

On the Guaranteed Number of Activations in XS-circuits

Sergey Agievich

Research Institute for Applied Problems of Mathematics and Informatics
Belarusian State University

September 15, 2020 [Minsk-Dorohovskoe]

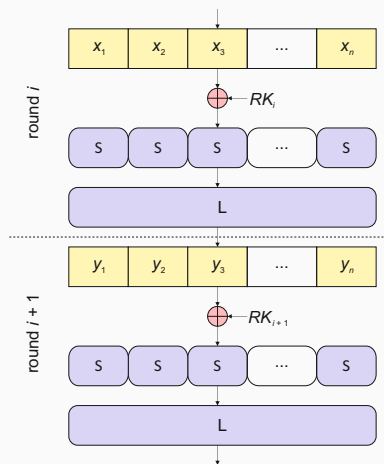


Table of contents

1. Introduction
2. XS-circuits
3. GNA in XS-circuits
4. Examples

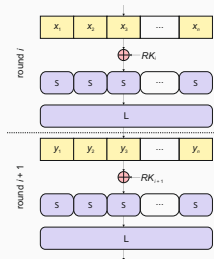
Introduction

XSL-circuits

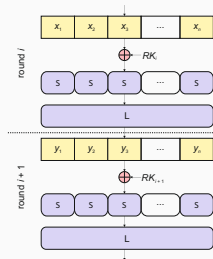


Activations

block #1

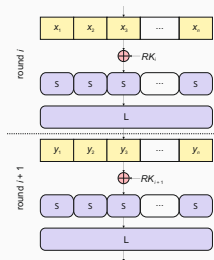


block #2

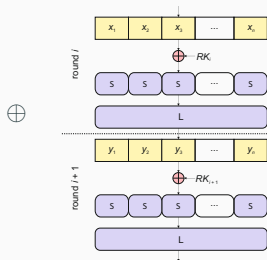


Activations

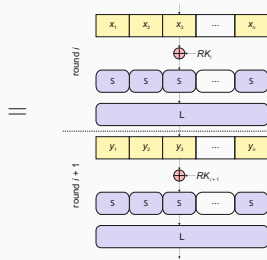
block #1



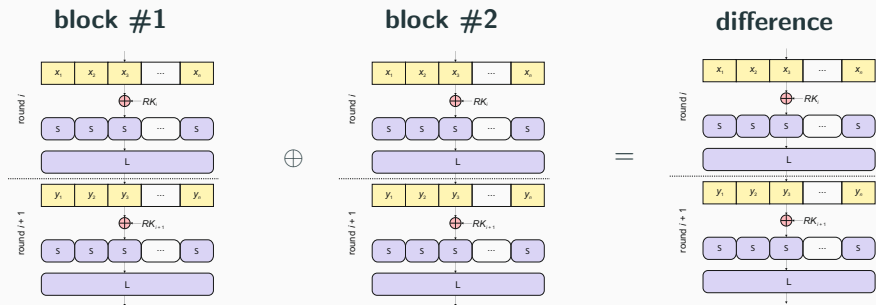
block #2



difference



Activations



Activation

The situation when an S-box gets a nonzero difference.

The Guaranteed Number of Activations (GNA)

The more activations, the stronger guarantees against differential attacks.

GNA(circuit, t)

The minimum number of activations over t rounds, where the minimum is over all different input blocks, keys / round keys[, and S -boxes].

GNA in XSL-circuits

If L is built using an MDS matrix, then

$$\#(\text{activations}_{i\text{th round}}) + \#(\text{activations}_{(i+1)\text{th round}}) \geq n + 1,$$

that is,

$$\text{GNA}(\text{XSL-circuit of dimension } n, t) \geq \frac{t(n+1)}{2} - n.$$

In other words, the *guaranteed activation rate* is close to $1/2$.

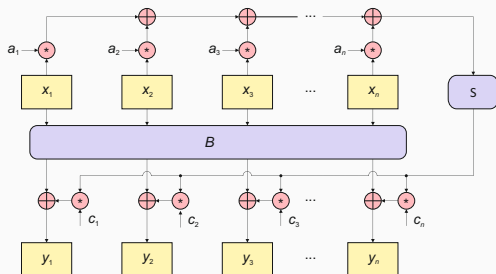
XS-circuits

XS-circuits

Parameters:

- a field $\mathbb{F}$ of characteristic 2 (an extension of $\mathbb{F}_2$);
- binary vectors $a = (a_1, \dots, a_n)^T$ and $c = (c_1, \dots, c_n)$;
- a binary matrix B of order n ;
- a round oracle S (a bijection over $\mathbb{F}$, an instantiation of S).

The round: $(a, B, c)[S]: \mathbb{F}^n \rightarrow \mathbb{F}^n, x \mapsto xB + S(xa)c$.



The t -round cascade: $(a, B, c)^t[S_1, \dots, S_t]$.

Usage areas of XS-circuits

Conventional block ciphers

S is a table or algorithmic (based on another circuit) S -box preceded by addition with a round key.

Wide-block ciphers

S is a key-dependent permutation of a (fixed-) block cipher.

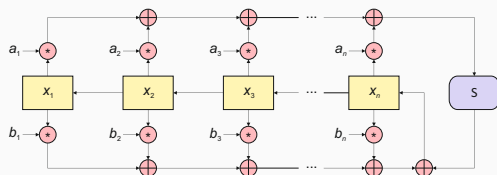
Arithmetic ciphers

S is a key-dependent permutation build using only operations of $\mathbb{F}$.

The 1st Canonical Form (CF1)

Regularity: $A = \begin{pmatrix} a & Ba & \dots & B^{n-1}a \end{pmatrix}$ and $C = \begin{pmatrix} cB^{n-1} \\ \vdots \\ cB \\ c \end{pmatrix}$ are invertible.

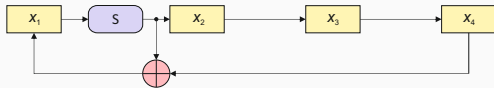
CF1:



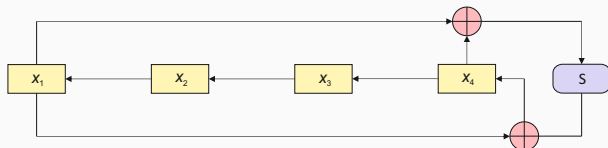
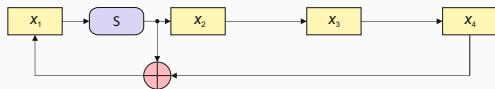
The cascade: $(x_1, \dots, x_n) \mapsto (x_{t+1}, \dots, x_{t+n})$, where

$$x_{\tau+n} = (x_{\tau}, \dots, x_{\tau+n-1})b + S_{\tau}((x_{\tau}, \dots, x_{\tau+n-1})a), \quad \tau = 1, 2, \dots, t.$$

CF1: SkipjackA



CF1: SkipjackA



GNA in XS-circuits

Differences

Conventions

- the cascade processes not one but two different input blocks simultaneously;
- $(x_{\tau+1}, \dots, x_{\tau+n})$ is the difference of the τ th round outputs;
- $u_{\tau} = (x_{\tau}, \dots, x_{\tau+n-1})a$ is the input difference for S_{τ} ;
- v_{τ} is the output difference for S_{τ} .

Observations

1. v_{τ} can be written as $(x_{\tau}, \dots, x_{\tau+n-1})b + x_{\tau+n}$.
2. $(u_1, v_1, u_2, v_2, \dots, u_t, v_t) = (x_1, x_2, \dots, x_{t+n})G$, where $G = G(n, a, b, t)$ is a matrix of dimensions $(t+n) \times 2t$.
3. $u_{\tau} = 0 \Leftrightarrow v_{\tau} = 0$.

Conventions

- $w = (u_1, v_1, u_2, v_2, \dots, u_t, v_t) = xG$, $x \in \mathbb{F}^{t+n}$;
- w is *feasible* if $(u_\tau = 0 \Leftrightarrow v_\tau = 0) \forall \tau$;
- $\text{wt}_2(w)$ is the number of nonzero pairs (u_τ, v_τ) ;
- the *activation profile* $\mathcal{T} \subseteq \{1, 2, \dots, t\}$: the set of indices of nonzero pairs (u_τ, v_τ) ;
- $\mathcal{W} = \{w : w \text{ is feasible}\}$.

GNA ($\mathbb{F}$ is fixed)

$$d(\mathcal{W}) = d(\mathbb{F}, n, a, b, t) = \min_{w \in \mathcal{W}, w \neq 0} \text{wt}_2(w).$$

GNA ($\mathbb{F}$ is arbitrary)

$$d(n, a, b, t) = \min_{\mathbb{F}} d(\mathbb{F}, n, a, b, t).$$

Lemma 1

Let vectors a and b define a regular XS-circuit of the first canonical form of dimension n . If $t \geq n$, then the matrix $G = G(n, a, b, t)$ has full rank: $\text{rank } G = t + n$.

Corollaries ($t \geq n$)

1. $\mathcal{C} = \{xG : x \in \mathbb{F}^{t+n}\} \subset \mathbb{F}^{2t}$ is a linear code with parameters $[2t, t + n]$.
2. $d(\mathcal{C})/2 \leq d(\mathcal{W}) \leq d(\mathcal{C})$, where $d(\mathcal{C})$ is the minimum distance of $\mathcal{C}$.

The case $\mathbb{F} = \mathbb{F}_2$

$$(u_\tau = 0 \Leftrightarrow v_\tau = 0) \xrightarrow{\mathbb{F}=\mathbb{F}_2} u_\tau = v_\tau$$

$\implies (u_\tau)$ is a linear recurrence sequence (LRS) over $\mathbb{F}_2$.

Facts

1. The characteristic polynomial of (u_τ) has the form $f(\lambda) = f_1 + f_2\lambda + \dots + f_n\lambda^{n-1} + \lambda^n$, where $(f_1, f_2, \dots, f_n) = a \oplus b$.
2. The number of activations over t rounds is the number of nonzero elements (units) in the segment $(u_1, \dots, u_t)$.
3. $d(\mathbb{F}_2, n, a, b, t)$ can be found by exhaustive search over all segments $(u_1, \dots, u_t)$ in time of order 2^nt .

Partitions of G

Partitions

Let $\mathcal{T} \subseteq \{1, 2, \dots, t\}$ be an activation profile. Divide G into two parts: G_0 and G_1 . G_1 consists of pairs of columns whose numbers are in $\mathcal{T}$ and G_0 consists of the remaining columns.

Feasible partitions

The partition (G_0, G_1) has to be *feasible*:

- 1) $\text{rank } G_0 < t + n$;
- 2) $\text{rank}(G_0 \mid g) > \text{rank } G_0$ for each column g of G_1 .

Lemma 2

Let vectors a and b define a regular XS-circuit of the first canonical form of dimension n . Let $t \geq n$ and k be the maximum number of pairs of columns in G_0 where the maximum is taken over all feasible partitions (G_0, G_1) of $G = G(n, a, b, t)$. Then $d(n, a, b, t) = t - k$.

The algorithm *

Interface: $(n, a, b, t) \mapsto d(n, a, b, t)$.

Steps:

1. If $t < n$, then return 0. If $t = n$, return 1.
2. Construct $G = G(n, a, b, t)$.
3. Set $k \leftarrow t - d(\mathbb{F}_2, n, a, b, t)$.
4. Make a list of all possible partitions of G into submatrices G_0 and G_1 such that G_0 contains exactly $k + 1$ pairs of columns of G .
5. For each partition (G_0, G_1) :
 - 5.1 if $\text{rank } G_0 \geq t + n - 1$, then continue;
 - 5.2 if $\exists$ a column $g \in G_1$ such that $\text{rank}(G_0 \mid g) = \text{rank } G_0$, continue;
 - 5.3 set $k \leftarrow k + 1$ and go to Step 4.
6. Return $t - k$.

Theorem

The algorithm is correct.

*Implemented at <https://github.com/agievich/xs>. Credits to Egor Lawrenov.

Linear activations

Apply the same approach to the dual circuit $(a, B, c)^T = (c^T, B^T, a^T)$.

Examples

The SMS4 / SM4 circuit

Used in the SMS4 /SM4 block cipher.

$$n = 4, \begin{pmatrix} B & a \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$\mathbb{F} = \mathbb{F}_2$$

$$f(\lambda) = \lambda^4 + \lambda^3 + \lambda^2 + \lambda + 1.$$

If $t = 5t_0 + t_1$, $0 \leq t_1 < 5$, then

$$d(\mathbb{F}_2, \text{SMS4}, t) = \begin{cases} 2t_0, & t_1 = 0, 1, 2, 3, \\ 2t_0 + 1, & t_1 = 4. \end{cases}$$

The activation rate is close to $2/5$.

$$\forall \mathbb{F}$$

$$d(\text{SMS4}, t) = d(\mathbb{F}_2, \text{SMS4}, t) \quad \forall t \leq 32.$$

The GFN1 circuit

Introduced in [ZMI90] as “Generalized Feistel Network of type 1”.

$$\begin{pmatrix} B & a \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

$$\mathbb{F} = \mathbb{F}_2$$

$$f(\lambda) = \lambda^n + \lambda^{n-1} + 1.$$

$n = 2, 3, 4$: $f(\lambda)$ is primitive and the activation rate over $2^n - 1$ rounds can potentially achieve the value $2^{n-1}/(2^n - 1) > 1/2$.

$$n = 4, t = 15$$

	$\forall \mathbb{F}$	$\mathbb{F} = \mathbb{F}_2$
GNA	$d(4, \text{GFN1}, 15) = 7$	$d(\mathbb{F}_2, 4, \text{GFN1}, 15) = 8$
The best profile	000111101 <u>100100</u>	000111101 <u>011001</u>

Activation times

The i th activation time, ρ_i

The minimum number of rounds that guarantees i activations.

i	1	2	3	4	5	6	7	8	9	10	11	12
$\rho_i(\text{GFN1}^\dagger)$	4	7	8	10	12	13	14	17	20	22	23	25
$\rho_i(\text{SMS4})$	4	5	9	10	14	15	19	20	24	25	29	30

[†]of dimension 4