Revisiting Yoyo Tricks on AES

Sandip Kumar Mondal, Mostafizar Rahman, Santanu Sarkar and Avishek Adhikari

Department of Pure Mathematics,
University of Calcutta, Kolkata,
FSE 2024

25th March, 2024

Content

- Introduction
- Description of AES-128
- Distinguishing Game
- Yoyo Game on Substitution-Permutation Networks
- Revisiting Yoyo Attack on 5-round AES
- Revisiting Yoyo Attack on 6-round AES
- Results
- Conclusion

Introduction

- At Asiacrypt 2017, Rønjom et al. presented key-independent distinguishers for different numbers of rounds of AES, ranging from 3 to 6 rounds, in their work titled "Yoyo Tricks with AES".
- The reported data complexities for these distinguishers were 3, 4, $2^{25.8}$, and $2^{122.83}$, respectively.
- In this work, we revisit those key-independent distinguishers and analyze their success probabilities.

Description of AES-128

- **SubBytes (*SB*):** This function replaces each byte in the state with a new byte, using an 8-bit Sbox table.
- **ShiftRows (*SR*):** This function cyclically shifts each row of the state by a different amount. In general, the i-th row of the state is rotated left by i bytes (for $0 \leq i \leq 3$).
- **MixColumns (*MC*):** This function mixes the columns of the state using a linear transformation.
- **AddRoundKey (*ARK*):** This function adds the round subkey (generated from the secret key) to the state.

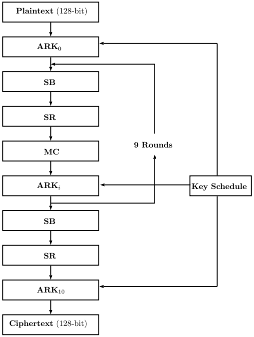


Figure: AES 128

Distinguishing Game: Distinguishing Oracles $\mathcal{O}_0$ and $\mathcal{O}_1$

$$\begin{array}{ccc} \underline{\textbf{Adv}} & & \underline{\textbf{Challenger}(\mathcal{O}_0/\mathcal{O}_1)} \\ & & b \leftarrow_{\$} \{0,1\} \\ & \xrightarrow{\quad x_i \quad} & \\ & \xleftarrow{y_i = \mathcal{O}_b(x_i)} & \\ & \xrightarrow{\quad b' \quad} & \\ & & \textbf{Adv} \text{ wins if } b' = b \end{array}$$

x_i :i-th query, y_i :i-th response. After the query-response phase, **Adv** submits a bit b'

Success Probability of **Adv**: $SP_{\mathcal{O}_0,\mathcal{O}_1}(\textbf{Adv}) = Pr[A^{\mathcal{O}_b} = b]$

Some Definitions

Definition

Zero Difference Pattern: Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$. Define $\nu(\alpha)$ $= (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{F}_2^n$ where $z_i = 1$ if $\alpha_i = 0$ and $z_i = 0$ otherwise. Then $\nu(\alpha)$ is the Zero Difference Pattern for α.

For example if
$\alpha = (0x12a4b534, 0x00000000, 0x00000000, 0x86af31bc) \in \mathbb{F}_{2^{32}}^4$
then $\nu(\alpha) = (0,1,1,0)$.
Here $wt(\nu(\alpha)) = 2$.

Some Definitions

Definition

For a vector $v \in \mathbb{F}_2^n$ and a pair of states $\alpha, \beta \in \mathbb{F}_q^n$ define a new state $\rho^v(\alpha, \beta) \in \mathbb{F}_q^n$ such that the i-th component is defined by

$$\rho^v(\alpha, \beta)_i = \begin{cases} \alpha_i, & \text{if } v_i = 1 \\ \beta_i, & \text{if } v_i = 0. \end{cases} \tag{1}$$

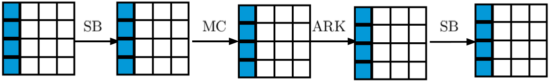
For example, if we take $v = (0, 1, 0, 1) \in \mathbb{F}_2^4$ and if $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)$ then
$\rho^v(\alpha, \beta) = (\beta_0, \alpha_1, \beta_2, \alpha_3)$ and $\rho^v(\beta, \alpha) = (\alpha_0, \beta_1, \alpha_2, \beta_3)$

SIMPLESWAP

Algorithm 1: Swaps the first word where texts are different and returns one text

function SIMPLESWAP(x^0, x^1)
$x'^0 \leftarrow x^1$
for *i from* 0 *to* 3 **do**
    if $x_i^0 \neq x_i^1$ **then**
        $x_i'^0 \leftarrow x_i^0$
        return x'^0

Reduced Round AES

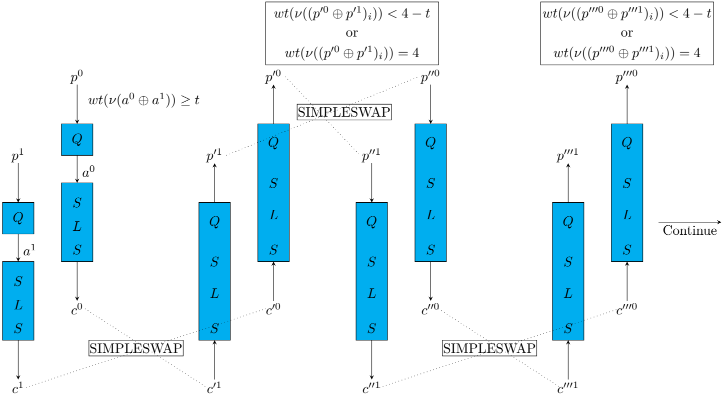


$S = SB \circ MC \circ SB$
$L = SR \circ MC \circ SR$
$Q = SR \circ MC \circ SB$
$R^4 = S \circ L \circ S$
$R^5 = S \circ L \circ S \circ Q$
$R^6 = S \circ L \circ S \circ L \circ S$

Right Pair and Wrong Pair

- A pair p^0, p^1 is said to be a `RightPair` if it satisfies some condition. Note that, this property is required to be satisfied in the intermediate round.
- A pair p^0, p^1 is considered a `WrongPair` if it does not meet the intermediate-round criteria.
- When the oracle is a random permutation, then every pair is supposed to be a `WrongPair`.
- Based on this intermediate-round property, some probabilistic property on the final output is derived to correctly detect a `RightPair`.

RightPair for 5-round AES



Distinguisher for 5-round AES

Algorithm 2: Distinguisher for 5-round AES

Input: x, y and t

Output: 1 for the AES and -1 otherwise.

while $i < x$ **do**

  $i \leftarrow i + 1$;

  $p^{i,1}, p^{i,2} \leftarrow$ generate random pair with $wt(\nu(p^{i,1} \oplus p^{i,2})) = 3$;

  $j \leftarrow 0$, `WrongPair` $\leftarrow$ False;

  while $j < y$ *and* $\mathtt{WrongPair} = \mathit{False}$ **do**

    ---

    if *condition not satisfied* **then**

      `WrongPair` $=$ True

  if $\mathtt{WrongPair} = \mathit{False}$ **then**

    return 1;

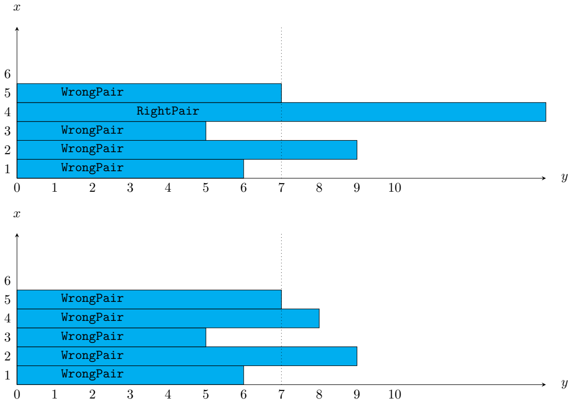
return -1;

Experimental Verification

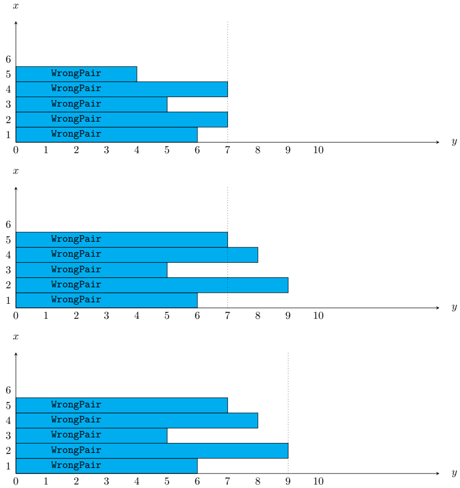
$\#N$	Blackbox Primitive	x	y	Detected as AES	Detected as RP	Experimental Success Probability
100	AES	$2^{13.4}$	$2^{11.4}$	100	0	0.5
100	RP	$2^{13.4}$	$2^{11.4}$	100	0	

Table: Experimental results for 5-round AES when t=2. Here, $\#N$ denotes the number of experiments.

Discussion


x
6
5
4
3
2
1
WrongPair
RightPair
WrongPair
WrongPair
WrongPair
0 1 2 3 4 5 6 7 8 9 10
y
x
6
5
4
3
2
1
WrongPair
WrongPair
WrongPair
WrongPair
WrongPair
0 1 2 3 4 5 6 7 8 9 10
y

Discussion


x
y
WrongPair
WrongPair
WrongPair
WrongPair
WrongPair
0 1 2 3 4 5 6 7 8 9 10
1 2 3 4 5 6

Success Probability of Algorithm 2

$$p^{x,y,t}_{AES_5} = 1 - \Big(1 - \Big(\sum_{\substack{m<t \\ m\in[0,3]}} \Big(1 - \sum_{r\in[4-t,3-m]} \binom{4}{r} (q^{-1})^r (1-q^{-1})^{(4-r)}\Big)^{4y} \times \kappa_m + \sum_{\substack{m\geq t \\ m\in[0,3]}} \kappa_m\Big)\Big)^x.$$

where $\kappa_m = \binom{4}{m}(q^{-1})^m(1-q^{-1})^{4-m}$ and $q = 2^8$

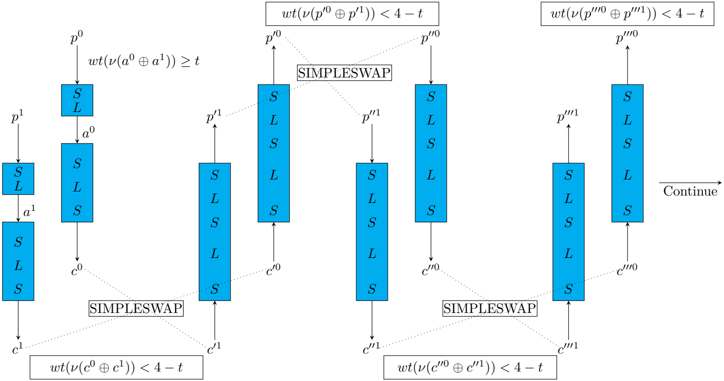
$$p^{x,y,t}_{\mathcal{RP}_5} = \Big(1 - \Big(1 - \sum_{r\in[4-t,3]} \binom{4}{r} (q^{-1})^r (1-q^{-1})^{(4-r)}\Big)^{4y}\Big)^x.$$

Success Probability of Algorithm 2

The success probability of Algorithm 2 is

$$\frac{p^{x,y,t}_{AES_5} + p^{x,y,t}_{\mathcal{RP}_5}}{2}.$$

RightPair for 6-round AES



Distinguisher for 6-round AES

Algorithm 3: Distinguisher for 6-round AES

Input: x, y and t

Output: 1 for the AES and -1 otherwise.

```
while i < x do
    i ← i + 1;
    p^{i,1}, p^{i,2} ← generate random pair with p^{i,1} ≠ p^{i,2};
    j ← 0, WrongPair ← False;
    while j < y and WrongPair = False do
        ________________
        if condition not satisfied then
            WrongPair = True
    if WrongPair = False then
        return 1;
return −1;
```

Success Probability of Algorithm 3

$$p_{AES_6}^{x,y,t} = 1 - (1 - (\sum_{\substack{m<t \\ m\in[0,3]}} (1 - \sum_{r\in[4-t,3-m]} \binom{4}{r} (q^{-4})^r (1-q^{-4})^{(4-r)})^{2y} \times \mu_m + \sum_{\substack{m\geq t \\ m\in[0,3]}} \mu_m))^x.$$

where $\mu_m = \binom{4}{m}(q^{-4})^m(1-q^{-4})^{4-m}$ and $q = 2^8$

$$p_{\mathcal{RP}_6}^{x,y,t} = (1 - (1 - \sum_{r\in[4-t,3]} \binom{4}{r} (q^{-4})^r (1-q^{-4})^{(4-r)})^{2y})^x.$$

Success Probability of Algorithm 3

Similar to the 5-round distinguisher, the success probability of Algorithm 3 is

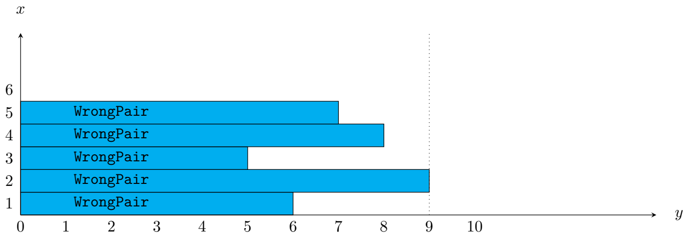
$$\frac{p_{AES_6}^{x,y,t} + p_{\mathcal{RP}_6}^{x,y,t}}{2}.$$

Results

Round	Value of x	Value of y	Data Complexity	Time Complexity	Success Probability
5	$2^{13.4}$	$2^{11.4}$	$2^{26.8}$	$2^{24.8}$ XOR + $2^{26.8}$ MAs	0.5
	$2^{13.4}$	$2^{15.25}$	$2^{30.65}$	$2^{28.65}$ XOR + $2^{30.65}$ MAs	0.81
	$2^{15.60}$	$2^{15.37}$	$2^{32.97}$	$2^{30.97}$ XOR + $2^{32.97}$ MAs	0.99
6	$2^{61.4}$	$2^{60.4}$	$2^{123.8}$	$2^{122.8}$ XOR + $2^{123.8}$ MAs	0.5
	$2^{61.4}$	$2^{65.76}$	$2^{129.15}$	$2^{128.15}$ XOR + $2^{129.15}$ MAs	0.50004

Table: Success probability and data complexity of Algorithm 2 and 3 for different values of x and y when $t = 2$.

Average Data Complexity



Average Data Complexity

Number of Experiments	Blackbox Cipher	Value of y	Found as AES	Found as Random	Success Probability (Theoretical)	Overall Success Probability (Experimental)	Overall Success Probability (Theoretical)
100	AES	$2^{15.7}$	61	39	0.6264	0.805	0.8132
100	RANDOM (AES20)	$2^{15.7}$	0	100	1.0		
100	RANDOM (drand48)	$2^{15.7}$	0	100			

Table: Results for 5-round distinguisher when t=2 and $x = 2^{13.4}$.

Value of y	Success Probability (When Oracle is AES)	Success Probability (When Oracle is Random Permutation)	Success Probability (Overall)
$2^{66.12}$	0.6283	0.9999	0.8141
$2^{66.13}$	0.6283	1.0	0.8141

Table: Theoretical results for 6-round distinguishers when t=2 and $x = 2^{61.4}$

The average complexity for 5-round AES is $2^{26.82}$.
The average complexity for 6-round AES is $2^{123.82}$.

Conclusion

We would like to emphasize the significance of the success probability in cryptographic attack algorithms. It is crucial to establish the validity of these attacks by demonstrating a substantial success probability while maintaining a complexity lower than that of an exhaustive search.

References

- Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, Advances in Cryptology- ASIACRYPT 2017 - 23rd International Conference on the Theory and Appli-cations of Cryptology and Information Security, Hong Kong, China, December3-7, 2017, Proceedings, Part I, volume 10624 of Lecture Notes in ComputerScience, pages 217–243. Springer, 2017.
- Dhiman Saha, Mostafizar Rahman, and Goutam Paul. New yoyo tricks with AES-based permutations. IACR Trans. Symmetric Cryptol., 2018(4):102–127, 2018.
- Joan Daemen and Vincent Rijmen. Plateau characteristics. IET Inf. Secur., 1(1):11–17, 2007.

Any Questions?