Int. J. Inf. Secur. (2009) 8:1–11
DOI 10.1007/s10207-008-0059-9

REGULAR CONTRIBUTION

Related-key rectangle attack on 36 rounds of the XTEA block cipher

Jiqiang Lu

Published online: 2 July 2008
© Springer-Verlag 2008

Abstract XTEA is a 64-round block cipher with a 64-bit block size and a 128-bit user key, which was designed as a short C program that would run safely on most computers. In this paper, we present a related-key rectangle attack on a series of inner 36 rounds of XTEA without making a weak key assumption, and a related-key rectangle attack on the first 36 rounds of XTEA under certain weak key assumptions. These are better than any previously published cryptanalytic results on XTEA in terms of the numbers of attacked rounds.

Keywords Block cipher · XTEA · Related-key rectangle attack

1 Introduction

The block cipher TEA (Tiny Encryption Algorithm) was designed by Wheeler and Needham [22] as a short C language program that would run safely on most machines. It has no preset tables or long set up times, and achieves a high performance by performing simple operations on 32-bit words. TEA has a simple Feistel structure, but it uses a large number (i.e. 64) rounds of iterations to make itself secure. Though written in C, TEA can readily be implemented in a range of languages, including assembler. However, due to its simple key schedule, Kelsey et al. [9] described a related-key attack on it in 1997. To secure TEA against related-key attacks, Needham and Wheeler [20] presented an extended TEA, known as XTEA, which retains the original objectives of simplicity and efficiency. XTEA accepts a 64-bit block size and a 128-bit user key, and has a total of 64 rounds as well. As one of the fastest and most efficient block ciphers in existence, XTEA is used for some real-life cryptographic applications.

The published cryptanalytic results on XTEA are as follows. In 2002, Moon et al. [19] presented an impossible differential [2,14] attack on 14 rounds of XTEA. In 2003, Hong et al. [6] presented a differential [5] attack on 15 rounds of XTEA and a truncated differential [13] attack on 23 rounds of XTEA, where the former attack is due to a 13-round differential with probability $2^{-54.795}$ and the latter attack is due to a 8-round truncated differential. In 2004, Ko et al. [15] presented related-key truncated differential attacks on the first 25 rounds and a series of inner 27 rounds of XTEA, building on the 8-round truncated differential due to Hong et al. This is the best currently published cryptanalytic result on XTEA without making a weak key assumption, prior to the work described in our paper. In 2006, Lee et al. [16] presented a related-key rectangle attack on 34 rounds of XTEA under a class of weak keys.

In this paper, we further analyse the security of XTEA against related-key rectangle attacks. We first present a related-key rectangle attack on the inner 36 rounds from Rounds 16–51 of XTEA without making a weak key assumption, which is based on the following several observations: we build a 24-round related-key rectangle distinguisher with probability $2^{-124.92}$ for Rounds 21–44, after exploiting some short related-key differentials with high probabilities; we use the early abort technique [18] to break three more rounds—Rounds 45–47, where we just guess part of the 32 bits of an unknown round subkey to conduct an early abort; and there are only 64 user key bits in the remaining nine rounds. Finally, we present a related-key rectangle attack on the first

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

J. Lu (✉)
Information Security Group, Royal Holloway,
University of London, Egham, Surrey TW20 OEX, UK
e-mail: lvjiqiang@hotmail.com

Table 1 Summary of previous and our new cryptanalytic results on XTEA

Attack type	Rounds	Data	Time	Paper
Impossible differential	14	$2^{62.5}$ CP	2^{85}	[19]
Differential	15	2^{59} CP	2^{120}	[6]
Truncated differential	23	$2^{20.55}$ CP	$2^{120.65}$	[6]
Related-key truncated	25	116 RK-CP	$2^{110.05}$	[15]
differential	27	$2^{20.5}$ RK-CP	$2^{115.15}$	[15]
Related-key rectangle	36	$2^{64.98}$ RK-CP	$2^{126.44}$	This
	34[a]	2^{62} RK-CP	$2^{31.94}$	[16]
	36[a]	$2^{63.83}$ RK-CP	$2^{104.33}$	This

CP Chosen Plaintexts, *RK* Related-Key, Time unit: Encryptions, [a]Under weak key assumptions

36 rounds of XTEA under certain weak key assumptions, following the work described in [16]. Table 1 summarises previous and our new cryptanalytic results on XTEA.

The related-key rectangle attack [4,7,11] is a combination of the related-key attack [1,12] and the rectangle attack [3]. The related-key attack requires an assumption that the attacker knows the specific differences between one or more pairs of unknown keys; this assumption may make it difficult or even infeasible to conduct in many cryptographic applications, but some of the current real-world applications may allow for practical related-key attacks [8], for example, key-exchange protocols. As a variant of the boomerang attack [21] and an improvement of the amplified boomerang attack [10], rectangle attack shares the same basic idea of using two (or more) short differentials with larger probabilities instead of a long differential with a smaller probability.

The remainder of this paper is organised as follows. In the next section, we briefly describe some notation, the XTEA cipher and related-key rectangle attacks. In Sects. 3 and 4, we present our cryptanalytic results. Section 5 concludes this paper.

2 Preliminaries

2.1 Notation

In the following descriptions, a number without a prefix is in decimal (base 10) notation, a number with prefix $0x$ is in hexadecimal (base 16) notation, bits of a 32-bit value is numbered from 0 to 31 in an order of from left to right, with the least significant bit being referred as the 0-th bit, and the most significant bit being referred as the 31-th bit. We use the following notation.

- $\oplus$: bitwise logical exclusive OR (XOR)
- & : bitwise logical AND
- $\boxplus$: addition modulo 2^{32}
- $\boxtimes$: multiplication modulo 2^{32}
- $<<$ ($>>$) : left (right) shift
- $||$: string concatenation
- $\lfloor x \rfloor$: the largest integer that is less than or equal to x
- e_j : a 32-bit value 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 value that has zeros in bits 0 to $j-1$, a one in bit j and indeterminate values in bits $(j+1)$ to 31, $(0 \le j \le 30)$
- $\star$: an arbitrary 32-bit value, where two values represented by the $\star$ symbol may be different
- η_j^l : a l-bit value with zeros in all positions but bit j, where the value l will be specified in the text, $(0 \le j \le l-1)$
- $\eta_{j,\sim}^l$: a l-bit value that has zeros in bits 0 to $j-1$, a one in bit j and indeterminate values in the remaining bits, where the value l will be specified in the text, $(0 \le j \le l-1)$

The notion of difference used in this paper is with respect to the $\oplus$ operation.

2.2 The XTEA block cipher

XTEA takes as input a 64-bit plaintext, and has a total of 64 rounds. Its encryption procedure is as follows.

1. Represent a 64-bit plaintext P as two 32-bit words (L_1, R_1).
2. For $i = 1$ to 64:

$$R_{i+1} = L_i \boxplus (((R_i << 4 \oplus R_i >> 5) \boxplus R_i) \oplus \left(\lfloor \frac{i}{2} \rfloor \boxtimes \theta \boxplus W_i\right)),$$
$$L_{i+1} = R_i;$$

3. The 64-bit ciphertext C is (L_{65}, R_{65}).

In the above description, $\theta = 0x9e3779b9$, and W_i is the 32-bit subkey in the ith round. Figure 1 shows one round of XTEA.

XTEA uses a simple key schedule, which only accepts a 128-bit user key K. Represent K as four 32-bit words

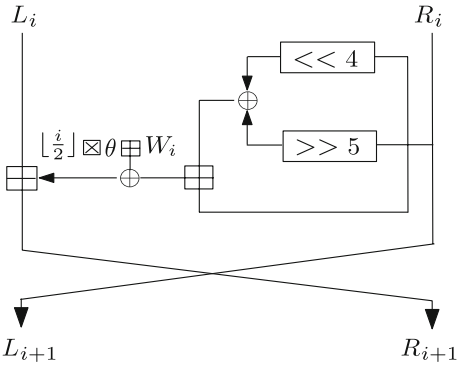

Fig. 1 The ith round of XTEA

(K_0, K_1, K_2, K_3), then the ith round subkey W_i is generated as $W_i = K_{(\lfloor \frac{i}{2} \rfloor \boxtimes \theta >> 11)\&3}$. See Table 2 for details.

2.3 Description of related-key rectangle attacks

A related-key rectangle attack [4,7,11] is based on a related-key rectangle distinguisher, which treats a block cipher $E : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ as a cascade of two sub-ciphers $E = E^1 \circ E^0$.

A right quartet consists of two pairs of plaintexts $(P, P^* = P \oplus \alpha)$ and $(P', P'^* = P' \oplus \alpha)$ satisfying the following three conditions.

$$C1 : E^0_{K_A}(P) \oplus E^0_{K_B}(P^*) = E^0_{K_C}(P') \oplus E^0_{K_D}(P'^*) = \beta,$$
$$C2 : E^0_{K_A}(P) \oplus E^0_{K_C}(P') = E^0_{K_B}(P^*) \oplus E^0_{K_D}(P'^*) = \gamma,$$
$$C3 : E^1_{K_A}(E^0_{K_A}(P)) \oplus E^1_{K_C}(E^0_{K_C}(P')) = E^1_{K_B}(E^0_{K_B}(P^*)) \oplus E^1_{K_D}(E^0_{K_D}(P'^*)) = \delta,$$

where K_A, K_B, K_C and K_D are unknown related user keys, and they 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. See Fig. 2.

If we assume that the intermediate values after E^0 distribute uniformly over all possible values, then we can get $E^0_{K_A}(P) \oplus E^0_{K_C}(P') = \gamma$ with probability 2^{-n}. Once this occurs, by C1 we know that $E^0_{K_B}(P^*) \oplus E^0_{K_D}(P'^*) = \gamma$ holds with probability 1, for $E^0_{K_B}(P^*) \oplus E^0_{K_D}(P'^*) = (E^0_{K_A}(P) \oplus E^0_{K_B}(P^*)) \oplus (E^0_{K_C}(P') \oplus E^0_{K_D}(P'^*)) \oplus (E^0_{K_A}(P) \oplus E^0_{K_C}(P')) = \beta \oplus \beta \oplus \gamma = \gamma$. As a result, 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 $\widehat{q} = (\sum_{\gamma'} \Pr^2(\Delta\gamma' \to \Delta\delta))^{\frac{1}{2}}$; while for a random cipher, this probability is about $2^{-n\times 2} = 2^{-2n}$.

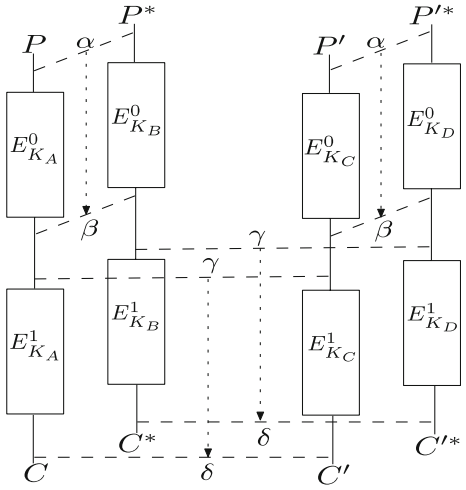

Fig. 2 A related-key rectangle distinguisher

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

3 Attacking 36-round XTEA without making a weak key assumption

In this section, we exploit a 24-round related-key rectangle distinguisher of XTEA without making a weak key assumption, and finally mount a related-key rectangle attack on 36 rounds of XTEA by using several observations.

3.1 A 24-round related-key rectangle distinguisher

The XTEA round function has a slow avalanche effect; for example, we can learn that the most significant bit of the left

Table 2 The key schedule of XTEA

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
W_i	K_0	K_3	K_1	K_2	K_2	K_1	K_3	K_0	K_0	K_0	K_1	K_3	K_2	K_2	K_3	K_1
i	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
W_i	K_0	K_0	K_1	K_0	K_2	K_3	K_3	K_2	K_0	K_1	K_1	K_1	K_2	K_0	K_3	K_3
i	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
W_i	K_0	K_2	K_1	K_1	K_2	K_1	K_3	K_0	K_0	K_3	K_1	K_2	K_2	K_1	K_3	K_1
i	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
W_i	K_0	K_0	K_1	K_3	K_2	K_2	K_3	K_2	K_0	K_1	K_1	K_0	K_2	K_3	K_3	K_2

half of an input will definitely not affect the least significant bit of the left half of the output after eight rounds. Considering this, to be conservative we will keep as many rounds as possible for the first related-key differential of the 24-round distinguisher.

Let $E = E^1 \circ E^0$ denote the 24 rounds from Rounds 21–44 of XTEA, where E^0 denotes Rounds 21–36, and E^1 denotes Rounds 37–44. The first related-key differential for the 24-round distinguisher is the following 16-round related-key differential $\Delta\alpha \to \Delta\beta$ with probability $2^{-32.49}$ for E^0: $(e_{21,26,30}, e_{26}) \to (e_{11,16,20}, e_{6,24,26})$, where the user key difference is $K_A \oplus K_B = K_C \oplus K_D = (0, 0, 0, e_{31})$. The second related-key differential for the 24-round distinguisher is the following 8-round related-key differential $\Delta\gamma \to \Delta\delta$ with probability 1 for E^1: $(e_{31}, 0) \to (0, e_{31})$, where the user key difference is $K_A \oplus K_C = K_B \oplus K_D = (0, 0, e_{31}, 0)$. See Table 3 for more details of the two related-key differentials.

During the calculations of the probabilities, we use the following general result.

Theorem 1 (from [17]) *Let $Z = X \boxplus Y$, $Z^* = X^* \boxplus Y^*$, $\Delta X = X \oplus X^*$, $\Delta Y = Y \oplus Y^*$ and $\Delta Z = Z \oplus Z^*$, where X, Y, X^* and Y^* are 32-bit words. Given three 32-bit differences ΔX, ΔY and ΔZ, if the probability* $\Pr[(\Delta X, \Delta Y) \to \Delta Z] > 0$, *then* $\Pr[(\Delta X, \Delta Y) \to \Delta Z] = 2^{-s}$, *where the integer s is given by $s = |\{i | 0 \le i \le 30, not((\Delta X)_i = (\Delta Y)_i = (\Delta Z)_i)\}|$.*

Table 3 The two related-key differentials in the 24-round related-key rectangle distinguisher, where the difference in a round is the input difference to this round

Round(i)	$(\Delta L_i, \Delta R_i)$	ΔW_i	Prob.
21	$(e_{21,26,30}, e_{26})$	0	$2^{-4.16}$
22	(e_{26}, e_{31})	e_{31}	$2^{-1.52}$
23	$(e_{31}, 0)$	e_{31}	1
24	(0,0)	0	1
⋮	⋮	⋮	⋮
30	(0,0)	0	1
31	(0,0)	e_{31}	1
32	$(0, e_{31})$	e_{31}	$2^{-1.52}$
33	(e_{31}, e_{26})	0	$2^{-4.16}$
34	$(e_{26}, e_{21,26,30,31})$	0	$2^{-5.15}$
35	$(e_{21,26,30,31}, e_{16,26})$	0	$2^{-8.31}$
36	$(e_{16,26}, e_{11,16,20})$	0	$2^{-7.67}$
output	$(e_{11,16,20}, e_{6,24,26})$	/	/
37	$(e_{31}, 0)$	e_{31}	1
38	(0,0)	0	1
⋮	⋮	⋮	⋮
43	(0,0)	0	1
44	(0,0)	e_{31}	1
output	$(0, e_{31})$	/	/

Take the probability in Round 22 as an example to explain how to obtain the probabilities in those rounds with a probability less than 1. By Theorem 1, it follows that, after passing through the right addition modulo 2^{32} in Round 22, the right-half input difference e_{31} to Round 22 generates the difference $e_{26,31}$ with probability 2^{-1}, the difference $e_{26,27,31}$ with probability 2^{-2}, the difference $e_{26,27,28,31}$ with probability 2^{-3}, the difference $e_{26,27,28,29,31}$ with probability 2^{-4}, the difference $e_{26,27,28,29,30,31}$ with probability 2^{-5}, and the difference $e_{26,27,28,29,30}$ with probability 2^{-5}. After being XORed with the subkey difference e_{31} and, finally, added to the left-half difference e_{26} in the left addition modulo 2^{32} in Round 22, the differences $e_{26,31}$, $e_{26,27,31}$, $e_{26,27,28,31}$, $e_{26,27,28,29,31}$, $e_{26,27,28,29,30,31}$ and $e_{26,27,28,29,30}$ generate the zero difference with probabilities 2^{-1}, 2^{-2}, 2^{-3}, 2^{-4}, 2^{-5} and 2^{-5}, respectively. Hence, this one-round related-key differential $(e_{26}, e_{31}) \to (e_{31}, 0)$ has a probability of $2^{-2} + 2^{-4} + 2^{-6} + 2^{-8} + 2 \cdot 2^{-10} \approx 2^{-1.52}$. The same calculation is applied to the other rounds with a probability less than 1, as well as the probabilities in the differentials described in the following. However, we do not count those whose contribution is negligible; that is, the probabilities in Table 3 are lower bounds.

In the following, we need to compute the square sum of the probabilities of all the possible 16-round differentials $\Delta\alpha \to \Delta\beta^*$ with the same input difference α to E^0, which is computationally infeasible. To address this problem, we just count some of those in which only the last one-round (Case A), two-round (Case B) or five-round (Case C) related-key differential characteristic is different from the 16-round related-key differential $\Delta\alpha \to \Delta\beta$ in Table 3.

Case A: The last one-round (i.e. Round 36) related-key differential characteristic has the form $(e_{16,26}, e_{11,16,20}) \to (e_{11,16,20}, \Delta R_{37})$.
From an analysis of this one-round differential, we know that there exists at least the following number of possible differences for ΔR_{37}:

- 1 possible ΔR_{37} (i.e. $e_{6,24,26}$) with a probability of at least $2^{-7.67}$;
- 4 possible ΔR_{37} (i.e. $e_{6,7,24,26}$, $e_{6,17,24,26}$, $e_{6,24,25,26}$, $e_{6,24,25}$) with a probability of at least $2^{-8.67} + 2^{-9.72} \approx 2^{-8.10}$;
- 7 possible ΔR_{37} (i.e. $e_{6,7,8,24,26}$, $e_{6,7,24,25}$, $e_{6,17,24,25}$, $e_{6,7,17,24,26}$, $e_{6,17,18,24,26}$, $e_{6,17,24,25,26}$, $e_{6,7,24,25,26}$) with a probability of at least $2^{-9.67} + 2^{-11.86} \approx 2^{-9.38}$;
- 2 possible ΔR_{37} (i.e. $e_{6,24,25,27}$, $e_{6,24,25,26,27}$) with a probability of at least $2^{-9.67} + 2^{-12.85} \approx 2^{-9.52}$;
- 10 possible ΔR_{37} with a probability of at least $2^{-10.67}$;

- 15 possible ΔR_{37} with a probability of at least $2^{-11.67}$;
- 21 possible ΔR_{37} with a probability of at least $2^{-12.67}$;
- 28 possible ΔR_{37} with a probability of at least $2^{-13.67}$.

Therefore, we can compute a square sum of at least $2^{-7.67\times2} + 4 \cdot 2^{-8.1\times2} + 7 \cdot 2^{-9.38\times2} + 2 \cdot 2^{-9.52\times2} + 10 \cdot 2^{-10.67\times2} + 15 \cdot 2^{-11.67\times2} + 21 \cdot 2^{-12.67\times2} + 28 \cdot 2^{-13.67\times2} \approx 2^{-13.25}$ for the probabilities of the one-round differentials $(e_{16,26}, e_{11,16,20}) \rightarrow (e_{11,16,20}, \Delta R_{37})$.

Case B: The last two-round (i.e. Rounds 35 and 36) related-key differential characteristic is of the form $(e_{21,26,30,31}, e_{16,26}) \rightarrow (e_{16,26}, \Delta R_{36}) \rightarrow (\Delta R_{36}, \Delta R_{37})$. Here, we only consider $\Delta R_{36} \in \{e_{11,16,20}, e_{11,16,20,21,31}, e_{11,16,20,21}, e_{11,16,20,31}\}$.
After an analysis we learn that these four possibilities of ΔR_{36} have the same probability $2^{-8.31}$ for the one-round differentials $(e_{21,26,30,31}, e_{16,26}) \rightarrow (e_{16,26}, \Delta R_{36})$.
Similar to that described in Case A, we can compute a square sum of at least $2^{-14.04}$ for the case $\Delta R_{36} = e_{11,16,20,31}$, a square sum of at least $2^{-15.55}$ for the case $\Delta R_{36} = e_{11,16,20,21}$ and a square sum of at least $2^{-16.26}$ for the case $\Delta R_{36} = e_{11,16,20,21,31}$.

Case C: The last five-round (i.e. Rounds 32–36) related-key differential characteristic has the form $(0, e_{31}) \rightarrow (e_{31}, \Delta R_{33}) \rightarrow (\Delta R_{33}, \Delta R_{34}) \rightarrow (\Delta R_{34}, \Delta R_{35}) \rightarrow (\Delta R_{35}, \Delta R_{36}) \rightarrow (\Delta R_{36}, \Delta R_{37})$. Here, we only consider $(\Delta R_{34}, \Delta R_{35}) \in \{(e_{21,26,30,31}, e_{16,26}), (e_{21,26,30,31}, e_{16,26,31}), (e_{21,26,30}, e_{16,31}), (e_{21,26,30}, e_{16})\}$.
After an analysis we know that the four possibilities of $(\Delta R_{34}, \Delta R_{35})$ have the same probability of at least $2^{-10.83} + 2^{-13.55} + 2^{-17.56} \approx 2^{-10.62}$ for the three-round differential $(0, e_{31}) \rightarrow (\Delta R_{34}, \Delta R_{35})$.
Then, a detailed analysis reveals the following results for the one-round differential $(\Delta R_{34}, \Delta R_{35}) \rightarrow (\Delta R_{35}, \Delta R_{36})$:

- a probability of at least $2^{-8.31}$ for the eight cases $\Delta R_{34} = e_{21,26,30,31}$ and $(\Delta R_{35}, \Delta R_{36}) \in \{(e_{16,26}, e_{11,16,20,21,31}), (e_{16,26,31}, e_{11,16,20,21,26,31}), (e_{16,26,31}, e_{11,16,20,26,31}), (e_{16,26,31}, e_{11,16,20,21,26}), (e_{16,26,31}, e_{11,16,20,26}), (e_{16,26}, e_{11,16,20,31}), (e_{16,26}, e_{11,16,20,21}), (e_{16,26}, e_{11,16,20})\}$;
- a probability of at least $2^{-7.46}$ for the eight cases $\Delta R_{34} = e_{21,26,30}$ and $(\Delta R_{35}, \Delta R_{36}) \in \{(e_{16}, e_{11,16,20,26,30}), (e_{16}, e_{11,16,20,21,26,30,31}), (e_{16,31}, e_{11,16,20,21,30,31}), (e_{16}, e_{11,16,20,21,26,30}), (e_{16}, e_{11,16,20,26,30,31}), (e_{16,31}, e_{11,16,20,30}), (e_{16,31}, e_{11,16,20,21,30}), (e_{16,31}, e_{11,16,20,30,31})\}$.

Subsequently, similar to that described in Case A, we can get the following results for the one-round differentials $(\Delta R_{35}, \Delta R_{36}) \rightarrow (\Delta R_{36}, \Delta R_{37})$:

- a square sum of at least $2^{-17.11}$ for the probabilities of the differentials from either of the two cases $(\Delta R_{34}, \Delta R_{35}, \Delta R_{36}) \in \{(e_{21,26,30,31}, e_{16,26,31}, e_{11,16,20,26}), (e_{21,26,30,31}, e_{16,26,31}, e_{11,16,20,26,31})\}$;
- a square sum of at least $2^{-18.13}$ for the probabilities of the differentials from either of the two cases $(\Delta R_{34}, \Delta R_{35}, \Delta R_{36}) \in \{(e_{21,26,30,31}, e_{16,26,31}, e_{11,16,20,21,26}), (e_{21,26,30,31}, e_{16,26,31}, e_{11,16,20,21,26,31})\}$;
- a square sum of at least $2^{-18.22}$ for the probabilities of the differentials from each of the eight cases with $\Delta R_{34} = e_{21,26,30}$.

Thus, with the three cases above, we can compute a square sum for the probabilities of the differentials $\Delta\alpha \rightarrow \Delta\beta^*$ of at least $(2^{-4.16} \cdot 2^{-1.52} \cdot 2^{-10.62})^2 \cdot (2^{-8.31\times2} \cdot 2^{-13.25} + 2^{-8.31\times2} \cdot 2^{-14.04} + 2^{-8.31\times2} \cdot 2^{-15.55} + 2^{-8.31\times2} \cdot 2^{-16.26} + 2 \cdot 2^{-8.31\times2} \cdot 2^{-17.11} + 2 \cdot 2^{-8.31\times2} \cdot 2^{-18.13} + 8 \cdot 2^{-7.46\times2} \cdot 2^{-18.22}) \approx 2^{-60.92}$.

As the 8-round related-key differential $\Delta\gamma \rightarrow \Delta\delta$ for E_1 has a probability of 1, we can learn that this distinguisher has a probability of at least $\sum_{\beta^*}[\Pr(\Delta\alpha \rightarrow \Delta\beta^*)^2 \cdot 2^{-64}] = 2^{-60.92} \cdot 2^{-64} = 2^{-124.92}$ for E, while it has a probability of 2^{-128} for a random cipher.

3.2 Attacking rounds 16–51

We next observe three properties of XTEA, as follows.

Property 1 *In the key schedule of XTEA, only 64 user key bits (K_0, K_1) are involved in the nine rounds: Rounds 16–20 and 48–51.*

From the XTEA round structure, we know the following property holds.

Property 2 *For any four rounds i to $i+3$ with a round subkey difference being zero or e_{31}, if the difference just after the ith round is $(0, e_{31})$, then the difference just after the $(i+1)$th round has the form $(e_{31}, e_{26,\sim})$, the difference just after the $(i+2)$th round has the form $(e_{26,\sim}, e_{21,\sim})$, and the difference just after the $(i+3)$th round has the form $(e_{21,\sim}, e_{16,\sim})$.*

For expediency, we denote by $\widetilde{W}_i$ the 32-bit value $(\lfloor \frac{i}{2} \rfloor \boxtimes \theta \boxplus W_i)$ in the ith round. We know that the addition modulo operation definitely preserves the least significant differences in the original positions, and may preserve the other differences in the original positions or propagate them to the more significant positions, but never to the less significant positions. Thus, we can get the following property.

Property 3 *Given a pair of intermediate values (x_l, x_r) and $(\widehat{x}_l, \widehat{x}_r)$ with difference $(e_{j+5,\sim}, e_{j,\sim})$ after the ith round $(1 \le j \le 26)$, to determine if it could produce a difference with the form $(\xi, e_{j+5,\sim})$ just before the ith round, we*

only need to guess the most significant $(32 - j)$ *bits of* $\widetilde{W}_i$ *and the carry bit occurred in the* $(j - 1)$ *bit of the left addition modulo* 2^{32} *operation in the* i*th round, where* ξ *denotes a (possible) particular 32-bit difference.*

Property 1 enables us to go through the nine rounds from Rounds 16–20 and Rounds 48–51 by guessing only 64 user key bits (K_0, K_1). Properties 2 and 3 allow us to break Rounds 45 and 47 by using the early abort technique [18]. The main idea of the early abort technique is to partially determine whether or not a candidate quartet in a (related-key) rectangle attack is useful earlier than usual; if not, we can discard it immediately, which results in less computations in the following steps and may allow us to break more rounds by guessing the subkeys involved, depending on how many candidates are remaining. As mentioned earlier, when we conduct an early abort, we guess only part of the 32 bits of an unknown $\widetilde{W}_i$; otherwise, our attack would be infeasible.

We use plaintext structures in our attack. For a plaintext pair to produce the difference $(e_{21,26,30}, e_{26})$ just before Round 21, the input difference to Round 16 should have the form $(\star, e_{1,\sim})$.

As a result, the above analysis enables us to give the following attack procedure breaking the 36 rounds from Rounds 16–51 of XTEA.

1. Choose a structure S of $2^{62.96}$ plaintexts P_l, where the second rightmost bits of P_l are fixed to be identical, $(l = 1, \ldots, 2^{62.96})$. In a chosen-plaintext attack scenario, obtain all the corresponding ciphertexts for every P_l under the two user keys K_A and K_C, denoted by C_l and C'_l, respectively. Choose the structure $\overline{S}$ of the 2^{63} plaintexts $\overline{P}_j$, where the second rightmost bits of $\overline{P}_j$ are fixed to be the complement of the second rightmost bit value in S, $(j = 1, \ldots, 2^{63})$. In a chosen-plaintext attack scenario, obtain all the corresponding ciphertexts for every $\overline{P}_j$ under the two user keys K_B and K_D, denoted by $\overline{C}^*_j$ and $\overline{C}'^*_j$, respectively. Here, $K_A \oplus K_B = K_C \oplus K_D = (0, 0, 0, e_{31})$, and $K_A \oplus K_C = K_B \oplus K_D = (0, 0, e_{31}, 0)$.
2. Guess the 64 user key bits (K_0, K_1), compute the subkeys $(W_{16}, \ldots, W_{20})$, and do as follows.
   (a) Partially encrypt every plaintext P_l in S with $(W_{16}, \ldots, W_{20})$ through Rounds 16–20 to get its intermediate value just after Round 20, denoted by ε_l. Then, partially decrypt $\varepsilon_l \oplus (e_{21,26,30}, e_{26})$ with $(W_{16}, \ldots, W_{20})$ through Rounds 16–20 to get its plaintext, denoted by $\widetilde{P}_l$; find $\widetilde{P}_l$ in $\overline{S}$. We denote by $\widetilde{C}^*_l$ and $\widetilde{C}'^*_l$ the corresponding ciphertexts for $\widetilde{P}_l$ encrypted under K_B and K_D, respectively. This step generates a total of $2^{62.96}$ plaintext pairs with difference $(e_{21,26,30}, e_{26})$ after Round 20 for every guess of (K_0, K_1), which can propose about $2^{62.96\times 2}/2 = 2^{124.92}$ candidate quartets.
   (b) Compute the subkeys $(W_{48}, \ldots, W_{51})$ with the (K_0, K_1) guessed above. Then, partially decrypt all the 2^{64} ciphertexts with $(W_{48}, \ldots, W_{51})$ through Rounds 48–51 to get their intermediate values just before Round 48; we denote the intermediate values for the ciphertexts C_l, $\widetilde{C}^*_l$, C'_l and $\widetilde{C}'^*_l$ by T_l, $\widetilde{T}^*_l$, T'_l and $\widetilde{T}'^*_l$, respectively. Store the quartets $(T_l, T'_l, \widetilde{T}^*_l, \widetilde{T}'^*_l)$ in a hash table. Finally, check if both $T_{l_1} \oplus T'_{l_2}$ and $\widetilde{T}^*_{l_1} \oplus \widetilde{T}'^*_{l_2}$ have the form $(e_{21,\sim}, e_{16,\sim})$, for $1 \le l_1 \le l_2 \le 2^{62.96}$. If one or more quartets pass this test, then record all the qualified $(T_{l_1}, \widetilde{T}^*_{l_1}, T'_{l_2}, \widetilde{T}'^*_{l_2})$, and go to Step 3; otherwise, repeat Step 2 with another subkey pair.
3. Guess the most significant 16 bits $\widetilde{W}_{47,16-31}$ of the 32-bit value $\widetilde{W}_{47}$, and do as follows.
   (a) For each remaining quartet $(T_{l_1}, \widetilde{T}^*_{l_1}, T'_{l_2}, \widetilde{T}'^*_{l_2})$: partially decrypt T_{l_1} and T'_{l_2} with $\widetilde{W}_{47,16-31}$ under the two possibilities 0 and 1 of the carry bit occurred in bit 15 of the left add modulo operation to get the most significant 16 bits of both the left and right halves of their intermediate values just before Round 47, denoted by Q_{m,l_1} and Q'_{m,l_2}, respectively, and partially decrypt $\widetilde{T}^*_{l_1}$ and $\widetilde{T}'^*_{l_2}$ with $\widetilde{W}_{47,16-31} \oplus \eta^{16}_{15}$ under the two possibilities 0 and 1 of the carry bit occurred in bit 15 of the left add modulo operation to get the most significant 16 bits of both the left and right halves of their intermediate values just before Round 47, denoted by $\widetilde{Q}^*_{n,l_1}$ and $\widetilde{Q}'^*_{n,l_2}$, respectively, where $m, n \in \{0, 1\}$ denote the two possibilities of the carry bit. Finally, check if both $Q_{m,l_1} \oplus Q'_{m,l_2}$ and $\widetilde{Q}^*_{n,l_1} \oplus \widetilde{Q}'^*_{n,l_2}$ have the form $(\eta^{16}_{10,\sim}, \eta^{16}_{5,\sim})$. If one or more quartets $(T_{l_1}, \widetilde{T}^*_{l_1}, T'_{l_2}, \widetilde{T}'^*_{l_2})$ pass this test, then record all the qualified $(Q_{m,l_1}, \widetilde{Q}^*_{n,l_1}, Q'_{m,l_2}, \widetilde{Q}'^*_{n,l_2})$, and go to Step 3-(b); otherwise, repeat Step 3 with another guess of $\widetilde{W}_{47,16-31}$.
   (b) Guess the least significant 16 bits $\widetilde{W}_{47,0-15}$ of $\widetilde{W}_{47}$. For every remaining quartet $(T_{l_1}, \widetilde{T}^*_{l_1}, T'_{l_2}, \widetilde{T}'^*_{l_2})$: partially decrypt T_{l_1} and T'_{l_2} with $\widetilde{W}_{47} (= \widetilde{W}_{47,0-15} || \widetilde{W}_{47,16-31})$ to get their intermediate values just before Round 47, denoted by Q_{l_1} and Q'_{l_2}, respectively, and partially decrypt $\widetilde{T}^*_{l_1}$ and $\widetilde{T}'^*_{l_2}$ with $\widetilde{W}_{47} \oplus e_{31}$ to get their intermediate values just before Round 47, denoted by $\widetilde{Q}^*_{l_1}$ and $\widetilde{Q}'^*_{l_2}$, respectively. Finally, check if both $Q_{l_1} \oplus Q'_{l_2}$ and $\widetilde{Q}^*_{l_1} \oplus \widetilde{Q}'^*_{l_2}$ have the form $(e_{26,\sim}, e_{21,\sim})$. If one or more quartets $(T_{l_1}, \widetilde{T}^*_{l_1}, T'_{l_2}, \widetilde{T}'^*_{l_2})$ pass this test, record all the qualified $(Q_{l_1}, \widetilde{Q}^*_{l_1}, Q'_{l_2}, \widetilde{Q}'^*_{l_2})$, and go to Step 4;

otherwise, repeat this step with another guess of $\widetilde{W}_{47,0-15}$.

4. Compute the subkey $\widetilde{W}_{46}$ with the K_1 guessed above. Partially decrypt every remaining quartet $(Q_{l_1}, \widetilde{Q}^*_{l_1}, Q'_{l_2}, \widetilde{Q}'^*_{l_2})$ with $\widetilde{W}_{46}$ to get their intermediate values just before Round 46, denoted by $(R_{l_1}, \widetilde{R}^*_{l_1}, R'_{l_2}, \widetilde{R}'^*_{l_2})$, respectively. Finally, check if both $R_{l_1} \oplus R'_{l_2}$ and $\widetilde{R}^*_{l_1} \oplus \widetilde{R}'^*_{l_2}$ have the form $(e_{31}, e_{26,\sim})$. If one or more quartets $(Q_{l_1}, \widetilde{Q}^*_{l_1}, Q'_{l_2}, \widetilde{Q}'^*_{l_2})$ pass this test, record all the qualified $(R_{l_1}, \widetilde{R}^*_{l_1}, R'_{l_2}, \widetilde{R}'^*_{l_2})$, and go to Step 5; otherwise, repeat Step 3-(b) with another $\widetilde{W}_{47,0-15}$.
5. Guess the most significant 6 bits $\widetilde{W}_{45,26-31}$ of the 32-bit value $\widetilde{W}_{45}$, and do as follows.
   (a) For each remaining quartet $(R_{l_1}, \widetilde{R}^*_{l_1}, R'_{l_2}, \widetilde{R}'^*_{l_2})$: partially decrypt R_{l_1} and R'_{l_2} with $\widetilde{W}_{45,26-31}$ and $\widetilde{W}_{45,26-31} \oplus \eta^6_5$, respectively, under the two possibilities 0 and 1 of the carry bit occurred in bit 25 of the left add modulo operation to get the most significant 6 bits of the left and right halves of their intermediate values just before Round 45, denoted by U_{s,l_1} and U'_{s,l_2}, respectively, and partially decrypt $\widetilde{R}^*_{l_1}$ and $\widetilde{R}'^*_{l_2}$ with $\widetilde{W}_{45,26-31}$ and $\widetilde{W}_{45,26-31} \oplus \eta^6_5$, respectively, under the two possibilities 0 and 1 of the carry bit occurred in bit 25 of the left add modulo operation to get the most significant 6 bits of the left and right halves of their intermediate values just before Round 45, denoted by $\widetilde{U}^*_{t,l_1}$ and $\widetilde{U}'^*_{t,l_2}$, respectively, where $s, t \in \{0, 1\}$ denote the two possibilities of the carry bit. Finally, check if $U_{s,l_1} \oplus U'_{s,l_2} = \widetilde{U}^*_{t,l_1} \oplus \widetilde{U}'^*_{t,l_2} = (0, \eta^6_5)$. If one or more quartets $(R_{l_1}, \widetilde{R}^*_{l_1}, R'_{l_2}, \widetilde{R}'^*_{l_2})$ pass this test, then record them and go to Step 5-(b); otherwise, repeat Step 5 with another guess of $\widetilde{W}_{45,26-31}$.
   (b) Guess the least significant 26 bits $\widetilde{W}_{45,0-25}$ of $\widetilde{W}_{45}$. For every remaining quartet $(R_{l_1}, \widetilde{R}^*_{l_1}, R'_{l_2}, \widetilde{R}'^*_{l_2})$: partially decrypt R_{l_1} and R'_{l_2} with $\widetilde{W}_{45}(= \widetilde{W}_{45,0-25} || \widetilde{W}_{45,26-31})$ and $\widetilde{W}_{45} \oplus e_{31}$, respectively, to get their intermediate values just before Round 45, denoted by U_{l_1} and U'_{l_2}, respectively; and partially decrypt $\widetilde{R}^*_{l_1}$ and $\widetilde{R}'^*_{l_2}$ with $\widetilde{W}_{45}$ and $\widetilde{W}_{45} \oplus e_{31}$, respectively, to get their intermediate values just before Round 45, denoted by $\widetilde{U}^*_{l_1}$ and $\widetilde{U}'^*_{l_2}$, respectively. Finally, check if both $U_{l_1} \oplus U'_{l_2}$ and $\widetilde{U}^*_{l_1} \oplus \widetilde{U}'^*_{l_2}$ have the form $(0, e_{31})$. If one or more quartets pass this test, then record them, and go to Step 6; otherwise, repeat this step with another guess of $\widetilde{W}_{45,0-25}$.
6. Compute the subkey $\widetilde{W}_{21}$ with the K_2 indicated by $\widetilde{W}_{45}$. For every plaintext quartet $(P_{l_1}, \widetilde{P}^*_{l_1}, P'_{l_2}, \widetilde{P}'^*_{l_2})$ corresponding to a remaining quartet $(U_{l_1}, \widetilde{U}^*_{l_1}, U'_{l_2}, \widetilde{U}'^*_{l_2})$: partially encrypt ε_{l_1} and $\varepsilon_{l_1} \oplus (e_{21,26,30}, e_{26})$ with $\widetilde{W}_{21}$ to get their intermediate values just after Round 21, denoted by V_{l_1} and $\widetilde{V}^*_{l_1}$, respectively, and partially encrypt ε_{l_2} and $\varepsilon_{l_2} \oplus (e_{21,26,30}, e_{26})$ with $\widetilde{W}_{21} \oplus e_{31}$ to get their intermediate values just after Round 21, denoted by V_{l_2} and $\widetilde{V}'^*_{l_2}$, respectively. Finally, check if $V_{l_1} \oplus \widetilde{V}^*_{l_1} = V_{l_2} \oplus \widetilde{V}^*_{l_2} = (e_{26}, e_{31})$. If one or more quartets $(P_{l_1}, \widetilde{P}^*_{l_1}, P'_{l_2}, \widetilde{P}'^*_{l_2})$ pass this test, then record $(K_0, K_1, \widetilde{W}_{47}, \widetilde{W}_{45})$, and execute Step 7; otherwise, repeat Step 5-(b) with another guess of $\widetilde{W}_{45,0-25}$.
7. For a recorded $(K_0, K_1, \widetilde{W}_{47}, \widetilde{W}_{45})$, do a trial encryption with three plaintext/ciphertext pairs to determine the correct user key of the 36-round XTEA (If all the possible guesses during any of Steps 3∼5 are tested, repeat its previous steps with other guesses).

The attack requires $2 \cdot (2^{62.96} + 2^{63}) \approx 2^{64.98}$ related-key chosen plaintexts. The required memory for this attack is dominated by the ciphertexts, which is approximately $2^{64.98} \cdot 8 = 2^{67.98}$ memory bytes.

The time complexity of Step 2-(a) is about $2 \cdot 2^{62.96} \cdot 2^{64} \cdot \frac{5}{36} \approx 2^{125.12}$ 36-round XTEA encryptions. The time complexity of Step 2-(b) is dominated by the partial decryptions, which is about $2^{64} \cdot 2^{64} \cdot \frac{4}{36} \approx 2^{124.83}$ 36-round XTEA encryptions. Besides, Step 2-(b) requires about $2^{64} \cdot 2^{62.96} = 2^{126.96}$ memory accesses, which is negligible compared with the $2^{124.83}$ encryptions. In Step 2-(b), the probability that a quartet meets the filtering condition is $\left(\frac{1}{2^{22}} \cdot \frac{1}{2^{17}}\right)^2 = 2^{-78}$, so it follows that the expected number of the quartets passing the test for each guess is $2^{124.92} \cdot 2^{-78} = 2^{46.92}$; as the probability that one or more quartets pass the test for a wrong guess is about 1, almost all the 2^{64} possible (K_0, K_1) pass Step 2-(b).

In Step 3-(a), the time complexity is about $4 \cdot 2^{64} \cdot 2^{16} \cdot 2^{46.92} \cdot 2 \cdot \frac{1}{2} \cdot \frac{1}{36} \approx 2^{123.75}$, where $\frac{1}{2}$ means the average fraction of the key bits that are tested. In this step, the probability that a remaining quartet meets the filtering condition is $(\frac{1}{2^{10}} + \frac{1}{2^{10}})^2 = 2^{-18}$, so the expected number of the quartets passing the test for each guess is $2^{46.92} \cdot 2^{-18} = 2^{28.92}$, and the probability that one or more quartets pass the test for a wrong guess is about 1. Thus, it is expected that almost all the 2^{80} possible $(K_0, K_1, \widetilde{W}_{47,16-31})$ pass this step. In Step 3-(b), the time complexity is about $4 \cdot 2^{80} \cdot 2^{16} \cdot 2^{28.92} \cdot 2 \cdot \frac{1}{2} \cdot \frac{1}{36} \approx 2^{121.75}$, and the probability that a remaining quartet meets the filtering condition is $2^{-1\times 2} = 2^{-2}$, because both the pairs in a remaining quartet should produce the required carry bits occurred in bit 15 of the left add modulo operation; hence, the expected number of the quartets passing the test for each guess is $2^{28.92} \cdot 2^{-2} = 2^{26.92}$, and almost all the 2^{96} possible $(K_0, K_1, \widetilde{W}_{47})$ pass Step 3-(b).

In Step 4, the time complexity is about $4 \cdot 2^{96} \cdot 2^{26.92} \cdot \frac{1}{2} \cdot \frac{1}{36} \approx 2^{118.75}$. In this step, the probability that a remaining

quartet meets the filtering condition is $2^{-10\times 2} = 2^{-20}$, so the expected number of the quartets passing the test for each guess is $2^{26.92} \cdot 2^{-20} = 2^{6.92}$, and the probability that one or more quartets pass the test for a wrong guess is about 1. Thus, it is expected that almost all the 2^{96} possible $(K_0, K_1, \widetilde{W}_{47})$ pass this step.

In Step 5-(a), the time complexity is about $4 \cdot 2^{96} \cdot 2^6 \cdot 2^{6.92} \cdot 2 \cdot \frac{1}{2} \cdot \frac{1}{36} \approx 2^{105.75}$, and the probability that a remaining quartet meets the filtering condition is $\left(\frac{1}{2^5} + \frac{1}{2^5}\right)^2 = 2^{-8}$, so the expected number of the quartets passing the test for each guess is $2^{6.92} \cdot 2^{-8} = 2^{-1.08}$; the probability that one or more quartets pass the test for a wrong guess is $\sum_{i=1}^{2^{6.92}} [\binom{2^{6.92}}{i} \cdot (2^{-8})^i \cdot (1-2^{-8})^{2^{6.92}-i}] \approx 2^{-1.08}$. Hence, it is expected that about $2^{96} \cdot 2^6 \cdot 2^{-1.08} = 2^{100.92}$ possible $(K_0, K_1, \widetilde{W}_{47}, \widetilde{W}_{45,26-31})$ pass Step 5-(a). In Step 5-(b), the time complexity is about $4 \cdot 2^{100.92} \cdot 2^{26} \cdot \frac{1}{2} \cdot \frac{1}{36} \approx 2^{122.75}$. In this step, the probability that a remaining quartet meets the filtering condition is $2^{-1\times 2} = 2^{-2}$, as a result, it is expected that about $2^{126.92} \cdot 2^{-2} = 2^{124.92}$ possible $(K_0, K_1, \widetilde{W}_{47}, \widetilde{W}_{45})$ pass Step 5-(b).

In Step 6, the time complexity is about $4 \cdot 2^{124.92} \cdot \frac{1}{2} \cdot \frac{1}{36} \approx 2^{120.75}$. In this step, the probability that a remaining quartet meets the filtering condition is $2^{-4.16\times 2} = 2^{-8.32}$, so it follows that about $2^{124.92} \cdot 2^{-8.32} = 2^{116.6}$ possibilities of $(K_0, K_1, \widetilde{W}_{47}, \widetilde{W}_{45})$ are expected to pass this step, which result in about $2^{116.6}$ trials in Step 7.

Therefore, the attack has a total of about $2^{126.44} (\approx 2^{125.12} + 2^{124.83} + 2^{123.75} + 2^{121.75} + 2^{122.75})$ 36-round XTEA encryptions.

The probability that a wrong key is suggested in Step 7 is approximately 2^{-192}, so the expected number of suggested wrong 128-bit keys is about $2^{-192} \cdot 2^{116.6} = 2^{-75.4}$, which is extremely low. In Step 6, the expected number of quartets for the correct key guess is $2^{124.92} \cdot 2^{-124.92} = 1$, and the probability that one or more quartets pass the test for the correct key guess is approximately $\sum_{i=1}^{2^{124.92}} [\binom{2^{124.92}}{i} \cdot (2^{-124.92})^i \cdot (1-2^{-124.92})^{2^{124.92}-i}] \approx 0.63$. Therefore, with a success probability of 63%, the related-key rectangle attack can work out the 128-bit user key of the 36-round XTEA, faster than exhaustive key search.

4 Attacking 36-round XTEA under certain weak key assumptions

Generally speaking, a weak key is defined as a key under which the block cipher is more vulnerable to be attacked. It is usually required to have some particular characteristics, such as fixed bit values, etc. In a practical view, a related-key rectangle attack under weak key assumptions is much more difficult to conduct than that without making a weak key assumption.

4.1 A 33-round related-key rectangle distinguisher under a class of weak keys

In [16], Lee et al. gave a 33-round related-key rectangle distinguisher for Rounds 2–34 under a class of weak user keys (K_A, K_B, K_C, K_D).

Let $K_A = (K_0, K_1, K_2, K_3)$, $K_B = (K_0', K_1, K_2, K_3)$, $K_C = (K_0, K_1', K_2, K_3)$ and $K_D = (K_0', K_1', K_2, K_3)$ be a quartet of weak keys, such that the following conditions hold:

$$(\theta \cdot 4 \boxplus K_0) \oplus (\theta \cdot 4 \boxplus K_0') = e_{4,13,22,31}, \quad (1)$$

$$(\theta \cdot 8 \boxplus K_0) \oplus (\theta \cdot 8 \boxplus K_0') = e_{4,13,22,31}, \quad (2)$$

$$(\theta \cdot 9 \boxplus K_0) \oplus (\theta \cdot 9 \boxplus K_0') = e_{4,13,22,31}, \quad (3)$$

$$(\theta \cdot 5 \boxplus K_0) \oplus (\theta \cdot 5 \boxplus K_0') = e_{4,13,22,23,31}, \quad (4)$$

$$(\theta \cdot 13 \boxplus K_1) \oplus (\theta \cdot 13 \boxplus K_1') = e_{4,13,22,31}, \quad (5)$$

$$(\theta \cdot 14 \boxplus K_1) \oplus (\theta \cdot 14 \boxplus K_1') = e_{4,13,22,31}. \quad (6)$$

The first related-key differential $\Delta\alpha \to \Delta\beta$ for this distinguisher is the 18-round related-key differential $(0,0) \to (e_{4,13,22,31}, 0)$ with probability 2^{-19} for Rounds 2–19 under the class of weak keys with (K_0, K_0') satisfying Eqs. (1)–(4). The second related-key differential $\Delta\gamma \to \Delta\delta$ for this distinguisher is the 15-round related-key differential $(0,0) \to (0,0)$ with probability 2^{-9} for Rounds 20–34 under the class of weak keys with (K_1, K_1') satisfying Eqs. (5) and (6). Note that $(e_{4,13,22,31} << 4) \oplus (e_{4,13,22,31} >> 5) = 0$. After an analysis Lee et al. concluded that there are about $2^{108.21}$ weak key quartets (K_A, K_B, K_C, K_D). However, by performing a computer program, we get that there exist about $2^{19.73}$ qualified (K_0, K_0') pairs and about $2^{26.94}$ qualified (K_1, K_1') pairs, so the correct number of the weak key quartets should be about $2^{110.67}$.

Lee et al. computed a square sum of at least $2^{-36.76} (= 2^{-18.38\times 2})$ for the probabilities of all the 18-round related-key differential $\Delta\alpha \to \Delta\beta'$ for Rounds 2–19 by counting many possible differences β'. Thus, this 33-round related-key rectangle distinguisher under the class of weak keys has a probability of at least $2^{-118.76} (= 2^{-36.76} \cdot 2^{-9\times 2} \cdot 2^{-64})$ for the correct key, while it has a probability of 2^{-128} for a wrong key.

Finally, by guessing the 32-bit round key in Round 35, Lee et al. applied this 33-round distinguisher to mount a related-key rectangle attack on the 34 rounds from Rounds 2–35 of XTEA.

One might ask: why not append one-round related-key differential $(e_{4,13,22,31}, 0) \xrightarrow{e_{4,13,22,31}} (0,0)$ with probability 2^{-3} before the 33-round distinguisher to get a 34-round distinguisher under a new class of weak keys? This looks reasonable, but the fact is unfortunately that there does not exist such a pair (K_0, K_0') that simultaneously satisfies Eqs. (1)–(4) and

the additional condition $K_0 \oplus K_0^{'} = e_{4,13,22,31}$. Appending one-round related-key differential after the 33-round distinguisher is impossible as well.

4.2 Attacking rounds 1–36 under the class of weak keys

We find that Lee et al.'s attack can be extended to break Rounds 1–36 (the first 36 rounds) of XTEA by the following two observations: First, note that the same subkey K_1 is used in both Rounds 35 and 36 in the key schedule of XTEA, thus we can decrypt Rounds 35 and 36 by guessing the subkey pair $(K_1, K_1^{'})$, instead of just Round 35 in Lee et al.'s attack. Second, we can similarly use a key recovery in Round 1 to recover the subkey pair $(K_0, K_0^{'})$. Besides, from Eqs. (1)–(6) we can learn that $K_0 \oplus K_0^{'} = e_{4,\sim}$ and $K_1 \oplus K_1^{'} = e_{4,\sim}$ must hold.

The attack is similar to that given in Sect. 3.2. We briefly describe it as follows.

1. Choose $2^{33.83}$ structures S_i of 2^{28} plaintexts $P_{i,l}$ each, $i = 1, 2, \ldots, 2^{33.83}$, $l = 1, 2, \ldots, 2^{28}$, where in a structure the rightmost 36 bits of $P_{i,l}$ are fixed, and the other 28 bit positions take all the possible values. Choose other $2^{33.83}$ structures S_i' of 2^{28} plaintexts $P_{i,l}'$ each, where a structure is defined as above. In a chosen-plaintext attack scenario, obtain all the corresponding ciphertexts of $P_{i,l}$ under the weak user keys K_A and K_B, denoted by $C_{i,l}$ and $C_{i,l}^*$, respectively; and obtain all the corresponding ciphertexts of $P_{i,l}'$ under the weak user keys K_C and K_D, denoted by $C_{i,l}'$ and $C_{i,l}'^*$, respectively.
2. Guess a 32-bit subkey pair $(K_0, K_0^{'})$ for Round 1 under the weak key assumptions. Encrypt every plaintext $P_{i,l}$ through Round 1 with K_0 to get its intermediate value $x_{i,l}$ just after Round 1. Then, decrypt $x_{i,l}$ through Round 1 with $K_0^{'}$ to get its plaintext, denoted by $\widetilde{P}_{i,l}$. Find $\widetilde{P}_{i,l}$ in S_i. We denote by $\widetilde{C}_{i,l}$ and $\widetilde{C}_{i,l}^*$ the corresponding ciphertexts for $\widetilde{P}_{i,l}$ encrypted under K_A and K_B, respectively. Encrypt every plaintext $P_{i,l}'$ through Round 1 with K_0 to get its intermediate value $x_{i,l}'$ just after Round 1. Then, decrypt $x_{i,l}'$ through Round 1 with $K_0^{'}$ to get its plaintext, denoted by $\widetilde{P}'_{i,l}$. Find $\widetilde{P}'_{i,l}$ in S_i'. We denote by $\widetilde{C}_{i,l}'$ and $\widetilde{C}_{i,l}'^*$ the corresponding ciphertexts for $\widetilde{P}'_{i,l}$ encrypted under K_C and K_D, respectively. This step can propose about $(2^{33.83} \cdot 2^{28}/2)^2 = 2^{121.76}$ candidate quartets for every guess of $(K_0, K_0^{'})$.
3. Guess a 32-bit subkey pair $(K_1, K_1^{'})$ for Rounds 35 and 36 under the weak key assumptions, and do as follows.
   (a) Partially decrypt all the ciphertexts $C_{i,l}$ and $\widetilde{C}_{i,l}^*$ with K_1 to get their intermediate values just before Round 36, denoted by $T_{i,l}$ and $\widetilde{T}_{i,l}^*$, respectively; partially decrypt all the ciphertexts $C_{i,l}'$ and $\widetilde{C}_{i,l}'^*$ with $K_1^{'}$ to get their intermediate values just before Round 36, denoted by $T_{i,l}'$ and $\widetilde{T}_{i,l}'^*$, respectively. Store all the values $(T_{i,l}, \widetilde{T}_{i,l}^*, T_{i,l}', \widetilde{T}_{i,l}'^*)$ into a hash table. Finally, check if both $T_{i_1,l_1} \oplus T_{i_2,l_2}'$ and $\widetilde{T}_{i_1,l_1}^* \oplus \widetilde{T}_{i_2,l_2}'^*$ have the form $(0, e_{4,\sim})$, for $1 \le i_1 \le i_2 \le 2^{33.83}$ and $1 \le l_1, l_2 \le 2^{28}$. If 6 or more quartets pass this test, record all the qualified $(T_{i_1,l_1}, \widetilde{T}_{i_1,l_1}^*, T_{i_2,l_2}', \widetilde{T}_{i_2,l_2}'^*)$, and go to Step 3-(b); otherwise, repeat Step 3 with another subkey pair. There is a filtering condition of about $2^{-37\times 2} = 2^{-74}$ over the candidate quartets, so it is expected only about $2^{121.76} \cdot 2^{-74} = 2^{47.76}$ quartets remain after this step for every key guess of $(K_0, K_0^{'}, K_1, K_1^{'})$.
   (b) For every remaining quartet $(T_{i_1,l_1}, \widetilde{T}_{i_1,l_1}^*, T_{i_2,l_2}', \widetilde{T}_{i_2,l_2}'^*)$, partially decrypt T_{i_1,l_1} and $\widetilde{T}_{i_1,l_1}^*$ with K_1 to get their intermediate values just before Round 35, denoted by Q_{i_1,l_1} and $\widetilde{Q}_{i_1,l_1}^*$, respectively, and partially decrypt T_{i_2,l_2}' and $\widetilde{T}_{i_2,l_2}'^*$ with $K_1^{'}$ to get their intermediate values just before Round 35, denoted by Q_{i_2,l_2}' and $\widetilde{Q}_{i_2,l_2}'^*$, respectively. Then, check if both $Q_{i_1,l_1} \oplus Q_{i_2,l_2}'$ and $\widetilde{Q}_{i_1,l_1}^* \oplus \widetilde{Q}_{i_2,l_2}'^*$ are equal to zero. If the number of the quartets passing this test is greater than or equal to 6, then record $(K_0, K_0^{'}, K_1, K_1^{'})$, and go to Step 4; otherwise, repeat Step 3 with another subkey pair.
4. For a recorded $(K_0, K_0^{'}, K_1, K_1^{'})$, exhaustively search for the remaining 64 key bits with two pairs of plaintexts and ciphertexts. If a 128-bit key is suggested, output it as the user key of the 36-round XTEA; otherwise, go to Step 2.

The time complexity of the attack is dominated by the partial decryptions in Step 3-(a), which is about $4 \cdot 2^{60.83} \cdot 2^{46.67} \cdot \frac{1}{36} \approx 2^{104.33}$ 36-round XTEA encryptions. Step 3-(a) also requires about $2^{46.67} \cdot 2^{60.83} = 2^{107.5}$ memory accesses; this is negligible compared with the $2^{104.33}$ encryptions. Therefore, the attack is faster than exhaustive key search among the $2^{110.67}$ weak keys. The success probability of the attack is about 80%.

5 Conclusions

In this paper, we analyse the security of the XTEA block cipher against related-key rectangle attacks. We have presented a related-key rectangle attack on a series of inner 36 rounds of XTEA without making a weak key assumption, and a related-key rectangle attack on the first 36 rounds of XTEA under certain weak key assumptions. Like most cryptanalytic results on block ciphers, the presented attacks are theoretical. These are the best currently published cryptanalytic results on XTEA in terms of the numbers of attacked rounds.

Acknowledgements The author is very grateful to his supervisor Prof. Chris Mitchell and an anonymous referee for their comments.

References

1. Biham, E.: New types of cryptanalytic attacks using related keys. In: Helleseth, T. (ed.) Advances in Cryptology—Proceedings of EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Norway, 23–27 May 1993. Lecture Notes in Computer Science, vol. 765, pp. 398–409. Springer, Heidelberg (1993)
2. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) Advances in Cryptology—Proceedings of EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Czech Republic, 2–6 May 1999. Lecture Notes in Computer Science, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
3. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack—rectangling the Serpent. In: Pfitzmann, B. (ed.) Advances in Cryptology—Proceedings of EUROCRYPT '01, International Conference on the Theory and Application of Cryptographic Techniques, Austria, 6–10 May 2001. Lecture Notes in Computer Science, vol. 2045, pp. 340–357. Springer, Heidelberg (2001)
4. Biham, E., Dunkelman, O., Keller, N.: Related-key boomerang and rectangle attacks. In: Cramer, R. (ed.) Advances in Cryptology—Proceedings of EUROCRYPT '05, the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Denmark, 22–26 May 2005. Lecture Notes in Computer Science, vol. 3494, pp. 507–525. Springer, Heidelberg (2005)
5. Biham, E., Shamir, A.: Differential cryptanalysis of the Data Encryption Standard. Springer, Heidelberg (1993)
6. Hong, S., Hong, D., Ko, Y., Chang, D., Lee, W., Lee, S.: Differential cryptanalysis of TEA and XTEA. In: Lim, J., Lee, D. (eds.) Proceedings of ICISC '03, the 6th International Conference on Information Security and Cryptology, Korea, 27–28 November 2003. Lecture Notes in Computer Science, vol. 2971, pp. 402–417. Springer, Heidelberg (2004)
7. Hong, S., Kim, J., Lee, S., Preneel, B.: Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192. In: Gilbert, H., Handschuh, H. (eds.) Proceedings of FSE '05, the 12th Fast Software Encryption Workshop, France, 21–23 February 2005. Lecture Notes in Computer Science, vol. 3557, pp. 368–383. Springer, Heidelberg (2005)
8. Kelsey, J., Schneier, B., Wagner, D.: Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In: Koblitz, N. (ed.) Advances in Cryptology—Proceedings of CRYPTO '96, the 16th Annual International Cryptology Conference, USA, 18–22 August 1996. Lecture Notes in Computer Science, vol. 1109, pp. 237–251. Springer, Heidelberg (1996)
9. Kelsey, J., Schneier, B., Wagner, D.: Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. In: Han, Y., Okamoto, T., Qing, S. (eds.) Proceedings of ICICS '97, the First International Conference on Information and Communication Security, China, 11–14 November 1997. Lecture Notes in Computer Science, vol. 1334, pp. 233–246. Springer, Heidelberg (1997)
10. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round MARS and Serpent. In: Schneier, B. (ed.) Proceedings of FSE '00, the 7th Fast Software Encryption Workshop, USA, 10–12 April 2000. Lecture Notes in Computer Science, vol. 1978, pp. 75–93. Springer, Heidelberg (2001)
11. Kim, J., Kim, G., Hong, S., Lee, S., Hong, Dowon.: The related-key rectangle attack—application to SHACAL-1. In: Wang, H., Pieprzyk, J., Varadharajan, V. (eds.) Proceedings of ACISP '04, the 9th Australasian Conference on Information Security and Privacy, Australia, 13–15 July 2004. Lecture Notes in Computer Science, vol. 3108, pp. 123–136. Springer, Heidelberg (2004)
12. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) Advances in Cryptology—Proceedings of ASIACRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Australia, 13–16 December 1992. Lecture Notes in Computer Science, vol. 718, pp. 196–208. Springer, Heidelberg (1993)
13. Knudsen, L.R.: Trucated and higher order differentials. In: Gollmann, D. (ed.) Proceedings of FSE '96, the Third Fast Software Encryption Workshop, UK, 21–23 February 1996. Lecture Notes in Computer Science, vol. 1039, pp. 196–211. Springer, Heidelberg (1996)
14. Knudsen, L.R.: DEAL—a 128-bit block cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998)
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.) Proceedings of FSE '04, the 11th Fast Software Encryption Workshop, India, 5–7 February 2004. Lecture Notes in Computer Science, vol. 3017, pp. 299–316. Springer, Heidelberg (2004)
16. Lee, E., Hong, D., Chang, D., Hong, S., Lim, J.: A weak key class of XTEA for a related-key rectangle attack. In: Nguyen, P.Q. (Ed.) Progressin Cryptology—Proceedings of VIETCRYPT '06, the First International Conferenceon Cryptology in Vietnam, Vietnam, 25–28 September 2006. Lecture Notes in Computer Science, vol. 4341, pp. 286–297. Springer, Heidelberg (2006)
17. Lipmaa, H., Moriai, S.: Eficient algorithms for computing differential properties of addition. In: Matsui, M. (ed.) Proceedings of FSE '01, the 8th Fast Software Encryption Workshop, Japan, 2–4 April 2001. Lecture Notes in Computer Science, vol. 2355, pp. 336–350. Springer, Heidelberg (2002)
18. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Related-key rectangle attack on 42-round SHACAL-2. In: Katsikas, S.K., Lopez, J., Backes, M., Gritzalis, S., Preneel, B. (eds.) Proceedings of ISC '06, the 9th Information Security Conference, Greece, 30 August–2 September 2006. Lecture Notes in Computer Science, vol. 4176, pp. 85–100. Springer, Heidelberg (2006)
19. Moon, D., Hwang, K., Lee, W., Lee, S., Lim, J.: Impossible differential cryptanalysis of reduced round XTEA and TEA. In: Daemen, J., Rijmen, V. (eds.) Proceedings of FSE '02, the 9th Fast Software Encryption Workshop, Belgium, 4–6 February 2002. Lecture Notes in Computer Science, vol. 2365, pp. 49–60. Springer, Heidelberg (2002)
20. Needham, R.M., Wheeler, D.J.: TEA extensions. Technical report, the Computer Laboratory, University of Cambridge (1997) Archive available at: http://www.cl.cam.ac.uk/ftp/users/djw3/xtea.ps
21. Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) Proceedings of FSE '99, the 6th Fast Software Encryption Workshop, Italy, 24–26 March 1999. Lecture Notes in Computer Science, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)
22. Wheeler, D.J., Needham, R.M.: TEA, a tiny encryption algorithm. In: Preneel, B. (ed.) Proceedings of FSE '94, the Second Fast Software Encryption Workshop, Belgium, 14–16 December 1994. Lecture Notes in Computer Science, vol. 1008, pp. 363–366. Springer, Heidelberg (1995)

Author Biography

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.