Structural exchange attack against 6-round AES-128

Rachelle Heim Boissier

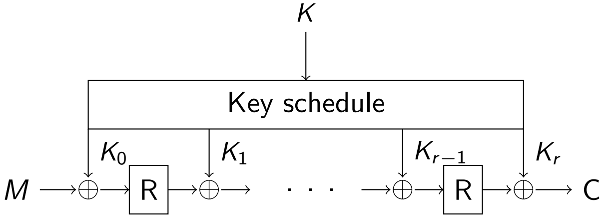
UVSQ

Joint work with Henri Gilbert and Jean-René Reinhard (ANSSI)

14 April 2022

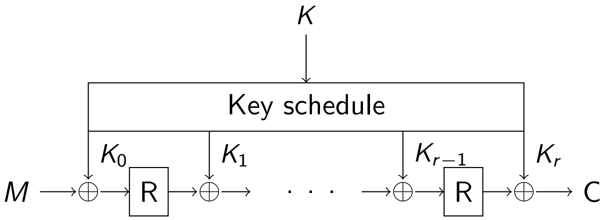
Key recovery attacks against block ciphers

General structure of an iterated block cipher:

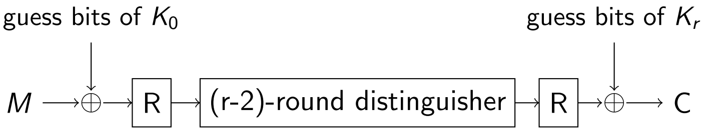


Key recovery attacks against block ciphers

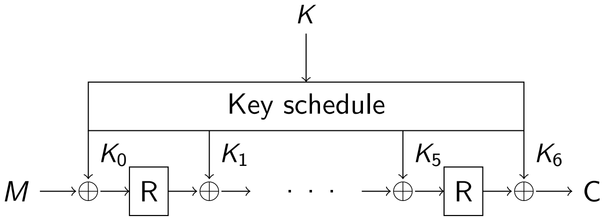
General structure of an iterated block cipher:



Key derivation attacks:



General structure of 6-round AES:

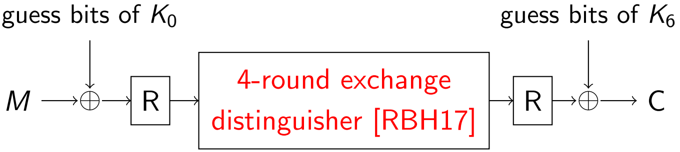


Key derivation attacks against AES:

Our contribution

- Starting point: new 4-round exchange distinguisher by Rønjom, Bardeh and Helleseth [RBH17, BR19]
- Motivation: investigate key derivation attacks using this distinguisher
- Our contribution: mounting such an attack against 6-round AES-128

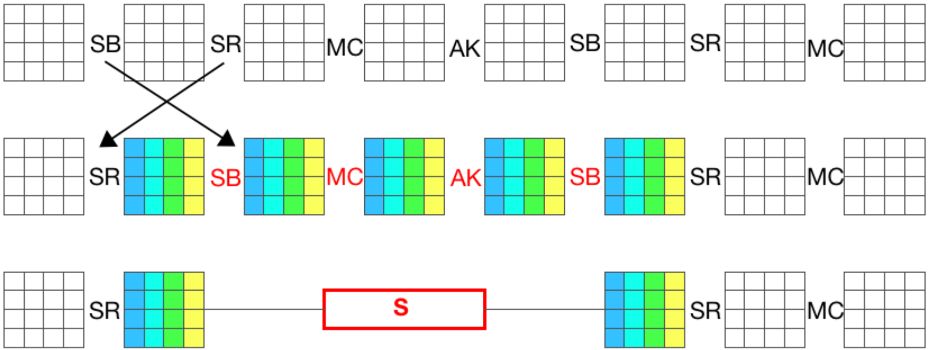
Structural exchange attack against AES:

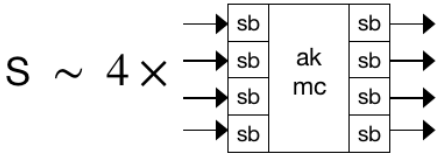


Outline

1. The 4-round exchange distinguisher [RBH17]
2. Key recovery attack on 6-round AES

Super S-box representation of 2 rounds of AES





Super S-box representation of 4-round AES

Super S-box representation (2 rounds)

$$R^2 = AK \circ MC \circ SR \circ S \circ SR$$

Super S-box representation of 4-round AES

Super S-box representation (2 rounds)

$$R^2 = AK \circ MC \circ SR \circ {\color{red}S} \circ SR$$

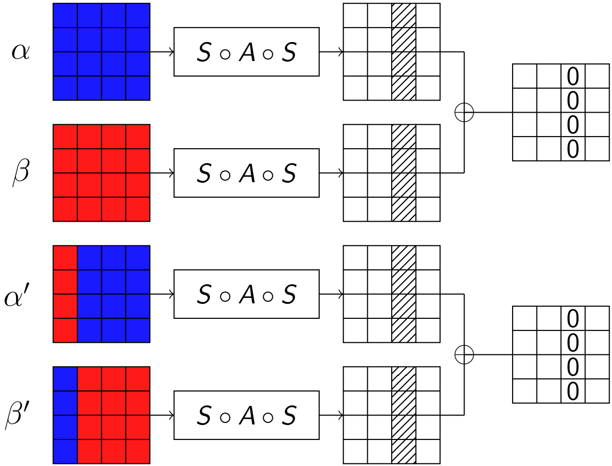
Super S-box representation (4 rounds)

$$\begin{aligned} R^4 &= R^2 \circ R^2 \\ &= AK \circ MC \circ SR \circ {\color{red}S} \circ \underbrace{{\color{blue}SR \circ AK \circ MC \circ SR}}_{\text{affine permutation } A} \circ {\color{red}S} \circ SR \\ &= AK \circ MC \circ SR \circ {\color{red}S} \circ {\color{blue}A} \circ {\color{red}S} \circ SR \end{aligned}$$

4-round exchange property [RBH17]

If

Then

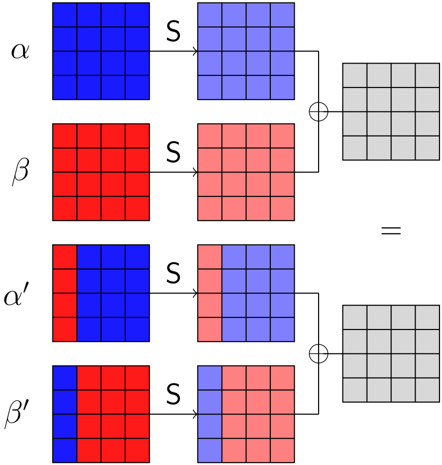


Exchange property

If $S \circ A \circ S(\alpha)$ and $S \circ A \circ S(\beta)$ are equal on a column, then this collision is preserved by any column exchange between α and β

4-round exchange property (proof)

If



Then

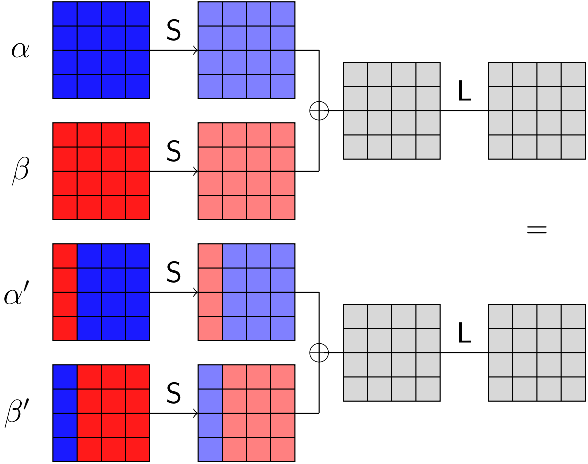
Since S operates independently on columns:

$$S(\alpha) \oplus S(\beta) = S(\alpha') \oplus S(\beta')$$

4-round exchange property (proof)

If

Then



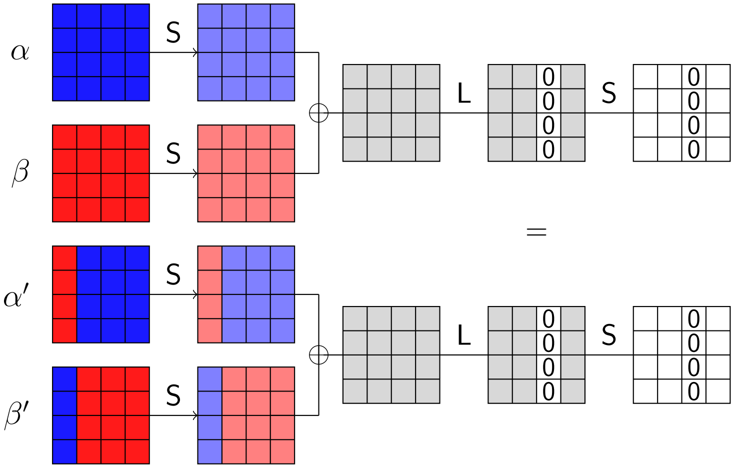
Since A is affine (A(x) = L(x)+C):

$$A \circ S(\alpha) \oplus A \circ S(\beta) = A \circ S(\alpha') \oplus A \circ S(\beta')$$

4-round exchange property (proof)

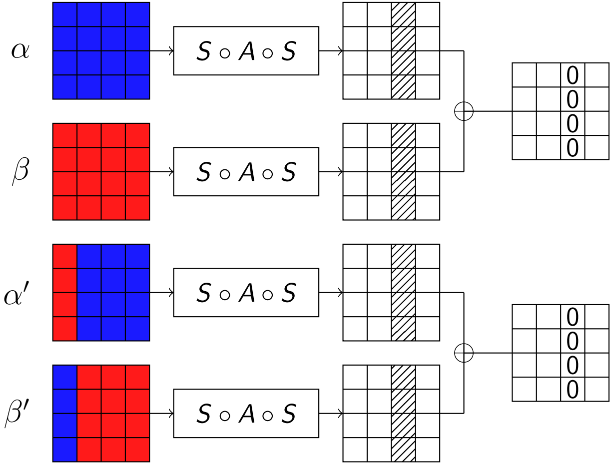
If

Then



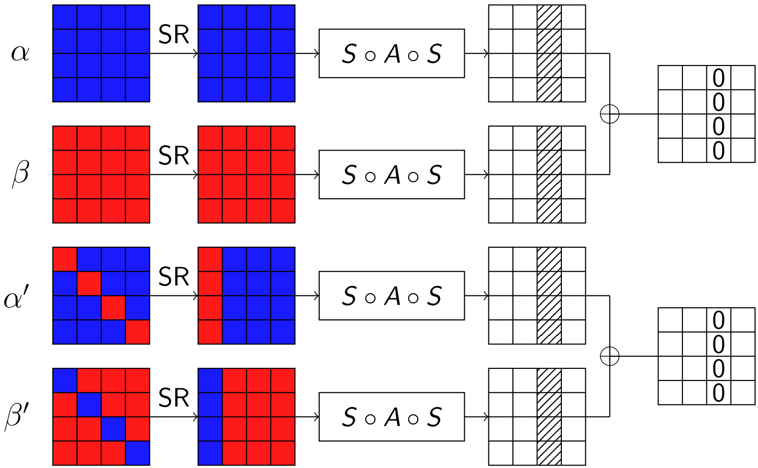
S preserves equality on columns

4-round exchange property [RBH17]



$$R^4 = \mathrm{AK} \circ \mathrm{MC} \circ \mathrm{SR} \circ \boxed{\mathrm{S} \circ \mathrm{A} \circ \mathrm{S}} \circ \mathrm{SR}$$

4-round exchange property [RBH17]

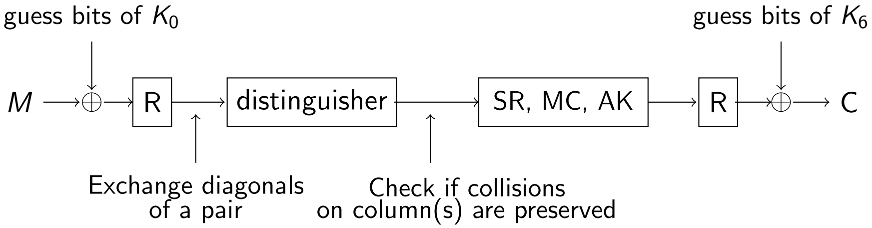


$$R^4 = \mathrm{AK} \circ \mathrm{MC} \circ \mathrm{SR} \circ \boxed{\mathrm{S} \circ \mathrm{A} \circ \mathrm{S}} \circ \mathrm{SR}$$

Outline

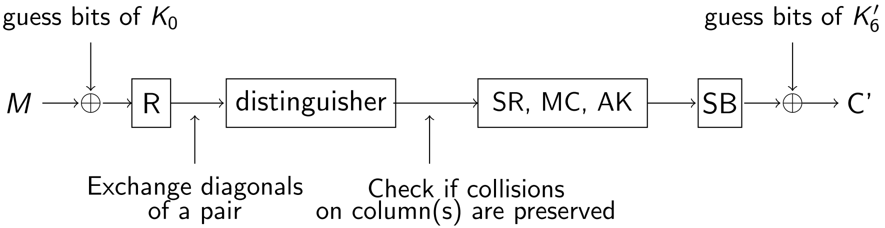
1. The 4-round exchange distinguisher [RBH17]
2. Key recovery attack on 6-round AES

Key recovery attack
General idea



Key recovery attack

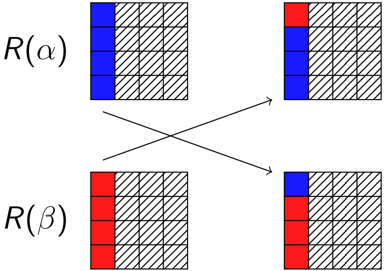
General idea



Diagonal exchange after one round

Property

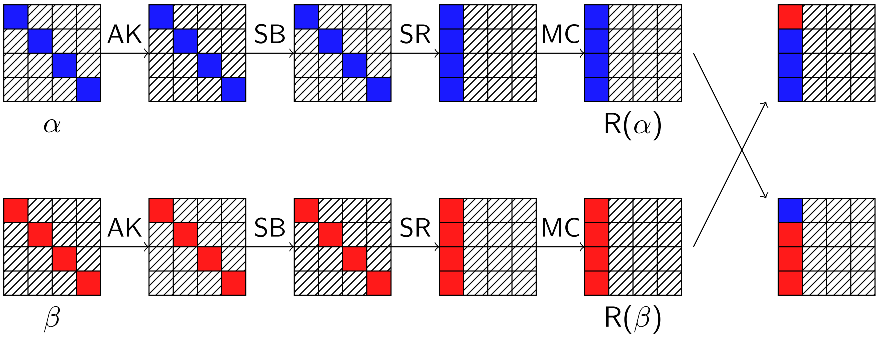
If $R(\alpha)$ and $R(\beta)$ are equal on three columns, then exchanging bytes of the remaining column is the same as exchanging diagonals.



Diagonal exchange after one round

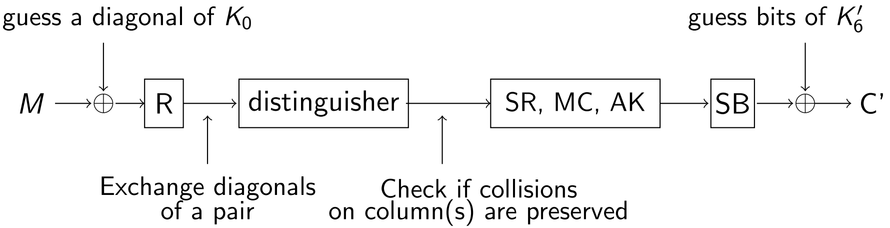
Observation

For a good hypothesis on one of the diagonal of K_0, if α and β are equal on the three other diagonals, then one can compute up to 7 new plaintext pairs $\{\alpha', \beta'\}$ which realise a diagonal exchange after one round



Key recovery attack

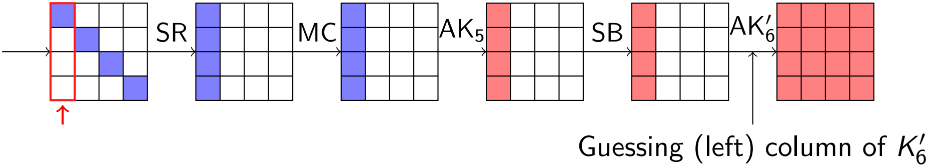
General idea



Detecting collisions on a column

Observation

Knowing one column of K_6' allows the detection of a collision on one byte per column.

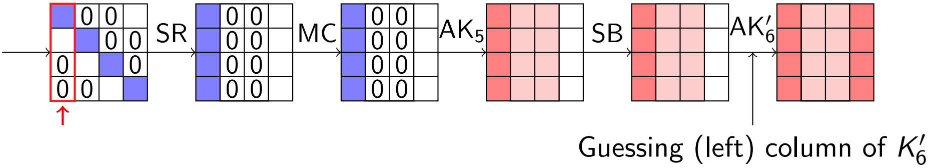


Probability that a collision on a byte is a collision on a column: $p = 2^{-24}$

Detecting collisions on a column (filtering trick)

Observation

Knowing one column of K_6' allows the detection of a collision on one byte per column.



Probability that a collision on a byte is a collision on a column: $p = 2^{-8}$

Key recovery attack

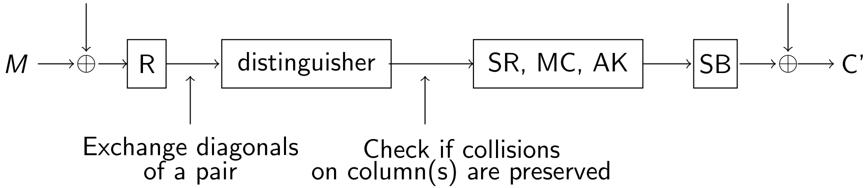
Do the following 2^{17} times:

1. Generate a structure of 2^{32} states that are all equal on 3 diagonals out of 4, encrypt them

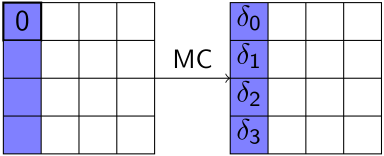
2. Find a pair of ciphertexts such that there is a collision on two columns

3. Guess a diagonal of K_0

4. Guess a column of K_6'

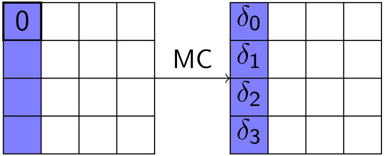


Improvement: guessing K_6' with MITM



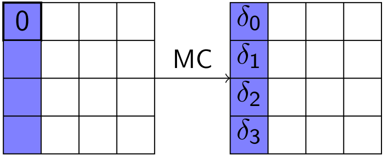
$$0 \stackrel{?}{=} 0E \cdot \delta_0 + 0B \cdot \delta_1 + 0D \cdot \delta_2 + 09 \cdot \delta_3$$

Improvement: guessing K_6' with MITM



$$0E \cdot \delta_0 + 0B \cdot \delta_1 \stackrel{?}{=} 0D \cdot \delta_2 + 09 \cdot \delta_3$$

Improvement: guessing K_6' with MITM



$$0E \cdot \delta_0 + 0B \cdot \delta_1 \stackrel{?}{=} 0D \cdot \delta_2 + 09 \cdot \delta_3$$

For each pair, compute separately $0E \cdot \delta_0 + 0B \cdot \delta_1$ and $0D \cdot \delta_2 + 09 \cdot \delta_3$ then look for collisions.

$\rightarrow$ Testing all K_6': complexity of 2^{17} instead of 2^{32}

Our contribution (1/2)

Family	Ref.	Rounds	Data	Time	Memory
Integral	[DKR97]	6	2^{32} CP	2^{72} E	2^{32}
	[FKL+00]	6	2^{32} CP	2^{42} E	2^{32}
Exchange	[BDK$^+$20]	6	2^{26} CP	2^{80} E	2^{28}
	Our attack	6	2^{50} CP	2^{64} E	2^{32}
Impossible Diff.	[BLNS18]	7	2^{105} CP	2^{113} E	2^{74}
	[LP21]	7	2^{105} CP	2^{111} E	2^{72}
MITM	[DFJ13]	7	2^{97} CP	2^{99} E	2^{98}

Survey of existing key-recovery attacks against AES

Our contribution (2/2)

Distinguisher	Rounds	Data	Time	Memory
Multiple-of-8 [GRR17]	5	2^{32} CP	$2^{35.6}$ XOR	2^{32}
Yoyo [RBH17]	5	2^{26} ACC	2^{25} XOR	small
Exchange [BR19]	5	2^{30} CP	2^{30} E	2^{37}
Yoyo [RBH17]	6	2^{123} ACC	2^{122} XOR	/
Exchange [BR19]	6	$2^{88.2}$ CP	$2^{88.2}$ E	$2^{88.2}$

Attack	Rounds	Data	Time	Memory
[BDK+20]	6	2^{26} CP	2^{80} E	2^{28}
Our attack	6	2^{50} CP	2^{64} E	2^{32}

→ The 4-round exchange distinguisher can be converted into a key recovery attack of near-practical complexity

Thank you for your attention!

Questions?