New Yoyo Tricks with AES-based Permutations

Dhiman Saha[1], **Mostafizar Rahman**[2], Goutam Paul[2]

[1]Indian Institute of Technology, Bhilai
[2]Indian Statistical Institute, Kolkata

FSE 2019
Paris, FRANCE

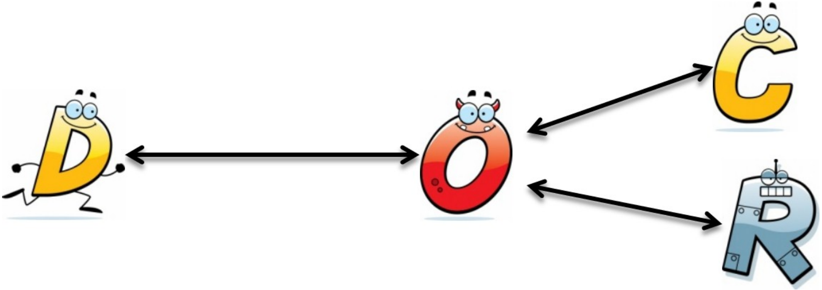
The Problem: Devising Distinguishers

Distinguish between **what** and **why**?

Exhibiting Non-random Behavior

The Distinguishing Setting

1. D tries to distinguish between C and R
2. Can make queries to O
3. O behaves as either C or R
4. At the end D has to guess who is O impersonating
5. D wins if its guess is right



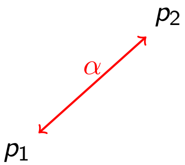
Lets play a Game

Setting: Adaptive Chosen Plaintext/Ciphertext

Will look similar to Boomerang Attack

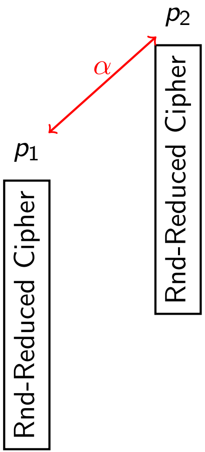
Select messages p_1, p_2 with $p_1 \oplus p_2 = \alpha$

Is there a special way to choose α?



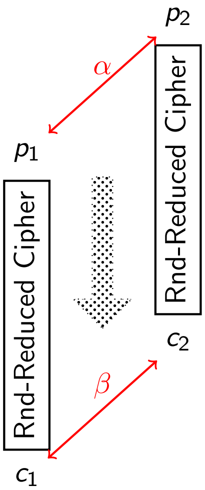
Apply some rounds of some cipher

How many rounds? What type of cipher?



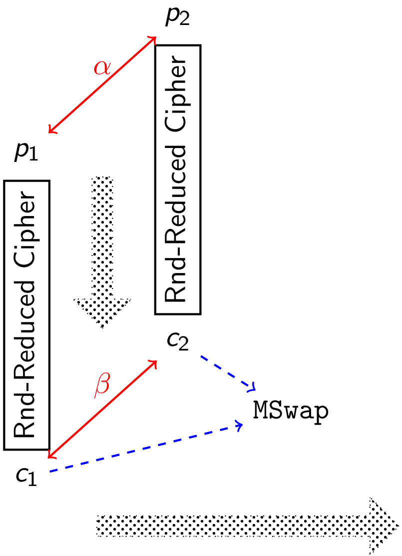
Get c_1, c_2 with $c_1 \oplus c_2 = \beta$

β is the ciphertext difference



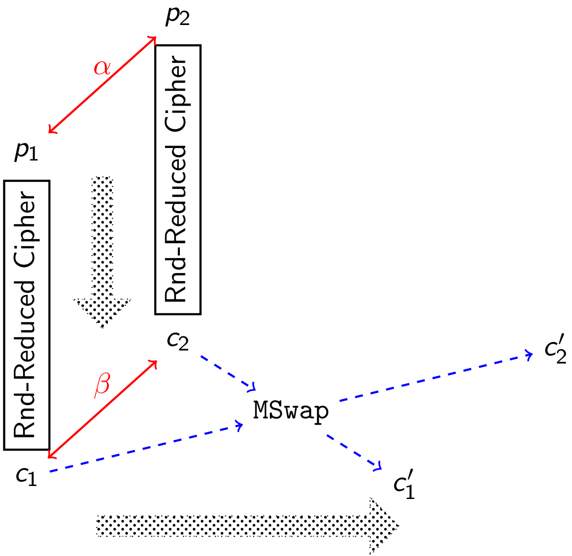
Use MSwap to swap bytes/words of c_1, c_2

How does this swap work?



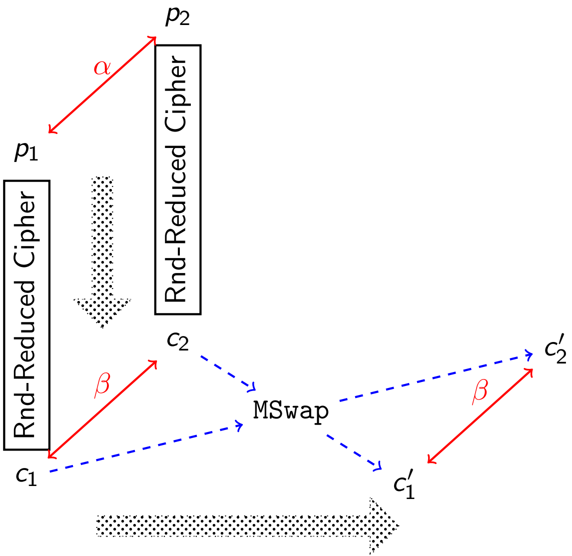
Generate new ciphertext pair c'_1, c'_2

What is the relation between c'_1, c'_2?

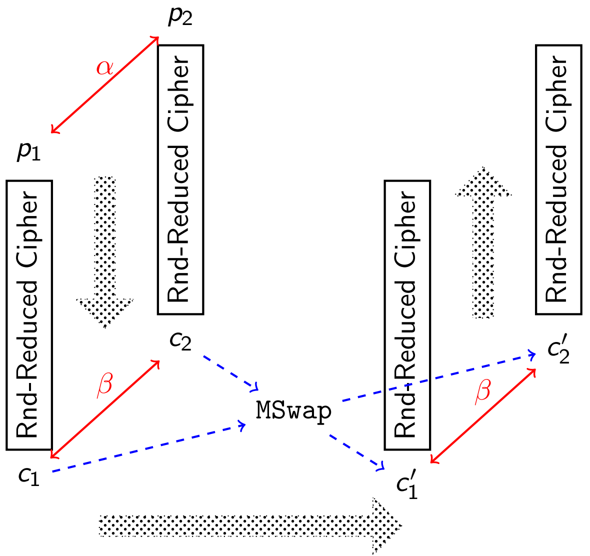


Invariant: $c_1' \oplus c_2' = \beta$

How does this part differ from the **Boomerang** Attack?

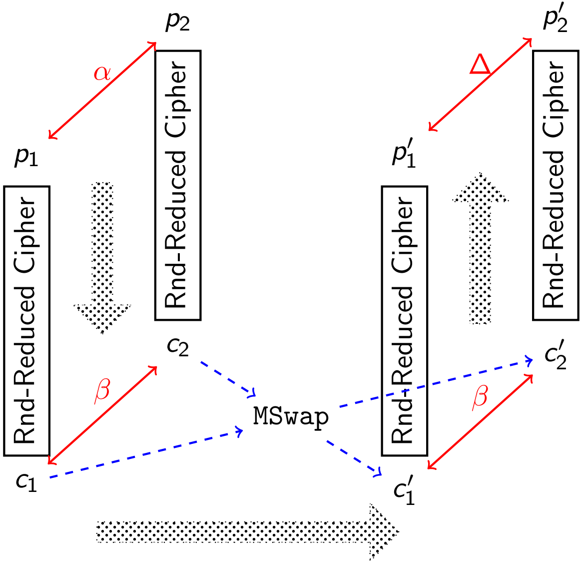


Invert same number of rounds



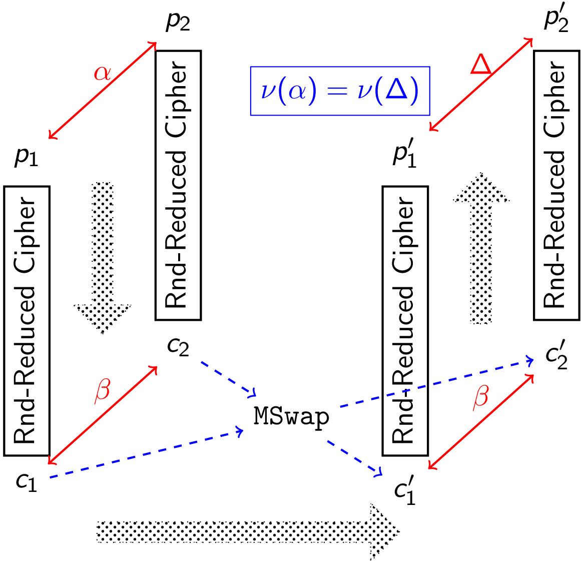
Get p_1', p_2' with $p_1' \oplus p_2' = \Delta$

Does Δ have a special property?



Hypothesis: Property ν induced in α is preserved by Δ

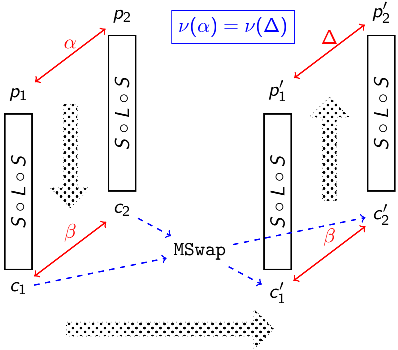
What is this **property** ν?



- Is there a special way to choose α?
  - Zero Difference Pattern (ZDP).
- How many rounds? What type of cipher?
  - **2-Rnd Generic SPN**
- How does the swap work?
  - Swap based on non-linear layer.
- Does Δ have a special property?
  - Same as α
- What is this **property** ν?
  - Zero Difference Pattern (ZDP)

$G_2' = L \circ S \circ L \circ S$ Two full generic Rounds

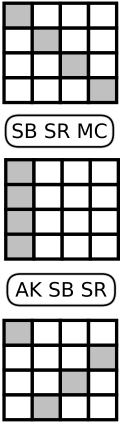
$G_2 = S \circ L \circ S$ $\leftarrow$ Dropping final linear layer (to simplify)

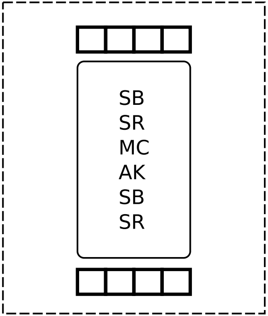


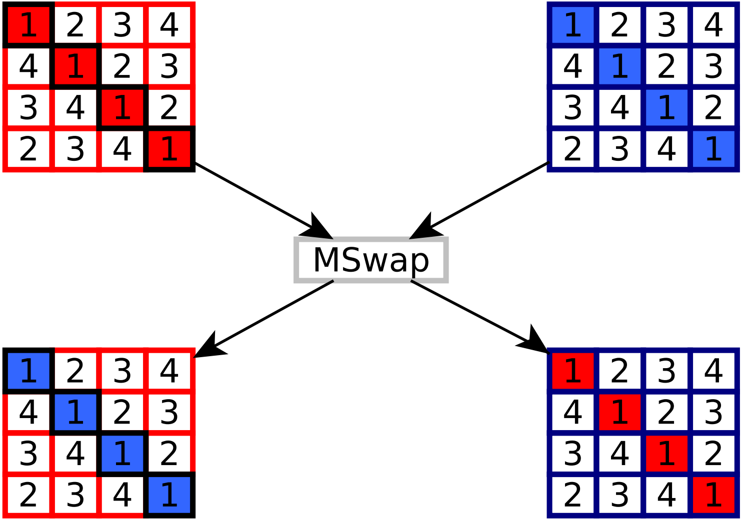
- ZDP of α is preserved by Δ

Applied to AES

- First Key-independent Yoyo Distinguishers of AES
- 5-round key recovery


SB SR MC
AK SB SR


SB
SR
MC
AK
SB
SR


1 2 3 4
4 1 2 3
3 4 1 2
2 3 4 1
1 2 3 4
4 1 2 3
3 4 1 2
2 3 4 1
MSwap
1 2 3 4
4 1 2 3
3 4 1 2
2 3 4 1
1 2 3 4
4 1 2 3
3 4 1 2
2 3 4 1

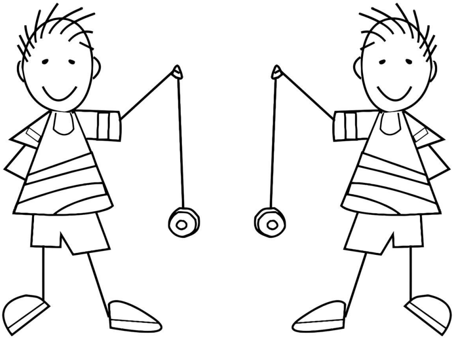
$$p_1 = \begin{array}{cccc} \texttt{fa} & \texttt{b1} & \texttt{5a} & \texttt{2f} \\ \texttt{b7} & \texttt{64} & \texttt{0e} & \texttt{f1} \\ \texttt{f8} & \texttt{9f} & \texttt{22} & \texttt{15} \\ \texttt{28} & \texttt{87} & \texttt{32} & \texttt{25} \end{array} \qquad p_2 = \begin{array}{cccc} \texttt{2e} & \texttt{b1} & \texttt{5a} & \texttt{2f} \\ \texttt{b7} & \texttt{70} & \texttt{0e} & \texttt{f1} \\ \texttt{f8} & \texttt{9f} & \texttt{f2} & \texttt{15} \\ \texttt{28} & \texttt{87} & \texttt{32} & \texttt{4c} \end{array}$$

$$\alpha = p_1 \oplus p_2 = \begin{array}{cccc} \texttt{d4} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{00} & \texttt{14} & \texttt{00} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{d0} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{69} \end{array}$$

$$ZDP(\alpha) = \{0, 1, 1, 1\} \qquad wt(ZDP(\alpha)) = 3$$

- New pairs of plaintexts and ciphertexts are made **adaptively** from the original pairs.
- While making new pairs a **certain property** is kept invariant.
- A common strategy is the use of **zero difference** in the pairs.
- An invariant property is verified at the end

Our Aim: How To Exploit Yoyo Further



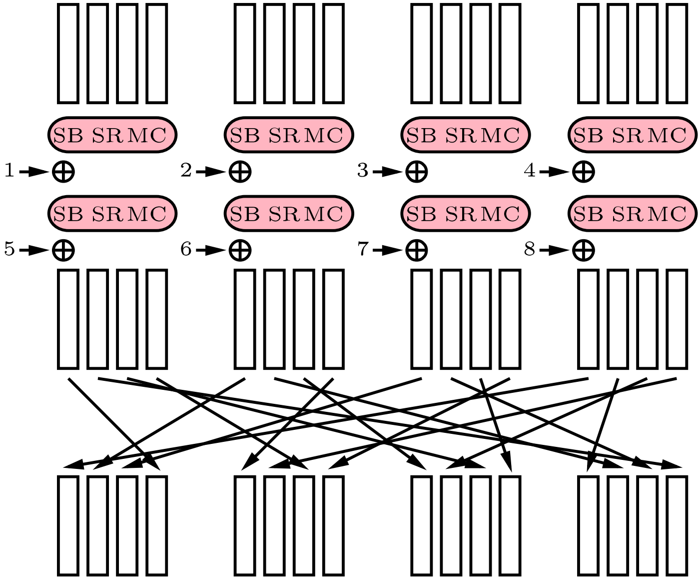
Our Target: `AES`-based Public Permutations

AESQ Permutation

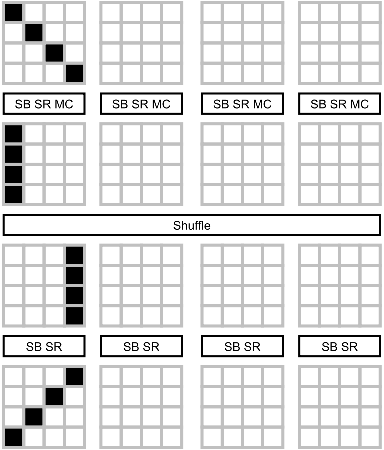
- Internal permutation of AE scheme PAEQ
- PAEQ $\leftarrow$ 2nd Round CAESAR candidate
- By Birukov and Kovratovich

AES in *Known-Key* Setting

- Known-key paradigm
- By Knudsen and Rijmen
- Under Known-key AES behaves as a public permutation

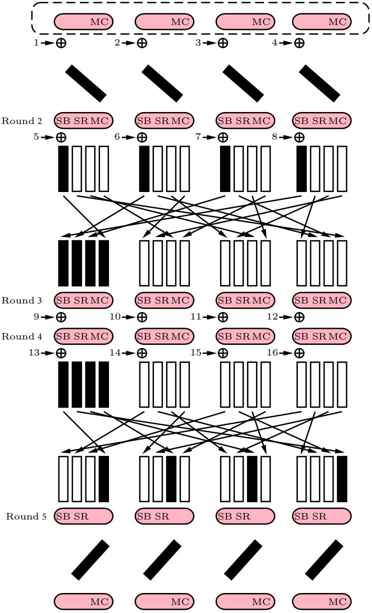

SB SR MC
SB SR MC
SB SR MC
SB SR MC
1
2
3
4
SB SR MC
SB SR MC
SB SR MC
SB SR MC
5
6
7
8

SuperSBox of AESQ



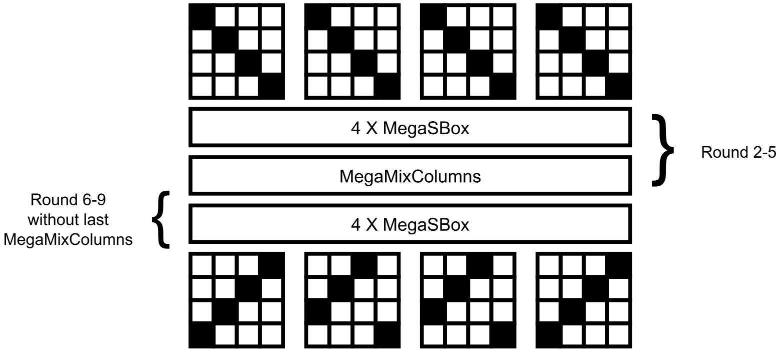
32-bit SuperSbox

- 16 SuperSBox-es
- Cover 1.5 Rounds
- **Must start from even round**



128-bit MegaSBox

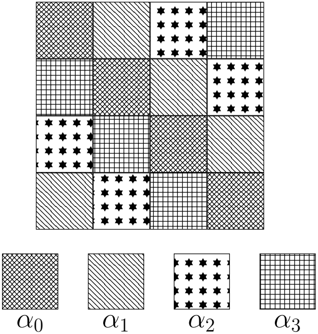
- 4 MegaSBox-es
- Cover 3.5 Rounds
- **Must start from even round**



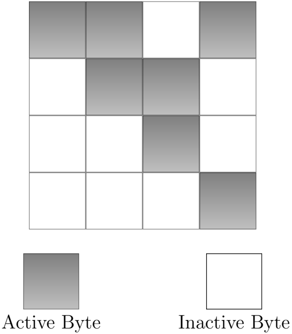
8-Rounds without last MegaMixColumns

Introducing **Nested** Zero Difference Pattern

$\alpha \leftarrow$ Sample State $\quad \nu(\alpha) = (0,0,1,0) \quad wt(\nu(\alpha)) = 1$



A sample state



$$\nu_1^2(\alpha_0) = (0,0,0,0), \qquad \nu_2^2(\alpha_1) = (0,0,1,1),$$
$$\nu_3^2(\alpha_2) = (1,1,1,1), \qquad \nu_4^2(\alpha_3) = (0,1,1,1)$$

$$wt(\nu^2(\alpha)) = 9$$

Strategy 1: Prepend-Append

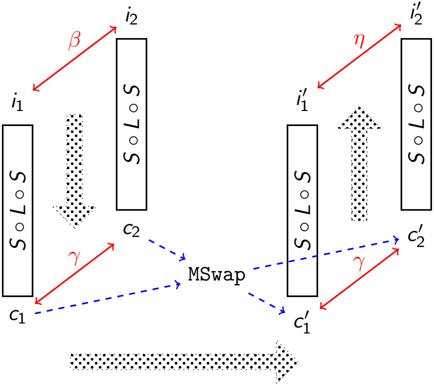
Probabilistic Yoyo

Using Classical Differentials

Basic Yoyo

$\Pr[\nu(\beta) = \nu(\eta)] = 1$

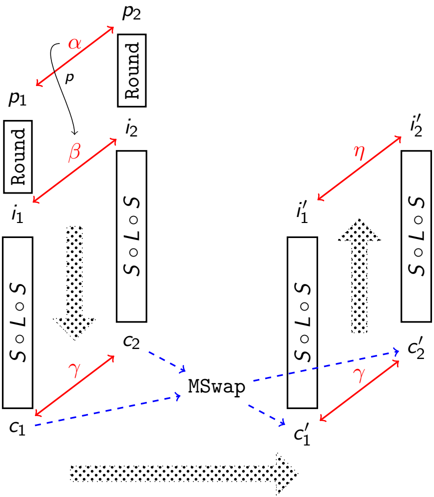
Deterministic Distinguisher



Prepend

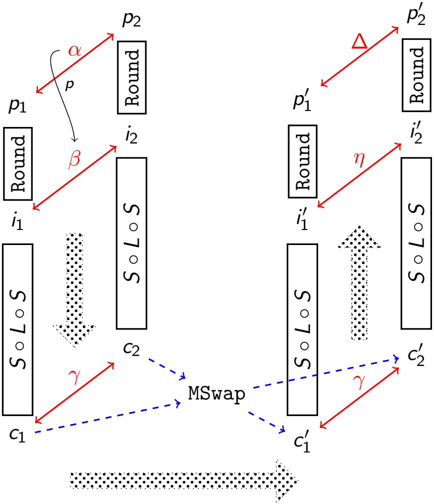
$\Pr[\alpha \to \beta] = p$

Using Classical Differentials

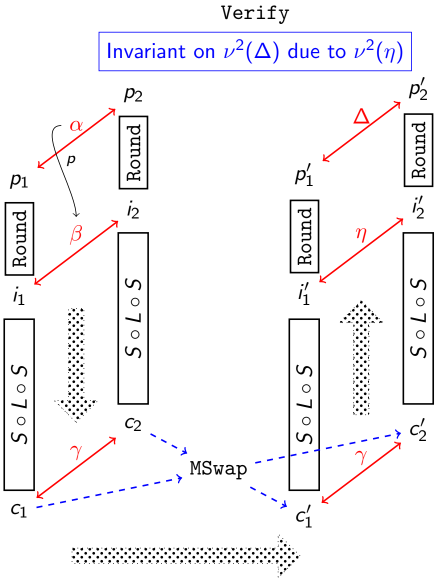


Some assumption on Nested ZDP of η

Induces a property on Δ



Probabilistic Yoyo Distinguisher

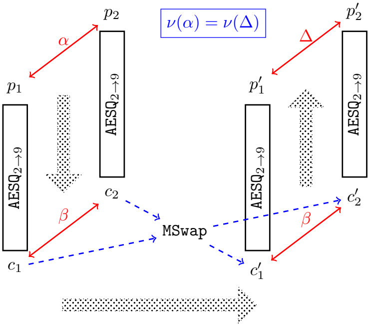


Application: AESQ

First 9-round Distinguisher starting from Round-1

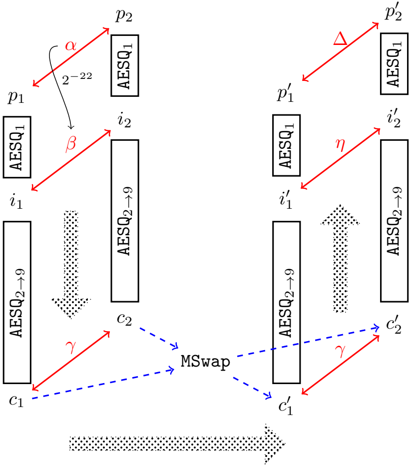
Practical Complexity

Basic Yoyo
8-Rounds

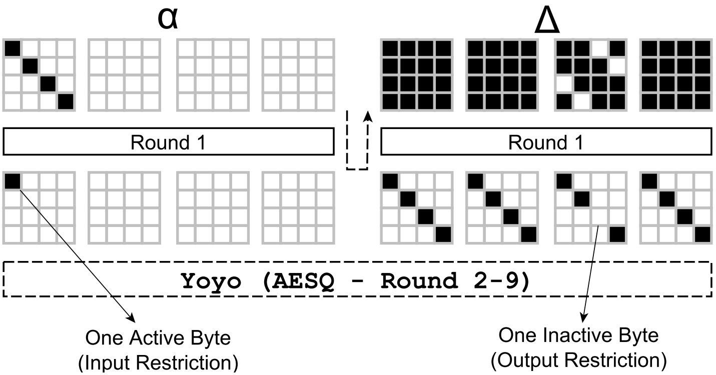


Verify

$\boxed{\exists i\ : wt(\nu^2(\Delta_i)) = 4}$



1-Round Extension



For $\texttt{AESQ}_{1-9}$

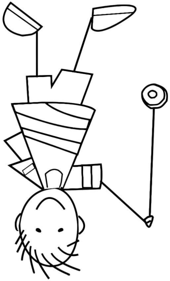
$$\Pr\left[\exists i : wt(\nu^2(\Delta_i)) = 4\right] \approx 2^{-26}$$

For $\mathcal{R}$

$$\Pr\left[\exists i : wt(\nu^2(\Delta_i)) = 4\right] \approx 2^{-28}$$

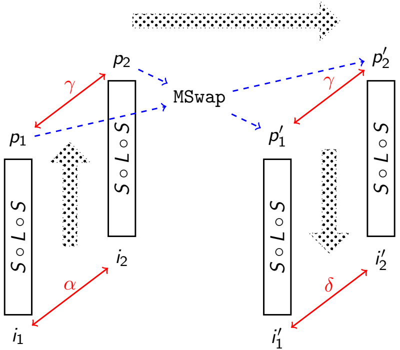
Strategy 2: Composing Impossible Differentials

The Inside-Out Technique



Inverted Yoyo

Inverted Yoyo

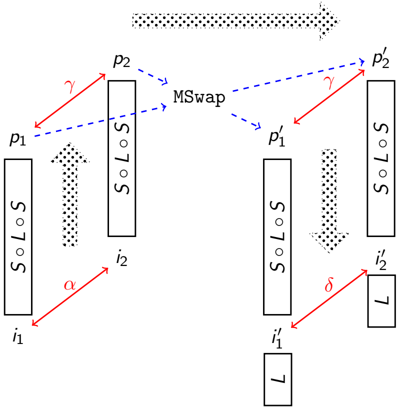


- By virtue of Yoyo
- $\Pr[\nu(\alpha) = \nu(\delta)] = 1$

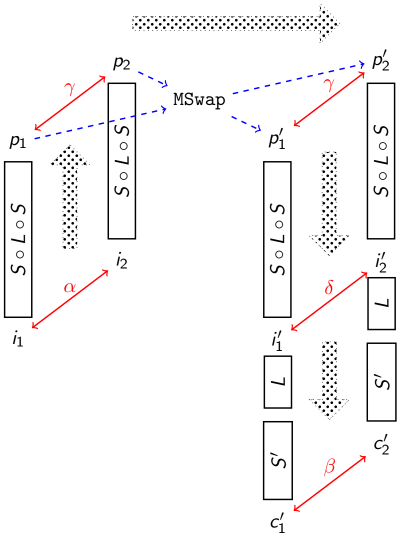
Assumption

Something on $\nu^2(\delta)$

Append L



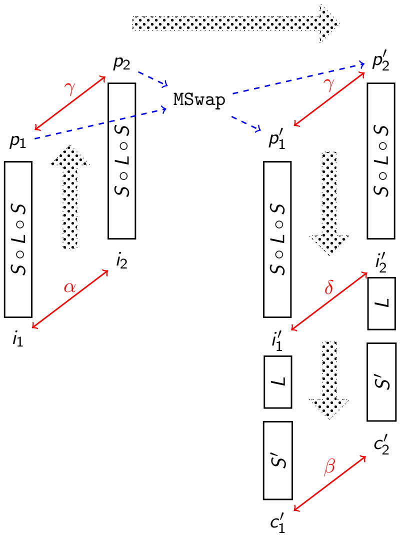
- Exploit Properties of L
- Effect of L on δ?
- Use $\nu^2(\delta)$ Assumption



Impossibility

- $\Pr[\nu^2(\delta) \to \nu^2(\beta)] = 0$

Probability of $\nu^2(\delta)$ Assumption Holding

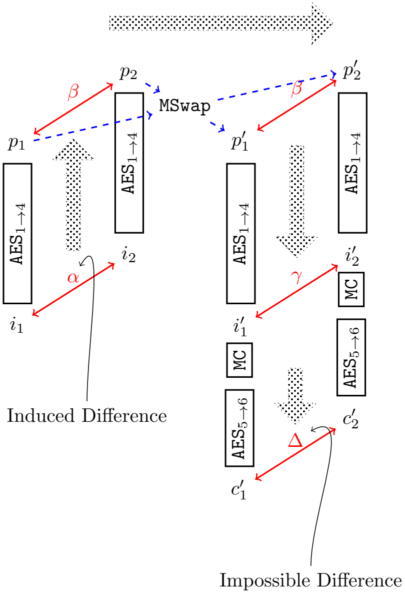


Application: AES, AESQ

6 Round AES (Practical)

9-10(Practical), 12 Round AESQ

Impossible Differential Yoyo Distinguisher on 6-Round AES

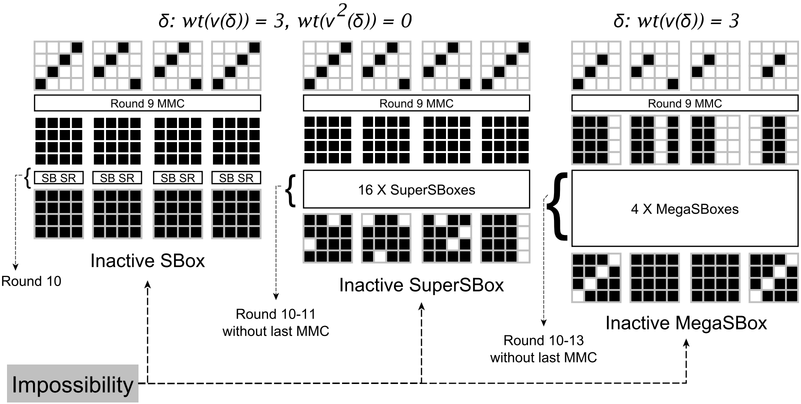


- One SuperSBox active in α
- One SuperSBox active in γ
- At least one byte active in γ
- **At least one column active after** `MC`
- All SuperSBoxes active after `MC`

Impossible

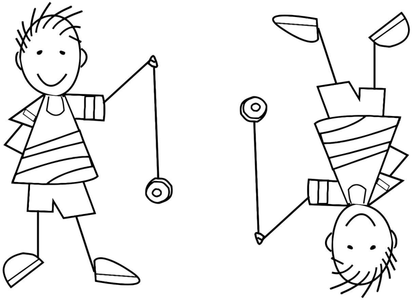
One **inactive** SuperSBox in Δ

Exploiting Same Property of MixColumns



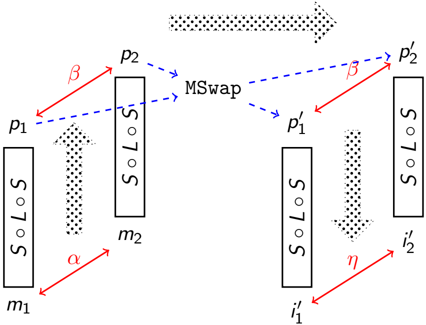
Impossibilities with different S' Layers

Strategy 3: Bi-directional Yoyo

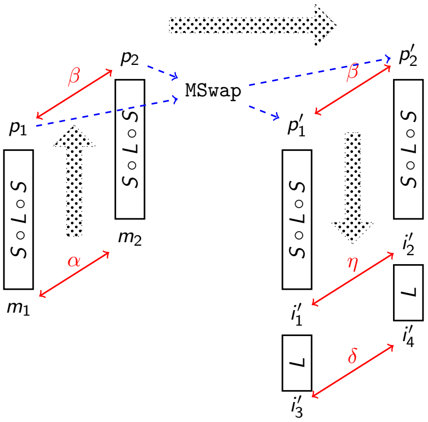


Composing Two Yoyo Games In Two-Directions

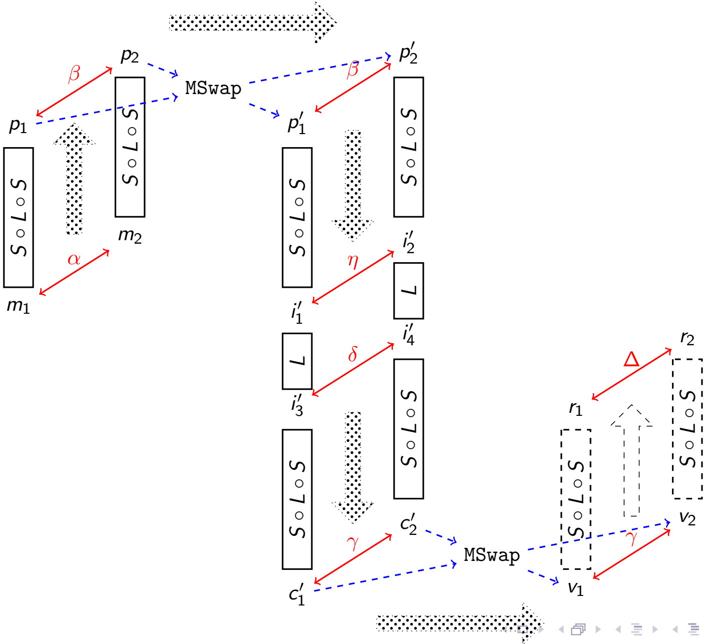
Inverted Yoyo



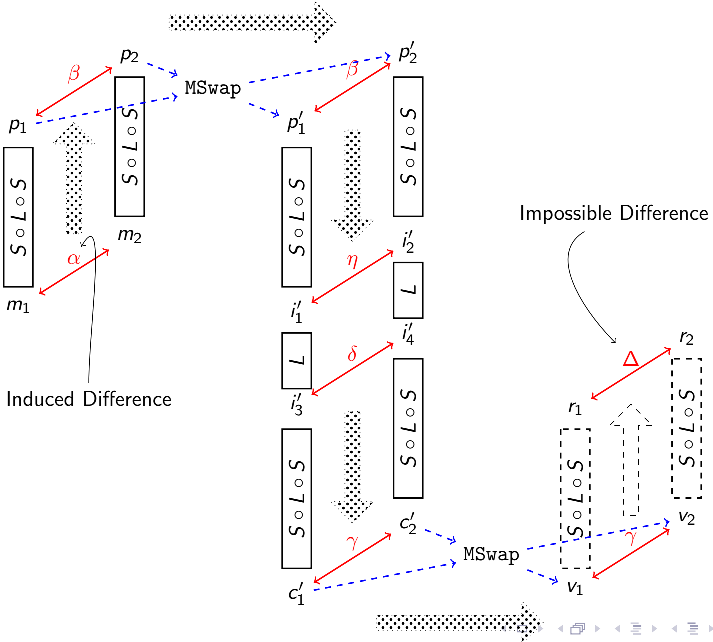
Adding Linear Layer



Composing 2nd Yoyo

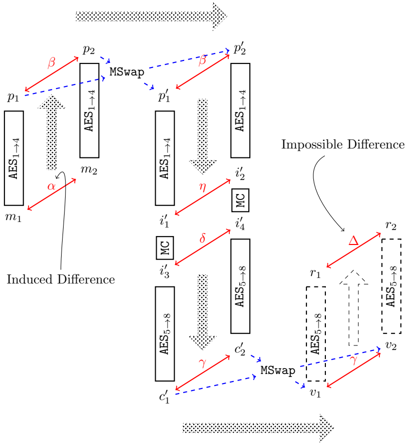


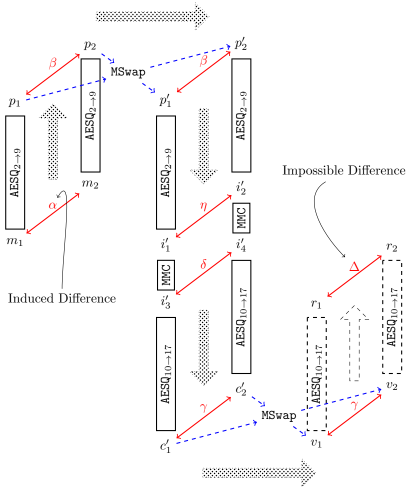
Impossible Differential Bi-directional Yoyo



Application: AES, AESQ

8 Round AES (Practial) 16 Round AESQ





Distinguishing Complexities

$\mathtt{AES}_{1\to 8} : 2^{30}$ $\mathtt{AESQ}_{2\to 17} : 2^{126}$

Distinguishers on AESQ

Rounds	Complexity Time	Complexity Memory	Technique	Reference
8	2^{32}		CICO	Designers
$8^{\dagger}$	1	Negligible	**YoYo**	**This Work**
9	$2^{26.08}$	Negligible	**YoYo**	**This Work**
$9^{\dagger}$	5	Negligible	**Improbable Differential YoYo**	**This Work**
$10^{\dagger}$	2^{28}	Negligible	**Improbable Differential YoYo**	**This Work**
$12^{\dagger}$	2^{126}	Negligible	**Impossible Differential YoYo**	**This Work**
$12^{\dagger}$	2^{256}	2^{256}	Rebound Attack	Designers
$12^{\dagger}$	2^{128}	Negligible	Rebound Attack	Bagheri et al.
$12^{\dagger}$	$2^{102.4}$	$2^{102.4}$	Time-memory Trade-off	Bagheri et al.
$12^{\dagger}$	$2^{128-x/4}$	2^{x}	Time-memory Trade-off	Bagheri et al.
$16^{\dagger}$	2^{192}	2^{128}	Rebound Attack	Bagheri et al.
$16^{\dagger}$	2^{188}	2^{128}	Multi Ltd.-Birthday Distinguisher	Bagheri et al.
$16^{\dagger}$	2^{192+x}	2^{128-x}	Time-memory Trade-off	Bagheri et al.
$16^{\dagger}$	2^{126}	Negligible	**Impossible Differential Bidirectional YoYo**	**This Work**

8-round Known-Key Distinguishers on AES

Time Complexity	Memory Complexity	Property	Reference
2^{64}	2^{64}	Uniform Distribution	Gilbert et al.
2^{48}	2^{32}	Differential Trail	Gilbert et al.
2^{44}	2^{32}	Multiple Differential Trail	Jean et al.
$\mathbf{2^{30}}$	**negligible**	**Impossible Differential Bi-directional Yoyo**	**This Work**
2^{23}	2^{16}	Extended 7-Round Multiple Differential Trail	Grassi et al.

Distinguishers reported in this work

	#R	Start → End	Complexity	Strategy	Remarks
AESQ	8	$2 \rightarrow 9$	1	Yoyo	Basic Yoyo
	9	$1 \rightarrow 9$	$2^{26.08}$	Yoyo + Nested ZDP	First 9 round Distinguisher starting from Round 1
	9	$2 \rightarrow 10$	5	Improbable Differential Yoyo	Uses the inside-out technique
	10	$2 \rightarrow 11$	2^{28}		
	12	$2 \rightarrow 13$	2^{126}	Impossible Differential Yoyo	
	16	$2 \rightarrow 17$	2^{126}	Bi-directional Impossible Differential Yoyo	Uses inside-out with bi-directional Yoyo
AES	6	$1 \rightarrow 6$	2^{30}	Impossible Differential Yoyo	Uses the inside-out technique
	8	$1 \rightarrow 8$	2^{30}	Bi-directional Impossible Differential Yoyo	Uses inside-out with bi-directional Yoyo

Summary

- New ways to extend basic Yoyo game
  - Classical Differentials
  - Impossible Differentials
  - Bi-directional Yoyo
- Using public permutations
- Best results achieved for `AESQ`
- New known-key distinguishers for `AES`
- All practical distinguishers experimentally verified
- Yoyo seems to be an effective generic cryptanalysis tool

Image Source: Google