Amplified Boomerang Attack Against Reduced-Round SHACAL

Jongsung Kim, Dukjae Moon, Wonil Lee, Seokhie Hong, Sangjin Lee, and Seokwon Jung

Center for Information Security Technologies(CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, Korea
{joshep,djmoon,nice,hsh,sangjin,jsw}@cist.korea.ac.kr

Abstract. SHACAL is a 160-bit block cipher based on the hash standard SHA-1, as a submission to NESSIE. SHACAL uses the XOR, modular addition operation and the functions of bit-by-bit manner. These operations and functions make the differential cryptanalysis difficult, i.e, it is hard to find a long differential characteristic with high probability. But, we can find short differential characteristics with high probabilities. Using this fact, we discuss the security of SHACAL against an amplified boomerang attack. We find a 36-step boomerang-distinguisher and present attacks on reduced-round SHACAL with various key sizes. We can attack 39-step SHACAL with 256-bit key, and 47-step SHACAL with 512-bit key. In addition, we present differential attacks of reduced-round SHACAL with various key sizes.

Keyword : SHACAL, Amplified boomerang attack, Boomerang-distinguisher

1 Introduction

SHACAL[3] is a 4-round block cipher (each line consists of 20 steps.) designed by H. Handschuh and D. Naccache and is one of the accepted NESSIE submissions. SHACAL was designed by using the hash standard SHA-1 in encryption mode for the first time in 2000. Also, H. Handschuh and D. Naccache introduced a modification[4] of SHACAL in its two versions SHACAL-1 and SHACAL-2 in 2001. In its basic version, SHACAL-1 is a 160-bit block cipher based on SHA-1 and in its extended version, SHACAL-2 is a 256-bit block cipher based on SHA-2. In this paper, we only attack reduced-round SHACAL-1. We will just call SHACAL-1 as SHACAL.

The main cryptanalytic results obtained on SHACAL so far are the analysis of the differential and linear attacks by the algorithm designers[3], and statistical evaluation by J. Nakahara Jr[7]. In [3], the algorithm designers proposed 10-step linear approximations with bias 2^{-6} in rounds 1,2 and 4 respectively, and a 10-step linear approximation with bias 2^{-5} in round 3. Also, they proposed a 10-step differential characteristic with probability 2^{-13} in rounds 1 and 3, and a

10-step differential characteristic with probability 2^{-26} in rounds 2 and 4. Using these 10-step linear approximations and differential characteristics, they concluded that a linear attack with less than 2^{80} known plaintexts is not applicable to full-round SHACAL, and that a differential attack with less than 2^{116} chosen plaintexts is not applicable to full-round SHACAL.

In this paper, we propose a 10-step differential characteristic with probability 2^{-12} in rounds 2 and 4. This characteristic has much higher probability than one proposed by the algorithm designers. Using this characteristic, we describe a 36-step boomerang-distinguisher. We use this boomerang-distinguisher to devise amplified boomerang attacks on reduced-round SHACAL with various key sizes. Moreover, we present a differential attack and compare the results of an amplified boomerang attack with those of a differential attack. Table 1 summarizes attacks on reduced-round SHACAL with respect to master key sizes. Amplified Boomerang attack is denoted by Amp.Boo. in Table 1, and a time complexity of n means that the time of an attack corresponds to performing n encryptions of the underlying cipher.

Master Key	Steps	Methods	Data	Time
128-bit	28	Amp.Boo.	$2^{127.5}$	$2^{127.2}$
128-bit	30	DC	2^{110}	$2^{75.1}$
160-bit	37	Amp.Boo.	$2^{158.8}$	$2^{87.8}$
160-bit	32	DC	2^{141}	2^{105}
256-bit	39	Amp.Boo.	$2^{158.5}$	$2^{250.8}$
256-bit	34	DC	2^{141}	2^{234}
512-bit	47	Amp.Boo.	$2^{158.5}$	$2^{508.4}$
512-bit	41	DC	2^{141}	2^{491}

Table 1. Our result of attacks on reduced-round SHACAL

2 Preliminaries

2.1 Description of SHACAL

SHA is a hash function which was introduced by the American National Institute for Standards and Technology in 1993, and is known as SHA-0. In 1995, a minor change to SHA-0 was made, this variant known as SHA-1. The standard now includes only SHA-1. SHACAL is a 160-bit block cipher based on the hash standard SHA-1. Description of SHACAL[3] is as follows.
Notation:

- $+$: Addition modulo 2^{32} of 32-bit words.
- $ROT_i(X)$: Rotate 32-bit word X to the left by i-bit positions.

- $\oplus$: Bitwise exclusive-or.
- & : Bitwise and.
- | : Bitwise or.

The procedure to encrypt a message is as follows.

1. Insert the 160-bit message $X(= X_1||X_2||X_3||X_4||X_5)$ where each X_i is a 32-bit word in the 32-bit words, A_0, B_0, C_0, D_0, E_0, by

$$A_0 = X_1,\ B_0 = X_2,\ C_0 = X_3,\ D_0 = X_4,\ E_0 = X_5.$$

2. Encrypt the 32-bit words, A_0, B_0, C_0, D_0, E_0 in a total of 80 steps. So, we have a ciphertext, $A_{80}, B_{80}, C_{80}, D_{80}, E_{80}$. Encryption process of the i^{th} step is as follows.

$$\begin{aligned}
&A_i = K_i + ROT_5(A_{i-1}) + f_i(B_{i-1}, C_{i-1}, D_{i-1}) + E_{i-1} + y_i \\
&B_i = A_{i-1} \\
&C_i = ROT_{30}(B_{i-1}) \\
&D_i = C_{i-1} \\
&E_i = D_{i-1}
\end{aligned}$$

for $i = 1, \cdots, 80$, where

$$\begin{aligned}
&f_i(B, C, D) = (B\&C)|(\neg B\&D), && (1 \le i \le 20) \\
&f_i(B, C, D) = B \oplus C \oplus D, && (21 \le i \le 40,\ 61 \le i \le 80) \\
&f_i(B, C, D) = (B\&C)|(B\&D)|(C\&D), && (41 \le i \le 60)
\end{aligned}$$

We call each f_i as f_{if} $(1 \le i \le 20)$, f_{xor} $(21 \le i \le 40,\ 61 \le i \le 80)$, and f_{maj} $(41 \le i \le 60)$, respectively. Each K_i is a 32-bit subkey of the i^{th} step. Each constant y_i is defined as

$$\begin{aligned}
y_i &= 5a827999_x, && (1 \le i \le 20) \\
y_i &= 6ed9eba1_x, && (21 \le i \le 40) \\
y_i &= 8f1bbcdc_x, && (41 \le i \le 60) \\
y_i &= ca62c1d6_x, && (61 \le i \le 80)
\end{aligned}$$

The key scheduling of SHACAL takes a maximum 512-bit key and shorter keys may be used by padding the key with zeros to a 512-bit string. However, SHACAL is not intended to be used with a key shorter than 128 bits. Let the 512-bit key string be denoted $K = [K_1||K_2|| \cdots ||K_{16}]$, where each K_i is a 32-bit word. The key expansion of 512 bits K to 2560 bits is defined by

$$K_i = ROT_1(K_{i-3} \oplus K_{i-8} \oplus K_{i-14} \oplus K_{i-16}),\quad (17 \le i \le 80)$$

2.2 Amplified Boomerang Attack

The amplified boomerang attack[6] is a chosen plaintext attack, while the boomerang attack[8] is an adaptive chosen plaintext and ciphertext attack. The main idea of the amplified boomerang attack is to use two short differential characteristics with high probabilities instead of a long characteristic with low probability.

Let a block cipher $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ be composed of a cascade $E = E_1 \circ E_0$. We assume that for E_0 there exists a differential characteristic $\alpha \to \beta$ with probability p, and for E_1 there exists a differential characteristic $\gamma \to \delta$ with probability q, where $pq \gg 2^{-n/2}$.

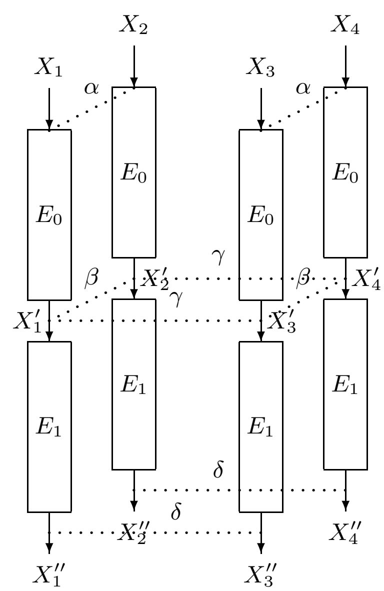

Fig. 1. Boomerang-Distinguisher

The amplified boomerang attack is based on building quartets of plaintexts (X_1, X_2, X_3, X_4) which satisfy several differential conditions. Assume that $X_1 \oplus X_2 = \alpha$ and $X_3 \oplus X_4 = \alpha$. We denote by X'_1, X'_2, X'_3, X'_4 the encrypted values of X_1, X_2, X_3, X_4 under E_0 respectively, and by $X''_1, X''_2, X''_3, X''_4$ the encrypted values of X'_1, X'_2, X'_3, X'_4 under E_1 respectively. We are interested in the cases where $X'_1 \oplus X'_2 = X'_3 \oplus X'_4 = \beta$ and $X'_1 \oplus X'_3 = \gamma$ (or $X'_1 \oplus X'_4 = \gamma$), as in these cases $X'_2 \oplus X'_4 = (X'_1 \oplus \beta) \oplus (X'_3 \oplus \beta) = \gamma$ (or $X'_2 \oplus X'_3 = \gamma$) as well. If the output difference of E_1 becomes δ when the input difference is γ, i.e

$X_1'' \oplus X_3'' = X_2'' \oplus X_4'' = \delta$ (or $X_1'' \oplus X_4'' = X_2'' \oplus X_3'' = \delta$), a quartet satisfying all these differential conditions is called a right quartet. An description of such a quartet is shown in Fig. 1.

If we have m pairs with difference α, we can calculate the fraction of the right quartets among all the quartets generated by m pairs. First, we have about mp pairs satisfying a differential characteristic $\alpha \to \beta$ for E_0. The mp pairs generate about $(mp)^2/2$ quartets consisting of two such pairs. Assuming that the intermediate encryption values distribute uniformly over all possible values, we get $X_1' \oplus X_3' = \gamma$ or $X_1' \oplus X_4' = \gamma$ with probability 2^{-n+1}. Second, for the $((mp)^2/2) \cdot 2^{-n+1}$ quartets satisfying above differential conditions, we can get right quartets with probability q^2 by the characteristic for E_1. Therefore, the expected number of right quartets is about $m^2 \cdot 2^{-n} \cdot (pq)^2$.

For a random permutation, the expected number of right quartets is about $m^2 \cdot 2^{-2n} (= (m^2/2) \cdot 2^{-2n+1})$. Therefore, if $pq > 2^{-n/2}$ and m is sufficiently large, we can have a boomerang-distinguisher which distinguishes between E and a random cipher.

3 Amplified Boomerang Attacks on SHACAL

We describe the differential properties of two operations and three step functions used in SHACAL. We find a 36-step boomerang-distinguisher of SHACAL using these properties and attack reduced round SHACAL.

3.1 Differential properties for SHACAL

We present two differential properties used in generating a differential charecteristic of SHACAL. What generates a differential probability on SHACAL is first, the use of both XOR and modular additions, and second, the functions f_{if}, f_{xor}, f_{maj}.

First, we consider the relation between XOR differences and modular addition. Let X, Y and X^*, Y^* be 32-bit words. We assume $Z = X + Y$ and $Z^* = X^* + Y^*$. If the words X and Y only differ in the position of bit i $(0 \le i \le 31)$, we denote by $X \oplus Y = e_i$ where the most significant bit (left) is a bit of position 31. Then, we have the following four relations [5] between XOR differences and modular addition. In the relations 3 and 4, the j indicates $0 \le j \le 30$.

1. If $X \oplus X^* = e_{31}$ and $Y = Y^*$, then it holds $Z \oplus Z^* = e_{31}$ with probability 1.
2. If $X \oplus X^* = e_{31}$ and $Y \oplus Y^* = e_{31}$, then it holds $Z = Z^*$ with probability 1.
3. If $X \oplus X^* = e_j$ and $Y = Y^*$, then it holds $Z \oplus Z^* = e_j$ with probability 1/2.
4. If $X \oplus X^* = e_j$ and $Y \oplus Y^* = e_j$, then it holds $Z = Z^*$ with probability 1/2.

Second, we consider differential probabilities for the functions f_{if}, f_{xor}, f_{maj}. These functions operate in the bit-by-bit manner. Thus, we can regard each f_i as a boolean function assigning from a 3-bit input to a 1-bit output. Table

2 [5] shows distribution of XOR differences through all three functions. The notation of the table is as follows. The first three columns represent the eight possible differences in the one-bit inputs, x, y, z. The next three columns indicate the differences in the outputs of each of the three functions. In the last three columns, a '0'('1') means that the difference will always be zero(one), and a '0/1' means that in half of the cases, the difference will be zero and in the other half of the cases, the difference will be one.

x	y	z	f_{xor}	f_{if}	f_{maj}
0	0	0	0	0	0
0	0	1	1	0/1	0/1
0	1	0	1	0/1	0/1
1	0	0	1	0/1	0/1
0	1	1	0	1	0/1
1	0	1	0	0/1	0/1
1	1	0	0	0/1	0/1
1	1	1	1	0/1	1

Table 2. The XOR differential distribution table of the f-functions

3.2 The 36-step Boomerang-distinguisher

Using the differential properties shown in the previous subsection, we describe two differential characteristics which make a boomerang-distinguisher for SHACAL. That is, the first differential characteristic is $\alpha \to \beta$ with probability p $(= 2^{-45})$ from steps 1 to 21, where the differences $\alpha = (0, e_{22}, e_{15}, e_{10}, e_5)$ and $\beta = (e_{2,7,14,24,29}, e_{19}, e_{12}, e_7, e_2)$ where $e_{i_1,\cdots,i_k}$ indicates $e_{i_1} \oplus \cdots \oplus e_{i_k}$. The second differential characteristic is $\gamma \to \delta$ with probability q $(= 2^{-31})$ from steps 22 to 36, where the differences $\gamma = (e_{1,5,8}, e_{1,3,5}, e_{3,13}, e_{1,5,13,31}, e_{6,10,13,31})$ and $\delta = (e_{9,19,29,31}, e_{14,29}, e_{7,29}, e_2, e_{29})$. Table 3 shows the first differential characteristic composed of 21 steps. In Table 3, the first row indicates an input difference of the 1^{st} step, and the second column of the i^{th} step indicates an output difference of the i^{th} step, and the third column of the i^{th} step indicates the probability with which an output difference of the $(i-1)^{th}$ step becomes an output difference of the i^{th} step. Note that the function f_{if} is used from steps 1 to 20, and the function f_{xor} is used at the 21^{th} step. We can easily check probabilities in Table 3 using the differential properties on SHACAL. Thus, we have the first differential characteristic $\alpha \to \beta$ with probability p $(= 2^{-45})$ from steps 1 to 21 shown in Table 3.

Table 4 shows the second differential characteristic composed of 15 steps. Note that the function f_{xor} is used from steps 22 to 36. Similarly, we can have the second differential characteristic $\gamma \to \delta$ with probability q $(= 2^{-31})$ from steps 22 to 36 shown in Table 4.

Step	ΔA	ΔB	ΔC	ΔD	ΔE	Prob
	0	e_{22}	e_{15}	e_{10}	e_5	
1	e_5	0	e_{20}	e_{15}	e_{10}	2^{-4}
2	0	e_5	0	e_{20}	e_{15}	2^{-3}
3	e_{15}	0	e_3	0	e_{20}	2^{-3}
4	0	e_{15}	0	e_3	0	2^{-2}
5	0	0	e_{13}	0	e_3	2^{-2}
6	e_3	0	0	e_{13}	0	2^{-2}
7	e_8	e_3	0	0	e_{13}	2^{-2}
8	0	e_8	e_1	0	0	2^{-2}
9	0	0	e_6	e_1	0	2^{-2}
10	0	0	0	e_6	e_1	2^{-2}
11	e_1	0	0	0	e_6	2^{-2}
12	0	e_1	0	0	0	2^{-1}
13	0	0	e_{31}	0	0	2^{-1}
14	0	0	0	e_{31}	0	2^{-1}
15	0	0	0	0	e_{31}	2^{-1}
16	e_{31}	0	0	0	0	1
17	e_4	e_{31}	0	0	0	2^{-1}
18	e_9	e_4	e_{29}	0	0	2^{-2}
19	e_{14}	e_9	e_2	e_{29}	0	2^{-3}
20	e_{19}	e_{14}	e_7	e_2	e_{29}	2^{-4}
21	$e_{2,7,14,24,29}$	e_{19}	e_{12}	e_7	e_2	2^{-5}

Table 3. The first differential characteristic for SHACAL

Two differential characteristics above can be regarded as extended ones for 10-step differential characteristics with high probabilities respectively. That is, in the first differential characteristic, the good 10-step characteristic is $(0,e_8,e_1,0,0) \rightarrow (e_9,e_4,e_{29},0,0)$ with probability 2^{-13} from steps 9 to 18, and in the second differential characteristic, the good 10-step characteristic is $(0,e_{1,3},e_{6,31},0,e_{3,6,31}) \rightarrow (e_{14,29},e_{9,31},e_2,e_{29},0)$ with probability 2^{-12} from steps 26 to 35. Especially, the 10-step characteristic from steps 26 to 35 has much higher probability than one proposed by algorithm designers[3]. Also, if we extend the differential characteristics in Table 3,4 to more steps, hamming weights in the differences of the five words become much bigger and the probabilities decrease rapidly. In the heuristic point of view, we conjecture that the 36-step boomerang-distinguisher using two differential characteristics in Table 3,4 is one of the longest boomerang-distinguishers such that $pq \gg 2^{-80}$ for SHACAL.

3.3 Attack Procedure

We present here amplified boomerang attacks on reduced-round SHACAL with various key sizes. We now present a method to use the 36-step boomerang-distinguisher to find subkey material.

Step	ΔA	ΔB	ΔC	ΔD	ΔE	Prob
	$e_{1,5,8}$	$e_{1,3,5}$	$e_{3,13}$	$e_{1,5,13,31}$	$e_{6,10,13,31}$	
22	0	$e_{1,5,8}$	$e_{1,3,31}$	$e_{3,13}$	$e_{1,5,13,31}$	2^{-3}
23	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	$e_{3,13}$	2^{-4}
24	$e_{1,3}$	$e_{1,8}$	0	$e_{3,6,31}$	$e_{1,3,31}$	2^{-4}
25	0	$e_{1,3}$	$e_{6,31}$	0	$e_{3,6,31}$	2^{-4}
26	e_1	0	$e_{1,31}$	$e_{6,31}$	0	2^{-3}
27	e_1	e_1	0	$e_{1,31}$	$e_{6,31}$	2^{-2}
28	0	e_1	e_{31}	0	$e_{1,31}$	2^{-1}
29	0	0	e_{31}	e_{31}	0	2^{-1}
30	0	0	0	e_{31}	e_{31}	1
31	0	0	0	0	e_{31}	1
32	e_{31}	0	0	0	0	1
33	e_4	e_{31}	0	0	0	2^{-1}
34	$e_{9,31}$	e_4	e_{29}	0	0	2^{-1}
35	$e_{14,29}$	$e_{9,31}$	e_2	e_{29}	0	2^{-3}
36	$e_{9,19,29,31}$	$e_{14,29}$	$e_{7,29}$	e_2	e_{29}	2^{-4}

Table 4. The second differential characteristic for SHACAL

Let $S = E_f \circ E = E_f \circ E_1 \circ E_0$ be reduced-round SHACAL such that E_0 indicates from steps 1 to 21, and E_1 indicates from steps 22 to 36. We find the subkey material of E_f in S. The first differential characteristic $\alpha \rightarrow \beta$ used in E_0 has the probability p $(= 2^{-45})$ and the second differential characteristic $\gamma \rightarrow \delta$ used in E_1 has the probability q $(= 2^{-31})$. The differences α, β, γ and δ are presented in the subsection 3.2. So, we have the 36-step boomerang-distinguisher with probability pq $(= 2^{-76})$ from steps 1 to 36.

For $m = 2^{157.5}$ pairs with the input difference α, the expected number of right quartets is 8 $(= (2^{157.5})^2 \cdot 2^{-160} \cdot (2^{-76})^2)$. From this fact, we can construct an algorithm to attack S with at least 160 bits key as follows.

1. **Choose $m(= 2^{157.5})$ pairs with the input difference α.**
   The expected number of possible quartets from the pool of m pairs is about $m^2(= 2^{315})$. We denote the plaintexts of a quartet by (P_1, P_2, P_3, P_4) where $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ and the corresponding ciphertexts by (C_1, C_2, C_3, C_4).

2. **Initialize the counter array with 0's.**
   The number of the counter array is equal to the number of possible keys for E_f.

3. **Check the differences $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta'$ where δ' is an element of the set composed of possible output differences for E_f with the input difference δ $(= (e_{9,19,29,31}, e_{14,29}, e_{7,29}, e_2, e_{29}))$.**

4. **For all the quartets which passed the last test, increase the counters by 1 which correspond to all subkeys K_f of E_f for which**

$E^{-1}_{f_{K_f}}(C_1) \oplus E^{-1}_{f_{K_f}}(C_3) = E^{-1}_{f_{K_f}}(C_2) \oplus E^{-1}_{f_{K_f}}(C_4) = \delta$.

5. **Check all counters, and output the subkey whose counter is greater than or equal to 7.**

First, using this algorithm, we show that the reduced 39-step SHACAL with 256-bit key can be broken by an attack which is faster than an exhaustive search for a master key. Since E_f consists of the 37^{th}, 38^{th} and 39^{th} steps, we can find the 96-bit subkey K_f.

In Step 1, we have 2^{315} quartets derived from $2^{157.5}$ pairs with the difference α. For these quartets, we can filter out wrong quartets through Step 3. In Step 3, we take δ' that belongs to the set $\{(?, ?, ?, e_{7,17,27,29}, e_{12,27})|$? is an arbitrary difference$\}$ composed of possible output differences for E_f with the input difference δ. So, we have 2^{187} candidates for right quartets among 2^{315} quartets, since a fraction of $(2^{-64})^2$ of these quartets remain. In Step 4, we guess a 96-bit subkey K_f and decrypt ciphertexts of the remaining quartets for guessed key. If a decrypted quartet passes through Step 4, the counter of guessed key is increased by 1. So, the expected value of counter of right subkey is greater than 7, since the expected number of right quartets is about 8. But, for a wrong subkey, the expected value of counter is equal to 0 or 1, since the expected number of quartets passed through Step 4 is $2^{-5} (= 2^{187} \cdot (2^{-96})^2)$. Thus, we can find the right key of E_f by the maximum likelihood method. The attack requires $2^{158.5}$ chosen plaintexts and processing equivalent to about $2^{158.5} \cdot 2^{96} \cdot \frac{3}{39} \simeq 2^{250.8}$ 39-step SHACAL encryptions.

Also, using the algorithm above, we can attack on reduced-round SHACAL with at least 256-bit keys. We assume that for $i = 0, 1, \cdots, 8$, the reduced $(39+i)$-step SHACAL uses the $(256 + 32 \cdot i)$-bit master key. Since E_f consists of $(i + 3)$ steps, we can find the $(32 \cdot (i + 3))$-bit subkey K_f for the reduced $(39 + i)$-step SHACAL by the algorithm above. Particularly, in the algorithm for the reduced $(39 + i)$-step SHACAL $(i \geq 2)$, there does not exist the filtering process (Step 3) since we use the 36-step boomerang-distinguisher to attack. The attack for $(39+i)$-step SHACAL requires $2^{158.5}$ chosen plaintexts and processing equivalent to about $2^{158.5} \cdot 2^{32 \cdot (i+3)} \cdot \frac{i+3}{39+i} (\leq 2^{252.4+32 \cdot i})$ $(39 + i)$-step SHACAL encryptions where $i = 0, 1, \cdots, 8$. Thus we can attack the reduced 47-step SHACAL with 512-bit key. Furthermore, we can attack on reduced-round SHACAL with less than 256-bit key except 128-bit key. In these cases, since the key sizes are small, the expected number of quartets passed through Step 3 (filtering process) should be less than $2^{156.5}$ to attack reduced-round SHACAL faster than the exhaustive search. Thus, we can attack the reduced 37-step SHACAL with 160-bit key and the reduced 38-step SHACAL with 192- or 224-bit master key. The attack for 37-step SHACAL requires $2^{158.5}$ chosen plaintexts and processing equivalent to about $2^2 \cdot 2^{315} \cdot 2^{-256} \cdot 2^{32} \cdot \frac{1}{37} \simeq 2^{87.8}$ 37-step SHACAL encryptions, and the attack for 38-step SHACAL requires $2^{158.5}$ chosen plaintexts and processing equivalent to about $2^2 \cdot 2^{315} \cdot 2^{-192} \cdot 2^{64} \cdot \frac{2}{38} \simeq 2^{184.8}$ 38-step SHACAL encryptions.

In the case of 128-bit key, we cannot use the above 36-step boomerang-distinguisher since the number of required plaintexts should be less than 2^{128}.

So, we must find a new boomerang-distinguisher with probability pq which is higher than $2^{-45.5}$ $(= \{2^3 \cdot (2^{-127})^2 \cdot 2^{160})\}^{1/2})$. We can find a 26-step boomerang-distinguisher with probability 2^{-45} from steps 1 to 26. We can attack on 28-step SHACAL. Since differential attack which is described in the next section is applied to SHACAL more effective than amplified boomerang attack, we omit the detailed explanation. See table 1 for the result of an attack on SHACAL with 128-bit key.

4 Differential Attacks on SHACAL

In this section, we present differential attacks on reduced-round SHACAL. First of all, we describe two differential characteristics which are expanded from the 21-step differential characteristic shown in Table 3. One is the 28-step differential characteristic $\alpha \rightarrow \beta'$ [1] with probability 2^{-107} from steps 1 to 28, the other is the 30-step differential characteristic $\alpha \rightarrow \beta''$ [2] with probability 2^{-138} from steps 1 to 30. We can easily check probabilities of these differential characteristics using the differential properties on SHACAL.

Using the 28-step differential characteristic, we show that the reduced 30-step SHACAL with 128-bit key can be broken by a differential attack which is faster than an exhaustive search for a master key. That is, we can find the 64-bit subkey of the 29^{th} and 30^{th} steps. Note that these steps are denoted by E_f. Attack procedure is as follows. First, we ask for 2^{109} pairs with the input difference α. Second, we check whether the output differences of these pairs are equal to $(?, ?, e_{0,3,13,17,18,20,23,25,30}, e_{1,5,10,12,23,27,28}, e_{8,10,25})$. Since a fraction of 2^{-96} of these pairs remain, we have about $2^{13}(= 2^{109} \cdot 2^{-96})$ analyzed pairs. And then, we guess a 64-bit subkey of the 29^{th} and 30^{th} steps and decrypt the analyzed pairs using a guessed key. If a difference of decrypted texts is β', the counter of a guessed key is increased. Since the signal-to-noise is extremely high, we can distinguish the right subkey in the key space. Thus, the attack requires 2^{110} chosen plaintexts and processing equivalent to about $2^{14} \cdot 2^{64} \cdot \frac{2}{30} \simeq 2^{75.1}$ 30-step SHACAL encryptions.

Also, we can attack on reduced-round SHACAL with at least 160-bit keys using the 30-step differential characteristic $\alpha \rightarrow \beta''$. To attack successfully, we must ask for 2^{140} pairs with the input difference α. The attack procedure is similar to that of reduced-round SHACAL with 128-bit key. Assume that for $i = 0, 1, 2, 3, 4$, the reduced $(32 + i + \theta(i))$-step SHACAL uses the $(160 + 32 \cdot i)$-bit master key. Here the controller $\theta(i)$ is defined as $\theta(0) = \theta(1) = 0$, $\theta(2) = \theta(3) = -1$ and $\theta(4) = -2$. Since E_f consists of $(i + \theta(i) + 2)$ steps, we can find the $(32 \cdot (i + \theta(i) + 2))$-bit subkey of the reduced $(32 + i + \theta(i))$-step SHACAL. The attack for $(32 + i + \theta(i))$-step SHACAL requires 2^{141} chosen plaintexts and processing equivalent to about $2^{141} \cdot 2^{-32 \cdot (3 - i - \theta(i))} \cdot 2^{32 \cdot (i + \theta(i) + 2)} \cdot \frac{i + \theta(i) + 2}{32 + i + \theta(i)} (\leq 2^{106 + 64 \cdot i + 64\theta(i)})$ $(32 + i + \theta(i))$-step SHACAL encryptions where $i = 0, 1, 2, 3, 4$.

[1] $\beta' = (e_{0,2,5,15,19,20,22,25,27}, e_{3,7,12,14,25,29,30}, e_{8,10,25}, e_{5,8,12,20,27}, e_{0,3,17,25,30})$

[2] $\beta'' = (e_{0,1,3,6,15,23,27,28,29}, e_{0,1,14,17,24,29,30}, e_{0,3,13,17,18,20,23,25,30}, e_{1,5,10,12,23,27,28}, e_{8,10,25})$

($2^{-32\cdot(3-i-\theta(i))}$ is a fraction of the analyzed pairs among all of the pairs.) The reason to exist the controller $\theta(i)$ is that we decrypt only analyzed pairs for a guessed key.

Also, for reduced-round SHACAL with at least 320-bit key, we can attack without the process of filtering out. Assume that for $j = 0, 1, \cdots, 6$, the reduced $(35+j)$-step SHACAL uses the $(320+32\cdot j)$-bit master key. Since E_f consists of $(j+5)$ steps, we can find the $(32\cdot(j+5))$-bit subkey for the reduced $(35+j)$-step SHACAL. The attack for $(35+j)$-step SHACAL requires 2^{141} chosen plaintexts and processing equivalent to about $2^{141} \cdot 2^{32\cdot(j+5)} \cdot \frac{j+5}{35+j} (\leq 2^{299+32\cdot j})$ $(35+j)$-step SHACAL encryptions where $j = 0, 1, \cdots, 6$. Thus, we can attack 41-step SHACAL with 512-bit key.

5 Conclusion

SHACAL has short differential characteristics with high probabilities and long ones with low probabilities. From this fact, we could find a 36-step boomerang-distinguisher and attack reduced-round SHACAL with various key sizes. And we discussed the security of reduced-round SHACAL against differential cryptanalysis(DC). In the comparison of an amplified boomerang attack and a differential attack, the latter is more efficient for SHACAL with a 128-bit key, but for SHACAL with other key sizes, the former is more efficient.

Acknowledgment. We would like to thank referees for their helpful comments.

References

1. E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
2. E. Biham, O. Dunkelman and N. Keller, *The Rectangle Attack-Rectangling the Serpent*, Proc. of Eurocrypt'2001, Springer-Verlag, LNCS 2045, pp.340-357, 2001
3. H. Handschuh, D. Naccache, *SHACAL*, In Proceedings of the First Open NESSIE Workshop, November 2000.
4. H. Handschuh, D. Naccache, *SHACAL*, NESSIE project, October 2001.
5. H. Handschuh, L. R. Knudsen, and M. J. Robshaw *Analysis of SHA-1 in Encryption Mode*, CT-RSA 2001, Springer-Verlag, LNCS 2020, pp.70-83, 2001.
6. J. Kelsey, T. Kohno, and B. Schneier, *Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent*, Proc. of FSE'2000, Springer-Verlag, LNCS 1978, pp.75-93, 2001
7. J. Nakahara Jr, *The Statistical Evaluation of the NESSIE Submission*, October 2001.
8. David Wagner, *The boomerang Attack*, proceedings of Fast Software Encryption, Lecture Notes in Computer Science 1636, pp.156-170, Springer-Verlag, 1999.