Tarannikov and Kirienko [TK00])

Any $(n-m)$-resilient n-variable representative function is in the form of

$$g(x_1, \ldots, x_q) \oplus x_{q+1} \oplus \ldots \oplus x_n \quad \textit{with} \quad q \leq p(m).$$

Example

$$p(3) = 4$$

$(n-4)$-Resilient Functions

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 2 (Tarannikov and Kirienko [TK00])

Any $(n-m)$-resilient n-variable representative function is in the form of

$$g(x_1, \ldots, x_q) \oplus x_{q+1} \oplus \ldots \oplus x_n \quad \textit{with} \quad q \leq p(m).$$

Example

$$p(3) = 4$$

Tarannikov & Kirienko [TK00]

$$p(4) = 10$$

An Algorithm for Classifying $(n-m)$-Resilient Functions

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 \,.$$

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2\,.$$

- $\mathcal{R}_{n,t}$: the set of t-resilient n-variable functions

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 \,.$$

- $\mathcal{R}_{n,t}$: the set of t-resilient n-variable functions
- $\mathcal{R}^*_{n,t}$: the set of **representative** t-resilient n-variable functions

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 \,.$$

- $\mathcal{R}_{n,t}$: the set of t-resilient n-variable functions
- $\mathcal{R}^*_{n,t}$: the set of **representative** t-resilient n-variable functions
- $\mathcal{R}^\dagger_{n,t}$: the set of **non-type-1 extension representative** t-resilient n-variable functions

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2\,.$$

- $\mathcal{R}_{n,t}$: the set of t-resilient n-variable functions
- $\mathcal{R}^*_{n,t}$: the set of **representative** t-resilient n-variable functions
- $\mathcal{R}^\dagger_{n,t}$: the set of **non-type-1 extension representative** t-resilient n-variable functions

Computational Complexity of Building $\mathcal{R}^\dagger_{n+1,t+1}$: $\quad |\mathcal{R}_{n,t}|^2$

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2\,.$$

Lemma 3:

$$f \text{ is representative} \quad \Rightarrow \quad f_0 \text{ is representative}\,.$$

Basic Approach

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 .$$

Lemma 3:

$$f \text{ is representative} \quad \Rightarrow \quad f_0 \text{ is representative} .$$

$\Rightarrow$ Comp. Comp.: $|\mathcal{R}^*_{n,t}| \cdot |\mathcal{R}_{n,t}|$

Basic Approach

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Siegenthaler's Construction

$$f(x, x_{n+1}) = \overline{x_{n+1}} \cdot f_0(x) \oplus x_{n+1} \cdot f_1(x) \quad \forall\, x \in \mathbb{F}_2^n \text{ and } x_{n+1} \in \mathbb{F}_2 \,.$$

Lemma 3:

$$f \text{ is representative} \quad \Rightarrow \quad f_0 \text{ is representative} \,.$$

$\Rightarrow$ Comp. Comp.: $|\mathcal{R}^*_{n,t}| \cdot |\mathcal{R}_{n,t}|$

$\Rightarrow$ Comp. Comp.: $|\mathcal{R}^*_{n,t}| \cdot |\mathcal{R}^*_{n,t}| \cdot 2^{n+1} \cdot n!$

Technique 1

Lemma 4:

In Siegenthaler's construction:

$$f_0 \text{ is a type-1 extension} \quad \Rightarrow \quad f \notin \mathcal{R}^{\dagger}_{n+1,t+1}$$

i.e., f cannot be a non-type-1 representative resilient function.

Technique 1

Lemma 4:

In Siegenthaler's construction:

$$f_0 \text{ is a type-1 extension} \quad \Rightarrow \quad f \notin \mathcal{R}^{\dagger}_{n+1,t+1}$$

i.e., f cannot be a non-type-1 representative resilient function.

$\Rightarrow$ Comp. Comp.: $\left(|\mathcal{R}^{\dagger}_{n,t}| \cdot |\mathcal{R}^{*}_{n,t}|\right) \cdot \left(2^{n+1} \cdot n!\right)$

Technique 3

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Lemma 6:

In Siegenthaler's construction,
the two functions f_0 and f_1 from $\mathcal{R}_{n,t}$ can form a function in $\mathcal{R}_{n+1,t+1}$, if

$$\{|\widehat{f_0^*}(\alpha)| \mid \alpha \in \mathbb{F}_2^n, \mathrm{hw}(\alpha) = t+1\} = \{|\widehat{f_1^*}(\alpha)| \mid \alpha \in \mathbb{F}_2^n, \mathrm{hw}(\alpha) = t+1\}$$

Results on the Number of Representative Pairs

Number of representative pairs to be considered for building $\mathcal{R}^{\dagger}_{n,n-4}$

n	5	6	7	8	9	10	11
N_0	1 711	32 896	167 331	259 560	284 635	289 180	289 941
N_1	1 429	26 385	89 855	43 874	8 009	773	62
N_2	1 266	24 356	79 631	28 450	1 919	61	3
N_3	133	1 911	6 423	1 779	149	8	1

Computations for Each Representative Pair

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

For each representative pair (f_0^*, f_1^*), we need to consider all equivalent functions to f_1^*.

$$f_1(x) = f_1^* \circ P(x \oplus a) \oplus b$$

with P, a mapping corresponding to a permutation of n variables, $a \in \mathbb{F}_2^n$, and $b \in \mathbb{F}_2$.

Computations for Each Representative Pair

For each representative pair (f_0^*, f_1^*), we need to consider all equivalent functions to f_1^*.

$$f_1(x) = f_1^* \circ P(x \oplus a) \oplus b$$

with P, a mapping corresponding to a permutation of n variables, $a \in \mathbb{F}_2^n$, and $b \in \mathbb{F}_2$.

Based on Siegenthaler's theorem, for all $\alpha \in \mathbb{F}_2^n$ with $\mathrm{hw}(\alpha) = t + 1$ we need

$$\widehat{f_1}(\alpha) = -\widehat{f_0^*}(\alpha) \quad \Rightarrow \quad |\widehat{f_1}(\alpha)| = |\widehat{f_0^*}(\alpha)|$$

Computations for Each Representative Pair

For each representative pair (f_0^*, f_1^*), we need to consider all equivalent functions to f_1^*.

$$f_1(x) = f_1^* \circ P(x \oplus a) \oplus b$$

with P, a mapping corresponding to a permutation of n variables, $a \in \mathbb{F}_2^n$, and $b \in \mathbb{F}_2$.

Based on Siegenthaler's theorem, for all $\alpha \in \mathbb{F}_2^n$ with $\mathrm{hw}(\alpha) = t + 1$ we need

$$\widehat{f_1}(\alpha) = -\widehat{f_0^*}(\alpha) \quad \Rightarrow \quad |\widehat{f_1}(\alpha)| = |\widehat{f_0^*}(\alpha)|$$

Since $\widehat{f_1}(\alpha) = (-1)^{\langle a,\alpha\rangle \oplus b} \cdot \widehat{f_1^*}(P(\alpha))$,

$$|\widehat{f_1^*}(P(\alpha))| = |\widehat{f_0^*}(\alpha)|$$

Summary

- Classification of all t-resilient functions with $(t+4)$ variables up-to the extended variable-permutation equivalence
- There are only 761 of such functions.

n	4	5	6	7	8	9	10
$\lvert\mathcal{R}^*_{n,n-4}\rvert$	58	256	578	720	754	760	761

Summary

- Classification of all t-resilient functions with $(t+4)$ variables up-to the extended variable-permutation equivalence
- There are only 761 of such functions.

n	4	5	6	7	8	9	10
$\lvert\mathcal{R}^*_{n,n-4}\rvert$	58	256	578	720	754	760	761

- Classification of $\mathcal{R}^*_{6,1}$: there are $1\,035\,596\,784 \approx 2^{30}$ of such functions.

Summary

- Classification of all t-resilient functions with $(t+4)$ variables up-to the extended variable-permutation equivalence
- There are only 761 of such functions.

n	4	5	6	7	8	9	10
$\lvert\mathcal{R}^*_{n,n-4}\rvert$	58	256	578	720	754	760	761

- Classification of $\mathcal{R}^*_{6,1}$: there are $1\,035\,596\,784 \approx 2^{30}$ of such functions.

Thank you for your attention!