Understanding the division property

Christina Boura

(joint work with Anne Canteaut)

ASK 2015, October 1, 2015

Introduction

- In Eurocrypt 2015, Yosuke Todo introduces a new property, called the division property.
- Combination (in some sense) of higher-order differential and saturation attacks.
- Construction of more powerful generic distinguishers for both SPN and Feistel constructions.
- Use of this new property for breaking full MISTY-1 (best paper award at CRYPTO 2015).

Notation

If $x, u \in \mathbf{F}_2^n$, we denote

$$x^u = \prod_{i=1}^{n} x_i^{u_i}$$

Example: $(n = 4)$

$x = (x_1, x_2, x_3, x_4) = (1, 1, 0, 1)$,
$u = (u_1, u_2, u_3, u_4) = (1, 0, 1, 0)$

$$x^u = {x_1}^{u_1} {x_2}^{u_2} {x_3}^{u_3} {x_4}^{u_4} = 1^1 1^0 0^1 1^0 = 0.$$

Division property

Let X be a multiset of elements in $\mathbf{F}_2^n$.

For $0 \leq k \leq n$, we say that X has the division property $\mathcal{D}_k^n$ if

$$\bigoplus_{x \in X} x^u = 0,$$

for all $u \in \mathbf{F}_2^n$ such that $wt(u) < k$.

Division property - Example

$$X = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\}.$$

Compute $\bigoplus_{x \in X} x^u$ for all $u \in \mathbf{F}_2^4$.

$$\bigoplus_{x \in X} x^u = 1,$$

for $u = 1011$, $u = 1101$ and $u = 1110$.

So, $\bigoplus_{x \in X} x^u = 0$ for all u with $wt(u) < 3$.

X has the division property $\mathcal{D}_3^4$.

Division property: a more general definition

For $\boldsymbol{u} = (u_1, \ldots, u_m), \boldsymbol{x} = (x_1, \ldots, x_m) \in \mathbf{F}_2^{n_1} \times \cdots \times \mathbf{F}_2^{n_m}$ define

$$\boldsymbol{x}^{\boldsymbol{u}} = x_1^{u_1} \cdots x_m^{u_m}$$

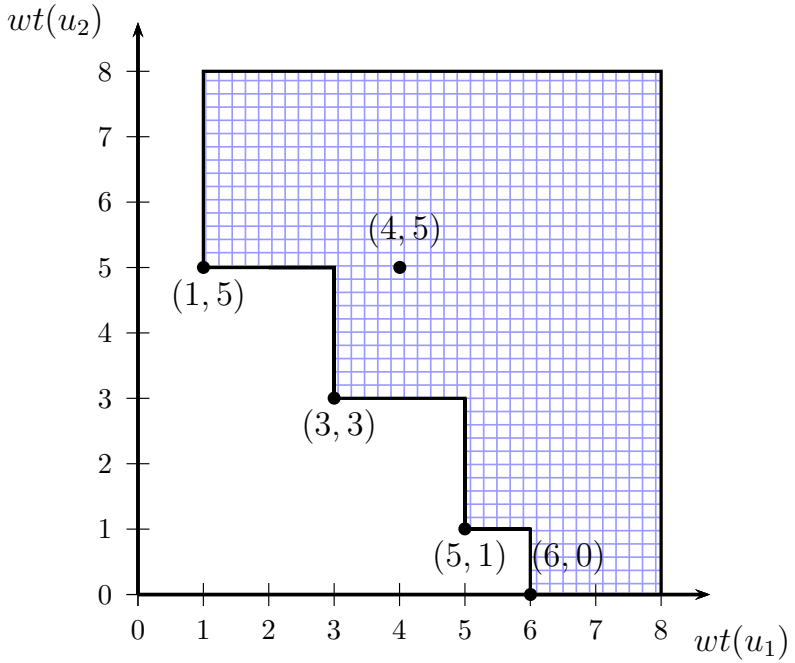
Let X be a multiset of elements in $\mathbf{F}_2^{n_1} \times \cdots \times \mathbf{F}_2^{n_m}$. X has the division property $\mathcal{D}^{n_1,\ldots,n_m}_{k^{(1)},\ldots,k^{(q)}}$ if

$$\bigoplus_{x \in X} \boldsymbol{x}^{\boldsymbol{u}} = 0 \text{ for all } \boldsymbol{u} \text{ such that } wt(\boldsymbol{u}) \not\succeq k^{(1)}, \ldots, wt(\boldsymbol{u}) \not\succeq k^{(q)}$$

(where $\boldsymbol{a} \succeq \boldsymbol{b}$ means that $a_i \geq b_i$ for all i).

Example

Let X be a multiset of elements in $\mathbf{F}_2^8 \times \mathbf{F}_2^8$ having the division property $\mathcal{D}^{8,8}_{[1,5],[3,3],[4,5],[5,1],[6,0]}$.



- If (u_1, u_2) is chosen in the **white** part : $\bigoplus_{(x_1,x_2)\in X} x_1^{u_1} x_2^{u_2} = 0$
- Else, the sum is unknown.

Using the division property in practice

- Prepare a set of plaintexts and evaluate its division property.
- Propagate the input texts and evaluate the division property of the output set after one round.
  - Use rules to propagate the property through the different cipher components (Sboxes, XOR, etc..)
- Repeat the procedure and compute the division property of the set of texts after several rounds.
- If after several rounds some exploitable information is found, then we get a distinguisher.

Unifying two classical attacks

Exploiting at the same time properties of saturation attacks and higher-order differential attacks

- Saturation attacks. Analyze the propagation of the following properties:
  - $\mathcal{A}$ (all): Each value appears the same number of times in the multiset.
  - $\mathcal{B}$ (balance): The XOR of all texts in the multiset is 0.
  - $\mathcal{C}$ (constant): The value is fixed to a constant for all texts in the multiset.
  - $\mathcal{U}$ (unknown): The multiset is indistinguishable from a random one.
- Higher-order differential attacks. Exploit the algebraic degree:
  - For every subspace V with $\dim V > \deg F$

$$\bigoplus_{v \in V} F(x+v) = 0, \text{ for every } x \in \mathbf{F}_2^n.$$

Improving upon saturation attacks

Let S be a permutation of algebraic degree d. Let X be the input multiset and $Y = S(X)$ the output multiset.

- If X has $\mathcal{A}$ then Y has $\mathcal{A}$.
- If X has $\mathcal{B}$ then Y has $\mathcal{U}$.

- If X is composed of 2^{d+1} chosen plaintexts, then Y has $\mathcal{B}$.

This last property is not exploited in classical saturation attacks!

Outline

1. Understanding $\mathcal{D}_k^n$ for some specific values of k
2. Propagation of the property through an Sbox
3. Todo's distinguisher on PRESENT

Outline

Some specific values of k

Question: What can be said about a multiset X that verifies a property $\mathcal{D}_k^n$, for some value of k?

- The cases $\mathcal{D}_1^n$, $\mathcal{D}_2^n$, $\mathcal{D}_n^n$, have been characterized.
  - [Todo 2015], [Sun et al. 2015]
- The cases $\mathcal{D}_k^n$, for $k \neq \{1, 2, n\}$ had not been exploited before.
  - We provide some insight on these cases **here**.

The property $\mathcal{D}_1^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

X fulfills $\mathcal{D}_1^n$ **if and only if** its cardinality is even.

Indeed,

- X has the property $\mathcal{D}_1^n$: For $u = (0, \ldots, 0) : \bigoplus_{x \in X} x^u = 0$

$$\Leftrightarrow \bigoplus_{x \in X} x_1^0 \ldots x_n^0 = \bigoplus_{x \in X} 1 = \#X \mod 2 = 0$$

- The inverse can be easily deduced.

The property $\mathcal{D}_2^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

X fulfills $\mathcal{D}_2^n$ **if and only if** its cardinality is even and it has the Balance property.

Balance property: For any i, $1 \leq i \leq n$ $\bigoplus_{x \in X} x_i = 0$.

Indeed, if X has the property $\mathcal{D}_2^n$:

- $\bigoplus_{x \in X} x_1^0 \dots x_n^0 = 0 \Rightarrow X$ has even cardinality.
- For all u with $wt(u) = 1$:
  $\bigoplus_{x \in X} x^u = \bigoplus_{x \in X} x_1^0 \dots x_{i-1}^0 x_i^1 \dots x_n^0 = \bigoplus_{x \in X} x_i = 0$
  $\Rightarrow X$ has the Balance property.

The inverse is proven easily.

Reduced set of a multiset

Let X be a multiset of elements in $\mathbf{F}_2^n$.

The corresponding reduced set $\tilde{X}$ is the set composed of all elements in X having an odd multiplicity.

Example: If $X = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x7}, \texttt{0x7}, \texttt{0xB}, \texttt{0xC}\}$ then

$$\tilde{X} = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x5}, \texttt{0xB}, \texttt{0xC}\}.$$

A multiset X fulfills $\mathcal{D}_k^n$ if and only if $\tilde{X}$ fulfills $\mathcal{D}_k^n$.

The property $\mathcal{D}_n^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

X fulfills $\mathcal{D}_n^n$ **if and only if** its reduced set $\tilde{X}$ is either empty or equal to $\mathbf{F}_2^n$.

This is proved for example in [Sun et al. 2015] in two ways.

- Direct proof by contradiction.
- By proving that for any k,

  if a multiset X has the property $\mathcal{D}_k^n$, then $\#X \geq 2^k$.

The property $\mathcal{D}_k^n$

Proposition. Let X be a multiset of elements in $\mathbf{F}_2^n$ such that $\tilde{X}$ is an (affine) subspace of dimension k. Then X satisfies $\mathcal{D}_k^n$.

Let $u \in \mathbf{F}_2^n$ be any element with $wt(u) < k$. Let

$$U = \{x \in \mathbf{F}_2^n : x_i = 1 \quad \forall i \in \mathsf{Supp}(u)\}$$

Then, for any $x \in \mathbf{F}_2^n$,

$$x^u = 1 \text{ if and only if } x \in U.$$

Therefore,

$$\bigoplus_{x \in X} x^u = |X \cap U| \bmod 2$$

Since X is an (affine) subspace of dimension k, $X \cap U$ is either empty or an (affine) subspace of dimension at least $k - wt(u) \geq 1$. Then, the size of $X \cap U$ is always even.

The property $\mathcal{D}_{n-1}^n$

Let X be a multiset of elements in $\mathbf{F}_2^n$.

Proposition. X satisfies $\mathcal{D}_{n-1}^n$ **if and only if** $\tilde{X}$ is an (affine) subspace of dimension $(n-1)$.

Idea of proof: By induction.

Example [Todo, Eurocrypt 2015]

For the multiset of elements of $\mathbf{F}_2^4$

$$X = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\},$$

the corresponding reduced set

$$\tilde{X} = \{\texttt{0x0}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\}$$

is a linear subspace of dimension 3 spanned by $\{\texttt{0x3}, \texttt{0x5}, \texttt{0x8}\}$.

So, it can be directly deduced (**without computation**) that

X has the property $\mathcal{D}_3^4$.

Outline

Propagation of the division property through an Sbox

- Let S be a permutation of $\mathbf{F}_2^n$ of algebraic degree d.
- Let X be a multiset having the division property $\mathcal{D}_k^n$.

Question: What is the division property of $Y = S(X)$?

- If $k = n$, then Y has the division property $\mathcal{D}_n^n$.

Proposition (Todo):

Y has the division property $\mathcal{D}^n_{\lceil \frac{k}{d} \rceil}$.

Example - MISTY S_7

MISTY's Sbox S_7 is a 7-bit Sbox of degree 3.

- The input set X has the property $\mathcal{D}_k^7$.
- The output set Y has the property $\mathcal{D}_{k'}^7$, with $k' = \lceil \frac{k}{3} \rceil$.

k	0	1	2	3	4	5	6	7
k'	0	1	1	1	2	2	2	7

Proof Sketch

Let the input set X have the division property $\mathcal{D}_k^n$. Then,

$$\bigoplus_{x \in X} x^u = 0, \text{ for all } u \in \mathbf{F}_2^n \text{ with } wt(u) < k.$$

Goal: Evaluate for which $v \in \mathbf{F}_2^n$, $\bigoplus_{x \in X} S(x)^v$ vanishes.

- If $\deg(S^v) < k$ then $\bigoplus_{x \in X} S(x)^v = 0$.
- If $\deg(S^v) \geq k$, $\bigoplus_{x \in X} S(x)^v$ is undetermined.

Obviously, $\deg(S^v) \leq wt(v) \times d$, so the sum becomes unknown if

$$wt(v) \times d \geq k.$$

An improvement idea

In the previous proof, the degree was bounded by

$$\deg(S^v) \leq wt(v) \times d$$

This bound is not tight!

The inverse permutation influences the degree

Let S be a permutation on $\mathbf{F}_2^n$.

Denote by $\delta_k(S)$ the max. degree of the product of k coordinates of S.

Theorem [B.–Canteaut 2013]. For any k and ℓ,

$$\delta_\ell(S) < n - k \text{ if and only if } \delta_k(S^{-1}) < n - \ell.$$

Getting a tighter result

Use the previous theorem to better estimate $\deg(S^v)$:

$$\deg(S^v) \leq \delta_{wt(v)}(S).$$

Then,

$$\delta_{\mathrm{wt}(v)}(S) < k \text{ iff } \delta_{n-k}(S^{-1}) < n - wt(v).$$

By re-writing the second inequality we get

$$\delta_{wt(v)}(S) < k \text{ iff } wt(v) < n - \delta_{n-k}(S^{-1}).$$

The quantity $\bigoplus_{x \in X}(S^v)(x)$ becomes unknown when

$$wt(v) \geq n - \delta_{n-k}(S^{-1}).$$

So Y has the division property $\mathcal{D}^n_{n-\delta_{n-k}(S^{-1})}$.

Example - Back to MISTY S_7

MISTY's inverse Sbox S_7^{-1} is a 7-bit Sbox of degree 3.

k	1	2	3	4	5	6	7
$\delta_k(S_7^{-1})$	3	5	5	6	6	6	7

- The input set X has the property $\mathcal{D}_k^7$.
- The output set Y has the property $\mathcal{D}_{k'}^7$, with
  - $k' = \lceil \frac{k}{3} \rceil$ (Todo's estimation)
  - $k' = 7 - \delta_{7-k}(S_7^{-1})$ (our estimation)

k	0	1	2	3	4	5	6	7
k' (Todo's)	0	1	1	1	2	2	2	7
k' (our)	0	1	1	1	2	2	**4**	7

For $k = 6$: $k' = 7 - \delta_{7-6}(S_7^{-1}) = 7 - 3 = 4$

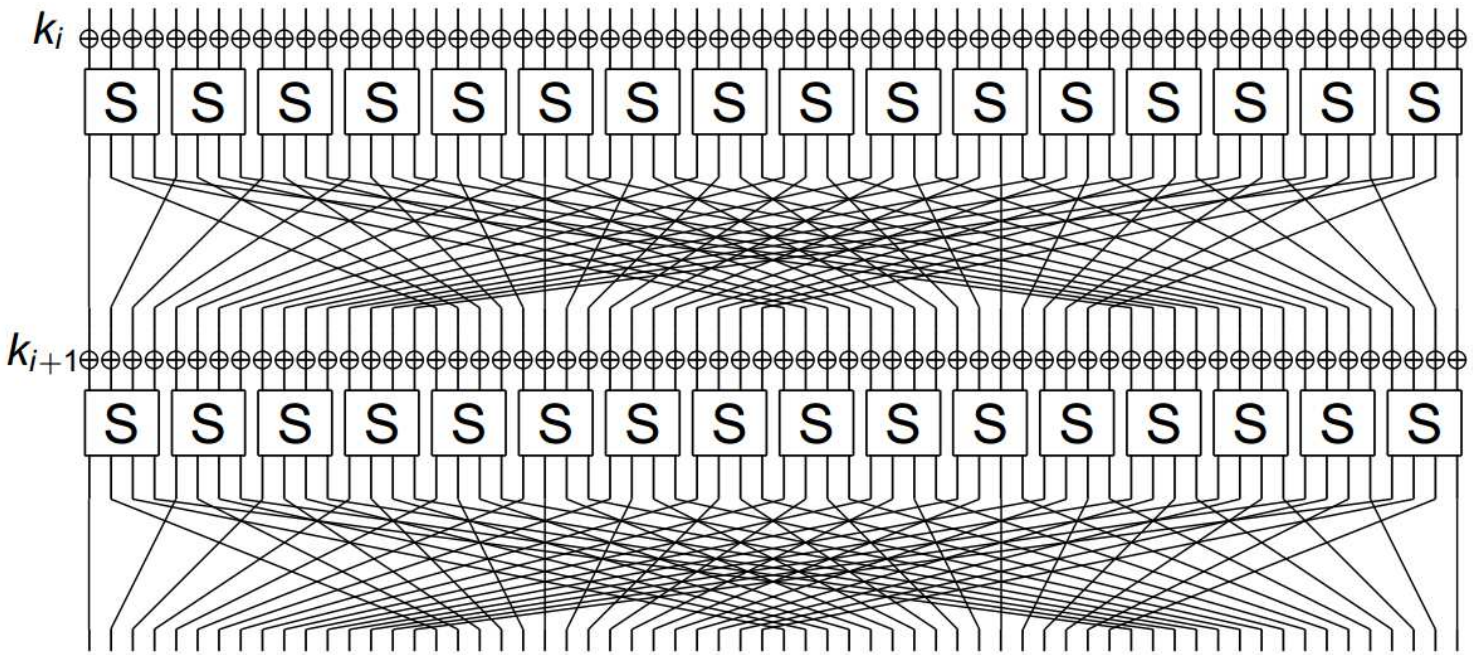
Outline

PRESENT

[Bogdanov – Knudsen – Le – Paar – Poschmann – Robshaw – Seurin – Vikkelsoe 2007]

64-bit block cipher with 80/128-bit key and 31 rounds.

- Confusion : Use of a 4-bit Sbox of degree 3.



Algebraic degree of PRESENT

Estimate the algebraic degree of PRESENT after several rounds:
Let R denote PRESENT's round function.

- **Trivial bound** : $\deg(R^{r+1}) \leq 3 \cdot \deg(R^r)$
- **Bound for SPN** [B.—Canteaut—De Cannière 2011]

$$\deg(R^{r+1}) \leq 64 - \frac{64 - \deg(R^r)}{3}$$

Rounds (r)	1	2	3	4	5	6	7
Degree	3	9	27	51	59	62	63

Distinguisher based on the algebraic degree

If after r rounds the degree is d, then for any subspace V of dimension $d+1$

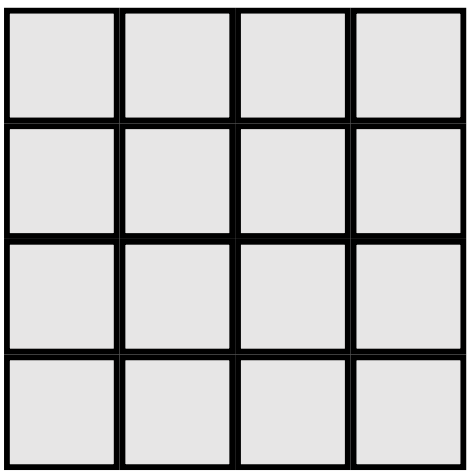
$$\bigoplus_{v \in V} R^r(x+v) = 0, \text{ for every } x \in \mathbf{F}_2^n.$$

$\rightarrow$ Distinguisher with 2^{r+1} plaintexts.

Rounds (r)	3	4	5	6
$\log_2$(#plaintexts)	28	52	60	63

Todo's distinguishers on PRESENT

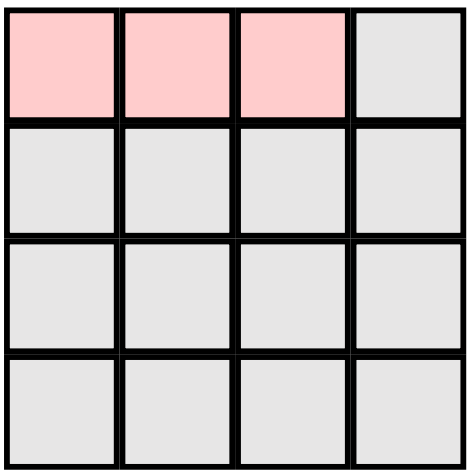
Equivalent representation of PRESENT's state (16 4-bit words)



Todo's distinguishers on PRESENT

Choose the number of required chosen plaintexts, say 2^D.

Example: $D = 12$

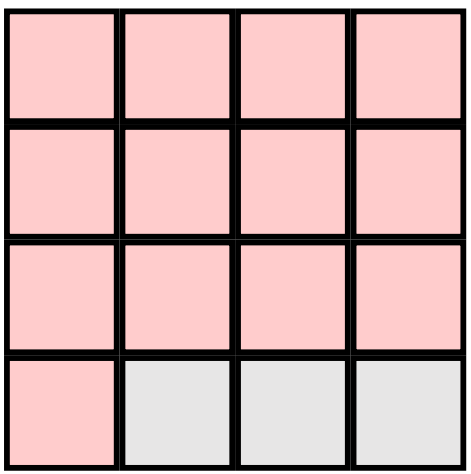


- ■ words take all possible values.
- ■ words are fixed to a constant value for all texts.

Todo's distinguishers on PRESENT

Choose the number of required chosen plaintexts, say 2^D.

Example: $D = 52$



- ■ words take all possible values.
- ■ words are fixed to a constant value for all texts.

Todo's distinguishers on PRESENT

Algorithm for computing the propagation of the division property.

- Confusion part: Compute the propagation for each Sbox. Only the degree is taken into account.
- Diffusion layer: The particular description of the linear layer is not exploited.

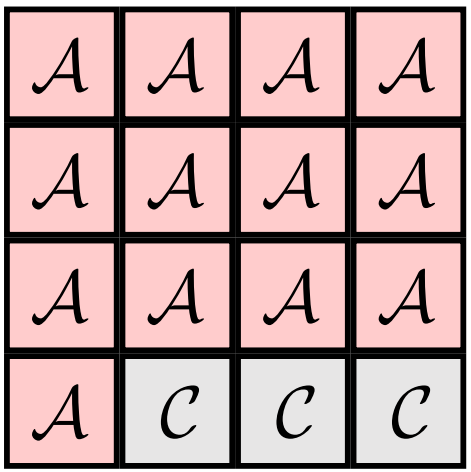
	$r = 3$	$r = 4$	$r = 5$	$r = 6$
Degree	28	52	60	63
Division property	12	28	52	60

Table: $\log_2(\#\text{plaintexts})$

How can these results be explained

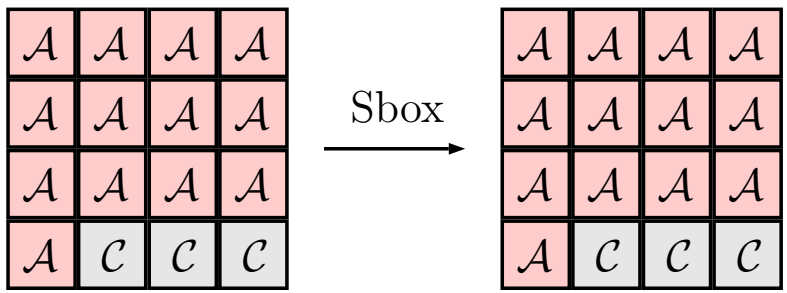
Combination of saturation and higher-order differential attack

- Saturate some words of the first round.



How can these results be explained

- Saturate some words of the first round.
- After the confusion layer, the all and constant properties remain unchanged.
- Start from a subspace after the non-linear layer and apply the bound on the degree.



- Gain of one round compared to the higher-order differential distinguisher.
- Prepend a one-round saturation property to the higher-order differential distinguisher.

New distinguishers on PRESENT (Work in progress)

We can obtain distinguishers reaching a higher number of rounds for PRESENT for the same data complexity.

Exploit the division property, but take into account

- Sbox properties
- linear layer properties

Example: With 2^{12} chosen plaintexts, distinguisher on 5 rounds (2 more rounds than Todo's generic method).

Conclusion

- New interesting property proposed recently by Todo.
- This property is far from being fully understood and many aspects of the division property are left to be explored.
- Better understand how the property is propagated through the linear and non-linear components.

Conclusion

- New interesting property proposed recently by Todo.
- This property is far from being fully understood and many aspects of the division property are left to be explored.
- Better understand how the property is propagated through the linear and non-linear components.

Thanks for your attention!