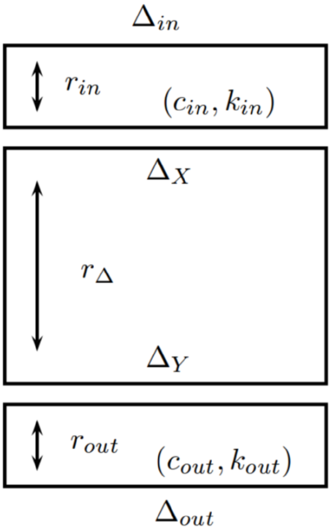
Minimalist model for Impossible Differentials

Patrick Derbez[1], Marie Euler[1,2]

[1] Univ Rennes, Inria, CNRS, IRISA
[2] DGA

Impossible Differential Cryptanalysis



Setup

top $P[\Delta_{in} \rightarrow \Delta_X] = 2^{-c_{in}}$

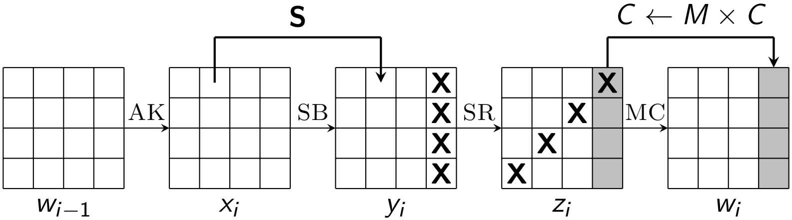
middle $P[\Delta_X \rightarrow \Delta_Y] = 0$

bottom $P[\Delta_{out} \rightarrow \Delta_Y] = 2^{-c_{out}}$

Main idea

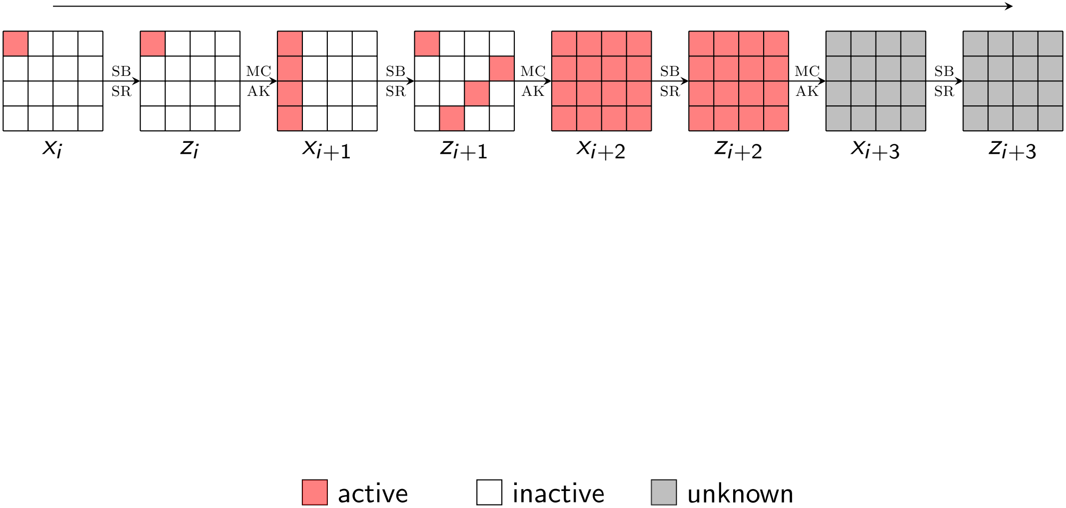
If a candidate key partially encrypts/decrypts a given pair to an impossible differential then this key is **wrong**.

The Advanced Standard Encryption

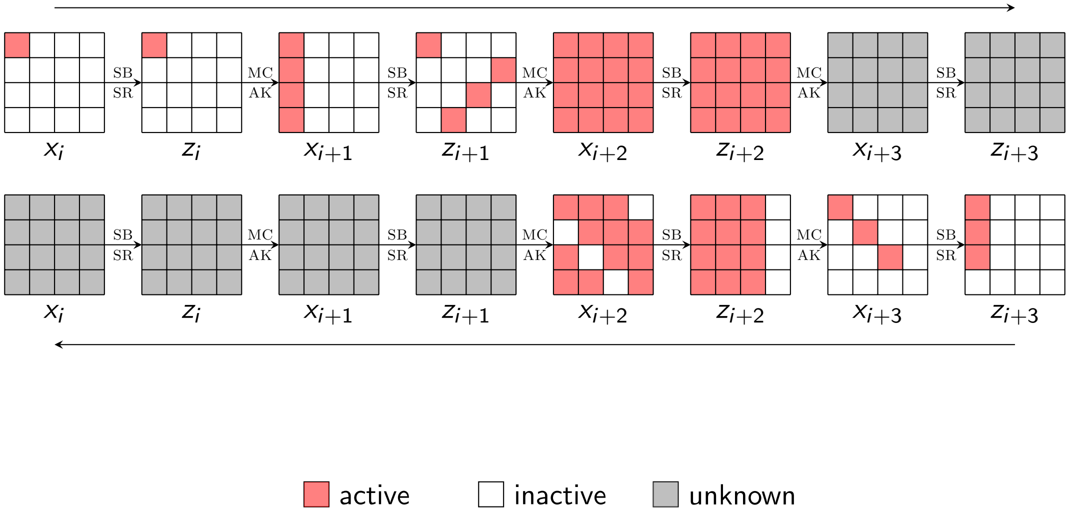


- **Standardized** in 2001 for 3 key lengths: 128, 192 and 256 bits
- Block size of 128 bits: 4×4 matrix of bytes
- An AES round applies $\mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB} \circ \mathrm{AK}$ to the state
- No MixColumns in the last round

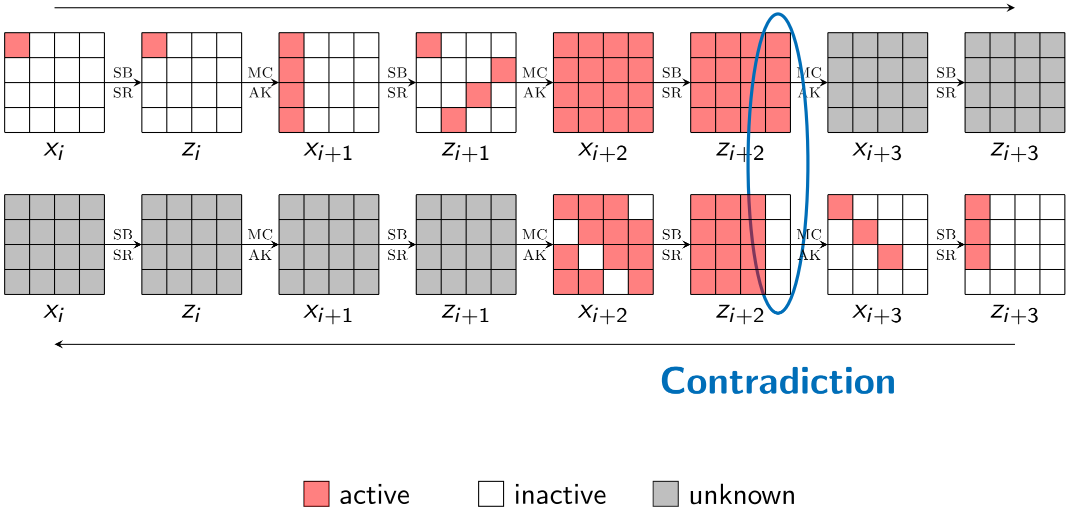
Impossible Differential on AES



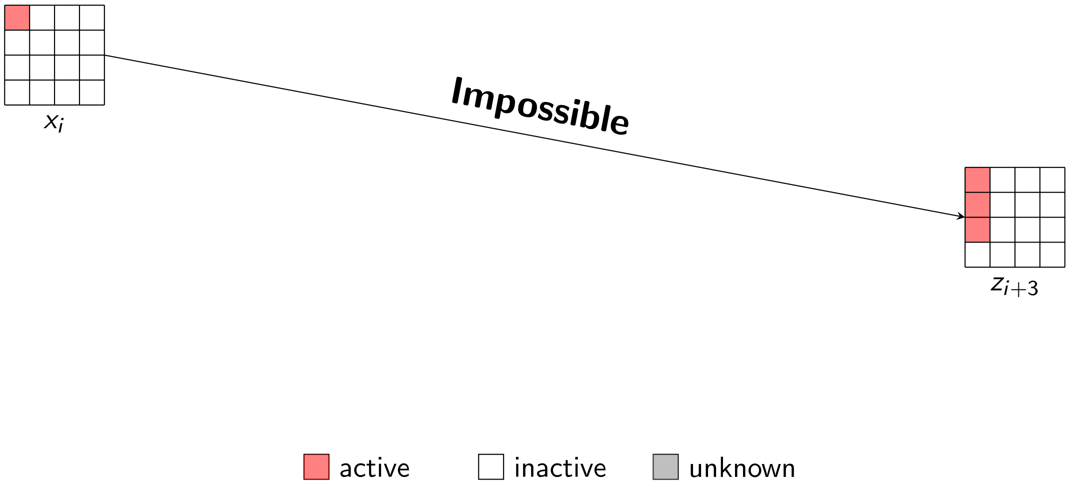
Impossible Differential on AES



Impossible Differential on AES



Impossible Differential on AES



Searching for Impossible Differentials (Models)

- **Basic model v1**
  - Fix both the input and output differences
  - Propagate them with probability 1

The differential is impossible if and only if the model has no solution

Searching for Impossible Differentials (Models)

- **Basic model v1**
  - Fix both the input and output differences
  - Propagate them with probability 1

The differential is impossible if and only if the model has no solution

- **Problems**
  - Both the input and the output differences have to be fixed
    - In the arbitrary S-box model, only inputs and outputs with 1 active S-box have to be tested. [SLG+16]
  - Negative model $\longrightarrow$ **unsuitable to search for attacks**

[SLG + 16] Sun et al. *Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis.* EUROCRYPT 2016

Searching for Impossible Differentials (Models)

- **Basic model v2** [ST17]
  - Fix both the input and output differences
  - Search for a differential characteristic

The differential is impossible if and only if the model has no solution

- **Problems**
  - Both the input and the output differences have to be fixed
    - In the arbitrary S-box model, only inputs and outputs with 1 active S-box have to be tested. [SLG+16]
  - Negative model $\longrightarrow$ **unsuitable to search for attacks**

[SLG + 16] Sun et al. *Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis.* EUROCRYPT 2016
[ST17] Sasaki et al. *New impossible differential search tool from design and cryptanalysis aspects.* EUROCRYPT 2017

Searching for Impossible Differentials (Models)

- **Model v3** [HSE23]
  - 2 trails propagating with probability 1
  - Enumerate all possible contradictions

The differential is impossible if and only if there is at least one contradiction

[HSE23] Hadipour et al. *Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks.* EUROCRYPT 2023

Searching for Impossible Differentials (Models)

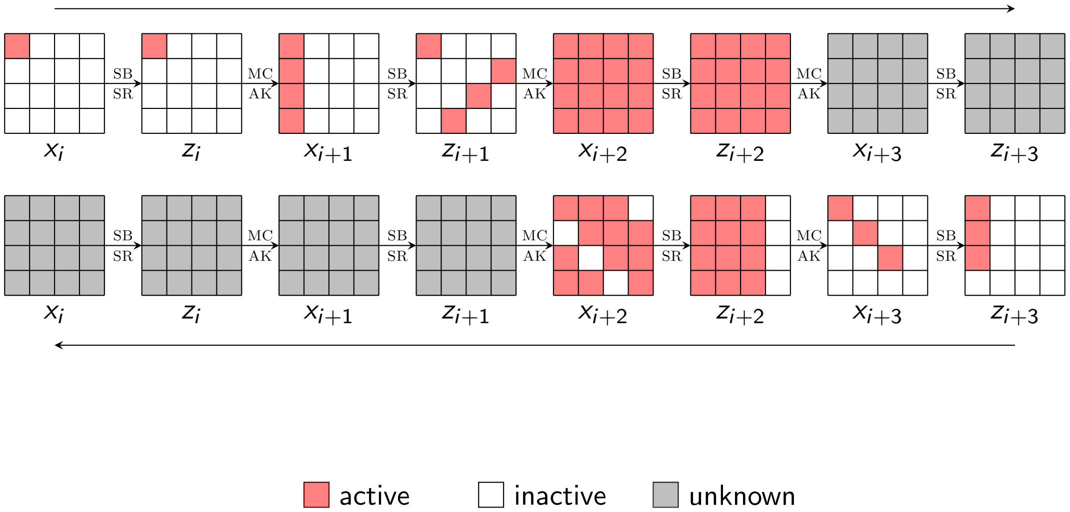
- **Model v3** [HSE23]
  - 2 trails propagating with probability 1
  - Enumerate all possible contradictions

The differential is impossible if and only if there is at least one contradiction

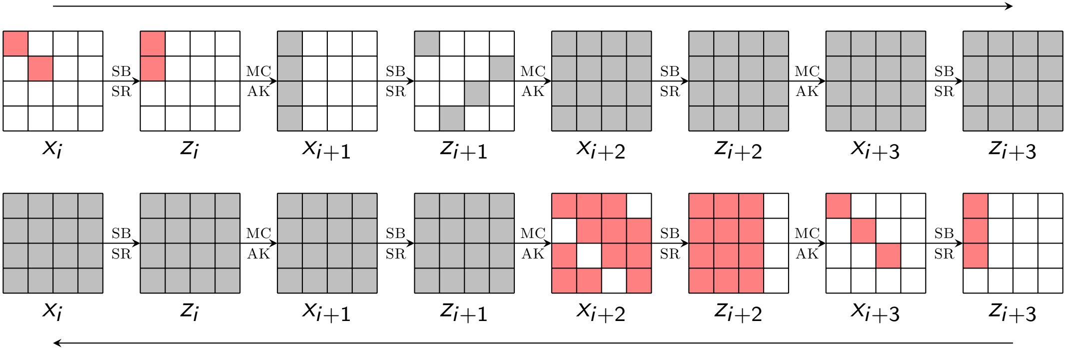
- **Limits**
  - One boolean variable per contradiction
  - Only handle direct contradictions

[HSE23] Hadipour et al. *Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks.* EUROCRYPT 2023

ID on AES - Indirect Contradictions

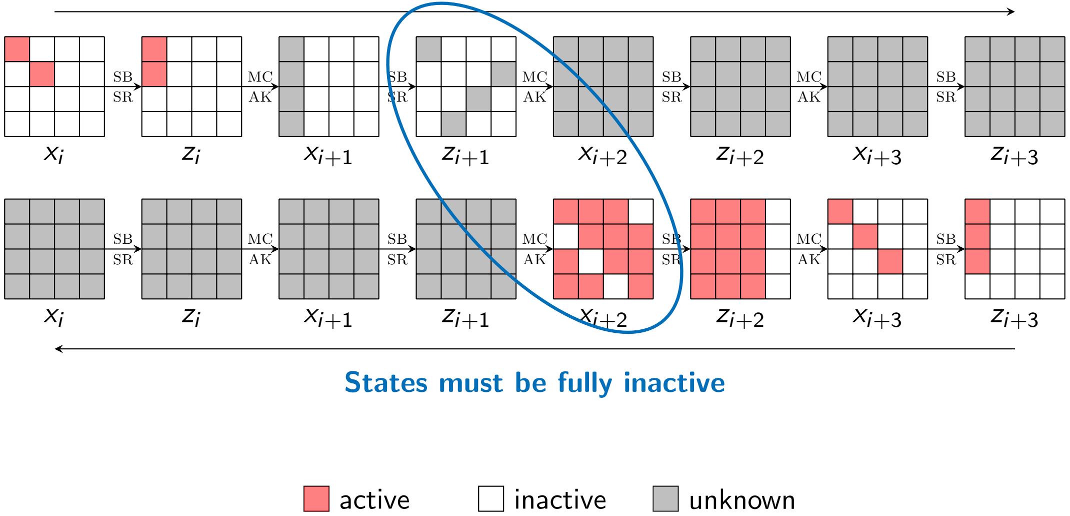


ID on AES - Indirect Contradictions

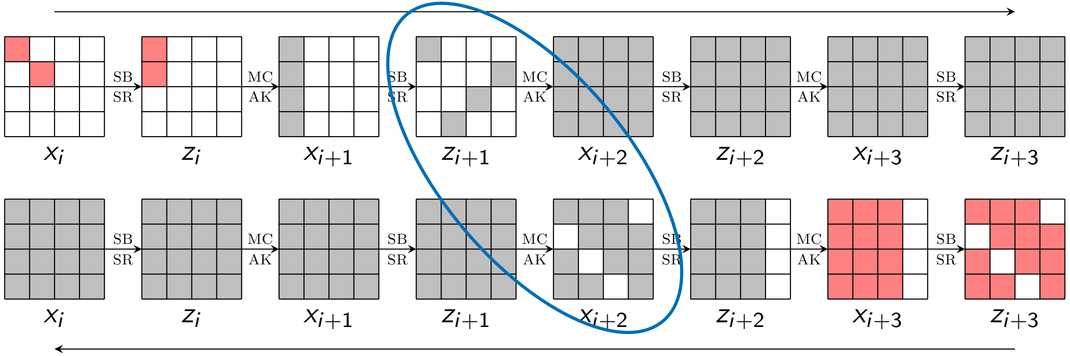


active inactive unknown

ID on AES - Indirect Contradictions



ID on AES - Indirect Contradictions

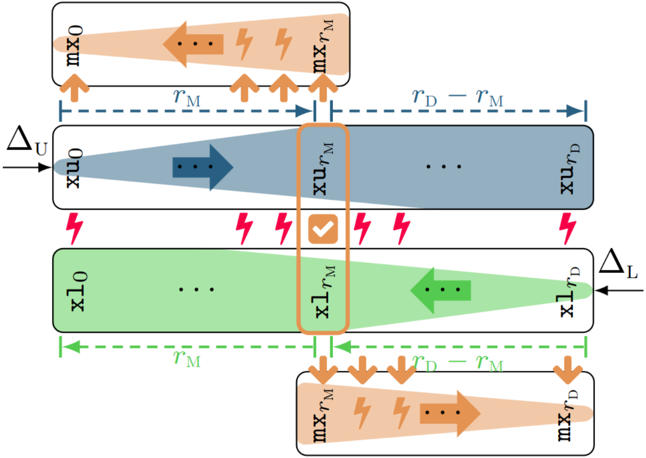


States must be fully inactive

active inactive unknown

Model for Indirect Contradictions

- New model by Chakraborty et al. [CHNE24]
- Second propagation of information from a middle round

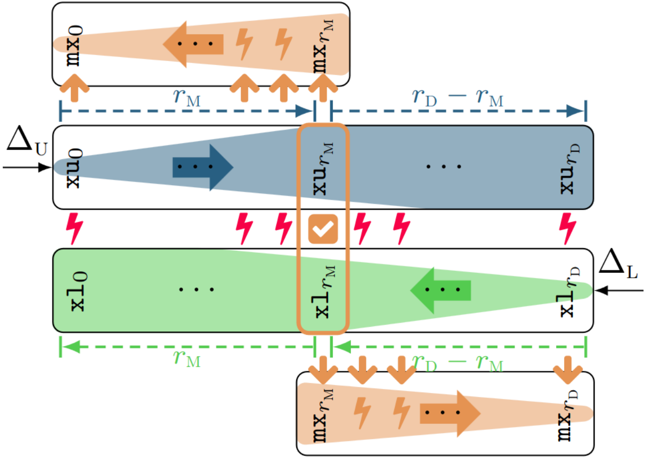


[CHNE24] Chakraborty et al. *Finding complete impossible differential attacks on AndRX ciphers and efficient distinguishers for ARX designs.* ToSC 2024-3

Model for Indirect Contradictions

- New model by Chakraborty et al. [CHNE24]
- Second propagation of information from a middle round

Are all indirect contradictions handled?



[CHNE24] Chakraborty et al. *Finding complete impossible differential attacks on AndRX ciphers and efficient distinguishers for ARX designs.* ToSC 2024-3

A Counter-Example

Let consider the two following S-boxes:

- $S_1 = [2, 9, 15, 4, 11, 14, 1, 2, 0, 3, 6, 13, 5, 8, 10, 7]$
- $S_2 = [1, 11, 6, 0, 14, 13, 5, 10, 12, 2, 9, 7, 3, 8, 15, 4]$

Claim: the model of [CHNE24] cannot prove the impossibility of the transition

$$1110 \xrightarrow{S_1} \xrightarrow{S_2} 1100$$

A Counter-Example

Let consider the two following S-boxes:

- $S_1 = [2, 9, 15, 4, 11, 14, 1, 2, 0, 3, 6, 13, 5, 8, 10, 7]$
- $S_2 = [1, 11, 6, 0, 14, 13, 5, 10, 12, 2, 9, 7, 3, 8, 15, 4]$

Claim: the model of [CHNE24] cannot prove the impossibility of the transition

$$1110 \xrightarrow{S_1} \xrightarrow{S_2} 1100$$

- $1110 \xrightarrow{S_1} 0{*}{*}{*}$
- $1100 \xrightarrow{S_2^{-1}} {*}{*}{*}0$

A Counter-Example

Let consider the two following S-boxes:

- $S_1 = [2, 9, 15, 4, 11, 14, 1, 2, 0, 3, 6, 13, 5, 8, 10, 7]$
- $S_2 = [1, 11, 6, 0, 14, 13, 5, 10, 12, 2, 9, 7, 3, 8, 15, 4]$

Claim: the model of [CHNE24] cannot prove the impossibility of the transition

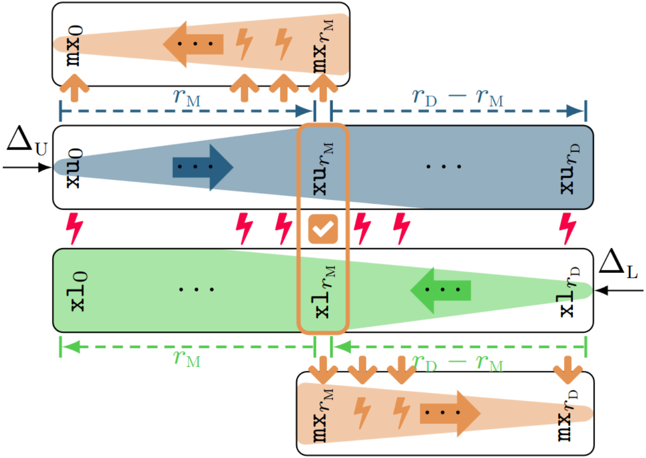
$$1110 \xrightarrow{S_1} \xrightarrow{S_2} 1100$$

- $1110 \xrightarrow{S_1} 0{*}{*}{*}$
- $1100 \xrightarrow{S_2^{-1}} {*}{*}{*}0$

- $0{*}{*}0 \xrightarrow{S_1^{-1}} 1110$ and $0{*}{*}0 \xrightarrow{S_2} 1100$ are valid
- **Need extra deduction steps:**
  - $0{*}{*}0 \xrightarrow{S_1^{-1}} 1110$ valid only if input is $00{*}0$
  - $0{*}{*}0 \xrightarrow{S_2} 1100$ valid only if input is $0{*}00$

Model for Indirect Contradictions

- New model by Chakraborty et al. [CHNE24]
- Second propagation of information from a middle round



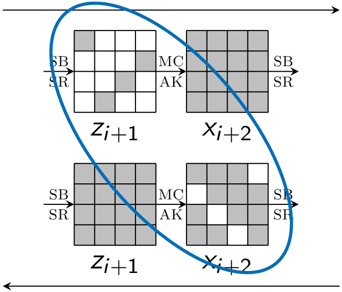
Are all indirect contradictions handled?

[CHNE24] Chakraborty et al. *Finding complete impossible differential attacks on AndRX ciphers and efficient distinguishers for ARX designs.* ToSC 2024-3

A New Idea

Do not search for ID but for probable ID

- An indirect contradiction implies that some *unknown* bits in both trails are resolved to either 0 and/or 1
- Search for pairs of input/output differences generating new 0s or 1s
- Check a posteriori whether the differential is **really impossible**



New zeros are created

MILP Model with Callbacks

Generator model

- Search for ID distinguisher/attack against a target
- Constraints for the ID distinguisher:
  1. at least a direct contradiction
  2. or at least a new 0 or 1 is created when merging the trails

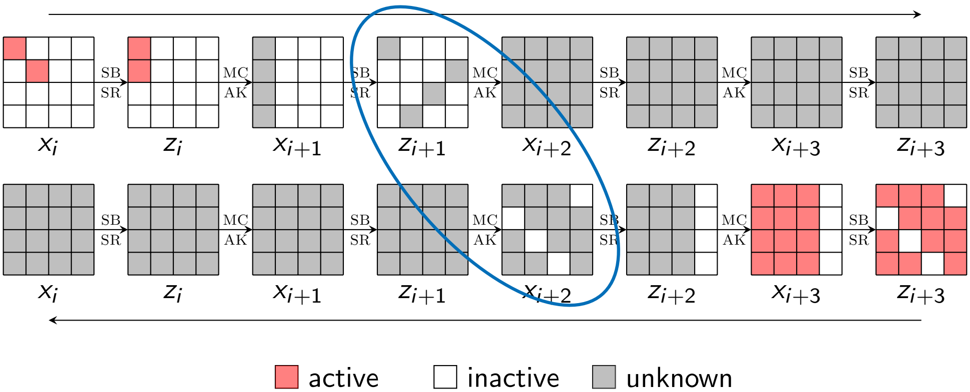
  } **Positive model!**
- Might output false positives ...

Validator model

- Called by the generator model on its solutions
- Verifies the validity of the distinguisher, otherwise discards it in the generator model
- Does not need to be a positive model and can be as precise as we wish (e.g. [ST17], quasidifferentials, ...)

Simplifying the Generator Model

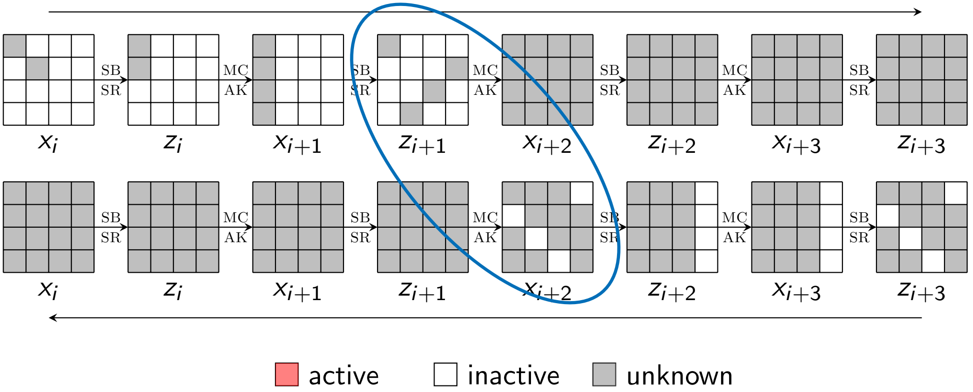
1s propagate badly through ciphers



Simplifying the Generator Model

1s propagate badly through ciphers $\longrightarrow$ **Remove them!**

A differential is impossible iff the only solution is to set all differences to zero



Simplifying the Generator Model

1s propagate badly through ciphers $\longrightarrow$ **Remove them!**

A differential is impossible iff the only solution is to set all differences to zero

Generator model

- Search for ID distinguisher/attack against a target
- Constraints for the ID distinguisher:
  1. at least a direct contradiction
  2. or at least a new 0 or 1 is created when merging the trails

  Positive model!
- Might output false positives ...

Simplifying the Generator Model

1s propagate badly through ciphers ⟶ **Remove them!**

A differential is impossible iff the only solution is to set all differences to zero

Generator model

- Search for ID distinguisher/attack against a target
- Constraints for the ID distinguisher:
  1. ~~at least a direct contradiction~~
  2. or at least a new 0 ~~or 1~~ is created when merging the trails

  Positive model!
- Might output false positives ...

Simplifying the Generator Model

1s propagate badly through ciphers $\longrightarrow$ **Remove them!**

A differential is impossible iff the only solution is to set all differences to zero

Generator model

- Search for ID distinguisher/attack against a target
- Constraints for the ID distinguisher:
  1. ~~at least a direct contradiction~~
  2. or at least a new 0 ~~or 1~~ is created when merging the trails

  } **Positive model!**
- Might output false positives ...

Limits

- Bit-oriented ciphers ... e.g. for `PRESENT`, the transition $1001 \xrightarrow{S} \ast\ast\ast0$ holds with probability 1 but not $\ast00\ast \xrightarrow{S} \ast\ast\ast0$
- **Solution:** allow $\ast00\ast \xrightarrow{S} \ast\ast\ast0$ and delegate to the validator model

Results

- We were able to retrieve the best attacks/distinguishers on **many ciphers**: AES, SKINNY, Midori, SIMON, SIMECK, SPECK
- We also applied it on ARADI and found a new 13-round attack with complexity $2^{224.47}$
- **Number of false positives:**

Version	r_D	Generated candidates (Valid ones)	Time	Deduced inactive cells	Active bits
Simeck-32	11	7 (2)	0.8s	6	2
	12	805 (0)	37s	-	-
Simeck-48	15	8 (1)	1s	4	2
	16	22 (0)	2.7s	-	-
Simeck-64	17	25 (1)	5s	6	2
	18	184 (0)	30s	-	-

(a) Objective function : maximize the number of deduced inactive cells

Summary

- A new, more complete, approach for **indirect contradictions**
- Searching for **probable** ID distinguishers instead of ID distinguisher
- Simplification of the model

Open question: Can we apply the same strategy to other cryptanalysis techniques?

Summary

- A new, more complete, approach for **indirect contradictions**
- Searching for **probable** ID distinguishers instead of ID distinguisher
- Simplification of the model

Open question: Can we apply the same strategy to other cryptanalysis techniques?

Thank you for your attention!