Related-Key Rectangle Attack on 42-Round SHACAL-2

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 Based on the compression function of the hash function standard SHA-256, SHACAL-2 is a 64-round block cipher with a 256-bit block size and a variable length key of up to 512 bits. In this paper, we present a related-key rectangle attack on 42-round SHACAL-2, which requires $2^{243.38}$ related-key chosen plaintexts and has a running time of $2^{488.37}$. This is the best currently known attack on SHACAL-2.

Key words: Block cipher, SHACAL-2, Differential cryptanalysis, Related-key rectangle attack

1 Introduction

In 2000, Handschuh and Naccache [7] proposed a 160-bit block cipher SHACAL based on the standardized hash function SHA-1 [19]. In 2001, they then proposed

⋆ 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.

two versions, known as SHACAL-1 and SHACAL-2 [8], where SHACAL-1 is the same as the original SHACAL, while SHACAL-2 is a 256-bit block cipher based on the compression function of SHA-256 [20]. Both SHACAL-1 and SHACAL-2 were submitted to the NESSIE (New European Schemes for Signatures, Integrity, and Encryption) project [18] and selected for the second phase of the evaluation; however, in 2003, SHACAL-1 was not recommended for a NESSIE portfolio because of concerns about its key schedule, while SHACAL-2 was selected to be in the NESSIE portfolio.

The published cryptanalytic results on SHACAL-2 are as follows: Hong *et al.* presented an impossible differential attack [2] on 30-round SHACAL-2 [9] and Shin *et al.* presented a differential-nonlinear attack on 32-round SHACAL-2 [21], which is a variant of the differential-linear attack [15]. Shin *et al.* also presented a square-nonlinear attack on 28-round SHACAL-2. Recently, Kim *et al.* [14] presented a related-key differential-nonlinear attack on 35-round SHACAL-2 and a related-key rectangle attack on 37-round SHACAL-2, where the latter attack is based on a 33-round related-key rectangle distinguisher. As far as the number of the attacked rounds is concerned, the Kim *et al.*'s related-key rectangle attack on 37-round SHACAL-2 is the best cryptanalytic result on SHACAL-2, prior to the work described in this paper.

Like the amplified boomerang attack [11] and the rectangle attack [3,4], the related-key rectangle attack [5,10,13] is also a variant of the boomerang attack [22]. As a result, it shares the same basic idea of using two short differentials with larger probabilities instead of a long differential with a smaller probability, but requires an additional assumption that the attacker knows the specific differences between one or two pairs of unknown keys. This additional assumption makes it very difficult or even infeasible to conduct in many cryptographic applications, but as demonstrated in [12], some of the current real-world applications may allow for practical related-key attacks [1], say key-exchange protocols and hash functions.

In this paper, based on relatively low difference propagations for the first several rounds in the key schedule of SHACAL-2, we explore a 34-round related-key rectangle distinguisher. We also introduce a differential property in SHACAL-2 such that we can apply the exploited "early abort" technique to discard some disqualified candidate quartets earlier than usual. Relying on the 34-round distinguisher and the "early abort" technique, we mount a related-key rectangle attack on 40-round SHACAL-2 when used with a 512-bit key. Finally, based on several more delicate observations, we eventually mount a related-key rectangle attack on 42-round SHACAL-2, which requires $2^{243.38}$ related-key chosen plaintexts and has a running time of $2^{488.37}$.

The rest of this paper is organized as follows: In the next section, we briefly describe some notation, the SHACAL-2 cipher and the related-key rectangle attack. In Sect. 3, we introduce four properties in SHACAL-2. In Sect. 4, we present our related-key rectangle attacks on 40 and 42-round SHACAL-2, respectively. Section 5 concludes this paper.

2 Preliminaries

2.1 Notation

The following notation will be used throughout this paper:

- $\oplus$: the bitwise logical exclusive OR (XOR) operation
- $\&$: the bitwise logical AND operation
- $\boxplus$: the addition modulo 2^{32} operation
- $\neg$: the complement operation
- e_j : a 32-bit word with zeros in all positions but bit j ($0 \leq j \leq 31$)
- $e_{i_1,\cdots,i_j} : e_{i_1} \oplus \cdots \oplus e_{i_j}$
- $e_{j,\sim}$: a 32-bit word that has 0's in bits 0 to $j-1$, 1 in bit j and unconcerned values in bits $(j+1)$ to 31

2.2 The SHACAL-2 Cipher

SHACAL-2 [8] uses the compression function of SHA-256 [20], where the plaintext enters the compression function as the chaining value, and the key enters the compression function as the message block. Its encryption procedure can be described as follows:

1. The 256-bit plaintext P is divided into eight 32-bit words A^0, B^0, C^0, D^0, E^0, F^0, G^0 and H^0.
2. For $i = 0$ to 63:
   $T_1^{i+1} = K^i \boxplus \Sigma_1(E^i) \boxplus Ch(E^i, F^i, G^i) \boxplus H^i \boxplus W^i$,
   $T_2^{i+1} = \Sigma_0(A^i) \boxplus Maj(A^i, B^i, C^i)$,
   $H^{i+1} = G^i$,
   $G^{i+1} = F^i$,
   $F^{i+1} = E^i$,
   $E^{i+1} = D^i \boxplus T_1^{i+1}$,
   $D^{i+1} = C^i$,
   $C^{i+1} = B^i$,
   $B^{i+1} = A^i$,
   $A^{i+1} = T_1^{i+1} \boxplus T_2^{i+1}$.
3. The ciphertext is $(A^{64}, B^{64}, C^{64}, D^{64}, E^{64}, F^{64}, G^{64}, H^{64})$,

where K^i is the i-th round key, W^i is the i-th round constant[1], and the four functions $Ch(X,Y,Z)$, $Maj(X,Y,Z)$, $\Sigma_0(X)$ and $\Sigma_1(X)$ are defined as follows, respectively,

$$\begin{aligned} Ch(X,Y,Z) &= (X\&Y) \oplus (\neg X\&Z), \\ Maj(X,Y,Z) &= (X\&Y) \oplus (X\&Z) \oplus (Y\&Z), \\ \Sigma_0(X) &= S_2(X) \oplus S_{13}(X) \oplus S_{22}(X), \\ \Sigma_1(X) &= S_6(X) \oplus S_{11}(X) \oplus S_{25}(X), \end{aligned}$$

[1] In the specifications of [8,20] the term K^i is used for the round constant, and the term W^i is used for the round subkey. In this paper, we use the more standard notation.

where $S_j(X)$ represents right rotation of X by j bits.

The key schedule of SHACAL-2 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 initial 16 rounds. Finally, the i-th round key ($16 \leq i \leq 63$) is generated as

$$\begin{aligned} K^i &= \sigma_1(K^{i-2}) \boxplus K^{i-7} \boxplus \sigma_0(K^{i-15}) \boxplus K^{i-16}, \\ &\textit{with } \sigma_0(X) = S_7(X) \oplus S_{18}(X) \oplus R_3(X), \\ &\qquad \sigma_1(X) = S_{17}(X) \oplus S_{19}(X) \oplus R_{10}(X), \end{aligned} \tag{1}$$

where $R_j(X)$ represents right shift of X by j bits[2].

2.3 The Related-Key Rectangle Attack

The related-key rectangle attack [5,10,13] treats the block cipher $E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ as a cascade of two sub-ciphers $E = E^1 \circ E^0$. It assumes that there exists a related-key differential $\alpha \rightarrow \beta$ with probability p^*_β for E^0 (*i.e.*, $Pr[E^0_K(X) \oplus E^0_{K^*}(X^*) = \beta | X \oplus X^* = \alpha] = p^*_\beta$), where K and K^* are two related keys with a known difference, and a regular differential $\gamma \rightarrow \delta$ with probability q_γ for E^1 (*i.e.*, $Pr[E^1_K(X) \oplus E^1_K(X^*) = \delta | X \oplus X^* = \gamma] = Pr[E^1_{K^*}(X) \oplus E^1_{K^*}(X^*) = \delta | X \oplus X^* = \gamma] = q_\gamma$). In our attack on SHACAL-2 we use a related-key differential for the first sub-cipher and a regular differential for the second sub-cipher, *i.e.*, our second differential has no key difference. Note that the related-key rectangle attack can also use related-key differentials for both the sub-ciphers in similar ways.

Let a quartet of plaintexts be denoted by (P_i, P^*_i, P_j, P^*_j) with $P_i \oplus P^*_i = P_j \oplus P^*_j = \alpha$, where P_i and P_j are encrypted under E_K, and P^*_i and P^*_j are encrypted under E_{K^*}. Out of N pairs of plaintexts with related-key difference α about $N \cdot p^*_\beta$ pairs have a related-key output difference β after E^0. These pairs can be combined into about $\frac{(N \cdot p^*_\beta)^2}{2}$ candidate quartets such that each quartet satisfies $E^0_K(P_i) \oplus E^0_{K^*}(P^*_i) = \beta$ and $E^0_K(P_j) \oplus E^0_{K^*}(P^*_j) = \beta$. Assuming that the intermediate values after E^0 distribute uniformly over all possible values, the event $E^0_K(P_i) \oplus E^0_K(P_j) = \gamma$ holds with probability 2^{-n}. Once this occurs, $E^0_{K^*}(P^*_i) \oplus E^0_{K^*}(P^*_j) = \gamma$ holds as well, for $E^0_{K^*}(P^*_i) \oplus E^0_{K^*}(P^*_j) = (E^0_K(P_i) \oplus E^0_{K^*}(P^*_i)) \oplus (E^0_K(P_j) \oplus E^0_{K^*}(P^*_j)) \oplus (E^0_K(P_i) \oplus E^0_K(P_j)) = \beta \oplus \beta \oplus \gamma = \gamma$. As a result, the expected number of the quartets satisfying both $E^1_K(P_i) \oplus E^1_K(P_j) = \delta$ and $E^1_{K^*}(P^*_i) \oplus E^1_{K^*}(P^*_j) = \delta$ is

$$\sum_{\beta,\gamma} \frac{(N \cdot p^*_\beta)^2}{2} \cdot 2^{-n} \cdot (q_\gamma)^2 = N^2 \cdot 2^{-n-1} \cdot (\widehat{p^*} \cdot \widehat{q})^2,$$

[2] We alert the reader to the somewhat confusing notation of $S(\cdot)$ as cyclic rotation and of $R(\cdot)$ as a shift operation.

where $\widehat{p^*} = \sqrt{\sum_{\beta'} Pr^2(\alpha \to \beta')}$ and $\widehat{q} = \sqrt{\sum_{\gamma'} Pr^2(\gamma' \to \delta)}$.

On the other hand, for a random cipher, the expected number of right quartets is about $\frac{N^2}{2} \cdot 2^{-2n} = N^2 \cdot 2^{-2n-1}$. Therefore, if $\widehat{p^*} \cdot \widehat{q} > 2^{-n/2}$ and N is sufficiently large, the related-key rectangle distinguisher can distinguish between E and a random cipher.

3 Properties in SHACAL-2

Property 1 *(from [21]) Let $Z = X \boxplus Y$ and $Z^* = X^* \boxplus Y^*$ with X, Y, X^*, Y^* being 32-bit words. Then, the following properties hold:*

1. *If $X \oplus X^* = e_j$ and $Y = Y^*$, then $Z \oplus Z^* = e_{j,j+1,\cdots,j+k-1}$ holds with probability $\frac{1}{2^k}$ ($j < 31, k \geq 1$ and $j + k - 1 \leq 30$). In addition, in case $j = 31$, $Z \oplus Z^* = e_{31}$ holds with probability 1.*
2. *If $X \oplus X^* = e_j$ and $Y \oplus Y^* = e_j$, then $Z \oplus Z^* = e_{j+1,\cdots,j+k-1}$ holds with probability $\frac{1}{2^k}$ ($j < 31, k \geq 1$ and $j + k - 1 \leq 30$). In addition, in case $j = 31$, $Z = Z^*$ holds with probability 1.*
3. *If $X \oplus X^* = e_{i,\sim}$, $Y \oplus Y^* = e_{j,\sim}$ and $i > j$, then $Z \oplus Z^* = e_{j,\sim}$ holds.*

A more general description of this property can be obtained from the following theorem in [16],

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

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

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

Property 2 *(from [21]) The two functions Ch and Maj operate in a bit-by-bit manner, therefore, each of them can be regarded as a boolean function from a 3-bit input to a 1-bit output. Table 1 shows the distribution probability of XOR differences through them. The first three rows represent the eight possible differences of the 3-bit inputs x, y, z, and the last two rows indicate the differences in the outputs of the two functions, where a "0" (resp., "1") means that the difference will always be 0 (resp., 1), and a "0/1" means that the difference will be 0 or 1 with probability $\frac{1}{2}$.*

Let's introduce two other properties in SHACAL-2, as follows.

Property 3 *Consider the difference propagation between a pair of data for any four consecutive rounds i to $i + 3$. If the difference $(\Delta A^i, \Delta B^i, \cdots, \Delta H^i)$ just before the i-th round is known, then we can easily learn that:*

1. *The differences ΔB^{i+1}, ΔC^{i+1}, ΔD^{i+1}, ΔF^{i+1}, ΔG^{i+1} and ΔH^{i+1} just before the $(i + 1)$-th round can be definitely determined, which are equal to ΔA^i, ΔB^i, ΔC^i, ΔE^i, ΔF^i and ΔG^i, respectively.*

Table1. Differential distribution of the functions Ch and Maj

x	0	0	0	1	0	1	1	1
y	0	0	1	0	1	0	1	1
z	0	1	0	0	1	1	0	1
Ch	0	0/1	0/1	0/1	1	0/1	0/1	0/1
Maj	0	0/1	0/1	0/1	0/1	0/1	0/1	1

2. *The differences ΔC^{i+2}, ΔD^{i+2}, ΔG^{i+2} and ΔH^{i+2} just before the $(i+2)$-th round can be definitely determined, which are equal to ΔB^{i+1}, ΔC^{i+1}, ΔF^{i+1} and ΔG^{i+1}, respectively.*
3. *The differences ΔD^{i+3} and ΔH^{i+3} just before the $(i+3)$-th round can be definitely determined, which are equal to ΔC^{i+2} and ΔG^{i+2}, respectively.*

Property 4 *Let the two related keys K and K^* have the difference e_{31} in both the 0-th and 9-th round keys and have all zero difference in the others of the first 16 round keys, then we can conclude by Eq. (1) that the round keys from 16 until 23 (*i.e.*, $K^{16}, K^{17}, \cdots, K^{23}$) have all zero differences, for the following equation holds with probability 1,*

$$\begin{aligned} K^{*16} &= \sigma_1(K^{*14}) \boxplus K^{*9} \boxplus \sigma_0(K^{*1}) \boxplus K^{*0} \\ &= \sigma_1(K^{14}) \boxplus (K^9 \oplus e_{31}) \boxplus \sigma_0(K^1) \boxplus (K^0 \oplus e_{31}) \\ &= \sigma_1(K^{14}) \boxplus K^9 \boxplus \sigma_0(K^1) \boxplus K^0 \\ &= K^{16}. \end{aligned}$$

4 Related-Key Rectangle Attacks on Reduced SHACAL-2

In this section, based on Properties 1, 2 and 4, we explore a 34-round related-key rectangle distinguisher, which can be directly used to mount a related-key rectangle attack on 38-round SHACAL-2. Furthermore, by Property 3, we can partially determine whether a candidate quartet is a valid one earlier than usual; if not, we can discard it immediately, which results in less computations in the left steps and may allow us to proceed by guessing one or more round subkeys, depending on how many candidate quartets are remaining. We call this technique "early abort". In the case for SHACAL-2, we find that the "early abort" technique can allow us to break two more rounds, that is to say, 40-round SHACAL-2 can be broken faster than an exhaustive key search. Finally, based on several delicate observations, we mount a related-key rectangle attack on 42-round SHACAL-2. The details are as follows.

A 34-Round Related-Key Rectangle Distinguisher The key schedule of SHACAL-2 has low difference propagations for the first several rounds. Particularly, as exploited in [14], if the two related user keys K and K^* have zero

differences in the first 16 rounds ($0 \sim 15$) except the eighth round key K^8, one can easily learn from Eq. (1) in the key schedule that the keys from rounds 16 until 22 ($K^{16}, K^{17}, \cdots, K^{22}$) have all zero differences. Consequently, Kim *et al.* [14] exploited a 23-round related-key differential characteristic[3] $\alpha \rightarrow \beta$ for Rounds $0 \sim 22$ with probability 2^{-33}: $(0, 0, e_{6,9,18,20,25,29}, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}) \rightarrow (0, 0, 0, 0, 0, 0, 0, 0)$. This 23-round related-key differential characteristic requires 22 fixed bits in any pair of plaintexts to increase the differential probability for Round 0.

Then, they exploited a 10-round differential characteristic $\gamma \rightarrow \delta$ for Rounds $23 \sim 32$ with probability 2^{-74}: $(0, e_{9,18,29}, 0, 0, e_{31}, e_{6,9,18,20,25,29}, 0, 0) \rightarrow (e_{11,23}, e_{3,14,15,24,25}, e_{5,27}, e_{9,18,29}, e_{31}, 0, 0, 0)$.

As a result, a 33-round related-key rectangle distinguisher with probability $2^{-470} (= (2^{-33} \cdot 2^{-74})^2 \cdot 2^{-256})$ can be obtained by combining these two differentials. Finally, by counting many possible 10-round differentials $\gamma' \rightarrow \delta$ for Rounds $23 \sim 32$, they obtained a lower bound $2^{-464.32} (= (2^{-33} \cdot 2^{-71.16})^2 \cdot 2^{-256})$ for the probability of this 33-round distinguisher. Based on this 33-round related-key rectangle distinguisher, Kim *et al.* presented a related-key rectangle attack on 37-Round SHACAL-2.

However, we find that the property that the 22-th round key is the furthest round key such that all the round keys from Rounds 16 to 22 have all zero differences is just for the case that the two related user keys K and K^* have non-zero difference in only one of the first 16 round keys. If we study the key schedule more delicately, allowing two, three or more round keys of the first 16 round keys have non-zero differences, we can get that the 23-th round key is the furthest round key such that all the round keys from Rounds 16 to 23 have all zero differences, which requires that K and K^* have the difference e_{31} in both the 0-th and 9-th round keys and have all zero differences in the others of the first 16 round keys. This observation has already been introduced as Property 4 in Sect. 3. Thus, we get one more round with a zero subkey difference than Kim *et al.*. Moreover, we observe that these related keys K and K^* produce $K^{24} = L_0 \boxplus L_1$ and $K^{*24} = L_0 \boxplus (L_1 \oplus e_{13,24,28})$, respectively, where $L_0 = \sigma_1(K^{22}) \boxplus K^{17} \boxplus K^8$ and $L_1 = \sigma_0(K^9)$.

Now, we face the problem: could these delicate properties of the key schedule incur a 34-round related-key rectangle distinguisher such that its probability is far greater than 2^{-512} ? Our answer is positive.

Note that e_{31} happens to be the difference in the eighth round key K_8 in the Kim *et al.*'s 23-round related-key differential characteristic. It follows that we can append one more round in the beginning of the Kim *et al.*'s 23-round related-key differential characteristic with the first round key difference e_{31}, which results in a 24-round related-key differential characteristic with probability 2^{-66}:

[3] We notice that the probability of the second round of the first differential characteristic presented in [14] is 2^{-13}, and not 2^{-11} as claimed. Hence, the 23-round related-key differential characteristic holds with probability 2^{-33}, not 2^{-31} as claimed in [14]. However, it can be repaired with a little more complexity by the way described below. The corrected probability 2^{-33} is used in our paper.

Table2. The 24-round related-key differential characteristic for E^0 (Rounds 1 to 24) and the preceding differential for E^b (Round 0), where $M = \{6, 9, 18, 20, 25, 29\}$

Round(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}	$\cdot$	$e_{9,13,19}$	$e_{18,29}$	e_{31}	$\cdot$	e_{31}	$\cdot$
1	0	0	e_M	e_{31}	0	$e_{9,13,19}$	$e_{18,29}$	e_{31}	0	1
2	e_{31}	0	0	e_M	0	0	$e_{9,13,19}$	$e_{18,29}$	0	2^{-12}
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	$e_{6,20,25}$	0	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
$\vdots$				$\vdots$					$\vdots$	$\vdots$
23	0	0	0	0	0	0	0	0	0	1
24	0	0	0	0	0	0	0	0	$\cdot$	2^{-6}
25	$e_{13,24,28}$	0	0	0	$e_{13,24,28}$	0	0	0	$\cdot$	$\cdot$

$(0, e_{6,9,18,20,25,29}, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}, e_{2,3,7,8,13,16,20,26,30}) \rightarrow (0, 0, 0, 0, 0, 0, 0, 0)$. Similar to the Kim *et al.*'s attack, we can adopt some delicate improvements to conduct a related-key rectangle attack on 38-round SHACAL-2 based on this 24-round related-key differential and our 10-round differential below. Nevertheless, to make maximal use of Property 3, we will use this appended round for a key recovery in our following attacks on 40 and 42-round SHACAL-2. Further, let's consider the round key difference $K^{24} \oplus K^{*24}$ in Round 24. Obviously, many difference possibilities are caused due to the addition modulo 2^{32} operations in the key schedule. This round key is then taken the addition modulo 2^{32} operation with the output of Round 23. Due to the zero difference in the output of Round 23, we can count over the possibilities for all the additions together when we compute $\widehat{p^*}$ in the following. Here, we can add one more round to the end of the Kim *et al.*'s 23-round related-key differential characteristic to obtain a 24-round ($1 \sim 24$) related-key differential characteristic $\alpha \rightarrow \beta$ with probability 2^{-38}: $(0, 0, e_{6,9,18,20,25,29}, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}) \rightarrow (e_{13,24,28}, 0, 0, 0, e_{13,24,28}, 0, 0, 0)$. See Table 2 for details. Note that our 24-round related-key differential characteristic described in Table 2 requires the following 12-bit conditions on the two inputs to Round 1, $(A^1, B^1, C^1, D^1, E^1, F^1, G^1, H^1)$ and $(A^{*1}, B^{*1}, C^{*1}, D^{*1}, E^{*1}, F^{*1}, G^{*1}, H^{*1})$ whose difference is α:

$$\begin{array}{cccc} a_6^1 = b_6^1, & a_9^1 = b_9^1, & a_{18}^1 = b_{18}^1, & a_{20}^1 = b_{20}^1, \\ a_{25}^1 = b_{25}^1, & a_{29}^1 = b_{29}^1, & a_{31}^1 = b_{31}^1, & e_9^1 = 0, \\ e_{13}^1 = 0, & e_{18}^1 = 1, & e_{19}^1 = 0, & e_{29}^1 = 1, \end{array} \tag{2}$$

Table3. The 10-round differential characteristic for E^1 (Rounds 25 to 34), where $M' = \{6, 9, 18, 20, 25, 29, 31\}$

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	·

where a_i^1, b_i^1 and e_i^1 are the i-th bits of A^1, B^1 and E^1, respectively. If the two input values to Round 1 meet the α difference and Eq. (2), we can remove the differential probabilities incurred by the Ch and Maj functions in Rounds 1 and 2 (for Round 2, only the condition $a_{31}^1 = b_{31}^1$ is used).

On the other hand, we can use the Kim *et al.*'s 10-round differential characteristic for Rounds 25 to 34 to construct a 34-round related-key rectangle distinguisher. However, we explore a more powerful 10-round differential characteristic $\gamma \rightarrow \delta$ for Rounds $25 \sim 34$: $(e_{31}, e_{31}, e_{6,9,18,20,25,29,31}, 0, 0, e_{9,13,19}, e_{18,29,31}, 0) \rightarrow (e_{6,9,18,20,25,29}, e_{31}, 0, 0, e_{6,20,25}, e_{31}, 0, 0)$ [4], which holds with probability 2^{-65}. See Table 3.

To compute $\widehat{p^*}$ (resp., $\widehat{q}$) (defined in Sect. 2.3), we need to sum the square of the probabilities of all the differentials with the input difference α through E^0 (resp., all the differentials with the output difference δ through E^1), which is computationally infeasible. As a countermeasure, to compute $\widehat{p^*}$, we can count some of such possible differentials that have the same first 23-round differences as the 24-round related-key differential characteristic in Table 2. The 192-bit difference $(\Delta B^{25}, \Delta C^{25}, \Delta D^{25}, \Delta F^{25}, \Delta G^{25}, \Delta H^{25})$ in such a possible output difference of Round 24 can be determined to be all 0's by the corresponding 192-bit difference in the input difference to Round 24, therefore, we only need to count the possible 64-bit output difference $(\Delta A^{25}, \Delta E^{25})$ of Round 24. By counting 42 possible differentials, we can compute a lower bound $2^{-37} (\approx (2^{-38 \cdot 2} + 6 \cdot 2^{-39 \cdot 2} + 15 \cdot 2^{-40 \cdot 2} + 20 \cdot 2^{-41 \cdot 2})^{\frac{1}{2}})$ for the probability $\widehat{p^*}$ of the 24-round differentials $\alpha \rightarrow \beta'$. The upper part of Table 4 gathers some of these differences according to their probabilities. Similarly, we can compute a lower bound $2^{-63.38} (= (2 \cdot 2^{-65 \cdot 2} + 22 \cdot 2^{-66 \cdot 2} + 32 \cdot 2^{-67 \cdot 2})^{\frac{1}{2}})$ for the probability $\widehat{q}$ of the 10-round differentials $\gamma' \rightarrow \delta$ by counting 56 out

[4] Note that this 10-round differential can be also used to improve the Kim *et al.*'s 33-round related-key rectangle distinguisher.

Table4. Possible differences in E^0 and E^1 with their respective probability

Prob.	$(\Delta A^{25}, \Delta E^{25})$ in E^0
2^{-38}	$(e_{13,24,28}, e_{13,24,28})$
2^{-39}	$(e_{13,14,24,28}, e_{13,24,28}), (e_{13,24,25,28}, e_{13,24,28}), (e_{13,24,28,29}, e_{13,24,28}),$ $(e_{13,24,28}, e_{13,14,24,28}), (e_{13,24,28}, e_{13,24,25,28}), (e_{13,24,28}, e_{13,24,28,29})$
Prob.	$(\Delta D^{25}, \Delta H^{25})$ in E^1
2^{-65}	$(0,0), (0, e_{31})$
2^{-66}	$(e_9, e_9), (e_{18}, e_{18}), (e_{29}, e_{29}), (0, e_9), (0, e_{13}), (0, e_{18}), (e_{18}, e_{31}), (e_9, e_{31}),$ $(0, e_{19}), (0, e_{29}), (0, e_{9,31}), (0, e_{13,31}), (0, e_{18,31}), (e_{29}, 0), (e_{18}, 0), (e_9, 0),$ $(0, e_{19,31}), (0, e_{29,31}), (e_9, e_{9,31}), (e_{18}, e_{18,31}), (e_{29}, e_{29,31}), (e_{29}, e_{31})$

of those that have the same last 9-round differential as the 10-round differential in Table 3: $(e_{31}, e_{31}, e_{6,9,18,20,25,29,31}, \Delta D^{25}, 0, e_{9,13,19}, e_{18,29,31}, \Delta H^{25}) \rightarrow (e_{6,9,18,20,25,29}, e_{31}, 0, 0, e_{6,20,25}, e_{31}, 0, 0)$. The lower part of Table 4 lists some of these $(\Delta D^{25}, \Delta H^{25})$ according to their probabilities. Therefore, we can obtain a lower bound $2^{-456.76} (= (2^{-37} \cdot 2^{-63.38})^2 \cdot 2^{-256})$ for the probability of our 34-round related-key rectangle distinguisher (Rounds 1 to 34).

4.1 Attacking 40-Round SHACAL-2

We are now ready to explain our related-key rectangle attack on 40-round SHACAL-2. Assume that 40-round SHACAL-2 uses related keys K and K^* whose difference is $(e_{31}, 0, 0, 0, 0, 0, 0, 0, 0, e_{31}, 0, 0, 0, 0, 0, 0)$. First, we use the 34-round related-key rectangle distinguisher to obtain a small portion of subkey candidates in Rounds 0, 35, 36, 37, 38 and 39. Second, we do an exhaustive search for the obtained subkey candidates and the remaining key bits to recover the 512-bit related keys K and K^*. In order to apply the 34-round distinguisher to this attack, we need to collect enough input pairs to Round 1 which meet the α difference and Eq. (2). For this, we use enough pairs of plaintext structures. The details of our attack are as follows:

1. Choose $2^{178.38}$ structures S_i of 2^{64} plaintexts $P_{i,l}$ each, $i = 1, 2, \cdots, 2^{178.38}$, $l = 1, 2, \cdots, 2^{64}$, where in each structure the 192 bits of words A, B, C, E, F, G are fixed. With a chosen plaintext attack scenario, obtain all their corresponding ciphertexts under the key K, denoted $C_{i,l}$.
2. Compute $2^{178.38}$ structures S_i^* of 2^{64} plaintexts each by XORing the plaintexts in S_i with the 256-bit value $(0, e_{6,9,18,20,25,29}, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}, 0)$. With a chosen plaintext attack scenario, obtain all their corresponding ciphertexts under the key K^*.
3. Guess a 32-bit subkey K^0 in Round 0 and compute $K^{*0} = K^0 \oplus e_{31}$. Encrypt each plaintext $P_{i,l}$ through Round 0 with K^0 to get its intermediate value just after Round 0. We denote the encrypted value by $x_{i,l}$. Check if $x_{i,l}$ meets

Eq. (2). If yes, compute $x^*_{i,l} = x_{i,l} \oplus \alpha$ and then decrypt $x^*_{i,l}$ through Round 0 with K^{*0} to get its plaintext, denoted by $P^*_{i,l}$. Find $P^*_{i,l}$ in S^*_i. We denote by $C^*_{i,l}$ the corresponding ciphertext for $P^*_{i,l}$.

4. Guess a 96-bit subkey pair $((K^{37}, K^{38}, K^{39}), (K^{*37}, K^{*38}, K^{*39}))$ in Rounds 37, 38 and 39. For the guessed subkey pair, do the following:
   (a) Decrypt all the ciphertexts $C_{i,l}$ through Rounds 37, 38 and 39 with K^{37}, K^{38} and K^{39} to get their intermediate values just before Round 37. We denote these values by $C^{37}_{i,l}$. Keep them in a table. Decrypt all the ciphertexts $C^*_{i,l}$ through Rounds 37, 38 and 39 with K^{*37}, K^{*38} and K^{*39} to get their intermediate values just before Round 37. We denote these values by $C^{*37}_{i,l}$. Keep them in another table.
   (b) Check if $C^{37}_{i_0,l_0} \oplus C^{37}_{i_1,l_1}$ and $C^{*37}_{i_0,l_0} \oplus C^{*37}_{i_1,l_1}$ belong to $\delta(2)$, for all $1 \leq i_0 < i_1 \leq 2^{178.38}$, $1 \leq l_0, l_1 \leq 2^{64}$ and all $1 \leq i_0 = i_1 \leq 2^{178.38}$, $1 \leq l_0 < l_1 \leq 2^{64}$, where $\delta(2)$ is the set of all the possible differences caused by the δ difference after 2 rounds. Record $(K^0, K^{37}, K^{38}, K^{39})$ and all the qualified quartets and then go to Step 5.
5. Guess a 32-bit subkey pair (K^{36}, K^{*36}) in Round 36. For the guessed subkey pair, do the following:
   (a) For each remaining quartet $(C^{37}_{i_0,l_0}, C^{37}_{i_1,l_1}, C^{*37}_{i_0,l_0}, C^{*37}_{i_1,l_1})$, decrypt $C^{37}_{i_0,l_0}$ and $C^{37}_{i_1,l_1}$ through Round 36 with K^{36} to get their intermediate values just before Round 36, and decrypt $C^{*37}_{i_0,l_0}$ and $C^{*37}_{i_1,l_1}$ through Round 36 with K^{*36} to get their intermediate values just before Round 36. We denote the decrypted quartet by $(C^{36}_{i_0,l_0}, C^{36}_{i_1,l_1}, C^{*36}_{i_0,l_0}, C^{*36}_{i_1,l_1})$.
   (b) Check if $C^{36}_{i_0,l_0} \oplus C^{36}_{i_1,l_1}$ and $C^{*36}_{i_0,l_0} \oplus C^{*36}_{i_1,l_1}$ belong to $\delta(1)$, where $\delta(1)$ is the set of all the possible differences caused by the δ difference after 1 round. Record $(K^0, K^{36}, K^{37}, K^{38}, K^{39})$ and all the qualified quartets and then go to Step 6.
6. Guess a 32-bit subkey pair (K^{35}, K^{*35}) in Round 35. For the guessed subkey pair, do the following:
   (a) For each remaining quartet $(C^{36}_{i_0,l_0}, C^{36}_{i_1,l_1}, C^{*36}_{i_0,l_0}, C^{*36}_{i_1,l_1})$, decrypt $C^{36}_{i_0,l_0}$ and $C^{36}_{i_1,l_1}$ through Round 35 with K^{35} to get their intermediate values just before Round 35, and decrypt $C^{*36}_{i_0,l_0}$ and $C^{*36}_{i_1,l_1}$ through Round 35 with K^{*35} to get their intermediate values just before Round 35. We denote the decrypted quartet by $(C^{35}_{i_0,l_0}, C^{35}_{i_1,l_1}, C^{*35}_{i_0,l_0}, C^{*35}_{i_1,l_1})$.
   (b) Check if $C^{35}_{i_0,l_0} \oplus C^{35}_{i_1,l_1} = C^{*35}_{i_0,l_0} \oplus C^{*35}_{i_1,l_1} = \delta$. If there exist more than 5 quartets passing this δ test, record $(K^0, K^{35}, K^{36}, K^{37}, K^{38}, K^{39})$ and go to Step 7. Otherwise, repeat Step 6 with another guessed key pair (if all the possible key pairs for Round 35 are tested, then repeat Step 5 with another guessed key pair for Round 36; if all the possible key pairs for Round 36 are tested, then repeat Step 4 with another guessed key pair for Rounds 37, 38 and 39; if all the possible key pairs for Rounds 37, 38 and 39 are tested, then repeat Step 3 with another guessed key pair for Round 0).

7. For a suggested $(K^0, K^{35}, K^{36}, K^{37}, K^{38}, K^{39})$, do an exhaustive search for the remaining 320 key bits using trial encryption. If a 512-bit key is suggested, output it as the master key of the 40-round SHACAL-2. Otherwise, run the above steps with another guess of subkey pair.

This attack requires $2^{243.38}$ related-key chosen plaintexts. The required memory for this attack is dominated by Step 4, which is approximately $2^{243.38} \cdot 32 \approx 2^{247.38}$ memory bytes.

The time complexities of Steps 1 and 2 are $2^{243.38}$ 40-round SHACAL-2 encryptions each. The time complexity of Step 3 is about $(2^{242.38} + 2^{230.38}) \cdot 2^{32} \cdot \frac{1}{40} \approx 2^{269.06}$ 40-round SHACAL-2 encryptions, for Eq. (2) has a 12-bit filtering. Moreover, for each guessed subkey pair, we have about $2^{230.38 \times 2}/2 = 2^{459.76}$ quartets tested in Step 4. Since the decryptions in Step 4 can be done independent of Step 3, Step 4 requires about $2^{231.38} \cdot 2^{192} \cdot \frac{3}{40} \approx 2^{419.64}$ 40-round SHACAL-2 encryptions and about $2^{231.38} \cdot 2^{192} \cdot 2^{32} = 2^{455.38}$ memory accesses.

From the difference δ, we can definitely determine the differences in words C, D, G, and H of every possible difference in the set $\delta(2)$. Moreover, we observe that there are about 2^{28} possible differences in word B and 2^{17} possible differences in F. Hence, there are about $2^{64+28+17} = 2^{109}$ possible differences in $\delta(2)$. It follows that about $2^{459.76} \cdot 2^{(-256+109)\cdot 2} = 2^{165.76}$ quartets are suggested in Step 4. Since Step 5-(a) runs about 2^{288} times (equivalent to the number of guessed subkey pairs), it requires about $2^{165.76} \cdot 4 \cdot 2^{288} \cdot \frac{1}{40} \approx 2^{450.43}$ 40-round SHACAL-2 encryptions. Similarly, $\delta(1)$ and δ additionally have a 64-bit and a 45-bit filterings, so about $2^{165.76} \cdot 2^{-64\cdot 2} = 2^{37.76}$ and $2^{37.76} \cdot 2^{-45\cdot 2} = 2^{-52.24}$ quartets (for each wrong guess of subkey pairs) are expected to be suggested in Steps 5 and 6, respectively, and thus Step 6 requires $2^{37.76} \cdot 4 \cdot 2^{352} \cdot \frac{1}{40} \approx 2^{386.43}$ 40-round SHACAL-2 encryptions. By the Poisson distribution $X \sim Poi(\lambda = 2^{-52.24})$, $Pr_X[X > 5] \approx 2^{-323}$, the expected number of wrong subkey pairs suggested in Step 6 is about $2^{-323} \cdot 2^{352} = 2^{29}$. It follows that the time complexity of Step 7 is about $2^{349} (= 2^{29} \cdot 2^{320})$ 40-round SHACAL-2 encryptions. Therefore, the total time complexity of this attack is about $2^{450.43}$ 40-round SHACAL-2 encryptions.

If the guessed subkey pair is right, then the expected number of the quartets suggested in Step 6 is about $2^{459.76} \cdot 2^{-456.76} = 2^3$, for about $2^{459.76}$ quartets are tested in this attack and the 34-round related-key rectangle distinguisher holds with probability $2^{-456.76}$. Thus, the probability that the number of remaining quartets for the right subkey pair is more than 5 is 0.8 by the Poisson distribution, $X \sim Poi(\lambda = 2^3)$, $Pr_X[X > 5] \approx 0.8$. Hence, this attack works with a success probability of 0.8.

Note: We can reduce the time complexity of our attack on 40-round SHACAL-2 in Section 4.1 to about $2^{448.43}$ 40-round SHACAL-2 encryptions by adopting the following two delicate improvements: First, we only guess the least significant 31 bits of the subkey K^0 in Step 3, due to the fact that the most significant bit in the key difference is fixed. Second, we guess the least significant 31 bits of the subkey pairs (K^{36}, K^{*36}) and the difference between their most significant bits to check the $\delta(1)$ test in Step 5, instead of guessing all the 32-bit values of the

subkey pairs. In Step 6, we guess the least significant 31 bits of the subkey pairs (K^{35}, K^{*35}) and the difference between their most significant bits to check the δ test. Since the total time complexity of this attack is dominated by Step 5-(a), it is reduced by a factor of 4.

4.2 Attacking 42-Round SHACAL-2

We find that the above attack can be improved to break as far as 42-round SHACAL-2 by guessing additive differences between related subkey pairs, instead of guessing actual values of them. Our improved attack is based on the following observations.

Observation 1: If we know the actual values of $(A^i, B^i, \cdots, H^i)$ and $(A^{*i}, B^{*i}, \cdots, H^{*i})$, and the additive difference between K^{i-1} and K^{*i-1}, then we know the actual values of $(A^{i-1}, B^{i-1}, \cdots, G^{i-1})$ and $(A^{*i-1}, B^{*i-1}, \cdots, G^{*i-1})$, and the additive difference between H^{i-1} and H^{*i-1}.

Observation 2: If we know the actual values of $(A^{i-1}, B^{i-1}, \cdots, G^{i-1})$ and $(A^{*i-1}, B^{*i-1}, \cdots, G^{*i-1})$, and the additive difference between H^{i-1} and H^{*i-1}, then we know the actual values of $(A^{i-5}, B^{i-5}, C^{i-5})$ and $(A^{*i-5}, B^{*i-5}, C^{*i-5})$, and the additive difference between D^{i-5} and D^{*i-5}.

Observation 3: The additive difference between 32-bit words X and Y is the same as their XOR difference if $X \oplus Y = 0$ or $X \oplus Y = e_{31}$.

Based on these observations the above attack algorithm can be improved to an attack on 42-round SHACAL-2. Here, we use the early abort technique one step earlier. Let's briefly describe the attack procedure as follows:

- We perform the above Steps 1, 2 and 3.
- In Step 4, we guess a 64-bit subkey pair $((K^{40}, K^{41}), (K^{*40}, K^{*41}))$ and an additive difference between K^{39} and K^{*39}, and then decrypt all the ciphertexts to obtain the actual values of $(A^{39}, B^{39}, \cdots, G^{39})$ and $(A^{*39}, B^{*39}, \cdots, G^{*39})$, and the additive difference between H^{39} and H^{*39} (by Observation 1). It allows to know (A^{35}, B^{35}, C^{35}) and $(A^{*35}, B^{*35}, C^{*35})$, and the additive difference between D^{35} and D^{*35} (by Observation 2), so we can discard some wrong quartets by checking if the decrypted quartets satisfy the first half of the δ difference. Since it has a 256-bit filtering for the decrypted quartets, about $2^{459.76} \cdot 2^{-256} = 2^{203.76}$ quartets are suggested. This step requires about $2^{64 \cdot 2+32} \cdot 2^{231.38} \cdot \frac{7}{42} = 2^{388.80}$ 42-round SHACAL-2 encryptions and $2^{64 \cdot 2+64} \cdot 2^{231.38} = 2^{423.38}$ memory accesses.
- In Step 5, we guess a 64-bit subkey pair of (K^{38}, K^{39}) and (K^{*38}, K^{*39}) (note the additive difference between K^{39} and K^{*39} is fixed in the previous step), and then decrypt all the remaining quartets to obtain their input values of round 38. Since H^{38} is the same as E^{35}, we can discard all the quartets which do not satisfy the $e_{6,20,25}$ XOR difference in H^{38}. It has a 64-bit

filtering for the decrypted quartets, so about $2^{203.76} \cdot 2^{-64} = 2^{139.76}$ quartets are suggested. This step requires about $2^{64 \cdot 4+32} \cdot 2^{203.76+2} \cdot \frac{1}{42} = 2^{488.37}$ 42-round SHACAL-2 encryptions.

– In Step 6, we guess an additive difference between K^{37} and K^{*37} to check if the remaining quartets satisfy the e_{31} difference in H^{37}, which is the same as F^{35}. In Step 7, we guess a 64-bit subkey pair of (K^{36}, K^{37}) and (K^{*36}, K^{*37}) (note the additive difference between K^{37} and K^{*37} is fixed in the previous step) to check if the remaining quartets satisfy zero difference in H^{36}, which is the same as G^{35}. In Step 8, we guess a 64-bit subkey pair of (K^{35}, K^{36}) and (K^{*35}, K^{*36}) (note the additive difference between K^{36} and K^{*36} is fixed in the previous step) to check if the remaining quartets satisfy zero difference in H^{35}. We go to the final step with the guessed subkey pair which has more than 5 remaining quartets. Finally, in Step 9, we do an exhaustive search to find the 512-bit master keys. Each of Steps 6, 7, 8 and 9 takes a dramatically less time complexity than Step 5.

Therefore, the time complexity of the attack is dominated by Step 5, which is about $2^{488.37}$ 42-round SHACAL-2 encryptions. Obviously, the attack is faster than an exhaustive key search.

5 Conclusions

In this paper, we exploit a 34-round related-key rectangle distinguisher after finding a delicate property in the key schedule of SHACAL-2. We also introduce a differential property that can allow us to apply the "early abort" technique to discard some disqualified candidate quartets earlier than usual. Based on them, we mount a related-key rectangle attack on 40-round SHACAL-2. Finally, based on several more delicate observations, we improve it to a related-key rectangle attack on 42-round SHACAL-2. Table 5 compares the results obtained in this paper with the previous ones on SHACAL-2 when used with 512 key bits.

Table5. Comparison of our result and previous ones on SHACAL-2

Type of Attack	*Rounds*	*Data*	*Time*	*Memory*	*Source*
Impossible differential	30	744CP	$2^{495.1}$	$2^{14.5}$	[9]
Differential-nonlinear	32	$2^{43.4}$CP	$2^{504.2}$	$2^{48.4}$	[21]
Square-nonlinear	28	$463 \cdot 2^{32}$CP	$2^{494.1}$	$2^{45.9}$	[21]
RK differential-nonlinear	35	$2^{42.32}$RK-CP	$2^{452.10}$	$2^{47.32}$	[14]
RK Rectangle	37†	$2^{235.16}$RK-CP	$2^{486.95}$	$2^{240.16}$	[14]
	40	$2^{243.38}$RK-CP	$2^{448.43}$	$2^{247.38}$	This paper
	42	$2^{243.38}$RK-CP	$2^{488.37}$	$2^{247.38}$	This paper

RK: Related-Key, CP: Chosen Plaintexts, Memory unit: Byte, Time unit: Encryption
†: The indicated attack complexity is a corrected one

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 helpful advice.

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, A. Biryukov and A. Shamir, Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials, Advances in Cryptology — EUROCRYPT'99, J. Stern (ed.), Volume 1592 of Lecture Notes in Computer Science, pp. 12–23, Springer-Verlag, 1999.
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, Related-key boomerang and rectangle attacks, Advances in Cryptology — EUROCRYPT'05, R. Cramer (ed.), Volume 3494 of Lecture Notes in Computer Science, pp. 507–525, Springer-Verlag, 2005.
6. E. Biham and A. Shamir, Differential cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
7. H. Handschuh and D. Naccache, SHACAL, Proceedings of first open NESSIE workshop, 2000. Archive available at *https://www.cosic.esat.kuleuven.be/nessie/ workshop/submissions.html*
8. H. Handschuh and D. Naccache, SHACAL, NESSIE, 2001. Archive available at *https://www.cosic.esat.kuleuven. be/nessie/tweaks.html*
9. S. Hong, J. Kim, G. Kim, J. Sung, C. Lee and S. Lee, Impossible differential attack on 30-round SHACAL-2, Proceedings of INDOCRYPT'03, T. Johansson and S. Maitra (eds.), Volume 2904 of Lecture Notes in Computer Science, pp. 97–106, Springer-Verlag, 2003.
10. 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.
11. 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
12. 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.
13. 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.

14. J. Kim, G. Kim, S. Lee, J. Lim and J. Song, Related-key attacks on reduced rounds of SHACAL-2, Proceedings of INDOCRYPT'04, A. Canteaut and K. Viswanathan (eds.), Volume 3348 of Lecture Notes in Computer Science, pp. 175–190, Springer-Verlag, 2004.
15. S. K. Langford and M. E. Hellman, Differential-linear cryptanalysis, Advances in Cryptology — CRYPTO'94, Y. Desmedt (ed.), Volume 839 of Lecture Notes in Computer Science, pp. 17–25, Springer-Verlag, 1994.
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. U.S. Department of Commerce, Secure Hash Standard FIPS 180-1, N.I.S.T., 1995.
20. U.S. Department of Commerce, Secure Hash Standard FIPS 180-2, N.I.S.T., 2002.
21. Y. Shin, J. Kim, G. Kim, S. Hong and S. Lee, Differential-linear type attacks on reduced rounds of SHACAL-2, Proceedings of ACISP'04, H. Wang, J. Pieprzyk, and V. Varadharajan (eds.), Volume 3108 of Lecture Notes in Computer Science, pp. 110–122, Springer-Verlag, 2004.
22. 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.