IEICE TRANS. FUNDAMENTALS, VOL.E91–A, NO.9 SEPTEMBER 2008

PAPER

Attacking 44 Rounds of the SHACAL-2 Block Cipher Using Related-Key Rectangle Cryptanalysis

Jiqiang LU[†a)], ***Student Member and*** **Jongsung KIM**[††b)], ***Nonmember***

SUMMARY SHACAL-2 is a 64-round block cipher with a 256-bit block size and a variable length key of up to 512 bits. It is a NESSIE selected block cipher algorithm. In this paper, we observe that, when checking whether a candidate quartet is useful in a (related-key) rectangle attack, we can check the two pairs from the quartet one after the other, instead of checking them simultaneously; if the first pair does not meet the expected conditions, we can discard the quartet immediately. We next exploit a 35-round related-key rectangle distinguisher with probability 2^{-460} for the first 35 rounds of SHACAL-2, which is built on an existing 24-round related-key differential and a new 10-round differential. Finally, taking advantage of the above observation, we use the distinguisher to mount a related-key rectangle attack on the first 44 rounds of SHACAL-2. The attack requires 2^{233} related-key chosen plaintexts, and has a time complexity of $2^{497.2}$ computations. This is better than any previously published cryptanalytic results on SHACAL-2 in terms of the numbers of attacked rounds.

key words: *block cipher, SHACAL-2, differential cryptanalysis, related-key rectangle attack*

1. Introduction

SHACAL-2 is a 64-round block cipher with a 256-bit block size and a variable length key of up to 512 bits, which was proposed in 2001 by Handschuh and Naccache [6] as a submission to the NESSIE (New European Schemes for Signatures, Integrity and Encryption) project [16]; it is based on the compression function of SHA-256 [17], an ISO hash function international standard, where the plaintext enters the compression function as the chaining value, and the key enters the compression function as the message block. In 2003, SHACAL-2 became a NESSIE selected block cipher algorithm, after a thorough analysis of its security and performance.

The published cryptanalytic results on SHACAL-2 are as follows. In 2003, Hong et al. [7] presented an impossible differential attack [2], [14] on 30-round SHACAL-2. In 2004, Shin et al. [18] presented a square-nonlinear attack on 28-round SHACAL-2 and a differential-nonlinear attack on 32-round SHACAL-2. Also in 2004, Kim et al. [12] presented a related-key differential-nonlinear attack on 35-round SHACAL-2 and a related-key rectangle attack [11] on 37-round SHACAL-2, where the latter is based on a 33-round related-key rectangle distinguisher. In 2006, Lu et al. [15] presented a related-key rectangle attack on 42-round SHACAL-2, after exploiting a 34-round related-key rectangle distinguisher with probability $2^{-456.76}$ and then adopting the proposed early abort technique. In 2007, Wang [20] presented a related-key rectangle attack on 43-round SHACAL-2, by extending Lu et al.'s 34-round related-key rectangle distinguisher to a 35-round distinguisher with probability $2^{-474.76}$.

In this paper, we find that there is a flaw in Wang's attack algorithm on 43-round SHACAL-2, which makes the attack infeasible. We exploit a more powerful 35-round related-key rectangle distinguisher which has a probability of 2^{-460}, following the previous work described in [15], [20]. More importantly, we observe that, when checking whether a candidate quartet is useful in a (related-key) rectangle attack, we can check the two pairs from the quartet one after the other, instead of checking them simultaneously; if the first pair does not meet the expected conditions, we can discard the quartet immediately. This can reduce the computation complexity of an attack, and, even more significantly, may allow us to break more rounds of a cipher. Taking advantage of this observation, we finally use the 35-round related-key rectangle distinguisher to conduct a related-key rectangle attack on the first 44 rounds of SHACAL-2. This is better than any previously published cryptanalytic results on SHACAL-2 in terms of the numbers of attacked rounds. Table 1 summarises both previous and our new cryptanalytic results on SHACAL-2 that uses 512 key bits.

The rest of this paper is organised as follows. In the next section, we describe some notation and the SHACAL-2 block cipher. In Sect. 3, we introduce our observation on related-key rectangle attacks. In Sect. 4, we give the 35-round related-key rectangle distinguisher with probability 2^{-460}, as well as the flaw in Wang's attack. In Sect. 5, we present our related-key rectangle attack on 44-round SHACAL-2. Section 6 concludes this paper.

Manuscript received January 28, 2008.
Manuscript revised March 21, 2008.

[†]The author is with the Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 OEX, UK.
He as well as his work was supported by a British Chevening/Royal Holloway Scholarship and the European Commission under contract IST-2002-507932 (ECRYPT).

[††]The author is with the Center for Information Security Technologies (CIST), Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea.
He was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2008-(C1090-0801-0025)).

a) E-mail: lvjiqiang@hotmail.com
b) E-mail: joshep@cist.korea.ac.kr
DOI: 10.1093/ietfec/e91–a.9.2588

Table 1 Summary of previous and our new cryptanalytic results on SHACAL-2.

Type of Attack	*Rounds*	*Data*	*Time*	*Memory*	*Source*
Impossible diff.	30	744 CP	$2^{495.1}$	$2^{14.5}$	[7]
Square	28	$2^{40.9}$ CP	$2^{494.1}$	$2^{45.9}$	[18]
Differential	32	$2^{43.4}$ CP	$2^{504.2}$	$2^{48.4}$	[18]
Related-key diff.	35	$2^{42.4}$ RK-CP	$2^{452.1}$	$2^{47.4}$	[12]
Related-key rectangle	37	$2^{235.2}$ RK-CP	2^{487}	$2^{240.2}$	[12]
	42	$2^{243.4}$ RK-CP	$2^{488.4}$	$2^{247.4}$	[15]
	43†	$2^{240.4}$ RK-CP	$2^{480.4}$	$2^{245.4}$	[20]
	44	2^{233} RK-CP	$2^{497.2}$	2^{238}	This

diff.: differential, CP: Chosen Plaintexts, RK: Related-Key,
Time unit: Encryptions, Memory unit: Bytes,
†: The attack has a flaw; see Sect. 4.2 of this paper.

2. Preliminaries

2.1 Notation

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

The notion of difference used throughout this paper is with respect to the $\oplus$ operation, unless otherwise stated explicitly.

2.2 The SHACAL-2 Block Cipher

SHACAL-2 [6] takes as input a 256-bit plaintext, and has a total of 64 rounds. Its encryption procedure can be described as follows.

1. The 256-bit plaintext P is represented as 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:

$$
\begin{aligned}
T_1^{i+1} &= K^i \boxplus \Sigma_1(E^i) \boxplus Ch(E^i, F^i, G^i) \boxplus H^i \boxplus W^i,\\
T_2^{i+1} &= \Sigma_0(A^i) \boxplus Maj(A^i, B^i, C^i),\\
H^{i+1} &= G^i,\\
G^{i+1} &= F^i,\\
F^{i+1} &= E^i,\\
E^{i+1} &= D^i \boxplus T_1^{i+1},\\
D^{i+1} &= C^i,\\
C^{i+1} &= B^i,\\
B^{i+1} &= A^i,\\
A^{i+1} &= T_1^{i+1} \boxplus T_2^{i+1}.
\end{aligned}
$$

3. The ciphertext C is $(A^{64}, B^{64}, C^{64}, D^{64}, E^{64}, F^{64}, G^{64}, H^{64})$.

In the above description, K^i is the i-th round key, W^i is the i-th round constant, and the four functions $\Sigma_0(X)$, $\Sigma_1(X)$, $Ch(X, Y, Z)$ and $Maj(X, Y, Z)$ are defined as follows.

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

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

The key schedule of SHACAL-2 accepts 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. 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. Finally, the i-th round key $(16 \le i \le 63)$ is generated as follows,

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

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

3. An Observation on Related-Key Rectangle Attacks

In this section, we introduce our observation on related-key rectangle attacks.

3.1 Description of Related-Key Rectangle Attacks

A related-key rectangle attack [4], [8], [11] is a combination of a related-key attack [1], [13] and a rectangle attack [3]. A related-key attack requires an assumption that the attacker knows the specific differences between one or more pairs of unknown keys; this assumption makes it difficult or even infeasible to conduct in many cryptographic applications, but some of the current real-world applications allow for practical related-key attacks [10], for example, key-exchange protocols and hash functions. A rectangle attack is a variant of the boomerang attack [19] and an improvement of the amplified boomerang attack [9]. As a result, they share the same basic idea of using two (or more) short differentials with larger probabilities instead of a long differential with a smaller probability.

A related-key rectangle attack is based on a related-key rectangle distinguisher, which treats a block cipher $\mathbf{E} : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ as a cascade of two subciphers $\mathbf{E} = \mathbf{E}^1 \circ \mathbf{E}^0$ and requires that there exists a related-key differential $\Delta\alpha \to \Delta\beta$ with probability p for $\mathbf{E}^0$: $\Pr_{X\in\{0,1\}^n}[\mathbf{E}^0_{K_A}(X) \oplus \mathbf{E}^0_{K_B}(X \oplus \alpha) = \beta] = \Pr_{X\in\{0,1\}^n}[\mathbf{E}^0_{K_C}(X) \oplus \mathbf{E}^0_{K_D}(X \oplus \alpha) = \beta] = p$, and a related-key differential $\Delta\gamma \to \Delta\delta$ with probability q for $\mathbf{E}^1$: $\Pr_{X\in\{0,1\}^n}[\mathbf{E}^1_{K_A}(X) \oplus \mathbf{E}^1_{K_C}(X \oplus \gamma) = \delta] = \Pr_{X\in\{0,1\}^n}[\mathbf{E}^1_{K_B}(X) \oplus \mathbf{E}^1_{K_D}(X \oplus \gamma) = \delta] = q$, where the four unknown user keys K_A, K_B, K_C and K_D satisfy $K_B = K_A \oplus \Delta K_0$, $K_C = K_A \oplus \Delta K_1$ and $K_D = K_C \oplus \Delta K_0$, with ΔK_0 and ΔK_1 being two known differences.

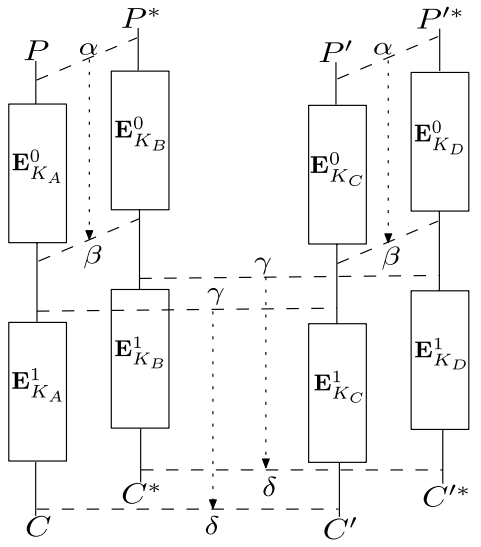


Fig. 1 A related-key rectangle distinguisher.

A quartet consists of two pairs of plaintexts $(P, P^* = P \oplus \alpha)$ and $(P', P'^* = P' \oplus \alpha)$. It is useful only if the two pairs (P, P^*) and (P', P'^*) satisfy the following three conditions; see Fig. 1.

$$\text{C1: } \mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_B}(P^*) = \mathbf{E}^0_{K_C}(P') \oplus \mathbf{E}^0_{K_D}(P'^*) = \beta, \quad (1)$$

$$\text{C2: } \mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_C}(P') = \mathbf{E}^0_{K_B}(P^*) \oplus \mathbf{E}^0_{K_D}(P'^*) = \gamma, \quad (2)$$

$$\text{C3: } \mathbf{E}^1_{K_A}(\mathbf{E}^0_{K_A}(P)) \oplus \mathbf{E}^1_{K_C}(\mathbf{E}^0_{K_C}(P')) = \mathbf{E}^1_{K_B}(\mathbf{E}^0_{K_B}(P^*)) \oplus \mathbf{E}^1_{K_D}(\mathbf{E}^0_{K_D}(P'^*)) = \delta. \quad (3)$$

By assuming that the intermediate values after $\mathbf{E}^0$ distribute uniformly over all possible values, we can get $\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_C}(P') = \gamma$ with probability 2^{-n}. Once this occurs, by C1 we know that $\mathbf{E}^0_{K_B}(P^*) \oplus \mathbf{E}^0_{K_D}(P'^*) = \gamma$ holds with probability 1, for $\mathbf{E}^0_{K_B}(P^*) \oplus \mathbf{E}^0_{K_D}(P'^*) = (\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_B}(P^*)) \oplus (\mathbf{E}^0_{K_C}(P') \oplus \mathbf{E}^0_{K_D}(P'^*)) \oplus (\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_C}(P')) = \beta \oplus \beta \oplus \gamma = \gamma$.

As a result, by summarising all the possible β and γ, we get that the probability that the quartet satisfies C3 is expected to be about $\sum_{\beta,\gamma}(\Pr(\Delta\alpha \to \Delta\beta))^2 \cdot 2^{-n} \cdot (\Pr(\Delta\gamma \to \Delta\delta))^2 = 2^{-n} \cdot (\widehat{p} \cdot \widehat{q})^2$, where $\widehat{p} = (\sum_\beta \Pr^2(\Delta\alpha \to \Delta\beta))^{\frac{1}{2}}$ and $\widehat{q} = (\sum_\gamma \Pr^2(\Delta\gamma \to \Delta\delta))^{\frac{1}{2}}$. For a random function, this probability is about $2^{-n\times 2} = 2^{-2n}$.

Therefore, if $\widehat{p} \cdot \widehat{q} > 2^{-n/2}$, the related-key rectangle distinguisher can distinguish between $\mathbf{E}$ and a random function, given sufficient chosen plaintext pairs.

Note that there exist three kinds of related-key rectangle attacks, which correspond to the following three cases.

- Type 1: $\Delta K_0 \neq 0, \Delta K_1 \neq 0$, (four keys);
- Type 2: $\Delta K_0 = 0, \Delta K_1 \neq 0$, (two keys);
- Type 3: $\Delta K_0 \neq 0, \Delta K_1 = 0$, (two keys).

3.2 The Observation

A typical related-key rectangle attack treats a block cipher $\mathbf{E} : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ as a cascade of four sub-ciphers $\mathbf{E} = \mathbf{E}^b \circ \mathbf{E}^1 \circ \mathbf{E}^0 \circ \mathbf{E}^a$, where $\mathbf{E}^1 \circ \mathbf{E}^0$ denotes the rounds for the rectangle distinguisher, $\mathbf{E}^a$ denotes the rounds before $\mathbf{E}^0$, and $\mathbf{E}^b$ denotes the rounds after $\mathbf{E}^1$. Suppose K^a_A, K^a_B, K^a_C and K^a_D are the subkeys used in $\mathbf{E}^a$, which correspond to K_A, K_B, K_C and K_D, respectively; and K^b_A, K^b_B, K^b_C and K^b_D are the subkeys used in $\mathbf{E}^b$, which correspond to K_A, K_B, K_C and K_D, respectively.

Given a guess for the subkeys used in $\mathbf{E}^a$ and $\mathbf{E}^b$, the attacker tries to check whether a candidate quartet $((\widetilde{P}, \widetilde{P}^*), (\widetilde{P}', \widetilde{P}'^*))$ meets the difference conditions required by the related-key rectangle distinguisher, that is, the following two conditions.

$$\mathbf{E}^a_{K^a_A}(\widetilde{P}) \oplus \mathbf{E}^a_{K^a_B}(\widetilde{P}^*) = \mathbf{E}^a_{K^a_C}(\widetilde{P}') \oplus \mathbf{E}^a_{K^a_D}(\widetilde{P}'^*) = \alpha, \quad (4)$$

$$\mathbf{E}^{b,-1}_{K^b_A}(\widetilde{C}) \oplus \mathbf{E}^{b,-1}_{K^b_C}(\widetilde{C}') = \mathbf{E}^{b,-1}_{K^b_B}(\widetilde{C}^*) \oplus \mathbf{E}^{b,-1}_{K^b_D}(\widetilde{C}'^*) = \delta, \quad (5)$$

where $\widetilde{C} = \mathbf{E}_{K_A}(\widetilde{P})$, $\widetilde{C}^* = \mathbf{E}_{K_B}(\widetilde{P}^*)$, $\widetilde{C}' = \mathbf{E}_{K_C}(\widetilde{P}')$, $\widetilde{C}'^* = \mathbf{E}_{K_D}(\widetilde{P}'^*)$, and $\mathbf{E}^{b,-1}$ denotes the inverse of $\mathbf{E}^b$.

In a chosen-plaintext attack scenario, the general approach to meet the conditions described in Eq. (4) is to choose the pairs $(\widetilde{P}, \widetilde{P}^*)$ and $(\widetilde{P}', \widetilde{P}'^*)$ in the following way.

1. Choose a plaintext, $\widetilde{P}$ say, and encrypt it with $\mathbf{E}^a$ under the guess for K^a_A; we denote the encrypted value by $\mathbf{E}^a_{K^a_A}(\widetilde{P})$.
2. Compute $\mathbf{E}^a_{K^a_A}(\widetilde{P}) \oplus \alpha$, and decrypt it with $\mathbf{E}^a$ under the guess for K^a_B; the decrypted value is what we look for $\widetilde{P}^*$.
3. Choose the pair $(\widetilde{P}', \widetilde{P}'^*)$ in the same way as described above.

Obviously, the quartet $((\widetilde{P}, \widetilde{P}^*), (\widetilde{P}', \widetilde{P}'^*))$, selected in the above way, meets the conditions described in Eq. (4). The remaining problem is to check whether it also meets the conditions described in Eq. (5).

The key schedules of some block ciphers make it possible for us to know the subkey differences involved in $\mathbf{E}^b$ from the user key differences ΔK_0 and ΔK_1, especifically those with linearity. Thus, to check whether the candidate quartet $((\widetilde{P}, \widetilde{P}^*), (\widetilde{P}', \widetilde{P}'^*))$ meets the conditions in Eq. (5), we do not need to guess all the four unknown subkeys; we just guess one or more of them, and then XOR them with the subkey differences to get the remaining unknown subkeys. Whereas the key schedules of some block ciphers make it impossible for us to determine the subkey differences involved in $\mathbf{E}^b$ from the user key differences ΔK_0 and ΔK_1; thus it is necessary to guess the four[†] unknown subkeys K^b_A, K^b_B, K^b_C and K^b_D to check whether the candidate quartet $((\widetilde{P}, \widetilde{P}^*), (\widetilde{P}', \widetilde{P}'^*))$ meets the conditions in Eq. (5).

[†]We consider the general related-key rectangle attack with four keys here; similar for the case with two keys.

Previously, this is usually done by guessing the four subkeys at once, and then simultaneously decrypting both the pairs $(\widetilde{C}, \widetilde{C}')$ and $(\widetilde{C}^*, \widetilde{C}'^*)$ to check whether they meet the conditions in Eq. (5). However, in 2006, Lu et al. [15] found that it may be possible to partially determine whether or not a candidate quartet in a related-key rectangle attack is useful one or more rounds earlier than usual. Specifically, from Eq. (5) we know the expected output difference δ after $\mathbf{E}^1$. Thus, if we know the expected output differences of one or more rounds after $\mathbf{E}^1$, we can guess part of the subkeys K_A^b, K_B^b, K_C^b and K_D^b such that we can check whether a candidate quartet meets one of the expected output differences of the one or more rounds after $\mathbf{E}^1$. If not, we can discard it immediately; otherwise, we guess part (or all) of the remaining of the subkeys K_A^b, K_B^b, K_C^b and K_D^b, and check the quartet similarly. Since some candidate quartets are discarded before the next subkey guess, this results in less computations in the following steps, and may allow us to break more rounds, depending on how many candidate quartets are remaining and how many subkeys are required to guess. This is called the early abort technique [15].

We further observe that the early abort technique can be conducted in a more efficient way. Our observation focuses on a single application of the early abort technique. To make things clearer, we assume that the round immediately following $\mathbf{E}^1$ is the target round for an application of the early abort technique, and, to simplify our explanation we assume that $\mathbf{E}^b$ has only this round (by this we can continue to use the above notation for the ciphertexts and subkeys without defining more). The observation is as follows. We can first guess the two subkeys K_A^b and K_C^b connected with the pair $(\widetilde{C}, \widetilde{C}')$, and then check whether the pair meets the condition $\mathbf{E}_{K_A^b}^{b,-1}(\widetilde{C}) \oplus \mathbf{E}_{K_C^b}^{b,-1}(\widetilde{C}') = \delta$. If the pair does not meet this condition, then we can discard the candidate quartet; if it does meet the condition, then we guess the other two subkeys K_B^b and K_D^b connected with the other pair $(\widetilde{C}^*, \widetilde{C}'^*)$, and check whether this pair meets the condition $\mathbf{E}_{K_B^b}^{b,-1}(\widetilde{C}^*) \oplus \mathbf{E}_{K_D^b}^{b,-1}(\widetilde{C}'^*) = \delta$. The candidate quartet is useful if, and only if, every pair meets the respective conditions.

This can reduce the computational workload of a related-key rectangle attack, and, even more significantly, may allow us to break more rounds of a cipher, depending on the distinguisher used and the round structure of the cipher. Note that this observation can be also used to improve a rectangle attack, although this improvement is usually small (generally, a factor of $\frac{1}{2}$ on the computational workload).

4. A 35-Round Related-Key Rectangle Distinguisher with Probability 2^{-460} of SHACAL-2

In this section, we exploit a 35-round related-key rectangle distinguisher with probability 2^{-460} for Rounds 0 to 34, following the previous work described in [15], [20]; the distinguisher belongs to Type 3. Besides, we give the flaw in Wang's attack on 43-round SHACAL-2.

4.1 The 34-Round Related-Key Rectangle Distinguisher Due to Lu et al.

In 2006, Lu et al. [15] gave a 24-round related-key differential $(0, 0, e_{6,9,18,20,\ 25,29}, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}) \rightarrow (e_{13,24,28}, 0, 0, 0, e_{13,24,28}, 0, 0, 0)$ with probability 2^{-38} for Rounds 1 to 24[†] and a 10-round differential $(e_{31}, e_{31}, e_{6,9,18,20,25,29,31}, 0, 0, e_{9,13,19}, e_{18,29,31}, 0) \rightarrow (e_{6,9,18,20,25,29}, e_{31}, 0, 0, e_{6,20,25}, e_{31}, 0, 0)$ with probability 2^{-65} for Rounds 25 to 34.

They computed a square sum of at least $2^{-74} (= 2^{-37\times 2})$ for the probabilities of all the 24-round related-key differentials for Rounds 1 to 24 that have only the output differences different from the above 24-round differential, and a square sum of at least $2^{-126.76} (= 2^{-63.38\times 2})$ for the probabilities of all the 10-round differentials for Rounds 25 to 34 that have only the input differences different from the above 10-round differential.

As a result, they exploited a 34-round related-key rectangle distinguisher with probability $2^{-456.76} (= 2^{-74} \cdot 2^{-126.76} \cdot 2^{-256})$ for Rounds 1 to 34, which was finally used to break the first 42 rounds of SHACAL-2 along with the proposed early abort technique.

4.2 The 35-Round Related-Key Rectangle Distinguisher Due to Wang

In 2007, Wang [20] found that Lu et al.'s 34-round related-key rectangle distinguisher can be extended to a 35-round distinguisher by appending one-round related-key differential with probability 1 at the beginning: given a plaintext pair $P = (A^0, B^0, C^0, D^0, E^0, F^0, G^0, H^0)$ and $\widetilde{P} = (\overline{A}^0, \overline{B}^0, \overline{C}^0, \overline{D}^0, \overline{E}^0, \overline{F}^0, \overline{G}^0, \overline{H}^0)$ with some fixed bits as described in Eq. (6), (where x_i^0 denotes the i-th bit of X^0), the 25-round related-key differential with probability 2^{-47} for Rounds 0 to 24 is $(0, e_{6,9,18,20,25,29}, e_{31}, 0, e_{9,13,19}, e_{18,29}, e_{31}, \Delta') \rightarrow (e_{13,24,28}, 0, 0, 0, e_{13,24,28}, 0, 0, 0)$, where $\Delta' = \Sigma_1(E^0) - \Sigma_1(E^0 \oplus e_{9,13,19})$ and the key difference is $K \oplus \widetilde{K} = (\Delta K^0, \Delta K^1, \cdots, \Delta K^{15}) = (e_{31}, 0, 0, 0, 0, 0, 0, 0, 0, e_{31},\ 0, 0, 0, 0, 0, 0, 0, 0)$. See Table 2 for more details.

$$\begin{aligned} &a_{31}^0 = b_{31}^0,\ a_i^0 = c_i^0,\ \text{for } i = 6, 9, 18, 20, 25, 29;\\ &b_9^0 = \neg e_9^0,\ a_i^0 = \neg f_i^0,\ \text{for } i = 19, 30;\\ &e_i^0 = 0,\ \text{for } i = 18, 29, 30;\\ &f_i^0 = g_i^0,\ \text{for } i = 9, 13, 19. \end{aligned} \tag{6}$$

The second differential for the 35-round distinguisher is the same 10-round differential as that used in the 34-round related-key rectangle distinguisher due to Lu et al.

As a result, Wang exploited a 35-round related-key rectangle distinguisher with probability $(2^{-46})^2 \cdot 2^{-126.76} \cdot 2^{-256} = 2^{-474.76}$, which was used to break the first 43 rounds of SHACAL-2.

[†]Certain input bits are fixed to meet several conditions.

Table 2 The 25-round related-key differential for Rounds 0 to 24, 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}	0	$e_{9,13,19}$	$e_{18,29}$	e_{31}	Δ'	e_{31}	1
1	0	0	e_M	e_{31}	0	$e_{9,13,19}$	$e_{18,29}$	e_{31}	0	2^{-11}
2	e_{31}	0	0	e_M	0	0	$e_{9,13,19}$	$e_{18,29}$	0	2^{-10}
3	0	e_{31}	0	0	$e_{6,20,25}$	0	0	$e_{9,13,19}$	0	2^{-7}
4	0	0	e_{31}	0	0	$e_{6,20,25}$	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
⋮				⋮					⋮	⋮
23	0	0	0	0	0	0	0	0	0	1
24	0	0	0	0	0	0	0	0	·	2^{-6}
output	$e_{13,24,28}$	0	0	0	$e_{13,24,28}$	0	0	0	/	/

Table 3 The 10-round differential for Rounds 25 to 34, 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	Prob.
25	0	0	e_M	e_{31}	0	$e_{9,13,19}$	$e_{13,18,29}$	$e_{13,31}$	2^{-11}
26	e_{31}	0	0	e_M	0	0	$e_{9,13,19}$	$e_{13,18,29}$	2^{-14}
27	0	e_{31}	0	0	$e_{6,20,25}$	0	0	$e_{9,13,19}$	2^{-7}
28	0	0	e_{31}	0	0	$e_{6,20,25}$	0	0	2^{-4}
29	0	0	0	e_{31}	0	0	$e_{6,20,25}$	0	2^{-3}
30	0	0	0	0	e_{31}	0	0	$e_{6,20,25}$	2^{-4}
31	0	0	0	0	0	e_{31}	0	0	2^{-1}
32	0	0	0	0	0	0	e_{31}	0	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}
output	e_M	e_{31}	0	0	$e_{6,20,25}$	e_{31}	0	0	/

However, we find a flaw in Wang's attack algorithm, which makes the attack infeasible.

4.2.1 A Flaw in Wang's Attack

In Wang's attack [20], the probability that 6 or more quartets pass the filtering condition in Step 6 is about $\sum_{i=6}^{2^{31.76}} [\binom{2^{31.76}}{i} \cdot (2^{-32\times2})^i \cdot (1 - 2^{-32\times2})^{2^{31.76}-i}] \approx 2^{-202.93}$, so it is expected that about $2^{448} \cdot 2^{-202.93} = 2^{245.07}$ guesses of $((K^{36}, \cdots, K^{42}), (K^{*36}, \cdots, K^{*42}))$ are suggested in Step 6. Thus, to find the 512-bit user key by exhaustively searching for the remaining 288 bits, Step 7 is expected to have a time complexity much larger than 2^{512}. Therefore, unlike what the author claimed, the attack cannot break 43-round SHACAL-2 (faster than an exhaustive key search).

4.3 A 35-Round Related-Key Rectangle Distinguisher with Probability 2^{-460}

We exploit a more powerful 10-round differential for Rounds 25 to 34: $(0, 0, e_{6,9,18,20,25,29}, e_{31}, 0, e_{9,13,19}, e_{18,19}, e_{31}) \rightarrow (e_{6,9,18,20,25,29}, e_{31}, 0, 0, e_{6,20,25}, e_{31}, 0, 0)$, which has a probability of 2^{-56}. See Table 3 for more details.

Using this 10-round differential with probability 2^{-56} and the 25-round related-key differential with probability 2^{-47} due to Wang, we get a new 35-round related-key rectangle distinguisher, which has a probability of at least 2^{-460} $(= (2^{-46} \cdot 2^{-56})^2 \cdot 2^{-256})$ for the correct key, and has a probability of $(2^{-256})^2 = 2^{-512}$ for a wrong key.

5. Related-Key Rectangle Attack on 44-Round SHACAL-2

Assume that the two related user keys are K and $\widetilde{K}$. First, we review the following differential property of SHACAL-2, which allows us to break more rounds by using the early abort technique proposed in [15].

Property 1 (from [15], [20]): If the values of $(A^i, B^i, \cdots, H^i)$ and $(\overline{A}^i, \overline{B}^i, \cdots, \overline{H}^i)$, and the additive difference between K^{i-1} and $\widetilde{K}^{i-1}$ are known, then we can get the values of $(A^{i-1}, B^{i-1}, \cdots, G^{i-1})$ and $(\overline{A}^{i-1}, \overline{B}^{i-1}, \cdots, \overline{G}^{i-1})$, the additive difference between H^{i-1} and $\overline{H}^{i-1}$, the values of $(A^{i-5}, B^{i-5}, C^{i-5})$ and $(\overline{A}^{i-5}, \overline{B}^{i-5}, \overline{C}^{i-5})$, and the additive dif-

ference between D^{i-5} and $\overline{D}^{i-5}$.

From the key schedule of SHACAL-2, we know that it is impossible to determine the subkey differences of the last few rounds (to be attacked) from the user key difference $K \oplus \widetilde{K}$; thus, to conduct an early abort on a candidate quartet it is necessary to guess the two unknown subkeys in every such a round, corresponding to K and $\widetilde{K}$. In previous related-key rectangle attacks on reduced-round SHACAL-2 presented in [15], [20], this is done by first guessing both the round subkeys at a time, then partially decrypting a candidate quartet to get its corresponding quartet just before this round, and finally checking whether it meets difference conditions. However, as described in Sect. 3, we can check the two pairs from a candidate quartet one after the other; more specifically, when we conduct an early abort on a candidate quartet, we first check whether one pair from the quartet is useful, by guessing only the single subkey involved. If not, then this quartet is not useful, thus we can discard it immediately; otherwise, we check the other pair by guessing the other subkey. The candidate quartet is useful if, and only if, both the pairs are useful.

We can use the 35-round distinguisher given in Sect. 4 to mount the following related-key rectangle attack on the first 44 rounds of SHACAL-2. The observation described in Sect. 3.2 plays a crucial role on the efficiency of our attack; otherwise, the distinguisher would enable us to break just the first 43 rounds of SHACAL-1 in a similar way as described in [15].

1. Choose a set S of 2^{232} plaintexts $P_i = (A_i^0, B_i^0, C_i^0, D_i^0, E_i^0, F_i^0, G_i^0, H_i^0)$, under the condition of Eq. (6), ($i = 1, 2, \cdots, 2^{232}$). In a chosen-plaintext attack scenario, obtain all their corresponding ciphertexts under the key K; we denote them by C_i, respectively.
2. Compute another set $\widetilde{S}$ of 2^{232} plaintexts $\widetilde{P}_i = (\overline{A}^0, \overline{B}^0, \overline{C}^0, \overline{D}^0, \overline{E}^0, \overline{F}^0, \overline{G}^0, \overline{H}^0) = (A_i^0, B_i^0 \oplus e_{6,9,18,20,25,29}, C_i^0 \oplus e_{31}, D_i^0, E_i^0 \oplus e_{9,13,19}, F_i^0 \oplus e_{18,29}, G_i^0 \oplus e_{31}, H_i^0 + \Sigma_1(E_i^0) - \Sigma_1(E_i^0 \oplus e_{9,13,19}) \bmod 2^{32})$. In a chosen-plaintext attack scenario, obtain all their corresponding ciphertexts under the related key $\widetilde{K} = K \oplus (e_{31}, 0, 0, 0, 0, 0, 0, 0, 0, e_{31}, 0, 0, 0, 0, 0, 0)$; we denote them by $\widetilde{C}_i$, respectively.
3. Guess a 128-bit subkey pair $((K^{40}, K^{41}, K^{42}, K^{43}), (\widetilde{K}^{40}, \widetilde{K}^{41}, \widetilde{K}^{42}, \widetilde{K}^{43}))$ in Rounds 40, 41, 42 and 43. Then, partially decrypt all the ciphertexts C_i through Rounds 43–40 with $(K^{43}, K^{42}, K^{41}, K^{40})$ to get their intermediate values just before Round 40; we denote them by C_i^{40}, respectively. Partially decrypt all the ciphertexts $\widetilde{C}_i$ through Rounds 43–40 with $(\widetilde{K}^{43}, \widetilde{K}^{42}, \widetilde{K}^{41}, \widetilde{K}^{40})$ to get their intermediate values just before Round 40; we denote them by $\widetilde{C}_i^{40}$, respectively. Keep $(C_i^{40}, \widetilde{C}_i^{40})$ in a hash table. This process proposes about $2^{232\times 2}/2 = 2^{463}$ candidate quartets $(C_{i_0}^{40}, \widetilde{C}_{i_0}^{40}, C_{i_1}^{40}, \widetilde{C}_{i_1}^{40})$, where $1 \le i_0 \le i_1 \le 2^{232}$. By Property 1, we know $(A_{i_0}^{35}, B_{i_0}^{35}, C_{i_0}^{35})$, $(A_{i_1}^{35}, B_{i_1}^{35}, C_{i_1}^{35})$, $(\overline{A}_{i_0}^{35}, \overline{B}_{i_0}^{35}, \overline{C}_{i_0}^{35})$, $(\overline{A}_{i_1}^{35}, \overline{B}_{i_1}^{35}, \overline{C}_{i_1}^{35})$, the additive difference between $D_{i_0}^{35}$ and $D_{i_1}^{35}$, and the additive difference between $\overline{D}_{i_0}^{35}$ and $\overline{D}_{i_1}^{35}$. Finally, we choose only the quartets $(C_{i_0}^{40}, \widetilde{C}_{i_0}^{40}, C_{i_1}^{40}, \widetilde{C}_{i_1}^{40})$ such that $(A_{i_0}^{35}, B_{i_0}^{35}, C_{i_0}^{35}) \oplus (A_{i_1}^{35}, B_{i_1}^{35}, C_{i_1}^{35}) = (e_{6,9,18,20,25,29}, e_{31}, 0)$, $(\overline{A}_{i_0}^{35}, \overline{B}_{i_0}^{35}, \overline{C}_{i_0}^{35}) \oplus (\overline{A}_{i_1}^{35}, \overline{B}_{i_1}^{35}, \overline{C}_{i_1}^{35}) = (e_{6,9,18,20,\ 25,29}, e_{31}, 0)$, and $D_{i_0}^{35} - D_{i_1}^{35} = \overline{D}_{i_0}^{35} - \overline{D}_{i_1}^{35} = 0$. If 6 or more quartets pass this test, record all the qualified quartets, and go to Step 4; otherwise, repeat this step with another guess.
4. For every remaining quartet $(C_{i_0}^{40}, C_{i_1}^{40}, \widetilde{C}_{i_0}^{40}, \widetilde{C}_{i_1}^{40})$, do the following.
   a. Guess a 32-bit subkey K^{39} in Round 39. Partially decrypt $C_{i_0}^{40}$ and $C_{i_1}^{40}$ through Round 39 with K^{39} to get their intermediate values just before Round 39; we denote them by $C_{i_0}^{39}$ and $C_{i_1}^{39}$, respectively. Thus, we can compute the the additive difference between $H_{i_0}^{38}$ and $H_{i_1}^{38}$ by Property 1; since $H_i^{38} = E_i^{35}$, we choose only the quartets $(C_{i_0}^{40}, C_{i_1}^{40}, \widetilde{C}_{i_0}^{40}, \widetilde{C}_{i_1}^{40})$ such that $H_{i_0}^{38} - H_{i_1}^{38} \in \{\pm 2^6 \pm 2^{20} \pm 2^{25}\}$. If 6 or more quartets pass this test, record all the qualified $(C_{i_0}^{40}, C_{i_1}^{40}, \widetilde{C}_{i_0}^{40}, \widetilde{C}_{i_1}^{40})$, and go to Step 4-(b); otherwise, repeat this step with another guess of K^{39}.
   b. Guess a 32-bit subkey $\widetilde{K}^{39}$ in Round 39. Partially decrypt $\widetilde{C}_{i_0}^{40}$ and $\widetilde{C}_{i_1}^{40}$ through Round 39 with $\widetilde{K}^{39}$ to get their intermediate values just before Round 39; we denote them by $\widetilde{C}_{i_0}^{39}$ and $\widetilde{C}_{i_1}^{39}$, respectively. Similarly, we choose only the quartets $(C_{i_0}^{40}, C_{i_1}^{40}, \widetilde{C}_{i_0}^{40}, \widetilde{C}_{i_1}^{40})$ such that $\overline{H}_{i_0}^{38} - \overline{H}_{i_1}^{38} \in \{\pm 2^6 \pm 2^{20} \pm 2^{25}\}$. If 6 or more quartets pass this test, record all the qualified $(C_{i_0}^{39}, C_{i_1}^{39}, \widetilde{C}_{i_0}^{39}, \widetilde{C}_{i_1}^{39})$, and go to Step 5; otherwise, repeat this step with another guess of $\widetilde{K}^{39}$.
5. For every remaining quartet $(C_{i_0}^{39}, C_{i_1}^{39}, \widetilde{C}_{i_0}^{39}, \widetilde{C}_{i_1}^{39})$, do the following.
   a. Guess a 32-bit subkey K^{38} in Round 38. Partially decrypt $C_{i_0}^{39}$ and $C_{i_1}^{39}$ through Round 38 with K^{38} to get their intermediate values just before Round 38; we denote them by $C_{i_0}^{38}$ and $C_{i_1}^{38}$, respectively. Thus, we can compute $E_{i_0}^{35}$, $E_{i_1}^{35}$, and the additive difference between $H_{i_0}^{37}$ and $H_{i_1}^{37}$. We choose only the quartets $(C_{i_0}^{39}, C_{i_1}^{39}, \widetilde{C}_{i_0}^{39}, \widetilde{C}_{i_1}^{39})$ such that $E_{i_0}^{35} \oplus E_{i_1}^{35} = e_{6,20,25}$ and $H_{i_0}^{37} - H_{i_1}^{37} \in \{\pm 2^{31}\}$. If 6 or more quartets pass this test, record all the qualified $(C_{i_0}^{39}, C_{i_1}^{39}, \widetilde{C}_{i_0}^{39}, \widetilde{C}_{i_1}^{39})$, and go to Step 5-(b); otherwise, repeat this step with another guess of K^{38}.
   b. Guess a 32-bit subkey $\widetilde{K}^{38}$ in Round 38. Partially decrypt $\widetilde{C}_{i_0}^{39}$ and $\widetilde{C}_{i_1}^{40}$ through Round 38 with $\widetilde{K}^{38}$ to get their intermediate values just before Round 38; we denote them by $\widetilde{C}_{i_0}^{38}$ and $\widetilde{C}_{i_1}^{38}$, re-

spectively. Thus, we can compute $\overline{E}^{35}_{i_0}$, $\overline{E}^{35}_{i_1}$, and the additive difference between $\overline{H}^{37}_{i_0}$ and $\overline{H}^{37}_{i_1}$. We choose only the quartets $(C^{40}_{i_0}, C^{40}_{i_1}, \widetilde{C}^{40}_{i_0}, \widetilde{C}^{40}_{i_1})$ such that $\overline{E}^{35}_{i_0} \oplus \overline{E}^{35}_{i_1} = e_{6,20,25}$ and $\overline{H}^{37}_{i_0} - \overline{H}^{37}_{i_1} \in \{\pm 2^{31}\}$. If 6 or more quartets pass this test, record all the qualified $(C^{38}_{i_0}, C^{38}_{i_1}, \widetilde{C}^{38}_{i_0}, \widetilde{C}^{38}_{i_1})$, and go to Step 6; otherwise, repeat this step with another guess of $\widetilde{K}^{38}$.

6. For every remaining quartet $(C^{38}_{i_0}, C^{38}_{i_1}, \widetilde{C}^{38}_{i_0}, \widetilde{C}^{38}_{i_1})$, do the following.
   a. Guess a 32-bit subkey K^{37} in Round 37. Partially decrypt $C^{38}_{i_0}$ and $C^{38}_{i_1}$ through Round 37 with K^{37} to get their intermediate values just before Round 37; we denote them by $C^{37}_{i_0}$ and $C^{37}_{i_1}$, respectively. Thus, we can compute $F^{35}_{i_0}$, $F^{35}_{i_1}$, and the additive difference between $H^{36}_{i_0}$ and $H^{36}_{i_1}$. We choose only the quartets $(C^{38}_{i_0}, C^{38}_{i_1}, \widetilde{C}^{38}_{i_0}, \widetilde{C}^{38}_{i_1})$ such that $F^{35}_{i_0} \oplus F^{35}_{i_1} = e_{31}$ and $H^{36}_{i_0} - H^{36}_{i_1} = 0$. If 6 or more quartets pass this test, record all the qualified $(C^{38}_{i_0}, C^{38}_{i_1}, \widetilde{C}^{38}_{i_0}, \widetilde{C}^{38}_{i_1})$, and go to Step 6-(b); otherwise, repeat this step with another guess of K^{37}.
   b. Guess a 32-bit subkey $\widetilde{K}^{37}$ in Round 37. Partially decrypt $\widetilde{C}^{38}_{i_0}$ and $\widetilde{C}^{38}_{i_1}$ through Round 37 with $\widetilde{K}^{37}$ to get their intermediate values just before Round 37; we denote them by $\widetilde{C}^{37}_{i_0}$ and $\widetilde{C}^{37}_{i_1}$, respectively. Thus, we can compute $\overline{F}^{35}_{i_0}$, $\overline{F}^{35}_{i_1}$, and the additive difference between $\overline{H}^{36}_{i_0}$ and $\overline{H}^{36}_{i_1}$. We choose only the quartets $(C^{38}_{i_0}, C^{38}_{i_1}, \widetilde{C}^{38}_{i_0}, \widetilde{C}^{38}_{i_1})$ such that $\overline{F}^{35}_{i_0} \oplus \overline{F}^{35}_{i_1} = e_{31}$ and $\overline{H}^{36}_{i_0} - \overline{H}^{36}_{i_1} = 0$. If 6 or more quartets pass this test, record all the qualified $(C^{37}_{i_0}, C^{37}_{i_1}, \widetilde{C}^{37}_{i_0}, \widetilde{C}^{37}_{i_1})$, and go to Step 7; otherwise, repeat this step with another guess of $\widetilde{K}^{37}$.
7. For every remaining quartet $(C^{37}_{i_0}, C^{37}_{i_1}, \widetilde{C}^{37}_{i_0}, \widetilde{C}^{37}_{i_1})$, do the following.
   a. Guess a 32-bit subkey K^{36} in Round 36. Partially decrypt $C^{37}_{i_0}$ and $C^{37}_{i_1}$ through Round 36 with K^{36} to get their intermediate values just before Round 36; we denote them by $C^{36}_{i_0}$ and $C^{36}_{i_1}$, respectively. Thus, we can compute the additive difference between $H^{35}_{i_0}$ and $H^{35}_{i_1}$. We choose only the quartets $(C^{37}_{i_0}, C^{37}_{i_1}, \widetilde{C}^{37}_{i_0}, \widetilde{C}^{37}_{i_1})$ such that $H^{35}_{i_0} - H^{35}_{i_1} = 0$. If 6 or more quartets pass this test, record all the qualified $(C^{37}_{i_0}, C^{37}_{i_1}, \widetilde{C}^{37}_{i_0}, \widetilde{C}^{37}_{i_1})$, and go to Step 7-(b); otherwise, repeat this step with another guess of K^{36}.
   b. Guess a 32-bit subkey $\widetilde{K}^{36}$ in Round 36. Partially decrypt $\widetilde{C}^{37}_{i_0}$ and $\widetilde{C}^{37}_{i_1}$ through Round 36 with $\widetilde{K}^{36}$ to get their intermediate values just before Round 36; we denote them by $\widetilde{C}^{36}_{i_0}$ and $\widetilde{C}^{36}_{i_1}$, respectively. Thus, we can compute the additive difference between $\overline{H}^{35}_{i_0}$ and $\overline{H}^{35}_{i_1}$. We choose only the quartets $(C^{37}_{i_0}, C^{37}_{i_1}, \widetilde{C}^{37}_{i_0}, \widetilde{C}^{37}_{i_1})$ such that $\overline{H}^{35}_{i_0} - \overline{H}^{35}_{i_1} = 0$. If 6 or more quartets pass this test, record $(K^{36}, K^{37}, \cdots, K^{42})$, and go to Step 8; otherwise, repeat this step with another guess of $\widetilde{K}^{36}$.
8. For a recorded $(K^{36}, K^{37}, \cdots, K^{43})$, exhaustively search for the remaining 256 bits with one known pair of plaintext and ciphertext. If a 512-bit key is suggested, output it as the user key of the 44-round SHACAL-2; otherwise, repeat Step 3 with another guess.

This attack requires 2^{233} related-key chosen plaintexts. The required memory for this attack is dominated by the ciphertexts, which is approximately $2^{233} \cdot 32 \approx 2^{238}$ memory bytes.

Step 3 has about $2 \cdot 2^{232} \cdot 2^{32\times 8} \cdot \frac{8}{44} \approx 2^{486.54}$ 44-round SHACAL-2 encryptions, and it also requires about $2^{32\times 8} \cdot 2^{232} \cdot \frac{232}{32} = 2^{490.86}$ memory accesses if conducted on a 32-bit computer, which is negligible compared with the $2^{486.54}$ encryptions. Due to the 128-bit filtering condition in Step 3, it is expected that only about $2^{463} \cdot (2^{-128})^2 = 2^{207}$ candidate quartets remain after Step 3 for every key guess.

The time complexity of Step 4-(a) is about $2 \cdot 2^{207} \cdot 2^{32\times 9} \cdot \frac{1}{44} \approx 2^{490.54}$ encryptions. There is a filtering condition of $\frac{2^3}{2^{32}} = 2^{-29}$ in either of Steps 4-(a) and (b). In Step 4-(a), by Poisson distribution, we can know that the probability that 6 or more quartets pass the test for a wrong guess is about 1, thus it follows that all the 2^{288} key guesses pass this step; and about $2^{207} \cdot 2^{-29} = 2^{178}$ candidate quartets remain after this step for every key guess. The time complexity of Step 4-(b) is about $2 \cdot 2^{178} \cdot 2^{32\times 10} \cdot \frac{1}{44} \approx 2^{493.54}$ encryptions. In Step 4-(b), the probability that 6 or more quartets pass the test for a wrong guess is also about 1, thus it follows that all the 2^{320} key guesses pass this step; and about $2^{178} \cdot 2^{-29} = 2^{149}$ candidate quartets remain after this step for every key guess.

The time complexity of Step 5-(a) is about $2 \cdot 2^{149} \cdot 2^{32\times 11} \cdot \frac{1}{44} \approx 2^{496.54}$ encryptions. There is a filtering condition of $\frac{2}{2^{32}} \cdot \frac{1}{2^3} = 2^{-34}$ in either of Steps 5-(a) and (b). In Step 5-(a), the probability that 6 or more quartets pass the test for a wrong guess is about 1, so it follows that all the 2^{352} key guesses pass this step; and about $2^{149} \cdot 2^{-34} = 2^{115}$ candidate quartets remain after this step for every key guess. The time complexity of Step 5-(b) is about $2 \cdot 2^{115} \cdot 2^{32\times 12} \cdot \frac{1}{44} \approx 2^{494.54}$ encryptions. In Step 5-(b), since the probability that 6 or more quartets pass the test for a wrong guess is also about 1, it follows that all the 2^{384} key guesses pass this step; and about $2^{115} \cdot 2^{-34} = 2^{81}$ candidate quartets remain after this step for every key guess.

The time complexity of Step 6-(a) is about $2 \cdot 2^{81} \cdot 2^{32\times 13} \cdot \frac{1}{44} \approx 2^{492.54}$ encryptions. There is a filtering condition of $\frac{1}{2^{32}} \cdot \frac{1}{2} = 2^{-33}$ in either of Steps 6-(a) and (b). In Step 6-(a), the probability that 6 or more quartets pass the test for a wrong guess is about 1 as well, thus it follows that all the 2^{416} key guesses pass this step; and about $2^{81} \cdot 2^{-33} = 2^{48}$ candidate quartets remain after this step for every key guess. The time complexity of Step 6-(b) is about $2 \cdot 2^{48} \cdot 2^{32\times 14} \cdot \frac{1}{44} \approx 2^{491.54}$ encryptions. In Step 6-(b), the probability that 6 or

Table 4 The time complexity of (each step of) the attack.

Step (i)	Time Complexity
1	2^{232} Encryptions
2	2^{232} Encryptions
3	$2^{486.54}$ Encryptions
4	$2^{490.54} + 2^{493.54} \approx 2^{493.71}$ Encryptions
5	$2^{496.54} + 2^{494.54} \approx 2^{496.87}$ Encryptions
6	$2^{492.54} + 2^{491.54} \approx 2^{493.13}$ Encryptions
7	$2^{490.54} + 2^{398.63} \approx 2^{490.54}$ Encryptions
8	$2^{464.51}$ Encryptions
total	$2^{497.2}$ Encryptions

more quartets pass the test for a wrong guess is about 1, thus it follows that all the 2^{448} key guesses pass this step; and about $2^{48} \cdot 2^{-33} = 2^{15}$ candidate quartets remain after this step for every key guess.

The time complexity of Step 7-(a) is about $2 \cdot 2^{15} \cdot 2^{32\times15} \cdot \frac{1}{44} \approx 2^{490.54}$ encryptions. There is a filtering condition of 2^{-32} in either of Steps 7-(a) and (b). In Step 7-(a), the probability that 6 or more quartets pass the test for a wrong guess is about $\sum_{i=6}^{2^{15}}[\binom{2^{15}}{i} \cdot (2^{-32})^i \cdot (1-2^{-32})^{2^{15}-i}] \approx 2^{-111.49}$, thus it follows that about the $2^{480} \cdot 2^{-111.49} = 2^{368.51}$ key guesses pass this step. The time complexity of Step 7-(b) is about $2 \cdot 2^{368.51+32} \cdot 6 \cdot \frac{1}{44} \approx 2^{398.63}$ encryptions. In Step 7-(b), the probability that 6 or more quartets pass the test for a wrong guess is about $(2^{-32})^6 = 2^{-192}$, so it is expected that only about $2^{368.51+32} \cdot 2^{-192} = 2^{208.51}$ guesses of $(K^{36}, K^{37}, \cdots, K^{43})$ pass Step 7-(b), which result in $2^{464.51}$ trials in Step 8.

Table 4 summarises the time complexity of each step of the attack. Therefore, the attack has a total time complexity of approximately $2^{497.2}$ 44-round SHACAL-2 computations, faster than an exhaustive search.

As about 2^{463} quartets are tested in this attack and the 35-round related-key rectangle distinguisher has a probability of 2^{-460}, we can learn that the expected number of the qualified quartets for the correct key guess in Step 7-(b) is about $2^{463} \cdot 2^{-460} = 8$. The probability that 6 or more quartets pass Step 7-(b) is $\sum_{i=6}^{2^{463}}[\binom{2^{463}}{i} \cdot (2^{-460})^i \cdot (1-2^{-460})^{2^{463}-i}] \approx 0.8$, therefore, the related-key rectangle attack works with a success probability of 80%.

6. Conclusions

SHACAL-2 is a NESSIE selected block cipher algorithm. In this paper, we observe that, when checking whether a candidate quartet is useful in a (related-key) rectangle attack, we can check the two pairs from the quartet one after the other, instead of checking them simultaneously; if the first pair does not meet expected conditions, we can discard the quartet immediately. Using this observation, we present a related-key rectangle attack on the first 44 rounds of SHACAL-2, after exploiting a 35-round related-key rectangle distinguisher with probability 2^{-460}. This is the best currently published cryptanalytic result on SHACAL-2.

Acknowledgments

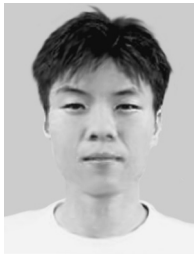
The authors are very grateful to Orr Dunkelman and Nathan Keller for their valuable discussions, and thank Gaoli Wang and the two anonymous reviewers for their comments.

References

[1] E. Biham, "New types of cryptanalytic attacks using related keys," EUROCRYPT'93, ed. T. Helleseth, LNCS 765, pp.398–409, Springer-Verlag, 1993.
[2] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," EUROCRYPT'99, ed. J. Stern, LNCS 1592, pp.12–23, Springer-Verlag, 1999.
[3] E. Biham, O. Dunkelman, and N. Keller, "The rectangle attack—Rectangling the serpent," EUROCRYPT'01, ed. B. Pfitzmann, LNCS 2045, pp.340–357, Springer-Verlag, 2001.
[4] E. Biham, O. Dunkelman, and N. Keller, "Related-key boomerang and rectangle attacks," EUROCRYPT'05, ed. R. Cramer, LNCS 3494, pp.507–525, Springer-Verlag, 2005.
[5] E. Biham and A. Shamir, Differential cryptanalysis of the Data Encryption Standard, Springer, 1993.
[6] H. Handschuh and D. Naccache, SHACAL, NESSIE, 2001.
[7] S. Hong, J. Kim, G. Kim, J. Sung, C. Lee, and S. Lee, "Impossible differential attack on 30-round SHACAL-2," INDOCRYPT'03, eds. T. Johansson and S. Maitra, LNCS 2904, pp.97–106, Springer-Verlag, 2003.
[8] S. Hong, J. Kim, S. Lee, and B. Preneel, "Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192," FSE'05, eds. H. Gilbert and H. Handschuh, LNCS 3557, pp.368–383, Springer-Verlag, 2005.
[9] J. Kelsey, T. Kohno, and B. Schneier, "Amplified boomerang attacks against reduced-round MARS and Serpent," FSE'00, ed. B. Schneier, LNCS 1978, pp.75–93, Springer-Verlag, 2001.
[10] J. Kelsey, B. Schneier, and D. Wagner, "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES," CRYPTO'96, ed. N. Koblitz, LNCS 1109, pp.237–251, Springer-Verlag, 1996.
[11] J. Kim, G. Kim, S. Hong, S. Lee, and D. Hong, "The related-key rectangle attack—Application to SHACAL-1," ACISP'04, eds. H. Wang, J. Pieprzyk, and V. Varadharajan, LNCS 3108, pp.123–136, Springer-Verlag, 2004.
[12] J. Kim, G. Kim, S. Lee, J. Lim, and J. Song, "Related-key attacks on reduced rounds of SHACAL-2," INDOCRYPT'04, eds. A. Canteaut and K. Viswanathan, LNCS 3348, pp.175–190, Springer-Verlag, 2004.
[13] L.R. Knudsen, "Cryptanalysis of LOKI91," ASIACRYPT'92, eds. J. Seberry and Y. Zheng, LNCS 718, pp.196–208, Springer-Verlag, 1993.
[14] L.R. Knudsen, "DEAL—A 128-bit block cipher," Technical report, Department of Informatics, University of Bergen, Norway, 1998.
[15] J. Lu, J. Kim, N. Keller, and O. Dunkelman, "Related-key rectangle attack on 42-round SHACAL-2," ISC'06, eds. S.K. Katsikas, J. Lopez, M. Backes, S. Gritzalis, and B. Preneel, LNCS 4176, pp.85–100, Springer-Verlag, 2006.
[16] NESSIE—New European Schemes for Signatures, Integrity and Encryption, https://www.cosic.esat.kuleuven.be/nessie/
[17] National Institute of Standards and Technology, USA, Secure Hash Standard FIPS 180-2, 2002.
[18] Y. Shin, J. Kim, G. Kim, S. Hong, and S. Lee, "Differential-linear type attacks on reduced rounds of SHACAL-2," ACISP'04, eds. H. Wang, J. Pieprzyk, and V. Varadharajan, LNCS 3108, pp.110–122, Springer-Verlag, 2004.
[19] D. Wagner, "The boomerang attack," FSE'99, ed. L.R. Knudsen, LNCS 1636, pp.156–170, Springer-Verlag, 1999.

[20] G. Wang, "Related-key rectangle attack on 43-Round SHACAL-2," ISPEC'07, eds. E. Dawson and D.S. Wong, LNCS 4464, pp.33–42, Springer-Verlag, 2007.

Jiqiang Lu was born in Gaomi city, Shandong province, CHINA, in November 1977. He received a B.Sc. degree in Applied Mathematics from Yantai University (CHINA) in July 2000 and a M.Eng. degree in Information and Communication Engineering from Xidian University (CHINA) in March 2003. He then served sequentially as a government officer in the Intellectual Property Office of Department of Science & Technology of Shandong Province (CHINA), a research assistant in Information and Communication University (KOREA), and a software engineer in ONETS Wireless&Internet Security Co. Ltd. (CHINA) and the Beijing R&D Institute, Huawei Technologies, Co. Ltd. (CHINA). Currently, he is a Ph.D. candidate in the Information Security Group, Royal Holloway, University of London (UK), and his research topic is cryptanalysis of block ciphers.



Jongsung Kim was born in Chungbuk, SOUTH KOREA, in 1978. He received a Bachelor degree in 2000 and a Master degree in 2002, both in Mathematics from Korea University (KOREA), a Ph.D. degree in Engineering from Katholieke Universiteit Leuven (BELGIUM) in 2006, and a Ph.D. degree in Information Security from Korea University in 2007. Currently, he is a post doctoral researcher of the Center for Information Security Technologies (CIST) at Korea University, and his research topic is symmetric-key cryptography.