Related-Key Rectangle Attack on 43-Round SHACAL-2*

Gaoli Wang

School of Mathematics and System Sciences, Shandong University,
Jinan, China
wanggaoli@mail.sdu.edu.cn

Abstract. SHACAL-2 is a 256-bit block cipher with up to 512 bits of key length based on the hash function SHA-2. It was recommended as one of the NESSIE projection selections. As far as the number of the attacked rounds is concerned, the best cryptanalytic result obtained on SHACAL-2 so far is the analysis of a related-key rectangle attack on the 42-round SHACAL-2 [13]. In this paper we present a related-key rectangle attack on 43-round out of the 64-round of SHACAL-2, which requires $2^{240.38}$ chosen plaintexts and has time complexity of $2^{480.4}$ 43-round SHACAL-2 encryptions. In this paper we also identify and fix some flaws in previous attack on SHACAL-2.

Keywords: Block cipher, SHACAL-2, Related-Key Rectangle attack, Differential characteristic.

1 Introduction

Differential cryptanalysis [3] is one of the most powerful known attacks on block ciphers, which was introduced by E. Biham and A. Shamir in 1990.

The related-key attack [4] was introduced by E. Biham in 1993, in which the attacker chooses the relationship between two unknown keys. The attack 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. Many cryptanalytic results of the attack were presented in [14,15,16,17].

The related-key boomerang and rectangle attacks were proposed by Kim et al. [8,9] and independently by Biham et al. [6]. This attack is a combination of the related-key and the rectangle attacks, and shares the features of rectangle and related-key attacks. The attacker examines quartets of plaintexts encrypted under four related keys. This attack exploits two types of related-key rectangle distinguishers to retrieve the related keys. Our distinguishers can be used in analyzing block ciphers which have a good related-key differential followed by another good related-key differential or which have a good related-key differential followed by a good differential.

* Supported by National Natural Science Foundation of China Key Project No.90604036, National Outstanding Young Scientist No.60525201 and 973 Program No.2007CB807902.

E. Dawson and D.S. Wong (Eds.): ISPEC 2007, LNCS 4464, pp. 33–42, 2007.

SHACAL-2 [2] is a 256-bit block cipher with up to 512-bit key length based on the hash function SHA-2. It was submitted to the NESSIE project (New European Schemes for Signatures, Integrity, an Encryption) and was recommended as one of the NESSIE projection selections. It has 64 rounds. The best cryptanalytic result obtained on SHACAL-2 so far is the analysis of a related-key rectangle on 42-round SHACAL-2 [13]. See Table 1 for a summary of our results and the comparison with the previous attacks.

Table 1. Comparison of our results with the previous attacks on SHACAL-2

Type of Attack	Number of Rounds	Complexity Data/Time/Memory
Impossible Differential	30	$744CP/2^{495.1}/2^{14.5}$[10]
Differential-Nonlinear	32	$2^{43.4}CP/2^{504.2}/2^{48.4}$[11]
Square-Nonlinear	28	$463 \cdot 2^{32}CP/2^{494.1}/2^{45.9}$[11]
Related-Key Differential-Nonlinear	35	$2^{42.32}$RK-CP$/2^{452.10}/2^{47.32}$[12]
Related-Key Rectangle	37	$2^{233.16}$RK-CP$/2^{484.95}/2^{238.16}$[12]
	40	$2^{243.38}$RK-CP$/2^{448.43}/2^{247.38}$[13]
	42	$2^{243.38}$RK-CP$/2^{488.37}/2^{247.38}$[13]
	43	$2^{240.38}$RK-CP$/2^{480.4}/2^{245.38}(New)$

CP: Chosen Plaintexts, RK-CP: Relate-Key Chosen Plaintexts,
Time: Encryption units, Memory: Bytes of memory

The rest of the paper is organized as follows: In Section 2, we introduce some useful properties of the nonlinear functions in SHACAL-2 and some notations, and give a short description of the related-key rectangle attack. In Section 3, we describe the related-key rectangle attack on 43-round SHACAL-2. Finally, we summarize the paper in section 4.

2 Background

2.1 Description of SHACAL-2

SHACAL-2 [2] is a 256-bit block cipher based on the compression function of the hash function SHA-2. The algorithm is composed of 64 rounds with variable key length of up to 512-bit, and it is advised to use keys of at least 128-bit.

For a 256-bit plaintext $P = A_0\|B_0\|C_0\|D_0\|E_0\|F_0\|G_0\|H_0$ the corresponding 256-bit ciphertext C is denoted by $A_{64}\|B_{64}\|C_{64}\|D_{64}\|E_{64}\|F_{64}\|G_{64}\|H_{64}$. The $r-th$ round of encryption is as follows.

$$T^1_{i+1} = H_i + g_1(E_i) + G_1(E_i, F_i, G_i) + Con_i + K_i \quad (1)$$
$$T^2_{i+1} = g_0(A_i) + G_0(A_i, B_i, C_i) \quad (2)$$
$$H_{i+1} = G_i \quad (3)$$
$$G_{i+1} = F_i \quad (4)$$
$$F_{i+1} = E_i \quad (5)$$

$$E_{i+1} = D_i + T^1_{i+1} \tag{6}$$
$$D_{i+1} = C_i \tag{7}$$
$$C_{i+1} = B_i \tag{8}$$
$$B_{i+1} = A_i \tag{9}$$
$$A_{i+1} = T^1_{i+1} + T^2_{i+1} \tag{10}$$

for $i = 0, ..., 63$ where $+$ denotes the addition modulo 2^{32} of 32-bit words, K_i are the 32-bit round subkeys, and Con_i denotes the 32-bit round constants which are different in each of the 64 rounds. The function in the above encryption process are as follows.

$$G_1(X,Y,Z) = I(X,Y,Z) = (X \wedge Y) \oplus (\neg X \wedge Z)$$
$$G_0(X,Y,Z) = J(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$
$$g_0(X) = ROTR_2(X) \oplus ROTR_{13}(X) \oplus ROTR_{22}(X)$$
$$g_1(X) = ROTR_6(X) \oplus ROTR_{11}(X) \oplus ROTR_{25}(X)$$

where $\neg X$ denotes the complement of 32-bit word X and $ROTR_i(X)$ means the right rotation of X by i bit positions.

The key scheduling algorithm of SHACAL-2 supports a maximum 512-bit key and shoter keys are padded by zeros to a 512-bit string. For a 512-bit key string $K = K_0K_1, ..., K_{15}$ the key expansion is as follows.

$$K_i = h_1(K_{i-2}) + K_{i-7} + h_0(K_{i-15}) + K_{i-16}, \ (16 \le i \le 63)$$
$$h_1(X) = ROTR_7(X) \oplus ROTR_{18}(X) \oplus SR_3(X)$$
$$h_0(X) = ROTR_{17}(X) \oplus ROTR_{19}(X) \oplus SR_{10}(X)$$

where SR_i denotes the right shift of 32-bit word X by i bit positions.

2.2 Some Basic Conclusions and Notations

In this section we will present some properties of the two nonlinear functions in our attack.

Proposition 1. *For the nonlinear function* $I(X,Y,Z) = (X \wedge Y) \oplus (\neg X \wedge Z)$ *, there are the following properties:*

1. $I(x,y,z) = I(\neg x,y,z)$ *if and only if* $y = z$.
   $I(0,y,z) = 0$ *and* $I(1,y,z) = 1$ *if and only if* $y = 1$ *and* $z = 0$.
   $I(0,y,z) = 1$ *and* $I(1,y,z) = 0$ *if and only if* $y = 0$ *and* $z = 1$.
2. $I(x,y,z) = I(x,\neg y,z)$ *if and only if* $x = 0$.
   $I(x,0,z) = 0$ *and* $I(x,1,z) = 1$ *if and only if* $x = 1$.
3. $I(x,y,z) = I(x,y,\neg z)$ *if and only if* $x = 1$.
   $I(x,y,0) = 0$ *and* $I(x,y,1) = 1$ *if and only if* $x = 0$.

Proposition 2. *For the nonlinear function* $J(X,Y,Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$ *, there are the following properties:*

1. $J(x,y,z) = J(\neg x,y,z)$ *if and only if* $y = z$.
   $J(0,y,z) = 0$ *and* $J(1,y,z) = 1$ *if and only if* $y = \neg z$.
2. $J(x,y,z) = J(x,\neg y,z)$ *if and only if* $x = z$.
   $J(x,0,z) = 0$ *and* $J(x,1,z) = 1$ *if and only if* $x = \neg z$.
3. $J(x,y,z) = J(x,y,\neg z$ *if and only if* $x = y$.
   $J(x,y,0) = 0$ *and* $J(x,y,1) = 1$ *if and only if* $x = \neg y$.

Notations. In order to describe our attack conveniently, we quote some notations.

1. The bit positions in a 32-bit word are labeled as $31, 30, 29, \ldots, 2, 1, 0$, where bit 31 is the most significant bit and bit 0 is the least significant bit.
2. $A_{i,j}$, $B_{i,j}$, $C_{i,j}$, $D_{i,j}$, and $E_{i,j}$ represent respectively the $j-th$ bit of A_i, B_i, C_i, D_i, and E_i where the least significant bit is the 1-st bit, and the most significant bit is the 32-th bit.
3. e_j represent the 32-bit word composed of 31 $0's$ and 1 in the $j-th$ place, $e_{j,k} = e_j \oplus e_k$ and $e_{j,k,l} = e_j \oplus e_k \oplus e_l$, etc.
4. $\Delta(A,B)$ denotes the difference between A and B.

2.3 Short Description of the Related-Key Rectangle Attack

The related-key rectangle attack was introduced in [8,9] and independently in [6]. Here we give a short description of this attack. Assume that a block cipher $E : \{0,1\}^n \times \{0,1\}^k \longrightarrow \{0,1\}^n$ can be described as $E = E_1 \cdot E_0$, such that there is a related-key differential $\alpha \longrightarrow \beta$ with probability p_β for E_0, and there is a related-key differential $\gamma \longrightarrow \delta$ with probability q_γ for E_1, i.e.,

$$Pr[\Delta(E_0(X,K), E_0(X^*,K^*)) = \beta | \Delta(X,X^*) = \alpha, \Delta(K,K^*) = \Delta K^*] = p_\beta$$

$$Pr[\Delta(E_1(Y^*,K^*), E_1(Y'^*,K'^*)) = \delta | \Delta(Y^*,Y'^*) = \gamma, \Delta(K^*,K'^*) = \Delta K'] = q_\gamma$$

We use the master key K and the related keys K^*, K' and K'^* with difference $\Delta(K,K^*) = \Delta(K',K'^*) = \Delta K^*$ and $\Delta(K,K') = \Delta(K^*,K'^*) = \Delta K'$. The related-key rectangle distinguisher is as follows:

1. Choose m_1 plaintext pairs (P_i, P_i^*) at random such that $\Delta(P_i,P_i^*) = \alpha$. Encrypt P_i and P_i^* under E_0 with key K and K^* respectively to get the intermediate values X_i and X_i^*. Encrypt X_i and X_i^* under E_1 with key K and K^* respectively to get the ciphertexts C_i and C_i^*.
2. Choose m_2 plaintext pairs $(P_j', P_j'^*)$ at random such that $\Delta(P_j',P_j'^*) = \alpha$. Encrypt P_j' and $P_j'^*$ under E_0 with key K' and K'^* respectively to get the intermediate values X_j' and $X_j'^*$. Encrypt X_j' and $X_j'^*$ under E_1 with key K' and K'^* respectively to get the ciphertexts C_j' and $C_j'^*$.
3. Search two pairs of plaintexts $P_i, P_i^\star$ and $P_j', P_j'^*$, and their corresponding ciphertexts C_i, C_i^* and $C_j', C_j'^*$ respectively, satisfying: $\Delta(P_i,P_i^*) = \Delta(P_j',P_j'^*) = \alpha$, $\Delta(X_i,X_i^*) = \Delta(X_j',X_j'^*) = \beta$, $\Delta(X_i,X_j') = \Delta(X_i^*,X_j'^*) = \gamma$, and $\Delta(C_i,C_j') = \Delta(C_i^*,C_j'^*) = \delta$.

A plaintext quartet $(P_i, P_i^*, P_j', P_j'^*)$ satisfying all these conditions is called a right quartet. More generally, a right quartet represents one which satisfies any β and γ difference conditions for given α and δ differences. As described in [7,8,9], the expected number of right quartets is $\sum_{\beta\gamma} m_1 m_2 2^{-n} p_\beta^2 q_\gamma^2 = m_1 m_2 2^{-n} p^2 q^2$, where $p = (\sum_\beta p_\beta^2)^{\frac{1}{2}}$, $q = (\sum_\gamma q_\gamma^2)^{\frac{1}{2}}$. For a random permutation the expected number of right quartets is $m_1 m_2 2^{-2n}$. Therefore as long as $pq > 2^{-\frac{n}{2}}$ we can distinguish between a random permutation and E, and use this distinguisher later to recover the key.

3 Related-Key Rectangle Attack on 43-Round SHACAL-2

As stated earlier, as far as the number of the attacked rounds is concerned, the best cryptanalytic result obtained on SHACAL-2 so far is the analysis of a related-key rectangle attack on 42-round SHACAL-2 [13]. They chose two pools of plaintexts of $2^{178.38} \times 2^{64} = 2^{242.38}$ each, and presented 12 bits conditions of the intermediate values, which will remove the differential probability incurred by the G_0 and G_1 functions in Rounds 1 and 2. They concluded that after Step 1, there remains $2^{242.38} \times 2^{-12} = 2^{230.38}$ intermediate values of each pool, then the expected number of the right quartets is $(2^{230.38})^2/2 \times 2^{-456.76} = 2^3$, where the distinguisher holds with probability $2^{-456.76}$. From the differential characteristic for E_0 in [13], we know that the differential in Step 0 is $(0, e_M, e_{31}, ?, e_{9,13,19}, e_{18,29}, e_{31}, ?) \longrightarrow (0, 0, e_M, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31})$. Obviously it needs some conditions of plaintext to ensure that the differential holds with probability 1. But [13] didn't present any condition of plaintexts. There is another flaw in [13] as follows. Considering $Q^l_{i_0,j_0} \oplus Q^l_{i_1,j_1}$ and $Q^{*l}_{i_0,j_0} \oplus Q^{*l}_{i_1,j_1}$, where $Q^l_{i_0,j_0}$, $Q^l_{i_1,j_1}$ are the intermediate values of S_i, and $Q^{*l}_{i_0,j_0}$, $Q^{*l}_{i_1,j_1}$ are the intermediate values of S_i^*, so it is sufficient to guess the subkeys k^l and k^{*l}, and it is not necessary to guess the additive difference between the subkeys k^l and k^{*l}. Therefore, there are some flaws in the attack procedure of the 42-round analysis in [13].

Our attack is based on the following observation.

Observation 1. Suppose the plaintext P_0 and P_1 are encrypted using the same key, and we know the actual values of $(A_0^i, B_0^i, C_0^i, D_0^i, E_0^i, F_0^i, G_0^i, H_0^i)$ and $(A_1^i, B_1^i, C_1^i, D_1^i, E_1^i, F_1^i, G_1^i, H_1^i)$, then we know the actual values of $(A_0^{i-1}, B_0^{i-1}, C_0^{i-1}, D_0^{i-1}, E_0^{i-1}, F_0^{i-1}, G_0^{i-1})$, $(A_1^{i-1}, B_1^{i-1}, C_1^{i-1}, D_1^{i-1}, E_1^{i-1}, F_1^{i-1}, G_1^{i-1})$ and the additive difference between H_0^{i-1} and H_1^{i-1}, hence we know the actual values of $(A_0^{i-5}, B_0^{i-5}, C_0^{i-5})$ and $(A_1^{i-5}, B_1^{i-5}, C_1^{i-5})$, and the additive difference between D_0^{i-5} and D_1^{i-5}.

3.1 Related-Key Differential Characteristics for SHACAL-2

In our attack, we use the differential characteristics based on [13], and our differential in Step 0 is

$$(0, e_M, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}, \Delta_{i,j}) \longrightarrow (0, 0, e_M, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31})$$

where $g_1(E^0 \oplus e_{9,13,19}) - g_1(E^0) + \Delta_{i,j} = 0$. From Prop.1 and Prop.2, the probability of Step 0 will be 1 if we fix some bits conditions presented in Table 2. Since $D^2 = B^0$, $H^2 = F^0$, according to the encryption algorithm, the probability of Step 2 will be increased up to 2^{-10} by the conditions $B_{0,i} = \neg F_{0,i} (i = 18, 29)$. From [13] we know that the probability from Step 2 to Step 24 is 2^{-37}, so the probability of our first differential characteristic is 2^{-46}. As stated in [13], the second differential characteristic is $2^{-63.38}$. So the 35-round related-key rectangle distinguisher holds with probability $2^{-474.76}$.

Table 3 present the details of the first 25-round related-key differential characteristic. The difference of the master keys is $(e_{31}, 0, 0, 0, 0, 0, 0, 0, e_{31}, 0, 0, 0, 0, 0, 0, 0)$.

Table 4 presents the details of the second 10-round related-key differential characteristic. This differential characteristic use the same master key.

Table 2. The fixed plaintext bits for SHACAL-2

A_0	B_0	E_0	F_0
$A_{0,31} = B_{0,31}, A_{0,i} = C_{0,i}$	$B_{0,i} = \neg F_{0,i} (i = 19, 30)$	$E_{0,31} = 0$	$F_{0,i} = G_{0,i}$
$(i = 6, 9, 18, 20, 25, 29)$	$B_{0,9} = \neg E_{0,9}$	$E_{0,i} = 0 (i = 18, 29)$	$(i = 9, 13, 19)$

Table 3. The First Related-Key Differential Characteristic for SHACAL-2

i	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔF_i	ΔG_i	ΔH_i	ΔK_i	$Prob.$
0	0	e_M	e_{31}	0	$e_{9,13,19}$	$e_{18,29}$	e_{31}	$\Delta_{i,j}$	e_{31}	1
1	0	0	e_M	e_{31}	0	$e_{9,13,19}$	$e_{18,29}$	0	0	2^{-11}
2	e_{31}	0	0	e_M	0	0	$e_{9,13,19}$	$e_{18,29}$	0	2^{-10}
3	0	e_{31}	0	0	$e_{6,20,25}$	0	0	$e_{9,13,19}$	0	2^{-7}
4	0	0	e_{31}	0	0	$e_{6,20,25}$	$G_4[7,$	0	0	2^{-4}
5	0	0	0	e_{31}	0	0	$e_{6,20,25}$	0	0	2^{-3}
6	0	0	0	0	e_{31}	0	0	$e_{6,20,25}$	0	2^{-4}
7	0	0	0	0	0	e_{31}	0	0	0	2^{-1}
8	0	0	0	0	0	0	e_{31}	0	0	2^{-1}
9	0	0	0	0	0	0	0	e_{31}	e_{31}	1
10	0	0	0	0	0	0	0	0	0	1
...	...	...	...	...	...	...	...	...	...	...
23	0	0	0	0	0	0	0	0	0	1
24	0	0	0	0	0	0	0	0	·	2^{-6}
25	$e_{13,24,28}$	0	0	0	$e_{13,24,28}$	0	0	0		

$g_1(E^0 \oplus e_{9,13,19}) - g_1(E^0) + \Delta_{i,j} = 0$, M={6,9,18,20,25,29}

3.2 The Key Recovery Attack Procedure for 43-Round SHACAL-2 with 512-Bit Keys

Assume that the master key is K and the related keys are K^* with differences $\Delta K = (e_{31}, 0, 0, 0, 0, 0, 0, 0, 0, e_{31}, 0, 0, 0, 0, 0, 0, 0)$. We will present a method to exploit the 35-round related-key rectangle distinguisher to find a master key

Table 4. The Second Related-Key Differential Characteristic for SHACAL-2

$Round(i)$	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔF_i	ΔG_i	ΔH_i	$Prob.$
25	e_{31}	e_{31}	$e_{M'}$	0	0	$e_{9,13,19}$	$e_{18,29,31}$	0	2^{-15}
26	e_{31}	e_{31}	e_{31}	$e_{M'}$	0	0	$e_{9,13,19}$	$e_{18,29,31}$	2^{-12}
27	0	e_{31}	e_{31}	e_{31}	$e_{6,20,25}$	0	0	$e_{9,13,19}$	2^{-7}
28	0	0	e_{31}	e_{31}	e_{31}	$e_{6,20,25}$	0	0	2^{-8}
29	0	0	0	e_{31}	e_{31}	e_{31}	$e_{6,20,25}$	0	2^{-7}
30	0	0	0	0	e_{31}	e_{31}	e_{31}	$e_{6,20,25}$	2^{-4}
31	0	0	0	0	0	e_{31}	e_{31}	e_{31}	1
32	0	0	0	0	0	0	e_{31}	e_{31}	2^{-1}
33	0	0	0	0	0	0	0	e_{31}	1
34	e_{31}	0	0	0	e_{31}	0	0	0	2^{-11}
35	$e_{6,9,18,20,25,29}$	e_{31}	0	0	$e_{6,20,25}$	e_{31}	0	0	

M'={6,9,18,20,25,29,31}

of 43-round SHACAL-2. The 256-bit value P is denoted by eight 32-bit words (A, B, C, D, E, F, G, H), and P^* is denoted by $(A^*, B^*, C^*, D^*, E^*, F^*, G^*, H^*)$. We denote the intermediate value just before round k by $Q^k_{i,j}$, and denote $Q^k_{i,j}$ by eight 32-bit words $A^k_{i,j}$, $B^k_{i,j}$, $C^k_{i,j}$, $D^k_{i,j}$, $E^k_{i,j}$, $F^k_{i,j}$, $G^k_{i,j}$ and $H^k_{i,j}$. Also, we denote $(\Delta A^{35}, \Delta B^{35}, \Delta C^{35}, \Delta D^{35}, \Delta E^{35}, \Delta F^{35}, \Delta G^{35}, \Delta H^{35})$ by Δ. The attack procedure for 43-round SHACAL-2 is performed as follows.

1. Choose $2^{175.38}$ structures S_i of plaintext $P_{i,j}$, $i = 1, 2, \ldots, 2^{175.38}$, $j = 1, 2, \ldots, 2^{64}$. XOR every 224 bits words (A, B, C, D, E, F, G) in S_i with the 224 bits value $(0, e_M, E_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31})$ (M={6,9,18,20,25,29}) and add 32-bit word H with 32-bit word $\Delta_{i,j}$ to get $2^{175.38}$ structures S^*_i, where in every structure the 192 bits words A, B, C, E, F, G are fixed, the 16 bits conditions presented in Table 2 are satisfied in every plaintext, and $g_1(E \oplus e_{9,13,19}) - g_1(E) + \Delta_{i,j} = 0$. Encrypt every plaintext in S_i and S^*_i using the key K and $K^* = K \oplus \Delta K$ to get the corresponding ciphertexts $C_{i,j}$ and $C^*_{i,j}$ respectively.
2. Guess two 96-bit subkeys (k^{42}, k^{41}, k^{40}) and $(k^{*42}, k^{*41}, k^{*40})$. For the guessed subkey pair, do the following:
   (a) Decrypt all the ciphertext $C_{i,j}$ and $C^*_{i,j}$ through rounds 42-40 using the subkey (k^{42}, k^{41}, k^{40}) and $(k^{*42}, k^{*41}, k^{*40})$ respectively to obtain the intermediate values $Q^{40}_{i,j}$ and $Q^{*40}_{i,j}$. We put all the intermediate values $Q^{40}_{i,j}$ in a table, and put $Q^{*40}_{i,j}$ in another table. We can get (A^{35}, B^{35}, C^{35}), $(A^*35, B^{*35}, C^{*35})$, $\Delta(D^{35}_{i_0,j_0}, D^{35}_{i_1,j_1})$ and $\Delta(D^{*35}_{i_0,j_0}, D^{*35}_{i_1,j_1})$ by observation 1.
   (b) Check whether $C^{40}_{i_0,j_0} \oplus C^{40}_{i_1,j_1}$ and $C^{*40}_{i_0,j_0} \oplus C^{*40}_{i_1,j_1}$ satisfy the first half of Δ. Record (k^{42}, k^{41}, k^{40}) and all the qualified quartets and then go to Step 3.
3. Guess two 32-bit subkeys k^{39}, k^{*39}, and decrypt all the remaining quartets $(Q^{40}_{i_0,j_0}, Q^{40}_{i_1,j_1}, Q^{*40}_{i_0,j_0}, Q^{*40}_{i_1,j_1})$ to obtain the actual values of $(A^{38}, B^{38}, C^{38}, D^{38}, E^{38}, F^{38}, G^{38})$, $(A^{*38}, B^{*38}, C^{*38}, D^{*38}, E^{*38}, F^{*38}, G^{*38})$, the additive

difference between $H^{38}_{i_0,j_0}$ and $H^{38}_{i_1,j_1}$, and the additive difference between $H^{*38}_{i_0,j_0}$ and $H^{*38}_{i_1,j_1}$, hence to get the actual values of $(A^{35}_{i_0,j_0}, B^{35}_{i_0,j_0}, C^{35}_{i_0,j_0})$, $(A^{35}_{i_1,j_1}, B^{35}_{i_1,j_1}, C^{35}_{i_1,j_1})$, $(A^{*35}_{i_0,j_0}, B^{*35}_{i_0,j_0}, C^{*35}_{i_0,j_0})$, $(A^{*35}_{i_1,j_1}, B^{*35}_{i_1,j_1}, C^{*35}_{i_1,j_1})$, the additive difference between $D^{35}_{i_0,j_0}$ and $D^{35}_{i_1,j_1}$, and the additive difference between $D^{*35}_{i_0,j_0}$ and $D^{*35}_{i_1,j_1}$ by observation 1. Since $H^{38} = E^{35}$ and $\Delta E^{35} = e_{6,20,25}$, we can discard all the quartets which do not satisfy $H^{38}_{i_1,j_1} - H^{38}_{i_0,j_0} \in \bigwedge_1$ and $H^{*38}_{i_1,j_1} - H^{*38}_{i_0,j_0} \in \bigwedge_1$, where $\bigwedge_1 = \{a + b + c | a = \pm 2^6, b = \pm 2^{20}, c = \pm 2^{25}\}$. Record $(k^{39}, k^{40}, k^{41}, k^{42})$ and all the qualified quartets and then go to Step 4.

4. Guess two 32-bit subkeys k^{38}, k^{*38}, and decrypt all the remaining quartets $(Q^{39}_{i_0,j_0}, Q^{39}_{i_1,j_1}, Q^{*39}_{i_0,j_0}, Q^{*39}_{i_1,j_1})$ to obtain the actual values of $(A^{37}, B^{37}, C^{37}, D^{37}, E^{37}, F^{37}, G^{37})$, $(A^{*37}, B^{*37}, C^{*37}, D^{*37}, E^{*37}, F^{*37}, G^{*37})$, the additive difference between $H^{37}_{i_0,j_0}$ and $H^{37}_{i_1,j_1}$, and the additive difference between $H^{*37}_{i_0,j_0}$ and $H^{*37}_{i_1,j_1}$. Since $H^{37} = F^{35}$ and $\Delta F^{35} = e_{31}$, we can discard all the quartets which do not satisfy $H^{37}_{i_1,j_1} - H^{37}_{i_0,j_0} \in \bigwedge_2$ and $H^{*37}_{i_1,j_1} - H^{*37}_{i_0,j_0} \in \bigwedge_2$, where $\bigwedge_2 = \{2^{31}, -2^{31}\}$. Record $(k^{38}, k^{39}, k^{40}, k^{41}, k^{42})$ and all the qualified quartets and then go to Step 5.
5. Guess two 32-bit subkeys k^{37}, k^{*37}, and decrypt all the remaining quartets $(Q^{38}_{i_0,j_0}, Q^{38}_{i_1,j_1}, Q^{*38}_{i_0,j_0}, Q^{*38}_{i_1,j_1})$ to obtain the actual values of $(A^{36}, B^{36}, C^{36}, D^{36}, E^{36}, F^{36}, G^{36})$, $(A^{*36}, B^{*36}, C^{*36}, D^{*36}, E^{*36}, F^{*36}, G^{*36})$, the additive difference between $H^{36}_{i_0,j_0}$ and $H^{36}_{i_1,j_1}$, and the additive difference between $H^{*36}_{i_0,j_0}$ and $H^{*36}_{i_1,j_1}$. Since $H^{36} = G^{35}$ and $\Delta G^{35} = 0$, we can discard all the quartets which do not satisfy $H^{36}_{i_1,j_1} = H^{36}_{i_0,j_0}$ and $H^{*36}_{i_1,j_1} = H^{*36}_{i_0,j_0}$. Record $(k^{37}, k^{38}, k^{39}, k^{40}, k^{41}, k^{42})$ and all the qualified quartets and then go to Step 6.
6. Guess two 32-bit subkeys k^{36}, k^{*36}, and decrypt all the remaining quartets $(Q^{37}_{i_0,j_0}, Q^{37}_{i_1,j_1}, Q^{*37}_{i_0,j_0}, Q^{*37}_{i_1,j_1})$ to obtain the actual values of $(A^{35}, B^{35}, C^{35}, D^{35}, E^{35}, F^{35}, G^{35})$, $(A^{*35}, B^{*35}, C^{*35}, D^{*35}, E^{*35}, F^{*35}, G^{*35})$, the additive difference between $H^{35}_{i_0,j_0}$ and $H^{35}_{i_1,j_1}$, and the additive difference between $H^{*35}_{i_0,j_0}$ and $H^{*35}_{i_1,j_1}$. Since $\Delta H^{35} = 0$, we can discard all the quartets which do not satisfy $H^{35}_{i_1,j_1} = H^{35}_{i_0,j_0}$ and $H^{*35}_{i_1,j_1} = H^{*35}_{i_0,j_0}$. If there exist more than 5 quartets passing this test, Record $(k^{36}, k^{37}, k^{38}, k^{39}, k^{40}, k^{41}, k^{42})$ and then go to Step 7. Otherwise, repeat Step 6 with another guessed subkeys. If all the possible key pairs in Step 6 are tested, then repeat Step 5 with another guessed subkeys. If all the possible key pairs in Step 5 are tested, then repeat Step 4 with another guessed subkeys. If all the possible key pairs in Step 4 are tested, then repeat Step 3 with another guessed subkeys. If all possible key pairs pairs in Step 3 are tested, then repeat Step 2 with another guessed subkeys.
7. For a suggested $(k^{36}, k^{37}, k^{38}, k^{39}, k^{40}, k^{41}, k^{42})$, exhaustively search for the remaining 288 key bits by trial encryption. If a 512-bit key is suggested, output it as the master key of 43-round SHACAL-2. Otherwise go to Step 2.

The data complexity of this attack is $2^{240.38}$ related-key chosen plaintexts. The memory requirements are about $2^{245.38} (= 2^{240.38} \times 32)$ memory bytes.

In Step 1, the time complexity is $2^{240.38}$ 43-round SHACAL-2 encryptions. The time complexity of Step 2 is about $2^{240.38} \times 2^{32\times 6} \times \frac{8}{43} \approx 2^{430}$ 43-round SHACAL-2 encryptions, and $2^{240.38} \times 2^{192} = 2^{432.38}$ memory access. For each guessed subkeys, we have $2^{239.38\times 2}/2 = 2^{477.76}$ quartets tested in Step 2. Since Sep 2 has a 256-bit filtering for the decrypted quartets, $2^{477.76} \times 2^{-256} = 2^{221.76}$ quartets are suggested in Step 2. The time complexity of Step 3 is about $2^{221.76} \times 2^{32\times 8} \times \frac{4}{43} \approx 2^{474.4}$ 43-round SHACAL-2 encryptions. Since there are 2^3 possible differences in $\bigwedge_1$, about $2^{221.76} \times (2^{-29})^2 = 2^{163.76}$ quartets are suggested in Step 3. The time complexity of Step 4 is about $2^{163.76} \times 2^{32\times 10} \times \frac{4}{43} \approx 2^{480.4}$ 43-round SHACAL-2 encryptions. Since there are 2 possible values in $\bigwedge_2$ (hence $\bigwedge_2$ has a 31-bit filterings), and $\Delta(H^{38})$ has a 3-bit filterings, about $2^{163.76} \times (2^{-31})^2 \times (2^{-3})^2 = 2^{95.76}$ quartets are suggested in Step 4. The time complexity of Step 5 is about $2^{95.76} \times 2^{32\times 12} \times \frac{4}{43} \approx 2^{476.4}$ 43-round SHACAL-2 encryptions. About $2^{95.76} \times (2^{-32})^2 \times = 2^{31.76}$ quartets are suggested in Step 5. The time complexity of Step 6 is about $2^{31.76} \times 2^{32\times 14} \times \frac{4}{43} \approx 2^{476.4}$ 43-round SHACAL-2 encryptions. About $2^{31.76} \times (2^{-32})^2 \times = 2^{-32.24}$ quartets are suggested in Step 6.

The expected number of right quartets are about $2^{477.76} \times 2^{-474.76} = 8$, for about $(2^{175.38}2^{64})^2/2 = 2^{477.76}$ quartets are tested in the attack and the 35-round related-key rectangle distinguisher holds with probability $2^{-474.76}$. Therefore the success rate of this attack (i.e. the probability that the number of remaining quartets for the right key pair is at least 6) is about 0.8 by the Poisson distribution $X \sim Poi(\lambda = 8)$, $Pr_X[X > 5] \approx 0.8$.

4 Conclusions

In this paper by using the related-key differential characteristics in [13], we fix some conditions (presented in Table 2) in each of the plaintexts, so that the differential of Step 0 will be hold with probability 1. Hence it will be not necessary to guess the subkey k^0 like in [13], which will reduce the time complexity. We can attack the 43-round SHACAL-2 using the related-key rectangle attack with data complexity of $2^{240.38}$ chosen plaintexts and time complexity of $2^{480.4}$ 43-round SHACAL-2 encryptions.

References

1. Helena Handschuh, David Naccache, SHACAL, preproceedings of NESSIE first workshop, Leuven, 2000.
2. H. Handschuh and D. Naccache, SHACAL: A Family of Block Ciphers, Submission to the NESSIE project, 2002.
3. E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Proceedings of CRYPTO 1990, LNCS 537, pp. 2-21, Springer, 1990.
4. E. Biham, New Types of Cryptanalytic Attacks Using Related Keys, Proceedings of EUROCRYPT 1993, pp. 398-409, LNCS 765, 1993.
5. E. Biham, O. Dunkelman and N. Keller, Rectangle Attacks on 49-Round SHACAL-1, Proceedings of Fast Software Encryption 2003,LNCS2887, pp. 22-35, Springer, 2003.

6. E. Biham, Orr Dunkelman, Nathan Keller, Related-Key Boomerang and Rectangle Attacks, Advances in Cryptology, proceedings of EUROCRYPT'05, Lecture Notes in Computer Science 3494, pp. 507-525, Springer-Verlag, 2005.
7. 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.
8. 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.
9. Seokhie. Hong, Jongsung. Kim, Sangjin. Lee, Bart Preneel, Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192, Proceedings of Fast Software Encryption 12, Lecture Notes in Computer Science 3557, pp. 368-383, Springer-Verlag, 2005.
10. S. Hong, J. Kim, G. Kim, J.Sung, C. Lee and S. Lee, Impossible Differential Attack on 30-Round SHACAL-2, INDOCRYPT 2003, LNCS 2904, pp. 97-106, Springer-Verlag, 2003.
11. Y. Shin, J. Kim, G. Kim, S. Hong and S. Lee, Differential-Linear Type Attack on Reduced Rounds of SHACAL-2, ACISP 2004, Springer Berlin / Heidelberg ISSN: 0302-9743.
12. J. Kim, G. Kim, S. Lee, J. Lim and J. Song, Related-Key Attacks on Reduced Rounds of SHACAL-2, Proceedings of INDOCRYPT 2004.
13. J. Lu, J. Kim, N. Keller, and O. Dunkelman, Related-Key Rectangle Attack on 42-Round SHACAL-2, In Proceedings of the 9th Information Security Conference (ISC 2006), Lecture Notes in Computer Science, Springer-Verlag, 16 pages, 2006.
14. 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.
15. J. Kelsey, B. Schneier and D. Wagner, Key Schedule Cryptanalysis of IDEA, GDES, GOST, SAFER, and Triple-DES, Proceedings of CRYPTO 1996, LNCS 1109, pp. 237-251, Springer, 1996.
16. 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.
17. 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.