Impossible Differential Cryptanalysis of reduced-round TEA and XTEA

Masroor Hajari*,Seyyed Arash Azimi*,Poorya Aghdaie†
*Information Systems and Security Lab (ISSL)
†Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
{hajari_masroor, arash_azimi,
aghdaie_poorya}@ee.sharif.edu

Mahmoud Salmasizadeh§, Mohammad Reza Aref*
§Electronics Research Institute
Sharif University of Technology
*Information Systems and Security Lab (ISSL)
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
{salmasi, aref}@sharif.edu

***Abstract*-TEA and XTEA are two lightweight Feistel block ciphers, each of which has a block size of 64 bits and a key size of 128 bits. These two ciphers have ARX structure, i.e. their round functions consist of modular addition, shift and XOR to be exact. Since each operation of TEA and XTEA can be done in a bitwise fashion, we are able to use early abort technique in the impossible differential attack that helps us to remove inappropriate pairs as soon as possible, hence decreasing time complexity. In this paper we present two new 15-round impossible differential characteristics, resulting in the first known impossible differential cryptanalysis mounted on 19 rounds of TEA and 25 rounds of XTEA.**

Keywords: Impossible Differential Cryptanalysis; Lightweight; Block Cipher; TEA; XTEA

I. INTRODUCTION

The majority of electrical devices and computer systems are designed to cope with the ever-increasing today's demands such as sufficient security level while the costs are affordable. Among the modern cryptographic algorithms available for IT, lightweight cryptography is generally regarded to have an inevitable role, providing indispensable security in resource-limited platforms such as sensor networks and RFID tags.

Lightweight block ciphers such as PRESENT[1], Clefia[2], Piccolo[3], HIGHT[4], LED[5], etc. have been designed to provide moderate security level, utilizing limited resources such as power, area and cost. In order to analyze security level of lightweight block ciphers, quite a few impossible differential attacks have been applied on Clefia[6], [7], Piccolo[8], [9], HIGHT[10], [11], etc.

TEA is a lightweight block cipher designed by Needham and Wheeler in 1994 [12]. Needham and Wheeler overcame quite a few weaknesses of TEA by designing XTEA algorithm in 1997 [13]. TEA was implemented in XBOX consoles by Microsoft as a hash function. Moreover, TEA and XTEA are used in Linux kernel.

Both TEA and XTEA have 64 rounds, a key size of 128 bits, and a block size of 64 bits. The round functions of both TEA and XTEA are comprised of addition modulo 2^{32} , shift and XOR as Feistel cipher.

The first known impossible differential cryptanalysis is presented by Moon et.al. mounted on 11 rounds of TEA and 14 rounds of XTEA by using 10-round and 12-round impossible differential characteristics, respectively [14]. Chen improved the impossible differential cryptanalysis by attacking to 17 rounds of TEA and 23 rounds of XTEA [10]. The results of previous attacks, including the two attacks mentioned above, and our attack is summarized in Table I and Table II.

Bitwise early abort is a technique applicable to ARX structures. After finding each bit of modular addition, inappropriate pairs are sieved. Therefore, unnecessary computations are cut.

Taking advantage of the ARX function, we are able to attack faster using early abort technique. Since the only nonlinear part of round functions of TEA and XTEA is modular addition, we are able to perform bitwise early abort, leading to remove the plaintexts that do not satisfy conditions of the attack without computing the entire bits of the output. Therefore, useless plaintexts are removed faster and the time complexity significantly decreases. Moreover, in order to apply the early abort technique, we find the corresponding carry of modular addition by proceeding from the most significant bit to the least significant bit. Doing so results in a considerable decrease in the time complexity.

Using the mentioned ploys and other techniques, we present the first 15-round impossible differential characteristics, leading to the best known impossible differential attacks for 19 rounds of TEA and 25 rounds of XTEA. The results show that we can recover the key of TEA by using $2^{63.6}$chosen plaintexts and $2^{125.05}$ 19-round encryptions and the key of XTEA by using $2^{63.6}$chosen plaintexts and $2^{126.15}$ 25-round encryptions. The results are shown in Table I and Table II.

TABLE I. IMPOSSIBLE DIFFERENTIAL ATTACKS ON TEA

Attack	Rounds	Time Complexity	Data Complexity	Memory (bytes)	Reference
IDC	11	2^{84} En	$2^{52.5}$CP	NA	[14]
TDC	17	$2^{123.37}$ En	1920CP	NA	[17]
IDC	17	$2^{106.6}$ En	2^{57}CP	2^{49}	[10]
IDC	19	$2^{125.05}$ En	$2^{63.6}$ CP	$2^{36.6}$	Section III
ZLC	21	$2^{121.52}$ En	$2^{62.62}$KP	negligible	[16]
ZLC	23	$2^{119.64}$ En	2^{64}	negligible	[16]

EN: Encryption, CP: Chosen Plaintexts, NA: Not Available, IDC: Impossible Differential Cryptanalysis, TDC: Truncated Differential Cryptanalysis, ZLC: Zero correlation Linear Cryptanalysis

This work was partially supported by Iran NSF (INSF) under Grant No. 92.32575 and INSF cryptography chair.

TABLE II. IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS OF XTEA

Attack	Rounds	Time Complexity	Data Complexity	Memory (bytes)	Reference
IDC	14	2^{85} En	$2^{62.5}$CP	NA	[14]
TDC	23	$2^{120.65}$En	$2^{20.55}$CP	NA	[17]
MITM	23	2^{117}En	18KP	NA	[18]
IDC	23	$2^{114.9}$En	$2^{62.3}$CP	$2^{94.3}$	[10]
IDC	23	$2^{105.6}$ En $+2^{101}$ MA	2^{63}CP	2^{103}	[10]
IDC	25	$2^{126.15}$En	$2^{63.6}$ CP	$2^{96.6}$	Section IV
ZLC	25	$2^{124.53}$En	$2^{62.3}$CP	2^{30}	[16]
ZLC	27	$2^{120.71}$ En	2^{64}	negligible	[16]

En: Encryption, CP: Chosen Plaintexts, MA: Memory Access, NA: Not Available, IDC: Impossible Differential Cryptanalysis, TDC: Truncated Differential Cryptanalysis, ZLC: Zero Correlation Linear Cryptanalysis, MITM: Meet In The Middle Attack

This paper is organized as follows. The second section is dedicated to the notations and some observations on both TEA and XTEA, including the 15-round impossible differential characteristics. We present the impossible differential attack on TEA and XTEA in the third and fourth sections, respectively. The last section concludes the paper.

II. PRELIMINARY

A. Notations

$\|$	: concatenation operation
$\oplus$	: Xor operation
$\boxplus$	: modular addition
MSB	: most significant bit
LSB	: least significant bit
LSB_x	: x least significant bits
ΔX	: Xor of X and X', i.e. $X \oplus X'$
D[i]	: difference of two 32-bit arrays in which the $LSB_{i-1} = 0$, i^{th} bit is 1 and the rest have arbitrary differences
O_i	: the i-bit array of zeros
$LS_4(\cdot)$ (or $4 \ll$)	: 4-bit shift to the left
$RS_5(\cdot)$ (or $\gg 5$)	: 5-bit shift to the right
$X\{j\}$	: j^{th}bit of $X \in \{0,1\}^{32}$
L_i	: left output subblock of round i
R_i	: right output subblock of round i

B. Brief description of TEA and XTEA

TEA and XTEA are 64-round Feistel lightweight block cipher with 64-bit block size and 128-bit key size.

Key scheduling. The key of TEA is divided up into four 32-bit parts. Each subkey is mapped to one of the four parts by key schedule algorithm that is as follows:

$$K = K_0 \parallel K_1 \parallel K_2 \parallel K_3$$

$$K_i = \begin{cases} K_0 & i = 1\ (mod 2) \\ K_2 & i = 0\ (mod 2) \end{cases} \quad K'_i = \begin{cases} K_1 & i = 1\ (mod 2) \\ K_3 & i = 0\ (mod 2) \end{cases}$$

Note that $K_i$and K'_i are clearly distinguishable in Fig. 2.

The key of XTEA is divided up into four 32-bit parts like TEA and the mapping of subkeys are shown in Fig. 1.

	Round Key															
Rounds [1 – 16]	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
Rounds [17 – 32]	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
Rounds [33 – 48]	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
Rounds [49 – 64]	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

Figure 1. Key schedule of XTEA [10]

Round constant. The round constant of TEA is as follows:

$$\delta = 0x9e3779b9$$

$$\delta_i = \begin{cases} \frac{i+1}{2} \cdot \delta\ (mod\ 2^{32}) \ , & i = 1\ (mod\ 2) \\ \frac{i}{2} \cdot \delta \quad (mod\ 2^{32}) , & i = 0\ (mod\ 2) \end{cases}$$

The round constant of XTEA is as follows:

$$\delta_i = \begin{cases} \frac{i-1}{2} \cdot \delta\ \ (mod\ 2^{32}) \ , & i = 1\ (mod\ 2) \\ \frac{i}{2} \cdot \delta \quad (mod\ 2^{32}) \ , & i = 0\ (mod\ 2) \end{cases}$$

Round function. Round function of TEA and XTEA are shown in Fig. 2 and Fig. 3, respectively.

C. Some observations on TEA and XTEA

Throughout the paper, following observations are used:

Observation 1. If we assume the plain text remains unchanged, keys which affect the cipher text comprise effective key. The effective key length of TEA is 126 bits.

Proof. The observation above is proved in [15].

Observation 2. For both of TEA and XTEA, if the input difference at round i is D$[m] \parallel D[m-5]$, then the input difference of the $(i+1)^{\text{th}}$ round will be equal to $D[m-5] \parallel D[m-10]$. Furthermore, if the input difference at round i is $[m-5] \parallel D[m]$, then the input difference of the $(i-1)^{\text{th}}$ round will be $D[m-10] \parallel D[m-5]$.

Proof. This observation is proved in [10].

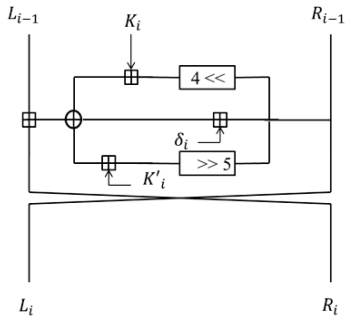

Figure 2. Round function of TEA

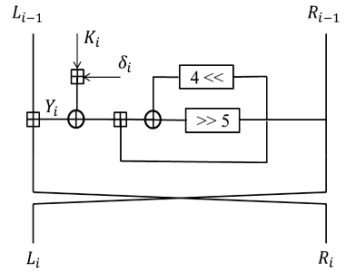

Figure 3. Round function of XTEA

Observation 3. Suppose that $X, Y \in \{0,1\}^{32}$and "$C\{i+1\}$" is the carry bit generated by the i^{th} bit of $Z = X \boxplus Y$.
If $X_i = Y_i$, then $C\{i+1\} = X_i = Y_i$.

Proof. $\begin{cases} X_i = Y_i = 1 \Rightarrow X_i + Y_i + C\{i\} > 1 \Rightarrow C\{i+1\} = 1 \\ X_i = Y_i = 0 \Rightarrow X_i + Y_i + C\{i\} < 2 \Rightarrow C\{i+1\} = 0 \end{cases}$

D. 15-round impossible differential characteristic

Based on observation 2, we have found two new 15-round differential characteristics for TEA and XTEA given by

$$D[31] \parallel O_{32} \nrightarrow_{15} O_{32} \parallel D[32]$$
$$D[32] \parallel O_{32} \nrightarrow_{15} O_{32} \parallel D[31]$$

The first impossible differential characteristic is depicted in Fig .4. We use both of the mentioned characteristics simultaneously to decrease sufficient data for our attacks.

Our first attempt at analyzing TEA and XTEA is motivated by combining two above-mentioned characteristics. The obtained 15-round impossible differential characteristic is:

$$x \parallel O_{62} \nrightarrow_{15} O_{32} \parallel y \parallel O_{30}$$

Where x and y are chosen from the following set:

$$\{(x,y)\} = \{(01,11),(01,10),(11,01),(10,01)\}$$

III. IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS OF TEA

In this section, we present the 19-round impossible differential cryptanalysis of TEA, using the first impossible differential characteristic introduced in section 2. A similar attack can be mounted for the second characteristic, simultaneously.

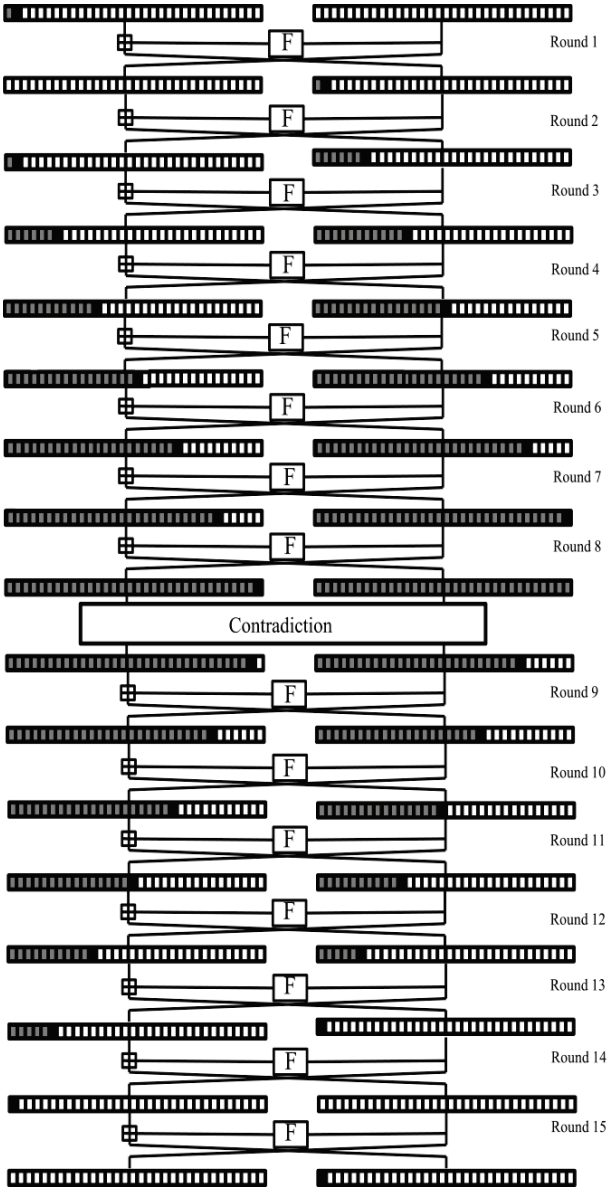

Figure 4. 15-Round impossible differential characteristic

Collecting data. We consider 2^n structures and every structure consists of $\frac{2^{19} \cdot 2^{17}}{2} = 2^{35}$ pairs. Note that for each pair (P, P') in a structure we have the following conditions.

$$LSB_{20}(L_0) = LSB_{20}(L'_0)$$
$$LSB_{25}(R_0) = LSB_{25}(R'_0)$$

TABLE III. SIEVING INAPPROPRIATE PAIRS OF TEA

Step	Round	Guessed Subkeys	Time Complexity (En)	Pairs Remained	Condition
1	1	K_0, K_2	$\frac{1}{19}\cdot 2\cdot 2^{n-13}\cdot 2^{63}=\frac{1}{19}\cdot 2^{n+51}$	2^{n-23}	$\Delta R_1 = D[31]$
2	19	–	$\frac{1}{19}\cdot 2\cdot 2^{n-23}\cdot 2^{63}=\frac{1}{19}\cdot 2^{n+41}$	2^{n-33}	$\Delta L_{18} = D[31]$
3	2 , 18	K_1, K_3	$\frac{1}{19}\cdot 2\cdot 2^{n-33}\cdot 2^{63}\cdot\frac{1}{32}\left[\sum_{i=1}^{26}2^{2i}+2^{54}+2^{54}\cdot\frac{1}{2}+2.\sum_{i=28}^{31}\left(2^{2i}\cdot\frac{1}{2^{2i-55}}+2^{2i}\cdot\frac{1}{2^{2i-54}}\right)\right.$ $\left.+2\cdot 2^{63}\cdot\frac{1}{2^9}+2\cdot 2^{63}\cdot\frac{1}{2^{10}}\right]=\frac{1}{19}\cdot 2^{n-33}\cdot 2^{63}\cdot 30\cdot\frac{1}{32}\cdot 2^{54}=\frac{30}{19}\cdot 2^{n+79}$	2^{n-44}	$\Delta R_1 = O_{32}$ $\Delta L_{18} = O_{32}$

Sieving inappropriate pairs. Given a pair, if its corresponding ciphertext does not have appropriate difference (see Fig. 5), the pair is sieved. The number of remained pairs is therefore given by $2^{n+35}\cdot 2^{-49}=2^{n-14}$.

As mentioned earlier, we consider both impossible differential characteristics; therefore, the number of remaining pairs is equal to $2^{n-14}\cdot 2=2^{n-13}$ pairs.

Since the effective key of TEA is 126 bits, as described in observation 1, we guess 2^{63} keys at step 1 as well as step 2 and 2^{63}keys at step 3. In step 1, we obtain R_1 and R_1'. A pair is remained if and only if $\Delta R_1 = D[31]$. Otherwise, we discard the pair. The time complexity of this step is given by $\frac{1}{19}\cdot 2\cdot 2^{n-13}\cdot 2^{63}=\frac{1}{19}\cdot 2^{n+51}En$. The probability that a pair is appropriate is equal to 2^{-10}; therefore, there will remain $2^{n-13}\cdot 2^{-10}=2^{n-23}$ pairs.

Similarly, other steps are performed to obtain remaining pairs, leading to recognizing wrong keys. The results are illustrated in Table III. Note that in order to reduce the time complexity, we utilize the early abort method.

Recovering the key. In order to find the correct key, we discard all wrong keys. Concerning each key, if at least one pair remains, the key will be discarded. The remaining keys are verified to find the correct key.

By substituting $n = 44.6$ and considering the ability of combining two impossible differential characteristics, the time complexity of sieving wrong pairs and finding correct key from the remaining candidates will be $2^{124.26}En$ and $2^{126}\cdot(1-2^{-11})^{2^{11.6}}=2^{123.81}En$, respectively. The data complexity of the attack is equal to $2^{n+19}=2^{63.6}$ chosen plaintexts and the required memory to save the sieved pairs is $2^{n-13}\cdot 2\cdot 128/8 = 2^{36.6}$ bytes.

IV. IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS OF XTEA

We utilize the new 15-round impossible differential characteristic to apply 25-round impossible differential cryptanalysis on XTEA. Similar to the previous attack, we only discuss the attack which uses the first impossible differential cryptanalysis while the complexities are calculated based on the combined characteristics. The attack is mounted within rounds of 17 to 41. Fig.5 represents the 25-round impossible differential cryptanalysis.

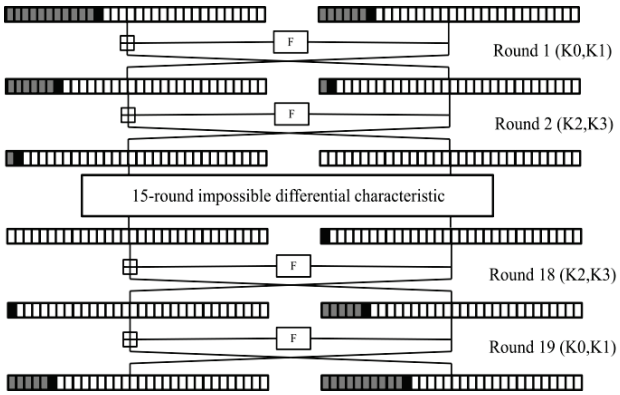

Figure 5. Impossible differential attack on TEA

Collecting data. All pairs which have identical LSB_{10} in right-hand subblock and identical LSB_5 in left-hand subblock make up a structure. The number of pairs in each structure can be found by inspection as $2^{49}\cdot 2^{47}/2 = 2^{95}$pairs. We need 2^n structures; Thus the total number of necessary pairs will be 2^{n+95} pairs.

Sieving inappropriate pairs. We discard the pairs that do not satisfy the constraints of ciphertext in a manner similar to that used in TEA described above (see Fig. 6). The number of remained pairs is equal to $2^{n+95}\cdot 2^{-19}=2^{n+76}$ and considering the combined impossible differential characteristic, we will have $2^{n+76}\cdot 2=2^{n+77}$ pairs.

Next, we guess the corresponding subkeys of each round and sieve inappropriate pairs. Table IV shows the details of sieving wrong pairs.

TABLE IV. SIEVING INAPPROPRIATE PAIRS OF XTEA

Step	Round	Guessed subkeys	Time Complexity (En)	Pairs Remained	Condition
1	17	K_0	$\frac{1}{25}\cdot 2\cdot 2^{n+77}\cdot 2^{32}=\frac{1}{25}\cdot 2^{n+110}$	2^{n+67}	$\Delta R_{17}=D[16]$
2	18	–	$\frac{1}{25}\cdot 2\cdot 2^{n+67}\cdot 2^{32}=\frac{1}{25}\cdot 2^{n+100}$	2^{n+57}	$\Delta R_{18}=D[21]$
3	41	–	$\frac{1}{25}\cdot 2\cdot 2^{n+57}\cdot 2^{32}=\frac{1}{25}\cdot 2^{n+90}$	2^{n+47}	$\Delta L_{40}=D[17]$
4	40	–	$\frac{1}{25}\cdot 2\cdot 2^{n+47}\cdot 2^{32}=\frac{1}{25}\cdot 2^{n+80}$	2^{n+37}	$\Delta L_{39}=D[22]$
5	19	K_1	$\frac{1}{25}\cdot 2\cdot 2^{n+37}\cdot 2^{64}=\frac{1}{25}\cdot 2^{n+102}$	2^{n+27}	$\Delta R_{19}=D[26]$
6	20	–	$\frac{1}{25}\cdot 2\cdot 2^{n+27}\cdot 2^{64}=\frac{1}{25}\cdot 2^{n+92}$	2^{n+17}	$\Delta R_{20}=D[31]$
7	39	K_3	$\frac{1}{25}\cdot 2^{n+17}\cdot 2^{64}\cdot\frac{1}{32}\left[\sum_{i=1}^{17}2^i+2.\sum_{i=18}^{27}(2^i\cdot\frac{1}{2^{i-17}})+\sum_{i=28}^{32}2^{i-10}\right]=\frac{74}{25}\cdot 2^{n+94}$	2^{n+7}	$\Delta L_{37}=D[32]$
8	38	–	$\frac{1}{25}\cdot 2\cdot 2^{n+7}\cdot 2^{96}=\frac{1}{25}\cdot 2^{n+104}$	2^{n-3}	$\Delta L_{38}=D[27]$
9	21, 37	K_2	$2^{n+109.3}$	2^{n-14}	$\Delta R_{21}=O_{32}$, $\Delta L_{36}=O_{32}$

Note that in step 7, we use bitwise early abort to reduce the time complexity. In step 9, in order to consider all the keys for the remained pairs, we first guess $K_2\{25\}$ to $K_2\{32\}$. Then, we take into account the keys which meet the condition $\delta_{21}\{24\}=K_2\{24\}$. For these keys, as discussed in observation 3, we can determine the carry $c\{25\}$ which is added to 25^{th}bit of $K_2 \boxplus \delta_{21}$, which yields $Y_{21}\{25\}$ where Y_i stands for the output of round function at round i. If the condition $L_{20}\{25\}=Y_{21}\{25\}$ is met, as described in observation 3, we can obtain the carry $c\{26\}$ which is added to 26^{th} bit of $Y_{21}\boxplus L_{20}$; therefore, R_{21} and R'_{21} are obtained. If the two conditions stated above do not hold, we perform the analogous manner mentioned above for the 23^{th} bit, and that we continue till the last bit. For those keys and pairs that the above conditions do not simultaneously hold for any of the 24 bits, we guess whole 32 bits of the subkey K_2 and do the rest of calculations like step 7. Likewise, we adopt the procedure above on round 37.

Recovering the key. Considering each key, if at least one pair remains, the key will be discarded. Those keys which are not discarded will be verified in order to find the correct one.

By selecting $n=14.6$, the time complexity for discarding wrong keys and finding the correct key from rest of the keys is $2^{123.9}En$ and $2^{128}\cdot(1-2^{-11})^{2^{11.6}}=2^{125.81}En$, respectively. The required data will be $2^{63.6}$chosen plaintexts and $2^{n+77}\cdot 2\cdot 128/8=2^{96.6}$ bytes of memory are needed.

V. CONCLUSIONS

In this paper, we have presented two impossible differential attacks based on the longest known impossible differential characteristics of both TEA and XTEA. While the previous impossible differential attacks were only mountable up to

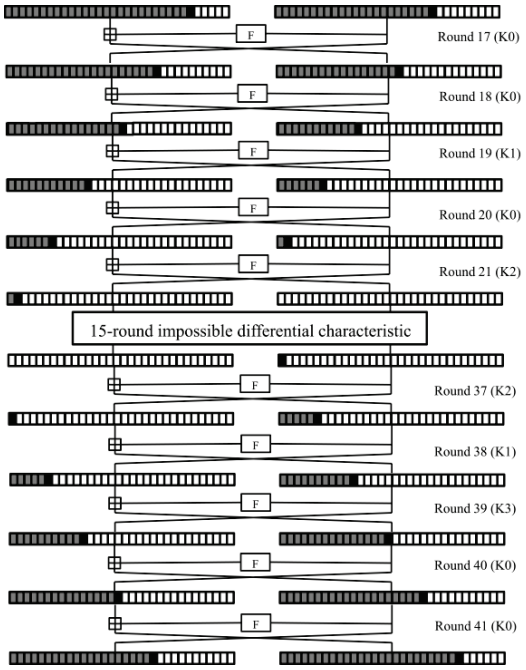

Figure 6. Impossible differential attack on XTEA

17 rounds of TEA and 23 rounds of XTEA, we presented two impossible differential attacks mounting on 19 rounds of TEA and 25 rounds of XTEA. We could recover the key of TEA using $2^{63.6}$ chosen plaintexts and $2^{125.05}$ encryptions. Moreover, we recovered the key of XTEA by using $2^{63.6}$ chosen plaintexts and $2^{126.15}$ encryptions.

REFERENCES

[1] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. JB Robshaw, Y. Seurin, and Ch. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher", Springer Berlin Heidelberg, 2007.

[2] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, "The 128-bit blockcipher CLEFIA." In Fast software encryption, pp. 181-195. Springer Berlin Heidelberg, 2007.

[3] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: an ultra-lightweight blockcipher, "In Cryptographic Hardware and Embedded Systems–CHES 2011, pp. 342-357. Springer Berlin Heidelberg, 2011.

[4] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. S. Koo, C. Lee et al. "HIGHT: a new block cipher suitable for low-resource device." In Cryptographic Hardware and Embedded Systems-CHES 2006, pp. 46-59. Springer Berlin Heidelberg, 2006.

[5] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw. "The LED block cipher." In *Cryptographic Hardware and Embedded Systems–CHES 2011*, pp. 326-341. Springer Berlin Heidelberg, 2011.

[6] H. Mala, M. Dakhilalian, and M. Shakiba. "Impossible differential attacks on 13-round CLEFIA-128." *Journal of Computer Science and Technology* 26, no. 4 (2011): 744-750.

[7] W. Wang, and X. Wang. "Improved Impossible Differential Cryptanalysis of CLEFIA." *IACR Cryptology ePrint Archive* 2007 (2007): 466.

[8] S. A. Azimi, Z. Ahmadian, J. Mohajeri, and M. R. Aref. "Impossible differential cryptanalysis of Piccolo lightweight block cipher." In *Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on*, pp. 89-94. IEEE, 2014

[9] M. Minier, "On the Security of Piccolo Lightweight Block Cipher against Related-Key Impossible Differentials." In *Progress in Cryptology–INDOCRYPT 2013*, pp. 308-318. Springer International Publishing, 2013.

[10] J. Chen, W. Meiqin, and B. Preneel. "Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT." In *Progress in Cryptology-AFRICACRYPT 2012*, pp. 117-137. Springer Berlin Heidelberg, 2012.

[11] O. Özen, V. Kerem, T. Cihangir, and K. Çelebi. "Lightweight block ciphers revisited: Cryptanalysis of reduced round PRESENT and HIGHT." In *Information security and privacy*, pp. 90-107. Springer Berlin Heidelberg, 2009.

[12] D. J. Wheeler, and R. M. Needham. "TEA, a tiny encryption algorithm." In *Fast Software Encryption*, pp. 363-366. Springer Berlin Heidelberg, 1995.

[13] D. J. Wheeler, and R. M. Needham. "Correction to xtea." *Unpublished manuscript, Computer Laboratory, Cambridge University, England* (1998).

[14] D. Moon, K. Hwang, W. Lee, S. Lee, and J. Lim. "Impossible differential cryptanalysis of reduced round XTEA and TEA" .*In Fast Software Encryption*, pp. 49-60. Springer Berlin Heidelberg, 2002.

[15] K. John, B. Schneier, and D. Wagner. "Key-schedule cryptanalysis of idea, g-des, gost, safer, and triple-des." In *Advances in Cryptology—CRYPTO'96*, pp. 237-251. Springer Berlin Heidelberg, 1996.

[16] A. Bogdanov, and M. Wang. "Zero correlation linear cryptanalysis with reduced data complexity." In *Fast Software Encryption*, pp. 29-48. Springer Berlin Heidelberg, 2012.

[17] S. Hong, D. Hong, Y. Ko, D. Chang, W. Lee, and S. Lee. "Differential Cryptanalysis of TEA and XTEA." In *Information Security and Cryptology-ICISC 2003*, pp. 402-417. Springer Berlin Heidelberg, 2004.

[18] G. Sekar, N. Mouha, V. Velichkov, and B. Preneel. "Meet-in-the-middle attacks on reduced-round XTEA." In *Topics in Cryptology–CT-RSA 2011*, pp. 250-267. Springer Berlin Heidelberg, 2011.