The Boomerang Chain Distinguishers: New Record for 6-Round AES

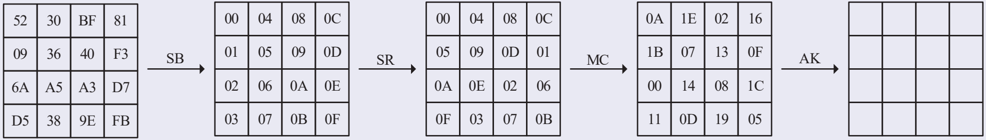
Xueping Yan
Joint work with Lin Tan, Hong Xu, Wenfeng Qi

Information Engineering University

December 8, 2024

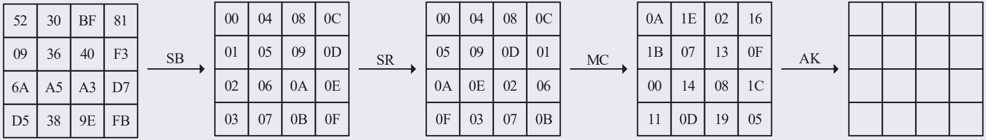
AES

- AES is the most widely used symmetric cipher. It was proposed by J. Daemen and V. Rijmen in 1997, and was standardized by NIST in 2000.
- AES is a SPN block cipher with 128-bit block, 128/192/256-bit keys, and 10/12/14 rounds. The round function consists of four operations: SubBytes (SB), ShiftRows (SR), MixColumns (MC) and AddRoundKey (AK).



AES

- AES is the most widely used symmetric cipher. It was proposed by J. Daemen and V. Rijmen in 1997, and was standardized by NIST in 2000.
- AES is a SPN block cipher with 128-bit block, 128/192/256-bit keys, and 10/12/14 rounds. The round function consists of four operations: SubBytes (SB), ShiftRows (SR), MixColumns (MC) and AddRoundKey (AK).



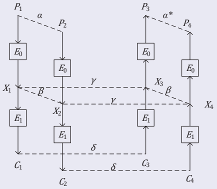
- Security evaluation of round-reduced AES is an important problem, where the distinguishing attacks have attracted much attention of scholars.

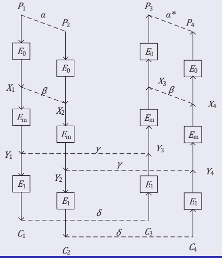
Overview of Distinguishers for 5 and 6 Rounds of AES

Technique	Rounds	Data	Time	Success Prob.	Ref.
Multiple-of-8	5	2^{32} CP	$2^{35.6}$ M	100%	Eurocrypt17
Exchange Attack	5	2^{30} CP	2^{30} E	63%	Asiacrypt19
Yoyo	5	$2^{29.95}$ ACPC	$2^{29.95}$ M	55%	FSE24
Yoyo	5	$2^{30.65}$ ACPC	$2^{30.65}$ M	81%	FSE24
Truncated Differential	6	$2^{89.4}$ CP	$2^{96.5}$ M	95%	FSE21
Exchange Attack	6	$2^{88.2}$ CP	$2^{88.2}$ E	73%	Asiacrypt19
Truncated Boomerang	6	2^{87} ACC	2^{87} E	84%	Eurocrypt23
Exchange Attack	6	2^{84} ACC	2^{83} E	63%	eprint19
Re-Boomerang	6	$2^{82.33}$ ACPC	$2^{82.33}$ E	64%	Our Result
Triple Boomerangs	6	$2^{77.82}$ ACPC	$2^{77.82}$ E	66%	Our Result
Boomerang Chain	6	$2^{76.57}$ ACPC	$2^{76.57}$ E	60%	Our Result

Boomerang Distinguisher

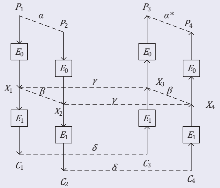
- Boomerang attack, proposed by D. Wagner in 1999, is an extension of differential cryptanalysis in the adaptively chosen plaintexts and ciphertexts setting.

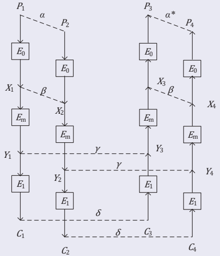




Boomerang Distinguisher

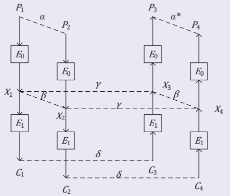
- Boomerang attack, proposed by D. Wagner in 1999, is an extension of differential cryptanalysis in the adaptively chosen plaintexts and ciphertexts setting.
- The boomerang probability $P_B = Pr(E^{-1}(E(X)+\delta) \oplus E^{-1}(E(X+\alpha)+\delta) = \alpha^*)$.
- If $P_B > 2^{-n}$, where n is the block size, then E can be distinguished from a random permutation by P_B^{-1} chosen plaintext pairs and P_B^{-1} adaptively chosen ciphertext pairs.

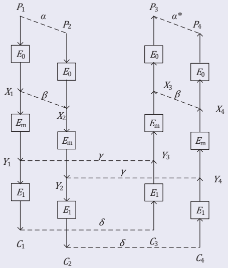




(Truncated) Boomerang Distinguisher

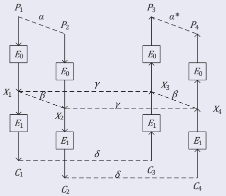
- Suppose $E = E_1 \circ E_0$, there exist differentials $\alpha \xrightarrow{E_0} \beta$ with probability $\overrightarrow{p}$, $\beta \xrightarrow{E_0^{-1}} \alpha^*$ with probability $\overleftarrow{p}$, and $\delta \xrightarrow{E_1^{-1}} \gamma$ with probability q.

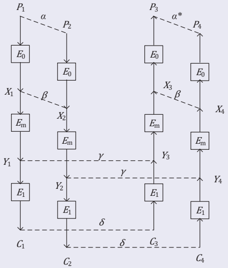




(Truncated) Boomerang Distinguisher

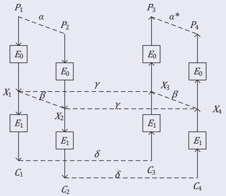
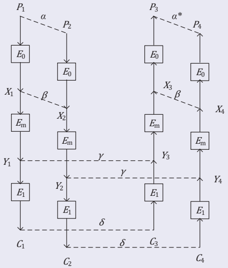
- Suppose $E = E_1 \circ E_0$, there exist differentials $\alpha \xrightarrow{E_0} \beta$ with probability $\overrightarrow{p}$, $\beta \xrightarrow{E_0^{-1}} \alpha^*$ with probability $\overleftarrow{p}$, and $\delta \xrightarrow{E_1^{-1}} \gamma$ with probability q.
- The probability of boomerang distinguisher is estimated by $P_B = \overrightarrow{p}\,\overleftarrow{p}\,q^2$.





(Truncated) Boomerang Distinguisher

- Suppose $E = E_1 \circ E_0$, there exist differentials $\alpha \xrightarrow{E_0} \beta$ with probability $\overrightarrow{p}$, $\beta \xrightarrow{E_0^{-1}} \alpha^*$ with probability $\overleftarrow{p}$, and $\delta \xrightarrow{E_1^{-1}} \gamma$ with probability q.
- The probability of boomerang distinguisher is estimated by $P_B = \overrightarrow{p}\overleftarrow{p}q^2$.
- Suppose $E = E_1 \circ E_m \circ E_0$ and the connection probability for E_m is r, then the boomerang probability is estimated by $P_B = \overrightarrow{p}\overleftarrow{p}q^2 r$.

Motivation

- The distinguishers on 5-round AES have very low data complexities ($\leq 2^{32}$), but the best distinguisher on 6-round AES has a very high data complexity 2^{84}. How to shorten the gap?

Motivation

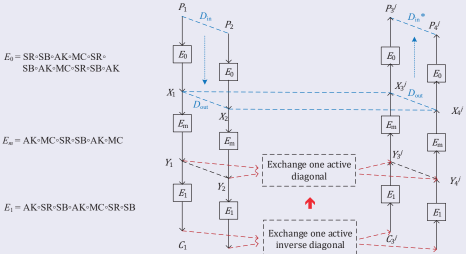
- The distinguishers on 5-round AES have very low data complexities ($\leq 2^{32}$), but the best distinguisher on 6-round AES has a very high data complexity 2^{84}. How to shorten the gap?
- The attacker is provided a wider space in the adaptively chosen plaintexts and ciphertexts setting. How to fully utilize the advantage of this setting to develop new cryptanalysis techniques?

Motivation

- The distinguishers on 5-round AES have very low data complexities ($\leq 2^{32}$), but the best distinguisher on 6-round AES has a very high data complexity 2^{84}. How to shorten the gap?
- The attacker is provided a wider space in the adaptively chosen plaintexts and ciphertexts setting. How to fully utilize the advantage of this setting to develop new cryptanalysis techniques?
- Boomerang cryptanalysis has shown the power for many block ciphers. The classical boomerang distinguisher usually uses one boomerang property. Whether we can use two or more boomerangs to enhance the distinguishing effect?

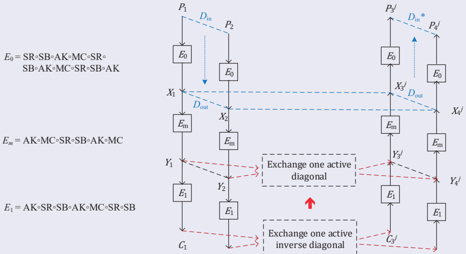
Our Ideas

- For the cipher $E = E_1 \circ E_m \circ E_0$, assume that there exist two boomerangs B_1 and B_2 with probabilities of P_{B_1} and P_{B_2}, respectively.



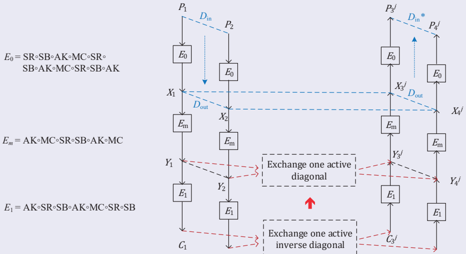
Our Ideas

- For the cipher $E = E_1 \circ E_m \circ E_0$, assume that there exist two boomerangs B_1 and B_2 with probabilities of P_{B_1} and P_{B_2}, respectively.
- B_1 and B_2 have the same truncated differential trail over E_0 in the forward direction $\mathcal{D}_{in} \xrightarrow{E_0} \mathcal{D}_{out}$, of which the probability is $\overrightarrow{p}$.



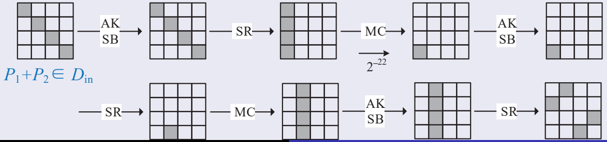
Our Ideas

- For the cipher $E = E_1 \circ E_m \circ E_0$, assume that there exist two boomerangs B_1 and B_2 with probabilities of P_{B_1} and P_{B_2}, respectively.
- B_1 and B_2 have the same truncated differential trail over E_0 in the forward direction $\mathcal{D}_{in} \xrightarrow{E_0} \mathcal{D}_{out}$, of which the probability is $\overrightarrow{p}$.
- (P_1, P_2) is called a **right pair** if it follows the truncated differential trail over E_0 in the forward direction, i.e., $P_1 + P_2 \in \mathcal{D}_{in}$ and $E_0(P_1) + E_0(P_2) \in \mathcal{D}_{out}$.



Our Ideas

- For the cipher $E = E_1 \circ E_m \circ E_0$, assume that there exist two boomerangs B_1 and B_2 with probabilities of P_{B_1} and P_{B_2}, respectively.
- B_1 and B_2 have the same truncated differential trail over E_0 in the forward direction $\mathcal{D}_{in} \xrightarrow{E_0} \mathcal{D}_{out}$, of which the probability is $\overrightarrow{p}$.
- (P_1, P_2) is called a **right pair** if it follows the truncated differential trail over E_0 in forward, i.e., $P_1 + P_2 \in \mathcal{D}_{in}$ and $E_0(P_1) + E_0(P_2) \in \mathcal{D}_{out}$.
- (P'_1, P'_2) is called a **friend pair** of (P_1, P_2) if $P'_1 + P'_2 = P_1 + P_2$ and the active cells of (P'_1, P'_2) are the same as them of (P_1, P_2). **Any friend pair of a right pair is also a right pair**.



Our Ideas

- Distinguishing the cipher E by B_2 needs about $P_{B_2}^{-1}$ chosen plaintext pairs, where $P_{B_2} = \overrightarrow{p}\,\overleftarrow{p}\,q^2 r$. If all plaintext pairs chosen are right pairs, it can be reduced by a factor of $\overrightarrow{p}^{-1}$.

Our Ideas

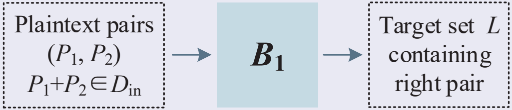
- Distinguishing the cipher E by B_2 needs about $P_{B_2}^{-1}$ chosen plaintext pairs, where $P_{B_2} = \overrightarrow{p}\overleftarrow{p}q^2r$. If all plaintext pairs chosen are right pairs, it can be reduced by a factor of $\overrightarrow{p}^{-1}$.
- How to get a right pair? A plaintext pair chosen randomly is a right pair with the probability $\overrightarrow{p}$.

Our Ideas

- Distinguishing the cipher E by B_2 needs about $P_{B_2}^{-1}$ chosen plaintext pairs, where $P_{B_2} = \overrightarrow{p}\overleftarrow{p}q^2r$. If all plaintext pairs chosen are right pairs, it can be reduced by a factor of $\overrightarrow{p}^{-1}$.
- How to get a right pair? A plaintext pair chosen randomly is a right pair with the probability $\overrightarrow{p}$.
- If by a related boomerang B_1, we can get a target set L of size $l < \overrightarrow{p}^{-1}$, which contains one right pair. Then the complexity will be improved from $P_{B_2}^{-1}$ to $l \cdot \overrightarrow{p} \cdot P_{B_2}^{-1}$.

Framework of Re-Boomerang Distinguisher

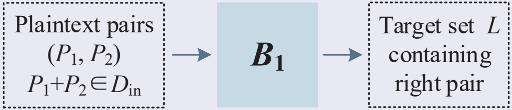
Step 1: Use the boomerang B_1 to obtain a target set L of size $l < \overrightarrow{p}^{-1}$, containing one right pair on average.



Framework of Re-Boomerang Distinguisher

Step 1: Use the boomerang B_1 to obtain a target set L of size $l < \overrightarrow{p}^{-1}$, containing one right pair on average.

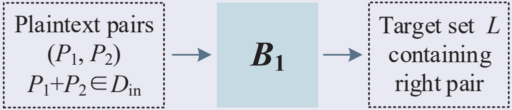
- Choose $P_{B_1}^{-1}$ plaintext pairs (P_1, P_2) such that $P_1 + P_2 \in \mathcal{D}_{in}$, and perform the boomerang distinguisher B_1. If there exists a returned pair satisfying the boomerang property of B_1, then save (P_1, P_2) in the target set L.



Framework of Re-Boomerang Distinguisher

Step 1: Use the boomerang B_1 to obtain a target set L of size $l < \overrightarrow{p}^{-1}$, containing one right pair on average.

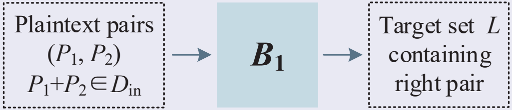
- Choose $P_{B_1}^{-1}$ plaintext pairs (P_1, P_2) such that $P_1 + P_2 \in \mathcal{D}_{in}$, and perform the boomerang distinguisher B_1. If there exists a returned pair satisfying the boomerang property of B_1, then save (P_1, P_2) in the target set L.
- There is $P_{B_1}^{-1} \cdot P_{B_1} = 1$ right pair in L on average.



Framework of Re-Boomerang Distinguisher

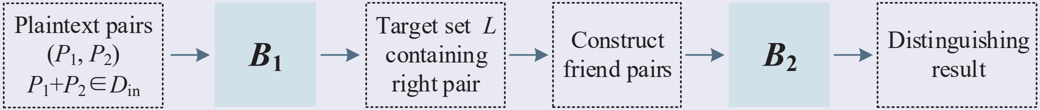
Step 1: Use the boomerang B_1 to obtain a target set L of size $l < \overrightarrow{p}^{-1}$, containing one right pair on average.

- Choose $P_{B_1}^{-1}$ plaintext pairs (P_1, P_2) such that $P_1 + P_2 \in \mathcal{D}_{in}$, and perform the boomerang distinguisher B_1. If there exists a returned pair satisfying the boomerang property of B_1, then save (P_1, P_2) in the target set L.
- There is $P_{B_1}^{-1} \cdot P_{B_1} = 1$ right pair in L on average.
- $l = 1 + P_{B_1}^{-1} P_{R_1}$, where P_{R_1} is the probability of a random pair satisfying the property of B_1.



Framework of Re-Boomerang Distinguisher

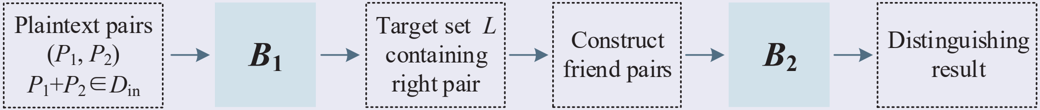
Step 2: For each plaintext pair in L, construct its 'friend pairs' and input to the boomerang B_2 to distinguish the cipher.



Framework of Re-Boomerang Distinguisher

Step 2: For each plaintext pair in L, construct its 'friend pairs' and input to the boomerang B_2 to distinguish the cipher.

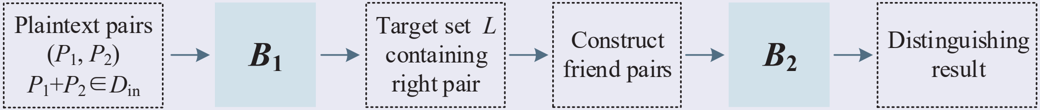
- For each pair (P_1, P_2) in L, construct its $\overrightarrow{p}P_{B_2}^{-1}$ friend pairs (P'_1, P'_2) and input them to B_2.



Framework of Re-Boomerang Distinguisher

Step 2: For each plaintext pair in L, construct its 'friend pairs' and input to the boomerang B_2 to distinguish the cipher.

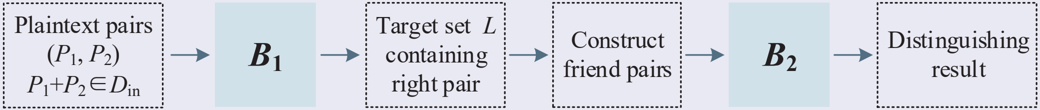
- For each pair (P_1, P_2) in L, construct its $\overrightarrow{p} P_{B_2}^{-1}$ friend pairs (P'_1, P'_2) and input them to B_2.
- For the cipher E, there exists one returned pair satisfying the boomerang property of B_2 on average.



Framework of Re-Boomerang Distinguisher

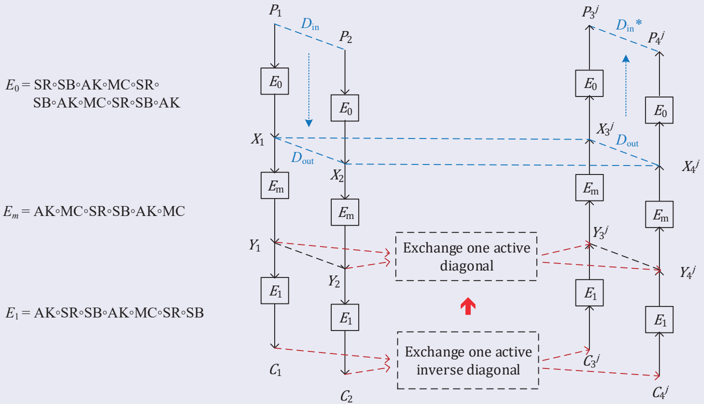
Step 2: For each plaintext pair in L, construct its 'friend pairs' and input to the boomerang B_2 to distinguish the cipher.

- For each pair (P_1, P_2) in L, construct its $\overrightarrow{p} P_{B_2}^{-1}$ friend pairs (P_1', P_2') and input them to B_2.
- For the cipher E, there exists one returned pair satisfying the boomerang property of B_2 on average.
- For a random permutation, the number of pairs satisfying the returned property of B_2 is $l \cdot \overrightarrow{p} P_{B_2}^{-1} P_{R_2} < 1$, where $l < \overrightarrow{p}^{-1}$ and $P_{B_2} > P_{R_2}$.

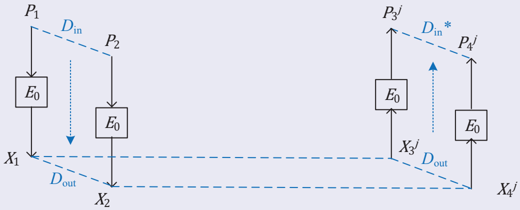


Exchanged Boomerangs for 6-Round AES

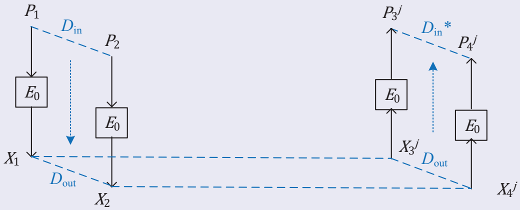
For 6-round AES, we combine truncated boomerangs with exchange technique to give exchanged boomerangs.



Truncated Boomerang for E_0

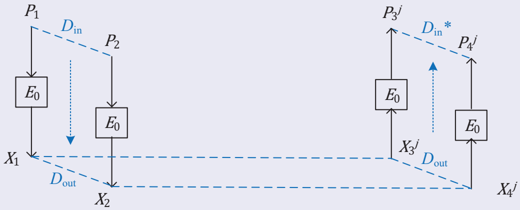


Truncated Boomerang for E_0



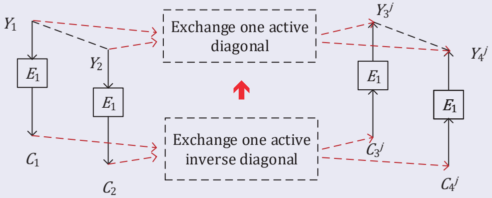
- $\mathcal{D}_{in} \xrightarrow{E_0} \mathcal{D}_{out}$ with probability $\overrightarrow{p}$ in the forward direction

Truncated Boomerang for E_0

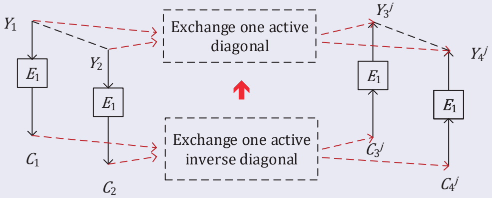


- $\mathcal{D}_{in} \xrightarrow{E_0} \mathcal{D}_{out}$ with probability $\overrightarrow{p}$ in the forward direction
- $\mathcal{D}_{out} \xrightarrow{E_0^{-1}} \mathcal{D}^*_{in}$ with probability $\overleftarrow{p}$ in the backward direction

Exchange Ciphertexts in E_1

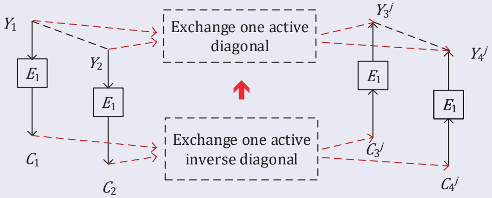


Exchange Ciphertexts in E_1



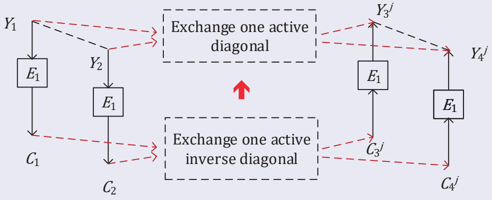
- Choose ciphertext pair (C_1, C_2) such that $C_1 + C_2$ has t inactive inverse diagonals, and exchange one active inverse diagonal of (C_1, C_2) to obtain $4 - t$ ciphertext pairs (C_3^j, C_4^j), $t = 0$ or 1, $j \in \{1, 2, ..., 4 - t\}$.

Exchange Ciphertexts in E_1



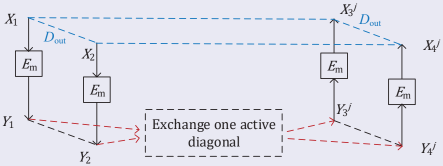
- Choose ciphertext pair (C_1, C_2) such that $C_1 + C_2$ has t inactive inverse diagonals, and exchange one active inverse diagonal of (C_1, C_2) to obtain $4 - t$ ciphertext pairs (C_3^j, C_4^j), $t = 0$ or 1, $j \in \{1, 2, ..., 4 - t\}$.
- $E_1 = AK \circ SR \circ SB \circ AK \circ MC \circ SR \circ SB$.

Exchange Ciphertexts in E_1

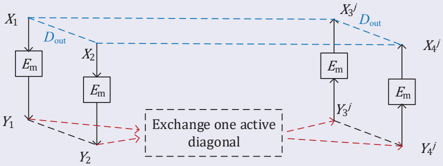


- Choose ciphertext pair (C_1, C_2) such that $C_1 + C_2$ has t inactive inverse diagonals, and exchange one active inverse diagonal of (C_1, C_2) to obtain $4 - t$ ciphertext pairs (C_3^j, C_4^j), $t = 0$ or 1, $j \in \{1, 2, ..., 4 - t\}$.
- $E_1 = AK \circ SR \circ SB \circ AK \circ MC \circ SR \circ SB$.
- $Y_1 + Y_2$ is inactive in t diagonals, and (Y_3^j, Y_4^j) are obtained by exchanging one active diagonal of (Y_1, Y_2), $t = 0$ or 1, $j \in \{1, 2, ..., 4 - t\}$.

Connection Probability for E_m



Connection Probability for E_m

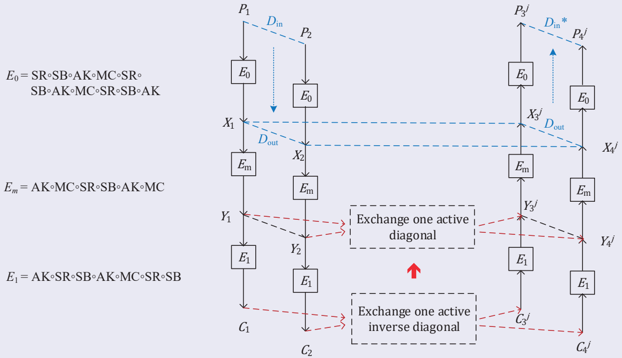


Theorem 1 Let E_m and $\mathcal{D}_{out}$ be defined as above, (X_1, X_2) an input pair of E_m such that $X_1 + X_2 \in \mathcal{D}_{out}$, and (Y_1, Y_2) the corresponding output pair such that $Y_1 + Y_2$ is inactive in t diagonals, $t = 0$ or 1. Let (Y_3^j, Y_4^j) be the pairs by exchanging one active diagonal of (Y_1, Y_2), and (X_3^j, X_4^j) the corresponding output pairs after E_m^{-1}, $j \in \{1, 2, ..., 4-t\}$. Then the probability r that there exists $j \in \{1, 2, ..., 4-t\}$ such that $X_3^j + X_4^j \in \mathcal{D}_{out}$ satisfies

$$r \geq (4-t) \cdot \sum_{d=1}^{3} \binom{4}{d} \cdot (2^{-8})^{4+(2-t)\cdot d}.$$

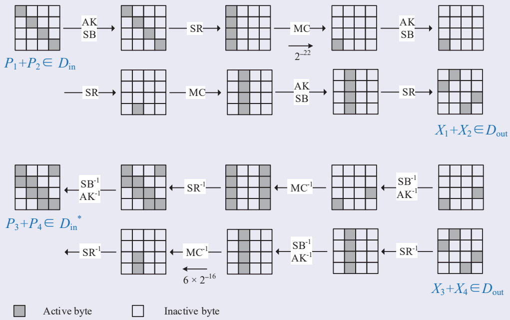
The Exchanged Boomerang

The probability of the exchanged boomerang for 6-round AES is estimated by $\overrightarrow{p}\overleftarrow{p}\,r\cdot\binom{4}{t}2^{-32t}$.



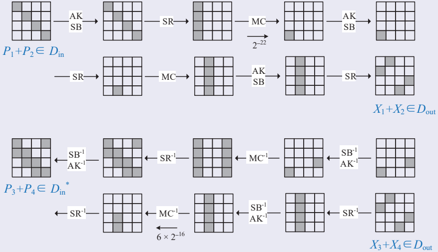
The First Boomerang B_1

- $\mathcal{D}_{in}$ is only active in the 0-th diagonal, $\mathcal{D}_{out}$ is only active in one inverse diagonal, and $\mathcal{D}_{in}^*$ is only active in two diagonals. $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 6 \times 2^{-16} = 2^{-13.42}$.
- Take $t = 1$, then the probability of B_1 is $P_{B_1} = \overrightarrow{p}\overleftarrow{p}r \cdot \binom{4}{t} 2^{-32t} \approx 2^{-101.84}$.



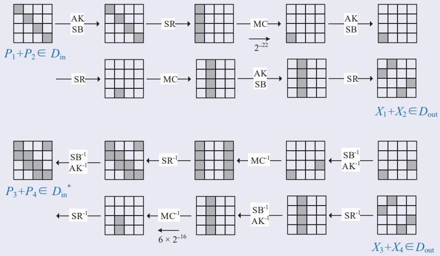
The First Boomerang B_1

- Choose $2^{38.84}$ plaintext structures, in which the 0-th diagonal takes all possible values and the rest bytes are any constants. Then we get $2^{101.84}$ plaintext pairs, and there is a pair following the trail of B_1 on average.



The First Boomerang B_1

- Choose $2^{38.84}$ plaintext structures, in which the 0-th diagonal takes all possible values and the rest bytes are any constants. Then we get $2^{101.84}$ plaintext pairs, and there is a pair following the trail of B_1 on average.
- After applying B_1, the number of pairs in the target set L is $l = 1 + P_{B_1}^{-1} P_{R_1} \approx 1 + 2^{12}$, where $P_{R_1} = 2^{-30} \cdot 3 \cdot 6 \cdot 2^{-64} \approx 2^{-89.84}$.



The Second Boomerang B_2

- In E_0, $\mathcal{D}_{in}$ and $\mathcal{D}_{out}$ are the same as them in B_1, and $\mathcal{D}^*_{in}$ is active in only one diagonal. $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 4 \times 2^{-24} = 2^{-22}$.
- Take $t = 0$, then the probability of B_2 is $P_{B_2} = \overrightarrow{p}\,\overleftarrow{p}\,r \approx 2^{-88}$.

The Second Boomerang B_2

- In E_0, $\mathcal{D}_{in}$ and $\mathcal{D}_{out}$ are the same as them in B_1, and $\mathcal{D}^*_{in}$ is active in only one diagonal. $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 4 \times 2^{-24} = 2^{-22}$.
- Take $t = 0$, then the probability of B_2 is $P_{B_2} = \overrightarrow{p}\,\overleftarrow{p}\,r \approx 2^{-88}$.
- For a right pair, the probability of B_2 is increased to $\overrightarrow{p}^{-1} \cdot P_{B_2} \approx 2^{-66}$.

The Second Boomerang B_2

- In E_0, $\mathcal{D}_{in}$ and $\mathcal{D}_{out}$ are the same as them in B_1, and $\mathcal{D}^*_{in}$ is active in only one diagonal. $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 4 \times 2^{-24} = 2^{-22}$.
- Take $t = 0$, then the probability of B_2 is $P_{B_2} = \overrightarrow{p}\,\overleftarrow{p}\,r \approx 2^{-88}$.
- For a right pair, the probability of B_2 is increased to $\overrightarrow{p}^{-1} \cdot P_{B_2} \approx 2^{-66}$.
- For each pair in L, construct 2^{66} friend pairs to input B_2, and then distinguish 6-round AES from a random permutation.

The Second Boomerang B_2

- In E_0, $\mathcal{D}_{in}$ and $\mathcal{D}_{out}$ are the same as them in B_1, and $\mathcal{D}^*_{in}$ is active in only one diagonal. $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 4 \times 2^{-24} = 2^{-22}$.
- Take $t = 0$, then the probability of B_2 is $P_{B_2} = \overrightarrow{p}\,\overleftarrow{p}\,r \approx 2^{-88}$.
- For a right pair, the probability of B_2 is increased to $\overrightarrow{p}^{-1} \cdot P_{B_2} \approx 2^{-66}$.
- For each pair in L, construct 2^{66} friend pairs to input B_2, and then distinguish 6-round AES from a random permutation.
- The size of L is $l = 1 + 2^{12}$.

The Second Boomerang B_2

- In E_0, $\mathcal{D}_{in}$ and $\mathcal{D}_{out}$ are the same as them in B_1, and $\mathcal{D}^*_{in}$ is active in only one diagonal. $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 4 \times 2^{-24} = 2^{-22}$.
- Take $t = 0$, then the probability of B_2 is $P_{B_2} = \overrightarrow{p}\,\overleftarrow{p}\, r \approx 2^{-88}$.
- For a right pair, the probability of B_2 is increased to $\overrightarrow{p}^{-1} \cdot P_{B_2} \approx 2^{-66}$.
- For each pair in L, construct 2^{66} friend pairs to input B_2, and then distinguish 6-round AES from a random permutation.
- The size of L is $l = 1 + 2^{12}$.
- The total number of input pairs of B_2 is about 2^{78}, reduced by a factor of 2^{10}.

The Re-Boomerang Distinguishing Process

1. Choose $2^{38.84}$ plaintext structures of size 2^{32} in which the four bytes in $SR^{-1}(Col(0))$ take all possible values and the rest bytes are any constants, and ask for the corresponding ciphertexts.
2. For each structure, insert 2^{32} ciphertexts into a hash table indexed by $SR(Col(i))$, and extract all ciphertext pairs (C_1, C_2) such that $(C_1 + C_2)_{SR(Col(i))} = 0$, $i = 0, 1, 2, 3$.
3. For each $j \in \{0, 1, 2, 3\} \setminus i$, exchange the j-th inverse diagonal of (C_1, C_2) to obtain (C_3, C_4), and ask for the decryption of (C_3, C_4) to obtain (P_3, P_4). If there exists one (P_3, P_4) such that $P_3 + P_4$ is active in only two diagonals, we store the corresponding plaintext pairs (P_1, P_2) to the set L.

The Re-Boomerang Distinguishing Process

4. For each (P_1, P_2) in L, construct 2^{66} 'friend pairs' (P'_1, P'_2) such that $P'_{1,SR^{-1}(Col(0))} = P_{1,SR^{-1}(Col(0))}$, $P'_{2,SR^{-1}(Col(0))} = P_{2,SR^{-1}(Col(0))}$, and in the other bytes P'_1 and P'_2 take any equal values except the value of P_1. Ask for the encryption of (P'_1, P'_2) to obtain (C'_1, C'_2).
5. Filter (C'_1, C'_2) such that $C'_1 + C'_2$ are active in four inverse diagonals. For each (C'_1, C'_2) and each $j \in \{0, 1, 2, 3\}$, we exchange the j-th inverse diagonal of (C'_1, C'_2) to obtain (C'_3, C'_4), and decrypt (C'_3, C'_4) to obtain (P'_3, P'_4). If there exists one pair (P'_3, P'_4) such that $P'_3 + P'_4$ is active in only one diagonal, the distinguishing result is "6-round AES", otherwise it is "a random permutation".

Complexity of Re-Boomerang Distinguisher

- The data and time complexities of a distinguishing process are both $2^{81.33}$. That is, $2^{70.84}$ CP, $2^{74.42}$ ACC, 2^{79} ACP and 2^{81} ACC.

Complexity of Re-Boomerang Distinguisher

- The data and time complexities of a distinguishing process are both $2^{81.33}$. That is, $2^{70.84}$ CP, $2^{74.42}$ ACC, 2^{79} ACP and 2^{81} ACC.
- The success probability is about $ps_1 \cdot ps_2 \approx (1 - e^{-1})^2 \approx 40\%$.

Complexity of Re-Boomerang Distinguisher

- The data and time complexities of a distinguishing process are both $2^{81.33}$. That is, $2^{70.84}$ CP, $2^{74.42}$ ACC, 2^{79} ACP and 2^{81} ACC.
- The success probability is about $ps_1 \cdot ps_2 \approx (1 - e^{-1})^2 \approx 40\%$.
- Repeat the re-boomerang distinguishing process twice, then the success probability is $P_s = 1 - (1 - ps_1 \cdot ps_2)^2 \approx 64\%$.

Complexity of Re-Boomerang Distinguisher

- The data and time complexities of a distinguishing process are both $2^{81.33}$. That is, $2^{70.84}$ CP, $2^{74.42}$ ACC, 2^{79} ACP and 2^{81} ACC.
- The success probability is about $ps_1 \cdot ps_2 \approx (1 - e^{-1})^2 \approx 40\%$.
- Repeat the re-boomerang distinguishing process twice, then the success probability is $P_s = 1 - (1 - ps_1 \cdot ps_2)^2 \approx 64\%$.
- The total data and time complexities are both $2^{82.33}$.

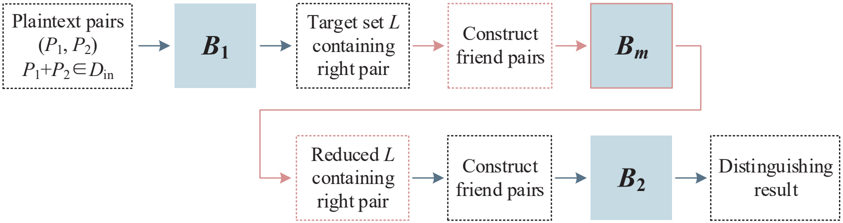
Complexity of Re-Boomerang Distinguisher

- The data and time complexities of a distinguishing process are both $2^{81.33}$. That is, $2^{70.84}$ CP, $2^{74.42}$ ACC, 2^{79} ACP and 2^{81} ACC.
- The success probability is about $ps_1 \cdot ps_2 \approx (1 - e^{-1})^2 \approx 40\%$.
- Repeat the re-boomerang distinguishing process twice, then the success probability is $P_s = 1 - (1 - ps_1 \cdot ps_2)^2 \approx 64\%$.
- The total data and time complexities are both $2^{82.33}$.
- The type-II error probability (the probability of accepting a random permutation as 6-round AES) is about

$$1 - (1 - 2^{-92})^{2^{78} \times 2} \approx 2^{-13}.$$

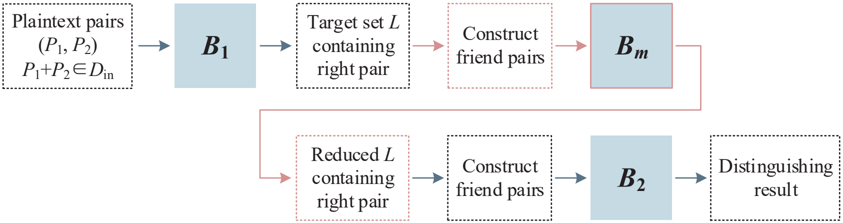
Triple Boomerangs Distinguisher

- In order to improve the complexity, we input a new boomerang B_m in the middle of the re-boomerang distinguisher, which is used to reduce the size of L.



Triple Boomerangs Distinguisher

- In order to improve the complexity, we input a new boomerang B_m in the middle of the re-boomerang distinguisher, which is used to reduce the size of L.
- The trails of B_m are the same as those of B_1 over E_0, and the other trails (over E_m and E_1) are the same as those of B_2.
- For a right pair, the probability of B_m is $\overleftarrow{p}\,r \approx 2^{-13.42} \times 2^{-44} = 2^{-57.42}$.



Use B_m to Reduce the Size of L

For each pair (P_1, P_2) in L, construct its $2^{57.42}$ friend pairs (P'_1, P'_2) and input them to B_m. If there exist no returned (P'_3, P'_4) satisfying the boomerang property of B_m, then we delete (P_1, P_2) from L.

Use B_m to Reduce the Size of L

For each pair (P_1, P_2) in L, construct its $2^{57.42}$ friend pairs (P_1', P_2') and input them to B_m. If there exist no returned (P_3', P_4') satisfying the boomerang property of B_m, then we delete (P_1, P_2) from L.

- If (P_1, P_2) is a right pair, it will be kept in L.

Use B_m to Reduce the Size of L

For each pair (P_1, P_2) in L, construct its $2^{57.42}$ friend pairs (P'_1, P'_2) and input them to B_m. If there exist no returned (P'_3, P'_4) satisfying the boomerang property of B_m, then we delete (P_1, P_2) from L.

- If (P_1, P_2) is a right pair, it will be kept in L.
- The boomerang property of B_m is satisfied randomly with probability $P_{R_m} = 4 \times 6 \times 2^{-64} \approx 2^{-59.42}$.

Use B_m to Reduce the Size of L

For each pair (P_1, P_2) in L, construct its $2^{57.42}$ friend pairs (P'_1, P'_2) and input them to B_m. If there exist no returned (P'_3, P'_4) satisfying the boomerang property of B_m, then we delete (P_1, P_2) from L.

- If (P_1, P_2) is a right pair, it will be kept in L.
- The boomerang property of B_m is satisfied randomly with probability $P_{R_m} = 4 \times 6 \times 2^{-64} \approx 2^{-59.42}$.
- If (P_1, P_2) is not right pair, it is kept in L with probability $1 - (1 - 2^{-59.42})^{2^{57.42}} \approx 2^{-2.18}$.

Use B_m to Reduce the Size of L

For each pair (P_1, P_2) in L, construct its $2^{57.42}$ friend pairs (P'_1, P'_2) and input them to B_m. If there exist no returned (P'_3, P'_4) satisfying the boomerang property of B_m, then we delete (P_1, P_2) from L.

- If (P_1, P_2) is a right pair, it will be kept in L.
- The boomerang property of B_m is satisfied randomly with probability $P_{R_m} = 4 \times 6 \times 2^{-64} \approx 2^{-59.42}$.
- If (P_1, P_2) is not right pair, it is kept in L with probability $1-(1-2^{-59.42})^{2^{57.42}} \approx 2^{-2.18}$.
- After B_m, the size of L is reduced to $1 + 2^{12} \times 2^{-2.18} = 1 + 2^{9.82}$.

Use B_m to Reduce the Size of L

- To increase the filtering effect of B_m, for each pair (P_1, P_2) in L, we can construct $2^{57.42} \cdot n$ friend pairs, $n \geq 1$.

Use B_m to Reduce the Size of L

- To increase the filtering effect of B_m, for each pair (P_1, P_2) in L, we can construct $2^{57.42} \cdot n$ friend pairs, $n \geq 1$.
- If the number of returned pairs satisfying the boomerang property of B_m is less than n, then delete (P_1, P_2) from L.

Use B_m to Reduce the Size of L

- To increase the filtering effect of B_m, for each pair (P_1, P_2) in L, we can construct $2^{57.42} \cdot n$ friend pairs, $n \geq 1$.
- If the number of returned pairs satisfying the boomerang property of B_m is less than n, then delete (P_1, P_2) from L.
- A wrong pair (P_1, P_2) is kept in L with the probability

$$p_f(n) = 1 - \sum_{k=0}^{n-1} \binom{2^{57.42} n}{k} \cdot (2^{-59.42})^k \cdot (1 - 2^{-59.42})^{2^{57.42} n - k}.$$

After filtering, the size of L is $1 + 2^{12} p_f(n)$.

Complexity of Triple Boomerangs Distinguisher

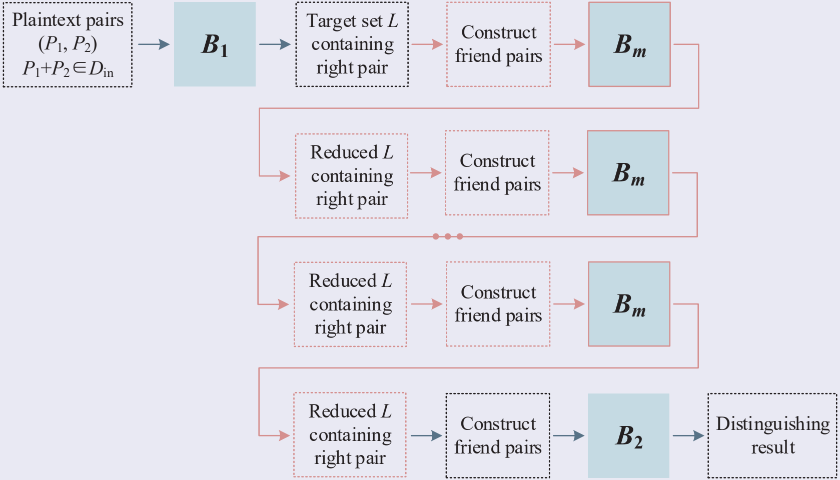
- The data and time complexities are about $D = T = 2^{74.64} + 2^{72.74}n + 2^{69.32}$.
- The success probability is $ps_1 \cdot ps_m(n) \cdot ps_2 \leq 40\%$.
- Repeat the triple boomerangs distinguisher w times, then the complexity is $w \cdot T$, and the success probability is $P_s = 1 - \left[1 - \left(1 - e^{-1}\right)^2 \cdot ps_m(n)\right]^w$.

Complexity of Triple Boomerangs Distinguisher

Table 1. The parameter w, complexities and success probability of the triple boomerangs distinguisher

n	w	$D = T$	Success Probability	n	w	$D = T$	Success Probability
1	3	$2^{80.81}$	63%	2	3	$2^{79.65}$	63%
3	3	$2^{78.79}$	64%	4	3	$2^{78.21}$	65%
5	3	$2^{77.91}$	65%	6	3	$2^{77.82}$	66%
7	3	$2^{77.83}$	67%	8	3	$2^{77.90}$	67%
9	3	$2^{78.00}$	68%	10	3	$2^{78.10}$	68%
11	3	$2^{78.20}$	69%	12	3	$2^{78.28}$	69%
13	3	$2^{78.37}$	70%	14	3	$2^{78.46}$	70%
15	3	$2^{78.54}$	71%	16	3	$2^{78.61}$	71%

The General Boomerang Chain Distinguisher



Two Improvements

- Repeat the middle boomerang trail B_m several times in the middle.
  - Denote by s the number of times B_m is repeated, then a boomerang chain consists of $s + 2$ boomerang trails, starting from B_1, repeating B_m s times, and ending with B_2.

Two Improvements

- Repeat the middle boomerang trail B_m several times in the middle.
  - Denote by s the number of times B_m is repeated, then a boomerang chain consists of $s+2$ boomerang trails, starting from B_1, repeating B_m s times, and ending with B_2.
- Increase the input data size for each boomerang.
  - The input of B_1: $2^{38.84}$ n_1 plaintext structures.
  - The input of the i-th middle boomerangs B_m, $2 \leq i \leq s+1$: $2^{57.42}$ n_i 'friend pairs' for each plaintext pair in L.
  - The input of B_2: 2^{66} n_{s+2} 'friend pairs' for each plaintext pair in L.

Complexity of Boomerang Chain distinguisher

Denote that the boomerang chain process is repeated w times to form a distinguisher. The time and data complexities of the distinguisher are

$$T = D = w \cdot \sum_{i=1}^{s+2} D_i.$$

The success probability of the distinguisher is

$$P_s = 1 - [1 - ps_1 \cdot ps_m(n_2) \cdot ps_m(n_3) \cdots ps_m(n_{s+1}) \cdot ps_2]^w .$$

Complexity of Boomerang Chain distinguisher

Table 2. The parameters $n_1, n_2, \ldots, n_{s+2}$, w, complexities and success probability of the boomerang chain distinguisher

s	$n_1, n_2, \ldots, n_{s+2}$	w	$D = T$	Success Probability
1	1,7,2	2	$2^{77.36}$	66%
2	1,2,13,5	2	$2^{76.57}$	60%
3	1,2,15,110,4	2	$2^{76.59}$	60%
4	1,2,14,116,122,5	2	$2^{76.60}$	60%

Experimental Simulation on Small-Scale AES

- We mount an experiment to the 64-bit small-scale AES, presented in FSE 2005.

Experimental Simulation on Small-Scale AES

- We mount an experiment to the 64-bit small-scale AES, presented in FSE 2005.
- The probabilities of B_1, B_m and B_2 are $P_{B_1} = 2^{-47.42}$, $P_{B_m} = 2^{-37.42}$ and $P_{B_2} = 2^{-42}$ respectively, and $\overrightarrow{p} = 2^{-10}$.
- The parameters of the 6-round boomerang chain distinguisher are the same as the second row of the Table above. That is, $B_1 \to B_m \to B_m \to B_2$. The distinguisher is performed twice, and the complexity is about $2^{37.7}$.
- We implement 500 experiments for random keys and plaintext structures. There are 346 results returning "6-round small-scale AES". The experimental success probability is about 69%.

Conclusion

- We extend the classical boomerang distinguisher to combine two or more related boomerangs with the technique of 'friend pairs' and propose the re-boomerang and boomerang chain distinguishers for 6-round AES.

Conclusion

- We extend the classical boomerang distinguisher to combine two or more related boomerangs with the technique of 'friend pairs' and propose the re-boomerang and boomerang chain distinguishers for 6-round AES.
- The boomerang chain distinguisher for 6-round AES has the data and time complexities $2^{76.57}$ and success probability 60%. Compared with the previous best result, the data complexity is reduced by a factor of 172, which is a new record for 6-round distinguisher on AES.

Conclusion

- We extend the classical boomerang distinguisher to combine two or more related boomerangs with the technique of 'friend pairs' and propose the re-boomerang and boomerang chain distinguishers for 6-round AES.
- The boomerang chain distinguisher for 6-round AES has the data and time complexities $2^{76.57}$ and success probability 60%. Compared with the previous best result, the data complexity is reduced by a factor of 172, which is a new record for 6-round distinguisher on AES.

Thanks for Your Attention!