Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA

Dukjae Moon, Kyungdeok Hwang, Wonil Lee, Sangjin Lee, and Jongin Lim

Center for Information and Security Technologies(CIST),
Korea University, Anam Dong, Sungbuk Gu,
Seoul, KOREA
{djmoon, kdhwang, wonil, sangjin, jilim}@cist.korea.ac.kr

Abstract. We present the impossible differential cryptanalysis of the block cipher XTEA[7] and TEA[6]. The core of the design principle of these block ciphers is an easy implementation and a simplicity. But this simplicity dose not offer a large diffusion property. Our impossible differential cryptanalysis of reduced-round versions of XTEA and TEA is based on this fact. We will show how to construct a 12-round impossible characteristic of XTEA. We can then derive 128-bit user key of the 14-round XTEA with $2^{62.5}$ chosen plaintexts and 2^{85} encryption times using the 12-round impossible characteristic. In addition, we will show how to construct a 10-round impossible characteristic of TEA. Then we can derive 128-bit user key of the 11-round TEA with $2^{52.5}$ chosen plaintexts and 2^{84} encryption times using the 10-round impossible characteristic.

1 Introduction

In 1990, E. Biham and A. Shamir proposed the differential cryptanalysis[1]. Later, it was regarded as a very useful method in attacking the known block ciphers. For these reasons, block ciphers have been designed to be secure against the differential cryptanalysis since the middle of 1990's. The differential cryptanalysis has also been advanced variously - truncated differential cryptanalysis[4], higher order differential cryptanalysis[5], impossible differential cryptanalysis[3], and so on.

In 1998, the impossible differential cryptanalysis[3] was proposed by E. Biham *et al.* This cryptanalysis is a chosen plaintext attack and applied to the reduced 31 rounds of Skipjack. The traditional differential cryptanalysis finds a key using the differential characteristic with high probability. But the impossible differential cryptanalysis uses the differential characteristic with probability zero. The general impossible differential cryptanalysis can be briefly described as follows: First of all, we must find an impossible differential characteristic. We then choose any plaintext pairs with the input difference of the impossible differential characteristic, and obtain the corresponding ciphertext pairs. We eliminate the ciphertext pairs which are not satisfied with a special property derived from the impossible differential characteristic. For each key value in the key space of the last one or two rounds, we decrypt the ciphertext pairs with that key value and if the differences of the decrypted ciphertext pairs satisfy the output difference of the impossible differential characteristic, then we eliminate the key value from the key space. We repeat the above process until the only one key value remains with very high probability.

In this paper, we describe an impossible differential cryptanalysis of 14-round XTEA. It is based on a 12-round impossible differential characteristic. We will be able to find the 128-bit user key of 14-round XTEA with $2^{62.5}$ chosen plaintexts and 2^{85} encryption times. In addition, we present an impossible differential cryptanalysis of 11-round TEA. To find the 128-bit user key of 11-round TEA, this cryptanalysis uses a 10-round impossible differential characteristic and requires $2^{52.5}$ chosen plaintexts and 2^{84} encryption times.

The paper is organized as follows: In Section 2, we introduce notation. The description of algorithms of TEA and XTEA is briefly given in Section 3. In Section 4, we explain how to construct a 12-round impossible differential characteristic of XTEA and a 10-round impossible differential characteristic of TEA. In Section 5, we describe our attack on 14-round XTEA and 11-round TEA. Finally, we summarize our results and conclude this paper.

2 Notation

We introduce notation as follows for some binary operations.

Exclusive-OR :
The operation of addition of n-tuples over the field $\mathbb{F}_2$ (also known as exlusive-or) is denoted by $x \oplus y$.

Integer Addition :
The addition operation of integers under modulo 2^n is denoted by $x \boxplus y$ (where $x\ ,\ y \in \mathbb{Z}_{2^n}$). The value of n will be clear from the context.

Bitwise Shifts :
The logical left shift of x by y bits is denoted by $x \ll y$. The logical right shift of x by y bits is denoted by $x \gg y$.

3 Description of TEA and XTEA

TEA(Tiny Encryption Algorithm)[6] was presented by David J. Wheeler *et al.* TEA was designed for a short program which would run on most machines and encrypt safely. This cipher used a simple key schedule. But because of the simple key schedule, the related key attack[8] was possible. To repair this weakness, designers of TEA proposed XTEA(TEA Extensions)[7] which evolved from TEA.

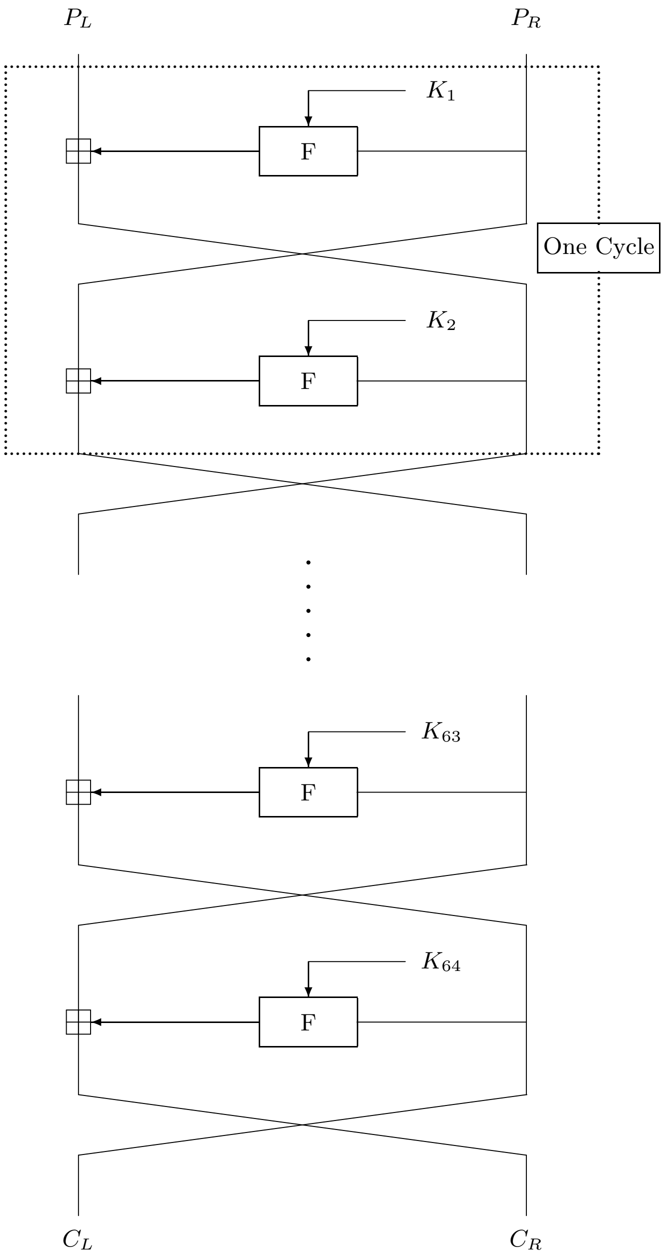

Fig. 1. The structure of TEA/XTEA

3.1 The Tiny Encryption Algorithm (TEA)

TEA is a 64-bit iterated block cipher with 64 rounds, as shown in Fig. 1. TEA can be represented as 32 cycles in which one cycle is two rounds. The round function F consists of the key addition, bitwise XOR and left and right shift operation. We can describe the output (Y_{i+1}, Z_{i+1}) of the i-th cycle of TEA with the input (Y_i, Z_i) as follows (See Fig. 2):

$$\begin{aligned} Y_{i+1} &= Y_i \boxplus F(Z_i, K[0,1], \delta_i), \\ Z_{i+1} &= Z_i \boxplus F(Y_{i+1}, K[2,3], \delta_i), \\ \delta_i &= \lfloor \frac{i+1}{2} \rfloor \cdot \delta, \end{aligned}$$

where the round function F is defined by

$$F(X, K[j,k], \delta_i) = ((X \ll 4) \boxplus K[j]) \oplus (X \boxplus \delta_i) \oplus ((X \gg 5) \boxplus K[k]).$$

The constant $\delta = 9E3779B9_h$ is derived from the golden number, where 'h' represents the hexadecimal number, e.g., $10_h = 16$.

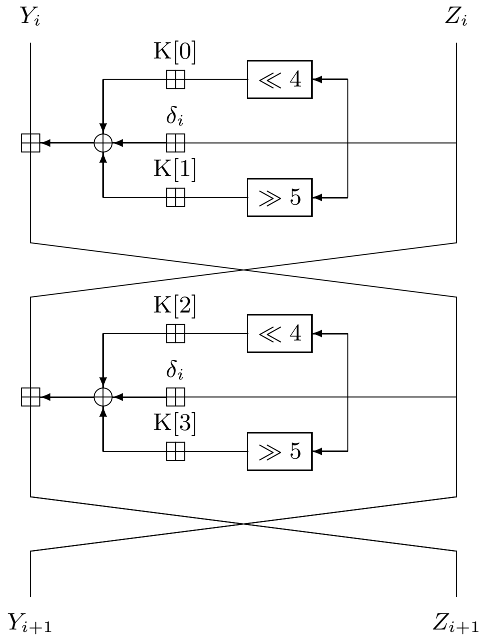

Fig. 2. The i-th cycle of TEA

The key schedule algorithm is very simple. The 128-bit user key K is split into four 32-bit blocks $K = (K[0], K[1], K[2], K[3])$. Then the round keys K_r

are as follows:

$$K_r = \begin{cases} (K[0], K[1]) & \text{if } r \text{ is odd} \\ (K[2], K[3]) & \text{if } r \text{ is even,} \end{cases}$$

where $r = 1, \cdots, 64$.

3.2 The TEA Extensions (XTEA)

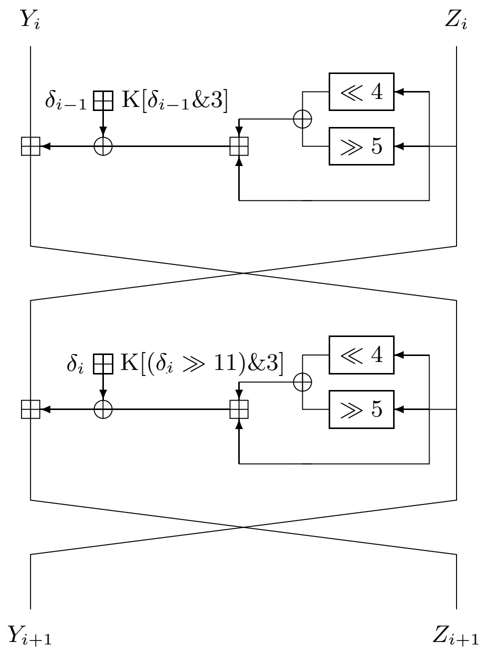

Fig. 3. The i-th cycle of XTEA

XTEA[7] is an evolutionary improvement of TEA. XTEA makes essentially use of arithmetic and logic operations like TEA. New features of XTEA are to use two bits of δ_i and the shift of 11 . This adjustments cause the indexes of round keys to be irregular. We can describe the output (Y_{i+1}, Z_{i+1}) of the i-th cycle of XTEA with the input (Y_i, Z_i) as follows (See Fig.3):

$$\begin{aligned} Y_{i+1} &= Y_i \boxplus F(Z_i, K_{2i-1}, \delta_{i-1}), \\ Z_{i+1} &= Z_i \boxplus F(Y_{i+1}, K_{2i}, \delta_i), \\ \delta_i &= \lfloor \frac{i+1}{2} \rfloor \cdot \delta, \end{aligned}$$

where the round function F is defined by

$$F(X, K_*, \delta_{**}) = ((X \ll 4) \oplus (X \gg 5)) \boxplus X \oplus \delta_{**} \boxplus K_*.$$

The constant $\delta = 9E3779B9_h$ is derived from the golden number.

To generate the round keys, first the 128-bit key K is split into four 32-bit blocks $K = (K[0], K[1], K[2], K[3])$, and then the round keys K_r are determined by

$$K_r = \begin{cases} K[\delta_{\frac{r-1}{2}} \ \&\ 3] & \text{if } r \text{ is odd} \\ K[(\delta_{\frac{r}{2}} \gg 11) \ \&\ 3] & \text{if } r \text{ is even,} \end{cases}$$

where $r = 1, \cdots, 64$.

4 Impossible differential characteristics

We found a 12-round impossible differential characteristic of XTEA, and a 10-round impossible differential characteristic of TEA. The round functions of XTEA and TEA use the addition as a nonlinear part that is due to the carry which only propagates upwards(diffusion in only one direction). Therefore, we will construct impossible differential characteristics in consideration of this fact and the structure of XTEA and TEA. For this work, we use notation as follows: an α_i is used to denote an arbitrary bit, where i is a positive integer and α is any small letter. And we denote by Λ_x an arbitrary 4-bit , where Λ is any capital letter.

4.1 A 12-round impossible differential characteristic of XTEA

In this subsection, we show how to construct a 12-round impossible differential characteristic of XTEA. As shown in Fig. 4 of Appendix, if the form of an input difference is

$$(A_x\ a_1a_210\ 0_x0_x0_x0_x0_x0_x \parallel b_1000\ 0_x0_x0_x0_x0_x0_x0_x), \tag{1}$$

then the difference after round 6 must be of the form

$$(N_xO_xP_xQ_xR_xS_x\ f_1f_210\ 0_x \parallel T_xU_xV_xW_xX_xY_xZ_x\ g_1g_2g_31). \tag{2}$$

On the other hand, we can predict the difference after round 6 from the output difference of round 12, i.e., to consider the differentials in the backward direction. Similarly to the 6-round differential characteristic with peobability 1, there is a backward 6-round differential characteristic with probability 1. It has the difference

$$(a_1000\ 0_x0_x0_x0_x0_x0_x0_x \parallel A_x\ b_1b_210\ 0_x0_x0_x0_x0_x0_x) \tag{3}$$

after round 12, and then it is clear that the difference after round 6 must be of the form

$$(T_xU_xV_xW_xX_xY_xZ_x\ g_1g_2g_31 \parallel N_xO_xP_xQ_xR_xS_x\ f_1f_210\ 0_x). \qquad (4)$$

Combining these two differential characteristics, we conclude that any pair with input difference (1) before round 1 and output difference (3) after round 12 must have differences of the form (2) = (4) after round 6. But this event never occurs. Therefore, this characteristic is a 12-round impossible characteristic of XTEA.

4.2 A 10-round impossible differential characteristic of TEA

Similarly, if the form of an input difference is $(A_xB_x\ a_1a_2a_31\ 0_x0_x0_x0_x0_x \parallel C_x\ b_1b_200\ 0_x0_x0_x0_x0_x0_x)$, then the difference after round 10 cannot be of the form $(A_x\ a_1a_200\ 0_x0_x0_x0_x0_x0_x \parallel B_xC_x\ b_1b_2b_31\ 0_x0_x0_x0_x0_x)$. See Fig.5 of Appendix for a detailed depiction of the 10-round impossible differential characteristic of TEA.

5 Impossible Differential Cryptanalysis

In this section, we will analyze 14-round XTEA and 11-round TEA using the impossible differential characteristics above. Our cryptanalysis of the 14-round XTEA uses a 2R-attack with the 12-round impossible differential characteristic (Fig. 4). And our crypanalysis of the 11-round TEA uses a 1R-attack with the 10-round impossible differential characteristic (Fig. 5).

5.1 Cryptanalysis of 14-round XTEA

We present an impossible differential cryptanalysis of the 14-round XTEA using the 12-round impossible differential characteristic (Fig. 4). We use structures of 2^7 plaintexts, where every differences of this plaintext pairs matches the difference of the form

$$(A_x\ a_1a_210\ 0_x0_x0_x0_x0_x0_H \parallel b_1000\ 0_x0_x0_x0_x0_x0_x0_x). \qquad (5)$$

Such structures propose about 2^{13} pairs of plaintexts. Given such $2^{55.5}$ structures ($2^{62.5}$ plaintexts , $2^{68.5}$ pairs), we collect the pairs whose ciphertext differences match the difference of the form

$$(A_xB_x\ a_1a_2a_31\ 0_x0_x0_x0_x0_x \parallel C_xD_xE_xF_x\ 1000\ 0_x0_x0_x). \qquad (6)$$

Then, the probability that a plaintext pair satisfies this condition is $(2^{-4})^9 \times (2^{-1}) \simeq 2^{-37}$. Thus only about $2^{31.5}$ pairs remain. For each of the remained pairs, we eliminate wrong key pairs of the 2^{64} possible values of the key space of the last two rounds by examining whether the decrypted values of the last two rounds have the output difference of the 12-round impossible differential characteristic. The probability that a key pair in the key space survives the test when each ciphertext pair is decrypted is $(1-2^{-26})(1-2^{-31})$. So, there remain only about $2^{64} \times \{(1-2^{-26})(1-2^{-31})\}^{2^{31.5}} < 2^{-3.4}$ wrong key pair of the last two rounds after analyzing $2^{31.5}$ pairs. It is thus expected that only one key pair (K_{13}, K_{14}) remains, and this pair must be the correct round key pair. This attack can be summarized as follows;

Goal : Finding round key pair (K_{13}, K_{14}).

1. Choose $2^{68.5}$ plaintext pairs from the $2^{55.5}$ structures, which the difference of each plaintext pair satisfies the difference (5). And ask for the corresponding ciphertext pairs.

2. Collect plaintext pairs whose ciphertext difference agrees with the difference (6).

3. Select a plaintext pair in the collected pairs which are derived from the process **2**.

4. For each key pair (K_{13}, K_{14}) in the key space,
   (a) Decrypt the corresponding ciphertext pair up to the position of 12-round output.
   (b) Compute the difference of the decrypted pair in (a).
   (c) Compare the result of (b) to the output difference of the 12-round impossible differential characteristic. If the two results are the same, then remove the selected key pair from the key space.

5. If $\mid K_{13} \mid \leq \varepsilon$ and $\mid K_{14} \mid \leq \varepsilon'$, stop. Otherwise, go to the process **3**. (ε and ε' are small integers.)

The required work of this attack is about $2^{85} \simeq 2^{64} \cdot 2^{-5} + 2^{64}\{(1-2^{-26})(1-2^{-31})\} \cdot 2^{-5} + \cdots + 2^{64}\{(1-2^{-26})(1-2^{-31})\}^{(2^{31.5}-1)} \cdot 2^{-5}$ encryptions where 2^{-5} means two round operations of XTEA encryption. Hence, we can find 64 bits of the user key with our method. The remaining 64 bits will be found by exhaustive search.

5.2 Cryptanalysis of 11-round TEA

We can also find 128-bit user key of 11-round TEA similarly with the above method. We use the 10-round impossible differential characteristic (Fig. 5). We obtain structures of 2^{17} plaintexts, where every differences of this plaintexts matches the input difference of the form

$$(A_x B_x \ a_1 a_2 a_3 1 \ 0_x 0_x 0_x 0_x 0_x \parallel C_x \ b_1 b_2 00 \ 0_x 0_x 0_x 0_x 0_x 0_x) \tag{7}$$

and collect the pairs whose ciphertext differences match the difference of the form

$$(A_x B_x \ a_1 a_2 a_3 1 \ 0_x 0_x 0_x 0_x 0_x \parallel C_x D_x E_x F_x \ 1000 \ 0_x 0_x 0_x). \tag{8}$$

Then, the probability that any plaintext pair satisfies the difference (8) is $(2^{-4})^9 \times (2^{-1}) \simeq 2^{-37}$, and the probability that a key is eliminated from the key space when each ciphertext pair is decrypted is 2^{-26}. Let the number of the pairs required to find one correct key be N, then the number N is about $2^{31.5}$ such that $2^{64} \times (1 - 2^{-26})^N < 1$. Therefore, the required number of chosen plaintext pairs is $2^{37} \times 2^{31.5} = 2^{68.5}$. Since we can collect 2^{33} pairs from one structure, we need $2^{35.5}$ structures. It follows that the attack requires $2^{35.5} \times 2^{17} = 2^{52.5}$ chosen plaintexts. We can get 64 bits of K_{11}. This attack can be summarized as follows;

Goal : Finding 11 round key.

1. Choose $2^{68.5}$ plaintext pairs from the $2^{35.5}$ structures, which the difference of each plaintext pair satisfies the difference (7). And ask for the corresponding ciphertext pairs.

2. Collect plaintext pairs whose ciphertext difference agrees with the difference (8).

3. Select a plaintext pair in the collected pairs which are derived from the process **2**.

4. For each key $K_{11}(= K[0],\ K[1])$ in the key space,
   (a) Decrypt the corresponding ciphertext pair up to the position of 10-round output.
   (b) Compute the difference of the decrypted pair in (a).
   (c) Compare the result of (b) to the output difference of the 10-round impossible differential characteristic. If the two results are the same, then remove the selected key from the key space.

5. If $\mid K_{11} \mid \leq \varepsilon$, stop. Otherwise, go to the process **3**. (ε is small integer.)

The required work of this attack is about $2^{84} \simeq 2^{64} \cdot 2^{-6} + 2^{64}(1-2^{-26}) \cdot 2^{-6} + \cdots + 2^{64}(1-2^{-26})^{2^{31.5}-1} \cdot 2^{-6}$ encryptions where 2^{-6} means one round operation of TEA encryption. Hence, we can find 64 bits of the user key with our method. The remaining 64 bits will be found by exhaustive search.

6 Conclusion

We described the algorithms of XTEA and TEA, and found the 12-round impossible differential characteristic of XTEA and the 10-round impossible differential characteristic of TEA. Using the 12-round impossible differential characteristic we attacked the 14-round XTEA with $2^{62.5}$ chosen plaintexts and 2^{85} encryptions. In TEA, using the 10-round impossible differential we attacked the 11-round with $2^{52.5}$ chosen plaintexts and 2^{84} encryptions.

TEA is designed for software implementation and XTEA is evolved from TEA to remove the simplicity of key schedule. However, XTEA is weaker than

TEA in the impossible differential cryptanalysis although the former is stronger than the latter in the related attack[2].

Acknowledgment

We would like to thank Seokhie Hong and Jaechul Sung for many helpful discussions.

References

1. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like cryptosystems*, Advances in Cryptology – CRYPTO'90, LNCS 537, Springer-Verlag,1991, pp.2–21.
2. E. Biham,*New Types of Cryptanalytic Attacks Using Related Keys*, Advances in Cryptology – EUROCRYT'93, Springer-Verlag,1994, pp.398–409.
3. E. Biham, A. Biryukov and A. Shamir, *Cryptanalysis of skipjack reduced to 31 round using impossible differentiala*, Advances in Cryptology – EUROCRYT'99, LNCS 1592, Springer-Verlag,1999, pp.12–23. Available at http://www.cs.technion.ac.il/ biham/Reports/Skipjack/.
4. L. R. Knudsen, *Truncated and Higher Order Differential*, Fast Software Encrytion Workshop 94, LNCS 1008, Springer-Verlag, 1995, pp.229–236.
5. S. Moriai, T. Shimoyama and T. Kaneko, *Higher Order Differential Attack of a CAST cipher*,Fast Software Encrytion Workshop 98, LNCS 1372, Springer-Verlag, 1998, pp.17–31.
6. D. Wheeler and R. Needham, *TEA, a Tiny Encryption Algorithm*, Fast Software Encryption, Second International Workshop Proceedings, Springer-Verlag, 1995, pp. 97-110.
7. D. Wheeler and R. Needham, *TEA Extensions*, October 1997.
8. J. Kelsey, B. Schneier and D. Wagner,*Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA*, In Information and Communications Security-Proceedings of ICICS 1997, Lecture Notes in Computer Science 1334, Springer-Verlag, 1997.

Appendix

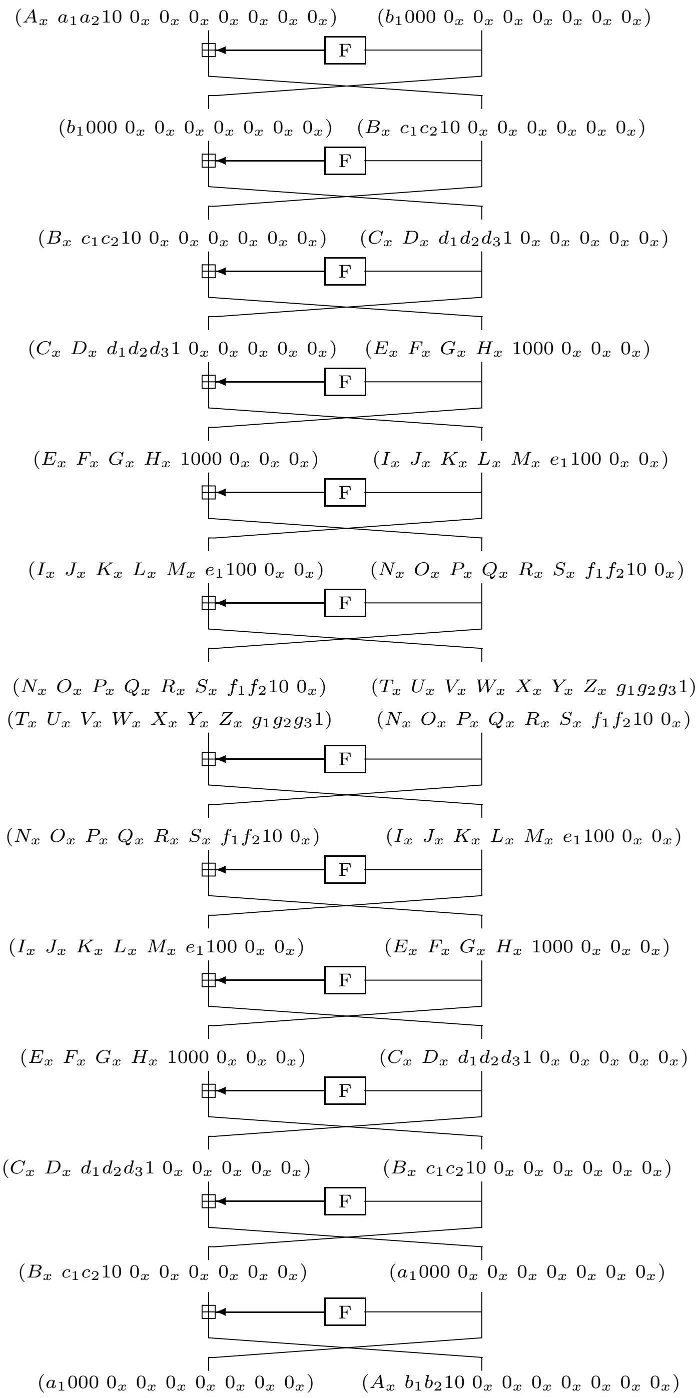

Fig. 4. 12-Round Impossible Differential Characteristic of XTEA

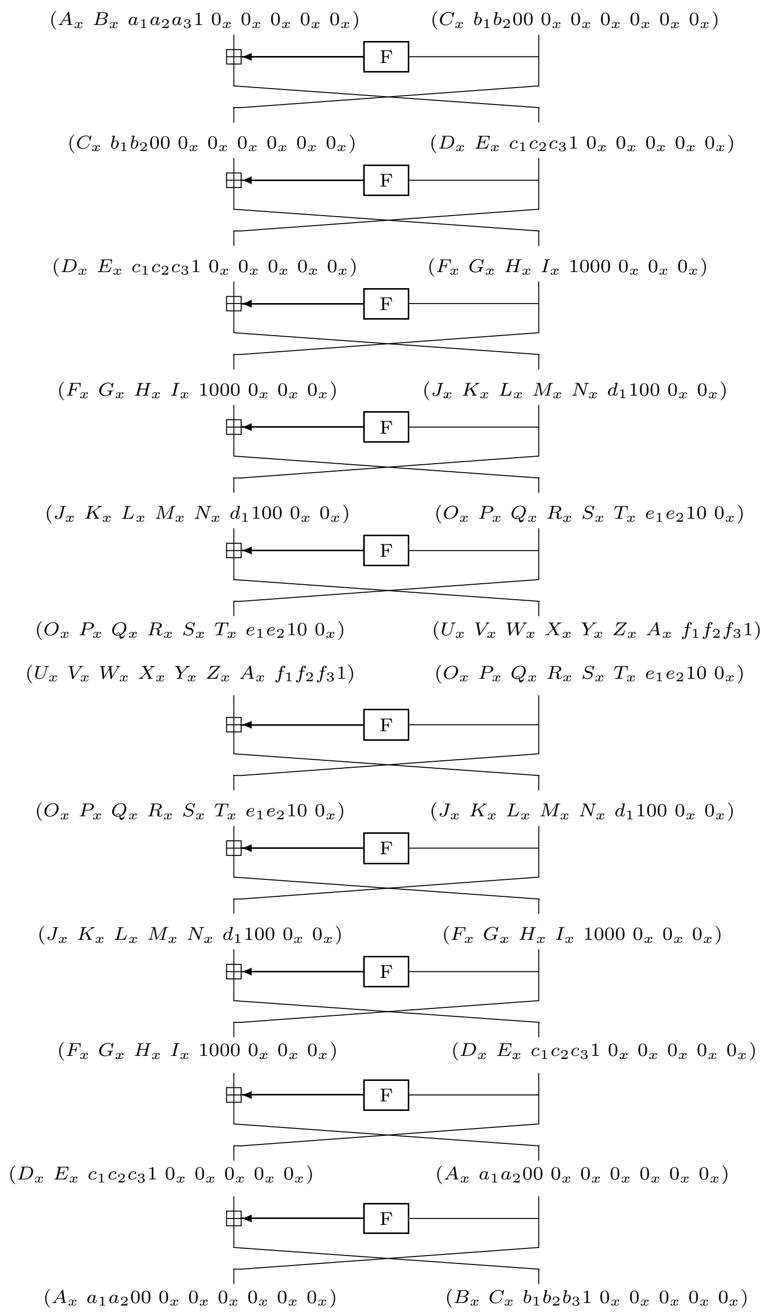

Fig. 5. 10-Round Impossible Differential Characteristic of TEA