Related-Key Boomerang Attacks on AES

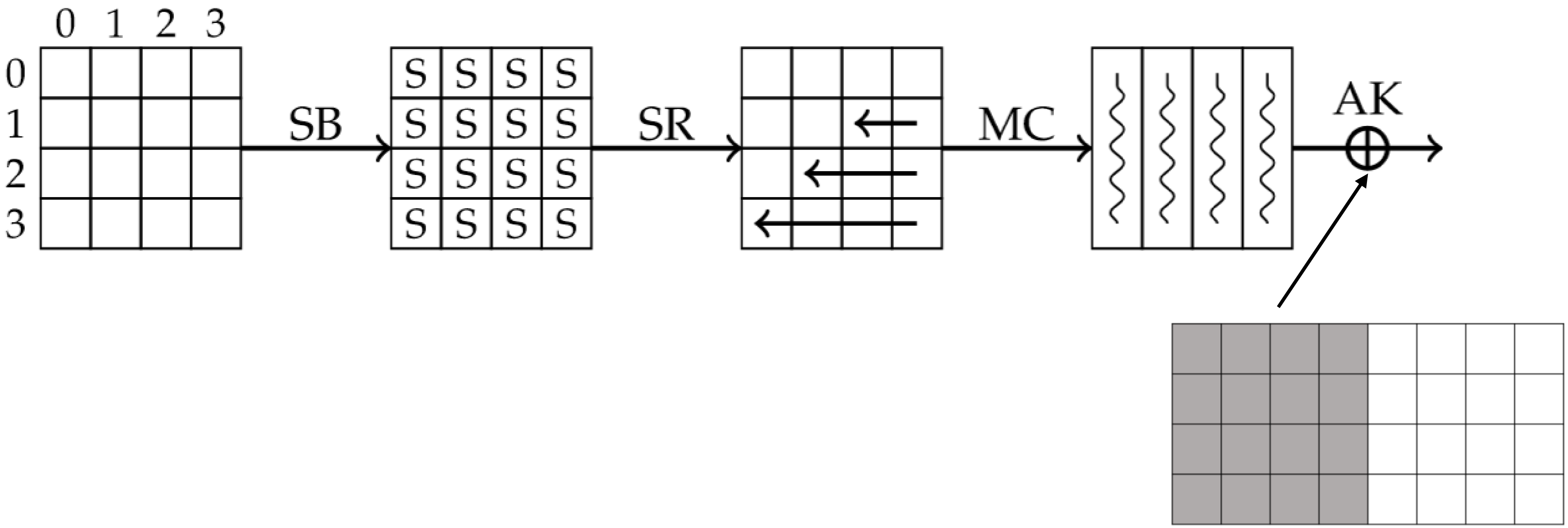
Halil İbrahim Kaplan

2021

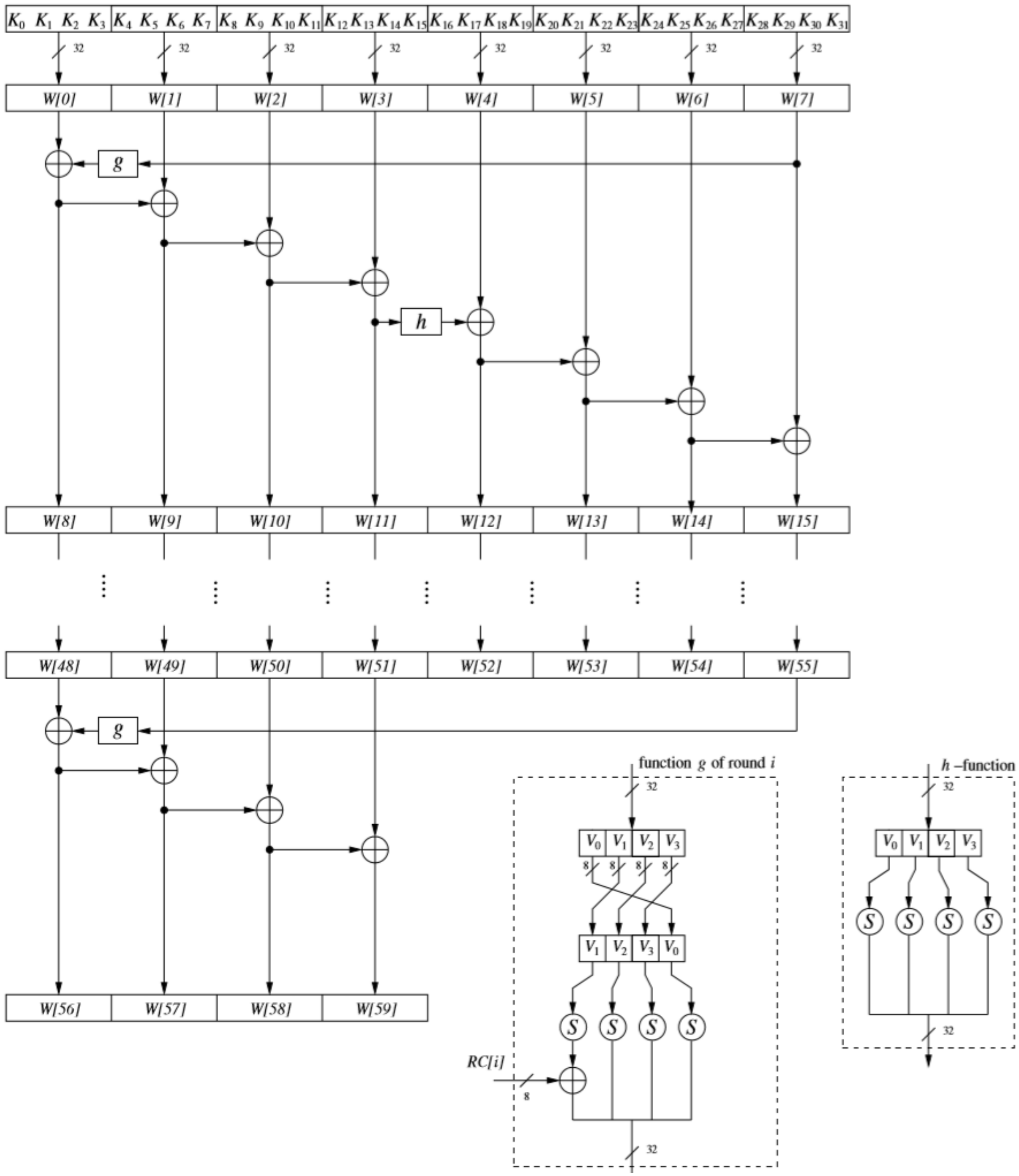
TÜBİTAK
BİLGEM

Overview

- Preliminaries
- Related-Key Boomerang Attack on 7-Round AES-192
- Related-Key Boomerang Attack on Full AES-256


0
1
2
3
SB
S
SR
MC
AK

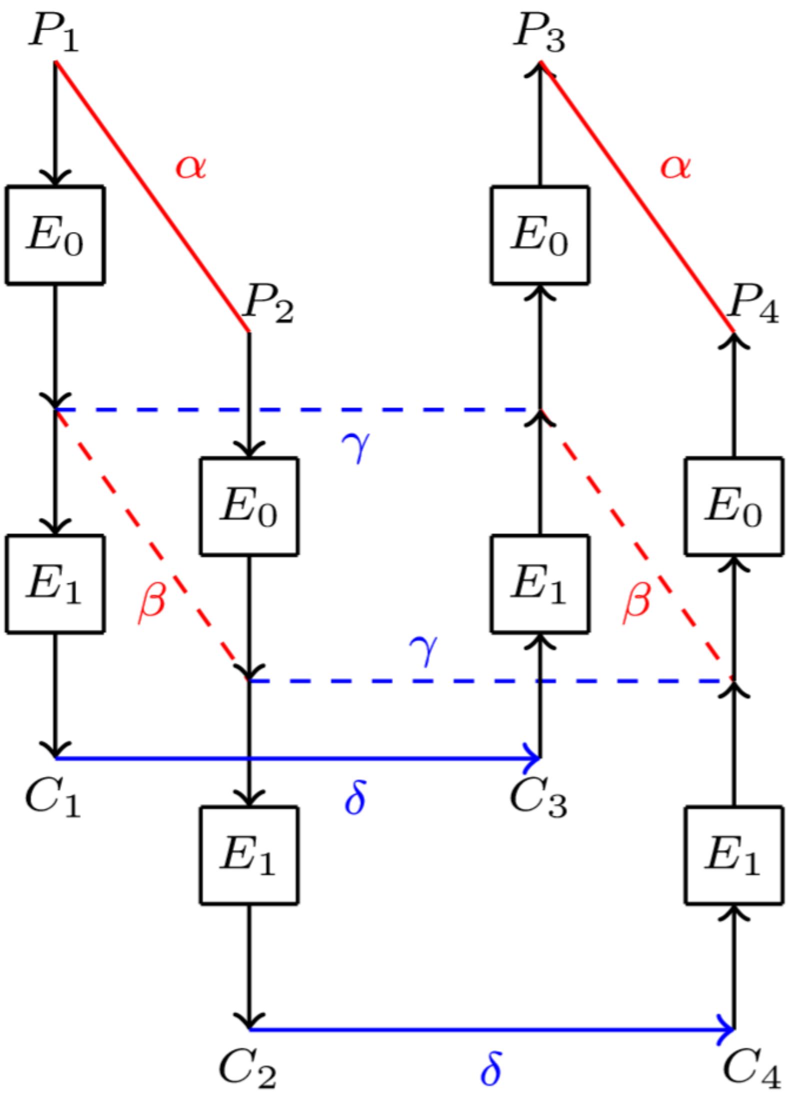
7 ROUND



K_0 K_1 K_2 K_3 K_4 K_5 K_6 K_7 K_8 K_9 K_{10} K_{11} K_{12} K_{13} K_{14} K_{15} K_{16} K_{17} K_{18} K_{19} K_{20} K_{21} K_{22} K_{23} K_{24} K_{25} K_{26} K_{27} K_{28} K_{29} K_{30} K_{31}
32
W[0] W[1] W[2] W[3] W[4] W[5] W[6] W[7]
g
h
W[8] W[9] W[10] W[11] W[12] W[13] W[14] W[15]
W[48] W[49] W[50] W[51] W[52] W[53] W[54] W[55]
g
W[56] W[57] W[58] W[59]
function g of round i
V_0 V_1 V_2 V_3
8
V_1 V_2 V_3 V_0
S
RC[i]
h –function

Boomerang Attack :

- Cipher E divided into two sub-ciphers
- $E = E_0 \circ E_1$
- E_0: P[α ⟶ β]= p
- E_1: P[γ ⟶ δ]= q
- The two trails are assumed to be independent.
- Distinguish probability:
- Pr[E^{-1}(E(x)⊕δ)⊕E^{-1}(E(x⊕α)⊕δ)= α]= p^2q^2



Related-Key Attack Model :

Class of cryptanalytic attacks in which the attacker knows or chooses a relation between several keys and is given access to encryption/decryption functions with all these keys.

The relation between the keys can be an arbitrary bijective function R (or even a family of such functions) chosen in advance by the attacker.

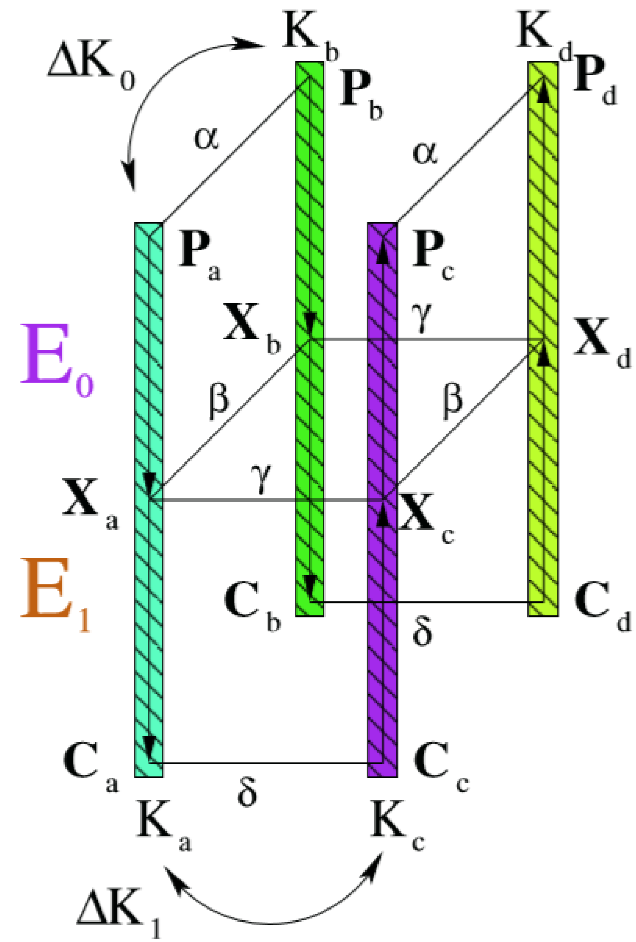
EX:

$$K_2 = \underbrace{F^{-1}(F}_{\text{Single round of the AES-256 key schedule}}(K_1) \oplus \underbrace{C}_{\text{Constant C (chosen by the attacker)}}) = RC(K_2)$$

Related Key Boomerang Attack :

$K_b = K_a \oplus \Delta K_0$
$K_c = K_a \oplus \Delta K_1$
$K_d = K_a \oplus \Delta K_0 \oplus \Delta K_1$

- Choose P_a and compute $P_a = P_a \oplus \alpha$
- Encrypt P_a under K_a and P_b under K_b
- Compute $C_c = C_a \oplus \delta$ and $C_d = C_b \oplus \delta$
- Decrypt C_c under K_c and C_d under K_d
- Test whether $P_c \oplus P_d = \alpha$
- If $P_c \oplus P_d = \alpha$ then (P_a , P_b , P_c , P_d) forms a right quartet.



NOTATION:

AES operations:

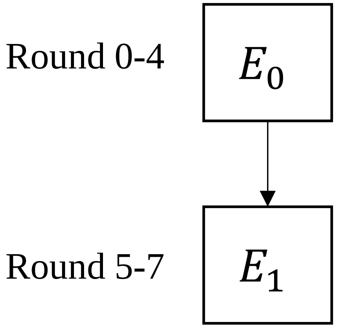
SubBytes (SB)

ShiftRows (SR)

MixColumn (MC)

AddRoundKey (AK)

AES-192 = $E_0 \ o \ E_1$



State Matrix =

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Related-Key Boomerang Attack on 7-Round AES-192

The Structure of the Keys :

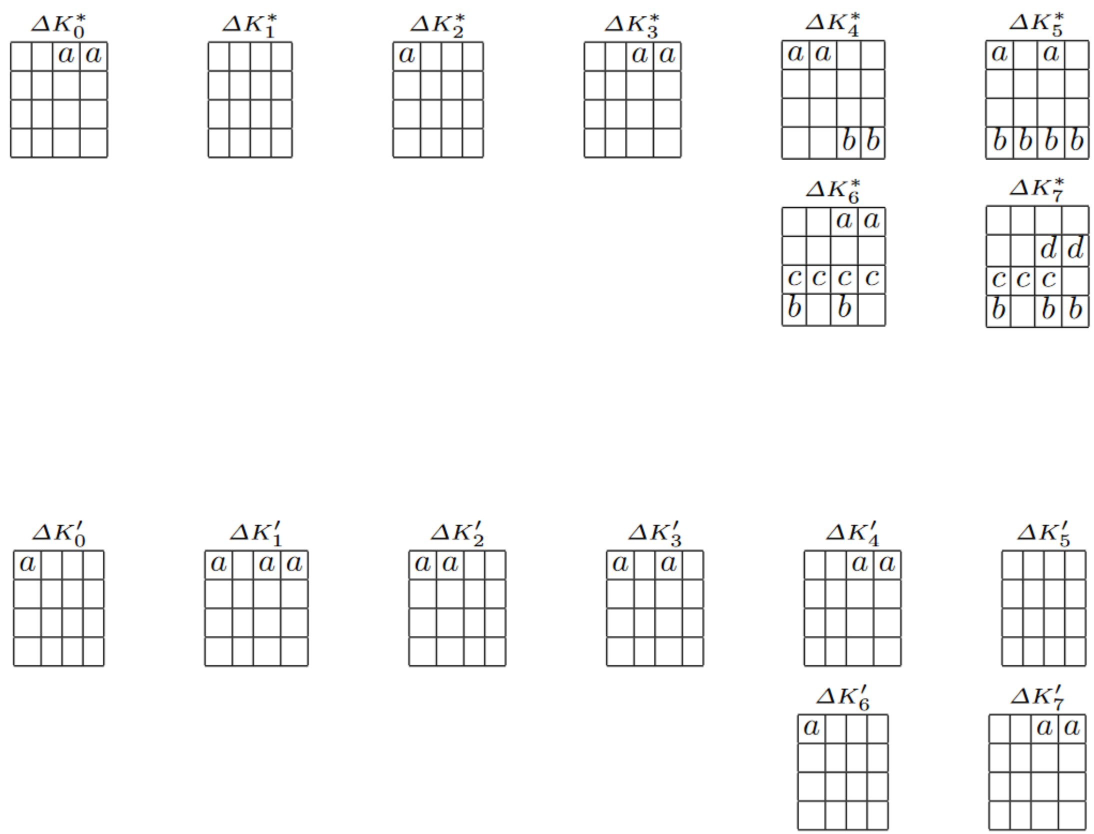
$$K_b = K_a \oplus \Delta K^*$$
$$K_c = K_a \oplus \Delta K'$$
$$K_d = K_a \oplus \Delta K^* \oplus \Delta K'$$

Choose the key differences as

$$\Delta K^* = \begin{array}{|c|c|c|c|c|c|}\hline & & a & a & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline\end{array} \quad \text{and} \quad \Delta K' = \begin{array}{|c|c|c|c|c|c|}\hline a & & & & a & \\ \hline & & & & & \\ \hline & & & & & \\ \hline & & & & & \\ \hline\end{array}$$

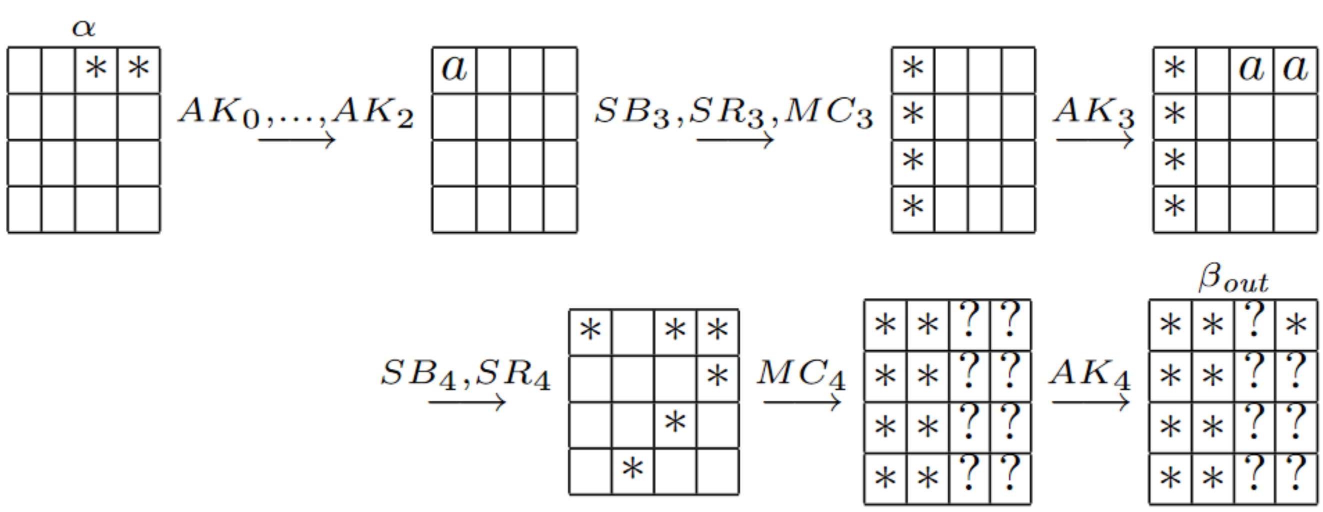
The Structure of the Keys :

Using the key schedule algorithm of AES-192 and key differences ΔK^* and $\Delta K'$, we can derive the round key differences



The Related-Key Differential E_0 for rounds 1 −4:

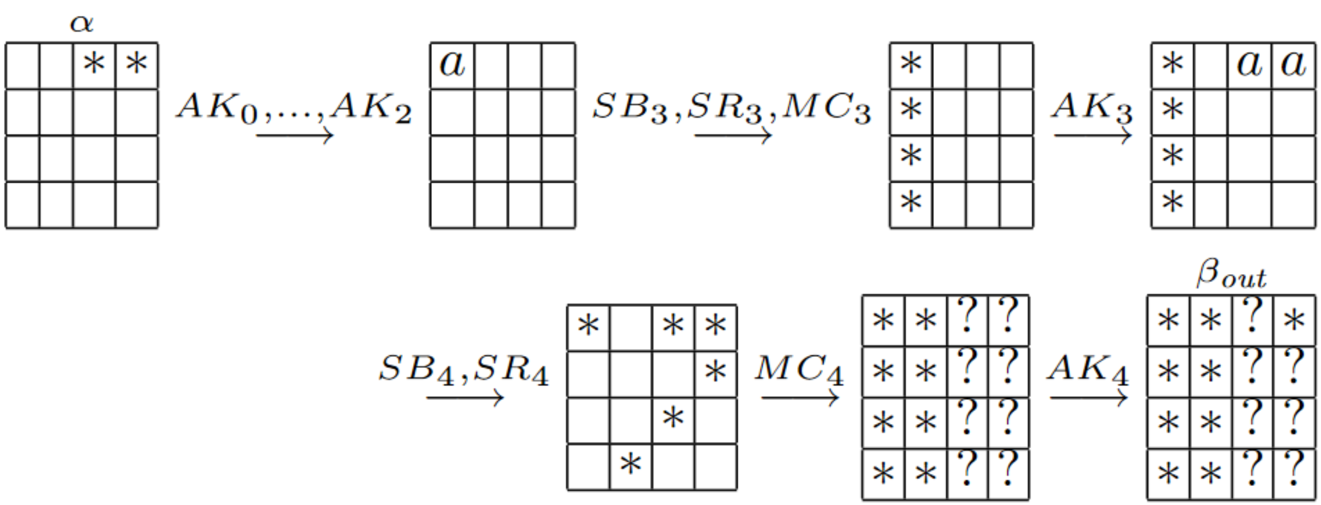
- The input difference α of E_0 has a non-zero difference in bytes 8 and 12.
- These differences are of value a with the probability 2^{-16}.
- This is the probability that two randomly chosen non-zero bytes are of value a.



Related-Key Boomerang Attack on 7-Round AES-192

The Related-Key Differential E_0 for rounds 1 −4:

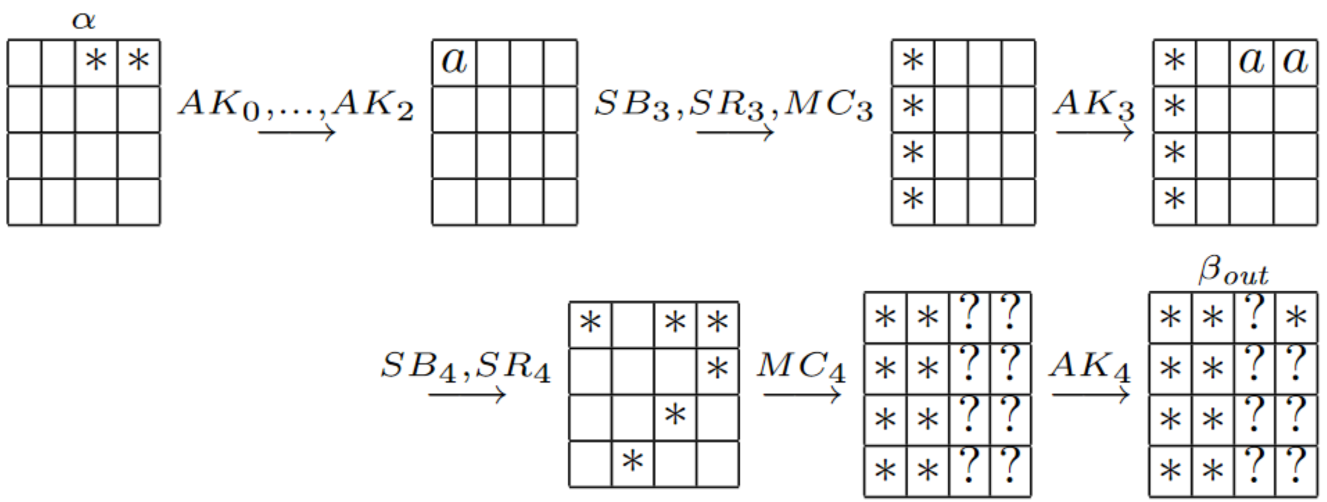
- The whitening key addition AK_0 generates a zero difference in each byte of the state matrix.
- These zero differences remain until AK_2 is applied, since ΔK_1 has only zero differences and does not alter the differences in the state matrix.
- AK_2 generates an a difference in byte 0, which is transformed into a non-zero difference after SB_3.



Related-Key Boomerang Attack on 7-Round AES-192

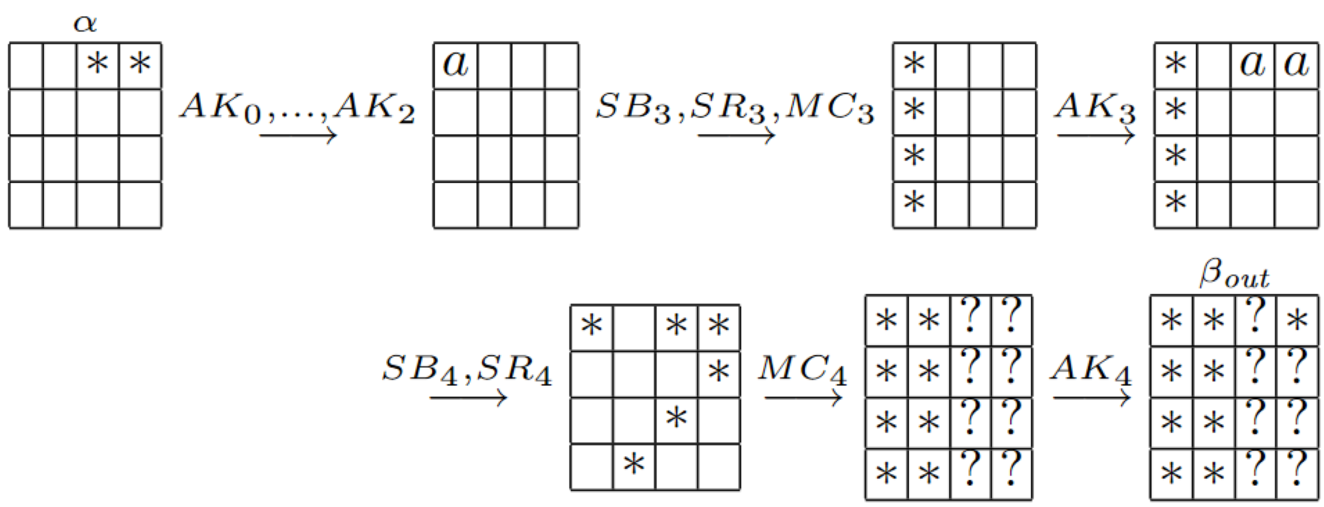
The Related-Key Differential E_0 for rounds 1 −4:

- MC_3 creates a non-zero difference in bytes 0,1,2 and 3, while AK_3 inserts an a difference in bytes 8 and12.
- After applying SR_4 we just have one non-zero byte in column 0 and 1 and two non-zero bytes in column 2 and 3



The Related-Key Differential E_0 for rounds 1 −4:

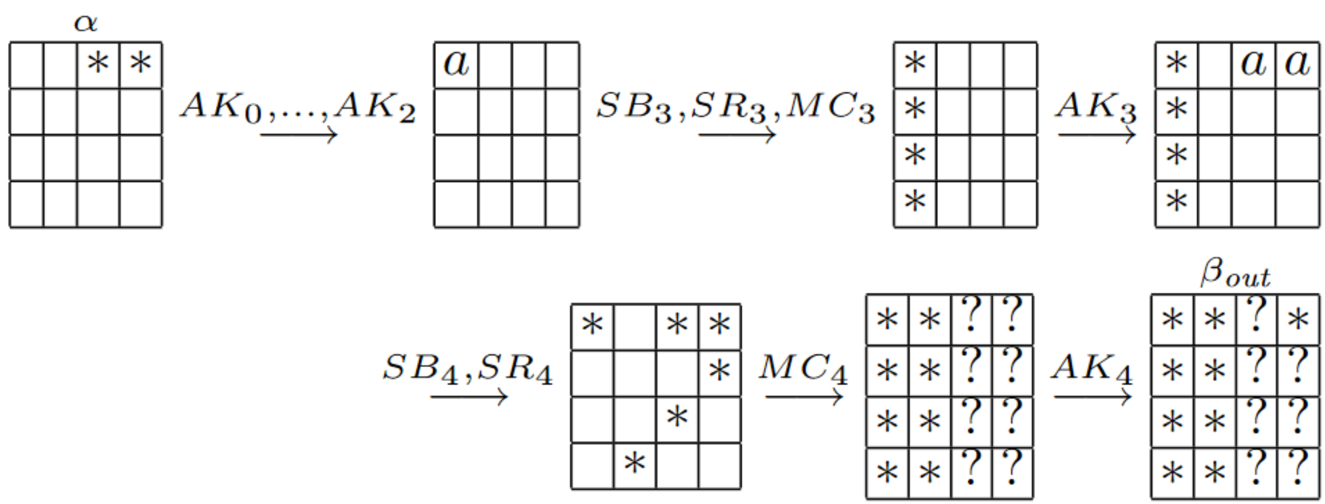
- Four non-zero bytes remain after MC_4 in column 0 and 1 with probability one, while we do not know which bytes of column 2 and 3 are non-zero. These bytes are labeled with ?.
- Then AK_4 places an a difference in byte 12. We call βout the difference obtaining after passing the related-key differential E_0.



The Related-Key Differential E_0 for rounds 1 −4:

So,

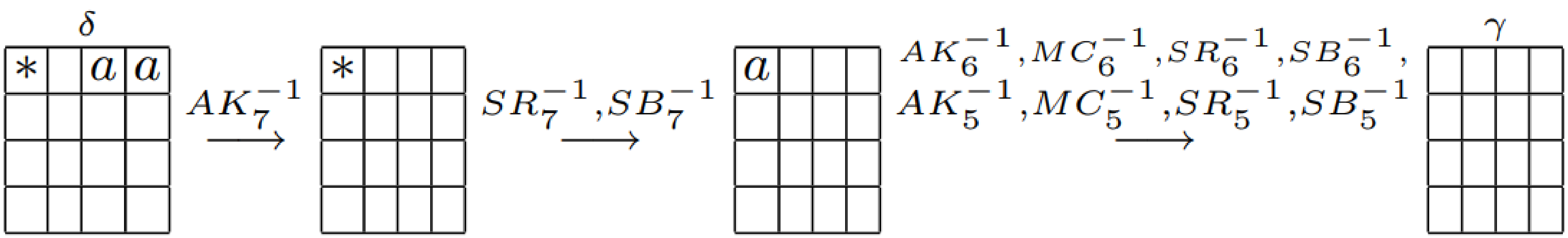
$$\Pr(\alpha \rightarrow \beta_{out}) = 2^{-16}$$



Related-Key Boomerang Attack on 7-Round AES-192

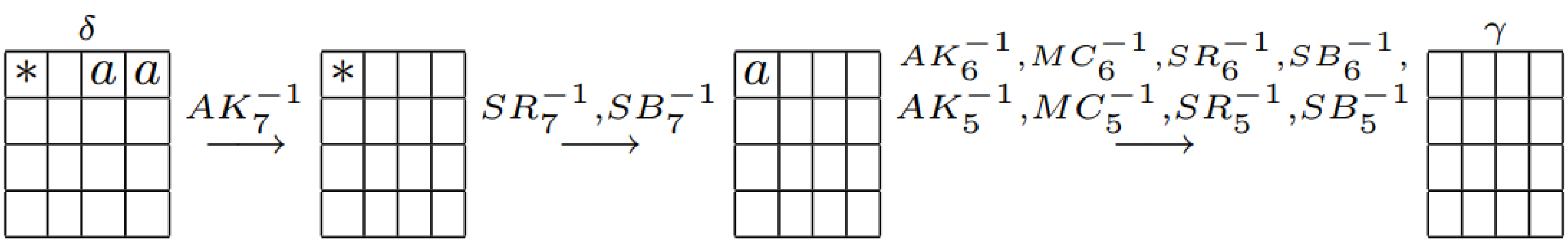
The Related-Key Differential ${E^1}^{-1}$ for rounds 7−5.

- The input difference δ consists of a non-zero difference in byte 0 and two a differences in bytes 8 and 12. This differences vanish after AK_7^{-1} , since $\Delta K_7'$has two a differences in bytes 8 and 12 while the other bytes of $\Delta K_7'$ have a zero difference. Only the nonzero difference in byte 0 remains.
- SB_7^{-1}generates an a difference in byte 0 with probability 2^{-8} since we assume that the S-Box acts like a random permutation



The Related-Key Differential $E^{1^{-1}}$ for rounds 7−5.

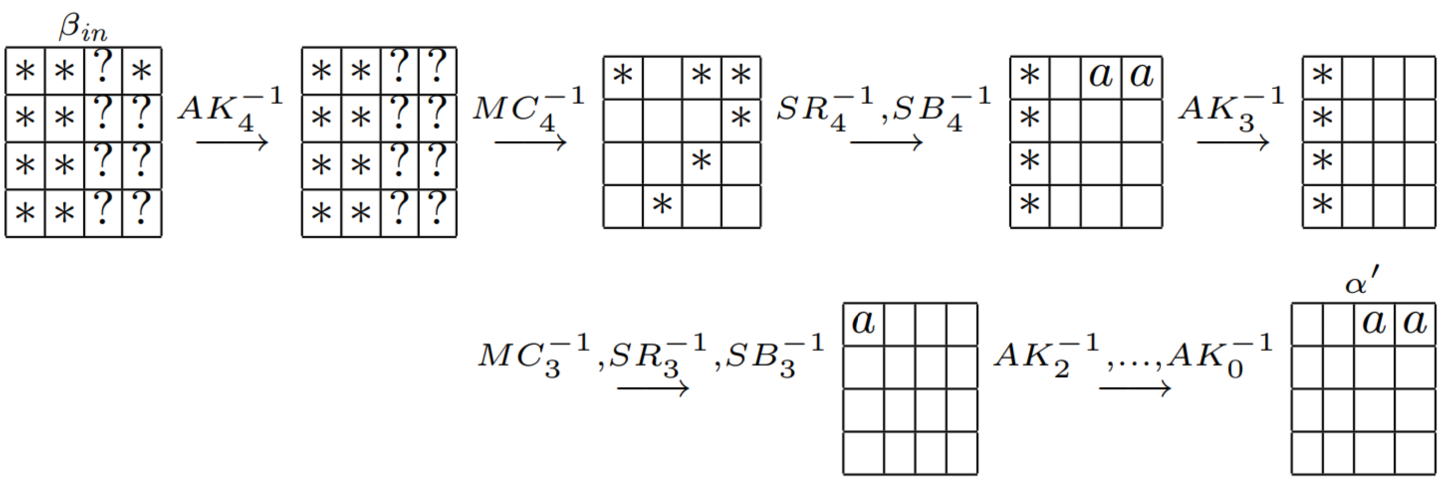
- If this occurs the text difference after SB_7^{-1} is equal to the subkey difference $\Delta K_6'$. Hence, all bytes have a zero difference after applying AK_6^{-1}. All bytes will also have a zero difference after AK_5^{-1}, since $\Delta K_5'$ has a zero difference in each byte.
- We call the text difference after applying $E^{1^{-1}}$ γ which consists of 16 zero bytes.
- The probability of $E^{1^{-1}}$ is Pr (γ ← δ) = 2^{-8}



Related-Key Boomerang Attack on 7-Round AES-192

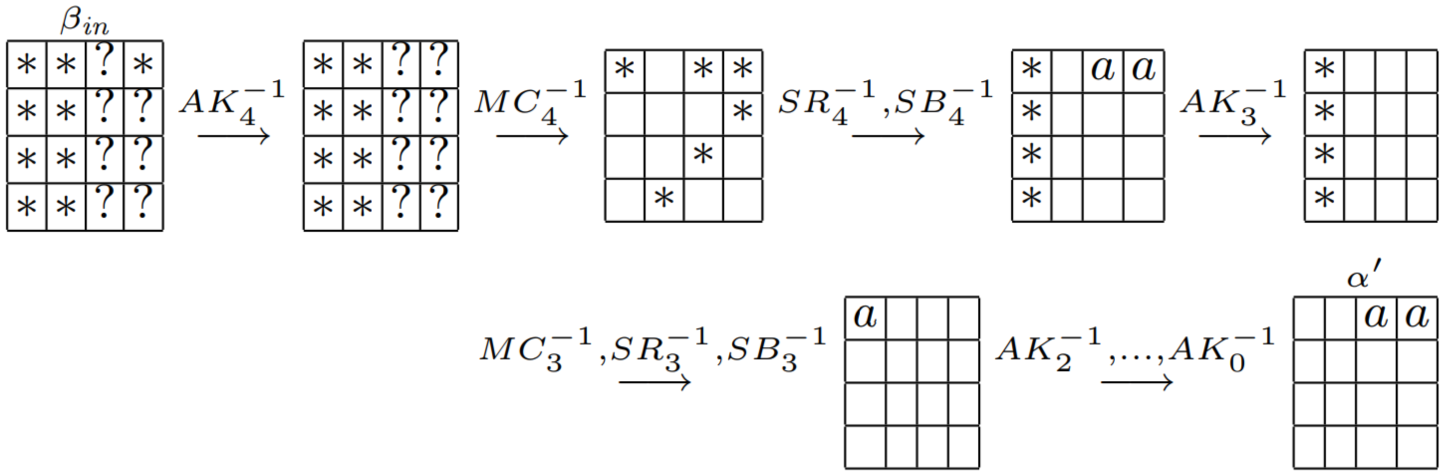
The Related-Key Differential $E^{0^{-1}}$ for rounds 4–1

- MC_4^{-1} can be undone with probability 1 .
- SB_4^{-1} then transforms a non-zero difference into an a difference with probability 2^{-8}. Regarding bytes 8 and 12 we have the probability 2^{-16} of doing so.
- The resulting a differences in bytes 8 and 12 are canceled out by AK_3^{-1}. After that MC_3^{-1}generates a non-zero with a fixed position from four non-zero bytes with probability 2^{-24}



The Related-Key Differential $E^{0^{-1}}$ for rounds 4−1

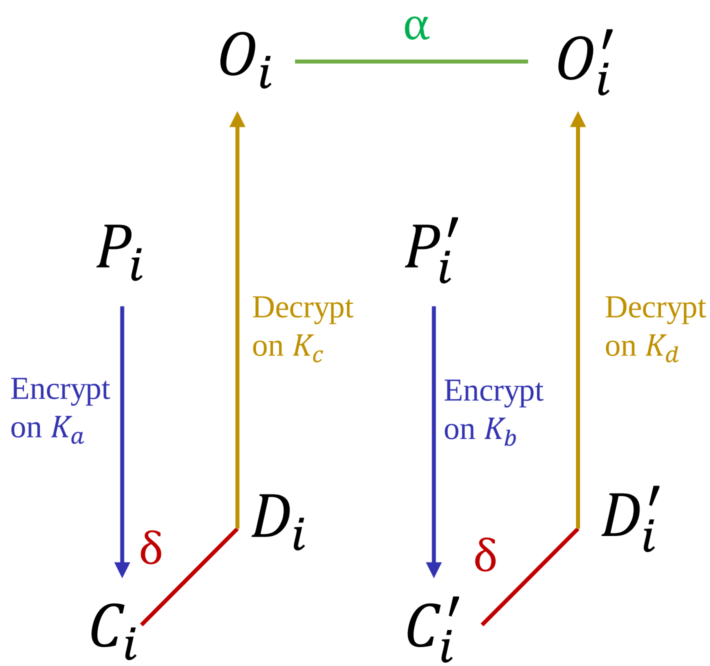
- We have only one a difference after SB_3^{-1} in byte 0 with probability$2^{-24} * 2^{-8} = 2^{32}$.
- This a difference is canceled out by AK_2^{-1}. We call α the difference that is the output of the related-key differential E_0^{-1} α has an a difference in the bytes 8 and 12.
- The differential E_0^{-1} has the probability Pr (α ←β_{in}) = $2^{-16} * 2^{-32} = 2^{-48}$



The Attack :

1. Choose $2^{49.5}$ structures $S_1, S_2, \ldots, S_{2^{49.5}}$ of 2^{16} plaintexts P_i, $i \in \{1, 2, \ldots, 2^{16}\}$, where all bytes are fixed except for bytes 8 and 12. Ask for encryption of P_i under K_a to obtain the ciphertexts C_i, i.e., $C_i = E_{K_a}(P_i)$.
2. Compute $2^{49.5}$ structures $S'_1, S'_2, \ldots, S'_{2^{49.5}}$ of 2^{16} plaintexts $P'_i = P_i$. Ask for encryption of the P'_i under K_b, where $K_b = K_a \oplus \Delta K^*$ to obtain the ciphertexts C'_i, i.e., $C'_i = E_{K_b}(P'_i)$.
3. Compute $2^{49.5}$ structures $S^*_1, S^*_2, \ldots, S^*_{2^{49.5}}$ of 2^{16} ciphertexts D_i, i.e, $D_i = C_i \oplus \delta$ where δ is a fixed difference with any non-zero byte difference in byte 0 and two a differences in bytes 8 and 12. Ask for decryption of D_i under K_c to obtain the plaintexts O_i, i.e., $O_i = E^{-1}_{K_c}(D_i)$.
4. Compute $2^{49.5}$ structures $S'^*_1, S'^*_2, \ldots, S'^*_{2^{49.5}}$ of 2^{16} ciphertexts D'_i, i.e., $D'_i = C'_i \oplus \delta$ where δ is as in Step 3. Ask for decryption of D'_i under K_d to obtain the plaintexts O'_i, i.e., $O'_i = E^{-1}_{K_d}(D'_i)$.
5. Store only those quartets (P_i, P'_j, O_i, O'_j), $i, j \in \{1, 2, \ldots, 2^{16}\}$ in the set M where $O_i \oplus O'_j$ have an a difference in bytes 8 and 12, while the remaining byte differences are zero.

The Attack :



α =

0	0	a	a
0	0	0	0
0	0	0	0
0	0	0	0

The Attack :

6. For each 8-bit key k_{a7} compute $k_{b7} = k_{a7}, k_{c7} = k_{a7}$ and $k_{d7} = k_{a7}$.

   For each quartet passing the test in Step 5:

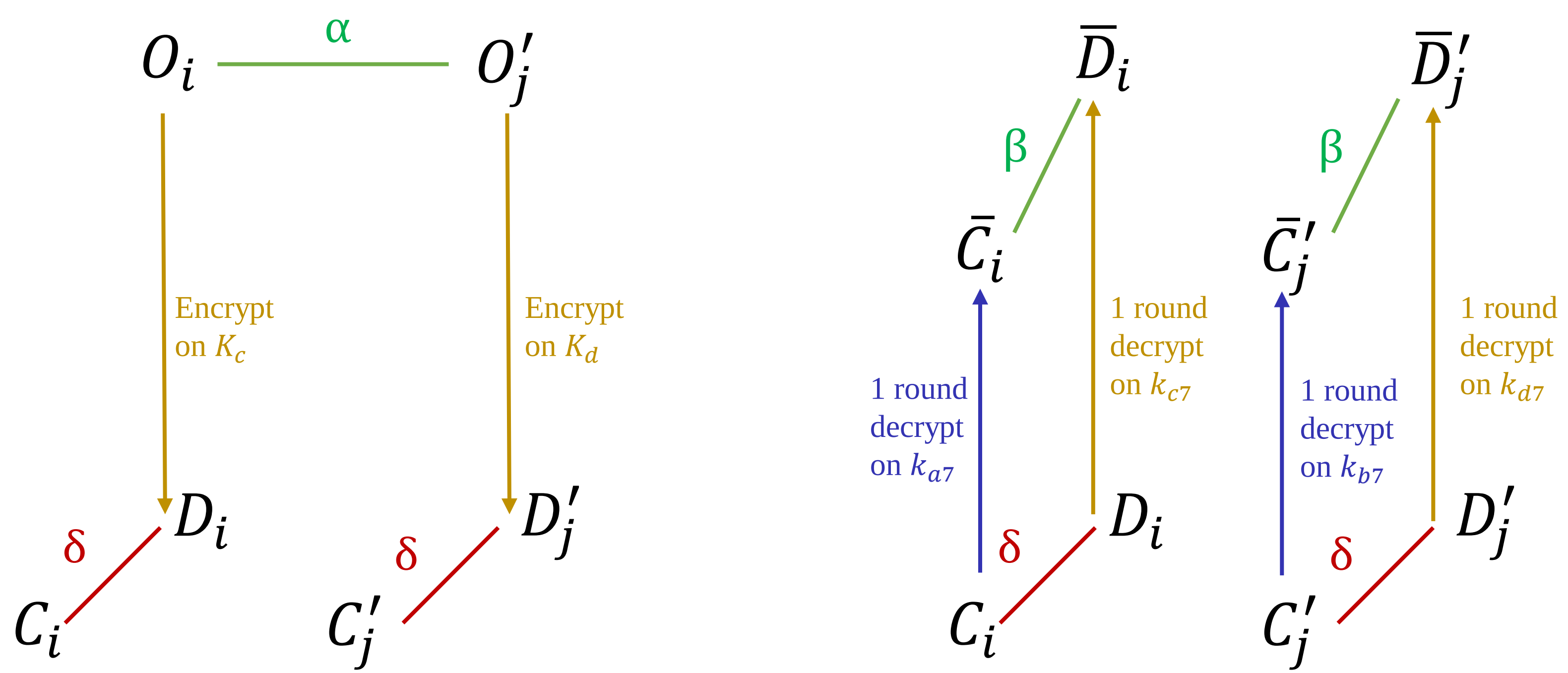
   6.1. Ask for encryption of (O_i, O'_j) under K_c, K_d to obtain (D_i, D'_j) and compute (C_i, C'_j) respectively.

   6.2. Partially decrypt a ciphertext quartet (C_i, C'_j, D_i, D'_j), i.e., $\bar{C}_i = d_{7k_{a7}}(C_i)$, $\bar{C}'_j = d_{7k_{b7}}(C'_j)$, $\bar{D}_i = d_{7k_{c7}}(D_i)$ and $\bar{D}'_j = d_{7k_{d7}}(O'_j)$.

   6.3. Increase the counter for the used 8-bit subkey k_{a7} by one if $\bar{C}_i \oplus \bar{D}_i$ and $\bar{C}'_j \oplus \bar{D}'_j$ have an a-difference in byte 0.

7. Output the 8-bit subkey k_{a7} which counts at least two quartets as the correct one.

The Attack :


O_i
α
O'_j
Encrypt
on K_c
Encrypt
on K_d
D_i
D'_j
δ
δ
C_i
C'_j
$\bar{D}_i$
$\bar{D}'_j$
β
β
$\bar{C}_i$
$\bar{C}'_j$
1 round
decrypt
on k_{c7}
1 round
decrypt
on k_{d7}
1 round
decrypt
on k_{a7}
1 round
decrypt
on k_{b7}
D_i
D'_j
δ
δ
C_i
C'_j

Analysis of the Attack :

We have $2^{49.5} * (2^{16})^2 = 2^{81.5}$ quartets.

Right quartet occurs with probability :

$$\Pr(\alpha \rightarrow \beta_{out}) * (\Pr(\gamma \leftarrow \delta))^2 * \Pr(\alpha \leftarrow \beta_{in}) = 2^{-16} * (2^{-8})^2 * 2^{48} = 2^{80}$$

So we expect,

$$2^{81.5} * 2^{-80} = 2^{1.5} \approx 3 \text{ right quartets.}$$

A random permutation of a difference $O_i \oplus O_j'$ has 14 zero byte difference with probability 2^{-112}

So we expect

$$2^{81.5} * 2^{-112} = 2^{-30.5} \text{ false quartets}$$

Analysis of the Attack :

We have $2^{49.5} * (2^{16})^2 = 2^{81.5}$ quartets.

Right quartet occurs with probability :

$$\Pr(\alpha \rightarrow \beta_{out}) * (\Pr(\gamma \leftarrow \delta))^2 * \Pr(\alpha \leftarrow \beta_{in}) = 2^{-16} * (2^{-8})^2 * 2^{48} = 2^{80}$$

So we expect,

$$2^{81.5} * 2^{-80} = 2^{1.5} \approx 3 \text{ right quartet.}$$

Data complexity : $2^{16} * 2^2 = 2^{18}$

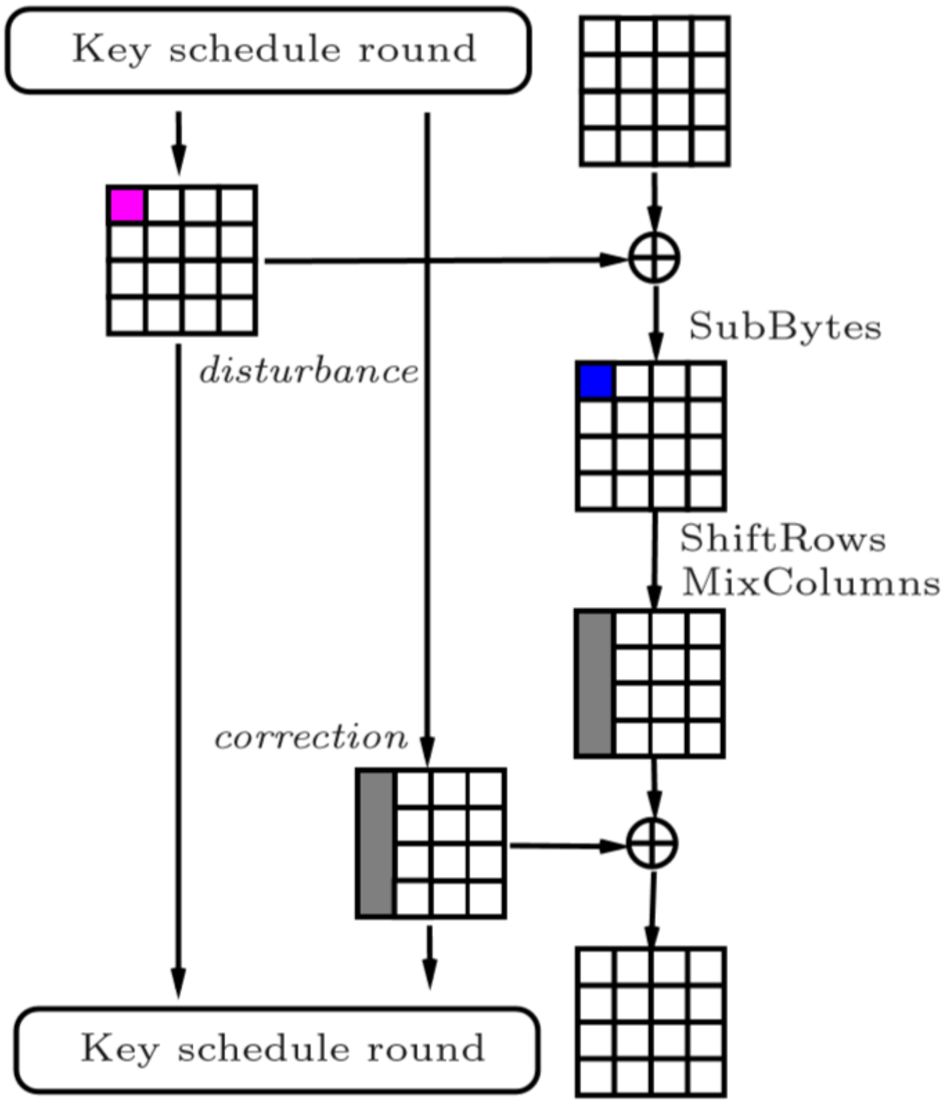
Time complexity : $2^{49.5} * 2^2 * 2^{16} = 2^{67.5}$ (7-Round AES-192 encryption)

Related-Key Boomerang Attack on Full AES-256

Local Collisions:

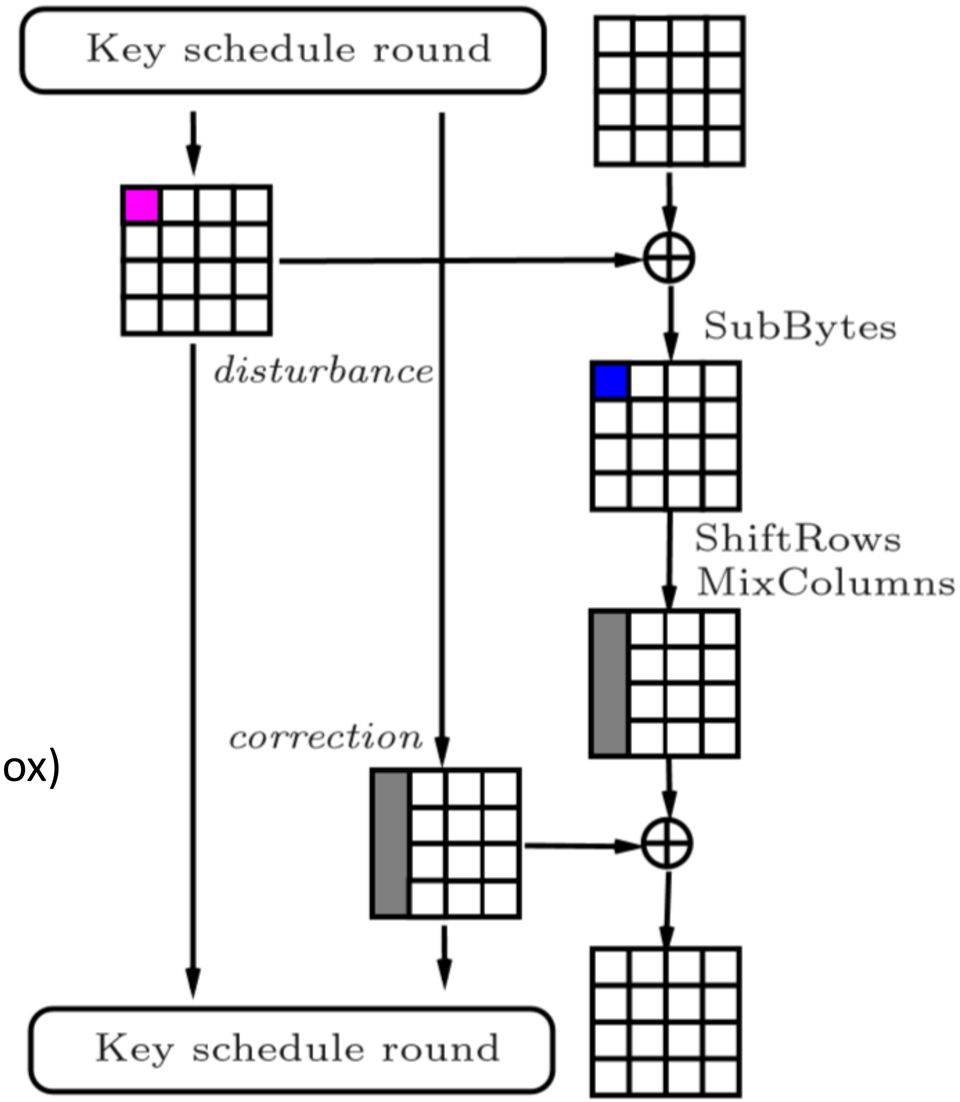
IDEA : Inject a difference into the internal state,causing a disturbance, and then to correct it with the next injections.

GOAL : Have as few disturbances as possible in order to reduce the complexity of the attack.



Related-Key Boomerang Attack on Full AES-256

Attacker cannot control the key itself and thus the attack should work for any key pair with a given difference.



This differential holds with probability 2^{-6}

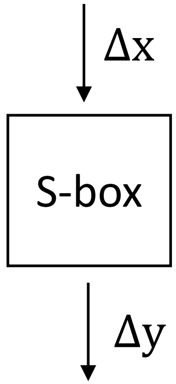
(if we use an optimal differential for an S-box)

Related-Key Boomerang Attack on Full AES-256

$$0\text{x}01 \xrightarrow{\text{SubBytes}} 0\text{x}1\text{f}; \quad \begin{pmatrix} 0\text{x}1\text{f} \\ 0 \\ 0 \\ 0 \end{pmatrix} \xrightarrow{\text{MixColumns}} \begin{pmatrix} 0\text{x}3\text{e} \\ 0\text{x}1\text{f} \\ 0\text{x}1\text{f} \\ 0\text{x}21 \end{pmatrix}$$

$$P = \frac{4}{256} = 2^{-6}$$

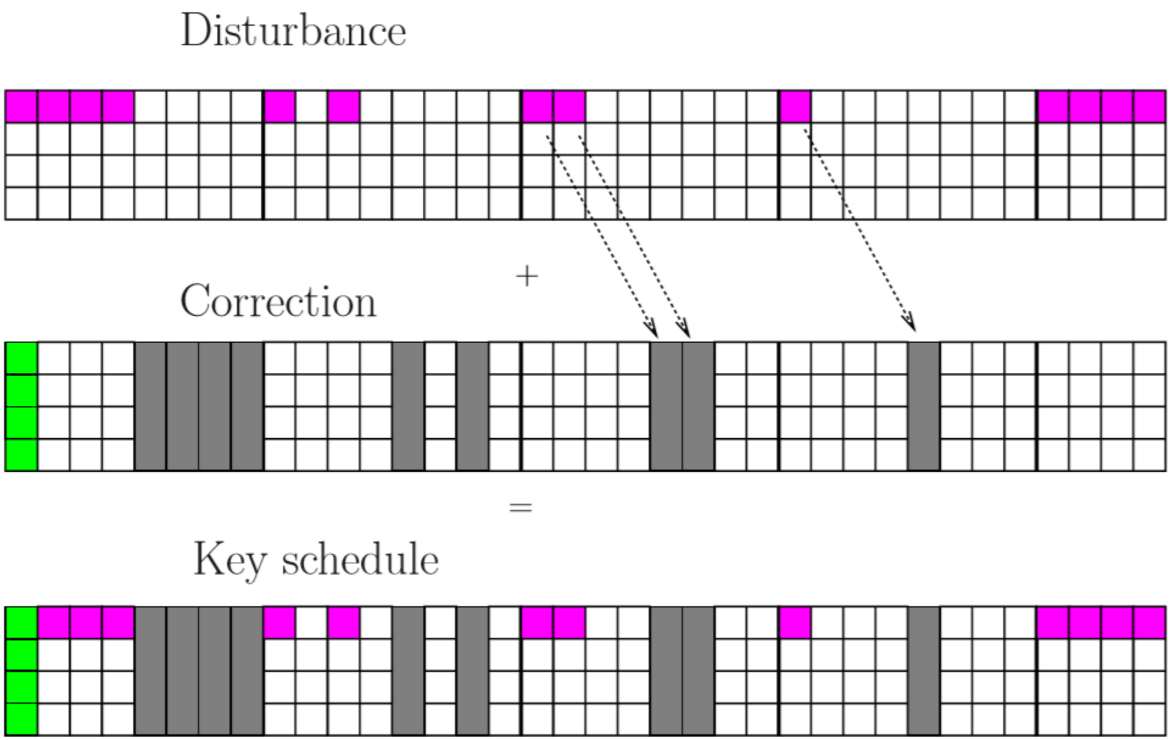
$$P = 1$$



$\Delta x = 0x01$

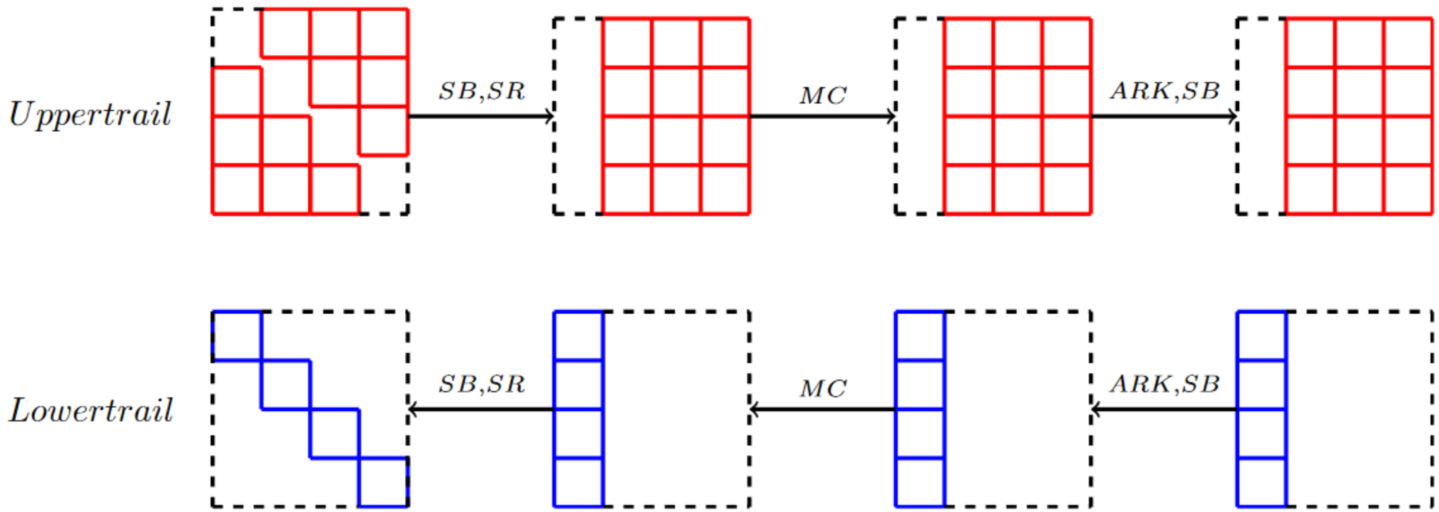
00	02	00	00	02	00	02	00	02	02	02	02	02	02	02	02	$\Delta y = [0x00 - 0x0f]$
00	02	00	00	02	02	00	00	02	02	02	00	00	00	02	$\boxed{04}$	$\Delta y = [0x10 - 0x1f]$
00	02	02	00	02	00	00	00	00	02	02	00	00	02	00	02	$\Delta y = [0x20 - 0x2f]$
02	02	00	00	00	02	02	02	02	02	02	02	00	00	00	02	
00	00	00	02	00	00	00	02	02	00	02	02	02	00	02	02	
00	02	00	02	02	00	00	00	02	02	02	00	00	00	00	00	
00	00	02	02	00	02	00	00	00	02	02	02	02	00	02	00	
00	00	02	00	00	02	00	00	02	02	00	00	00	02	00	00	
02	00	02	02	02	02	00	02	00	02	02	00	00	00	02	00	
00	02	00	02	00	00	00	02	00	02	00	02	00	02	00	02	
00	02	00	02	00	00	02	00	02	02	02	02	02	02	00	00	
02	00	02	00	02	02	02	02	00	00	02	00	02	00	00	00	
00	02	02	02	00	00	00	02	02	00	02	00	02	02	02	02	
02	00	02	02	00	00	00	00	02	00	00	00	02	02	00	00	
02	02	00	00	02	00	00	02	00	00	02	00	00	02	02	02	
00	00	02	00	00	00	02	02	02	00	02	02	00	00	00	02	

Related-Key Boomerang Attack on Full AES-256



Boomerang Switch

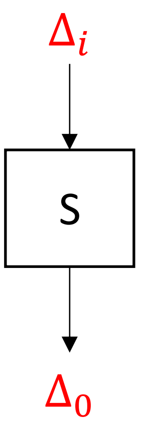
- By default, a cipher is decomposed into rounds.
- However, such decomposition may not be the best for the boomerang attack.
- We propose not only to further decompose the round into simple operations but also to exploit the existing parallelism in these operations. For example, some bytes may be independently processed.



- In such case we can switch in one byte before it is transformed and in another one after it is transformed

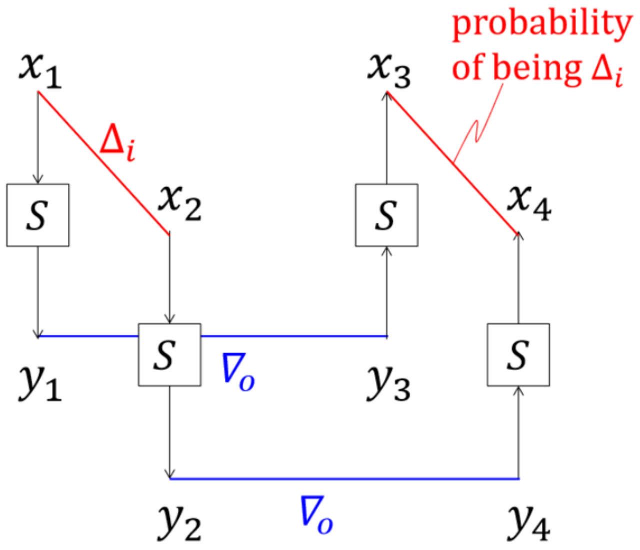
DDT

$$\#\{x \in \{0,1\}^n | S(x) \oplus S(x \oplus \Delta_i) = \Delta_o\}$$

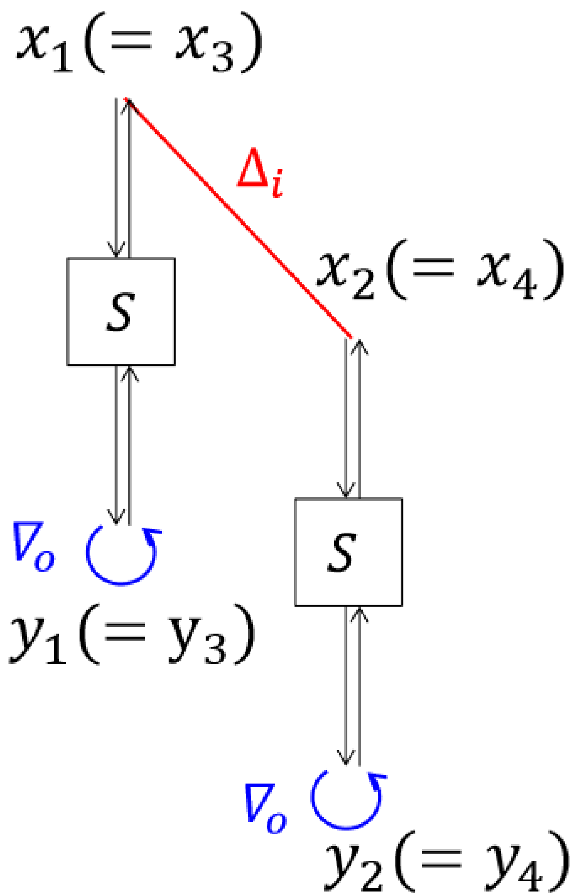


BCT

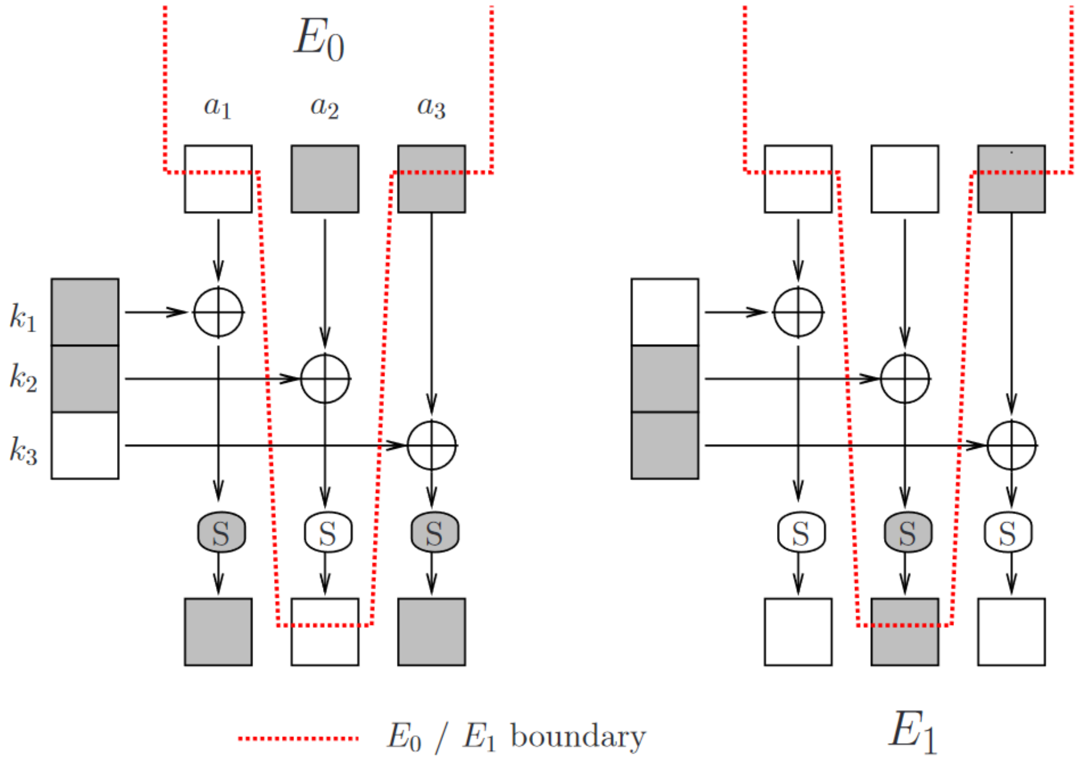
$$\#\{x \in \{0,1\}^n | S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i\}.$$



LADDER SWITCH



Boomerang Switch



Boomerang Switch

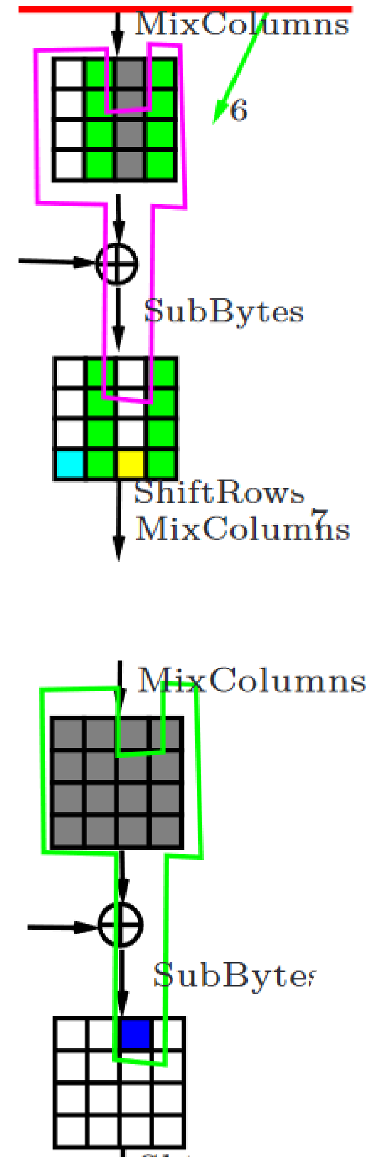
There is one active S-box in round 7 of the lower trail in byte $b^7_{0,2}$

On the other hand, the S-box in the same position is not active in the upper trail.

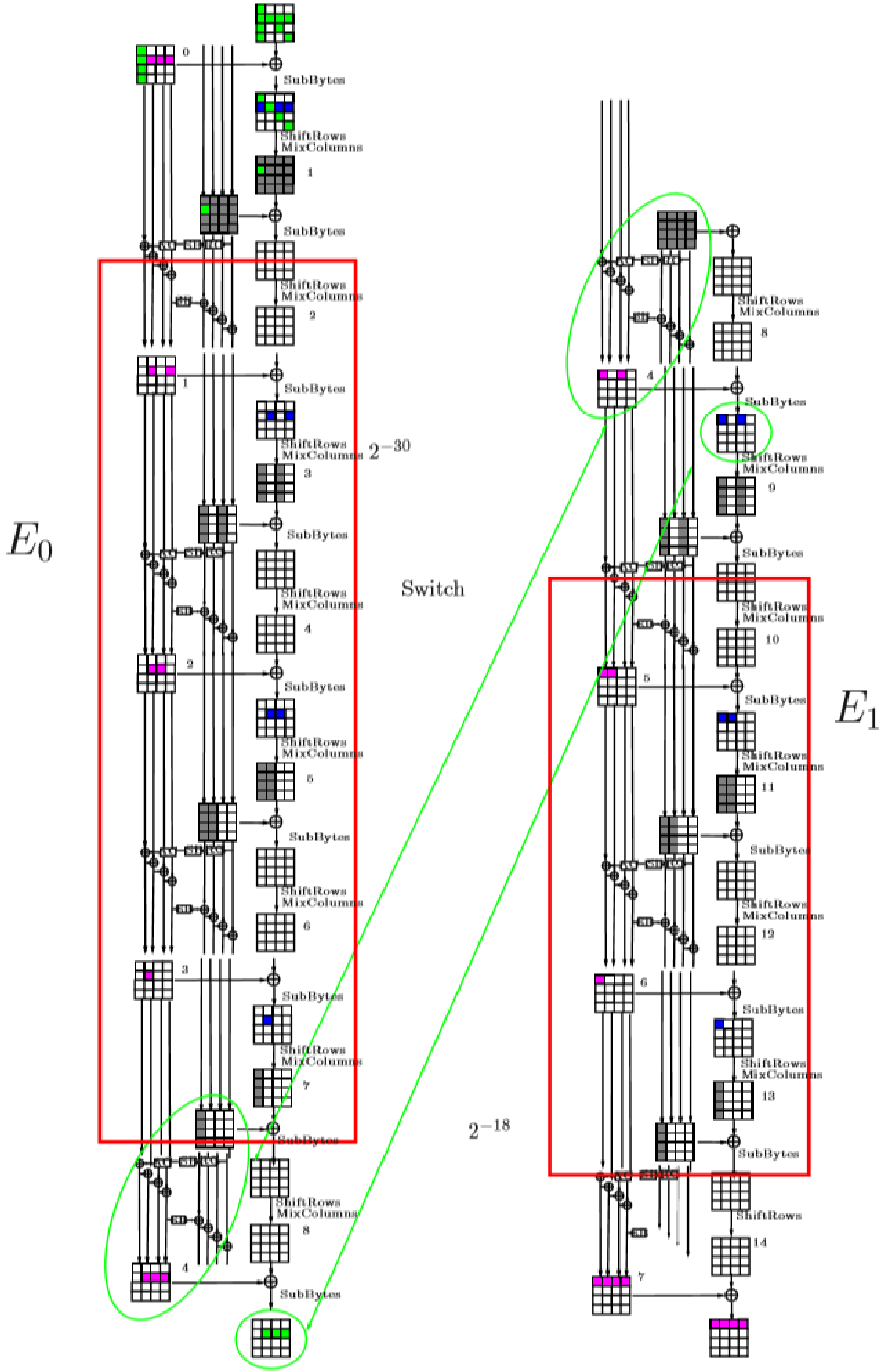
If we would switch after ShiftRows in round 6, we would “pay” the probability in round 7 afterwards.

However, we switch all the state except $b_{0,2}$ after MixColumns, and switch the remaining byte after the S-box application in round 7, where it is not active.

We thus do not pay for this S-box



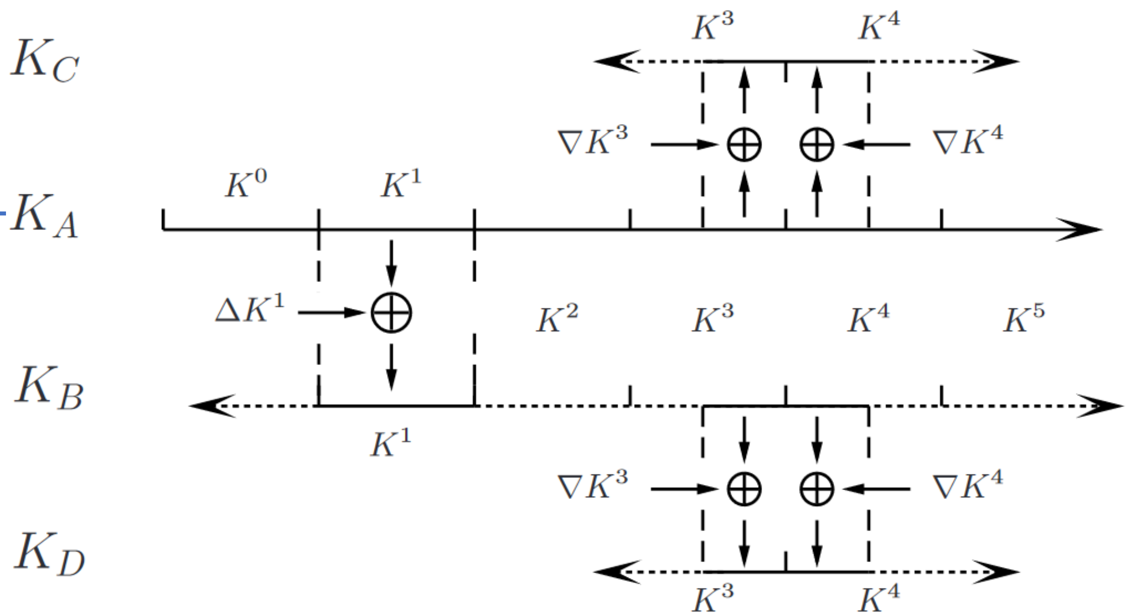
The Trail :



Related Keys :

1	00	00	00	00	3e	00	3e	00
	00	01	00	01	21	00	21	00
	00	00	00	00	1f	00	1f	00
	00	00	00	00	1f	00	1f	00
3	?	01	01	01	3e	3e	3e	3e
	X	00	00	00	1f	1f	1f	1f
	?	00	00	00	1f	1f	1f	1f
	?	00	00	00	21	21	21	21
4	01	00	01	00	3e	00	3e	00
	00	00	00	00	1f	00	1f	00
	00	00	00	00	1f	00	1f	00
	00	00	00	00	21	00	21	00

Master Key



Related-Key Boomerang Attack on Full AES-256

Related Keys :

ΔK^i					
0	? 00 00 00 3e 3e 3e 3e ? 01 01 01 ? 21 21 21 ? 00 00 00 1f 1f 1f 1f ? 00 00 00 1f 1f 1f 1f	1	00 00 00 00 3e 00 3e 00 00 01 00 01 21 00 21 00 00 00 00 00 1f 00 1f 00 00 00 00 00 1f 00 1f 00	2	00 00 00 00 3e 3e 00 00 00 01 01 00 21 21 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 1f 1f 00 00
3	00 00 00 00 3e 00 00 00 00 01 00 00 21 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 1f 00 00 00	4	00 00 00 00 3e 3e 3e 3e 00 01 01 01 ? ? ? ? 00 00 00 00 1f 1f 1f 1f 00 00 00 00 1f 1f 1f 1f		

∇K^i					
0	? ? ? ? ? ? ? 00 X X X X 1f 1f 1f 00 ? ? ? ? 1f 1f 1f 00 ? ? ? ? 21 21 21 00	1	? 01 ? 00 ? ? 00 00 X 00 X 00 1f 1f 00 00 ? 00 ? 00 1f 1f 00 00 ? 00 ? 00 21 21 00 00	2	? ? 00 00 ? 00 00 00 X X 00 00 1f 00 00 00 ? ? 00 00 1f 00 00 00 ? ? 00 00 21 00 00 00
3	? 01 01 01 3e 3e 3e 3e X 00 00 00 1f 1f 1f 1f ? 00 00 00 1f 1f 1f 1f ? 00 00 00 21 21 21 21	4	01 00 01 00 3e 00 3e 00 00 00 00 00 1f 00 1f 00 00 00 00 00 1f 00 1f 00 00 00 00 00 21 00 21 00	5	01 01 00 00 3e 3e 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 21 21 00 00
6	01 00 00 00 3e 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 21 00 00 00	7	01 01 01 01 ? ? ? ? 00 00 00 00 1f 1f 1f 1f 00 00 00 00 1f 1f 1f 1f 00 00 00 00 21 21 21 21		

Related-Key Boomerang Attack on Full AES-256

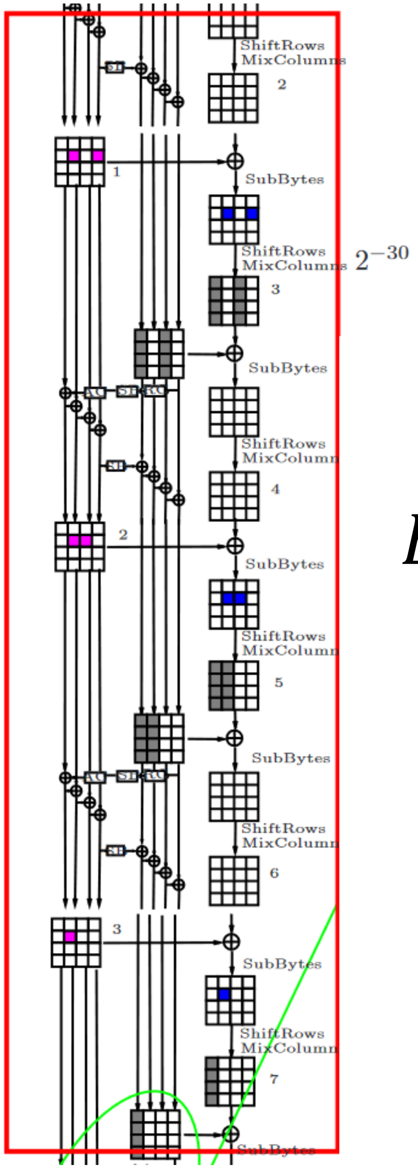
Internal State :

$\Delta P \quad \begin{matrix} ? & 00 & 00 & 00 \\ ? & ? & ? & ? \\ ? & 00 & ? & 00 \\ ? & 00 & 00 & ? \end{matrix}$	$\Delta A^1 \quad \begin{matrix} ? & 00 & 00 & 00 \\ 1f & ? & 1f & 1f \\ 00 & 00 & ? & 00 \\ 00 & 00 & 00 & ? \end{matrix}$	$\Delta A^3 \quad \begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 1f & 00 & 1f \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	$\Delta A^5 \quad \begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 1f & 1f & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$
$\Delta A^7 \quad \begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 1f & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	$\nabla A^7 \quad \begin{matrix} 1f & 1f & 1f & 1f \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	$\nabla A^9 \quad \begin{matrix} 1f & 00 & 1f & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	$\nabla A^{11} \quad \begin{matrix} 1f & 1f & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$
$\nabla A^{13} \quad \begin{matrix} 1f & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	$\Delta C \quad \begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$		

- The plaintext difference is specified in 9 bytes.
- We require that all the active S-boxes in the internal state should output the difference `0x1f` so that the active S-boxes are passed with probability 2^{-6}.
- The only exception is the first round where the input difference in nine active bytes is not specified.

Internal State :

- Let us start a boomerang attack with a random pair of plaintexts that fit the trail after one round.
- Active S-boxes in rounds 3–7 are passed with probability 2^{-6} each.
- The overall probability is $2^{-6^5} = 2^{-30}$

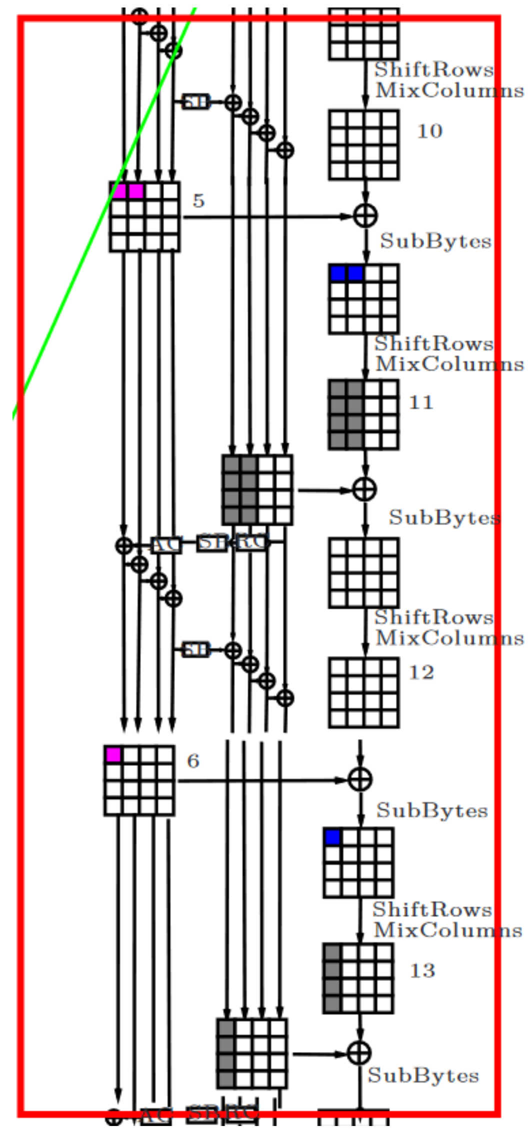


E_0

Internal State :

- Three S-boxes in rounds10–14 contribute to the probability, which is thus equal to 2^{-18}.
- Finally we get one boomerang quartet after the first round with probability

$$2^{-30} * 2^{-30} * 2^{-18} * 2^{-18} = 2^{-96}$$



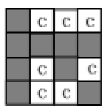
E_1

2^{-18}

Related-Key Boomerang Attack on Full AES-256

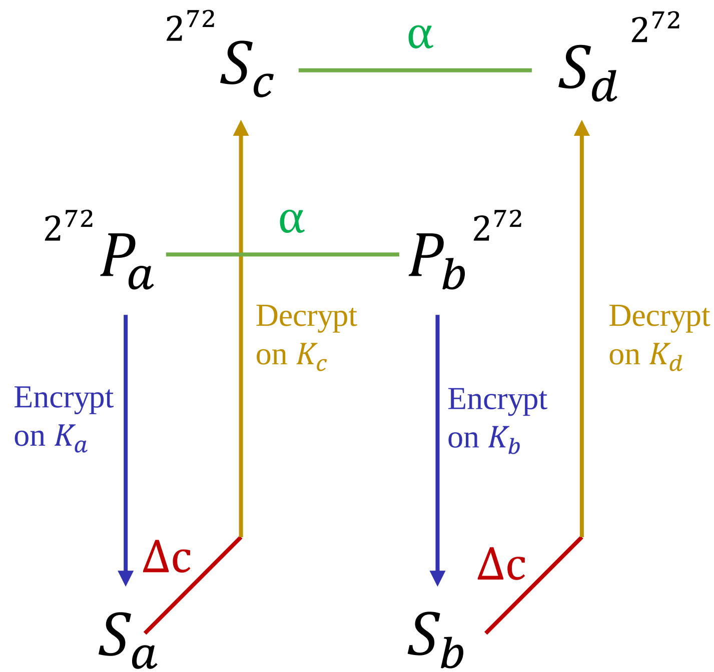
5.2 The Attack

The attack works as follows. Do the following steps $2^{25.5}$ times:

1. Prepare a structure of plaintexts as specified below.
2. Encrypt it on keys K_A and K_B and keep the resulting sets S_A and S_B in memory.
3. XOR Δ_C to all the ciphertexts in S_A and decrypt the resulting ciphertexts with K_C. Denote the new set of plaintexts by S_C.
4. Repeat previous step for the set S_B and the key K_D. Denote the set of plaintexts by S_D.
5. Compose from S_C and S_D all the possible pairs of plaintexts which are equal in 56 bits 

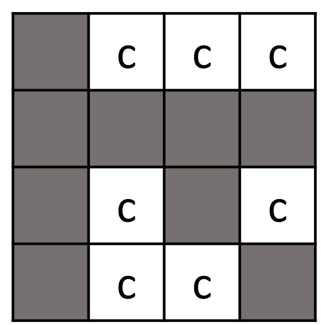
.
6. For every remaining pair check if the difference in $p_{i,0}, i > 1$ is equal on both sides of the boomerang quartet (16-bit filter). Note that $\nabla k^0_{i,7} = 0$ so $\Delta k^0_{i,0}$ should be equal for both key pairs (K_A, K_B) and (K_C, K_D).
7. Filter out the quartets whose difference can not be produced by active S-boxes in the first round (one-bit filter per S-box per key pair) and active S-boxes in the key schedule (one-bit filter per S-box), which is a $2 \cdot 2 + 2 = 6$-bit filter.
8. Gradually recover key values and differences simultaneously filtering out the wrong quartets.

Related-Key Boomerang Attack on Full AES-256



Store quartets (P_a , P_b , S_c , S_d) which satisfies

S_c , S_d =

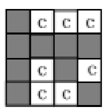


For (56 bits)

Related-Key Boomerang Attack on Full AES-256

5.2 The Attack

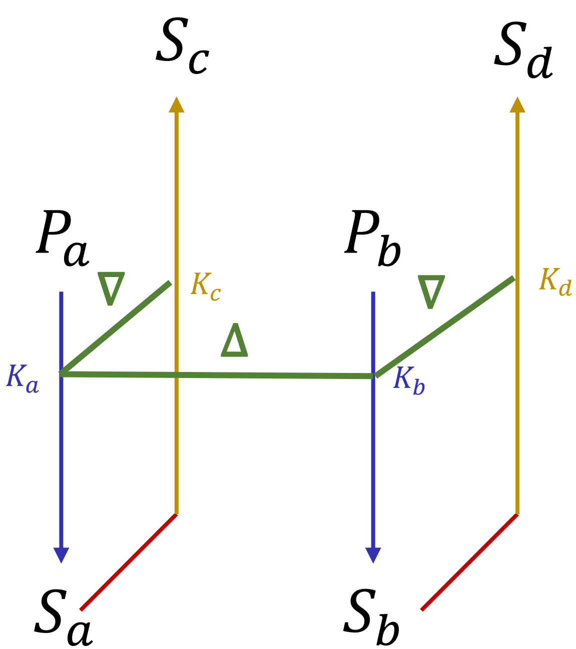
The attack works as follows. Do the following steps $2^{25.5}$ times:

1. Prepare a structure of plaintexts as specified below.
2. Encrypt it on keys K_A and K_B and keep the resulting sets S_A and S_B in memory.
3. XOR Δ_C to all the ciphertexts in S_A and decrypt the resulting ciphertexts with K_C. Denote the new set of plaintexts by S_C.
4. Repeat previous step for the set S_B and the key K_D. Denote the set of plaintexts by S_D.
5. Compose from S_C and S_D all the possible pairs of plaintexts which are equal in 56 bits 

.
6. For every remaining pair check if the difference in $p_{i,0}, i > 1$ is equal on both sides of the boomerang quartet (16-bit filter). Note that $\nabla k^0_{i,7} = 0$ so $\Delta k^0_{i,0}$ should be equal for both key pairs (K_A, K_B) and (K_C, K_D).
7. Filter out the quartets whose difference can not be produced by active S-boxes in the first round (one-bit filter per S-box per key pair) and active S-boxes in the key schedule (one-bit filter per S-box), which is a $2 \cdot 2 + 2 = 6$-bit filter.
8. Gradually recover key values and differences simultaneously filtering out the wrong quartets.

Related-Key Boomerang Attack on Full AES-256

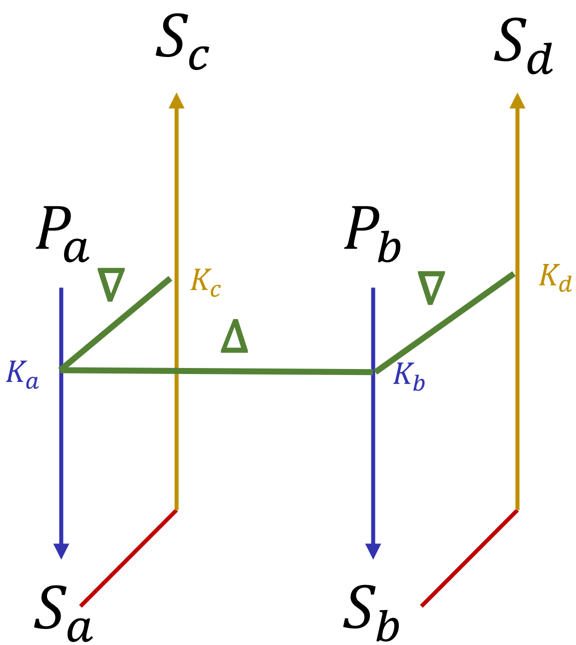
6. For every remaining pair check if the difference in $p_{i,0}$, i > 1 is equal on both sides of the boomerang quartet (16-bit filter). Note that $\nabla k_{i,7}^{0} = 0$ so $\Delta k_{i,0}^{0}$ should be equal for both key pairs (K_A, K_B) and $(K_C\ , K_D)$

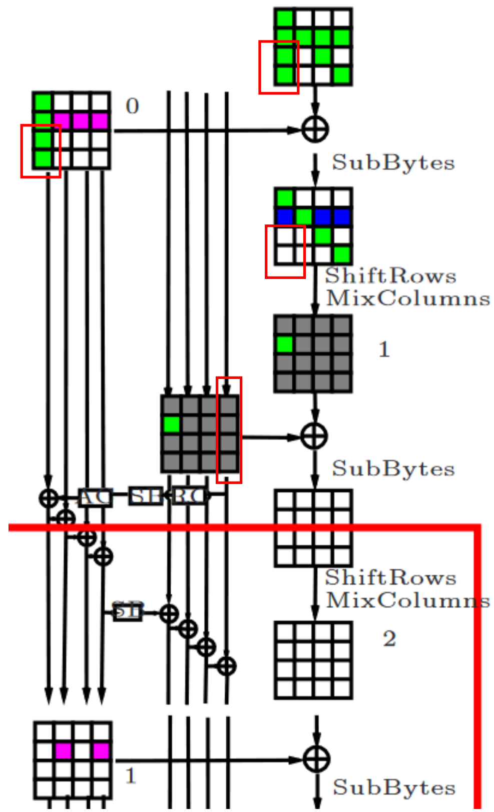


ΔK^i					
0	? 00 00 00 3e 3e 3e 3e ? 01 01 01 ? 21 21 21 ? 00 00 00 1f 1f 1f 1f ? 00 00 00 1f 1f 1f 1f	1	00 00 00 00 3e 00 3e 00 00 01 00 01 21 00 21 00 00 00 00 00 1f 00 1f 00 00 00 00 00 1f 00 1f 00	2	00 00 00 00 3e 3e 00 00 00 01 01 00 21 21 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 1f 1f 00 00
3	00 00 00 00 3e 00 00 00 00 01 00 00 21 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 1f 00 00 00	4	00 00 00 00 3e 3e 3e 3e 00 01 01 01 ? ? ? ? 00 00 00 00 1f 1f 1f 1f 00 00 00 00 1f 1f 1f 1f		

∇K^i					
0	? ? ? ? ? ? ? 00 X X X X 1f 1f 1f 00 ? ? ? ? 1f 1f 1f 00 ? ? ? ? 21 21 21 00	1	? 01 ? 00 ? ? 00 00 X 00 X 00 1f 1f 00 00 ? 00 ? 00 1f 1f 00 00 ? 00 ? 00 21 21 00 00	2	? ? 00 00 ? 00 00 00 X X 00 00 1f 00 00 00 ? ? 00 00 1f 00 00 00 ? ? 00 00 21 00 00 00
3	? 01 01 01 3e 3e 3e 3e X 00 00 00 1f 1f 1f 1f ? 00 00 00 1f 1f 1f 1f ? 00 00 00 21 21 21 21	4	01 00 01 00 3e 00 3e 00 00 00 00 00 1f 00 1f 00 00 00 00 00 1f 00 1f 00 00 00 00 00 21 00 21 00	5	01 01 00 00 3e 3e 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 1f 1f 00 00 00 00 00 00 21 21 00 00
6	01 00 00 00 3e 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 1f 00 00 00 00 00 00 00 21 00 00 00	7	01 01 01 01 ? ? ? ? 00 00 00 00 1f 1f 1f 1f 00 00 00 00 1f 1f 1f 1f 00 00 00 00 21 21 21 21		

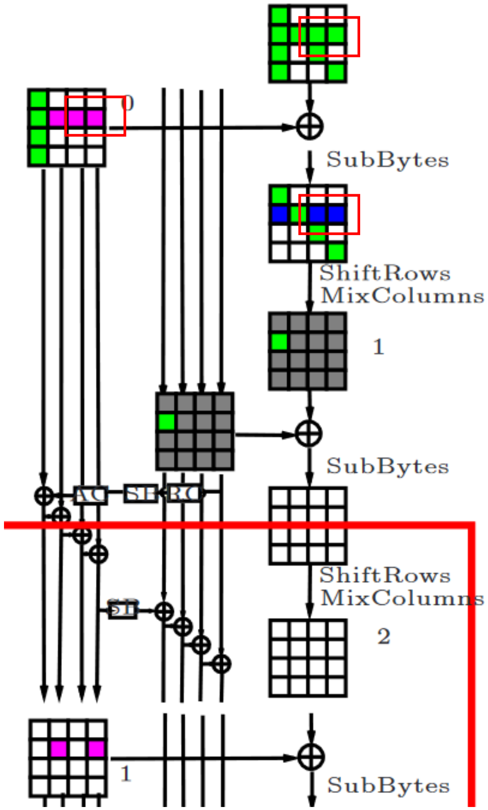
6. For every remaining pair check if the difference in $p_{i,0}$, i > 1 is equal on both sides of the boomerang quartet (16-bit filter). Note that $\nabla k^{0}_{i,7} = 0$ so $\Delta k^{0}_{i,0}$ should be equal for both key pairs (K_A, K_B) and $(K_C\ , K_D)$





7. Filter out the quartets whose difference cannot be produced by active S-boxes in the first round (one-bit filter per S-box per key pair) and active S-boxes in the key schedule (one-bit filter per S-box), which is a $2 * 2 + 2 = 6$-bit filter.

ΔP	$\begin{matrix} ? & 00 & 00 & 00 \\ ? & ? & ? & ? \\ ? & 00 & ? & 00 \\ ? & 00 & 00 & ? \end{matrix}$	ΔA^1	$\begin{matrix} ? & 00 & 00 & 00 \\ 1f & ? & 1f & 1f \\ 00 & 00 & ? & 00 \\ 00 & 00 & 00 & ? \end{matrix}$	ΔA^3	$\begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 1f & 00 & 1f \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	ΔA^5	$\begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 1f & 1f & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$
ΔA^7	$\begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 1f & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	∇A^7	$\begin{matrix} 1f & 1f & 1f & 1f \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	∇A^9	$\begin{matrix} 1f & 00 & 1f & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	∇A^{11}	$\begin{matrix} 1f & 1f & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$
∇A^{13}	$\begin{matrix} 1f & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$	ΔC	$\begin{matrix} 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{matrix}$				



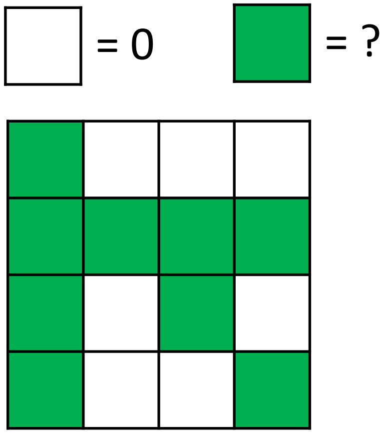
Related-Key Boomerang Attack on Full AES-256

Of 2^{72} texts per structure, we can compose 2^{144} ordered pairs.

We expect one right quartet per $2^{96-72} = 2^{24}$ structures, and three right quartets out of $2^{25.5}$ structures.

Let us now compute the number of noisy quartets.
About $2^{144-56-16} = 2^{72}$ pairs come out of step 6.

The next step applies a 6-bit filter, so we get
$2^{72+25.5-6} = 2^{91.5}$candidate quartets in total.



Key Recovery:

5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

1. First, consider 4-tuples of related key bytes in each position $(1, j), j < 4$. Two differences in a tuple are known by default. The third difference is unknown but is equal for all tuples (see Table 2, where it is denoted by X) and gets one of 2^7 values. We use this fact for key derivation and filtering as follows. Consider key bytes $k^0_{2,2}$ and $k^0_{2,3}$. The candidate quartet proposes 2^2 candidates for both 4-tuples of related-key bytes, or 2^4 candidates in total. Since the differences are related with the X-difference, which is a 9-bit filter, this step reveals two key bytes and the value of X and reduces the number of quartets to $2^{91.5-5} = 2^{86.5}$.
2. Now consider the value of $\Delta k^0_{1,0}$, which is unknown yet and might be different in two pairs of related keys. Let us notice that it is determined by the value of $k^0_{2,7}$, and $\nabla k^0_{2,7} = 0$, so that $\Delta k^0_{1,0}$ is the same for both related key pairs and can take 2^7 values. Each guess of $\Delta k^0_{1,0}$ proposes key candidates for byte $k^0_{2,0}$, where we have a 8-bit filter for the 4-tuple of related-key bytes. We thus derive the value of $k^0_{1,0}$ in all keys and reduce the number of candidate quartets to $2^{85.5}$.
3. The same trick holds for the unknown $\Delta k^0_{1,4}$, which can get 2^7 possible values and can be computed for both key pairs simultaneously. Each of these values proposes four candidates for $k^0_{1,1}$, which are filtered with an 8-bit filter. We thus recover $k^0_{1,1}$ and $\Delta k^0_{1,4}$ and reduce the number of quartets to $2^{79.5}$.
4. Finally, we notice that $\Delta k^0_{1,4}$ is completely determined by $k^0_{1,0}, k^0_{1,1}, k^0_{1,2}, k^0_{1,3}$, and $k^0_{2,7}$. There are at most two candidates for the latter value as well as for $\Delta k^0_{1,4}$, so we get a 6-bit filter and reduce the number of quartets to $2^{72.5}$.
5. Each quartet also proposes two candidates for each of key bytes $k^0_{0,0}$, $k^0_{2,2}$, and $k^0_{3,3}$. Totally, the number of key candidates proposed by each quartet is 2^6.

Related-Key Boomerang Attack on Full AES-256

1. First, consider 4-tuples of related key bytes in each position $(1, j), j < 4$. Two differences in a tuple are known by default. The third difference is unknown but is equal for all tuples (see Table 2, where it is denoted by X) and gets one of 2^7 values. We use this fact for key derivation and filtering as follows. Consider key bytes $k^0_{2,2}$ and $k^0_{2,3}$. The candidate quartet proposes 2^2 candidates for both 4-tuples of related-key bytes, or 2^4 candidates in total. Since the differences are related with the X-difference, which is a 9-bit filter, this step reveals two key bytes and the value of X and reduces the number of quartets to $2^{91.5-5} = 2^{86.5}$.

5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

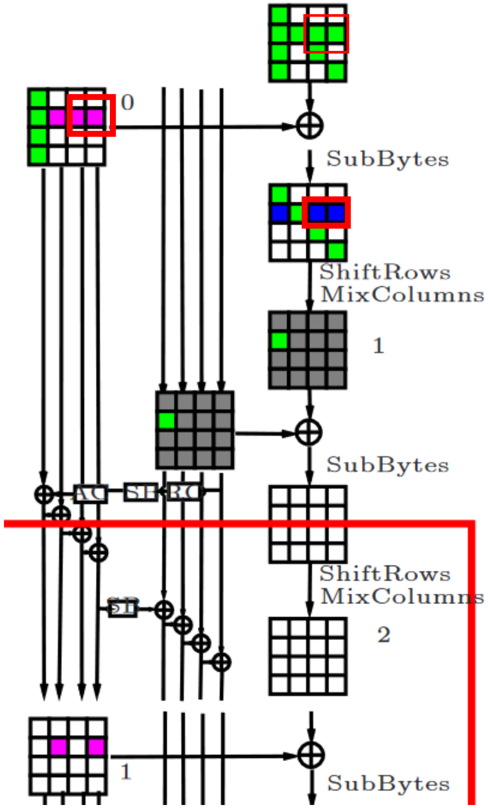
ΔK^i

i								
0	?	00	00	00	3e	3e	3e	3e
	?	01	01	01	?	21	21	21
	?	00	00	00	1f	1f	1f	1f
	?	00	00	00	1f	1f	1f	1f
1	00	00	00	00	3e	00	3e	00
	00	01	00	01	21	00	21	00
	00	00	00	00	1f	00	1f	00
	00	00	00	00	1f	00	1f	00
2	00	00	00	00	3e	3e	00	00
	00	01	01	00	21	21	00	00
	00	00	00	00	1f	1f	00	00
	00	00	00	00	1f	1f	00	00
3	00	00	00	00	3e	00	00	00
	00	01	00	00	21	00	00	00
	00	00	00	00	1f	00	00	00
	00	00	00	00	1f	00	00	00
4	00	00	00	00	3e	3e	3e	3e
	00	01	01	01	?	?	?	?
	00	00	00	00	1f	1f	1f	1f
	00	00	00	00	1f	1f	1f	1f

∇K^i

i								
0	?	?	?	?	?	?	?	00
	X	X	X	X	1f	1f	1f	00
	?	?	?	?	1f	1f	1f	00
	?	?	?	?	21	21	21	00
1	?	01	?	00	?	?	00	00
	X	00	X	00	1f	1f	00	00
	?	00	?	00	1f	1f	00	00
	?	00	?	00	21	21	00	00
2	?	?	00	00	?	00	00	00
	X	X	00	00	1f	00	00	00
	?	?	00	00	1f	00	00	00
	?	?	00	00	21	00	00	00
3	?	01	01	01	3e	3e	3e	3e
	X	00	00	00	1f	1f	1f	1f
	?	00	00	00	1f	1f	1f	1f
	?	00	00	00	21	21	21	21
4	01	00	01	00	3e	00	3e	00
	00	00	00	00	1f	00	1f	00
	00	00	00	00	1f	00	1f	00
	00	00	00	00	21	00	21	00
5	01	01	00	00	3e	3e	00	00
	00	00	00	00	1f	1f	00	00
	00	00	00	00	1f	1f	00	00
	00	00	00	00	21	21	00	00
6	01	00	00	00	3e	00	00	00
	00	00	00	00	1f	00	00	00
	00	00	00	00	1f	00	00	00
	00	00	00	00	21	00	00	00
7	01	01	01	01	?	?	?	?
	00	00	00	00	1f	1f	1f	1f
	00	00	00	00	1f	1f	1f	1f
	00	00	00	00	21	21	21	21

1. First, consider 4-tuples of related key bytes in each position $(1, j), j < 4$. Two differences in a tuple are known by default. The third difference is unknown but is equal for all tuples (see Table 2, where it is denoted by X) and gets one of 2^7 values. We use this fact for key derivation and filtering as follows. Consider key bytes $k^0_{2,2}$ and $k^0_{2,3}$. The candidate quartet proposes 2^2 candidates for both 4-tuples of related-key bytes, or 2^4 candidates in total. Since the differences are related with the X-difference, which is a 9-bit filter, this step reveals two key bytes and the value of X and reduces the number of quartets to $2^{91.5-5} = 2^{86.5}$.



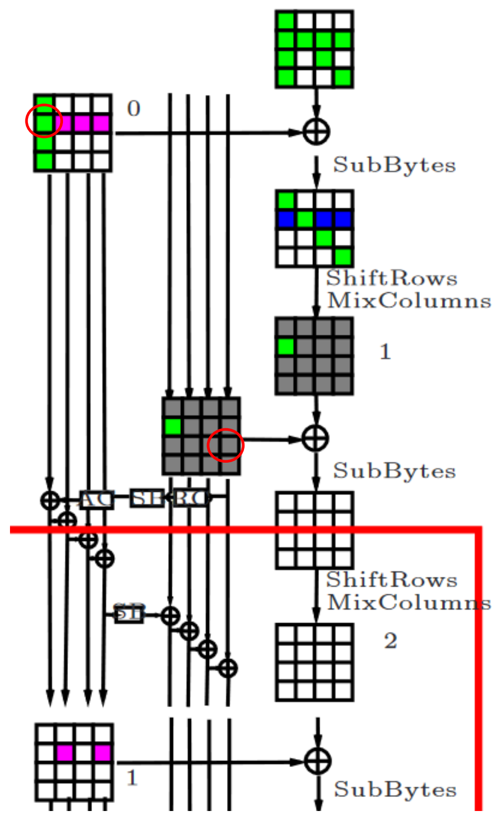
Related-Key Boomerang Attack on Full AES-256

2. Now consider the value of $\Delta k^0_{1,0}$, which is unknown yet and might be different in two pairs of related keys. Let us notice that it is determined by the value of $k^0_{2,7}$, and $\nabla k^0_{2,7} = 0$, so that $\Delta k^0_{1,0}$ is the same for both related key pairs and can take 2^7 values. Each guess of $\Delta k^0_{1,0}$ proposes key candidates for byte $k^0_{2,0}$, where we have a 8-bit filter for the 4-tuple of related-key bytes. We thus derive the value of $k^0_{1,0}$ in all keys and reduce the number of candidate quartets to $2^{85.5}$.

5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

<table>
<tr><th colspan="6">ΔK^i</th></tr>
<tr><td>0</td><td>? 00 00 00 3e 3e 3e 3e
? 01 01 01 ? 21 21 21
? 00 00 00 1f 1f 1f 1f
? 00 00 00 1f 1f 1f 1f</td><td>1</td><td>00 00 00 00 3e 00 3e 00
00 01 00 01 21 00 21 00
00 00 00 00 1f 00 1f 00
00 00 00 00 1f 00 1f 00</td><td>2</td><td>00 00 00 00 3e 3e 00 00
00 01 01 00 21 21 00 00
00 00 00 00 1f 1f 00 00
00 00 00 00 1f 1f 00 00</td></tr>
<tr><td>3</td><td>00 00 00 00 3e 00 00 00
00 01 00 00 21 00 00 00
00 00 00 00 1f 00 00 00
00 00 00 00 1f 00 00 00</td><td>4</td><td>00 00 00 00 3e 3e 3e 3e
00 01 01 01 ? ? ? ?
00 00 00 00 1f 1f 1f 1f
00 00 00 00 1f 1f 1f 1f</td><td></td><td></td></tr>
<tr><th colspan="6">∇K^i</th></tr>
<tr><td>0</td><td>? ? ? ? ? ? ? 00
X X X X 1f 1f 1f 00
? ? ? ? 1f 1f 1f 00
? ? ? ? 21 21 21 00</td><td>1</td><td>? 01 ? 00 ? ? 00 00
X 00 X 00 1f 1f 00 00
? 00 ? 00 1f 1f 00 00
? 00 ? 00 21 21 00 00</td><td>2</td><td>? ? 00 00 ? 00 00 00
X X 00 00 1f 00 00 00
? ? 00 00 1f 00 00 00
? ? 00 00 21 00 00 00</td></tr>
<tr><td>3</td><td>? 01 01 01 3e 3e 3e 3e
X 00 00 00 1f 1f 1f 1f
? 00 00 00 1f 1f 1f 1f
? 00 00 00 21 21 21 21</td><td>4</td><td>01 00 01 00 3e 00 3e 00
00 00 00 00 1f 00 1f 00
00 00 00 00 1f 00 1f 00
00 00 00 00 21 00 21 00</td><td>5</td><td>01 01 00 00 3e 3e 00 00
00 00 00 00 1f 1f 00 00
00 00 00 00 1f 1f 00 00
00 00 00 00 21 21 00 00</td></tr>
<tr><td>6</td><td>01 00 00 00 3e 00 00 00
00 00 00 00 1f 00 00 00
00 00 00 00 1f 00 00 00
00 00 00 00 21 00 00 00</td><td>7</td><td>01 01 01 01 ? ? ? ?
00 00 00 00 1f 1f 1f 1f
00 00 00 00 1f 1f 1f 1f
00 00 00 00 21 21 21 21</td><td></td><td></td></tr>
</table>

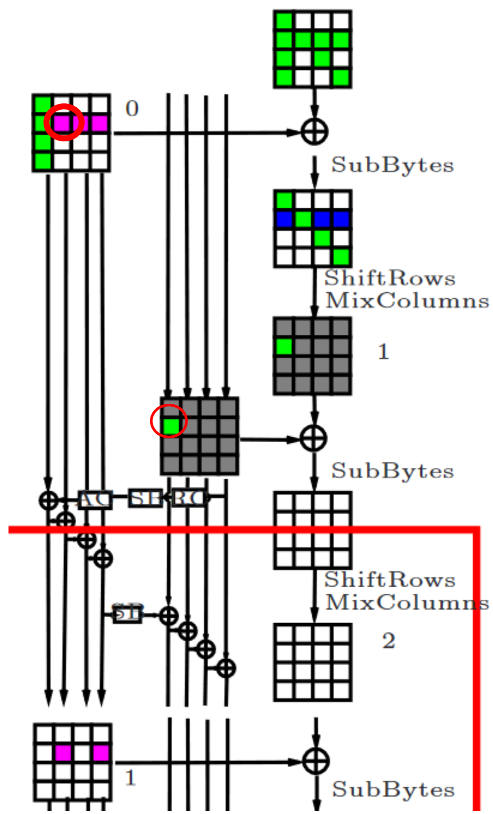
2. Now consider the value of $\Delta k^0_{1,0}$, which is unknown yet and might be different in two pairs of related keys. Let us notice that it is determined by the value of $k^0_{2,7}$, and $\nabla k^0_{2,7} = 0$, so that $\Delta k^0_{1,0}$ is the same for both related key pairs and can take 2^7 values. Each guess of $\Delta k^0_{1,0}$ proposes key candidates for byte $k^0_{2,0}$, where we have a 8-bit filter for the 4-tuple of related-key bytes. We thus derive the value of $k^0_{1,0}$ in all keys and reduce the number of candidate quartets to $2^{85.5}$.



5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

Related-Key Boomerang Attack on Full AES-256

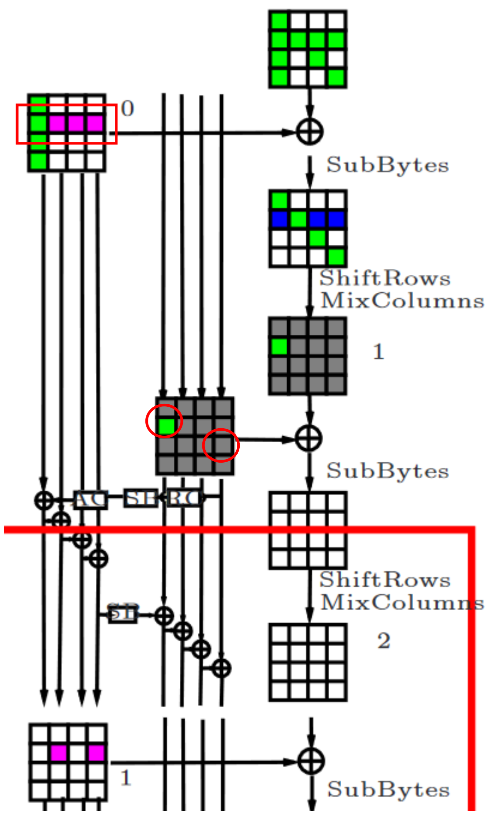
3. The same trick holds for the unknown $\Delta k^0_{1,4}$, which can get 2^7 possible values and can be computed for both key pairs simultaneously. Each of these values proposes four candidates for $k^0_{1,1}$, which are filtered with an 8-bit filter. We thus recover $k^0_{1,1}$ and $\Delta k^0_{1,4}$ and reduce the number of quartets to $2^{79.5}$.



5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

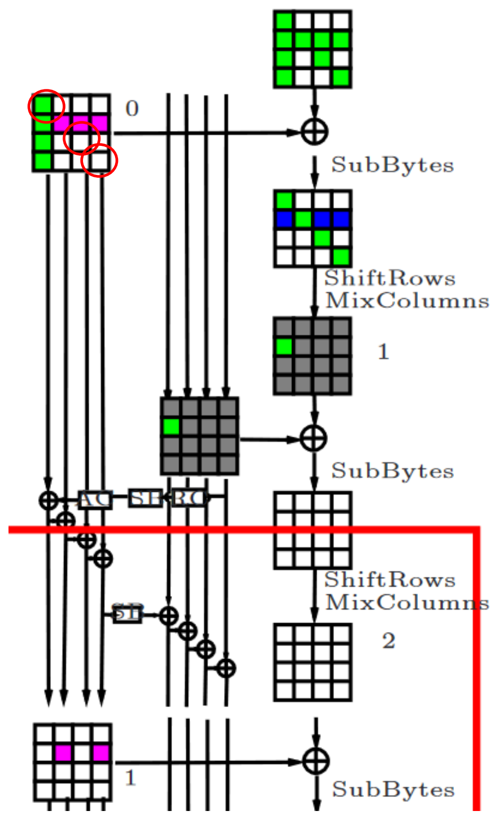
Related-Key Boomerang Attack on Full AES-256

4. Finally, we notice that $\Delta k^0_{1,4}$ is completely determined by $k^0_{1,0}, k^0_{1,1}, k^0_{1,2}, k^0_{1,3}$, and $k^0_{2,7}$. There are at most two candidates for the latter value as well as for $\Delta k^0_{1,4}$, so we get a 6-bit filter and reduce the number of quartets to $2^{72.5}$.



5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

5. Each quartet also proposes two candidates for each of key bytes $k^0_{0,0}$, $k^0_{2,2}$, and $k^0_{3,3}$. Totally, the number of key candidates proposed by each quartet is 2^6.



5							0
2	3	1	1	3D 4			
0D		5					0 4
0D			5				0

Related-Key Boomerang Attack on Full AES-256

We recover $3 * 7 + 8 * 8 = 85$ bits of K_A

With $2^{72} * 2^{25.5} * 4 = 2^{99.5}$ data and time and $2^{77.5}$ memory.

References

1. Michael Gorski, Stefan Lucks, New Related-Key Boomerang Attacks on AES, proceedings of INDOCRYPT 2008, Lecture Notes in Computer Science 5365, pp. 266–278, Springer-Verlag, 2008

2. Alex Biryukov, Dmitry Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, IACR ePrint report 2009/317, 2009. Available online at http://eprint.iacr.org/2009/317