Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192 [⋆]

Seokhie Hong[1], Jongsung Kim[2], Sangjin Lee[2], and Bart Preneel[1]

[1] Katholieke Universiteit Leuven, ESAT/SCD-COSIC, Kasteelpark Arenberg 10,
B-3001 Leuven-Heverlee, Belgium
{Seokhie.Hong, Bart.Preneel}@esat.kuleuven.ac.be
[2] Center for Information Security Technologies(CIST),
Korea University, Seoul, Korea
{joshep,sangjin}@cist.korea.ac.kr

Abstract. In this paper we propose a notion of related-key rectangle attack using 4 related keys. It is based on two consecutive related-key differentials which are independent of each other. Using this attack we can break SHACAL-1 with 512-bit keys up to 70 rounds out of 80 rounds and AES with 192-bit keys up to 8 rounds out of 12 rounds, which are faster than exhaustive search.

1 Introduction

Differential cryptanalysis [1] introduced by E. Biham and A. Shamir is one of the most powerful known attacks on block ciphers. After this attack was introduced, various variants of the attack have been proposed, such as the truncated differential attack [18], the higher order differential attack [18], the differential-linear attack [20], the impossible differential attack [3], the boomerang attack [23], the rectangle attack [4] and so on.

In 1993, E. Biham introduced the related-key attack [2] in which the attacker can choose the relationship between two unknown keys. It is based on a key scheduling algorithm and shows that a block cipher with a weak key scheduling algorithm may be vulnerable to this kind of attack. Several cryptanalytic results of this attack were reported in [6, 12, 13, 22].

In [10], P. Hawkes showed that the related-key attack can be combined with the differential-linear attack and that this combined attack can find a relatively large weak-key class of block cipher IDEA. After this, G. Jakimoski and Y. Desmedt [11] exploited a combination of the related-key and the impossible differential attacks to analyze 8-round AES with 192-bit keys. Recently, J. Kim et al. [15] introduced a combination of the related-key and the rectangle attacks,

[⋆] The first author was supported by the Post-doctoral Fellowship Program of Korea Science & Engineering Foundation (KOSEF). The second and the third authors were supported by the MIC(Ministry of Information and Communication), Korea, supervised by the IITA(Institute of Information Technology Assessment

Table 1. Comparison of our attacks with the previous ones

Block Cipher	Type of Attack	Number of Rounds	Complexity Data / Time
SHACAL-1 (80 rounds)	Differential	30(0-29)	2^{110}CP / $2^{75.1}$[17]
		41(0-40)	2^{141}CP / 2^{491}[17]
	Amplified Boomerang	47(0-46)	$2^{158.5}$CP / $2^{508.4}$[17]
	Rectangle	47(0-46)	$2^{151.9}$CP / $2^{482.6}$[5]
		49(22-70)	$2^{151.9}$CP / $2^{508.5}$[5]
		49(29-77)	$2^{151.9}$CC / $2^{508.5}$[5]
	Related-Key Rectangle	57(0-56)	$2^{154.75}$RK-CP / $2^{503.38}$ [15]
		59(0-58)	$2^{149.72}$RK-CP / $2^{498.30}$ [15]
		70(0-69)	$2^{151.75}$RK-CP / $2^{500.08}$ (New)
AES-192 (12 rounds)	Square	7(0-6)	2^{32}CP / 2^{184} [21]
	Partial Sums	7(0-6)	$19 \cdot 2^{32}$CP / 2^{155} [8]
		7(0-6)	$2^{128} - 2^{119}$CP / 2^{120}[8]
		8(0-7)	$2^{128} - 2^{119}$CP / 2^{188}[8]
	Related-Key Impossible	7(0-6)	2^{111}RK-CP / 2^{116} [11]
		8(0-7)	2^{88}RK-CP / 2^{183} [11]
	Related-Key Rectangle	8(0-7)	$2^{86.5}$RK-CP / $2^{86.5}$ (New)

CP: Chosen Plaintexts, RK-CP: Related-Key Chosen Plaintexts,
CC: Chosen Ciphertexts, Time: Encryption units

called the related-key rectangle attack, in which the attacker can use consecutive two differentials; one is a related-key differential and the other one is a differential.

Until now, a relation of two keys has been considered in almost all attacks relevant to related-key attacks but in this paper we consider 4 related keys. Our basic idea is similar to the related-rectangle attack presented in [15] except that our attack uses 4 related keys. In our attack we use two consecutive related-key (truncated) differentials which are independent of each other. Our attack allows us to break SHACAL-1 with 512-bit keys up to 70 rounds out of 80 rounds and AES with 192-bit keys up to 8 rounds out of 12 rounds. See Table 1 for a summary of our results and their comparison with the previous attacks.

Our paper is organized as follows. In Sect. 2, we introduce the related-key rectangle attack using 4 related keys. Two applications on SHACAL-1 and AES are presented in Sect. 3 and Sect. 4, respectively. We conclude our paper in Sect. 5.

2 The Related-Key Rectangle Attack

The related-key rectangle attack introduced in [15] is a combination of the related-key and the rectangle attacks. It exploits two types of related-key rectangle distinguishers to retrieve the related keys of the underlying block cipher. Each of these two types of distinguishers uses two consecutive differentials; one is a related-key differential and the other one is a differential. However, we can extend the range of distinguishers by considering two consecutive related-key differentials. The distinguishers presented in [15] can be useful in analyzing block ciphers which have a good related-key differential followed by a good differential, or which have a good differential followed by a good related-key differential, while our distinguishers can be efficiently used in analyzing block ciphers which have a good related-key differential followed by another good related-key differential.

We now describe two related-key rectangle distinguishers based on two consecutive related-key differentials. Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher that uses $\{0,1\}^k$ and $\{0,1\}^n$ as a key space and a plaintext/ciphertext space, respectively, and that is composed of a cascade $E = E^1 \circ E^0$, i.e., $E_K(P) = E^1_K \circ E^0_K(P)$.

A related-key rectangle distinguisher can be formed by building quartets of plaintexts $(P_i, P^*_i,\ P'_j, P'^*_j)$ that satisfy the below four differential conditions. Assume that P_i, P^*_i, P'_j and P'^*_j are encrypted by using keys K, K^*, K' and K'^*, respectively, where K, K^*, K' and K'^* are related to each other. Let I_i, I^*_i, I'_j and I'^*_j denote the intermediate encrypted values of P_i, P^*_i, P'_j and P'^*_j under E^0, respectively, and C_i, C^*_i, C'_j and C'^*_j denote the encrypted values of I_i, I^*_i, I'_j and I'^*_j under E^1, respectively. If the following four differential conditions are satisfied, we call such a quartet $(P_i, P^*_i, P'_j, P'^*_j)$ *a right quartet.*

- Differential Condition 1 : $P_i \oplus P^*_i = P'_j \oplus P'^*_j = \alpha$
- Differential Condition 2 : $I_i \oplus I^*_i = I'_j \oplus I'^*_j = \beta$
- Differential Condition 3 : $I_i \oplus I'_j = \gamma$
- Differential Condition 4 : $C_i \oplus C'_j = C^*_i \oplus C'^*_j = \delta$

In these four differential conditions, the α and the δ represent specific differences and the β and the γ represent arbitrary differences. Note that the differential conditions 2 and 3 allow us to get $I^*_i \oplus I'^*_j = \gamma$ with probability 1. See Fig. 1 for a description of such a right quartet. In Fig. 1, we set relations of K, K^*, K' and K'^* as follows: $K \oplus K^* = K' \oplus K'^* = \Delta K^*$ and $K \oplus K' = K^* \oplus K'^* = \Delta K'$, where the ΔK^* and the $\Delta K'$ represent specific key differences.

When does a right quartet described in Fig. 1 form a distinguisher? In order to answer this question, we first assume the following two related-key differentials of the E^0 and the E^1; for E^0 there exists a related-key differential $\alpha \rightarrow \beta$ with probability $p^*_{\alpha,\beta}$ and for E^1 there exists a related-key differential $\gamma \rightarrow \delta$ with probability $q^*_{\gamma,\delta}$. These assumptions mean that $p^*_{\alpha,\beta} = Pr_{X,K}[E^0_K(X) \oplus E^0_{K^*}(X^*) = \beta | X \oplus X^* = \alpha, K \oplus K^* = \Delta K^*]$, $q^*_{\gamma,\delta} = Pr_{X,K}[E^1_K(X) \oplus E^1_{K'}(X') = \delta | X \oplus X' = \gamma, K \oplus K' = \Delta K']$.

Assume that we have m_1 pairs of (P_i, P^*_i) and m_2 pairs of (P'_j, P'^*_j) with difference α. Then about $m_1 \cdot p^*_{\alpha,\beta}$ and $m_2 \cdot p^*_{\alpha,\beta}$ pairs satisfy the related-key differential $\alpha \rightarrow \beta$ for E^0. Thus we have about $m_1 \cdot m_2 \cdot (p^*_{\alpha,\beta})^2$ quartets satisfying the differential conditions 1 and 2. If we assume that the intermediate encryption values are distributed uniformly over all possible values, we get $I_i \oplus I'_j = \gamma$ with a probability 2^{-n}. This assumption enables us to obtain about $m_1 \cdot m_2 \cdot 2^{-n} \cdot (p^*_{\alpha,\beta})^2$ quartets satisfying the differential conditions 1, 2 and 3. As stated above, the differential conditions 2 and 3 allow us to get $I^*_i \oplus I'^*_j = \gamma$ with probability 1.

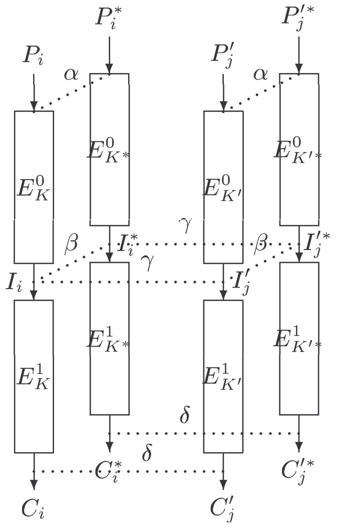

Fig. 1. A Related-Key Rectangle Distinguisher (A Right Quartet)

Moreover, each of the pairs (I_i, I'_j) and (I_i^*, I'^*_j) satisfies the related-key differential $\gamma \to \delta$ for E^1 with probability $q^*_{\gamma,\delta}$. Therefore, the expected number of right quartets is

$$\sum_{\beta,\gamma} m_1 \cdot m_2 \cdot 2^{-n} \cdot (p^*_{\alpha,\beta})^2 \cdot (q^*_{\gamma,\delta})^2 = m_1 \cdot m_2 \cdot 2^{-n} \cdot (\hat{p^*_\alpha})^2 \cdot (\hat{q^*_\delta})^2 \ ,$$

where $\hat{p^*_\alpha} = (\sum_\beta (p^*_{\alpha,\beta})^2)^{\frac{1}{2}}$ and $\hat{q^*_\delta} = (\sum_\gamma (q^*_{\gamma,\delta})^2)^{\frac{1}{2}}$.

For a random permutation the expected number of right quartets is $m_1 \cdot m_2 \cdot 2^{-2n}$, since there are $m_1 \cdot m_2$ possible quartets and each of the pairs (C_i, C'_j) and (C_i^*, C'^*_j) satisfies the δ difference with probability 2^{-n}. Thus, $\hat{p^*_\alpha} \cdot \hat{q^*_\delta} > 2^{-n/2}$ must hold for the related-key rectangle distinguisher to work. This kind of distinguisher will be used in attaking 70-round SHACAL with 512-bit keys.

The above related-key rectangle distinguisher can be extended by considering a number of output differences for E^1. That is, we can use a related-key truncated differential for E^1 whose input difference is of γ and output difference is in a set $D \neq \varnothing$. $q^*_{\gamma,D}$ denotes the probability of this related-key truncated differential. In this case, the expected number of right quartets is

$$\sum_{\beta,\gamma} m_1 \cdot m_2 \cdot 2^{-n} \cdot (p^*_{\alpha,\beta})^2 \cdot (q^*_{\gamma,D})^2 = m_1 \cdot m_2 \cdot 2^{-n} \cdot (\hat{p^*_\alpha})^2 \cdot (\hat{q^*_D})^2 \ ,$$

where $\hat{q_D^*} = (\sum_\gamma (q^*_{\gamma,D})^2)^{\frac{1}{2}}$. In the case of a random permutation, the expected number of right quartets is $m_1 \cdot m_2 \cdot 2^{-2n} \cdot |D|^2$, since there are $m_1 \cdot m_2$ possible quartets and each of the pairs (C_i, C'_j) and (C^*_i, C'^*_j) satisfies one of the differences in a set D with probability $2^{-n} \cdot |D|$ where $|D|$ is the number of elements in D. Thus, $\hat{p_\alpha^*} \cdot \hat{q_D^*} > 2^{-n/2} \cdot |D|$ must hold for the related-key rectangle distinguisher to work. This kind of distinguisher will be used in attacking 8-round AES with 192-bit keys.

3 Related-Key Rectangle Attack on Reduced Rounds of SHACAL-1

Firstly, we briefly describe SHACAL-1. Secondly, we describe a 59-round related-key rectangle distinguisher of SHACAL-1 and use it to attack 70-round SHACAL-1.

3.1 A Description of SHACAL-1

The SHACAL-1 cipher [9] is a 160-bit block cipher based on the compression function of the hash standard SHA-1 [19]. It consists of 80 rounds and uses a variable key length up to 512 bits.

A 160-bit plaintext P is composed of five 32-bit words A,B,C,D and E. X_r denotes the value of 32-bit word X before the *r-th* round. According to this notation, the plaintext P is divided into A_0,B_0,C_0,D_0 and E_0, and the corresponding ciphertext C is divided into A_{80},B_{80},C_{80},D_{80} and E_{80}. The *r-th* round of encryption is performed as follows:

$$\begin{aligned}
A_{r+1} &= K_r + ROTL_5(A_r) + f_r(B_r, C_r, D_r) + E_r + Cst_r \\
B_{r+1} &= A_r \\
C_{r+1} &= ROTL_{30}(B_r) \\
D_{r+1} &= C_r \\
E_{r+1} &= D_r
\end{aligned}$$

for $r = 0, \cdots, 79$, where $ROTL_j(X)$ represents rotation of the 32-bit word X to the left over j bits, K_r is the round subkey, Cst_r is the round constant, and

$$\begin{aligned}
f_r(B_r, C_r, D_r) &= (B_r \& C_r) | (\neg B_r \& D_r), && (0 \le r \le 19) \\
f_r(B_r, C_r, D_r) &= B_r \oplus C_r \oplus D_r, && (20 \le r \le 39,\ 60 \le r \le 79) \\
f_r(B_r, C_r, D_r) &= (B_r \& C_r) | (B_r \& D_r) | (C_r \& D_r), && (40 \le r \le 59).
\end{aligned}$$

As stated above, SHACAL-1 supports a variable key length up to 512 bits. However, SHACAL-1 is not intended to be used with a key shorter than 128 bits. In case a shorter key than 512 bits is inserted in the cipher, the key is padded with zeros to a 512-bit string. Let the 512-bit key string be denoted $K = [K_0||K_1|| \cdots ||K_{15}]$, where each K_i is a 32-bit word. The key expansion of

512 bits K to 2560 bits is defined by

$$K_i = ROTL_1(K_{i-3} \oplus K_{i-8} \oplus K_{i-14} \oplus K_{i-16}), \quad (16 \le i \le 79) \ .$$

3.2 Attack on 70-Round SHACAL-1 with 512-bit Keys

In the key schedule of SHACAL-1, fixing differences of any consecutive 16 round keys determines differences of the remaining 64 round keys. Indeed the key schedule of SHACAL-1 corresponds to a linear feedback shift register (LFSR) with left rotation. Moreover, the key schedule of SHACAL-1 has relatively low difference propagations. These weaknesses of the key schedule allow us to get two consecutive good related-key differential characteristics of SHACAL-1. That is, we can construct a 33-round related-key differential characteristic $\alpha \rightarrow \beta$ for rounds 0-32 (E^0) with probability 2^{-45} ($\approx p^*_{\alpha,\beta}$) and a 26-round related-key differential characteristic $\gamma \rightarrow \delta$ for rounds 33-58 (E^1) with probability 2^{-25} ($\approx q^*_{\gamma,\delta}$), where $\alpha = (0, e_{8,22,1}, e_{1,15}, e_{10}, e_{5,31})$, $\beta = (e_{1,5,15,30}, e_{10}, e_3,\ e_{30}, 0)$, $\gamma = (e_{1,8}, 0, e_{3,6,31}, e_{1,3,31}, e_{3,13,31})$ and $\delta = (e_{1,15},\ e_{10}, e_3, e_{30}, 0)$. Here, e_i denotes a 32-bit word that has $0's$ in all bit positions except for bit i and $e_{i_1,\cdots,i_k}$ denotes $e_{i_1} \oplus \cdots \oplus e_{i_k}$. These two consecutive related-key differential characteristics are combined to construct our 59-round related-key rectangle distinguisher of SHACAL-1.

The first 33-round related-key differential characteristic is same as that of [15] (Sect. 4) except for the condition of plaintext pairs. The 33-round related-key differential characteristic presented in [15] exploits plaintext pairs for which 6 bits are fixed, while our related-key differential characteristic has plaintext pairs for which 10 bits are fixed as follows:

$$\begin{array}{c} a_1 = a_1^* = 1,\ b_3 = b_3^* = 0,\ b_{10} = b_{10}^* = 1,\ b_{15} = b_{15}^* = 0,\ c_8 = c_8^* = 0\ , \\ c_{10} = c_{10}^* = 0,\ c_{22} = c_{22}^* = 0,\ d_8 = d_8^* = 0,\ d_{15} = d_{15}^* = 0,\ d_{22} = d_{22}^* = 0\ , \end{array} \qquad (1)$$

where $P = (A, \cdots, E)$, $P^* = (A^*, \cdots, E^*)$ and x_i is the $i\text{-}th$ bit of 32-bit word X. This stronger condition increases the probability of [15] by a factor of four. See Tables 2 and 3 in Appendix A for the details of this related-key differential characteristic and the associated key differences. As shown in Table 2, the difference of the master keys is $(e_{31}, e_{31}, e_{31}, e_{31}, 0, e_{31}, 0, e_{31},\ 0, 0, 0,\ 0, 0, 0, 0, e_{31})$. Let ΔK^* denote this difference of the master keys and Δk^* denote the difference of keys for rounds $59 \sim 69$ depicted in Table 2. These two notations will be used in our attack algorithm.

The second 26-round related-key differential characteristic is very similar to that of [15] (Sect. 5). The related-key differential characteristic presented in [15] works through rounds 21-47, while our related-key differential characteristic works through rounds 33-58. Since the SHACAL-1 cipher uses a different f function every 20 rounds, the probability of our related-key differential characteristic is slightly different from that of [15]. See Tables 4 and 5 for the details of this related-key differential characteristic and the associated key differences. As shown in Table 4, the difference of the master keys is $(0, e_{31}, e_{31}, e_{30}, 0, e_{29,30,31}, e_{31}, 0, e_{31}, e_{29}, 0, e_{30}, 0, e_{30}, e_{31}, e_{30,31})$. Let $\Delta K'$ be this difference of the master keys and $\Delta k'$ be the difference for rounds $59 \sim 69$ depicted in Table 4.

According to [15] we can increase the lower bounds for $\widehat{p_\alpha^*}$ and $\widehat{q_\delta^*}$ to $2^{-44.17}$ and $2^{-24.08}$. These lower bounds are derived from taking into account as many related-key differential characteristics associated with $\widehat{p_\alpha^*}$ or $\widehat{q_\delta^*}$ as possible. Since the value $\widehat{p_\alpha^*} \cdot \widehat{q_\beta^*}$ ($\approx 2^{-68.25}$) is greater than 2^{-80}, our related-key differential characteristics can form a 59-round related-key rectangle distinguisher of SHACAL-1.

We are now ready to show how to exploit the above 59-round distinguisher to attack 70-round SHACAL-1. We assume that the 70-round SHACAL-1 cipher uses the master key K as well as the related keys K^*, K', K'^* with differences $K \oplus K^* = K' \oplus K'^* = \Delta K^*$ and $K \oplus K' = K^* \oplus K'^* = \Delta K'$. The following is an attack procedure for 70-round SHACAL-1.

Input: Two pools of $2^{149.75}$ plaintext pairs.
Output: Master key quartet (K, K^*, K', K'^*)

1. Choose two pools of $2^{149.75}$ plaintext pairs (P_i, P_i^*) and $(P_j', P_j'^*)$ with the difference α and 10-bit fixed values of (1). With a chosen plaintext attack, the P_i, P_i^*, P_j' and $P_j'^*$ are encrypted using the keys K, K^*, K' and K'^*, respectively, relating in the ciphertexts C_i, C_i^*, C_j' and $C_j'^*$. We keep all these ciphertexts in a table.

2. Guess a 352-bit key quartet (k, k^*, k', k'^*) for rounds 59-69 where $k^* = k \oplus \Delta k^*$, $k' = k \oplus \Delta k'$ and $k'^* = k^* \oplus \Delta k'$. For (k, k^*, k', k'^*) do the following:

- **2.1** For each i, decrypt C_i and C_i^* through rounds 69-59 using k and k^*, and denote the decrypted values by T_i and T_i^*. Let $T' = T_i \oplus \delta$ and $T'^* = T_i^* \oplus \delta$ and encrypt them through rounds 59-69 using k' and k'^* and denote the encrypted values by C' and C'^*. Find a j such that $(C_j', C_j'^*) = (C', C'^*)$.
- **2.2** If the number of (i, j) satisfying Step 2.1 is greater than or equal to 6, go to Step 3. Otherwise, go to Step 2.

3 For the suggested key k, do an exhaustive search for the remaining 160 key bits using trial encryption. During this procedure, if a 512-bit key satisfies three known plaintext and ciphertext pairs, output this 512-bit key, denoted by $\mathcal{K}$, as the master key K of 70-round SHACAL-1. We also output $\mathcal{K} \oplus \Delta K^*, \mathcal{K} \oplus \Delta K'$ and $\mathcal{K} \oplus \Delta K^* \oplus \Delta K'$ as the related keys K^*, K' and K'^*. Otherwise, go to Step 2.

This attack requires two pools of $2^{149.75}$ plaintext pairs and thus the data complexity of this attack is $2^{151.75}$ related-key chosen plaintexts. This attack also requires about $2^{156.08}$ ($=2^{151.75} \cdot 20$) memory bytes since the memory complexity of this attack is dominated by Step 1.

We now analyze the time complexity of this attack. The time complexity of Step 1 is $2^{151.75}$ 70-round SHACAL-2 encryptions. In Step 2.1, this attack seeks colliding quartets for all i, j which seems to require a great amount of time complexity. However, this procedure can be done efficiently by sorting the ciphertext pairs, (C'_j, C'^*_j)'s by C'_j's. Hence the time complexity of Step 2.1 is dominated by the partial decryption/encryption procedure and thus the time complexity of Step 2 is about $2^{500.08}$ $(\approx 2^{352} \cdot 2^{151.75} \cdot \frac{1}{2} \cdot \frac{11}{70})$ on average. In order to estimate the time complexity of Step 3 we should check the expected number of wrong key quartets suggested in Step 2. In Step 2.1, the probability that for each wrong key quartet there exist at least 6 colliding quartets is about $2^{-132.49}$ $(\approx \sum_{i=6}^{t} \left(\binom{t}{i} \cdot (2^{-160 \cdot 2})^i \cdot (1 - 2^{-160 \cdot 2})^{t-i}\right))$ where $t = 2^{299.50}$ and t represents the number of all possible quartets generated by the two pools of $2^{149.75}$ plaintext pairs. From the above analysis we expect about $2^{218.51}$ $(\approx 2^{352} \cdot 2^{-132.49} \cdot \frac{1}{2})$ wrong key quartets on average which are suggested in Step 2 and thus Step 3 requires about $2^{378.51}$ $(\approx 2^{218.51} \cdot 2^{160})$ 70-round SHACAL-1 encryptions. Therefore, the time complexity of this attack is about $2^{500.08}$ 70-round SHACAL-1 encryptions.

In Step 3, the probability that each 512-bit wrong key is suggested is about 2^{-480} $(\approx 2^{-160 \cdot 3})$. It follows that the expected number of 512-bit wrong keys which are suggested in Step 3 is about $2^{-101.49}$ $(= 2^{-480} \cdot 2^{378.51})$. Thus, the possibility that the output of the above attack algorithm is a wrong key quartet is very low. Moreover, the expected number of right quartets is about 8 $(= (2^{149.75})^2 \cdot 2^{-160} \cdot (2^{-68.25})^2)$ and thus the expected number of colliding quartets for the right key quartet is about 8. This is due to the fact $\hat{p_\alpha} \cdot \hat{q_\delta} \approx 2^{-68.25}$. Since the probability that for the right key quartet there exist at least 6 colliding quartets is about 0.80 $(\approx \sum_{i=6}^{t}(\binom{t}{i} \cdot (2^{-160} \cdot 2^{-68.25 \cdot 2})^i \cdot (1 - 2^{-160} \cdot 2^{-68.25 \cdot 2})^{t-i}))$ where $t = 2^{299.50}$, the success rate of this attack is about 0.80.

4 Related-Key Rectangle Attack on Reduced Rounds of AES

Firstly, we briefly describe AES [7]. Secondly, we describe a 7-round related-key rectangle distinguisher of AES and use it to attack 8-round AES.

4.1 A Description of AES

AES encrypts data blocks of 128 bits with 128, 192 or 256-bit key. A round function of AES consists of four basic transformations as follows:

– ByteSub (BS): 8 × 8 S-box transformation
– ShiftRow (SR): Left rotation of each row
– MixColumn (MC): Matrix multiplication in each column
– AddRoundKey (KA): Key exclusive-or

Each round function of AES applies the BS, SR, MC and KA steps in order, but the MC is omitted in the last round. Before the first round, an extra KA step is applied. We call the key used in this step a whitening key. In this paper we concentrate on the 192-bit key version of the AES which is composed of 12 rounds. For more details of the above four transformations, refer to [7].

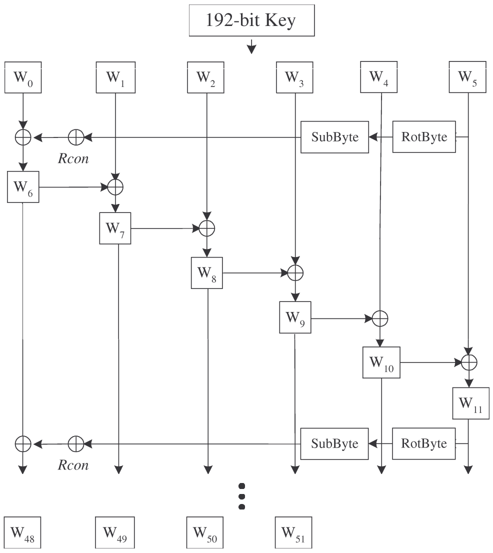

Fig. 2. AES Key schedule(KS) for 192-bit keys

The 192-bit key schedule is described in Fig. 2. In Fig. 2, the whitening key is (W_0, W_1, W_2, W_3), the subkey of round 0 is $(W_4, W_5,\ W_6,\ W_7)$, the subkey of round 1 is $(W_8, W_9, W_{10}, W_{11})$, $\cdots$, the subkey of round 11 is $(W_{48}, W_{49}, W_{50}, W_{51})$, where the 192-bit master key is $W_0||W_1||\cdots||W_5$ and W_i is a 32-bit word. The *Rcon* denotes fixed constants and the SubByte is a byte-wise S-box transformation and the RotByte represents one byte left rotation.

4.2 Attack on 8-Round AES -192

We describe two related-key truncated differentials on which our 7-round related-key rectangle distinguisher is based and then we present our related-key rectangle attack on 8-round AES with 192-bit keys. Before describing the two related-key truncated differentials, we define some notations.

- K_w, K_w^*, K'_w, K'^*_w: whitening keys generated from master keys K, K^*, K', K'^*, respectively.
- K_i, K_i^*, K'_i, K'^*_i: subkeys of round i generated from master keys K, K^*, K', K'^*, respectively.
- a: a fixed nonzero byte value.
- b: output difference of S-box for fixed input difference a.
- $*$: a variable and unknown byte.
- $\Delta K^*, \Delta K', \Delta P^*, \Delta I'$: particular differences described in Figs. 3 and 4.
- $\Delta T, \Delta O$: particular difference set described in Fig. 4.
- $E_K(\cdot)$: 8-round AES encryption with key K.

- $E_K^0(\cdot)$: 4-round AES encryption from round 0 to round 3 with key K but excluding the exclusive-or with K_3.
- $E_K^1(\cdot)$: 3-round AES encryption from round 4 to round 6 with key K including the exclusive-or with K_3

Figs. 3 and 4 show our two related-key truncated differentials with probability 1. If the master key difference is ΔK^* (resp., $\Delta K'$), then the subkey difference in rounds 0-2 (resp., 3-6) is $\Delta K_w^*, \Delta K_0, \Delta K_1^*$ and ΔK_2^* (resp., $\Delta K_3', \Delta K_4', \Delta K_5'$ and $\Delta K_6'$) described in Fig. 3 (resp., Fig. 4).

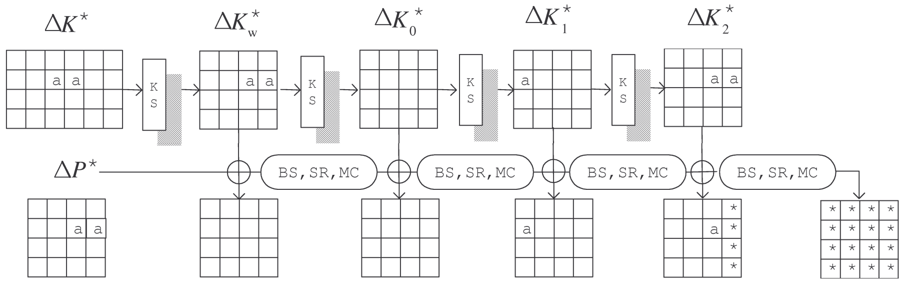

Fig. 3. The first related-key truncated differential for rounds 0-3 (E^0) of AES

Let K and K^* be two keys with difference ΔK^* and P and P^* be two plaintexts with difference ΔP^*. If the plaintexts P and P^* are encrypted under E_K^0 and $E_{K^*}^0$, respectively, then P and P^* satisfy the 4-round related-key truncated differential, described in Fig. 3. A similar argument can be applied to two keys, K and K', and two intermediate values, I and I'. Let K and K' be two keys with difference $\Delta K'$ and P and P' be two plaintexts. If $E_K^0(P) \oplus E_{K'}^0(P') = \Delta I'$, i.e., $I \oplus I' = \Delta I'$, then I and I' satisfy the 3-round related-key truncated differential described in Fig. 4. Note that the output difference of this 3-round differential is one of the elements in ΔT. In Fig. 4, b is an unknown variable which can be one of $2^7 - 1$ elements since the b is the output difference of the S-box for a given input difference a, and $b' = 2b \oplus a$.

As stated above, these two related-key truncated differentials can form a 7-round related-key rectangle distinguisher which has a relatively high probability. In order to compute the probability of this distinguisher we need the following two assumptions.

Assumption 1. The key quartet (K, K^*, K', K'^*) is related as follows;

$$K \oplus K^* = K' \oplus K'^* = \Delta K^*, \ K \oplus K' = K^* \oplus K'^* = \Delta K' \ .$$

Assumption 2. A plaintext quartet (P, P^*, P', P'^*) is related as follows;

$$P \oplus P^* = P' \oplus P'^* = \Delta P^* \ .$$

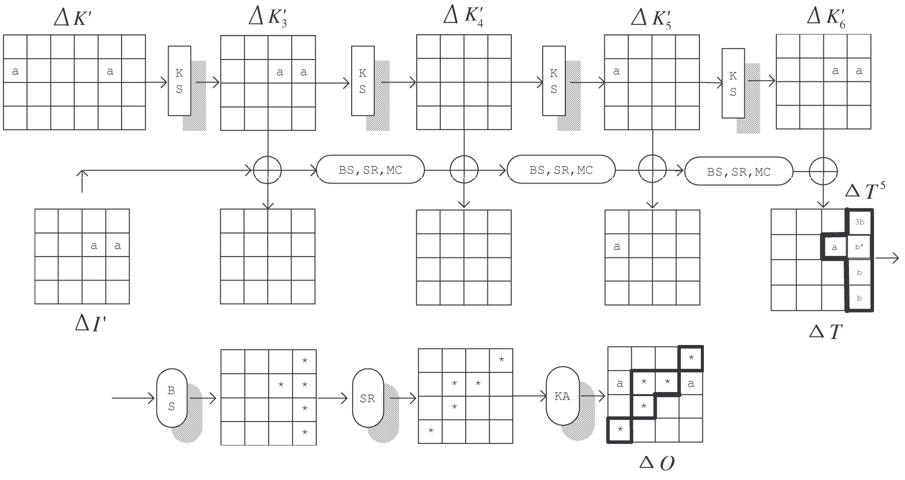

Fig. 4. The second related key truncated differential for rounds 4-6 (E^1) of AES

Let I, I^*, I' and I'^* be $E^0_K(P)$, $E^0_{K^*}(P^*)$, $E^0_{K'}(P')$ and $E^0_{K'^*}(P'^*)$, respectively. Then the probability that $I \oplus I^*$ is equal to $I' \oplus I'^*$ is about $(2^{-32} \cdot 2^{-7})^2 \cdot (2^7 - 2) \cdot 2^{32} + (2^{-32} \cdot 2^{-6})^2 \cdot 2^{32} \approx 2^{-38.97}$. It follows from performing a counting over all the differentials that the active S-box with input difference a and the other four active S-boxes can produce. Since the ShiftRow and the Mixcolumn are linear layers, the ShiftRow and the Mixcolumn of the last round can be ignored in computing the probability (See Fig. 3). Moreover the probability that $I \oplus I' = I^* \oplus I'^* = \Delta I'$ is 2^{-128} under the condition that $I \oplus I^* = I' \oplus I'^*$. So the probability that

$$I \oplus I^* = I' \oplus I'^* \text{ and } I \oplus I' = I^* \oplus I'^* = \Delta I' \tag{2}$$

is $2^{-38.97} \cdot 2^{-128} = 2^{-166.97}$. Hence $E^1_K(I) \oplus E^1_{K'}(I')$ and $E^1_{K^*}(I^*) \oplus E^1_{K'^*}(I'^*)$ are in the difference set ΔT with probability $2^{-166.97}$. But the same statement can be applied to a random cipher with probability $(2^{-128} \cdot (2^7 - 1))^2 \approx 2^{-242}$. The quartet (P, P^*, P', P'^*) satisfying (2) is called a right quartet. Recall that the number of elements in ΔT is $2^7 - 1$.

Now we are ready to explain our attack. We want to find 5 bytes of each subkey K_7, K^*_7, K'_7, K'^*_7 whose byte positions are marked as $*$ on ΔO depicted in Fig. 4. Since the keys K, K^*, K' and K'^* are related, the number of possible key quartets is $2^{40} \cdot (2^7 - 1) \cdot 2^{16} \approx 2^{63}$ rather than $(2^{40})^4$. In order to understand the relations of the round keys of round 7 refer to Fig. 5. In Fig. 5, b is an output difference of S-box for fixed input difference a which can be one of $2^7 - 1$ elements and c and d are unknown varibles.

The basic idea of our attack is simple. Let (P, P^*, P', P'^*) be right quartet and (C, C^*, C', C'^*) be the corresponding ciphertext quartet. Define $D_k(\cdot)$ as a partial

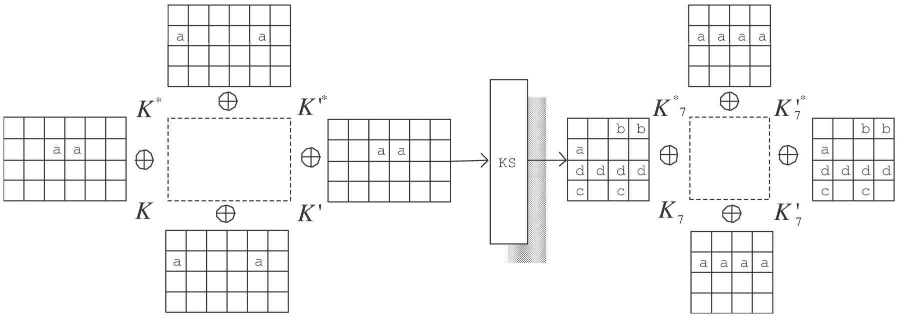

Fig. 5. Differential Property of 4 related keys for rounds 0-7 of AES

one round decryption with k, where k is a 5-byte key candidate of round 7. Then we guess a 5-byte key quartet (k, k^*, k', k'^*) and check that $D_k(C) \oplus D_{k'}(C') \in \Delta T^5$ and $D_{k^*}(C^*) \oplus D_{k'^*}(C'^*) \in \Delta T^5$ where ΔT^5 is a set described in Fig. 4. If the number of ciphertext quartets passing the above test is more than an appropriate threshold, we consider the guessed key quartet as the right one.

Input: Two pools of $2^{84.5}$ plaintext pairs.
Output: 5-byte key quartet of round 7.

1. Choose $2^{84.5}$ plaintext pairs (P_i, P_i^*) and $2^{84.5}$ plaintext pairs (P'_j, P'^*_j) with $P_i \oplus P_i^* = P'{}_j \oplus P'^*_j = \Delta P^*$. With a chosen plaintext attack, the P_i, P_i^*, P'_j, P'^*_j are encrypted using the keys K, K^*, K' and K'^*, respectively, relating in the ciphertexts C_i, C_i^*, C'_j and C'^*_j. We keep all these ciphertexts in a table.
2. Check that $C_i \oplus C'_j \in \Delta O$ and $C_i^* \oplus C'^*_j \in \Delta O$ for all i, j.
3. Guess a 5-byte key quartet (k, k^*, k', k'^*) for round 7.
  3.1 For all ciphertext quartets $(C_i, C_i^*, C'_j, C'^*_j)$ passing the test of Step 2, check that $D_k(C_i) \oplus D_{k'}(C'_j) \in \Delta T^5$ and $D_{k^*}(C_i^*) \oplus D_{k'^*}(C'^*_j) \in \Delta T^5$.
  3.2 If the number of quartets $(C_i, C_i^*, C'_j, C'^*_j)$ passing Step 3.1 is greater than or equal to 3, output the guessed key quartet (k, k^*, k', k'^*) as the right key quartet of round 7. Otherwise, go to Step 3.

This attack requires two pools of $2^{84.5}$ plaintext pairs and thus the data complexity of this attack is $2^{86.5}$ related-key chosen plaintexts. This attack also requires about $2^{90.83}$ $(= 2^{86.5} \cdot 20)$ memory bytes since the memory complexity of this attack is dominated by Step 1.

From the two pools of $2^{84.5}$ plaintext pairs we can make 2^{169} plaintext quartets. Step 2 requires $2^{84.5}$ searches of $2^{84.5}$ ciphertext pairs. This procedure can be done efficiently by sorting the ciphertext pairs, (C'_j, C'^*_j)'s by C'_j's. In Step 2, by assuming that the intermediate encryption values are distributed uniformly over all possible values we get $C_i \oplus C'_j \in \Delta O$ and $C_i^* \oplus C'^*_j \in \Delta O$ with probability

2^{-176} ($= 2^{-11\cdot 8\cdot 2}$) for a wrong quartet $(C_i, C_i^*, C_j', C_j'^*)$. This probability follows from the fact that all elements of ΔO have a identically fixed value in 11 bytes. However, the difference set ΔO is induced by the difference set ΔT and the probability that each ciphertext quartet passes the test of Step 2 is same as that of our 7-round related-key rectangle distinguisher. Hence, the expected number of ciphertext quartets passing the test of Step 2 is about $2^{169}\cdot(2^{-166.97}+2^{-176}) \approx 2^2$. Using this expected number we can estimate the time complexity of Step 3, i.e., Step 3 requires about 2^{63} ($= 2^{63}\cdot 2^2 \cdot 2^2 \cdot \frac{1}{8}\cdot\frac{1}{2}$) 8-round AES encryptions on average. Hence, the time complexity of this attack is dominated by Step 1 and thus this attack requires about $2^{86.5}$ 8-round AES encryptions.

For each wrong key quartet and each ciphertext quartet, the probability of passing the test of Step 3.1 is at most 2^{-6}. Note that the largest number in DC table of S-box used in AES is 4. This probability may occur when two of k, k^*, k', k'^* are correct and each of the rest two of them is correct except for one byte. In this case the probability that Step 3 outputs the guessed wrong key quartet is at most $(2^{-6})^3$. Since the number of these kinds of wrong key quartets is at most $2\cdot 5\cdot(2^8-1)$, the probability that Step 3 outputs such a wrong key quartet is at most 0.01. In this manner we can check all cases for wrong key quartets. For each of all other cases the probability that Step 3 outputs a wrong key quartet is much less than 0.01 and thus the probability that this attack outputs a wrong key quartet is approximately 0.01. Since the probability that for the right key quartet there exist at least 3 quartets passing the test of Step 3.1 is about 0.77 ($\approx \sum_{i=3}^{2^{169}} \binom{2^{169}}{i}(2^{-166.97})^i(1-2^{-166.97})^{2^{169}-i}$), the success rate of this attack is about 0.76 ($\approx 0.77\cdot(1-0.01)$).

5 Conclusion

In this paper we proposed a new notion of related-key rectangle attack using 4 related keys and showed that it could break SHACAL-1 with 512-bit keys up to 70 rounds out of 80 rounds and AES with 192-bit keys up to 8 rounds out of 12 rounds. It is worthwhile to apply this attack to other block ciphers and to study simple key scheduling algorithms which may be resistant to this kind of attack.

References

1. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Proceedings of CRYPTO 1990, LNCS 537, pp. 2-21, Springer, 1990.
2. E. Biham, *New Types of Cryptanalytic Attacks Using Related Keys*, Proceedings of EUROCRYPT 1993, pp. 398-409, LNCS 765, 1993.
3. E. Biham, A. Biryukov and A. Shamir, *Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials*, Proceedings of EUROCRYPT 1999, LNCS 1592, pp. 12-23, Springer, 1999.
4. E. Biham, O. Dunkelman and N. Keller, *The Rectangle Attack - Rectangling the Serpent*, Proceedings of EUROCRYPT 2001, LNCS 2045, pp. 340-357, Springer, 2001.

5. E. Biham, O. Dunkelman and N. Keller, *Rectangle Attacks on 49-Round SHACAL-1*, Proceedings of Fast Software Encryption 2003, LNCS 2887, pp. 22-35, Springer, 2003.
6. M. Blunden and A. Escott, *Related Key Attacks on Reduced Round KASUMI*, Proceedings of Fast Software Encryption 2001, LNCS 2355, pp. 277-285, Springer, 2002.
7. J. Daemen and V. Rijmen, *The Design of Rijndael*, Springer, 2002
8. N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner and D. Whiting, *Improved Cryptanalysis of Rijndael*, Proceedings of Fast Software Encryption 2000, LNCS 1978, pp. 213-230, Springer, 2001.
9. H. Handschuh and D. Naccache, *SHACAL*, Proceedings of NESSIE first workshop, Leuven, 2000.
10. P. Hawkes, *Differential-Linear Weak-Key Classes of IDEA*, Proceedings of EUROCRYPT 1998, LNCS 1403, pp. 112-126, Springer, 1998.
11. G. Jakimoski and Y. Desmedt, *Related-Key Differential Cryptanalysis of 192-bit Key AES Variants*, Proceedings of Selected Areas in Cryptography 2003, LNCS 3006, pp. 208-221, Springer, 2004.
12. J. Kelsey, B. Schneier and D. Wagner, *Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES*, Proceedings of CRYPTO 1996, LNCS 1109, pp. 237-251, Springer, 1996.
13. J. Kelsey, B. Schneir and D. Wagner, *Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA*, Proceedings of International Conference on Information and Communications Seucrity 1997, LNCS 1334, pp. 233-246, Springer, 1997.
14. J. Kelsey, T. Kohno and B. Schneier, *Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent*, Proceedings of Fast Software Encryption 2001, LNCS 1978, pp. 75-93, Springer, 2002.
15. J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, *The Related-Key Rectangle Attack-Application to SHACAL-1*, Proceedings of International Conference on Information Security and Privacy 2004, LNCS 3108, pp. 123-136, Springer, 2004.
16. J. Kim, G. Kim, S. Lee, J. Lim and J. Song, *Related-Key Attacks on Reduced Rounds of SHACAL-2*, Proceedings of INDOCRYPT 2004, To appear.
17. J. Kim, D. Moon, W. Lee, S. Hong, S. Lee and S. Jung, *Amplified Boomerang Attack against Reduced-Round SHACAL*, Proceedings of ASIACRYPT 2002, LNCS 2501, pp. 243-253, Springer, 2002.
18. L.R. Knudsen, *Trucated and Higher Order Differentials*, Proceedings of Fast Software Encryption 1996, LNCS 1039, pp. 196-211, Springer, 1996.
19. U.S. Department of Commerce. *FIPS 180-1*: Secure Hash Standard, Federal Information Processing Standards Publication, N.I.S.T., April 1995.
20. S.K. Langford and M.E. Hellman, *Differential-Linear Cryptanalysis*, Proceedings of CRYPTO 1994, LNCS 839, pp. 17-25, Springer, 1994.
21. S. Lucks, *Attacking seven rounds of Rijndael under 192-bit and 256-bit keys*, Proceedings of AES3, NIST.
22. Y. Ko, S. Hong, W. Lee, S. Lee and J. Kang, *Related Key Differential Attacks on 26 Rounds of XTEA and Full Rounds of GOST*, Proceedings of Fast Software Encryption 2004, LNCS 3017, pp. 299-316, Springer, 2004.
23. D. Wagner, *The Boomerang Attack*, Proceedings of Fast Software Encryption 1999, LNCS 1636, pp. 156-170, Springer, 1999.

A The First Related-Key Differential Characteristic and the Associated Key Differences of SHACAL-1

Table 2. Key Differences Used in the First Related-Key Differential Characteristic

i	ΔK_i^*	i	ΔK_i^*	i	ΔK_i^*	i	ΔK_i^*	i	ΔK_i^*	i	ΔK_i^*	i	ΔK_i^*
0	e_{31}	10	0	20	0	30	0	40	e_3	50	$e_{3,7}$	60	$e_{3,7}$
1	e_{31}	11	0	21	0	31	e_0	41	e_4	51	e_5	61	$e_{2,4,7,9,10}$
2	e_{31}	12	0	22	0	32	e_1	42	0	52	e_7	62	$e_{3,7,11}$
3	e_{31}	13	0	23	0	33	0	43	$e_{1,3,4}$	53	e_8	63	$e_{2,3,4,9}$
4	0	14	0	24	0	34	e_1	44	e_5	54	0	64	$e_{3,5,11}$
5	e_{31}	15	e_{31}	25	0	35	e_2	45	$e_{2,3}$	55	$e_{3,5,7,8}$	65	$e_{3,12}$
6	0	16	0	26	0	36	0	46	e_5	56	e_9	66	$e_{3,5}$
7	e_{31}	17	0	27	0	37	$e_{2,3}$	47	$e_{1,2,6}$	57	$e_{2,5,6}$	67	$e_{3,5,6,9,11,12}$
8	0	18	0	28	0	38	e_3	48	e_{31}	58	e_9	68	e_{13}
9	0	19	0	29	e_0	39	e_1	49	$e_{3,5,6}$	59	$e_{2,3,5,6,10}$	69	$e_{3,5,9,10}$

Table 3. The First Related-Key Differential Characteristic

Round (i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔK_i^*	Prob.
0	0	$e_{8,22,1}$	$e_{1,15}$	e_{10}	$e_{5,31}$	e_{31}	
1	e_5	0	$e_{6,20,31}$	$e_{1,15}$	e_{10}	e_{31}	2^{-2}
2	0	e_5	0	$e_{6,20,31}$	$e_{1,15}$	e_{31}	2^{-5}
3	$e_{1,15}$	0	e_3	0	$e_{6,20,31}$	e_{31}	2^{-6}
4	0	$e_{1,15}$	0	e_3	0	0	2^{-3}
5	0	0	$e_{13,31}$	0	e_3	e_{31}	2^{-3}
6	e_3	0	0	$e_{13,31}$	0	0	2^{-3}
7	e_8	e_3	0	0	$e_{13,31}$	e_{31}	2^{-3}
8	0	e_8	e_1	0	0	0	2^{-2}
9	0	0	e_6	e_1	0	0	2^{-2}
10	0	0	0	e_6	e_1	0	2^{-2}
11	e_1	0	0	0	e_6	0	2^{-2}
12	0	e_1	0	0	0	0	2^{-1}
13	0	0	e_{31}	0	0	0	2^{-1}
14	0	0	0	e_{31}	0	0	2^{-1}
15	0	0	0	0	e_{31}	e_{31}	2^{-1}
16	0	0	0	0	0	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
28	0	0	0	0	0	0	1
29	0	0	0	0	0	e_0	1
30	e_0	0	0	0	0	0	2^{-1}
31	e_5	e_0	0	0	0	e_0	2^{-1}
32	e_{10}	e_5	e_{30}	0	0	e_1	2^{-2}
33	$e_{1,5,15,30}$	e_{10}	e_3	e_{30}	0		2^{-4}

B The Second Related-Key Differential Characteristic and the Associated Key Differences of SHACAL-1

Table 4. Key Differences Used in the Second Related-Key Differential Characteristic

i	$\Delta K'_i$	i	$\Delta K'_i$	i	$\Delta K'_i$	i	$\Delta K'_i$	i	$\Delta K'_i$	i	$\Delta K'_i$	i	$\Delta K'_i$
0	0	10	0	20	e_{31}	30	0	40	0	50	0	60	e_1
1	e_{31}	11	e_{30}	21	e_{30}	31	e_{31}	41	e_{31}	51	0	61	e_2
2	e_{31}	12	0	22	e_{31}	32	0	42	0	52	0	62	0
3	e_{30}	13	e_{30}	23	$e_{30,31}$	33	e_{31}	43	0	53	0	63	$e_{2,3}$
4	0	14	e_{31}	24	e_{31}	34	0	44	0	54	0	64	e_3
5	$e_{29,30,31}$	15	$e_{30,31}$	25	e_{30}	35	0	45	0	55	e_0	65	e_1
6	e_{31}	16	e_{31}	26	e_{31}	36	0	46	0	56	0	66	e_3
7	0	17	$e_{30,31}$	27	e_{31}	37	0	47	0	57	e_0	67	e_4
8	e_{31}	18	e_{31}	28	e_{31}	38	0	48	0	58	e_1	68	0
9	e_{29}	19	$e_{30,31}$	29	e_{31}	39	0	49	0	59	0	69	$e_{1,3,4}$

Table 5. The Second Related-Key Differential Characteristic

Round (i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	$\Delta K'_i$	Prob.
33	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	$e_{3,13,31}$	e_{31}	
34	$e_{1,3}$	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	0	2^{-4}
35	0	$e_{1,3}$	$e_{6,31}$	0	$e_{3,6,31}$	0	2^{-4}
36	e_1	0	$e_{1,31}$	$e_{6,31}$	0	0	2^{-3}
37	e_1	e_1	0	$e_{1,31}$	$e_{6,31}$	0	2^{-2}
38	0	e_1	e_{31}	0	$e_{1,31}$	0	2^{-1}
39	0	0	e_{31}	e_{31}	0	0	2^{-1}
40	0	0	0	e_{31}	e_{31}	0	1
41	0	0	0	0	e_{31}	e_{31}	2^{-1}
42	0	0	0	0	0	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
54	0	0	0	0	0	0	1
55	0	0	0	0	0	e_0	1
56	e_0	0	0	0	0	0	2^{-1}
57	e_5	e_0	0	0	0	e_0	2^{-1}
58	e_{10}	e_5	e_{30}	0	0	e_1	2^{-3}
59	$e_{1,15}$	e_{10}	e_3	e_{30}	0		2^{-4}