

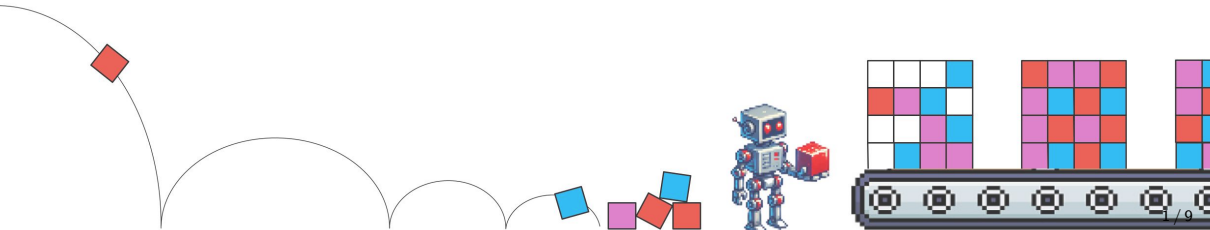
# MILP tool for complete Differential MITM attacks

*Inria*

Bastien Michel  
COSMIQ team  
Inria, Paris



European Research Council  
Established by the European Commission



# Overview

---

## 1. Differential MITM

## 2. Tool

# Differential MITM

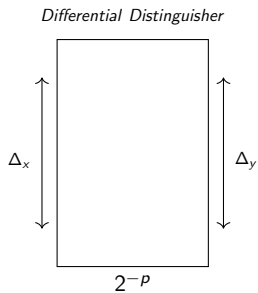
---

- Presented in [NPBD<sup>+</sup>23] at Crypto 2023

# Differential MITM

---

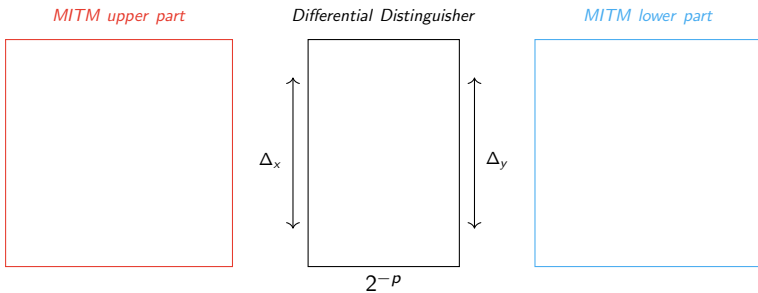
- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



# Differential MITM

---

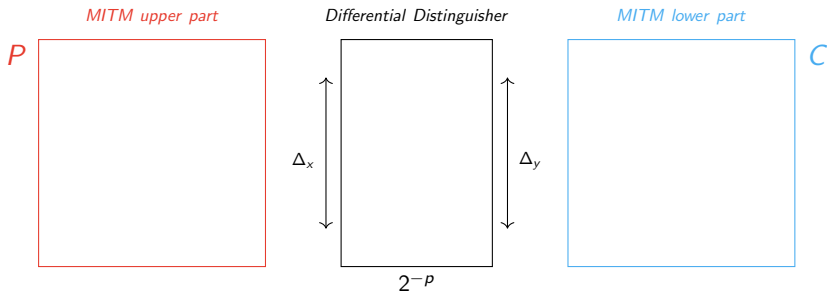
- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



# Differential MITM

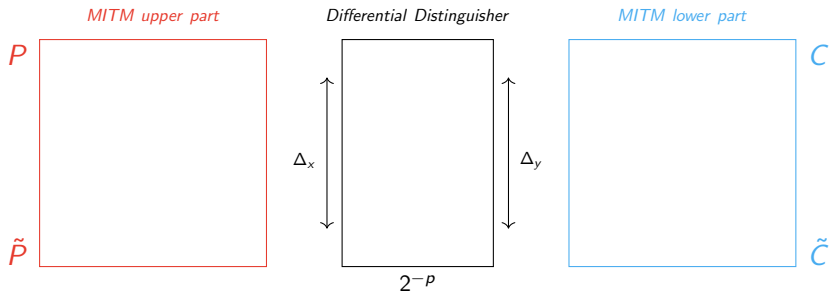
---

- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



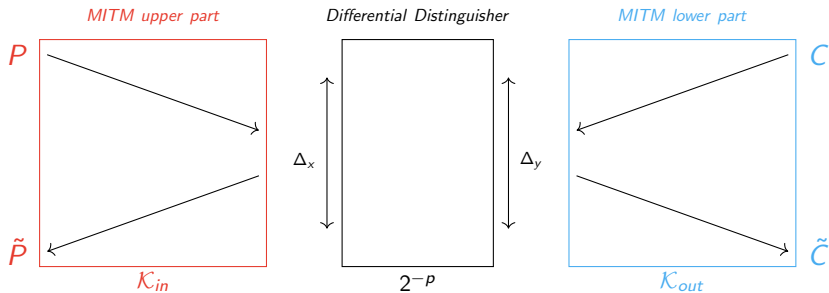
# Differential MITM

- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



# Differential MITM

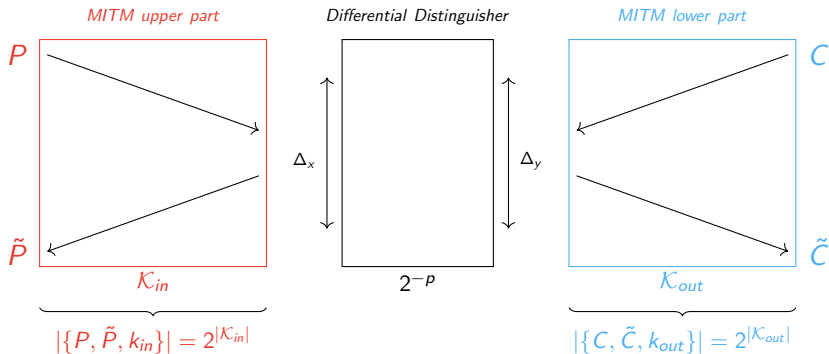
- Presented in [NPBD<sup>+</sup>23] at Crypto 2023





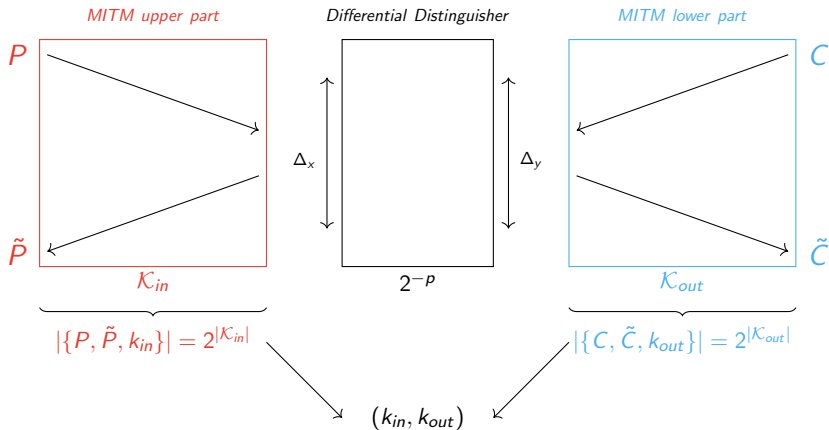
# Differential MITM

- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



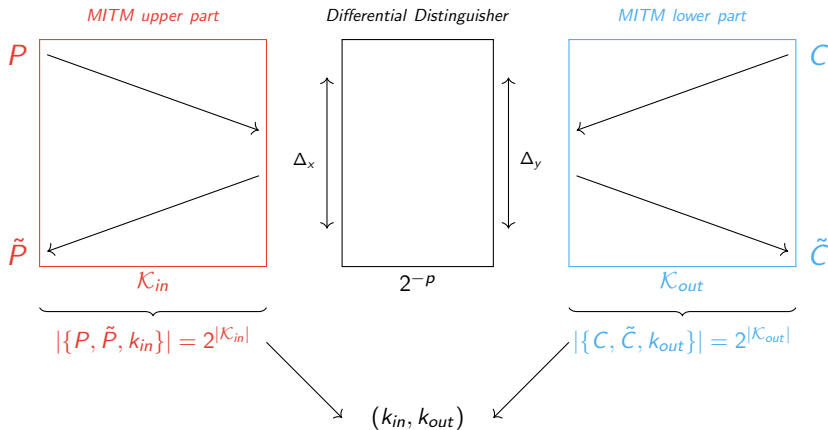
# Differential MITM

- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



# Differential MITM

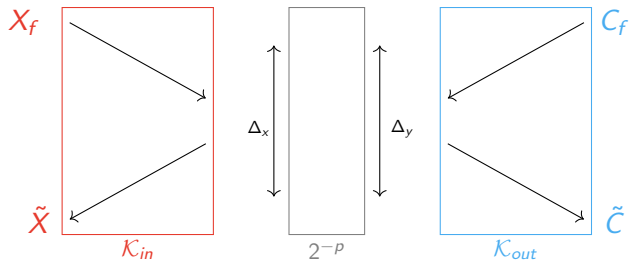
- Presented in [NPBD<sup>+</sup>23] at Crypto 2023



$$\mathcal{T} = 2^P (2^{k_{in}} + 2^{k_{out}} + 2^{k_{in} + k_{out} - k_{in} \cap k_{out} - n})$$

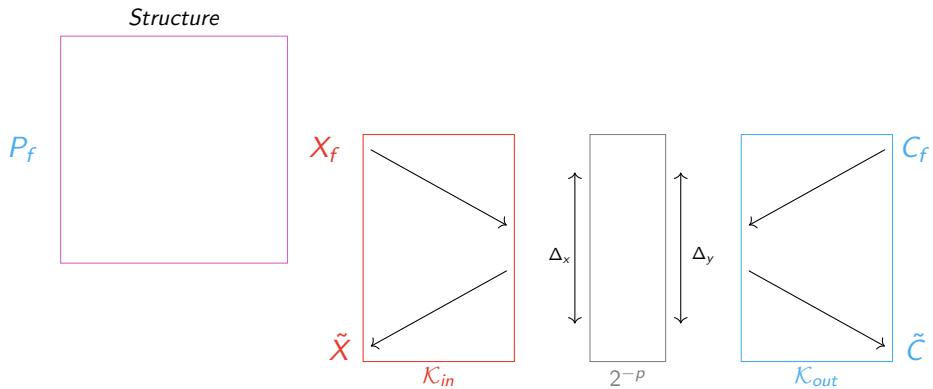
# Parallel Partitioning

---



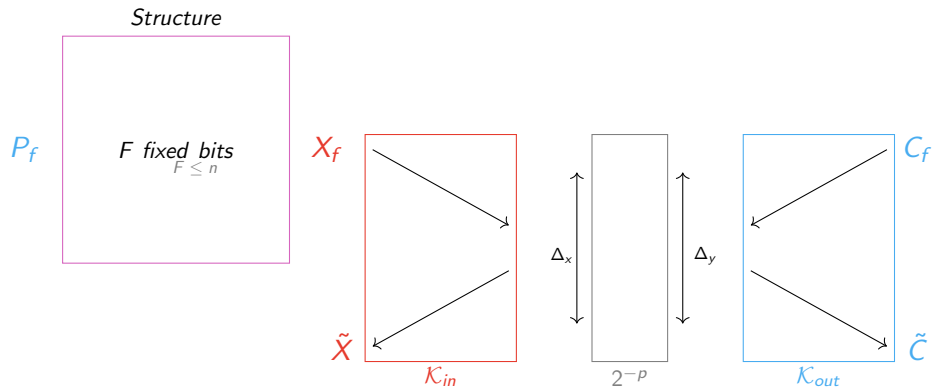
# Parallel Partitioning

---

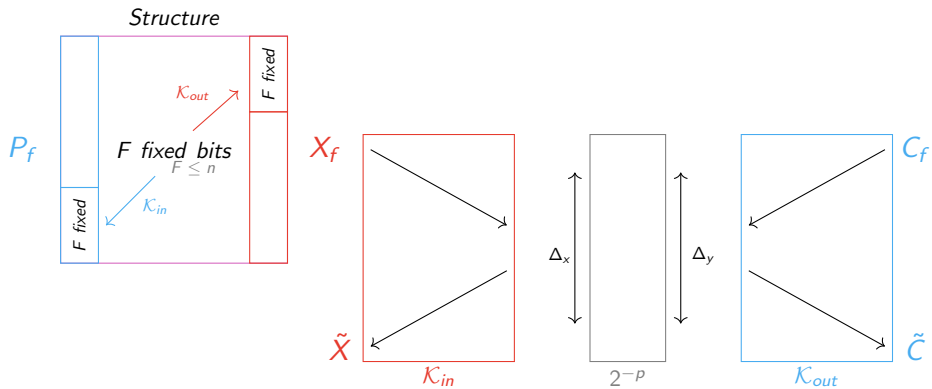


# Parallel Partitioning

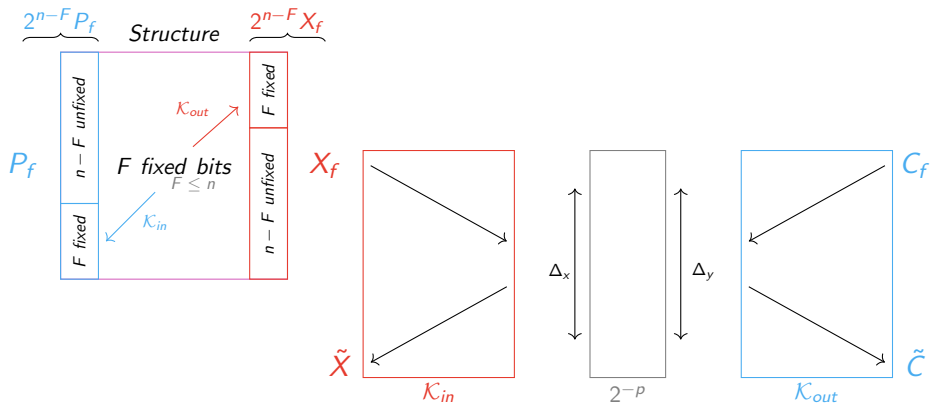
---



# Parallel Partitioning

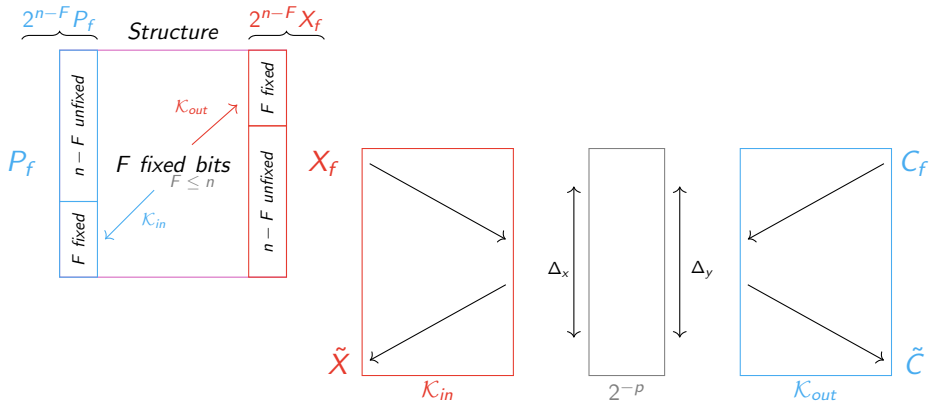


# Parallel Partitioning





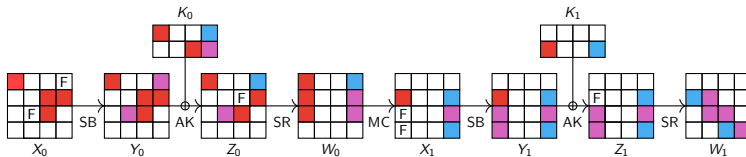
# Parallel Partitioning



$$\mathcal{T} = 2^{p-(n-F)} (2^{n-F} 2^{k_{in}} + 2^{n-F} 2^{k_{out}} + 2^{2(n-F)+k_{in}+k_{out}-k_{in} \cap k_{out}-F-F_{filter}})$$

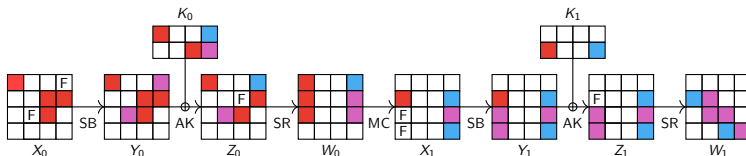
# Structure (example on Skinny)

In [AKM<sup>+</sup>24] and [NPBD<sup>+</sup>23], structures on 2 rounds were added by hand :

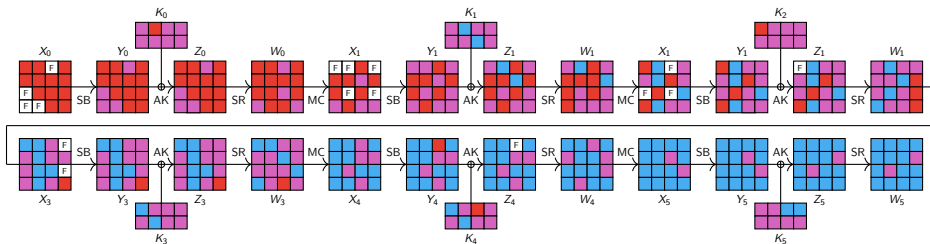


# Structure (example on Skinny)

In [AKM<sup>+</sup>24] and [NPBD<sup>+</sup>23], structures on 2 rounds were added by hand :



In [DHS<sup>+</sup>21], an automated tool is used to find structures on 6 rounds for MITM attacks (improved in [BGST22] with superposition) :



# Automating the search of the attack

---

## Problem

**Searching** for the **optimal attack** can be very **complex** by hand because of the technicality of the attack.

# Automating the search of the attack

---

## Problem

**Searching** for the **optimal attack** can be very **complex** by hand because of the technicality of the attack.

## Solution

**Develop a tool** that **search** for the distinguisher, the MITM key recovery path and the structure at the same time to find the **optimal attack**.

# Automating the search of the attack

---

## Problem

**Searching** for the **optimal attack** can be very **complex** by hand because of the technicality of the attack.

## Solution

**Develop a tool** that **search** for the distinguisher, the MITM key recovery path and the structure at the same time to find the **optimal attack**.

## State of the art

1. In [AKM<sup>+</sup>24] a **MILP model** was proposed to find the **optimal distinguisher and MITM propagation**, the structure was then added by hand.
2. In [DHS<sup>+</sup>21], an **automated tool** is used to **found structures** on more than two rounds.

# Automating the search of the attack

---

## Problem

**Searching** for the **optimal attack** can be very **complex** by hand because of the technicality of the attack.

## Solution

**Develop a tool** that **search** for the distinguisher, the MITM key recovery path and the structure at the same time to find the **optimal attack**.

## State of the art

1. In [AKM<sup>+</sup>24] a **MILP model** was proposed to find the **optimal distinguisher and MITM propagation**, the structure was then added by hand.
2. In [DHS<sup>+</sup>21], an **automated tool** is used to **found structures** on more than two rounds.

## Objective

Develop an **improved tool** that search for the **optimal attack** including **complex structure**.

# Brief look at the tool

---

## Current Model

The current model is **dedicated** (Skinny and Craft) and take as **arguments** the **size of each part** (structure, MITM and distinguisher).



# Brief look at the tool

---

## Current Model

The current model is **dedicated** (Skinny and Craft) and take as **arguments** the **size of each part** (structure, MITM and distinguisher).

## Search Time

For attacks on 23 rounds Skinny, around **13 000 to 16 000 integer variables** are used and search time can go from **30 minutes to 7-8 hours**.

# Brief look at the tool

## Current Model

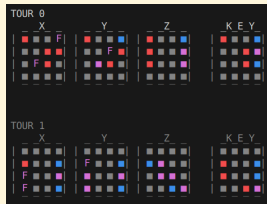
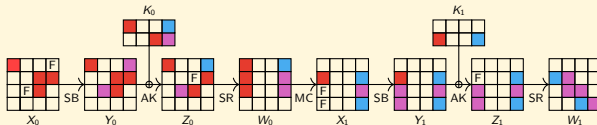
The current model is **dedicated** (Skinny and Craft) and take as **arguments** the **size of each part** (structure, MITM and distinguisher).

## Search Time

For attacks on 23 rounds Skinny, around **13 000 to 16 000 integer variables** are used and search time can go from **30 minutes to 7-8 hours**.

## Human Friendly Results

We expect the tool to have a **nice interface**, so the results it finds can be used simply by any cryptanalyst. For now we **display** the **full path** of the attacks and all the parameters of the attacks directly in the terminal.



# Current results and future work

---

## First Results

**Recover** the full truncated differential MITM **attacks** on Skinny and Craft **proposed in [AKM<sup>+</sup>24]**

# Current results and future work

---

## First Results

**Recover** the full truncated differential MITM **attacks** on Skinny and Craft **proposed in [AKM<sup>+</sup>24]**

## Current limitation

1. **Convergence time** is **too long** with too many variables restricting our study to blocks of 16 cells.
2. Optimal attack **search** needs to be performed for **every round parameters** (structure, distinguisher and MITM size) since the model cannot change them automatically (overcome with parallelization) .
3. **Convergence time** is **too long** for classic differential **distinguisher** on **more than 10 rounds**.

# Current results and future work

---

## First Results

**Recover** the full truncated differential MITM **attacks** on Skinny and Craft **proposed in [AKM<sup>+</sup>24]**

## Current limitation





1. **Convergence time** is **too long** with too many variables restricting our study to blocks of 16 cells.
2. Optimal attack **search** needs to be performed for **every round parameters** (structure, distinguisher and MITM size) since the model cannot change them automatically (overcome with parallelization) .
3. **Convergence time** is **too long** for classic differential **distinguisher** on **more than 10 rounds**.

## Next Objective

1. **Generalize the tool** for **SPN** - AES like ciphers.
2. **Decrease the time search** by decreasing the number of variables and inequalities.
3. Improve the distinguisher search with **mix truncated and classic differential trails**.
4. **Improve** the structure part to include more **complex structures**.

# References

---

-  Zahra Ahmadian, Akram Khalesi, Dounia M'foukh, Hossein Moghimi, and María Naya-Plasencia, *Improved differential meet-in-the-middle cryptanalysis*, Springer-Verlag, 2024.
-  Zhenzhen Bao, Jian Guo, Danping Shi, and Yi Tu, *Superposition meet-in-the-middle attacks: Updates on fundamental security of aes-like ciphers*, Springer-Verlag, 2022.
-  Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, and Lei Hu, *Meet-in-the-middle attacks revisited: Key-recovery, collision, and preimage attacks*, Springer-Verlag, 2021.
-  María Naya-Plasencia, Christina Boura, Nicolas David, Patrick Derbez, and Gregor Leander, *Differential meet-in-the-middle cryptanalysis*, Springer-Verlag, 2023.