Integral Resistance of Block Ciphers with Key Whitening by Modular Addition

CRYPTO 2025 ,

Christof Beierle, Phil Hebborn, Gregor Leander, and Yevhen Perehuda
Ruhr University Bochum

Gefördert durch
Deutsche Forschungsgemeinschaft

Motivation

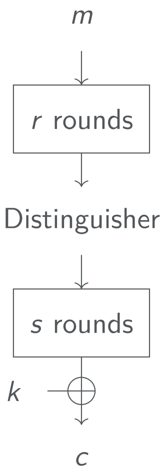
erc SymTrust

Focus on Security Arguments

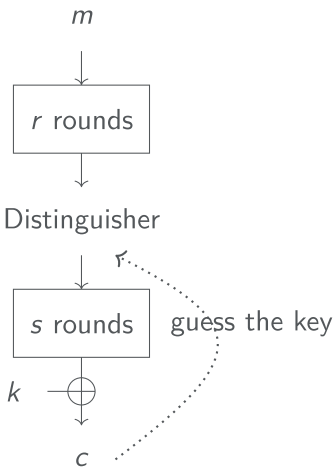
Give strong security arguments for symmetric cryptographic primitives

State-of-the-art: Many arguments for linear and differential attacks. Few for integral cryptanalysis

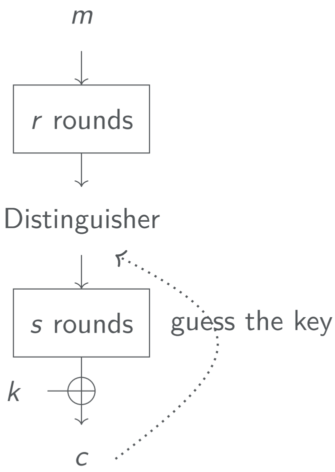
Distinguisher and Key Recovery



Distinguisher and Key Recovery



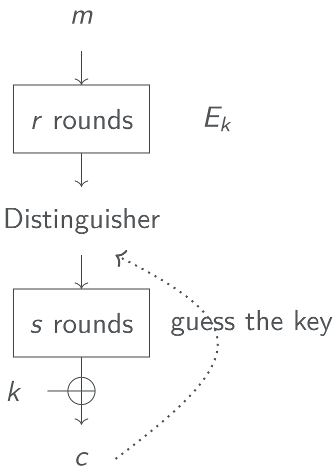
Distinguisher and Key Recovery



Here:

- Integral distinguisher
- Aim: Argue the non-existence
- Ignore the key-guessing

Distinguisher and Key Recovery



Here:

- Integral distinguisher
- Aim: Argue the non-existence
- Ignore the key-guessing

Integral Distinguisher

Lars Ramkilde Knudsen

- Invented by Lars Knudsen
- Originally on AES-like designs
- Many improvements since then: e.g. division property, monomial prediction, geometric approach, ...

General Setting

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Zero-Sum

Given a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ find a set $M \subseteq \mathbb{F}_2^n$ s.t.

$$\sum_{x \in M} E_k(x) = 0$$

- Enough if it happens on some bits

To simplify we consider only Boolean functions

$$f_k : \mathbb{F}_2^n \to \mathbb{F}_2$$

(think of one bit of the cipher-text)

Security Argument

Given $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$

Goal

Show that for any (non trivial) set $M \subseteq \mathbb{F}_2^n$ it holds

$$\sum_{x \in M} f_k(x) \neq 0$$

Security Argument

Given $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$

Goal

Show that for any (non trivial) set $M \subseteq \mathbb{F}_2^n$ it holds

$$\sum_{x \in M} f_k(x) \neq 0 \text{ (as a function in the key)}$$

Security Argument

Given $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$

Goal

Show that for any (non trivial) set $M \subseteq \mathbb{F}_2^n$ it holds

$$\sum_{x \in M} f_k(x) \neq 0 \text{ (as a function in the key)}$$

This is the same as linear independence of the functions $k \mapsto f_k(x)$.

Goal

Show that the functions $(k \mapsto f_k(x))_{x \in \mathbb{F}_2^n}$ are linear independent.

How to Reduce the Problem

Goal

Show that the functions $(k \mapsto f_k(x))_{x \in \mathbb{F}_2^n}$ are linear independent.

Those are 2^n (hopefully unstructured) functions 🤯

How to Reduce the Problem

Goal

Show that the functions $(k \mapsto f_k(x))_{x \in \mathbb{F}_2^n}$ are linear independent.

Those are 2^n (hopefully unstructured) functions 🤯

Hebborn et al (AC21)

Can be drastically simplified by two ingredients:

- Look at the ANF
- Use pre-whitening keys

ANF

Every function can be written in its algebraic normal form

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

where

$$x^u = \prod_i x_i^{u_i} \text{ and } p_u : \mathbb{F}_2^\kappa \to \mathbb{F}_2$$

p_u can be computed *linearly* from $(k \mapsto f_k(x))$ (*and vice versa*)

Goal for ANF

$(k \mapsto f_k(x))_{x \in \mathbb{F}_2^n}$ are linear independent $\Leftrightarrow$ $(k \mapsto p_u(k))_{u \in \mathbb{F}_2^n}$ are linear independent.

ANF

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u$$

Goal for ANF

$(k \mapsto p_u(k))_{u \in \mathbb{F}_2^n}$ are linear independent.

Each p_u can be written as

$$p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

Using division property/ monomial prediction we can compute (some!) $\lambda_v^{(u)}$

Whitening Keys (2^n becomes n)

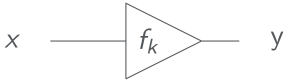
$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

Still 2^n (unstructured, hard to evaluate) functions 🤯

Whitening Keys (2^n becomes n)

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

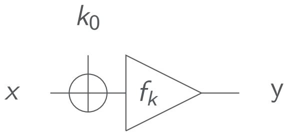
Still 2^n (unstructured, hard to evaluate) functions 🤯



Whitening Keys (2^n becomes n)

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

Still 2^n (unstructured, hard to evaluate) functions 🤯

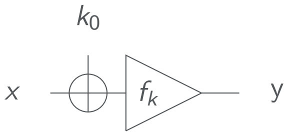


$$\widehat{f}_{k_0,k}(x) = f_k(x + k_0) = \sum_u p_u(k)(x + k_0)^u$$

Whitening Keys (2^n becomes n)

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

Still 2^n (unstructured, hard to evaluate) functions 🤯

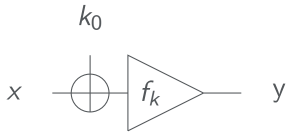


$$\widehat{f}_{k_0,k}(x) = f_k(x + k_0) = \sum_u p_u(k)(x + k_0)^u = \sum_u q_u(k, k_0) x^u$$

Whitening Keys (2^n becomes n)

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

Still 2^n (unstructured, hard to evaluate) functions 🤯



$$\widehat{f}_{k_0,k}(x) = f_k(x + k_0) = \sum_u p_u(k)(x + k_0)^u = \sum_u q_u(k, k_0) x^u$$

Theorem 1

If p_w are linear independent for $wt(w) = n - 1$ then all q_u are linear independent.

Nice... But

Theorem 1

If p_w are linear independent for $wt(w) = n - 1$ then all q_u are linear independent.

- Still n functions
- requires computation of n^2 values $\lambda_v^{(u)}$
- Only XOR-whitening keys handled

$\Rightarrow$ Practically expensive and limited scope.

Nice... But

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 1

If p_w are linear independent for $wt(w) = n - 1$ then all q_u are linear independent.

- Still n functions
- requires computation of n^2 values $\lambda_v^{(u)}$
- Only XOR-whitening keys handled

$\Rightarrow$ Practically expensive and limited scope.

Our work

Generalize to include modular addition of whitening keys and reduce computational complexity.

Notions of Order: The Influence of Pre-whitening Keys

XOR

$$(x \oplus k_0)^u = \sum_{v \leq u} k_0^{u \oplus v} x^v$$

$$v \leq u \Leftrightarrow \; v_i \leq u_i$$

Notions of Order: The Influence of Pre-whitening Keys

XOR

$$(x \oplus k_0)^u = \sum_{v \leq u} k_0^{u \oplus v} x^v$$

$v \leq u \Leftrightarrow \; v_i \leq u_i$

Modular-Add-Case (Braeken, Semaev)

$$(x \boxplus k_0)^u = \sum_{v \leq u} k_0^{u \boxminus v} x^v.$$

$v \leq u$ as integers

Notions of Order: The Influence of Pre-whitening Keys

CASA
Cyber Security in the Age of Large-Scale Adversaries

XOR	Modular-Add-Case (Braeken, Semaev)
$$(x \oplus k_0)^u = \sum_{v \leq u} k_0^{u \oplus v} x^v$$	$$(x \boxplus k_0)^u = \sum_{v \leq u} k_0^{u \boxminus v} x^v.$$

$v \leq u \Leftrightarrow \; v_i \leq u_i$

$v \leq u$ as integers

In a nutshell: Every v that is influenced becomes linear independent

Notions of Order: The Influence of Pre-whitening Keys

- Everything that is influenced becomes linear independent
- f_k balanced $\Rightarrow u = (1...1) = 2^n - 1$ is excluded.

XOR

$$v \leq u \Leftrightarrow \; v_i \leq u_i$$

n elements of $\mathrm{wt} = n - 1$ needed

Notions of Order: The Influence of Pre-whitening Keys

- Everything that is influenced becomes linear independent
- f_k balanced $\Rightarrow u = (1...1) = 2^n - 1$ is excluded.

XOR	Modular-Add-Case
$v \leq u \Leftrightarrow \; v_i \leq u_i$	$v \leq u$ as integers

n elements of $\mathrm{wt} = n - 1$ needed

$u = 2^n - 2$ alone is sufficient.

Notions of Order: The Influence of Pre-whitening Keys

- Everything that is influenced becomes linear independent
- f_k balanced $\Rightarrow u = (1...1) = 2^n - 1$ is excluded.

XOR	Modular-Add-Case
$v \leq u \Leftrightarrow \; v_i \leq u_i$	$v \leq u$ as integers

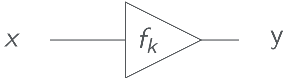
n elements of wt $= n - 1$ needed

$u = 2^n - 2$ alone is sufficient.

Condition gets much weaker + computationally cheaper

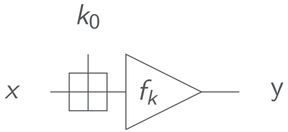
Mod Add Whitening Keys (2^n becomes 1!)

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$



Mod Add Whitening Keys (2^n becomes 1!)

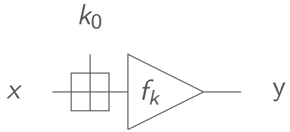
$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$



$$\widetilde{f}_{k_0,k}(x) = f_k(x \boxplus k_0) = \sum_u p_u(k)(x \boxplus k_0)^u$$

Mod Add Whitening Keys (2^n becomes 1!)

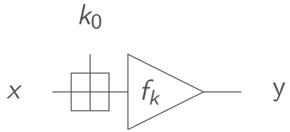
$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$



$$\widetilde{f}_{k_0,k}(x) = f_k(x \boxplus k_0) = \sum_u p_u(k)(x \boxplus k_0)^u = \sum_u q_u(k, k_0) x^u$$

Mod Add Whitening Keys (2^n becomes 1!)

$$f_k(x) = \sum_{u \in \mathbb{F}_2^n} p_u(k) x^u \text{ with } p_u(k) = \sum_{v \in \mathbb{F}_2^\kappa} \lambda_v^{(u)} k^v$$

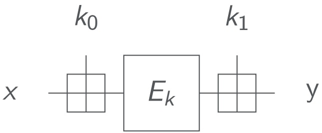


$$\widetilde{f}_{k_0,k}(x) = f_k(x \boxplus k_0) = \sum_u p_u(k)(x \boxplus k_0)^u = \sum_u q_u(k, k_0) x^u$$

Theorem 2

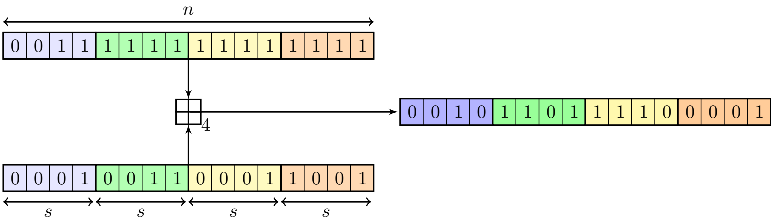
If $p_{2^n-2} \neq 0$ all q_u are linear independent.

What else (I/III): Post-whitening Keys



- Allows to lift the idea to vectorial version
- Still enough to compute one coefficient

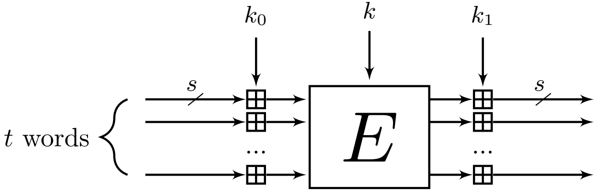
What else (II/III): Word-wise Addition



- Used for better performance
- ARX ciphers
- Give a unified view

What else (II/III): A Unified Framework

General Theorem to handle all those cases.



- $t = n$: XOR-whitening keys
- $t = 1$: Mod-Add-whitening keys

What else (III/III): d-th Order Integral Resistance

CASA
Cyber Security in the Age of Large-Scale Adversaries

Zero-Sum

Given a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ find a set $M \subseteq \mathbb{F}_2^n$ s.t.

$$\sum_{x \in M} E_k(x) = 0$$

- Enough if it happens on some bits ✓
- Enough if equation has low degree

What else (III/III): d-th Order Integral Resistance

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Zero-Sum

Given a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ find a set $M \subseteq \mathbb{F}_2^n$ s.t.

$$\sum_{x \in M} E_k(x) = 0$$

- Enough if it happens on some bits ✓
- Enough if equation has low degree

We introduce d-th order integral resistance to capture that.

What else (III/III): d-th Order Integral Resistance

CASA
Cyber Security in the Age of Large-Scale Adversaries

Zero-Sum

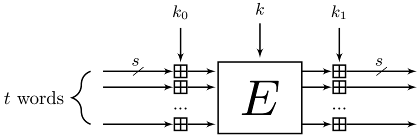
Given a block cipher $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ find a set $M \subseteq \mathbb{F}_2^n$ s.t.

$$\sum_{x \in M} E_k(x) = 0$$

- Enough if it happens on some bits ✓
- Enough if equation has low degree ✓

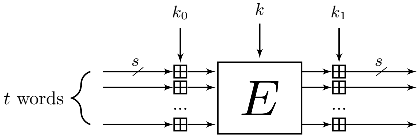
We introduce d-th order integral resistance to capture that.

The End!



- No surprise that modular key addition makes it more resistant
- But: surprise how nice everything works out
- More in the paper: full proof, concrete examples, link to data, inverse cipher

The End!



- No surprise that modular key addition makes it more resistant
- But: surprise how nice everything works out
- More in the paper: full proof, concrete examples, link to data, inverse cipher

Thank you for your attention!