The Delicate Issues of Addition with Respect to XOR Differences

Gaoli Wang[1,⋆], Nathan Keller[2,⋆⋆], and Orr Dunkelman[3,⋆⋆⋆]

[1] School of Mathematics and System Sciences, Shandong University
Jinan 250100, China
wanggaoli@mail.sdu.edu.cn

[2] Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, Israel
nkeller@math.huji.ac.il

[3] Katholieke Universiteit Leuven
Dept. of Electrical Engineering ESAT/SCD-COSIC
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
orr.dunkelman@esat.kuleuven.be

Abstract. In this paper we analyze the previous attacks on the block cipher SHACAL-1 and show that all the differential-based attacks fail due to mistreatment of XOR differences through addition. We show that the previously published differential and rectangle attacks on SHACAL-1 fail as some of the underlying differentials are impossible. The related-key rectangle attacks on the cipher generally fail, but if some conditions are imposed on the key (i.e., for a weak key class) they work. After identifying the flaws in previous attacks, we present possible fixes to these attacks. We then present some modified differentials which lead to a related-key rectangle attack which can be applied to 2^{504} weak keys. Our observations are then used to improve a related-key rectangle attack on IDEA by a factor of 2.

Keywords: Related-Key Rectangle attack, Block cipher, SHACAL-1, IDEA.

1 Introduction

Differential cryptanalysis [5] was introduced by Biham and Shamir in 1990, and it is one of the most powerful known attacks on block ciphers. The related-key attack [1] was introduced by Biham in 1993. The attack considers the encryption under two unknown but related keys. The attack's applicability depends on the

[⋆] Supported by National Natural Science Foundation of China Key Project No.90604036 and 973 Program No.2007CB807902.

[⋆⋆] The research presented in this paper was supported by the Adams fellowship.

[⋆⋆⋆] This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy).

C. Adams, A. Miri, and M. Wiener (Eds.): SAC 2007, LNCS 4876, pp. 212–230, 2007.

key schedule algorithm and shows that a block cipher with a weak key schedule algorithm may be vulnerable to this kind of attack. Many cryptanalytic results of this attack model were presented in [6,10,11,12,15].

Illuminated by the complex local collisions of the analysis of SHA-0 which were pointed in the earlier papers in 1997 by X.Y.Wang [25], SHA-0 [24], and SHA-1 [22], we show that in the case of SHACAL-1 [8], all previous differential attacks [2,7,10,13,14,17] fail due to this fact. For example, we show that the attack of [10] uses a differential that can never be satisfied. For other attacks, e.g., the related-key rectangle attack on the full SHACAL-1 in [7], we show that the attack is applicable only to a weak key class (of 2^{496} keys). We show that the combination of XOR differentials (or related-key XOR differentials) when the addition operation is used should be done in a very delicate manner.

After pointing out the problems in the various attacks on SHACAL-1, we try to salvage them. Some of the attacks are fully salvaged, while some others are either shortened (due to lower probabilities of the differentials), or are applicable only in a weak key class (which is larger than previously known).

We then present a related-key rectangle attack on the full SHACAL-1. We use two related-key differentials, where the first one of 33 rounds is built using the technique of modular differences, achieving high probability and correctness. The new attack has a data complexity of 2^{146} related-key chosen plaintexts and time complexity of 2^{465} encryptions. The attack is successful against one out of 256 keys (or more precisely one quartet of keys out of 256 quartets). We summarize the results on SHACAL-1 and our findings in Table 1.

The attack is applicable against the largest set of weak keys (one out of 256). Finally, we show how to improve the 6.5-round rectangle attack on IDEA from [4] by using the additive properties of the differentials. We succeed in reducing the time complexity of the attack by a factor of two.

The rest of the paper is organized as follows: in Section 2, we give the notations used in the paper, present SHACAL-1 and introduce some useful properties of the nonlinear functions in SHACAL-1. Section 3 describes the flaws in previous attacks against SHACAL-1. We present fixes to the various problems in Section 4. In Section 5 we give a related-key rectangle attack on the full SHACAL-1 which can be applied to one out of 2^8 keys (quartets of keys). We improve the 6.5-round related-key rectangle attack on IDEA in Section 6. Finally, we summarize the paper in Section 7.

2 Background

2.1 Notations

Throughout the paper we shall use the following notations which are partially based on these of [21,23]:

- We shall address the words in a little endian manner, where x_0 is the least significant bit of x, and x_{31} is the most significant bit of 32-bit words.

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

Attack	Rounds	Complexity		Observation
		Data	Time	
Differential [14]	30 (0–29)	2^{110} CP	$2^{75.1}$	AF
Differential [14]	41 (0–40)	2^{141} CP	2^{491}	AF
Differential [17]	49 (0–48)	2^{141} CP	$2^{496.5}$	AF
Differential [17]	55 (15–69)	2^{154} CP	$2^{507.3}$	AF
Amplified Boomerang [14]	47 (0–46)	$2^{158.5}$ CP	$2^{508.4}$	AF
Rectangle [2]	47 (0–46)	$2^{151.9}$ CP	$2^{482.6}$	AF
Rectangle [2]	49 (29–77)	$2^{151.9}$ CC	$2^{508.5}$	AF
Rectangle [17]	51 (0–50)	$2^{153.7}$ CP	$2^{503.7}$	AF
Rectangle [17]	52 (28–79)	2^{160} CP	$2^{510.0}$	AF
Related-Key Rectangle [13]	57 (0–56)	$2^{154.8}$ RK-CP	$2^{503.4}$	AF
Related-Key Rectangle [13]	59 (0–58)	$2^{149.7}$ RK-CP	$2^{503.4}$	AF
Related-Key Rectangle [10]	70 (0–69)	$2^{151.8}$ RK-CP	$2^{500.1}$	AF
Related-Key Rectangle [7]	80 (0–79)	$2^{159.8}$ RK-CP	$2^{420.0}$	WK (2^{496})
Related-Key Rectangle [7]	80 (0–79)	$2^{153.8}$ RK-CP	$2^{501.2}$	WK (2^{498})
Related-Key Rectangle (*New*)	70 (0–69)	2^{146} RK-CP	2^{145}	WK (2^{504})
Related-Key Rectangle (*New*)	80 (0–79)	2^{146} RK-CP	2^{465}	WK (2^{504})
Related-Key Rectangle (*New*)	70 (0–69)	2^{144} RK-CP	2^{174}	WK (2^{504})
Related-Key Rectangle (*New*)	80 (0–79)	2^{144} RK-CP	2^{494}	WK (2^{504})
Differential (*New*)	39 (30–68)	2^{144} CC	2^{176}	
Differential (*New*)	49 (20–68)	2^{144} CC	2^{496}	
Rectangle (*New*)	41 (0–40)	$2^{150.3}$ CP	$2^{176.9}$	
Rectangle (*New*)	51 (0–50)	$2^{150.3}$ CP	$2^{496.9}$	

CP: Chosen Plaintexts, CC: Chosen Ciphertexts.
RK-CP: Relate-Key Chosen Plaintexts.
AF: The Attack is Flawed, WK: Weak Key Class (with size).

- $x_i[j]$ and $x_i[-j]$ denote the resulting values by only changing the jth bit of the word x_i. In case the change of the bit is from 0 to 1, then $x_i[j]$ is used and the sign is considered to be positive. Otherwise, $x_i[-j]$ is used and the sign of the difference is negative.
- $x_i[\pm j_1, \pm j_2, \ldots, \pm j_l]$ is the value obtained by changing j_1th, j_2th, ..., j_lth bits of x_i. The "+" sign (which may be omitted) means that the bit is changed from 0 to 1, where the "−" denotes the opposite change.
- $[j]$ denotes a difference in bit j such that the pair (x, x^*) satisfies $x_i^* - x_i = 2^j$ (i.e., $x_i^* = x_i[j]$). $[-j]$ denotes a difference in bit j such that the pair (x, x^*) satisfies $x_i^* - x_i = -2^j$ (i.e., $x_i^* = x_i[-j]$). Similarly, $[j_1, j_2]$ denotes $x_i^* - x_i = 2^{j_1} + 2^{j_2}$ and $[j_1, -j_2]$ denotes $x_i^* - x_i = 2^{j_1} - 2^{j_2}$, etc.
- e_j represents the 32-bit word composed of 31 $0's$ and 1 in the jth place, $e_{j,k} = e_j \oplus e_k$ and $e_{j,k,l} = e_j \oplus e_k \oplus e_l$, etc.
- $\Delta(A, A^*)$ denotes $A^* - A$ or $A^* \oplus A$ according the the value attached to it. $\Delta(A, A^*) = e_j$ stands for XOR difference, i.e., $A^* \oplus A = e_j$. Otherwise $\Delta(A, A^*) = [j]$ stands for an modular difference, i.e., $A^* - A = 2^j$ and $A^* \oplus A = e_j$.

2.2 Description of SHACAL-1

SHACAL-1 [8] is a 160-bit block cipher supporting variable key lengths (0,. . . ,512 bits). It is based on the compression function of the hash function SHA-1 [20] introduced by NIST. The 160-bit plaintext P is divided into five 32-bit words A_0, B_0, C_0, D_0 and E_0. The encryption process iterates the following round function for 80 rounds:

$$\begin{aligned}
A_{i+1} &= K_i + ROTL_5(A_i) + F_i(B_i, C_i, D_i) + E_i + Con_i \\
B_{i+1} &= A_i \\
C_{i+1} &= ROTL_{30}(B_i) \\
D_{i+1} &= C_i \\
E_{i+1} &= D_i
\end{aligned}$$

for $i = 0, \ldots, 79$, where $ROTL_j(X)$ represents rotation of the 32-bit word X to the left by j bits, K_i is the round subkey, Con_i is the round constant, and

$$\begin{aligned}
F_i(X,Y,Z) &= IF(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z), && (0 \leq i \leq 19) \\
F_i(X,Y,Z) &= XOR(X,Y,Z) = X \oplus Y \oplus Z, && (20 \leq i \leq 39, 60 \leq i \leq 79) \\
F_i(X,Y,Z) &= MAJ(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), && (40 \leq i \leq 59)
\end{aligned}$$

The ciphertext is composed of A_{80}, B_{80}, C_{80}, D_{80} and E_{80}.

The key schedule of SHACAL-1 supports a variable key length of 0–512 bits. Keys shorter than 512 bits are first padded with as many zeroes as needed to obtain 512 bits. Let the 512-bit (padded) key be $K = K_0 K_1 \ldots K_{15}$, where K_i is a 32-bit word. The key expansion of 512-bit K to 2560 bits is as follows:

$$K_i = ROTL_1(K_{i-3} \oplus K_{i-8} \oplus K_{i-14} \oplus K_{i-16}), \quad (16 \leq i \leq 79)$$

We note that in [8] a minimal key length of 128-bit is required.

2.3 Several Propositions on the Differential Behavior of Addition and *IF*

In this section we present some properties of additive differences and XOR differences, as well as some properties of the nonlinear function $IF(X,Y,Z)$ which were summarized in [22].

Proposition 1. *Let A_1, A_2 and B be n-bit words, and let $C_i = A_i + B \pmod{2^n}$ for $i = 1, 2$. If $A_1 \oplus A_2 = e_j$ for $0 \leq j \leq n-2$, then $C_1 \oplus C_2 = e_j$ if and only if $C_{i,j} = A_{i,j}$ for $i = 1, 2$ and $0 \leq j \leq n-2$.*

Proof. Assume without loss of generality that $A_{1,j} = 0$. Thus, $A_{2,j} = 1$, and $A_1 + 2^j = A_2$. It follows that $C_2 = C_1 + 2^j$. Hence, if $C_{1,j} = 0$ then $C_{2,j} = 1$ and there is no carry due to the difference, i.e., $C_1 \oplus C_2 = e_j$. In the other way, if $C_1 \oplus C_2 = e_j$, there was no carry by the addition of 2^j to C_1, which means that $C_{1,j} = 0$. Q.E.D.

Proposition 2. *Let A_1, A_2, B_1 and B_2 be n-bit words, and let $C_i = A_i + B_i \pmod{2^n}$ for $i = 1, 2$. If $A_1 \oplus A_2 = B_1 \oplus B_2 = e_j$ for some bit $0 \le j \le n-2$, then $C_1 = C_2$ if and only if $A_{i,j} = \neg B_{i,j}$ for $i = 1, 2$.*

Proof. Without loss of generality assume that $A_{1,j} = 0$ and that $A_{2,j} = 1$, thus, $A_2 = A_1 + 2^j$. If $B_{1,j} = 1$, then it follows that $B_2 = B_1 - 2^j$, and thus $C_1 = C_2$. To prove the other direction we note that $C_1 = C_2$ requires that $B_2 = B_1 - 2^j \pmod{2^n}$. As B_1 and B_2 differ only in one bit, i.e., bit j, it follows that $B_{1,j} = 1$ and $B_{2,j} = 0$. Q.E.D.

Proposition 3. *For the nonlinear function $IF(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$, the following properties hold [21,23]:*

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

3 Flaws in Previously Published Attacks

We find all previous differential attacks on SHACAL-1 have some flaws illuminated by Wang's modular difference. In some cases, these flaws prevent the attacks from being applicable to all keys. The first flaw, which affects the attacks in [2,10,13,14,17] is an impossibility flaw, i.e., the differentials which are used in these attacks can not hold. The second flaw, which affects the related-key attacks in [7,10,13] is the fact that the related-key differential holds only if the key satisfies some conditions. The third flaw is wrong keys which suggest the same number of "right" pairs/quartets as the right key. We show that the same pairs suggest even wrong keys.

3.1 The Use of Differentials with Probability 0

In the attacks of [2,10,13,14,17] there is a part of the differentials (or the related-key differentials) which cannot hold. We present the problem with the related-key differential of [10], but note that the key difference has no affect on the problem, and thus it exists in all the attacks mentioned earlier.

The related-key rectangle attack on 70-round SHACAL-1 [10] uses a 33-round related-key differential characteristic for rounds 0–32 with probability 2^{-45}. The differential characteristic in [10] from round 6 to round 12 is shown in Table 2.

We shall now prove that this differential characteristic can never hold, i.e., the actual probability is 0. Let A, B, C, D, E and A^*, B^*, C^*, D^*, E^* be the intermediate encryption values corresponding to a pair which allegedly satisfies this differential.

Table 2. The differential Characteristic in [10] from Round 6 to Round 12

i	$\varDelta A_i$	$\varDelta B_i$	$\varDelta C_i$	$\varDelta D_i$	$\varDelta E_i$	$\varDelta K_i$	*Prob.*
6	e_3	0	0	$e_{13,31}$	0	0	2^{-3}
7	e_8	e_3	0	0	$e_{13,31}$	e_{31}	2^{-3}
8	0	e_8	e_1	0	0	0	2^{-2}
9	0	0	e_6	e_1	0	0	2^{-2}
10	0	0	0	e_6	e_1	0	2^{-2}
11	e_1	0	0	0	e_6	0	2^{-2}
12	0	e_1	0	0	0	0	2^{-1}

1. According to $A_{i+1} = K_i + ROTL_5(A_i) + F_i(B_i, C_i, D_i) + E_i + Con_i$ and proposition 1, we get that $A_{7,8} = A_{6,3}$ and $A^*_{7,8} = A^*_{6,3}$.
2. From the encryption algorithm and proposition 1, we get that $A_{11,1} = E_{10,1} = A_{6,3}$, $A^*_{11,1} = E^*_{10,1} = A^*_{6,3}$, $E_{11,6} = A_{7,8}$ and $E^*_{11,6} = A^*_{7,8}$.
3. From 1 and 2, we obtain that $A_{11,1} = E_{11,6}$ and $A^*_{11,1} = E^*_{11,6}$. By $A_{i+1} = K_i + ROTL_5(A_i) + F_i(B_i, C_i, D_i) + E_i + Con_i$ and proposition 2, we obtain that $A_{12} \neq A^*_{12}$, i.e., $\varDelta A_{12} \neq 0$, which is a contradiction with $\varDelta A_{12} = 0$ in the differential characteristic.

To summarize the above, as there is no carry from the addition of the differences in round 6, the sign of $A_{7,8}$ is the same as the sign of $A_{6,3}$. The sign of $A_{6,3}$ is then copied to $A_{11,1}$ (as there is no carry). Thus, when these two differences enter the addition in round 12 they have the same sign, and thus, cannot cancel each other. Therefore the attack on 70-round SHACAL-1 [10] is infeasible (as well as other attacks which use this transition).

We note that when considering only XOR differences (as was done in [10]), the probabilities of the differential is larger than 0. However, only when we consider modular difference, this problem is found.

3.2 Conditions on the Keys

The related-key differential attacks [7,10,13] have to deal with another issue which follows from the addition operation. Some of the XOR differences of the differentials can hold only if some key conditions are applied. We show that the related-key attacks in [7,10,13] imposes conditions on the keys, so they can actually be used only for weak key classes. The attack in [13] has one such condition, the attack in [10] has 2 conditions, and the attack in [7] has 16 conditions. Thus, the attack of [7] is applicable only for a weak key class with the size of 2^{496} keys (rather than all the keys as implicitly assumed in [7]).

Consider rounds 26–34 of the first related-key differential used in [7] which are depicted in Table 3. Consider for example the difference e_2 in A_{27}, we know the the sign of this difference is as the sign of key difference that caused it. In order for this difference to be canceled during the addition of round 27 (with the key difference of K_{27}), by proposition 2 it must hold that the sign of the key difference is opposite to that of $A_{27,2}$. This imposes a condition on the keys

Table 3. The Related-Key Differential Characteristic in [7] (Steps 26–34)

i	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔK_i	$Prob.$
26	0	0	0	0	0	e_2	2^{-1}
27	e_2	0	0	0	0	e_7	2^{-1}
28	0	e_2	0	0	0	e_2	2^{-1}
29	0	0	e_0	0	0	$e_{0,3}$	2^{-2}
30	e_3	0	0	e_0	0	$e_{0,8}$	2^{-2}
31	0	e_3	0	0	e_0	$e_{0,3}$	2^{-2}
32	0	0	e_1	0	0	$e_{1,4}$	2^{-2}
33	e_4	0	0	e_1	0	$e_{1,9}$	2^{-2}
34	0	e_4	0	0	e_1		

used in the attack, as otherwise, there is going to be a carry, and the related-key differential cannot hold. We note that the same problem exists in the first related-key differential of [7] in five other places, in rounds 0–1, 4–5, 29–30, 32–33, and rounds 26–31 (where the sign of the difference in E_{31} should be the opposite of the sign of the key difference).

The same is true for the second related-key differential used in rounds 34-69, where 10 conditions are imposed on the key. As a side observation, we note that when the keys satisfy these conditions, the probability of the transitions is increased, as we are assured that the required differences cancel. Thus, while this defines a weak key class which contains one out of 2^{16} keys (or more precisely a quartet of keys), for these weak keys, the probabilities of the differentials are actually 2^{-35} and 2^{-29} rather than 2^{-41} and 2^{-39} for the first and second differentials, respectively.

In Table 4 we summarize for the three related-key attacks the number of conditions imposed on any of the related-key differentials, derive the weak key class size, and the actual data and time complexities of the attacks in the weak key class. We ignored the impossibility issues that were mentioned earlier, but we remind the reader that these attacks still fail due to the previously mentioned reasons.

3.3 Wrong Keys That Pass the Basic Attacks

While this problem is the smallest of all, this observation can actually be used to reduce the time complexities of the attacks (usually by a negligible factor). Consider for example the last step in the attack from [7]:

> *"Partially decrypt all the remaining quartets (under the corresponding keys) . . . For each of the remaining quartets, check whether* $C'''_{a_E} \oplus C'''_{c_E} = \delta_E = e_1$ *. . . "*

Consider for example the case where the most significant bit of the real key is flipped. As noted in [7], this has no affect on the difference of the pair. Thus, when checking the real key, and the real key with a flipped most significant bit, the same quartets are suggested. More accurately, if we consider the additive

Table 4. Conditions on the Keys in Previous Related-Key Attacks and the Effect on their Complexities

Attack	Rounds	Conditions on		Complexity		Number of
		1st Differential	2nd Differential	Data	Time	Weak Keys
[13]	57	1	0	$2^{153.8}$ RK-CP	$2^{501.4}$	2^{511}
[13]	59	0	0	$2^{149.7}$ RK-CP	$2^{498.3}$	2^{512}
[10]	70	1	0	$2^{150.8}$ RK-CP	$2^{498.1}$	2^{511}
[7]	80	6	10	$2^{143.8}$ RK-CP	$2^{388.0}$	2^{496}
[7]	80	6	8	$2^{139.8}$ RK-CP	$2^{473.1}$	2^{498}

The first three attacks fail.
The number of weak keys is the number of weak keys quartets out of all the 2^{512} possible ones which satisfy the related-key XOR differences.

differences in the last step of the attack, the additive difference depends on the additive difference of the subkey and the data, and not on the actual key bits. Thus, all bit positions which are more significant than all the bits with difference in the key, has no affect whatsoever on the difference of a pair.

Thus, in the case of the attack from [7] the number of subkeys which has more than two quartets is increased by 2^{27}. One one hand this increases the time complexity of the exhaustive key search phase by a factor of 2^{27}. On the other hand, as there is no point in guessing these key bits during the normal execution of the attack (again besides in the exhaustive key search phase), their guesses and partial decryptions during the attacks can be eliminated.

We observe that the each of these keys is suggested by the *same* quartet. Thus, increasing the data used in the attack has no effect on the correctness of the attack.

4 Fixing the Previous Attacks

We concentrate at showing how to fix the the differential attack on 55-round SHACAL-1 from [17]. We show that by using the correct modular differences we obtain a valid attack on 49-round SHACAL-1. The new modular differential uses the cases where we add two difference, either they have the opposite signs (and produce no carry) or they are in the most significant bit. We also note that when a difference in the most significant bit is introduced, its sign might change without producing a carry. This might be useful in cases where a difference is introduced, and we need to change its sign (the change of sign occurs with probability 1/2, and it may happen without carry, while for other bit positions this occurs with probability 1/2, but produces a carry).

We summarize in Table 5 the parameters of the fixed attacks: the new number of rounds, the new data and time complexity. We also list the major changes that must be done to these attacks to make them work. We note that the best attack on SHACAL-1 in the regular model (i.e., with one key) is a 51-round rectangle attack on rounds 0–50.

Table 5. The results of the fixed attacks on SHACAL-1

Attack	Rounds	Complexity		Comments
		Data	Time	
Differential [14]	28 (0–27)	2^{93} CP	2^{93}	Using the new differentials from Appendix B. Fixing 6 input bits
Differential [14]	40 (0–39)	2^{98} CP	2^{482}	As before, not using the early abort technique.
Differential [17]	49 (20–68)	2^{144} CC	2^{496}	See Section 4.1
Amplified Boomerang [14]	47 (0–46)	$2^{154.5}$ CP	$2^{502.4}$	Changing the first differential to the first 21 rounds of the differential from Appendix B.
Rectangle [2]	47 (0–46)	$2^{149.7}$ CP	$2^{478.2}$	Same change as the amplified boomerang attack. $\hat{p} = 2^{-41.42}$ rather than $2^{-43.62}$, $t_b = 12.7$ (rather than 9.9) and $r_b = 32$ rather than 25.
Rectangle [2]	48 (30–77)	$2^{149.7}$ CC	$2^{482.1}$	As before, not using the early abort technique. $t_f = 12.7$ (originally 9.9), $r_f = 32$ (origanlly 32).
Rectangle [17]	51 (0–50)	$2^{150.3}$ CP	$2^{496.9}$	Using the 24-round differential from Appendix B. Fixing 6 plaintext bits, $\hat{p} = 2^{-44}$ (rather than $2^{-47.39}$).
Rectangle [17]	50 (30–79)	2^{160} CP	$2^{505.0}$	$\hat{q} = 2^{-47.9}$ (orignally $2^{-47.8}$), $t_f = 73.7$ (originally 24.9), and $r_f = 90$ (originally 31).
Related-Key Rectangle [13]	57 (0–56)	$2^{143.6}$ RK-CP	2^{481}	Change the first related-key differential to the first one from Appendix A. $p = 2^{-35}$ after fixing 9 plaintext bits.
Related-Key Rectangle [13]	59 (0–58)	$2^{146.5}$ RK-CP	$2^{479.0}$	Replace the first differential to the 21 first rounds of the differential from Appendix B. $\hat{p} = 2^{-35.4}$ after fixing 6 plaintext bits.
Related-Key Rectangle [10]	70 (0–69)	$2^{142.7}$ RK-CP	$2^{481.9}$	As before, change the first related-key differential.

CP: Chosen Plaintexts, CC: Chosen Ciphertexts, RK-CP: Relate-Key Chosen Plaintexts.
WK: Weak Key Class (with size).

4.1 Fixing the Differential Attacks

For the differential attack in [17] we change the used differential. The basic 24-round differential is given in Table 9 in the Appendix. The basic 24-round differential from [17] (which is extended 16 more rounds) has four contradictions. Thus, we first start by fixing the first three by changing the differential conditions from XOR ones to modular ones. The fourth contradiction is solved by rotating the differential such that the problematic addition occurs with both differences in the most significant bit.

The new 24-round differential has probability of 2^{-52}, compared to the claimed probability of the flawed differential of 2^{-50}. It is possible to improve the probability of the new differential by a factor of 2^6 by fixing several plaintext bits which ensure the transitions that we seek. For example, by fixing $C_{0,22} = D_{0,22}$, we make sure that despite the difference in $B_{0,22}$, there is no difference in $IF(B_{0,22}, C_{0,22}, D_{0,22})$. We also note that by negating the signs (i.e., flipping all the signs) in the differential, we obtain a second differential with the same probability.

The extension of this differential forward and backward is a bit more complex than in [17]. This is mostly due to the fact that we have to maintain the correctness of the differential by restricting the signs of the differences. In Table 10 in the appendix we present a possible extension of the 24-round differential to the six rounds before the differential (the 24-round differential can be used also for rounds 40–63). Table 11 presents a possible extension of the 24-round differential (whether this is in rounds 24–29 or in rounds 64–68). Thus, it is possible to construct a 36-round differential for SHACAL-1 in rounds 33–68 with probability 2^{-157} (which can be improved to 2^{-144} by fixing the equivalent of 13 plain text bits).

Using this 36-round differential, we can attack rounds 18–68. This is done in a chosen ciphertext attack. The attacker has to fix 10 bits to satisfy the additive requirements of the differential, and thus, it is impossible to use the differential as-is (as its probability is 2^{-157}, i.e., 2^{157} pairs are needed). However, if we use structures of 2^{32} ciphertexts each, we eliminate the last round of the differential (round 68), and thus increase the probability of the differential by a factor of 2^{-14}, and reduce 2 conditions on the ciphertexts. In exchange for that, we cannot automatically distinguish right pairs (as each plaintext has 2^{32} candidate counterparts).

The attacker obtains 2^{144} chosen ciphertexts (in 2^{112} structures), and asks for their decryption. Then, he guesses the subkeys of rounds 68, and rounds 20–29, partially encrypts the obtained plaintexts, and then repeats the early abort technique found in [17] and in our attack described later. The resulting attack has a time complexity of about 2^{496} encryptions.

5 A New Related-Key Rectangle Attack on the Full SHACAL-1

The key schedule of SHACAL-1 is operated by a linear shift feedback register, and has slow diffusion, i.e., low difference propagations. If we fix a difference of any consecutive 16 subkeys, the differences in the remaining 64 subkeys are known. The key schedule weaknesses of SHACAL-1 allows us to obtain two consecutive good related-key differential characteristics. We can constructed a 33-round related-key differential characteristic for rounds 0–32 (E_0) without any conditions on the key. For the rounds 33–65 (E_1) we use a differential characteristic based on the the second differential used in [7] and we impose 8 conditions on the key. The characteristics are given in the Appendix. We combine the two related-key differential characteristics to obtain a 66-round related-key rectangle distinguisher for SHACAL-1.

5.1 Related-Key Differential Characteristics for SHACAL-1

We first propose a 66-round related-key rectangle distinguisher based on the differentials found in the Appendix. The input difference for the first sub-cipher

Table 6. Values for Plaintexts bits that Increase the Probability of the Differential of Table 7

A_0	B_0	C_0	D_0
$A_{0,3}=1, A_{0,12}=B_{0,12}$	$B_{0,16}=1, B_{0,20}=0, B_{0,10}=C_{0,8}$	$C_{0,1}=1$	$D_{0,3}=1$
$A_{0,20}=1$	$B_{0,31}=0$		

Table 7. The First Related-Key Differential Characteristic for SHACAL-1

Round(i)	$\varDelta A_i$	$\varDelta B_i$	$\varDelta C_i$	$\varDelta D_i$	$\varDelta E_i$	$\varDelta K_i$	*Probability*
0	$[-8,1]$	$[3]$	$[-20,3]$	$[16,31]$	$2^{13}-2^{10}-2^{6}$	e_{31}	
1	$[-10]$	$[-8,1]$	$[1]$	$[-20,3]$	$[16,31]$	e_{31}	2^{-1}
2	$[15]$	$[-10]$	$[-6,31]$	$[1]$	$[-20,3]$	0	2^{-1}
3	$[3]$	$[15]$	$[-8]$	$[-6,31]$	$[1]$	0	2^{-4}
4	$[1]$	$[3]$	$[13]$	$[-8]$	$[-6,31]$	e_{31}	2^{-5}
5	0	$[1]$	$[1]$	$[13]$	$[-8]$	0	2^{-3}
6	$[-8]$	0	$[31]$	$[1]$	$[13]$	0	2^{-3}
7	0	$[-8]$	0	$[31]$	$[1]$	0	2^{-2}
8	$[1]$	0	$[-6]$	0	$[31]$	e_{31}	2^{-3}
9	0	$[1]$	0	$[-6]$	0	0	2^{-1}
10	$[1]$	0	$[31]$	0	$[-6]$	e_{31}	2^{-3}
11	0	$[1]$	0	$[31]$	0	0	2^{-1}
12	0	0	$[31]$	0	$[31]$	e_{31}	2^{-2}
13	0	0	0	$[31]$	0	0	2^{-1}
14	0	0	0	0	$[31]$	e_{31}	2^{-1}
15	0	0	0	0	0	0	1
...	...	...	...	...	...	...	...
30	0	0	0	0	0	e_0	1
31	e_0	0	0	0	0	0	2^{-1}
32	e_5	e_0	0	0	0	0	2^{-1}
33	$e_{0,10}$	e_5	e_{30}	0	0	e_1	2^{-2}

The key difference is $\varDelta K^* = (e_{31}, e_{31}, 0, 0, e_{31}, 0, 0, 0, e_{31}, 0, e_{31}, 0, e_{31}, 0, e_{31}, 0)$.

is $\alpha = ([-8,1],[3],[3,-20],[16,31],2^{13}-2^{10}-2^{6})$, and the output difference is $\beta = (e_{10,0}, e_5, e_{30}, 0, 0)$ under key difference $\varDelta K^*$ with probability 2^{-35}. For the second sub-cipher the input difference $\gamma = (e_1, e_1, 0, e_{30,31}, e_{31})$ becomes output difference $\delta = (0, e_3, 0, 0, e_0)$ under key difference $\varDelta K'$ with probability 2^{-36}. The second differential defines a weak key class which contains one out of 2^8 keys, for these weak keys, the probability of the second differential is increased to $2^{-28}(= 2^{-36} \cdot 2^8)$. The probability of the first three rounds of the first differential can be increased by a factor of 2^9 by fixing the equivalent of 9 plaintext bits (presented in Table 6) in each of the plaintexts of the pair, and after the increase the probability of the first differential is 2^{-35}. Thus, starting with N plaintext pairs with input difference α and fixed the 9 bits in each of the plaintexts to the first sub-cipher we expect $N^2 \cdot (p^2q^2 2^{-160}) = N^2 \cdot 2^{-286}$ right quartets. Therefore, Given 2^{144} related-key chosen plaintext pairs, we expect

$4(= (2^{144})^2 \cdot 2^{-160} \cdot (2^{-63})^2)$ right quartets, while for a random cipher only $2^{-32}(= (2^{144})^2 \cdot (2^{-160})^2)$ are expected.

The following is the derivation for the sufficient conditions in round 0 of Table 7. The input difference in round 0 is $\alpha = ([-8, 1], [3], [3, -20], [16, 31], 2^{13} - 2^{10} - 2^6)$, and the desired output difference in round 0 of $([-10], [-8, 1], [1], [3, -20], [16, 31])$.

1. According to (2) of Proposition 1, the condition $B_{0,20} = 0$ ensures that the change in the 20th bit in C_0 results in no change in A_1.
2. According to (3) of Proposition 1, the condition $B_{0,16} = 1$ ensures that the change in the 16th bit in D_0 results in no change in A_1.
3. According to (3) of Proposition 1, the condition $B_{0,31} = 0$ ensures that the change in the 31st bit in D_0 and $\Delta K_1 = 2^{31}$ result in no change in A_1.
4. From the property of the function F_0, the condition $D_{0,3} = 1$ ensures that the changes in the 2nd bits of B_0 and C_0 result in no change in A_1.
5. From $\Delta E_0 = 2^{13} - 2^{10} - 2^6$ and $\Delta A_0 = -2^8 + 2$, the condition $A_{1,10} = 1$ ensures that $A_1 = A_1[-10]$.

Therefore $\Delta A_1 = [-10]$ holds with the probability of 2^{-1} by fixing the equivalent to 4 bits in the plaintexts.

In the same way, we can prove that the conditions $C_{0,1} = 1$, $B_{0,10} = C_{0,8}$ and $A_{0,3} = A_{0,20} = 1$ ensure that $\Delta A_2 = [15]$ holds with the probability of 2^{-1}, and the condition $A_{0,12} = B_{0,12}$ ensures that $\Delta A_3 = [3]$ holds with the probability of 2^{-4}.

5.2 The Key Recovery Attack Procedure for the Full SHACAL-1 with 512-Bit Keys

Let the four different unknown keys be $K, K^* = K \oplus \Delta K^*, K' = K \oplus \Delta K', K'^* = K' \oplus \Delta K^*$, where ΔK^* is the key difference of the first related-key differential and $\Delta K'$ is the key difference for the second key differential. Assume the plaintexts P, P^*, P' and P'^* are encrypted under the keys K, K^*, K' and K'^* respectively. Denote the intermediate values encrypted under E_0 by IM, IM^*, IM' and IM'^*, respectively. (P, P^*) and (P', P'^*) are the pairs with respect to the first differential, and (IM, IM'), (IM^*, IM'^*) are the pairs with respect to the second differential, i.e. (C, C'), (C^*, C'^*) are the pairs with respect to the second differential.

We denote the 160-bit value X_i is by the five 32-bit words X_{iA}, X_{iB}, X_{iC}, X_{iD} and X_{iE}. Also, we denote the set of all possible additive differences of ΔA_{67} by S'. The attack finds the four related-keys using 2^{146} related-key chosen plaintexts using the following algorithm:

1. Choose two pools of 2^{144} plaintext pairs (P_i, P_i^*) and (P'_j, P'^*_j) such that
   (a) $P_i^* - P_i = P'^*_j - P'_j = \alpha$;
   (b) P_i and P_j^* have the fixed bits as given in Table 6 and required by the modular differential, i.e., for P_i: $P_{iA,3} = P_{iA,8} = P_{iA,20} = P_{iB,16} = P_{iC,1} = P_{iC,20} = P_{iD,3} = 1$, $P_{iA,1} = P_{iB,3} = P_{iB,20} = P_{iB,31} = P_{iC,3} = P_{iD,16} = 0$, and $P_{iA,12} = P_{iB,12}$, $P_{iB,10} = P_{iC,8}$.

Table 8. The Second Related-Key Differential Characteristic for SHACAL-1

Round(i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	ΔK_i	*Probability*
33	e_1	e_1	0	$e_{30,31}$	e_{31}	$e_{1,6,30}$	
34	0	e_1	e_{31}	0	$e_{30,31}$	$e_{1,30}$	2^{-3}
35	0	0	e_{31}	e_{31}	0	$[a1]$	2^{-2}
36	e_1	0	0	e_{31}	e_{31}	$[-a6]$	2^{-1}
37	0	e_1	0	0	e_{31}	$e_{1,31}$	2^{-1}
38	0	0	e_{31}	0	0	e_{31}	2^{-1}
39	0	0	0	e_{31}	0	$[s1]e_{31}$	1
40	e_1	0	0	0	e_{31}	$[-s6]e_{31}$	2^{-1}
41	0	e_1	0	0	0	0	2^{-1}
42	e_1	0	e_{31}	0	0	$[-s6]e_{31}$	2^{-2}
43	0	e_1	0	e_{31}	0	e_{31}	2^{-2}
44	e_1	0	e_{31}	0	e_{31}	$[-s6]$	2^{-3}
45	0	e_1	0	e_{31}	0	e_{31}	2^{-2}
46	e_1	0	e_{31}	0	e_{31}	$[-s6]$	2^{-3}
47	0	e_1	0	e_{31}	0	$[-s1]e_{31}$	2^{-2}
48	0	0	e_{31}	0	e_{31}	0	2^{-3}
49	0	0	0	e_{31}	0	e_{31}	2^{-1}
50	0	0	0	0	e_{31}	e_{31}	2^{-1}
51	0	0	0	0	0	0	1
...	...	...	...	...	...	...	...
60	0	0	0	0	0	0	1
61	0	0	0	0	0	$[t2]$	1
62	e_2	0	0	0	0	$[-t7]$	2^{-1}
63	0	e_2	0	0	0	e_2	2^{-1}
64	0	0	e_0	0	0	$[b3]e_0$	2^{-1}
65	e_3	0	0	e_0	0	$[-b8]e_0$	2^{-2}
66	0	e_3	0	0	e_0	$e_{0,3}$	2^{-2}

The key difference is $\Delta K' = (e_{1,6,28,29,31},\ e_{0,4,6,28,30,31},\ e_{5,28,30},\ e_{29,0},\ e_{1,4,5,29,30},\ e_{1,6,29,30,31},\ e_{1,6,29},\ e_{6,29,30,31},\ e_{29,30},\ e_{0,31},\ e_5,\ e_1,\ e_{1,4,6,30},\ e_{1,6,30,31},\ e_{4,6,29,30,31},\ e_{1,29})$. [?i] denotes [i] or [-i]. When [?i] denotes [i], then [-?i] denotes [-i], and vice versa.

(c) P_i, P_i^*, P'_j and P'^*_j are encrypted using the keys K, K^*, K' and K'^*, respectively, which result in the ciphertexts C_i, C_i^*, C'_j, and C'^*_j.

2. Guess a 323-bit key quartet (k, k^*, k', k'^*) for rounds 70–79 and $K_{69,1}$, $K_{69,3}$, $K_{69,4}$. For the guessed key quartet (k, k^*, k', k'^*), and decrypt all the ciphertexts C_i, C_i^*, C'_j, C'^*_j from round 79 to round 70 and compute the additive difference before round 69. Denote the corresponding intermediate values by U_i, U_i^*, U'_j, U'^*_j, respectively. Then we obtain words A, B, C, D of all words and the additive difference for all the pairs U_{iE}, U^*_{iE} and all the pairs U'_{iE}, U'^*_{iE}. Find all quartets $(U_i, U_i^*, U'_j, U'^*_j)$ satisfying $U_{iC,D,E} \oplus U'_{jC,D,E} \in S$ and $U^*_{iC,D,E} \oplus U'^*_{jC,D,E} \in S$, where $S = \{(a, b, c) : ROTR_{30}(a) \in S', b = ROTL_{30}(\Delta A_{66}) = 0, c = ROTL_{30}(\Delta B_{66}) = e_1\}$. Discard all other quartets.
3. Guess the remainder bits of K_{69} and bits 1,9 of K_{68}. For each of the guessed subkeys:

   (a) Decrypt the remaining quartets to get U_{iE}, U'_{jE}, U^*_{iE} and U'^*_{jE}. Partially decrypt all the remaining quartets $(U_i, U^*_i, U'_j, U'^*_j)$ using the keys k, k^*, k' and k'^* respectively, and denote the resulting intermediate values by $(Z_i, Z^*_i, Z'_j,$
$Z'^*_j)$. We will get A, B, C, D of Z_i (Z^*_i, Z'_j, Z'^*_j), and the additive difference between Z_{iE} and Z'_{jE} (and the additive difference between Z^*_{iE} and Z'^*_{jE}). Check whether $Z_{iE} \oplus Z'_{jE} = \varDelta C_{66} = 0$ and discard all the quartets that do not satisfy the condition.
   (b) For each of the remaining quartets, check whether $Z^*_{iE} \oplus Z'^*_{jE} = \varDelta C_{66} = 0$ and discard all the quartets that do not satisfy the condition.
4. Guess the remainder bits of K_{68} and bits 1,4 of K_{67}. For each of the guessed subkeys:
   (a) Decrypt the quartets to get Z_{iE}, Z'_{jE}, Z^*_{iE} and Z'^*_{jE}. Partially decrypt all the remaining quartets $(Z_i, Z^*_i, Z'_j, Z'^*_j)$ using the keys k, k^*, k' and k'^* respectively, and denote the resulting intermediate values by $(Y_i, Y^*_i, Y'_j,$ $Y'^*_j)$. We will get A, B, C, D of Y_i (Y^*_i, Y'_j, Y'^*_j), and the additive difference between Y_{iE} and Y'_{jE} (and the additive difference between Y^*_{iE} and Y'^*_{jE}). Check whether $Y_{iE} \oplus Y'_{jE} = \varDelta D_{66} = 0$ and discard all the quartets that do not satisfy the condition.
   (b) For each of the remaining quartets, check whether $Y^*_{iE} \oplus Y'^*_{jE} = \varDelta D_{66} = 0$ and discard all the quartets that do not satisfy the condition.
5. Guess the remainder bits of K_{67} and bits 0,3 of K_{66}. For each of the guessed subkeys:
   (a) Decrypt the quartets to get Y_{iE}, Y'_{jE}, Y^*_{iE} and Y'^*_{jE}. Partially decrypt all the remaining quartets $(Y_i, Y^*_i, Y'_j, Y'^*_j)$ using the keys k, k^*, k' and k'^* respectively, and denote the resulting intermediate values by $(X_i, X^*_i,$ $X'_j, X'^*_j)$. We will get A, B, C, D of X_i (X^*_i, X'_j, X'^*_j), and the additive difference between X_{iE} and X'_{jE} (and the additive difference between X^*_{iE} and X'^*_{jE}). Check whether $X_{iE} \oplus X'_{jE} = \varDelta E_{66} = e_0$ and discard all the quartets that do not satisfy the condition.
   (b) For each of the remaining quartets, check whether $X^*_{iE} \oplus X'^*_{jE} = \varDelta E_{66} = e_0$ and discard all the quartets that do not satisfy the condition.
6. Exhaustively search for the remaining 94 key bits by trial encryption for the suggested key k.

The first 9 fixed bits as given in Step 1(b) of P_i ensure that the probability of the first differential is increased by a factor of 2^9. According to the input difference of the plaintexts, we will know that P^*_i, P'_j and P'^*_j also have the 9 fixed bits as given in Table 6, i.e. $P^*_{iA,3} = 1$, $P'_{iA,3} = 1$, $P'^*_{iA,3} = 1$, $P^*_{iA,12} = P^*_{iB,12}$, $P'_{iA,12} = P'_{iB,12}$, $P'^*_{iA,12} = P'^*_{iB,12}$, etc. Besides these bits, the nature of the modular differential, i.e., the signs, set 6 more bits to predetermined values. These 6 bits in Step 1(b) are deduced as follows: for each bit whose difference according to the differential from Table 7 is positive, we set P_i to be zero and P^*_i to be one (and of course P'_j to zero and P'^*_j to one as well). If the difference is negative, we perform the same but with opposite values.

This means our related-key differential characteristic exploits plaintexts pairs for which 15 bits are effectively fixed respectively. P_i, P^*_i, P'_i and P'^*_i has 15

Table 9. The Fixed 24-Round Differential Characteristic for SHACAL-1 for the Attack in [17]

Round (i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Probability
0	$[-0]$	$[22]$	$[-16]$	0	$[6]$	
1	$[5]$	$[-0]$	$[20]$	$[-16]$	0	2^{-3}
2	$[10]$	$[5]$	$[-30]$	$[20]$	$[-16]$	2^{-4}
3	$[-15]$	$[10]$	$[3]$	$[-30]$	$[20]$	2^{-4}
4	0	$[-15]$	$[8]$	$[3]$	$[-30]$	2^{-3}
5	$[-30]$	0	$[-13]$	$[8]$	$[3]$	2^{-4}
6	0	$[-30]$	0	$[-13]$	$[8]$	2^{-2}
7	$[8]$	0	$[-28]$	0	$[-13]$	2^{-3}
8	0	$[8]$	0	$[-28]$	0	2^{-1}
9	0	0	$[6]$	0	$[-28]$	2^{-2}
10	$[-28]$	0	0	$[6]$	0	2^{-2}
11	$[-1]$	$[-28]$	0	0	$[6]$	2^{-2}
12	0	$[-1]$	$[-26]$	0	0	2^{-1}
13	0	0	$[-31]$	$[-26]$	0	2^{-2}
14	0	0	0	$[-31]$	$[-26]$	2^{-2}
15	$[-26]$	0	0	0	$[-31]$	2^{-2}
16	0	$[-26]$	0	0	0	1
17	0	0	$[-24]$	0	0	2^{-1}
18	0	0	0	$[-24]$	0	2^{-1}
19	0	0	0	0	$[-24]$	2^{-1}
20	$[-24]$	0	0	0	0	2^{-1}
21	$[-29]$	$[-24]$	0	0	0	2^{-1}
22	$[-2, \pm 24]$	$[-29]$	$[-22]$	0	0	2^{-2}
23	$[-7, \pm 22]$	$[-2, \pm 24]$	$[-27]$	$[-22]$	0	2^{-3}
24	$[\pm\{2, 22, 24\}, -12]$	$[-7, \pm 22]$	$[-0, \pm 22]$	$[-27]$	$[-22]$	2^{-5}

fixed bits respectively, and we choose 2^{144} pairs (P_i, P_i^*) and (P'_j, P'^*_j), which can be realized while each plaintext has 160 bits.

According to the key schedule of SHACAL-1, we know that for the pairs we consider, $\Delta K_{67} = e_{1,4}$, $\Delta K_{68} = e_{1,9}$ and $\Delta K_{69} = e_{1,3,4}$. A pair which satisfies the differential has difference in bit $B_{66,3}$, i.e., the difference in B_{66} is either $[3]$ or $[-3]$ (or more precisely, after the XOR of the three words the difference is either $[3]$ or $[-3]$), in bit $E_{66,0}$ (difference $[0]$ or $[-0]$) and in bits $0, 3$ of the subkey, i.e., it is either $[0, 3]$,$[0, -3]$,$[-0, 3]$, or $[-0, -3]$. Thus, there are only 9 possible additive differences in A_{67}: 0, $[1]$, $[-1]$, $[1, 4]$, $[-1, -4]$, $[4]$, $[-4]$, $[-1, 4]$ and $[1, -4]$. As noted earlier, that means that there is no point in guessing bits 4–31 of the subkey of round 66. Similarly, that means that in order to verify that a pair might satisfy the differential, given A_{70}, B_{70}, C_{70}, D_{70}, E_{70}, in order to achieve $\Delta E_{69} = e_1$, we can consider the modular difference of the key, and disregard the bits in positions 5–31. Thus, we only guess bits 1,3,4 of the subkey in round 69, i.e. actually only guess its key modular difference since we know whether the XOR difference between K_{69} and K'_{69} satisfy the differential.

The data complexity of this attack is 2^{146} related-key chosen plaintexts. The memory requirements are about $2^{150.33} (= 2^{146} \times 20)$ memory bytes.

In Step 1, the time complexity is 2^{146} SHACAL-1 encryptions. The time complexity of Step 2 is about $2^{465} = (2^{323} \times 2^{146} \times \frac{1}{2} \times \frac{11}{80})$ encryptions on average. The factor $\frac{1}{2}$ means the average fraction of 323-bit subkey which are used in Step 2. We guess 3 bits of K_{69} and there are 2^{32} the modular difference between E_{69} and $E_{69}\prime$, so the probability of $\Delta E_{69} = e_1$ is $2^{-29} = \frac{2^3}{2^{32}}$. Also we know that there are about 9 possible ΔA_{67} values in S' and the attack starts with 2^{288} quartets, therefore we expect that $2^{288} \times (2^{-32} \times 2^{-29} \times \frac{9}{2^{32}})^2 = 2^{108}$ quartets pass Step 2.

For a given subkey guess, Step 3 consists of $2^{108} \times 2^{29} \times 2^2 = 2^{139}$ partial decryptions of one SHACAL-1 round. Therefore, the time complexity of Step 3 is about $2^{323} \times 2^{139} \times 4 \times \frac{1}{2} \times \frac{1}{80} = 2^{457}$. The time complexity of the other steps are relatively smaller. Hence, the time complexity of this attack is about 2^{465} SHACAL-1 encryptions.

A different method can be adopted in the attack. The last round of the second differential can be removed, then we will get a 66-round related-key rectangle distinguisher with probability 2^{-61}. Using the similar analysis approach, we can present a related-key rectangle attack on SHACAL-1 with data complexity of 2^{144} chosen plaintexts and time complexity of $2^{494} = (2^{354} \times 2^{144} \times \frac{1}{2} \times \frac{11}{80})$ SHACAL-1 encryptions.

6 Improving the Attack on IDEA

A careful investigation of the way XOR differences behave through addition can also be used to improve results of previous attacks. Consider for example the related-key rectangle attack on 6.5-round IDEA from [4]. The attack uses two related-key differentials, where the first related-key differential starts with an input difference $(0, 0, 0001_x, 0)$, while the key difference is in bit 40, and with probability 1/2 the key difference cancels the input difference. While in [4], the probability of this first part of the differential was assumed to be half, it is actually 1 for plaintext pairs with the opposite sign of the key difference, and 0 for plaintext pairs with the same sign.

The above observation lead to an obvious improvement. The attacker first considers only pairs with the same sign in the differing bit, and applies the attack. If the attack fails, the attacker repeats the attack with the opposite sign.

We note that this approach indeed increases the value of $\hat{p}$ by a factor of two. Thus, for the right guess of the sign, the data complexity can be reduced by a factor of two (recall that the number of pairs is proportional to $1/\hat{p}\hat{q}$). However, the actual sign of the key difference is unknown, thus the attack has to be repeated twice — once for each guess (each time with half the data).

However, we gain a factor of two in the time complexity, as in each application we have only a quarter of the number of quartets that we expected in the original attack. As the attack is repeated twice, then the total number of analyzed quartets is reduced by a factor of two.

We note that for a differential attack a similar scenario holds (no reduction in the data complexity, but a possible reduction in the time complexity). However, for boomerang attacks, as the data complexity is proportional to $1/\hat{p}^2\hat{q}^2$, then we expect a reduction in the data complexity besides the probable reduction in time complexity.

7 Conclusion

In this paper we identified the misuse of XOR differences through addition. The observation led us to examine all the differential-based attacks on SHACAL-1, showing that these attacks fail. After pointing out the problems and by using modular differences, we fix some of the attacks, and present the best known (valid) attack on SHACAL-1 in the one key model (a rectangle attack on the first 51 rounds).

We continue to present a new related-key rectangle attack on the full SHACAL-1, which is applicable to one out of 256 keys (rather than out of 2^{14} for the previously best result). The new attack uses 2^{146} chosen plaintexts (or 2^{144} chosen plaintexts) and has a time complexity of 2^{465} SHACAL-1 encryptions (or 2^{494} SHACAL-1 encryptions, respectively).

We verified all the differentials that we used in the paper. Each differential was tested under 100 keys (or 100 key pairs), where each time we verified several rounds of the differential. The sets of rounds were chosen to be overlapping to reduce the chance that some condition from one round affects the differential's behavior in a later round.

We conclude that differential attacks should be very carefully applied when XOR differences are used in addition. We note that the related-key rectangle attack based on the modular differences can be applied to analyze other block ciphers, thus increasing the toolbox of the cryptanalyst.

References

1. Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 398–409. Springer, Heidelberg (1994)
2. Biham, E., Dunkelman, O., Keller, N.: Rectangle Attacks on 49-Round SHACAL-1. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 22–35. Springer, Heidelberg (2003)
3. Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
4. Biham, E., Dunkelman, O., Keller, N.: New Cryptanalytic Results on IDEA. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 412–427. Springer, Heidelberg (2006)
5. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
6. Blunden, M., Escott, A.: Related Key Attacks on Reduced Round KASUMI. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 277–285. Springer, Heidelberg (2002)

7. Dunkelman, O., Keller, N., Kim, J.: Related-Key Rectangle Attack on the Full SHACAL-1. In: Proceedings of SAC 2006. LNCS, Springer, Heidelberg (to appear)
8. Handschuh, H., Naccache, D.: SHACAL. In: Preproceedings of NESSIE first workshop, Leuven (2000)
9. Handschuh, H., Naccache, D.: SHACAL: A Family of Block Ciphers, the NESSIE project (submission, 2002)
10. Hong, S., Kim, J., Kim, G., Lee, S., Preneel, B.: Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 368–383. Springer, Heidelberg (2005)
11. Kelsey, J., Schneier, B., Wagner, D.: Key-Schedule Cryptoanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 237–251. Springer, Heidelberg (1996)
12. Kelsey, J., Schneier, B., Wagner, D.: Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. In: Han, Y., Quing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 233–246. Springer, Heidelberg (1997)
13. Kim, J., Kim, G., Hong, S., Lee, S., Hong, D.: The Related-Key Rectangle Attack — Application to SHACAL-1. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) ACISP 2004. LNCS, vol. 3108, pp. 123–136. Springer, Heidelberg (2004)
14. Kim, J., Moon, D., Lee, W., Hong, S., Lee, S., Jung, S.: Amplified Boomerang Attack against Reduced-Round SHACAL. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 243–253. Springer, Heidelberg (2002)
15. Ko, Y., Hong, S., Lee, W., Lee, S., Kang, J.S.: Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 299–316. Springer, Heidelberg (2004)
16. Lai, X., Massey, J.L., Murphy, S.: Markov Ciphers and Differential Cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (1991)
17. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Differential and Rectangle Attacks on Reduced-Round SHACAL-1. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 17–31. Springer, Heidelberg (2006)
18. Rivest, R.: The MD4 Message-Digest Algorithm. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 303–311. Springer, Heidelberg (1991)
19. Rivest, R.: The MD5 Message-Digest Algorithm, Network Working Group Request for Comments 1321 (April 1992)
20. US National Bureau of Standards, Secure Hash Standard, Federal Information Processing Standards Publications No. 180-2 (2002)
21. Wang, X.Y., Lai, X.J., Feng, D., Chen, H., Yu, X.: Cryptanalysis of the Hash Functions MD4 and RIPEMD. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 1–18. Springer, Heidelberg (2005)
22. Wang, X.Y., Lisa, Y., Yu, H.B.: Finding collisions on the Full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36. Springer, Heidelberg (2005)
23. Wang, X.Y., Yu, H.B.: How to Break MD5 and Other Hash Functions. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)
24. Wang, X.Y., Yu, H.B., Lisa, Y.: Efficient Collision Search Attacks on SHA-0. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 1–16. Springer, Heidelberg (2005)
25. Wang, X.Y.: The Collision attack on SHA-0 (in Chinese) (to appear) (1997), www.infosec.sdu.edu.cn

A The New Related-Key Differentials of SHACAL-1

B A New Differentials of SHACAL-1

Table 10. Extension of the Fixed Differential for Rounds 33–40

Round (i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Probability
33	$[\pm\{8, 10, 24\}]$	$[\pm\{2, 4, 8, 20, 22, 25, 29, 31\}, -15]$	$[\pm\{0, 18, 22, 27\}, 2, 7]$	$[\pm\{6, 10, 13, 22\}, -29, -30]$	$[\pm\{0, 4, 6, 10, 18, 22, 27\}, -2, 24]$	
34	$[-2, \pm 20, 24, 25, \pm 29]$	$[\pm\{8, 10, 24\}]$	$Mask_1$	$[\pm\{0, 18, 22, 27\}, 2, 7]$	$[\pm\{6, 10, 13, 22\}, -29, -30]$	2^{-18}
35	$[-2, \pm 8, \pm 20, -29]$	$[-2, \pm 20, 24, 25, \pm 29]$	$[\pm\{6, 8, 22\}]$	$Mask_1$	$[\pm\{0, 18, 22, 27\}, 2, 7]$	2^{-14}
36	$[8]$	$[-2, \pm 8, \pm 20, -29]$	$[-0, \pm 18, 22, 23, \pm 27]$	$[\pm\{6, 8, 22\}]$	$Mask_1$	2^{-9}
37	0	$[8]$	$[-0, \pm 6, \pm 18, -27]$	$[-0, \pm 18, 22, 23, \pm 27]$	$[\pm\{6, 8, 22\}]$	2^{-8}
38	$[-18]$	0	$[6]$	$[-0, \pm 6, \pm 18, -27]$	$[-0, \pm 18, 22, 23, \pm 27]$	2^{-4}
39	$[22]$	$[-18]$	0	$[6]$	$[-0, \pm 6, \pm 18, -27]$	2^{-4}
40	$[-0]$	$[22]$	$[-16]$	0	$[6]$	2^{-3}

$[\pm\{j_1, j_2, \ldots, j_l\}]$ stands for $[\pm j_1, \pm j_2, \ldots, \pm j_l]$ and $Mask_1 = [\pm\{0, 2, 6, 18, 20, 23, 27, 29\}, -13]$

Table 11. Extension of the Fixed Differential for Rounds 64–69

Round (i)	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Probability
64	$[\pm\{2, 22, 24\}, -12]$	$[-7, \pm 22]$	$[-0, \pm 22]$	$[-27]$	$[-22]$	
65	$[\pm 0, -17, -22, \pm 29]$	$[\pm\{2, 22, 24\}, -12]$	$[-5, \pm 20]$	$[-0, \pm 22]$	$[-27]$	2^{-6}
66	$[\pm\{12, 20, 24\}, -22, -28]$	$[\pm 0, -17, -22, \pm 29]$	$[\pm\{0, 20, 22\}, -10]$	$[-5, \pm 20]$	$[-0, \pm 22]$	2^{-7}
67	$[0, -2, \pm\{5, 10, 25\}, -27]$	$[\pm\{12, 20, 24\}, -22, -28]$	$[\pm 0, -17, -22, \pm 29]$	$[\pm\{0, 20, 22\}, -10]$	$[-5, \pm 20]$	2^{-7}
68	$[-0, -7, \pm\{12, 17, 20, 22, 24, 28\}]$	$[0, -2, \pm\{5, 10, 25\}, -27]$	$[\pm\{10, 18, 22\}, -20, -26]$	$[\pm 0, -17, -22, \pm 29]$	$[\pm\{0, 20, 22\}, -10]$	2^{-11}
69	$[\pm 0, -10, -12]$	$[-0, -7, \pm\{12, 17, 20, 22, 24, 28\}$	$[-0, \pm\{3, 8, 23\}, -25, 30]$	$[\pm\{10, 18, 22\}, -20, -26]$	$[\pm 0, -17, -22, \pm 29]$	2^{-14}

$[\pm\{j_1, j_2, \ldots, j_l\}]$ stands for $[\pm j_1, \pm j_2, \ldots, \pm j_l]$