Differential and Rectangle Attacks on Reduced-Round SHACAL-1

Jiqiang Lu[1,⋆], Jongsung Kim[2,3,⋆⋆], Nathan Keller[4,⋆⋆⋆], and Orr Dunkelman[5,†]

[1] Information Security Group, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Jiqiang.Lu@rhul.ac.uk
[2] ESAT/SCD-COSIC, Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
Kim.Jongsung@esat.kuleuven.be
[3] Center for Information Security Technologies(CIST), Korea University
Anam Dong, Sungbuk Gu, Seoul, Korea
joshep@cist.korea.ac.kr
[4] Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, Israel
nkeller@math.huji.ac.il
[5] Computer Science Department, Technion
Haifa 32000, Israel
orrd@cs.technion.ac.il

Abstract. SHACAL-1 is an 80-round block cipher with a 160-bit block size and a key of up to 512 bits. In this paper, we mount rectangle attacks on the first 51 rounds and a series of inner 52 rounds of SHACAL-1, and also mount differential attacks on the first 49 rounds and a series of inner 55 rounds of SHACAL-1. These are the best currently known cryptanalytic results on SHACAL-1 in an one key attack scenario.

Keywords: Block cipher, SHACAL-1, Differential cryptanalysis, Amplified boomerang attack, Rectangle attack.

1 Introduction

The 160-bit block cipher SHACAL-1 was proposed by Handschuh and Naccache [9,10] based on the compression function of the standardized hash function

⋆ This author as well as his work was supported by a Royal Holloway Scholarship and the European Commission under contract IST-2002-507932 (ECRYPT).

⋆⋆ This author was financed by a Ph.D grant of the Katholieke Universiteit Leuven and by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD) (KRF-2005-213-D00077) and supported by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the European Commission through the IST Programme under Contract IST2002507932 ECRYPT.

⋆⋆⋆ This author was supported by the Adams fellowship.

† This author was partially supported by the Israel MOD Research and Technology Unit.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 17–31, 2006.

SHA-1 [20]. It was selected for the second phase of the NESSIE (New European Schemes for Signatures, Integrity, and Encryption) project [18], but was not recommended for the NESSIE portfolio in 2003 because of concerns about its key schedule. Since SHACAL-1 is the compression function of SHA-1 used in encryption mode, there is much significance to investigate its security against different cryptanalytic attacks.

The security of SHACAL-1 against differential cryptanalysis [2] and linear cryptanalysis [17] was first analyzed by the proposers. Subsequently, Nakahara Jr. [19] conducted a statistical evaluation of the cipher. In 2002, Kim *et al.* [15] presented a differential attack on the first 41 rounds of SHACAL-1 with 512 key bits and an amplified boomerang attack on the first 47 rounds of SHACAL-1 with 512 key bits, where the former attack is due to a 30-round differential characteristic with probability 2^{-138}, while the latter attack is based on a 36-round amplified boomerang distinguisher (see Ref. [15] for the two differentials) that was conjectured by the authors to be the longest distinguisher (*i.e.*, the distinguisher with the greatest number of rounds). However, in 2003, Biham *et al.* [5] pointed out that the step for judging whether a final candidate subkey is the right one in the amplified boomerang attacks presented in [15] is incorrect due to a flaw in the analysis on the number of wrong quartets that satisfy the conditions of a right quartet. They then corrected it with the fact that all the subkeys of SHACAL-1 are linearly dependent on the user key. Finally, by converting the Kim *et al.*'s 36-round boomerang distinguisher to a 36-round rectangle distinguisher, Biham *et al.* presented rectangle attacks on the first 47 rounds and two series of inner 49 rounds of SHACAL-1 with 512 key bits. These are the best cryptanalytic results on SHACAL-1 in an one key attack scenario, prior to the work described in this paper. Other cryptanalytic results on SHACAL-1 include the related-key rectangle attacks [7,11,14]; however, these related-key attacks [1] are very difficult or even infeasible to be conducted in most cryptographic applications, though certain current applications may allow for them, say key-exchange protocols [13].

In this paper, we exploit some better differential characteristics than those previously known in SHACAL-1. More specifically, we exploit a 24-round differential characteristic with probability 2^{-50} for rounds 0 to 23 such that we construct a 38-round rectangle distinguisher with probability $2^{-302.3}$. Based on this distinguisher, we mount rectangle attacks on the first 51 rounds and a series of inner 52 rounds of SHACAL-1 with 512 key bits. We also exploit a 34-round differential characteristic with probability 2^{-148} for rounds 0 to 33 and a 40-round differential characteristic with probability 2^{-154} for rounds 30 to 69, which can be used to mount differential attacks on the first 49 rounds and a series of inner 55 rounds of SHACAL-1 with 512 key bits, respectively.

The rest of this paper is organised as follows. In the next section, we briefly describe the SHACAL-1 cipher, the amplified boomerang attack and the rectangle attack. In Sections 3 and 4, we present rectangle and differential attacks on the aforementioned reduced-round versions of SHACAL-1, respectively. Section 5 concludes this paper.

2 Preliminaries

2.1 The SHACAL-1 Cipher

The encryption procedure of SHACAL-1 can be described as follows,

1. The 160-bit plaintext P is divided into five 32-bit words $A_0||B_0||C_0||D_0||E_0$.
2. For $i = 0$ to 79:
   $A_{i+1} = K_i \boxplus ROT_5(A_i) \boxplus f_i(B_i, C_i, D_i) \boxplus E_i \boxplus W_i$,
   $B_{i+1} = A_i$,
   $C_{i+1} = ROT_{30}(B_i)$,
   $D_{i+1} = C_i$,
   $E_{i+1} = D_i$.
3. The ciphertext is $(A_{80}||B_{80}||C_{80}||D_{80}||E_{80})$,

where $\boxplus$ denotes addition modulo 2^{32}, $ROT_i(X)$ represents left rotation of X by i bits, $||$ denotes string concatenation, K_i is the i-th round key, W_i is the i-th round constant,[1] and the function f_i is defined as,

$$f_i(B,C,D) = \begin{cases} f_{\text{if}} = (B\&C)|(\neg B\&D) & 0 \le i \le 19 \\ f_{\text{xor}} = B \oplus C \oplus D & 20 \le i \le 39, 60 \le i \le 79 \\ f_{\text{maj}} = (B\&C)|(B\&D)|(C\&D) & 40 \le i \le 59 \end{cases}$$

where & denotes the bitwise logical AND, $\oplus$ denotes the bitwise logical exclusive OR (XOR), $\neg$ denotes the complement, and $|$ represents the bitwise OR operations.

The key schedule of SHACAL-1 takes as input a variable length key of up to 512 bits; Shorter keys can be used by padding them with zeros to produce a 512-bit key string, however, the proposers recommend that the key should not be shorter than 128 bits. The 512-bit user key K is divided into sixteen 32-bit words $K_0, K_1, \cdots, K_{15}$, which are the round keys for the first 16 rounds. Each of the remaining round keys is generated as $K_i = ROT_1(K_{i-3} \oplus K_{i-8} \oplus K_{i-14} \oplus K_{i-16})$.

2.2 Amplified Boomerang and Rectangle Attacks

Amplified boomerang attack [12] and rectangle attack [3] are both variants of the boomerang attack [21]. As a result, they share the same basic idea of using two short differentials with larger probabilities instead of a long differential with a smaller probability.

Amplified boomerang attack treats a block cipher $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ as a cascade of two sub-ciphers $E = E^1 \circ E^0$. It assumes that there exist two differentials: one differential $\alpha \to \beta$ through E^0 with probability p (*i.e.*, $Pr[E^0(X) \oplus E^0(X^*) = \beta | X \oplus X^* = \alpha] = p$), and the other differential $\gamma \to \delta$ through E^1 with probability q (*i.e.*, $Pr[E^1(X) \oplus E^1(X^*) = \delta | X \oplus X^* = \gamma] = q$), with p and q satisfying $p \cdot q \gg 2^{-n/2}$. Two pairs of plaintexts $(P_1, P_2 = P_1 \oplus \alpha)$ and $(P_3, P_4 = P_3 \oplus \alpha)$ is called a right quartet if the following three conditions hold:

[1] We note that this is the opposite to Refs. [9,10,20]; however, we decide to stick to the common notation K_i as a round subkey.

C1: $E^0(P_1) \oplus E^0(P_2) = E^0(P_3) \oplus E^0(P_4) = \beta$;
C2: $E^0(P_1) \oplus E^0(P_3) = E^0(P_2) \oplus E^0(P_4) = \gamma$;
C3: $E^1(E^0(P_1)) \oplus E^1(E^0(P_3)) = E^1(E^0(P_2)) \oplus E^1(E^0(P_4)) = \delta$.

If we take N pairs of plaintexts with the difference α, then we have approximately $N \cdot p$ pairs with the output difference β after E^0, which generate about $\frac{(N \cdot p)^2}{2}$ candidate quartets. Assuming that the intermediate values after E^0 distribute uniformly over all possible values, we get $E^0(P_1) \oplus E^0(P_3) = \gamma$ with probability 2^{-n}. Once this occurs, $E^0(P_2) \oplus E^0(P_4) = \gamma$ holds as well, as $E^0(P_2) \oplus E^0(P_4) = E^0(P_1) \oplus E^0(P_2) \oplus E^0(P_3) \oplus E^0(P_4) \oplus E^0(P_1) \oplus E^0(P_3) = \gamma$. As a result, the expected number of right quartets is about $\frac{(N \cdot p)^2}{2} \cdot 2^{-n} \cdot q^2 = N^2 \cdot 2^{-n-1} \cdot (p \cdot q)^2$. On the other hand, for a random cipher, the expected number of right quartets is approximately $N^2 \cdot 2^{-2n}$. Therefore, if $p \cdot q > 2^{-n/2}$ and N is sufficiently large, the amplified boomerang distinguisher can effectively distinguish between E and a random cipher with an enough bias.

Rectangle attack achieves advantage over an amplified boomerang attack by allowing β to take any possible value β' in E^0 and γ to take any possible value γ' in E^1, as long as $\beta' \neq \gamma'$. Starting with N pairs of plaintexts with the difference α, the expected number of right quartets is about $N^2 \cdot (\widehat{p} \cdot \widehat{q})^2 \cdot 2^{-n}$, where $\widehat{p} = (\sum_{\beta'} Pr^2(\alpha \to \beta'))^{\frac{1}{2}}$, $\widehat{q} = (\sum_{\gamma'} Pr^2(\gamma' \to \delta))^{\frac{1}{2}}$.

3 Rectangle Attacks on Reduced-Round SHACAL-1

We exploit a 24-round differential characteristic with probability 2^{-50} for rounds 0–23: $(e_{29}, 0, 0, 0, e_{2,7}) \to (e_{14,29}, e_{9,31}, e_2, e_{29}, 0)$. Table 1 describes the full differential.

- By combining the 24-round differential with a differential composed of rounds 24–35 of the second differential of [15] (which has probability 2^{-20} in these rounds), a 36-round distinguisher with probability $2^{-300} (= (2^{-50} \cdot 2^{-20})^2 \cdot 2^{-160})$ is obtained, gaining a factor of 2^{12} over the probability of the most powerful currently known 36-round one due to Kim *et al.*.
- By combining the 24-round differential with a differential composed of rounds 23–35 of the second differential of [15] (which has probability 2^{-24} in these rounds), a 37-round distinguisher with probability $2^{-308} (= (2^{-50} \cdot 2^{-24})^2 \cdot 2^{-160})$ is obtained.
- By combining the 24-round differential with a differential composed of rounds 21–34 of the second differential of [15] (which has probability 2^{-27} in these rounds), a 38-round distinguisher with probability $2^{-314} (= (2^{-50} \cdot 2^{-27})^2 \cdot 2^{-160})$ is obtained.

These amplified boomerang distinguishers can be used to mount amplified boomerang attacks on certain reduced-round versions of SHACAL-1 with different lengths of user keys. Nevertheless, due to the nature that all the possible β and γ (as long as they are different) can be used in a rectangle distinguisher,

Table 1. A 24-round differential with probability 2^{-50} for Rounds 0 to 23

Round(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Prob.	Round(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Prob.
input	e_{29}	0	0	0	$e_{2,7}$	2^{-2}	13	0	e_8	e_1	0	0	2^{-2}
1	e_7	e_{29}	0	0	0	2^{-2}	14	0	0	e_6	e_1	0	2^{-2}
2	e_{12}	e_7	e_{27}	0	0	2^{-3}	15	0	0	0	e_6	e_1	2^{-2}
3	e_{17}	e_{12}	e_5	e_{27}	0	2^{-4}	16	e_1	0	0	0	e_6	2^{-1}
4	e_{22}	e_{17}	e_{10}	e_5	e_{27}	2^{-4}	17	0	e_1	0	0	0	2^{-1}
5	0	e_{22}	e_{15}	e_{10}	e_5	2^{-4}	18	0	0	e_{31}	0	0	2^{-1}
6	e_5	0	e_{20}	e_{15}	e_{10}	2^{-3}	19	0	0	0	e_{31}	0	2^{-1}
7	0	e_5	0	e_{20}	e_{15}	2^{-3}	20	0	0	0	0	e_{31}	1
8	e_{15}	0	e_3	0	e_{20}	2^{-2}	21	e_{31}	0	0	0	0	2^{-1}
9	0	e_{15}	0	e_3	0	2^{-2}	22	e_4	e_{31}	0	0	0	2^{-1}
10	0	0	e_{13}	0	e_3	2^{-2}	23	$e_{9,31}$	e_4	e_{29}	0	0	2^{-3}
11	e_3	0	0	e_{13}	0	2^{-2}	*output*	$e_{14,29}$	$e_{9,31}$	e_2	e_{29}	0	/
12	e_8	e_3	0	0	e_{13}	2^{-2}							

these amplified boomerang distinguishers can be converted into rectangle distinguishers so that the resultant rectangle attacks can work more efficiently. Here, we will just present rectangle attacks on SHACAL-1 with 512 key bits based on the 38-round distinguisher.

3.1 Attacking Rounds 0 to 50

Let $E_f \circ E^1 \circ E^0$ be the 51-round SHACAL-1 with 512 key bits, where E^0 denotes rounds 0 to 23, E^1 denotes rounds 24 to 37, and E_f denotes rounds 38 to 50.

To compute $\widehat{p}$ (resp., $\widehat{q}$) (defined in Section 2.2) in such an attack, we need to summarize all the possible output differences β' for the input difference α through E^0 (resp., all the possible input differences γ' having an output difference δ through E^1), which is computationally infeasible. As a countermeasure, we can count as many such possible differentials as we can.

For simplicity, we compute $\widehat{p}$ by just counting the 24-round differentials that only have variable output differences $(\Delta A_{24}, e_{9,31}, e_2, e_{29}, 0)$ compared with the 24-round differential, where ΔA_{24} is an element from the set $\{(\overbrace{0, \cdots, 0, \underbrace{1, \cdots, 1}_{m}}^{2},$ $1, \overbrace{0, \cdots, 0, \underbrace{1, \cdots, 1}_{j}}^{14}, 1, \overbrace{0, \cdots, 0, \underbrace{1, \cdots, 1}_{k}}^{9}, 0, 0, 0, 0, 0)|0 \le m \le 2, 0 \le j \le 14, 0 \le k \le 9\}$, for such an output difference with the form is possible for the input difference $(e_{9,31}, e_4, e_{29}, 0, 0)$ to round 23. It was shown in [16] that the following Theorem 1 holds for the addition difference,

Theorem 1. *[16] Given three 32-bit differences ΔX, ΔY and ΔZ. If the probability $Prob[(\Delta X, \Delta Y) \xrightarrow{\boxplus} \Delta Z] > 0$, then*

$$Prob[(\Delta X, \Delta Y) \xrightarrow{\boxplus} \Delta Z] = 2^s,$$

where the integer s is given by $s = \#\{i|0 \le i \le 30, not((\Delta X)_i = (\Delta Y)_i = (\Delta Z)_i)\}$.

Thus, we can compute a loose lower bound $\widehat{p} = 2^{-49.39}$ by only counting the 46 differentials with $k + j + m \le 5$; when $k + j + m > 5$ the contribution is negligible. We note that the more the counted possible differentials, the better the resultant $\widehat{p}$, but according to our results the improvement is negligible.

Biham *et al.* [5] got a lower bound $\widehat{q}$ in their attack as $\widehat{q} = 2^{-30.28}$ by only changing the first one or two rounds in the Kim *et al.*'s second differential. Since our 38-round distinguisher just uses the first 14 rounds from round 21 to 34 in the Kim *et al.*'s second differential, throwing round 35 away, therefore, $2^{-26.28}(= 2^{-30.28} \cdot 2^4)$ is the right value for the $\widehat{q}$ in our attack.

Now, we conclude that the distinguisher holds a lower bound probability $2^{-311.34}(\approx (2^{-49.39} \cdot 2^{-26.28})^2 \cdot 2^{-160})$. However, we can adopt the following two techniques to further reduce the complexity of the attack:

T1) Fix the four fixed bits $a_9 = a_9^* = 0$, $b_9 = b_9^* = 0$, $b_{31} = b_{31}^* = 0$ and $c_{29} = c_{29}^* = 0$ in any pair of plaintexts $P = (A, B, C, D, E)$ and $P^* = (A^*, B^*, C^*, D^*, E^*)$, where x_i is the i-th bit of X. This increases the probability of the characteristic in the first round by a factor of 4. Thus, a lower bound probability $2^{-47.39}(= 2^2 \cdot 2^{-49.39})$ is obtained for the above 46 possible 24-round differentials with such four bits fixed in any pair.

T2) Count many possible 14-round differentials $\gamma' \to \delta'$ for each input difference γ' to round 24 in our distinguisher. For expediency, we count those 14-round differentials that only have variable output differences $(\Delta A_{38}, e_{9,31}, e_2, e_{29}, 0)$ compared with the 14-round differential from round 21 to 34 in the Kim *et al.*'s second differential. In our observation on this 1-round difference, there are at least two possible ΔA_{38} (*i.e.*, $e_{29}, e_{14,29}$) with probability 2^{-3}, four possible ΔA_{38} (*i.e.*, $e_{5,14,29}, e_{14,15,29}, e_{14,29,30}, e_{14,29,30,31}$) with probability 2^{-4}, and seven possible ΔA_{38} (*i.e.*, $e_{5,14,29,30,31}, e_{14,15,29,30,31}, e_{5,6,14,29}, e_{5,14,15,29}, e_{14,15,16,29}, e_{5,14,29,30}, e_{14,15,29,30}$) with probability 2^{-5}. We denote the set of these 13 differences by $\mathcal{S}$. Thus, these 13 possible 14-round differentials hold a lower bound probability of $2^{-23.76}(\approx 2 \cdot 2^{-26.28} + 4 \cdot 2^{-27.28} + 7 \cdot 2^{-28.28})$.

Finally, this rectangle distinguisher holds a lower bound probability $2^{-302.3}(\approx (2^{-47.39} \cdot 2^{-23.76})^2 \cdot 2^{-160})$ for the right key, while it now holds with a probability of $2^{-312.6}(\approx (2^{-160} \cdot (2 + 4 + 7))^2)$ for a wrong key. The number of available plaintext pairs decreases to 2^{155} due to the four fixed bits.

Consequently, we can apply this rectangle distinguisher to break the first 51 rounds of SHACAL-1.

Attack Procedure

1. Choose $2^{152.65}$ pairs of plaintexts with difference $\alpha = (e_{29}, 0, 0, 0, e_{2,7})$ and four fixed bits as described above: (P_i, P_i'), for $i = 1, 2, \cdots, 2^{152.65}$. Ask for their encryption under 51-round SHACAL-1 to obtain their corresponding ciphertext pairs (C_i, C_i'). The $2^{152.65}$ pairs generate about $2^{305.3}$ candidate quartets $((P_{i_1}, P_{i_1}'), (P_{i_2}, P_{i_2}'))$, where $1 \le i_1, i_2 \le 2^{152.65}$.

2. Guess a 352-bit key K_f for rounds 40 to 50 in E_f, do follows,
   2.1 Partially decrypt all the ciphertext pairs (C_i, C'_i) with K_f to get their intermediate values just before round 40: $(E^{-1}_{K_f}(C_i), E^{-1}_{K_f}(C'_i))$. Then, for each quartet $((C_{i_1}, C'_{i_1}), (C_{i_2}, C'_{i_2}))$, check if both the two 96-bit differences in words C, D and E positions of $E^{-1}_{K_f}(C_{i_1}) \oplus E^{-1}_{K_f}(C_{i_2})$ and $E^{-1}_{K_f}(C'_{i_1}) \oplus E^{-1}_{K_f}(C'_{i_2})$ belong to the set $\{(u, e_{7,29}, e_2) | ROT_{30}(u) \in \mathcal{S}\}$. If the number of the quartets passing this test is greater than or equal to 6, then go to Step 2.2; Otherwise, repeat Step 2 with another guess for K_f.
   2.2 Guess a 32-bit subkey K_{39} for round 39, and then decrypt each remaining quartet $((E^{-1}_{K_f}(C_{i_1}), E^{-1}_{K_f}(C'_{i_1})), (E^{-1}_{K_f}(C_{i_2}), E^{-1}_{K_f}(C'_{i_2})))$ with K_{39} to get their intermediate values just before round 39: $((E^{-1}_{K_{39}}(E^{-1}_{K_f}(C_{i_1})), E^{-1}_{K_{39}}(E^{-1}_{K_f}(C'_{i_1}))), (E^{-1}_{K_{39}}(E^{-1}_{K_f}(C_{i_2})), E^{-1}_{K_{39}}(E^{-1}_{K_f}(C'_{i_2}))))$. We denote them by $((X_{i_1}, X'_{i_1}), (X_{i_2}, X'_{i_2}))$. Finally, check if both the two 128-bit differences in words B, C, D and E positions of $X_{i_1} \oplus X_{i_2}$ and $X'_{i_1} \oplus X'_{i_2}$ belong to the set $\{(u, e_{7,29}, e_2, e_{29})\}$. If the number of the quartets passing this test is greater than or equal to 6, then go to Step 2.3; Otherwise, repeat this step with another guess for K_{39} (If all the values of K_{39} fail, then go to Step 2).
   2.3 Guess a 32-bit subkey K_{38} for round 38, and then decrypt each remaining quartet $((X_{i_1}, X'_{i_1}), (X_{i_2}, X'_{i_2}))$ with K_{38} to get their intermediate values just before round 38: $((E^{-1}_{K_{38}}(X_{i_1}), E^{-1}_{K_{38}}(X'_{i_1})), (E^{-1}_{K_{38}}(X_{i_2}), E^{-1}_{K_{38}}(X'_{i_2})))$. We denote them by $((\overline{X}_{i_1}, \overline{X'}_{i_1}), (\overline{X}_{i_2}, \overline{X'}_{i_2}))$. Finally, check if both the two 160-bit differences $\overline{X}_{i_1} \oplus \overline{X}_{i_2}$ and $\overline{X'}_{i_1} \oplus \overline{X'}_{i_2}$ belong to the set $\{(u, e_{7,29}, e_2, e_{29}, 0)\}$. If the number of the quartets passing this test is greater than or equal to 6, then record (K_f, K_{38}, K_{39}) and go to Step 3; Otherwise, repeat this step with another guess for K_{38} (If all the values of K_{38} fail, then go to Step 2.2; If all the values of K_{39} fail, then go to Step 2).
3. For a suggested (K_{38}, K_{39}, K_f), exhaustively search the remaining 96 key bits using trial encryption. Three known pairs of plaintexts and ciphertexts are enough for this trial process. If a 512-bit key is suggested, output it as the master key of the 51-round SHACAL-1. Otherwise, go to Step 2.

This attack requires $2^{153.65}$ chosen plaintexts. The required memory for this attack is dominated by the ciphertext pairs, which is about $2^{153.65} \cdot 20 \approx 2^{157.97}$ memory bytes.

The time complexity of Step 1 is $2^{153.65}$ 51-round SHACAL-1 encryptions; The time complexity of Step 2.1 is dominated by the partial decryptions, which is about $2^{352} \cdot 2^{153.65} \cdot \frac{11}{51} \approx 2^{503.44}$. In Step 2.1, since the probability that a quartet meets the filtering condition in this step is $(\frac{13}{2^{96}})^2 \approx 2^{-184.6}$, the expected number of the quartets passing the test for each subkey candidate is $2^{305.3} \cdot 2^{-184.6} \approx 2^{120.7}$, and it is evident that the probability that the number of quartets passing the test for a wrong subkey is no less than 6 is about 1. Thus, almost all the 2^{352} subkeys pass through Step 2.1. In Step 2.2, the time complexity is about $2^{352} \cdot 2^{32} \cdot 2^{120.7} \cdot 4 \cdot \frac{1}{51} \approx 2^{501.03}$. In this step, since the probability that a

remaining quartet meets the filtering condition in this step is $2^{-32} \cdot 2^{-32} \approx 2^{-64}$, the expected number of the quartets passing the test for each subkey candidate is $2^{120.7} \cdot 2^{-64} \approx 2^{56.7}$. Again, almost all the 2^{384} subkeys pass through Step 2.2. In Step 2.3, the time complexity is about $2^{384} \cdot 2^{32} \cdot 2^{56.7} \cdot 4 \cdot \frac{1}{51} \approx 2^{469.03}$. In this step, since the probability that a remaining quartet meets the filtering condition in this step is also 2^{-64}, the expected number of the quartets passing the test for each subkey candidate is $2^{56.7} \cdot 2^{-64} \approx 2^{-7.3}$, and the probability that the number of quartets passing the test for a wrong subkey is no less than 6 is about $\sum_{i=6}^{2^{56.7}} (\binom{2^{56.7}}{i} \cdot (2^{-64})^i \cdot (1-2^{-64})^{2^{56.7}-i}) \approx 2^{-53.29}$. Thus, on average, about $2^{416} \cdot 2^{-53.29} = 2^{362.71}$ subkeys pass through Step 2.3, which result in $2^{362.71} \cdot 2^{96} \approx 2^{458.71}$ 51-round encryptions in Step 3. Therefore, this attack totally requires about $2^{153.65} + 2^{503.44} + 2^{501.03} + 2^{469.03} + 2^{458.71} \approx 2^{503.7}$ encryptions.

Since the probability that a wrong 512-bit key is suggested in Step 3 is about $2^{-480} (= 2^{-160 \cdot 3})$, the expected number of suggested wrong 512-bit keys is about $2^{-480} \cdot 2^{458.71} \approx 2^{-21.29}$, which is quite low. While the expected number of quartets passing the difference test in Step 2.5 for the right key is 8 ($= 2^{305.3} \cdot 2^{-302.3}$), and the probability that the number of quartets passing the difference test in Step 2.5 for the right subkey is no less than 6 is about $\sum_{i=6}^{2^{305.3}} (\binom{2^{305.3}}{i} \cdot (2^{-302.3})^i \cdot (1-2^{-302.3})^{2^{305.3}-i}) \approx 0.81$. Therefore, with a probability of 0.81, we can break the 51-round SHACAL-1 with 512 key bits by using the amplified boomerang attack, faster than an exhaustive search.

3.2 Attacking Rounds 28–79

A generic key recovery algorithm based on a rectangle distinguisher was presented by Biham *et al.* in [4] and then updated in [6] recently, which treats a block cipher $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ as $E = E_f \circ E^1 \circ E^0 \circ E_b$, where E^0 and E^1 constitute the rectangle distinguisher, while E_b and E_f are some rounds before and after the rectangle distinguisher, respectively. In this subsection, we will use their results to break the 52 rounds from round 28 to 79 of SHACAL-1.

To apply the generic attack procedure [4], we need to determine the following six parameters:

- m_b: the number of subkey bits in E_b to be attacked.
- m_f: the number of subkey bits in E_f to be attacked.
- r_b: the number of bits that are active or can be active before the attacked round, given that a pair has the difference α at the entrance of the rectangle distinguisher.
- r_f: the number of bits that are active or can be active after the attacked round, given that a pair has the difference δ at the output of the rectangle distinguisher.
- 2^{t_b}: the number of possible differences before the attacked round, given that a pair has the difference α at the entrance of the rectangle distinguisher.
- 2^{t_f}: the number of possible differences after the attacked round, given that a pair has the difference δ at the output of the rectangle distinguisher.

Our attack is applied in the backward direction, that is to say, it is a chosen ciphertext attack. Anyway, as the data requirement of the attack is the entire code book, it can be easily used as a known plaintext attack.

Let E_b denote round 79, E^0 denote rounds 64 to 78, E^1 denote rounds 41 to 63, and E_f denote rounds 38 to 40. We first describe the two differentials to be used in this rectangle distinguisher. By cyclically rotating the last 23-round differential in the 24-round differential to the right by 9 bit positions, we can get a 23-round differential with probability $q = 2^{-49}$: $(e_{30}, e_{20}, 0, 0, 0) \rightarrow (e_{5,20}, e_{0,22}, e_{25}, e_{20}, 0)$. This 23-round differential is used in E^1, while the Kim *et al.*'s second differential with probability $p = 2^{-31}$ in [15] is used in E^0. Similarly, we can compute a lower bound probability $\widehat{q} = 2^{-47.77}$ for the 23-round differentials that only have variable output differences compared with the 23-round differential described above. As mentioned before, a lower bound $\widehat{p} = 2^{-30.28}$ has been got by only changing the first one or two rounds in the Kim *et al.*'s second differential. Therefore, this 38-round rectangle distinguisher holds at least a probability of $2^{-316.1} (\approx (2^{-47.77} \cdot 2^{-30.28})^2 \cdot 2^{-160})$ for the right key, while it holds probability 2^{-320} for a wrong key.

As we attack one round (*i.e.*, round 79) before the distinguisher, we can compute m_b, r_b, and t_b as follows: There is only one 32-bit subkey K_{79} in E_b, therefore, $m_b = 32$. A pair with a difference $(e_{9,19,29,31}, e_{14,29}, e_{7,29}, e_2, e_{29})$ before round 79 has a difference with the form $(R, e_{9,19,29,31}, e_{12,27}, e_{7,29}, e_2)$ after round 79. Obviously, the bit differences in the three least significant bits of R will definitely be 0, while the bit differences in the other 29 bit positions will be variable. As a result, $r_b = 29 + 4 + 2 + 2 + 1 = 38$. In our analysis, R has exactly 15648 possible values. So, $t_b = log_2^{15648} \approx 13.9$.

There are three rounds (*i.e.*, rounds 38 to 40) after the distinguisher, thus $m_f = 96$. A pair that has a difference $(e_{30}, e_{20}, 0, 0, 0)$ before round 41 has a difference with the form $(e_{20}, 0, 0, 0, S)$ before round 40, where S has the following 12 possible values: $e_{25,30}$, $e_{25,30,31}$, $e_{25,26,30}$, $e_{25,26,30,31}$, $e_{25,26,27,30}$, $e_{25,26,27,30,31}$, $e_{25,26,27,28,30}$, $e_{25,26,27,28,30,31}$, $e_{25,26,27,28,29,30}$, $e_{25,26,27,28,29,30,31}$, $e_{25,26,27,28,29,31}$, $e_{25,26,27,28,29}$. These differences can be reached from a difference with the form $(0, 0, 0, S, T)$ before round 39, where T has bits 20 to 31 active, of which bits 21 to 24 must take one of the five possible values $1_x, 3_x, 7_x, F_x$, and $1F_x$ according to the carry, while bits 25 to 31 cannot be predicted as they all depend on the exact value of S. This set of differences can be caused by differences with the form $(0, 0, S, T, U)$ before round 38, where U has bits 20 to 31 active. Thus, $r_f = 7 + 12 + 12 = 31$, and there are at most $12 \cdot (5 \cdot 2^7) \cdot 2^{12} = 31457280$ possible differences with the form $(0, 0, S, T, U)$ before round 38, so $t_f = log_2(31457280) \approx 24.9$.

Assigning these parameters to the Biham *et al.*'s generic attack procedure leads to a rectangle attack on rounds 38 to 79. Then, with an exhaustive key search for the remaining 10 rounds, we can attack 52-round SHACAL-1. The attack procedure is summarized as follows.

Attack Procedure

(a) Based on the above 38-round rectangle distinguisher, apply the Biham *et al.*'s generic attack procedure [6] on the 42 rounds from round 38 to 79 of

SHACAL-1. Output the four 32-bit subkey candidates for rounds 38, 39, 40 and 79 with the maximal counter number.

(b) Find the ten 32-bit subkeys for rounds 28 to 37 using an exhaustive search.

According to [6], the time complexity of Step (a) in our attack is about $2^{m_b+m_f+1} + N + N^2 \cdot (2^{r_f-n-1} + 2^{t_f-n-1} + 2^{2t_f+2r_b-2n-3} + 2^{m_b+t_b+2t_f-2n-2} + 2^{m_f+t_f+2t_b-2n-2}) = 2^{129} + 2^{160} + 2^{320} \cdot (2^{31-161} + 2^{24.9-161} + 2^{2\cdot 24.9+2\cdot 38-323} + 2^{32+13.9+2\cdot 24.9-322} + 2^{96+24.9+2\cdot 13.9-322}) \approx 2^{190.02}$ memory accesses. In Step (b), by guessing the subkeys of rounds 28 to 37, it is possible to partially encrypt all the plaintexts and then apply the previous Step (a). Each subkey guess requires 2^{160} partial encryptions and $2^{190.02}$ memory accesses, therefore, the total time complexity is $2^{320} \cdot 2^{160} \cdot \frac{10}{52} \approx 2^{477.6}$ 52-round SHACAL-1 encryptions and $2^{320} \cdot 2^{190.02} = 2^{510.02}$ memory accesses.

Note: There exists another attack on the 52 rounds from round 28 to 79, which is composed of a similar rectangle attack on rounds 35 to 77, followed by an exhaustive search on the 288-bit subkeys of rounds 28 to 34, 78 and 79. Let E_b denote round 77, E^0 denote rounds 64 to 76, E^1 denote rounds 38 to 63, and E_f denote rounds 35 to 37. For E^0 we use the 13-round differential composed of rounds 23 to 35 in the second differential of [15], which holds probability $p = 2^{-24}$. The 26-round differential $(0, 0, e_{19,24}, e_{14,19,24}, e_{14}) \rightarrow (e_{14,31}, e_{16,26}, e_{19}, e_{14}, 0)$ with probability $q = 2^{-55}$ is used in E^1, which is obtained by cyclically rotating the 24-round differential to the left by 17 bit positions and appending two more rounds before the input. We computed a lower bound on the related probabilities $\widehat{p} = 2^{-23.48}$ and $\widehat{q} = 2^{-53.77}$. Therefore, the distinguisher holds at least a probability of $2^{-314.5} (\approx (2^{-53.77} \cdot 2^{-23.48})^2 \cdot 2^{-160})$ for the right key, while it holds probability 2^{-320} for a wrong key. As before we computed that $m_b = 32$, $r_b = 38$, $t_b = 13.9$, $m_f = 96$, $r_f = 12+17+18 = 47$, and $t_f = log_2^(9 \cdot 64 \cdot 12 \cdot 2^{13} \cdot 2^{18}) \approx 43.8$. Finally, we can break 52-round SHACAL-1. According to [6], the data complexity is $N = 2^{\frac{n}{2}+2}/(\widehat{p} \cdot \widehat{q}) = 2^{80+53.77+23.48+2} = 2^{159.25}$ chosen plaintexts/ciphertexts with difference $(e_{9,19,29,31}, e_{14,29}, e_{7,29}, e_2, e_{29})$ before round 76, however, this cannot be guaranteed if we start with chosen ciphertexts. Alternatively, we apply the attack as a known plaintext attack. With $2^{159.625}$ known plaintexts, we can get $2^{318.25}$ pairs, of which about $2^{158.25} (= 2^{318.25} \cdot 2^{-160})$ would have the desired difference. This attack requires $2^{288} \cdot 2^{159.625} \cdot \frac{9}{52} \approx 2^{445.1}$ encryptions and the time complexity is about $2^{288} \cdot [2^{m_b+m_f+1} + N + N^2 \cdot (2^{r_f-n-1} + 2^{t_f-n-1} + 2^{2t_f+2r_b-2n-3} + 2^{m_b+t_b+2t_f-2n-2} + 2^{m_f+t_f+2t_b-2n-2})] = 2^{288} \cdot [2^{129} + 2^{159.25} + 2^{318.5} \cdot (2^{-114} + 2^{-117.2} + 2^{-157.4} + 2^{-185} + 2^{-147.4}) \approx 2^{204.65}] = 2^{492.65}$ memory accesses.

4 Differential Attacks on Reduced-Round SHACAL-1

The 24-round differential in Table 1 can be extended to a 30-round differential $(e_{29}, 0, 0, 0, e_{2,7}) \rightarrow (e_{0,4,12,17,24,25,27,29}, e_{7,17,19,31}, e_{0,5,15,27,30}, e_{5,17,25,27,29}, e_{2,5,22,27})$ with probability 2^{-93}, which has a significantly higher probability than the

longest currently known (30-round) differential with probability 2^{-138} due to Kim *et al.*. More importantly, it can be extended to as long as a 34-round differential $(e_{29}, 0, 0, 0, e_{2,7}) \rightarrow (e_{0,5,7,12,13,15,17,20,28,29}, e_{5,7,9,23,25,29}, e_{3,12,15,18,20,25,27,30}, e_{5,7,13,15,17,23,25,29}, e_{2,10,15,22,23,25,27,30})$ with probability 2^{-148}.

These differentials with different rounds can be used to attack different reduced round variants of SHACAL-1. Here, we just present the differential attack on SHACAL-1 with 512 key bits based on the 34-round differential.

4.1 Attacking Rounds 15–69

The 34-round differential can be applied to the 34 rounds from round 40 to 73, due to the differential distribution of the two functions f_{if} and f_{maj}. Then, by appending 10 more rounds before round 40 and removing the last 4 rounds in the above 34-round differential, we exploit a 40-round differential characteristic with probability 2^{-154} for rounds 30 to 69: $(e_{4,8,11,13,16}, e_{3,8,11,13,31}, e_{1,6,11,16,21,29,31}, e_{1,4,8,11,13,16,21}, e_{3,9,11,13,16,18,21,29,31}) \rightarrow (e_{0,4,12,17,24,25,27,29}, e_{7,17,19,31}, e_{0,5,15,27,30}, e_{5,17,25,27,29}, e_{2,5,22,27})$.

This 40-round differential can be used to mount a chosen ciphertext attack on the 55 rounds from round 15 to 69. By counting the 30 possible 40-round differentials that only have variable input differences $(e_{4,8,11,13,16}, e_{3,8,11,13,31}, e_{1,6,11,16,21,29,31}, e_{1,4,8,11,13,16,21}, \Delta E_{30})$ compared with the 40-round differential described above (where ΔE_{30} are shown in Table 2), we can conclude these 40-round differentials hold a lower bound probability $2^{-150} (= 2 \cdot 2^{-154} + 28 \cdot 2^{-155})$ for a right key, while they hold a probability of $2^{-155.09} (\approx 30 \cdot 2^{-160})$ for a wrong key. Consequently, we can break the 55-round SHACAL-1 as follows.

Table 2. Possible input differences ΔE_{30} in Round 30 with their respective probabilities

Prob.	ΔE_{30}
2^{-154}	$e_{3,9,11,13,16,18,21,29,31}$, $e_{3,4,9,11,13,16,18,21,29,31}$
2^{-155}	$e_{3,4,5,9,11,13,16,18,21,29,31}$, $e_{3,5,9,11,13,16,18,21,29,31}$, $e_{3,5,6,9,11,13,16,18,21,29,31}$,
	$e_{3,4,5,6,9,11,13,16,18,21,29,31}$, $e_{3,7,9,11,13,16,18,21,29,31}$, $e_{3,4,7,9,11,13,16,18,21,29,31}$,
	$e_{3,9,10,11,13,16,18,21,29,31}$, $e_{3,4,9,10,11,13,16,18,21,29,31}$, $e_{3,9,10,13,16,18,21,29,31}$,
	$e_{3,4,9,10,13,16,18,21,29,31}$, $e_{3,9,11,12,13,16,18,21,29,31}$, $e_{3,4,9,11,12,13,16,18,21,29,31}$,
	$e_{3,9,11,12,16,18,21,29,31}$, $e_{3,4,9,11,12,16,18,21,29,31}$, $e_{3,9,11,13,14,16,18,21,29,31}$,
	$e_{3,4,9,11,13,14,16,18,21,29,31}$, $e_{3,9,11,13,16,17,18,21,29,31}$, $e_{3,4,9,11,13,16,17,18,21,29,31}$,
	$e_{3,9,11,13,16,17,21,29,31}$, $e_{3,4,9,11,13,16,17,21,29,31}$, $e_{3,9,11,13,16,18,19,21,29,31}$,
	$e_{3,4,9,11,13,16,18,19,21,29,31}$, $e_{3,9,11,13,16,18,21,22,29,31}$, $e_{3,4,9,11,13,16,18,21,22,29,31}$,
	$e_{3,9,11,13,16,18,21,29,30,31}$, $e_{3,4,9,11,13,16,18,21,29,30,31}$, $e_{3,9,11,13,16,18,21,29,30}$,
	$e_{3,4,9,11,13,16,18,21,29,30}$

Attack Procedure

1. Choose 2^{153} pairs of ciphertexts with difference $(e_{0,4,12,17,24,25,27,29}, e_{7,17,19,31}, e_{0,5,15,27,30}, e_{5,17,25,27,29}, e_{2,5,22,27})$: (C_i, C_i'), for $i = 1, \cdots, 2^{153}$. Decrypt them to get their corresponding plaintext pairs (P_i, P_i').

2. Guess a 352-bit key K_f for rounds 15 to 25, do follows,

   2.1 Partially encrypt each pair (P_i, P_i') using K_f to get their intermediate values just after round 25: $(E_{K_f}(P_i), E_{K_f}(P_i'))$. Then, check if the 32-bit difference ΔA_{26} in $E_{K_f}(P_i) \oplus E_{K_f}(P_i')$ belongs to $\{ROT_2(\Delta E_{30}) | \Delta E_{30}$ *are those in Table* 2$\}$. If the number of the pairs (P_i, P_i') passing this test is greater than or equal to 6, then record K_f and all the qualified pairs (P_i, P_i') and go to Step 2.2; Otherwise, repeat this step with another K_f.

   2.2 Guess a 32-bit subkey K_{26} for round 26, then partially encrypt each pair $(E_{K_f}(P_i), E_{K_f}(P_i'))$ with K_{26} to get their intermediate values just after round 26. We denote these values by (X_i, X_i'). Finally, check if the 64-bit difference $(\Delta A_{27}, \Delta B_{27})$ in $X_i \oplus X_i'$ belongs to $\{(e_{3,6,10,13,15,18,23}, ROT_2(\Delta E_{30}))\}$. If the number of the pairs $(E_{K_f}(P_i), E_{K_f}(P_i'))$ passing this test is greater than or equal to 6, then record (K_f, K_{26}) and all the qualified pairs (X_i, X_i') and go to Step 2.3; Otherwise, repeat this step with another K_{26}.

   2.3 Guess a 32-bit subkey K_{27} for round 27, then partially encrypt each remaining pair (X_i, X_i') with K_{27} to get their intermediate values just after round 27. We denote them by $(\overline{X}_i, \overline{X}_i')$. Finally, check if the 96-bit difference $(\Delta A_{28}, \Delta B_{28}, \Delta C_{28})$ in $\overline{X}_i \oplus \overline{X}_i'$ belongs to the set $\{(e_{1,3,8,13,18,23,31}, e_{3,6,10,13,15,18,23}, ROT_2(\Delta E_{30}))\}$. If the number of the pairs (X_i, X_i') passing this test is greater than or equal to 6, then record (K_f, K_{26}, K_{27}) and all the qualified pairs $(\overline{X}_i, \overline{X}_i')$ and go to Step 2.4; Otherwise, repeat this step with another K_{27}.

   2.4 Guess a 32-bit subkey K_{28} for round 28, then partially encrypt each remaining pair $(\overline{X}_i, \overline{X}_i')$ with K_{28} to get their intermediate values just after round 28. We denote them by $(\widehat{X}_i, \widehat{X}_i')$. Finally, check if the 128-bit difference $(\Delta A_{29}, \Delta B_{29}, \Delta C_{29}, \Delta D_{29})$ in $\widehat{X}_i \oplus \widehat{X}_i'$ belongs to $\{(e_{3,8,11,13,31}, e_{1,3,8,13,18,23,31}, e_{3,6,10,13,15,18,23}, ROT_2(\Delta E_{30}))\}$. If the number of the pairs $(\overline{X}_i, \overline{X}_i')$ passing this test is greater than or equal to 6, then record $(K_f, K_{26}, K_{27}, K_{28})$ and all the qualified pairs $(\widehat{X}_i, \widehat{X}_i')$ and go to Step 2.5; Otherwise, repeat this step with another K_{28}.

   2.5 Guess a 32-bit subkey K_{29} for round 29, then partially encrypt each remaining pair $(\widehat{X}_i, \widehat{X}_i')$ with K_{29}, and finally check if the 160-bit difference $E_{K_{29}}(\widehat{X}_i) \oplus E_{K_{29}}(\widehat{X}_i')$ belongs to $\{(e_{4,8,11,13,16}, e_{3,8,11,13,31}, e_{1,3,8,13,18,23,31}, e_{3,6,10,13,15,18,23}, ROT_2(\Delta E_{30}))\}$. If the number of the pairs $(\widehat{X}_i, \widehat{X}_i')$ passing this test is greater than or equal to 6, then record $(K_f, K_{26}, K_{27}, K_{28}, K_{29})$; Otherwise, repeat Step 2 with another 352-bit key.

3. For a suggested $(K_f, K_{26}, K_{27}, K_{28}, K_{29})$, do an exhaustive search for the remaining 32 key bits using trial encryption. Four known pairs of plaintexts and ciphertexts are enough for this trial process. If a 512-bit key is suggested, output it as the master key of the 55-round SHACAL-1; Otherwise, repeat Step 2 with another 352-bit key.

This attack requires 2^{154} chosen plaintexts. The memory for this attack is also dominated by the ciphertext pairs, so it requires about $2^{154} \cdot 20 \approx 2^{158.32}$ memory bytes.

The time complexity of Step 1 is 2^{154} 55-round SHACAL-1 encryptions; The time complexity of Step 2.1 is dominated by the partial decryptions, which is about $2^{352} \cdot 2^{154} \cdot \frac{11}{55} \approx 2^{503.68}$. In Step 2.1, since the probability that a pair meets the filtering condition in this step is $\frac{30}{2^{32}} \approx 2^{-27.09}$, the expected number of the pairs passing the test for each subkey candidate is $2^{153} \cdot 2^{-27.09} \approx 2^{125.91}$, and the probability that the number of pairs passing this test for a wrong subkey is no less than 6 is about $\sum_{i=6}^{2^{153}} \binom{2^{153}}{i} \cdot (2^{-27.09})^i \cdot (1-2^{-27.09})^{2^{153}-i}) \approx 1$. Thus, almost all the 2^{352} subkeys pass through Step 2.1. In Step 2.2, the time complexity is about $2^{352} \cdot 2^{32} \cdot 2^{125.91} \cdot 2 \cdot \frac{1}{55} \approx 2^{505.13}$. In this step, since the probability that a remaining pair meets the filtering condition in this step is 2^{-32}, the expected number of the pairs passing the test for each subkey candidate is $2^{125.91} \cdot 2^{-32} \approx 2^{93.91}$, and the probability that the number of pairs passing the test for a wrong subkey is no less than 6 is about $\sum_{i=6}^{2^{125.91}} \binom{2^{125.91}}{i} \cdot (2^{-32})^i \cdot (1-2^{-32})^{2^{125.91}-i}) \approx 1$. Thus, almost all the 2^{384} subkeys pass through Step 2.2. Similarly, we can get that the time complexity in either of Step 2.3, 2.4 and 2.5 is also $2^{505.13}$; Besides, almost all the 2^{448} subkeys pass through Step 2.4, and the expected number of the pairs passing the test in Step 2.4 for each subkey candidate is $2^{93.91} \cdot 2^{-32\times 2} \approx 2^{29.91}$. In Step 2.5, since the probability that a remaining pair meets the filtering condition in this step is also 2^{-32}, the expected number of the pairs passing the test for each subkey candidate is $2^{29.91} \cdot 2^{-32} \approx 2^{-2.09}$, and the probability that the number of pairs passing the test for a wrong subkey is no less than 6 is about $\sum_{i=6}^{2^{29.91}} \binom{2^{29.91}}{i} \cdot (2^{-32})^i \cdot (1-2^{-32})^{2^{29.91}-i}) \approx 2^{-22.03}$. Thus, on average, about $2^{448} \cdot 2^{32} \cdot 2^{-22.03} \approx 2^{457.97}$ subkeys pass through Step 2.5, which result in $2^{457.97} \cdot 2^{32} \approx 2^{489.97}$ encryptions in Step 3. Therefore, this attack totally requires about $2^{154} + 2^{503.68} + 4 \cdot 2^{505.13} + 2^{489.97} \approx 2^{507.26}$ encryptions.

Since the probability that a wrong 512-bit key is suggested in Step 3 is about $2^{-640} (= 2^{-160 \cdot 4})$, the expected number of suggested wrong 512-bit keys is about $2^{-640} \cdot 2^{489.97} \approx 2^{-150.03}$, which is extremely low. The expected number of the pairs passing the test in Step 2.5 for the right key is 8 $(= 2^{153} \cdot 2^{-150})$ and the probability that the number of the pairs passing the test in Step 2.5 for the right subkey is no less than 6 is about $\sum_{i=6}^{2^{153}} \binom{2^{153}}{i} \cdot (2^{-150})^i \cdot (1-2^{-150})^{2^{153}-i}) \approx 0.8$. Therefore, with a probability of 0.8, we can break the 55-round SHACAL-1 with 512 key bits by using the differential attack.

4.2 Attacking Rounds 0–48

We can learn that the 64 possible 34-round differentials that have only variable output differences ($e_{0,5,7,12???,17,20,28???}$, $e_{5,7,9,23,25,29}$, $e_{3,12,15,18,20,25,27,30}$, $e_{5,7,13,15,17,23,25,29}$, $e_{2,10,15,22,23,25,27,30}$) compared with the one described earlier hold a probability of $2^{-138} (= 64 \cdot 2^2 \cdot 2^{-148})$ for the right key, and hold a probability of $2^{-154} (= 64 \cdot 2^{-160})$ for a wrong key, where "i???" $(i = 12, 28)$ means that the bit in i position takes 1 and each of the three bits in $i+1$, $i+2$ and

$i+3$ positions takes an arbitrary value from $\{0,1\}$. Similarly, using 2^{141} pairs of plaintexts with difference $(e_{29},0,0,0,e_{2,7})$ and such four fixed bits as described in Section 3.1, the attack requires about $2^{146.32}(\approx 2^{142}\cdot 20)$ memory bytes and $2^{496.45}(\approx 2^{352}\cdot 2^{142}\cdot\frac{11}{49}+4\cdot 2^{384}\cdot 2^{141}\cdot\frac{64}{2^{32}}\cdot 2\cdot\frac{1}{49})$ encryptions.

5 Conclusions

In this paper, we exploit some better rectangle distinguishers and differential characteristics than those previously known in SHACAL-1. Based on them, we finally mount rectangle attacks on the first 51 rounds and a series of inner 52 rounds of SHACAL-1, and mount differential attacks on the first 49 rounds and a series of inner 55 rounds of SHACAL-1. These are the best currently known cryptanalytic results on SHACAL-1 in an one key attack scenario.

Acknowledgments

The authors are very grateful to Jiqiang Lu's supervisor Prof. Chris Mitchell for his valuable editorial comments and to the anonymous referees for their comments. Jiqiang Lu would like to thank Prof. Eli Biham for his help.

References

1. E. Biham, New types of cryptanalytic attacks using related keys, Advances in Cryptology — EUROCRYPT'93, T. Helleseth (ed.), Volume 765 of Lecture Notes in Computer Science, pp. 398–409, Springer-Verlag, 1993.
2. E. Biham and A. Shamir, Differential cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
3. E. Biham, O. Dunkelman, and N. Keller, The rectangle attack — rectangling the Serpent, Advances in Cryptology — EUROCRYPT'01, B. Pfitzmann (ed.), Volume 2045 of Lecture Notes in Computer Science, pp. 340–357, Springer-Verlag, 2001.
4. E. Biham, O. Dunkelman, and N. Keller, New results on boomerang and rectangle attacks, Proceedings of FSE'02, J. Daemen and V. Rijmen (eds.), Volume 2365 of Lecture Notes in Computer Science, pp. 1–16, Springer-Verlag, 2002.
5. E. Biham, O. Dunkelman, and N. Keller, Rectangle attacks on 49-round SHACAL-1, Proceedings of FSE'03, T. Johansson (ed.), Volume 2887 of Lecture Notes in Computer Science, pp. 22–35, Springer-Verlag, 2003.
6. O. Dunkelman, Techniques for cryptanalysis of block ciphers, Ph.D dissertation of Technion, 2006. Available at *http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-info.cgi?2006/PHD/PHD-2006-02*
7. O. Dunkelman, N. Keller, and J. Kim, Related-key rectangle attack on the full SHACAL-1, Proceedings of SAC'06, to appear in Lecture Notes in Computer Science, Springer-Verlag, 2006.
8. H. Handschuh, L. R. Knudsen, and M. J. Robshaw, Analysis of SHA-1 in encryption mode, Proceedings of CT-RSA'01, D. Naccache (ed.), Volume 2020 of Lecture Notes in Computer Science, pp. 70–83, Springer-Verlag, 2001.

9. H. Handschuh and D. Naccache, SHACAL, Proceedings of The First Open NESSIE Workshop, 2000. Available at *https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions.html*
10. H. Handschuh and D. Naccache, SHACAL, NESSIE, 2001. Available at *https://www.cosic.esat.kuleuven.be/nessie/tweaks.html*
11. S. Hong, J. Kim, S. Lee, and B. Preneel, Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192, Proceedings of FSE'05, H. Gilbert and H. Handschuh (eds.), Volume 3557 of Lecture Notes in Computer Science, pp. 368–383, Springer-Verlag, 2005.
12. J. Kelsey, T. Kohno, and B. Schneier, Amplified boomerang attacks against reduced-round MARS and Serpent, Proceedings of FSE'00, B. Schneier (ed.), Volume 1978 of Lecture Notes in Computer Science, pp. 75–93, Springer-Verlag, 2001
13. J. Kelsey, B. Schneier, and D. Wagner, Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES, Advances in Cryptology — CRYPTO'96, N. Koblitz (ed.), Volume 1109 of Lecture Notes in Computer Science, pp. 237–251, Springer–Verlag, 1996.
14. J. Kim, G. Kim, S. Hong, S. Lee, and D. Hong, The related-key rectangle attack — application to SHACAL-1, Proceedings of ACISP'04, H. Wang, J. Pieprzyk, and V. Varadharajan (eds.), Volume 3108 of Lecture Notes in Computer Science, pp. 123–136, Springer-Verlag, 2004.
15. J. Kim, D. Moon, W. Lee, S. Hong, S. Lee, and S. Jung, Amplified boomerang attack against reduced-round SHACAL, Advances in Cryptology — ASIACRYPT'02, Y. Zheng (ed.), Volume 2501 of Lecture Notes in Computer Science, pp. 243–253, Springer-Verlag, 2002.
16. H. Lipmaa and S. Moriai, Efficient algorithms for computing differential properties of addition, Proceedings of FSE'01, M. Matsui (ed.), Volume 2355 of Lecture Notes in Computer Science, pp. 336–350, Springer-Verlag, 2001.
17. M. Matsui, Linear cryptanalysis method for DES cipher, Advances in Cryptology — EUROCRYPT'93, T. Helleseth (ed.), Volume 765 of Lecture Notes in Computer Science, pp. 386–397, Springer-Verlag, 1994.
18. NESSIE, *https://www.cosic.esat.kuleuven.be/nessie/*
19. J. Nakahara Jr, The statistical evaluation of the NESSIE submission, 2001.
20. U.S. Department of Commerce, Secure Hash Standard FIPS 180-1, N.I.S.T., 1995.
21. D. Wagner, The boomerang attack, Proceedings of FSE'99, L. Knudsen (ed.), Volume 1636 of Lecture Notes in Computer Science, pp. 156–170, Springer-Verlag, 1999.