Improved Related-Key Boomerang Cryptanalysis of AES-256

Hadi Soleimany, Alireza Sharifi, Mohammadreza Aref
Information Systems and Security Lab (ISSL)
EE Department, Sharif University of Technology, Tehran, Iran
E-mail: hadi.soleimany@gmail.com, asharifi@alum.sharif.edu, aref@sharif.edu

***Abstract*— A specific class of differential cryptanalytic approach, known as Related Key Boomerang Attack, has been successfully applied to several symmetric cryptographic primitives in particular encryption schemes such as Advanced Encryption Standard (AES). In this paper, we propose a new related-key boomerang attack on 8-round AES-256, a couple of ones on 9-round following the work of Gorski et al. In the first one, we attacked 8-round AES-256 with the time complexity of 2^{79} and the data complexity of 2^{59}. The extended 8-round attack on 9-round AES-256 is more efficient than previous attacks from both time and data complexity perspectives.**

Keywords- Related-Key Boomerang Attack, Advanced Encryption Standard

I. INTRODUCTION

Rijndael is an iterated block cipher with variable key and block lengths of 128 to 256 bits in steps of 32 bits. Rijndael versions with a block length of 128 bits, and key lengths of 128,192 and 256 bits have been adopted as the Advanced Encryption Standard (AES) [3]. Because of the worldwide use of AES, it is essential to reevaluate the security of AES under various cryptanalytic techniques. In this paper, we study the security of 256-bit key version of AES against the related-key boomerang attack. Differential cryptanalysis [4] analyzes the evolvement of the difference between a pair of plaintexts in the following round outputs (differentials) in an iterated block cipher. After Differential Cryptanalysis was introduced, various variants of this attack have been proposed such as the truncated differential attack [5], the higher order differential attack [5], the differential-linear attack [6], the boomerang attack [7], the rectangle attack [8] and the impossible differential attack [9].

The boomerang attack [7] is a strong extension of differential cryptanalysis to break more rounds than differential attacks can do, since the cipher is treated as a cascade of two sub-ciphers, using short differentials in each sub-cipher. These differentials are combined in an adaptive chosen plaintext and ciphertext attack to exploit properties of the cipher that have a high probability.

Related-key attacks [10, 11], concentrate on the information which can be obtained from two encryptions using related (but unknown) keys. These kind of attacks use the key schedule algorithm and the encryption algorithm weaknesses to find the values of the keys. Several cryptanalytic results of this attack were reported in [12-14].

Biryukov [15] propose a boomerang attack on the AES-128 which can break up to 5 and 6 out of 10 rounds. The related-key boomerang attack was published first in [16], but was not used to attack the AES. Gorski and Lucks present the first related-key boomerang attack on 7 rounds of AES-192 using 4 related keys and 9 rounds of AES-192 using 64 related keys [1]. After that Fleischmann et al. [2] use related key boomerang cryptanalysis to attack on 9 round AES-256. Following these works, we present three attacks on 8 and 9 round AES-256 with lower complexity and related keys. Table 1 summarizes existing attacks on AES-256 and our new attacks.

TABLE I. A SUMMARY OF THE PREVIOUS ATTACKS ON REDUCED AES-256 AND OUR NEW ATTACKS

Keys	Rounds	Data	Workload	Type	Reference
8	1	$2^{128}-2^{119}$	2^{204}	Partial Sum	[17]
8	1	2^{32}	2^{209}	Meet In The Middle	[22]
8	1	$2^{111.1}$	$2^{227.8}$	Imp. Diff.	[18]
8	1	$2^{89.1}$	$2^{229.7}$	Imp. Diff.	[18]
8	1	$2^{116.5}$	$2^{247.5}$	Imp. Diff.	[21]
8	2	2^{53}	2^{215}	RK Diff.	[20]
8	2	2^{112}	2^{143}	RK Diff.	[20]
8	2	2^{64}	2^{191}	RK Diff.	[20]
8	2	2^{88}	2^{167}	RK Diff.	[20]
8	2	2^{119}	2^{85}	RK Diff.	[23]
8	2	$2^{103.5}$	$2^{102.5}$	RK Diff.	[23]
8	2^{7}	2^{59}	2^{79}	RK Bommerang	Section4
9	256	2^{85}	$2^{224}\times 5$	Partial Sum	[17]
9	4	2^{99}	2^{120}	RK Rectangle	[19]
9	$2^{15.5}$	2^{67}	$2^{142.3}$	RK Bommerang	[2]
9	2^{7}	2^{59}	2^{119}	RK Bommerang	Section5.1
9	2^{7}	2^{67}	$2^{135.3}$	RK Bommerang	Section5.2

The paper is organized as follows: In Section 2 we briefly describe the AES algorithm and in Section 4 we propose our attack on 8-round AES-256. Two new related-key

This work was partially supported by Iran Telecommunications Research Center and the Cryptography Chair of the Iranian NSF.

978-1-4244-5943-8/10/$26.00 ©2010 IEEE

boomerang attacks on 9 round AES-256 are introduced in Sections 5. Section 6 summarize and concludes the paper.

II. A BRIEF DESCRIPTION OF AES

The Advanced Encryption Standard (AES) [3] is a symmetric key block cipher that supports key sizes of 128, 192 and 256 bits. The 128-bit plaintexts are represented by a 4×4 matrix of bytes, where each byte represents a value in $GF(2^8)$. An AES round is composed of four operations:

• *SubBytes* (SB): a bytewise transformation that applies on each of the current block an 8-bit to 8-bit nonlinear S-box.

• *ShiftRows* (SR): a linear operation that rotates on the left all the rows of the current matrix (0 for the first row, 1 for the second, 2 for the third and 3 for the fourth).

• *MixColumns* (MC): another linear operation represented by a 4×4 matrix M, where M is

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

Each column of the input matrix is multiplied by M in the $GF(2^8)$. The inverse of M in $GF(2^8)$ is

$$\begin{pmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{pmatrix}$$

• *AddRoundKey* (AK): a simple XOR operation between the input matrix and the subkey of the current round.

The MixColumns operation is omitted in the last round and an initial key addition is performed before the first round for whitening. We also assume that the MixColumns operation is omitted in the last round of the reduced-round variants. The number of rounds (N_r) is variable depending on the key length ($32\times N_k$), 10 rounds for 128-bit key, 12 for 192-bit key and 14 for 256-bit key.

A. Notations

In this paper we use the following notations: x_i^I denotes the input block of the round i, while x_i^S, x_i^R, x_i^M and x_i^O denotes the intermediate values after applying SubBytes, ShiftRows, MixColumns and AddRoundKey operations of round i, respectively. Obviously, $x_{i-1}^O = x_i^I$ holds for $i \geq 2$. We denote the subkey of the i-th round by k_i and the initial whitening subkey by k_0. In some cases, we are interested in interchanging the order of the MixColumns operation and the subkey addition. As these operations are linear, they can be interchanged, by first XORing the data with an equivalent key and then applying the MixColumns operation. We denote the equivalent subkey for the modified version by w_i, i.e. $w_i = MC^{-1}(k_i)$, and x_i^W denotes the intermediate value after applying AddRoundKey with equivalent subkey. Let $x_{i,col(j)}$ denotes the j-th column of x_i where $j \in \{0,1,2,3\}$. We also denote the byte in the m-th row and n-th column of x_i by $x_{i,m,n}$ where $m,n \in \{0,1,2,3\}$. Another notation for bytes of x_i is an enumeration $\{0,1,2,...,15\}$ where the byte $x_{i,m,n}$ corresponds to byte $4n+m$ of x_i, i.e. x_i is exhibited as an array of 4×4 bytes with byte indexed as shown in Figure 1.

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

Figure 1: Byte coordinate of 128-bit data block

We use the notation $x_i = ((x_{i,col(0)}),(x_{i,col(1)}),(x_{i,col(2)}),(x_{i,col(3)}))$ to show x_i column-wise. The column j of x_i is represented as $(x_{i,0,j}, x_{i,1,j}, x_{i,2,j}, x_{i,3,j})$.

III. RELATED KEY BOOMERANG ATTACK

Boomerang attack is a kind of statistical-structural attack. The scenario of these attacks involves two main steps. The first one is distinguishing the cryptosystem output sequence from a random sequence with a complexity lower than the exhaustive search. The second step is the key recovery step in which we find the key bits of cryptosystem using the distinguishing characteristic.

A. Distinguisher step

During the distinguisher step we treat the cipher $E(P)$ as a cascade of two sub-ciphers $E(P) = E_1 o(E_0(P))$. Consider two pairs of (P_a, P_b) and (P_c, P_d) have the related key differential of $(\alpha \to \beta)$ for E_0 and two pairs of (P_a, P_c) and (P_b, P_d) have the related key differential of $(\delta \to \gamma)$ for E_1^{-1}. We call the (P_a, P_b, P_c, P_d) a *correct related-key boomerang quartet*. We

can show that the pairs of (P_c, P_d) has the related key differential of ($\beta \to \alpha$) for E_0^{-1} (see Figure 2):

$$\begin{aligned} & E_0(P_c) \oplus E_0(P_d) \\ & = E_0(P_a) \oplus E_0(P_b) \oplus E_0(P_a) \\ & \oplus E_0(P_c) \oplus E_0(P_b) \oplus E_0(P_d) \\ & = E_0(P_a) \oplus E_0(P_b) \oplus E_1^{-1}(C_a) \\ & \oplus E_1^{-1}(C_c) \oplus E_1^{-1}(C_b) \oplus E_1^{-1}(C_d) \\ & = \beta \oplus \gamma \oplus \gamma \\ & = \beta \end{aligned}$$

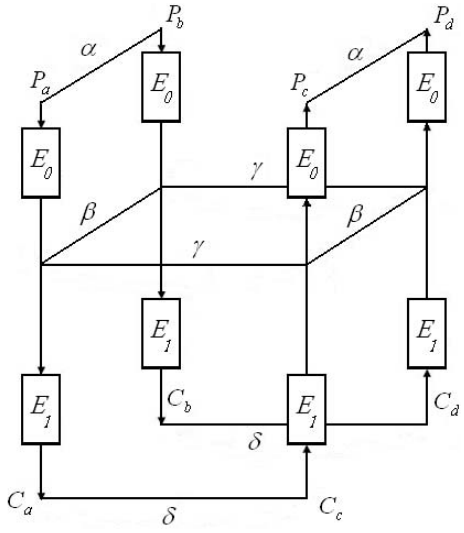

Figure 2: Related Key Boomerang Distinguisher

To achieve C_a and C_b and to generate the correct related-key boomerang quartets, we encrypt the P_a and $P_b = P_a \oplus \alpha$. Now, we decrypt $C_c = C_a \oplus \delta$ and $C_d = C_b \oplus \delta$ to achieve P_c and P_d.

For obtaining the boomerang distinguishing characteristic, we use the related key differential of ($\alpha \to \beta$), ($\beta \to \alpha\beta$) and ($\delta \to \gamma$). So the probability of having a correct related-key boomerang quartet which must be greater than the probability of a random quartets occurring is:

$$Pr(\alpha \to \beta) \cdot Pr(\beta \to \alpha\beta) \cdot Pr(\delta \to \gamma) > 2^{-n} = 2^{-128}$$

B. Key recovery step

In this step we just work on the set stored by the related-key boomerang distinguisher. Consider the pairs of plaintexts (P_a, P_b)with differences α and corresponding ciphertexts (C_a, C_b). Decrypt $C_c = C_a \oplus \delta$ and $C_d = C_b \oplus \delta$ to achieve P_c and P_d . Now consider the quartets (P_a, P_b, P_c, P_d) as a correct related-key boomerang quartet when $P_c \oplus P_d = \alpha$. For every correct related-key boomerang quartet, guess a whitening key and encrypt the pairs (P_a, P_b) and (P_c, P_d) . For the assumed key compute the output difference of the first round and check the differential characteristic. If the characteristic is hold, increase the corresponding counter of the assumed key. Finally the subkey which has a counter with a larger number is the correct key.

IV. Related-Key Boomerang Attack on 8-Round AES-256

We attack a 8-round 256-bit key AES. In this attack E_0 is rounds 1-5 of AES-256 and E_1 is rounds 6-8. The basic differential characteristic ($\alpha \to \beta$) used in rounds 1-5 is also the best known 5-round differential characteristic of AES-256. This characteristic and the basic differential characteristic used in rounds 6-8 are presented in Figures 5 and 6, respectively.

A. The structure of the related keys

In the related key boomerang attack we use two pairs of the related keys as follows:

$$\Delta K = K_a \oplus K_b = K_c \oplus K_d$$

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

ΔK is used for the first related key differential E_0 and $\Delta K'$ is used for the second related key differential E_1. The attacker just knows these related keys and wants to find the cipher key. The related key differences and the round subkey differences are shown in Figures 3 and 4, while the key differences $\Delta K_0', \Delta K_1' \ldots \Delta K_{10}'$ occur with the probability of 2^{-7}. An a difference will be transformed into a certain f by the S-box once. The difference f can be one of $2^7 - 1$ values.

K0				K1				K2				K3			
W0	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
0	0	0	0	a	a	0	0	0	0	0	0	a	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

K4				K5				K6				K7			
W16	W17	W18	W19	W20	W21	W22	W23	W24	W25	W26	W27	W28	W29	W30	W31
0	0	0	0	a	a	a	a	0	0	0	0	a	0	a	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	b'	b'	b'	b'	c	c	c	c

K8				K9				K10			
W32	W33	W34	W35	W36	W37	W38	W39	W40	W41	W42	W43
0	0	0	0	a	a	0	0	0	0	0	0
0	0	0	0	0	0	0	0	f	f	f	f
d	d	d	d	e	e	e	e	d	0	d	0
b'	0	b'	0	c	0	c	0	b'	b'	0	0

Figure 3: Sub-key differences derived from ΔK

K0				K1				K2				K3			
W0	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
0	0	0	0	a	a	a	a	0	0	0	0	a	0	a	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
f	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

K4				K5				K6				K7			
W16	W17	W18	W19	W20	W21	W22	W23	W24	W25	W26	W27	W28	W29	W30	W31
0	0	0	0	a	a	0	0	0	0	0	0	a	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

K8				K9			
W32	W33	W34	W35	W36	W37	W38	W39
0	0	0	0	a	a	a	a
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 4: Sub-key differences derived from $\Delta K'$

In the rest of this section we present a method of breaking 8-round AES-256 using a boomerang distinguisher.

B. The attack procedure

The eight round attack will be as follows:

1. Prepare a pool of plaintexts $P_{a,i}$, $i = 0,\ldots,2^{57}-1$ which have all possible values in eight bytes (0,3,4,5,9,10,14,15) and arbitrary constant in the other bytes. Encrypt the pool under K_a and obtain a pool of 2^{57} ciphertexts $C_{a,i}$.

2. Repeat the previous step for $P_{b,i} = P_{a,i}$ and $K_b = K_a \oplus \Delta K$ to obtain a pool of 2^{64} ciphertexts $C_{b,i}$.

3. Repeat the following steps for every f:

3.1. Construct a pool of modified ciphertexts: $C_{c,i} = C_{a,i} \oplus \delta$, where δ is a 128-bit value, of which, byte 0 is non-zero and other bytes are zeros. Decrypt the pool $C_{c,i}$ under $K_c = K_a \oplus \Delta K'$ to obtain the plaintexts $P_{c,i}, i.e., P_{c,i} = E_{K_c}^{-1}(C_{c,i})$.

3.2. Repeat the previous step for $C_{d,i} = C^{b,i} \oplus \delta$ and $K_d = K_c \oplus \Delta K'$ to obtain a pool of 2^{57} plaintexts $P^{d,i} = E_{K_d}^{-1}(C_{d,i})$.

3.3. Pick only those quartets $(P_{a,i}, P_{b,j}, P_{c,i}, P_{d,j})$ where $P_{c,i}, P_{d,j}$ have zero difference in 8 bytes (1,2,6,7,8,11,12,13).

3.4. For each of the quartets that passes the previous step, guess a 8-bit sub-key $k_{a,8}$ of K_a that enters the one S-box corresponding to a non-constant byte and consequently compute k_b, k_c and k_d. Using the guessed key value partially decrypt one round and check that $\Delta x_{7,Col(0)}^{MC} = (0,0,0,0)$, for both pairs (C_a, C_c) and (C_b, C_d).

3.5. For each of the quartets that pass previous step, guess a 32-bit sub-key $k_{a,0}$ of K_a in the position of (0,5,10,15) and consequently compute k_b, k_c and k_d. Using the guessed key value partially encrypt one round and check that $\Delta x_{1,Col(0)}^{M} = (a,0,0,0)$, for both pairs (P_a, P_b) and (P_c, P_d).

3.6. Guess a 32-bit subkey $k_{a,0}$ of K_a in the positions of bytes 3, 4, 9, 14 and compute k_b, k_c and k_d. Partially encrypt each quartet $(P_{a,i}, P_{b,j}, P_{c,i}, P_{d,j})$ left from the previous step. Check if $\Delta x_{1,Col(0)}^{MC} = (a,0,0,0)$.

C. The related key differential trail

1) $(\alpha \to \beta_{out})$

The used α has a non-zero difference in bytes (0,3,4,5,9,10,14,15). It is easy to conclude that $x_{1,Col(0)}^{SR}$ and $x_{1,Col(1)}^{SR}$ are non-zero bytes and the two others are zero bytes and the first two columns of x^M are $(a,0,0,0)$ with the probability of 2^{-64}. We call β_{out}, the difference obtained after passing the related-key differential E_0. The trail x_1^M to x_6^O holds with probability 1. So the probability of the differential E_0, i.e., the transformation of an α difference into a β_{out} difference, is $Pr(\alpha \to \beta_{out}) = 2^{-64}$ (see Figure 5).

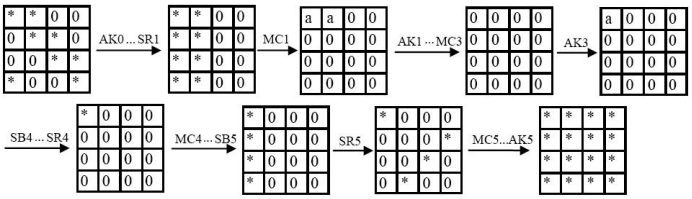

Figure 5: The related key differential $\alpha \to \beta$

2) $(\delta \to \gamma)$

From the bottom up direction of the related-key boomerang distinguisher, the related-key differential E_1^{-1}, is used with the round-key differences of $\Delta K'$. The input difference δ consists of one non-zero difference in byte 0. The suitable trail generates $(0,0,0,0)$ in $x_{7,Col(0)}^{M}$ with the

probability of 2^{-8} . It is easily concluded that $Pr(\delta \to \gamma) = 2^{-8}$. Also the $Pr(\delta_1 = \delta_2)$ is one in this paper. So the probability of the differential E_1 , i.e., the transformation of an δ difference into a γ difference and $Pr(\delta_1 = \delta_2)$ is 2^{-8} (see Figure 6).

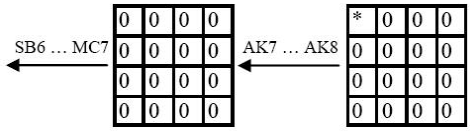

Figure 6: The related key differential $\delta \to \gamma$ (8-round AES-256)

3) $(\beta_{in} \to \alpha)$

Using the results of the previous step which states $Pr(\gamma_1 = \gamma_2) = 1$, we easily conclude that $\beta_{out} = \beta_{in}$. This means that β_{in} and β_{out} are not only equal in the same positions of non-zero differences but also in each byte. Δk_5 has no unfixed bytes and Δx_5^M can go back with probability one. This means we know that four non-zero byte differences occur in the bytes 0,7,10 and 13 of Δx_5^R, while the other bytes are zero. With the probability of 2^{-24}, x_4^M has a non-zero difference in byte 0, while the remaining bytes are zero. $\Delta x_{3,Col(0)}^O$ is $(a,0,0,0)$ after the next S-box operation with the probability of 2^{-8} .The further steps operate such that the output difference of E_0^{-1} is α . The differential E_0^{-1} has the probability $Pr(\beta_{in} \to \alpha) = 2^{-32}$ (see Figure 5).

D. Complexity of the 8-round attack

A correct related-key boomerang quartet occurs with probability

$Pr_c = Pr(\alpha \to \beta_{out}) \cdot Pr(\delta \to \gamma)^2 \cdot Pr(\gamma_1 = \gamma_2) \cdot Pr(\beta_{in} \to \alpha)$

$= 2^{-64} \cdot (2^{-8})^2 \cdot 1 \cdot 2^{-32} = 2^{-112}$

Two pools of 2^{57} plaintexts can be combined to approximately $\frac{(2^{57})^2}{2} = 2^{113}$ quartets. So the data complexity of this attack is $2^2 \cdot 2^{57} = 2^{59}$.

The time complexity of the attack consists of four parts:

• Steps 1 and 2 require 2^{57} 8-round AES-256 encryption.

• Since Step 3 runs at most 2^7 times, the time complexity of Steps 3.1 and 3.2 is $2 \cdot 2^7 \cdot 2^{57} = 2^{65}$

• The probability of the existence of mentioned quartets in Step 3.3 is 2^{-64}. So we have $2^{113} \cdot 2^{-64} = 2^{49}$ quartets to decrypt in Step 3.4 and the time complexity is $\frac{1}{8} \cdot \frac{1}{16} \cdot 2^7 \cdot 2^8 \cdot 2^2 \cdot 2^{49} = 2^{59}$ 8-round AES-256 encryption.

• After the previous step, $2^{49} \cdot (2^{-7})^2 = 2^{35}$ quartets remain. Step 3.5 requires $\frac{1}{8} \cdot \frac{4}{16} \cdot 2^7 \cdot 2^{32} \cdot 2^8 \cdot 2^2 \cdot 2^{35} = 2^{79}$ 8-round AES-256 encryption, because for each of 2^8 guessed keys in previous step, we should guess 2^{32} values in bytes 0, 5, 10 and 15 for $k_{a,0}$ and for all of these keys, we should check four bytes for each of the 2^{35} remained quartets. Since $2^{35} \cdot 2^{-64} = 2^{-29}$ quartets remain from the previous step, Step 3.6 requires $\frac{1}{8} \cdot \frac{4}{16} \cdot 2^7 \cdot 2^{32} \cdot 2^{32} \cdot 2^8 \cdot 2^2 \cdot 2^{-29} = 2^{47}$ 8-round AES-256 encryption. At last $2^{-29} \cdot 2^{-64} = 2^{-93}$ quartets will remain.

V. Related-Key Boomerang Attack on 9-Round AES-256

In this section we explain two attacks on 9-round AES-256.

A. Extended 8-Round AES-256 Attack

The first one is the extension of the related-key boomerang attack in the previous section to a 9-round attack, by guessing 32 bits of $k_{a,9}$ at the bytes 0, 7, 10 and 13. Moreover, we change the order of MC_8 and AK_8 , which allows us to mount the 8-round attack inside the 9-round attack. The attack works as follows:

• Guess 32 bits of $k_{a,9}$ at the bytes 0, 7, 10 and 13. Therefore we have to guess 8 bits for the unknown values of e in ΔK and compute subkeys $k_{b,9}$, $k_{c,9}$, $k_{d,9}$.

• Ask for encryption of P_a under K_a to obtain C_a .

• Compute the intermediate value $x_{a,8}^O$ at bytes 0, 7, 10 and 13 by decrypting C_a under $k_{a,9}$.

• Compute the intermediate value $x_{c,8}^O = x_{a,8}^O \oplus \delta$ at bytes 0, 7, 10 and 13. Compute C_c by encrypting $x_{c,8}^O$ under $k_{c,9}$. Ask for decryption of C_c under K_c to obtain P_c .

• Ask for encryption of $P_b = P_a \oplus \alpha$ under K_b to obtain C_b .

• Compute the intermediate value $x_{b,8}^O$ at bytes 0, 7, 10 and 13 by decrypting C_b under $k_{b,9}$.

• Compute the intermediate value $x^O_{d,8} = x^O_{b,8} \oplus \delta$ at bytes 0, 7, 10 and 13. Compute C_d by encrypting $x^O_{d,8}$ under $k_{d,9}$. Ask for decryption of C_d under K_d to obtain P_d.

• Check if $P_c \oplus P_d = \alpha$.

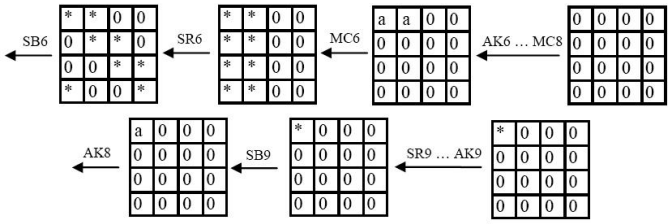

Figure 7: The related key differential $\delta \rightarrow \gamma$ (9-round AES-256)

The data complexity of this 9-round attack on AES-256 remains 2^{59} chosen plaintexts and ciphertexts. The time complexity increases to $2^{32} \cdot 2^8 \cdot (8/9) \cdot 2^{79} = 2^{119}$ 9-round AES-256 encryptions.

K0				K1				K2				K3			
W0	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15
a	0	0	0	f	0	0	0	a	a	a	a	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

K4				K5				K6				K7			
W16	W17	W18	W19	W20	W21	W22	W23	W24	W25	W26	W27	W28	W29	W30	W31
a	0	a	0	0	0	0	0	a	a	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

K8				K9				K10			
W32	W33	W34	W35	W36	W37	W38	W39	W40	W41	W42	W43
a	0	0	0	0	0	0	0	a	a	a	a
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0

Figure 8: Sub-key differences derived from $\Delta K'$

B. 9-Round AES-256 Attack

The second attack is very similar to the 8-round attack which was explained in the previous section. In this attack E_0 is rounds 1-5 of AES-256 and E_1 is rounds 6-9. The $(\alpha \rightarrow \beta_{out})$ and $\beta_{in} \rightarrow \alpha$ trails are the same as the 8-round attack. The basic differential characteristic used in rounds 6-9 ($\delta \rightarrow \gamma$) is presented in Figure 7 respectively. The input difference δ consists of one non-zero difference in byte 0. The suitable trail generates $(0,0,0,0)$ in $x^M_{8,Col(0)}$ with the probability of 2^{-8}. It is easily concluded that $Pr(\delta \rightarrow \gamma) = 2^{-8}$. Also the $Pr(\delta_1 = \delta_2)$ is 2^{-56} in this paper. So the probability of the differential E_1, i.e., the transformation of an δ difference into a γ difference and $Pr(\delta_1 = \delta_2)$ is $(2^{-8})^2 \cdot 2^{-56} = 2^{-72}$ (see Figure 7).

Also this attack uses the previous ΔK and the new $\Delta K'$ which is used for the second related key differential E_1. The related key difference $\Delta K'$ and the round subkey differences are shown in Figure 8, while the key differences $\Delta K'_0, \Delta K'_1 \ldots \Delta K'_{10}$ occur with the probability of 2^{-7}. An a difference will be transformed into a certain f by the S-box once. The difference f can be one of $2^7 - 1$ values.

1) The Attack Procedure

The procedure of the 9-round AES-256 attack is very similar to the attack on 8-round AES-256, while we have $2^{42.5}$ structures of 2^{64} plaintexts $P_{a,i}$ and $P_{b,i}$, instead of one structure of 2^{57} plaintexts in the 8-round attack.

2) Complexity of 9-Round AES-256 Attack

Two pools of 2^{64} plaintexts can be combined to $\frac{(2^{64})^2}{2} = 2^{127}$ quartets. Due to analyzing the structures separately, the data complexity of the attack is $2^2 \cdot 2^{64} = 2^{66}$ chosen plaintexts, while the time complexity is about $2^{42.5} \cdot 2^{92.83} = 2^{135.33}$ nine round encryptions and 2^{-79} quartets remain after the attack procedure. Using $2^{42.5}$ structures, we obtain $2^{42.5} \cdot 2^{127} = 2^{169.5}$ quartets in total. Therefore, about $2^{42.5} \cdot 2^{-79} = 2^{-36.5}$ false related key boomerang quartets remain.

VI. Summary and Conclusion

We presented four attacks on AES. The first attack, applicable to 8-round AES-256, has a data complexity of about 2^{59} chosen plaintexts ciphertexts and a time complexity of 2^{79} 8-round AES-256 encryptions. The second attack requires 2^{59} chosen plaintexts ciphertexts and a time complexity of 2^{119} encryptions for 9-round AES-256. As shown in Table 1, the time complexity of the best previous attack on 9-round AES-256 is decreased by the factor 2^1 in this paper, and meanwhile the data complexity is improved by the factor 2^{40}.

REFERENCES

[1] Gorski, M., Lucks, S. "New Related-Key Boomerang Attacks on AES" INDOCRYPT 2008, Lecture Notes in Comput. Sci., vol 5365, Springer-Verlag, 2008, pp. 266–278.

[2] Fleischmann, E., Gorski, M., Lucks, S. "Attacking 9 and 10 Rounds of AES-256". ACISP 2009, Lecture Notes in Comput. Sci., vol 5594, Springer-Verlag, 2009, pp. 60–72.

[3] Daemen, J., and Rijmen, V., "The Design of Rijndael:AES-the Advanced Encryption Standard", Springer-Verlag, 2002.

[4] Biham, E., and Shamir, A., "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology., 1991,4(1), pp. 3-72.

[5] Knudsen, L.R., "Truncated and Higher Order Differentials". proc of Fast Software Encryption 1994, Lecture Notes in Comput. Sci., vol 1008, Springer-Verlag, 1995, pp. 196-211.

[6] Langford, S.K., Hellman, M.E., "Differential-Linear Cryptanalysis". proc of CRYPTO 1994, Lecture Notes in Comput. Sci., vol 839, Springer-Verlag, 1994, pp. 17-25.

[7] Wagner, D., "The Boomerang Attack". proc of Fast Software Encryption 1999, Lecture Notes in Comput. Sci., vol 1636, Springer-Verlag, 1999, pp. 156-170.

[8] Biham, E., Dunkelman, O., Keller, N., "The Rectangle Attack - Rectangling the Serpent". proc of EUROCRYPT 2001, Lecture Notes in Comput. Sci., vol 2045, Springer-Verlag, 2001, pp. 340-357.

[9] Biham, E., Biryukov, A., and Shamir, A., "Cryptanalysis of Skipjack Reduced to 31 Rounds". Advances in Cryptology, proc. of EUROCRYPT '99, Lecture Notes in Comput. Sci., vol 1592, Springer-Verlag, 1999, pp. 12-23.

[10] Biham, E., "New Types of Cryptanalytic Attacks Using Related Keys". Journal of Cryptology., 1994,7(4),pp. 229-246.

[11] Knudsen, L.R., "Cryptanalysis of LOKI91". proc of AUSCRYPT 1992, Lecture Notes in Comput. Sci., vol 718, Springer-Verlag, 1993, pp. 196-208.

[12] Kelsey, J., Kohno, T., Schneier, B., "Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES". proc of CRYPTO 1996, Lecture Notes in Comput. Sci., vol 1109, Springer-Verlag, 1996, pp. 237-251.

[13] Kelsey, J., Schneier, B., Wagner, D., "Related Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2 and TEA". proc of Information and Communications security - ICICS 1997, Lecture Notes in Comput. Sci., vol 1334, Springer-Verlag, 1997, pp. 233-246.

[14] Blunden, M., Escott, A., "Related Key Attacks on Reduced Round KASUMI". proc of Fast Software Encryption 2001, Lecture Notes in Comput. Sci., vol 2355, Springer-Verlag, 2001, pp. 277-285.

[15] Biryukov, A. "The Boomerang Attack on 5 and 6-Round Reduced AES". AES 2005, Lecture Notes in Comput. Sci., vol 3373, Springer-Verlag,,2005, pp. 11–15.

[16] Biham, E., Dunkelman, O., Keller, N. "Related-Key Boomerang and Rectangle Attacks". EUROCRYPT 2005, Lecture Notes in Comput. Sci., vol 3494, Springer-Verlag, 2005, pp. 507–525.

[17] Ferguson, N., Kelsey, J., Lucks S., et al., "Improved cryptanalysis of Rijndael", Proc. Fast Software Encryption (FSE '00), Lect. Notes Comput. Sci., 2001, 1978, pp. 213–230.

[18] Lu, J., Dunkelman, O., Keller, N. and Kim, J., "New Impossible Differential Attacks on AES", INDOCRYPT 2008, pp. 279-293.

[19] Kim, J., Hong, S., Preneel, B., "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256". proc of Fast Software Encryption 2007, Lecture Notes in Comput. Sci., vol 4356, Springer-Verlag, 2007, pp. 15-20.

[20] Zhang, W., Wu, W. and Zhang, L., "Related-Key Differential Attacks on Reduced-Round AES-256". https://www.lois.cn/LOIS-AES/data/AES-256.pdf

[21] Zhang, W., Wu, W. and Feng, D., "New Results on Impossible Differential Cryptanalysis of Reduced AES". ICISC 2007, Lecture Notes in Computer Science Vol 4817, Springer-Verlag, 2007, pp. 239–250,

[22] Demirci, H. and Selcuk, A., "A Meet-in-the-Middle Attack on 8-Round AES". FSE 2008, Lecture Notes in Comput. Sci., vol 5806, Springer-Verlag, 2008, pp. 116-126.

[23] Soleimany, H., Sharifi, A. and Aref, M.R., "Improved Related-Key Impossible Differential Attacks on 8-Round AES-256". IEEE International Zurich Seminar on Communications, IZS 2010.