Group-theoretical methods for the cryptanalysis of block ciphers

Roberto Civino
University of L'Aquila - Italy

CrypTO Conference 2023

26 May 2023

Block ciphers

Ingredients

- $n \in \mathbb{N}$ such that performing 2^n operations is unfeasible $n \sim 128$
- $V \stackrel{\text{def}}{=} \mathbb{F}_2^n$ the message space

Block ciphers

Ingredients

- $n \in \mathbb{N}$ such that performing 2^n operations is unfeasible
- $V \stackrel{\text{def}}{=} \mathbb{F}_2^n$ the message space

Definition

a *block cipher* is a set of 2^n encryption functions indexed by parameters called *keys*

$$\Phi = \{f_k \mid 1 \leq k \leq 2^n\} \subset \mathrm{Sym}(V)$$

Block ciphers

Ingredients

- $n \in \mathbb{N}$ such that performing 2^n operations is unfeasible
- $V \stackrel{\text{def}}{=} \mathbb{F}_2^n$ the message space

Definition

a *block cipher* is a set of 2^n encryption functions indexed by parameters called *keys*

$$\Phi = \{f_k \mid 1 \leq k \leq 2^n\} \subset \mathrm{Sym}(V)$$

- mf_k is the encryption of the message $m \in V$ using the key k

Block ciphers

Ingredients

- $n \in \mathbb{N}$ such that performing 2^n operations is unfeasible
- $V \stackrel{\text{def}}{=} \mathbb{F}_2^n$ the message space

Definition

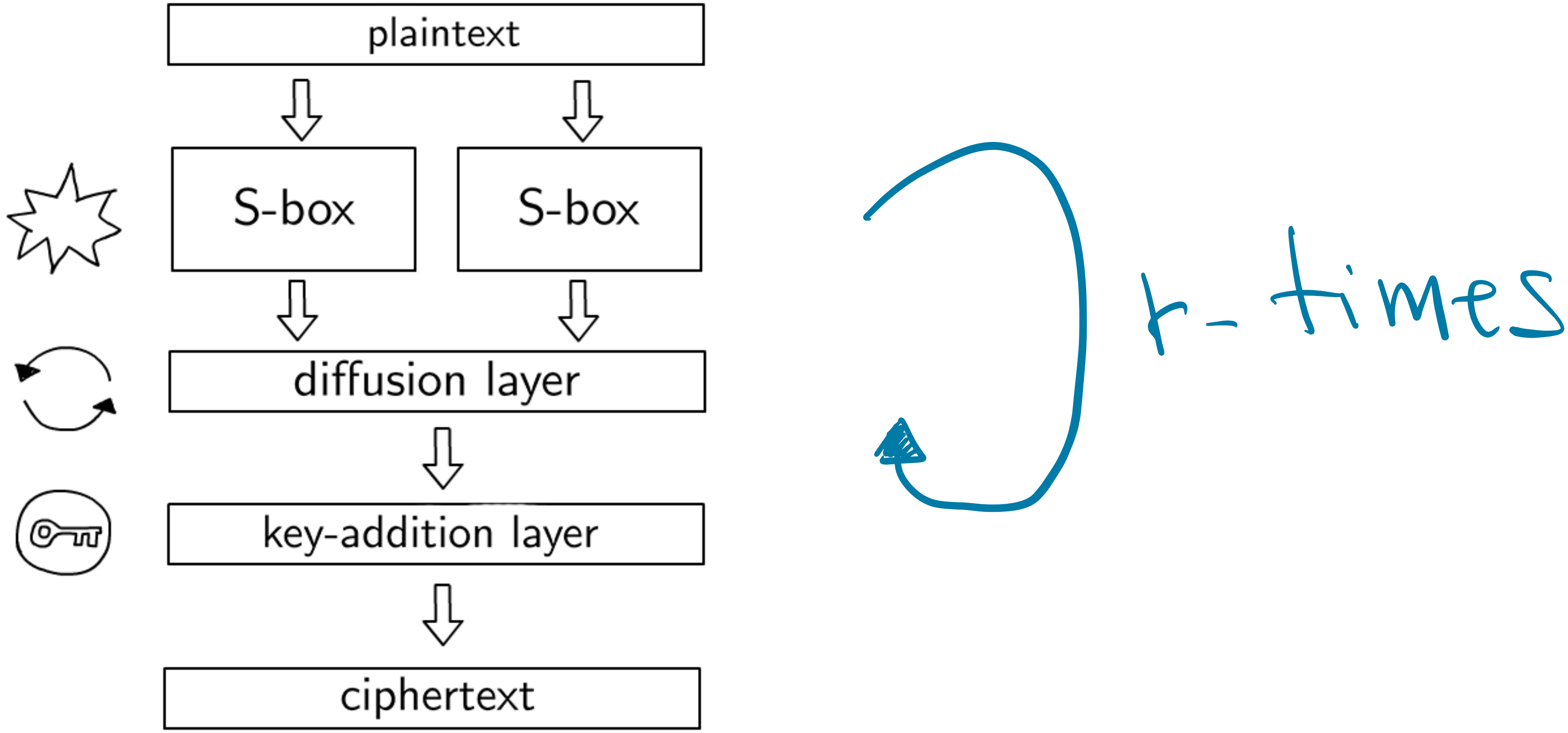
a *block cipher* is a set of 2^n encryption functions indexed by parameters called *keys*

$$\Phi = \{f_k \mid 1 \leq k \leq 2^n\} \subset \mathrm{Sym}(V)$$

- mf_k is the encryption of the message $m \in V$ using the key k
- there exists an efficient algorithm to reconstruct f_k

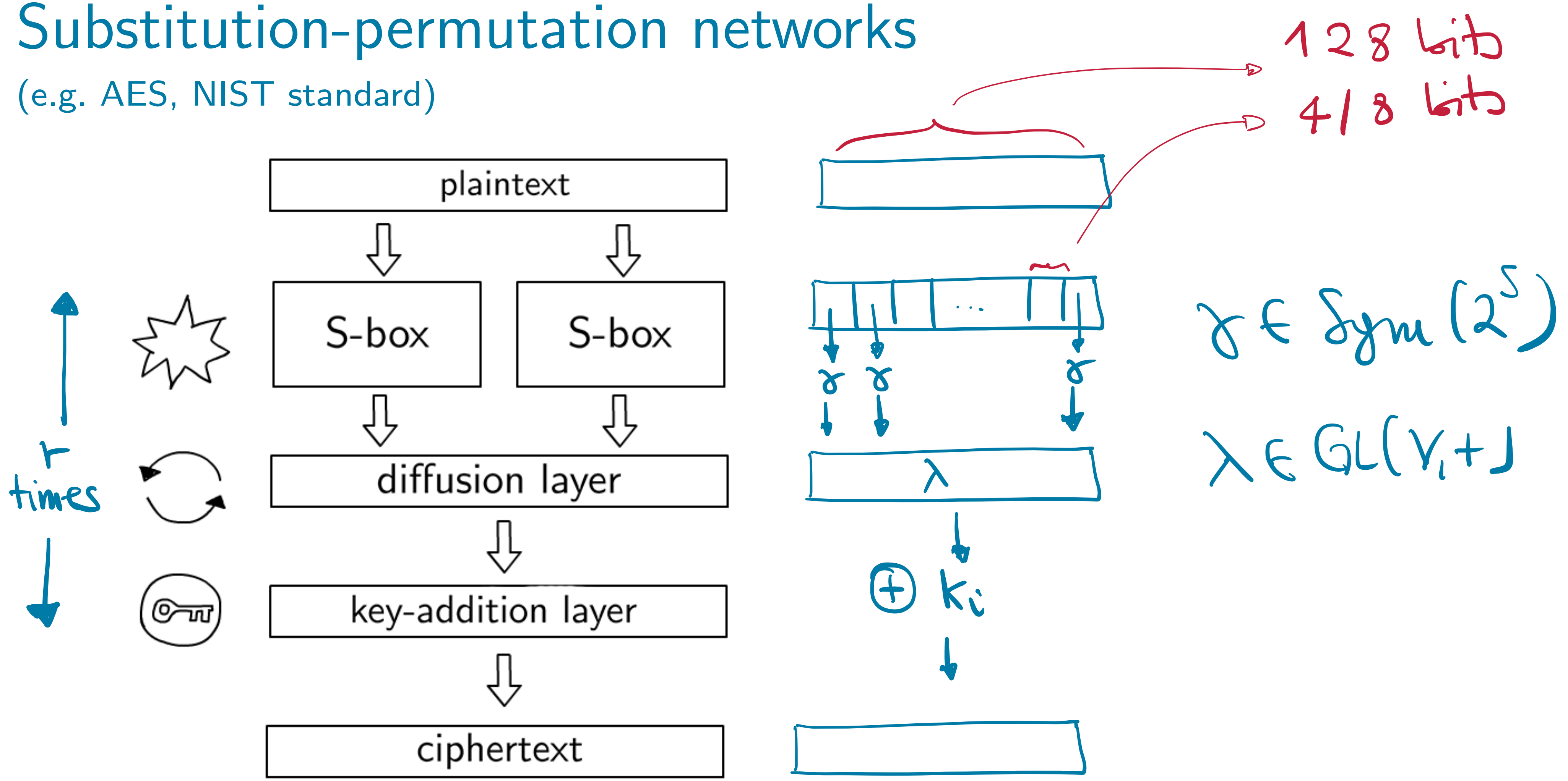
Substitution-permutation networks

(e.g. AES, NIST standard)



Substitution-permutation networks

(e.g. AES, NIST standard)

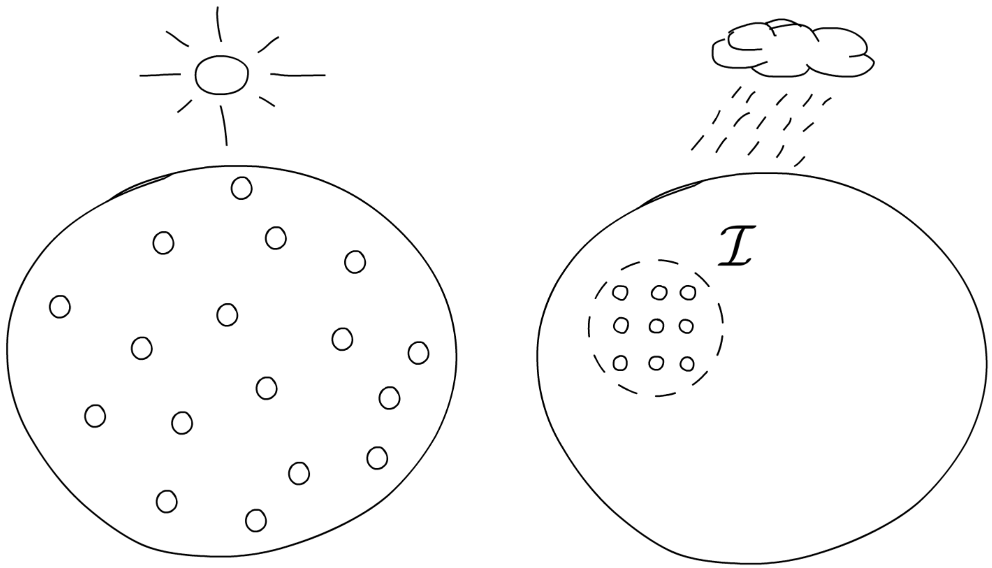


- $f_k = \gamma\lambda\sigma_{k_1} \dots \gamma\lambda\sigma_{k_r}$
- $\gamma, \lambda, k \mapsto (k_1, k_2, \dots, k_r)$ are public

Cryptanalysis...

... means finding an invariant property $\mathcal{I}$ such that

$$\mathbb{P}(f \in \Phi \text{ satisfies } \mathcal{I}) >> \mathbb{P}(f \in \mathrm{Sym}(V) \text{ satisfies } \mathcal{I})$$



a good cipher vs a bad cipher in $\mathrm{Sym}(V)$

A famously exploited invariant

A famously exploited invariant

Definition

the *derivative w.r.t.* $\Delta \in \mathbb{F}_2^n$ of $f = f_k \in \Phi$ is

$$f_\Delta : V \to V, \quad x \mapsto xf + (x + \Delta)f$$

A famously exploited invariant

Definition

the *derivative w.r.t.* $\Delta \in \mathbb{F}_2^n$ of $f = f_k \in \Phi$ is

$$f_\Delta : V \to V, \quad x \mapsto xf + (x + \Delta)f$$

(classical) differential cryptanalysis

show that, for some or for all the keys, derivatives w.r.t. some fixed Δs have small images [BS91]

A famously exploited invariant

Definition

the *derivative w.r.t.* $\Delta \in \mathbb{F}_2^n$ of $f = f_k \in \Phi$ is

$$f_\Delta : V \to V, \quad x \mapsto xf + (x + \Delta)f$$

(classical) differential cryptanalysis

show that, for some or for all the keys, derivatives w.r.t. some fixed Δs have small images [BS91]

$$\Uparrow$$

exhibit a pair (Δ_I, Δ_O) such that the equation

$$xf_{\Delta_I} = xf + (x + \Delta_I)f = \Delta_O$$

has *more* solution than expected ($\Rightarrow \mathrm{Im}(f_{\Delta_I})$ is *smaller*)

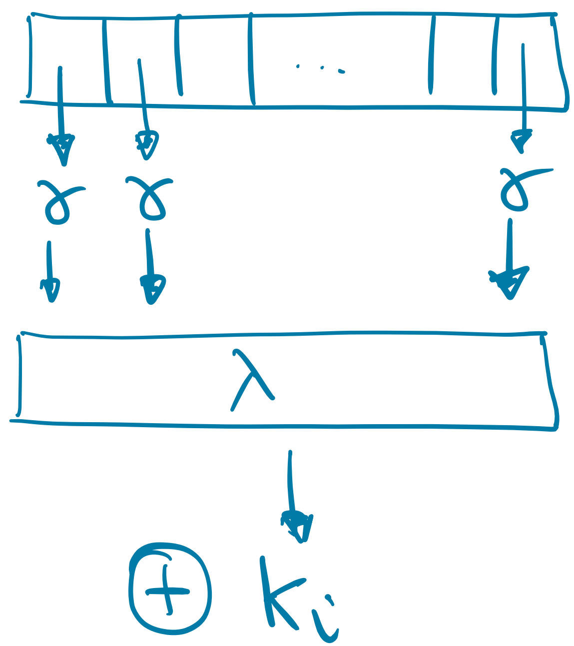
The classical solution

(unprovable) claim

if the encryption functions are such that

- γ has derivatives with large image [computationally feasable]
- λ has *good* diffusion properties

then f_ks have large derivative images



The classical solution

(unprovable) claim

if the encryption functions are such that

- γ has derivatives with large image [computationally feasable]
- λ has *good* diffusion properties

then f_ks have large derivative images

diffusion and key addition, being affine operations, do not alter the difference distribution!

- $x\lambda + (x + \Delta)\lambda = \Delta\lambda$ for all x
- $x\sigma_k + (x + \Delta)\sigma_k = (x + k) + (x + \Delta + k) = \Delta$ for all x and k

An alternative approach

everything is optimized to maximize the non-linearity w.r.t. the operation $+$ used to perform the key addition induced by

$$T \stackrel{\text{def}}{=} \{\sigma_b : b \in V \mid \sigma_b : x \mapsto x + b\} < \mathrm{Sym}(V)$$

- T is elementary abelian regular
- $\forall a, b \in V \quad a\sigma_b = a + b$

An alternative approach

consider another elementary abelian regular group

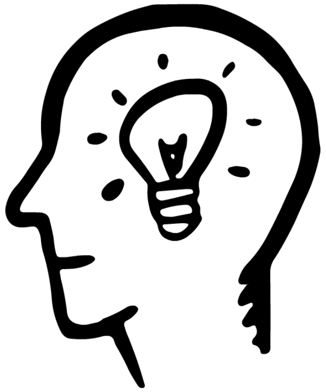
$$T_\circ \stackrel{\text{def}}{=} \{\tau_b : b \in V \mid \tau_b : 0 \mapsto b\} < \mathrm{Sym}(V)$$

- $\forall a, b \in V \quad a \circ b \stackrel{\text{def}}{=} a\tau_b$
- $(V, \circ)$ is a vector space over $\mathbb{F}_2$

Looking at new derivatives

if Φ is a secure block ciphers w.r.t. (classical) differential cryptanalysis[1], how large the images of $\circ$-*derivatives are?* [2]

$$f^{\circ}_{\Delta} : x \mapsto xf \circ (x \circ \Delta)f$$



[1] i.e. f_ks have derivatives with large images

[2] spoiler: can be small!

Braces coming into play

before we even start, we assume $T_\circ < \mathrm{AGL}(V, +)$ [computational]

Braces coming into play

before we even start, we assume $T_\circ < \mathrm{AGL}(V, +)$ [computational]

1. $\circ$-derivatives of γ have smaller images OK 👍

Braces coming into play

before we even start, we assume $T_\circ < \mathrm{AGL}(V, +)$ [computational]

1. $\circ$-derivatives of γ have smaller images OK 👍
2. $x\lambda \circ (x \circ \Delta)\lambda = ?$ Not-OK 👎
[big issue, see later]

Braces coming into play

before we even start, we assume $T_\circ < \mathrm{AGL}(V, +)$ [computational]

1. $\circ$-derivatives of γ have smaller images OK 👍
2. $x\lambda \circ (x \circ \Delta)\lambda = ?$ Not-OK 👎
   [big issue, see later]
3. $(x + k) \circ (x \circ \Delta + k) = ?$

Braces coming into play

before we even start, we assume $T_\circ < \mathrm{AGL}(V, +)$ [computational]

1. $\circ$-derivatives of γ have smaller images OK 👍
2. $x\lambda \circ (x \circ \Delta)\lambda = ?$ Not-OK 👎
   [big issue, see later]
3. $(x + k) \circ (x \circ \Delta + k) = ?$

$$(x + k) \circ (x \circ \Delta + k) = x\sigma_k + (x \circ \Delta)\sigma_k$$

Braces coming into play

before we even start, we assume $T_\circ < \mathrm{AGL}(V, +)$ [computational]

1. $\circ$-derivatives of γ have smaller images OK
2. $x\lambda \circ (x \circ \Delta)\lambda = ?$ Not-OK
   [big issue, see later]
3. $(x + k) \circ (x \circ \Delta + k) = ?$

$$(x + k) \circ (x \circ \Delta + k) = x\sigma_k + (x \circ \Delta)\sigma_k \tag{1}$$

if $\sigma_k \in \mathrm{AGL}(V, \circ)$, then Eq. (1) does not depend on x, therefore we require $T_+ < \mathrm{AGL}(V, \circ)$ [cryptanalytic]

Binary bi-braces

we want to construct $T_\circ$ such that T_+ normalizes $T_\circ$ and $T_\circ$ normalizes T_+, i.e. a *(binary) bi-brace*

Binary bi-braces

we want to construct $T_\circ$ such that T_+ normalizes $T_\circ$ and $T_\circ$ normalizes T_+, i.e. a *(binary) bi-brace*

in this setting we have, given

$$\begin{aligned} W_\circ &\stackrel{\text{def}}{=} \{a : a \in V \mid \sigma_a = \tau_a\} \\ &= \{a : a \in V \mid \forall b \in V \quad a + b = a \circ b\} \\ &= \mathrm{Soc}(V, +, \circ), \end{aligned}$$

Theorem ([CDVS06, CCS21])

$1 \leq \dim(W_\circ) \leq n - 2$

Binary bi-braces

we want to construct $T_\circ$ such that T_+ normalizes $T_\circ$ and $T_\circ$ normalizes T_+, i.e. a *(binary) bi-brace*

in this setting we have, given

$$\begin{aligned} W_\circ &\stackrel{\text{def}}{=} \{a : a \in V \mid \sigma_a = \tau_a\} \\ &= \{a : a \in V \mid \forall b \in V \quad a + b = a \circ b\} \\ &= \mathrm{Soc}(V, +, \circ), \end{aligned}$$

Theorem ([CDVS06, CCS21])

$1 \leq \dim(W_\circ) \leq n - 2$

and

$$U_\circ \stackrel{\text{def}}{=} V \cdot V = \langle a \cdot b \mid a, b \in V \rangle$$

where $a \cdot b = a + b + a \circ b$ is such that $U_\circ \leq W_\circ$ and $V \cdot V \cdot V = 0$

Construction

from $T_\circ < \mathrm{AGL}(V, +)$ we have that, for each $b \in V$,

$$\tau_b = M_b \sigma_b \in \mathrm{AGL}(V, +)$$

Construction

from $T_\circ < \mathrm{AGL}(V,+)$ we have that, for each $b \in V$,

$$\tau_b = M_b \sigma_b \in \mathrm{AGL}(V,+)$$

Theorem ([CCS21])

let $d = \dim(W_\circ)$ *and* $W_\circ$ *being spanned by the last* d *vector of the canonical basis* $\{e_i\}_{i=1}^n$ *of* V*, then for each* $1 \le i \le n-d$ *we have*

$$M_{e_i} = \begin{pmatrix} 1_{n-d} & \Sigma_{e_i} \\ 0 & 1_d \end{pmatrix}$$

for some $\Sigma_{e_i} \in \mathbb{F}_2^{(n-d,d)}$ *[precise constraints omitted here]*

Solving the issue with the key addition

$$(x + k) \circ (x \circ \Delta + k) = \Delta + \underbrace{\Delta \cdot k}_{\in U_\circ}$$

Solving the issue with the key addition

$$(x + k) \circ (x \circ \Delta + k) = \Delta + \underbrace{\Delta \cdot k}_{\in U_\circ}$$

we have $\dim(W_\circ) = n - 2 \Rightarrow \dim(U_\circ) = 1$

$$\Downarrow$$

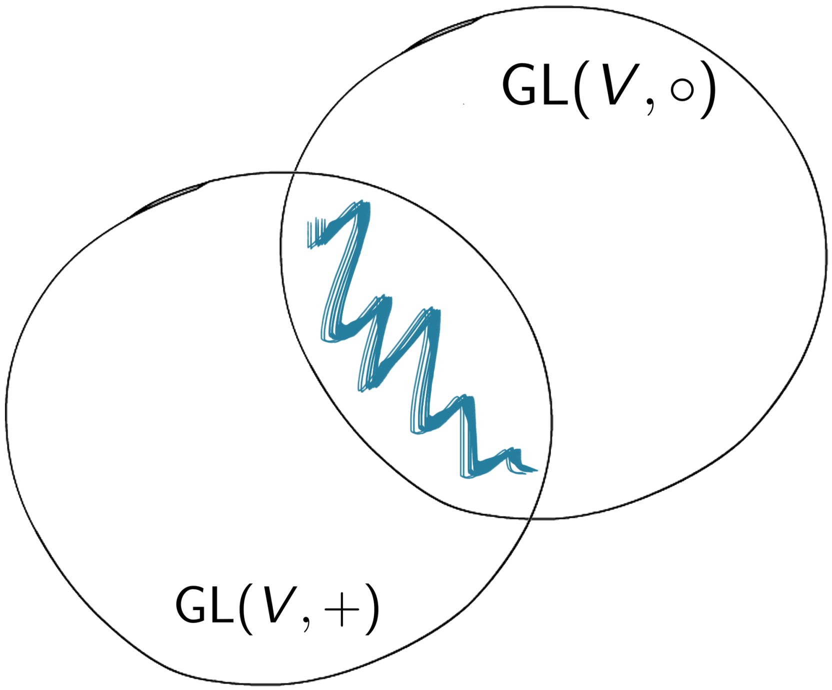
$$(x + k) \circ (x \circ \Delta + k) = \begin{cases} \Delta & p = 1/2 \\ \Delta + u & p = 1/2 \end{cases}$$

The issue with the diffusion layer

we need $x\lambda \circ (x \circ \Delta)\lambda = \Delta\lambda$

The issue with the diffusion layer

we need $x\lambda \circ (x \circ \Delta)\lambda = \Delta\lambda$



The issue with the diffusion layer

we need $x\lambda \circ (x \circ \Delta)\lambda = \Delta\lambda$

problem: the automorphisms of the brace

we equivalently need that

- $\lambda \in \mathrm{GL}(V, +) \cap \mathrm{GL}(V, \circ)$ or
- $\lambda \in \mathrm{Aut}(V, +, \circ)$ or
- $\lambda \in \mathrm{Aut}(V, +, \cdot)$

A first solution

if, again, $d = n - 2$

$$M_{e_1} = \left(\begin{array}{c|c} \mathbb{1}_2 & \begin{matrix} 0 \\ b \end{matrix} \\ \hline 0 & \mathbb{1}_{n-2} \end{array}\right) \text{ and } M_{e_2} = \left(\begin{array}{c|c} \mathbb{1}_2 & \begin{matrix} b \\ 0 \end{matrix} \\ \hline 0 & \mathbb{1}_{n-2} \end{array}\right)$$

for some $b \in \mathbb{F}_2^{n-2} \setminus \{0\}$

A first solution

if, again, $d = n - 2$

$$M_{e_1} = \left(\begin{array}{c|c} \mathbb{1}_2 & \begin{matrix} 0 \\ b \end{matrix} \\ \hline 0 & \mathbb{1}_{n-2} \end{array}\right) \text{ and } M_{e_2} = \left(\begin{array}{c|c} \mathbb{1}_2 & \begin{matrix} b \\ 0 \end{matrix} \\ \hline 0 & \mathbb{1}_{n-2} \end{array}\right)$$

for some $b \in \mathbb{F}_2^{n-2} \setminus \{0\}$

Theorem ([CBS19])

$\lambda \in \mathrm{GL}(V, +) \cap \mathrm{GL}(V, \circ)$ *if and only if*

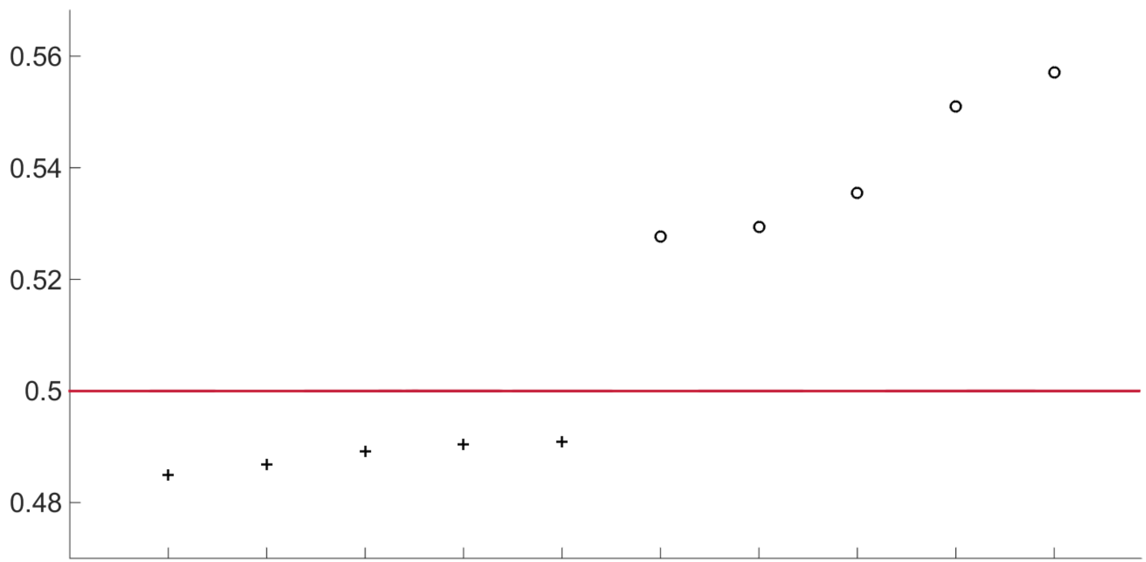
$$\lambda = \begin{pmatrix} A_2 & B \\ 0 & D_{n-2} \end{pmatrix}$$

such that $A \in \mathrm{GL}(2, +)$, $D \in \mathrm{GL}(n-2, +)$ *such that* $bD = b$ *and* $B \in \mathbb{F}_2^{(2,n-2)}$

Putting things together

we designed [CBS19] the first example of cipher which is

- resistant to classical differential cryptanalysis
- weak w.r.t. the revised differential attack using an operation $\hat{\circ} = (\circ, +, +, \ldots, +)$ such that $\dim(W_{\hat{\circ}}) = n - 2$



Doing better?

- attacks w.r.t. operations of the type $\hat{\circ} = (\circ, \circ, \ldots, \circ)$

Doing better?

- attacks w.r.t. operations of the type $\hat{\circ} = (\circ, \circ, \dots, \circ)$

  $$\Downarrow$$

  determine the automorphisms of the product of braces $(V, +, \hat{\circ})$ with $\dim(W_\circ) = s - 2$

  [ongoing work with M. Calderini and R. Invernizzi]

Doing better?

- attacks w.r.t. operations of the type $\hat{\circ} = (\circ, \circ, \ldots, \circ)$

  $$\Downarrow$$

  determine the automorphisms of the product of braces $(V, +, \hat{\circ})$ with $\dim(W_\circ) = s - 2$

  [ongoing work with M. Calderini and R. Invernizzi]
- attacks w.r.t. operations with $\dim(W) < n - 2$

Doing better?

- attacks w.r.t. operations of the type $\hat{\circ} = (\circ, \circ, \dots, \circ)$

$$\Downarrow$$

determine the automorphisms of the product of braces $(V, +, \hat{\circ})$ with $\dim(W_\circ) = s - 2$

[ongoing work with M. Calderini and R. Invernizzi]

- attacks w.r.t. operations with $\dim(W) < n - 2$

$$\Downarrow$$

determine the group of automorphisms of binary bi-braces

[ongoing work with V. Fedele]

¿Questions?

Bibliography

E. Biham and A. Shamir.
Differential cryptanalysis of DES-like cryptosystems.
J. Cryptology, 4(1):3–72, 1991.

R. Civino, C. Blondeau, and M. Sala.
Differential attacks: using alternative operations.
Des. Codes Cryptogr., 87(2-3):225–247, 2019.

M. Calderini, R. Civino, and M. Sala.
On properties of translation groups in the affine general linear group with applications to cryptography.
J. Algebra, 569:658–680, 2021.

A. Caranti, F. Dalla Volta, and M. Sala.
Abelian regular subgroups of the affine group and radical rings.
Publ. Math. Debrecen, 69(3):297–308, 2006.