Related Key Differential Attacks on 27 rounds of XTEA and Full-round GOST ⋆

Youngdai Ko[1], Seokhie Hong[1], Wonil Lee[1], Sangjin Lee[1], and Ju-Sung Kang[2]

[1] Center for Information Security Technologies (CIST),
Korea University, Anam Dong, Sungbuk Gu, Seoul, Korea
{koyd, hsh, wonil, sangjin}@cist.korea.ac.kr
[2] Section 0741, Information Security Technology Division, ETRI
161 Kajong-Dong, Yusong-Gu, Taejon, 305-350, Korea
{jskang}@etri.re.kr

Abstract. In this paper, we present a related key truncated differential attack on 27 rounds of XTEA which is the best known attack so far. With an expected success rate of 96.9%, we can attack 27 rounds of XTEA using $2^{20.5}$ chosen plaintexts and with a complexity of $2^{115.15}$ 27-round XTEA encryptions. We also propose several attacks on GOST. First, we present a distinguishing attack on full-round GOST, which can distinguish it from a random permutation with probability $1-2^{-64}$ using a related key differential characteristic. We also show that H. Seki et al.'s idea combined with our related key differential characteristic can be applied to attack 31 rounds of GOST . Lastly, we propose a related key differential attack on full-round GOST. In this attack, we can recover 12 bits of the master key with 2^{35} chosen plaintexts, 2^{36} encryption operations and an expected success rate of 91.7%.

Keywords : Related key differential attack, Distinguishing attack, XTEA, GOST, Differential characteristic.

1 Introduction

XTEA [10] was proposed as a modified version of TEA [7] by R. Needham and D. Wheeler in order to resist related key attacks [5]. XTEA is a very simple block cipher using only exclusive-or operations, additions, and shifts. Until now, the best known result on XTEA is a truncated differential attack on 23 rounds of XTEA (8∼30 or 30∼52) proposed in [3]. In this paper, we present related key truncated differential attacks on 25 (1∼25) and 27 (4∼30) rounds of XTEA.

GOST was proposed in the former Soviet Union [2]. It has a very simple round function and key schedule. GOST uses key addition modulo 2^{32} in each round function. So, the probability of a differential characteristic depends not only on the value of input-output differences but also on the value of the round key. In order to reduce the effect of the round key addition, H. Seki et al. introduced

⋆ This work is supported by the MOST research fund(M1-0326-08-0001).

a specific set of differential characteristics and proposed a differential attack on 13 rounds of GOST as well as a related key differential attack on 21 rounds of GOST [8].

Here, we present several attacks on GOST. First, we introduce a distinguishing attack on full-round GOST which can distinguish it from a random oracle with probability $1 - 2^{-64}$ using a related key differential characteristic. We also present a related key differential attack on 31 rounds of GOST using our related key differential characteristic combined with H. Seki et al.'s set of differential characteristics. Finally, we describe a related key differential attack on full-round GOST. In this attack, we can recover 12 bits of the master key with 2^{35} chosen plaintexts, 2^{36} encryption operations and an expected success rate of 91.7%.

Table. 1 and 2 depict recent results on XTEA and GOST, respectively.

Table 1. Various attacks on reduced-round XTEA

Attack method	paper	Rounds	# of Chosen Plaintexts	Total Complexity
Impossible Diff. attack	[6]	14	$2^{62.5}$	2^{85}
Diff. attack	[3]	15	2^{59}	2^{120}
Truncated Diff. attack	[3]	23	$2^{20.55}$	$2^{120.65}$
R·K Truncated Diff.	this paper	27	$2^{20.5}$	$2^{115.15}$

Table 2. Various attacks on GOST

Attack method	paper	Rounds	# of C·P	Total Complexity
R·K Diff. attack	[4]	24	theoretical	theoretical
A set of Diff. Char.	[8]	13	2^{51}	Not mentioned.
R·K Diff. attack	[8]	21	2^{56}	Not mentioned.
Distinguishing attack	this paper	full	2	2
R·K Diff. attack	this paper	31	2^{26}	2^{39}
R·K Diff. attack	this paper	full	2^{35}	2^{36}

The following is the outline of this paper. In Section 2, we present the notations used in this paper. In Section 3, we describe an 8-round related key truncated differential characteristic of XTEA and propose related key truncated differential attacks on 25 (1∼25) and 27 (4∼30) rounds of XTEA. In Section 4, we present a distinguishing attack and a related key differential attack on 31 rounds of GOST and full-round GOST. We conclude in Section 5.

2 Notations

Here, we describe several notations used in this paper. Let $\boxplus$, $\oplus$, $\cdot$, $\lll$ and $\ggg$ be addition modulo 2^{32}, exclusive-or, multiplication modulo 2^{32} and left and right shift operations, respectively. Let $\lll$ be left rotation and $\|$ be concatenation of two binary strings. Let e_i be a 32-bit binary string in which the i-th bit is one and the others are zero. Let $A[i]$ be the i-th bit of a 32-bit block A. Let $A[i \sim j]$ denote $A[j] \parallel A[j-1] \parallel \cdots \parallel A[i]$.

3 Related Key Truncated Differential Attacks on XTEA

In this section, we first briefly describe the XTEA algorithm and introduce an 8-round related key truncated differential characteristic of XTEA, which is similar to that of [3] [1]. Then, we show that related key differential cryptanalysis can be applied to attack several reduced-round versions of XTEA using this 8-round related key truncated differential characteristic.

3.1 Description of XTEA

XTEA is a 64-round Feistel block cipher with 64-bit block size and 128-bit key size. Operations used in XTEA are just exclusive-or, additions and shifts. As shown in Fig. 1, XTEA has a very simple round function. Let δ be the constant value $9e3779b9_x$ and $P = (L_n, R_n)$ be the input to the n-th round, for $1 \le n \le 64$. Then the output of the n-th round is (L_{n+1}, R_{n+1}), where $L_{n+1} = R_n$ and R_{n+1} is computed as follows :

For each i ($1 \le i \le 32$), if $n = 2i - 1$

$$R_{n+1} = L_n \boxplus (((R_n \ll 4 \oplus R_n \gg 5) \boxplus R_n) \oplus ((i-1) \cdot \delta \boxplus K_{((i-1)\cdot\delta \gg 11)\&3}),$$

and if $n = 2i$,

$$R_{n+1} = L_n \boxplus (((R_n \ll 4 \oplus R_n \gg 5) \boxplus R_n) \oplus (i \cdot \delta \boxplus K_{(i\cdot\delta \gg 11)\&3}).$$

XTEA has a very simple key schedule: the 128-bit master key K is split into four 32-bit blocks $K_0,\ K_1,\ K_2,\ K_3$. Then, for $r = 1, \cdots, 64$, the round keys K_r are derived from the following equation :

$$K_r = \begin{cases} K_{(\frac{r-1}{2}\cdot\delta \gg 11)\&3} & \text{if } r \text{ is odd} \\ K_{(\frac{r}{2}\cdot\delta \gg 11)\&3} & \text{if } r \text{ is even} \end{cases}$$

Table. 3 depicts the entire key schedule.

[1] There is an explicit separation between our truncated differential characteristic and that of [3]. We use the internal difference caused by the specific related key and plaintext pair, whereas S. Hong et al. [3] used the difference resulting from the plaintext pair only. So, we call this characteristic related key truncated differential characteristic in this paper.

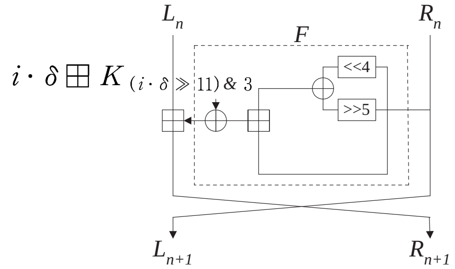

L_n
R_n
F
$i \cdot \delta \boxplus K_{(i \cdot \delta \gg 11)\,\&\,3}$
<<4
>>5
L_{n+1}
R_{n+1}

Fig. 1. $2i$-th round of XTEA

Table 3. Key schedule of XTEA

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

3.2 8-Round Related Key Truncated Differential Characteristic

In [3], S. Hong et al. suggested an 8-round truncated differential characteristic in order to attack 23 rounds of XTEA (8∼30 or 30∼52). Here, we construct a similar 8-round related key truncated differential characteristic. See Fig. 2. Let Ψ be our 8-round related key truncated differential characteristic described in Fig. 2. Let γ be 0^{32} or e_{30} and RK_i be the round key of the i-th round. We consider identical input values (zero difference) to the i-th round and a related round key pair RK_i and $RK'_i = RK_i \oplus e_{30}$. Then, the value of the 30-th bit of the right output difference in the i-th round is always one, and the other bits are all zero (except for the 31-st bit). Note that the 31-st bit is unknown. (However, we do not need to consider this value). That is, the output difference of the i-th round is $(0, e_{30})$ or $(0, e_{31} \oplus e_{30})$ with probability 1. As shown in Fig. 2, there are three possible colors for every bit: white, black, and gray. Every white bit denotes a zero difference. The bit which we focus on is the black bit. Note that the value of the black bit does not change throughout Ψ, while its position is shifted up to 5 bits to the right per round. And the values of the gray bits are irrelevant. That is, if for each j $(i+1 \leq j \leq i+7)$ the relation between RK_j and RK'_j is $RK'_j = RK_j \oplus \gamma$ ($\gamma = 0^{32}$ or e_{30}), then by the property of the round function F of XTEA, the black bit will be located at bit position 0 in the left output difference with probability 1, after $(i+7)$ rounds.

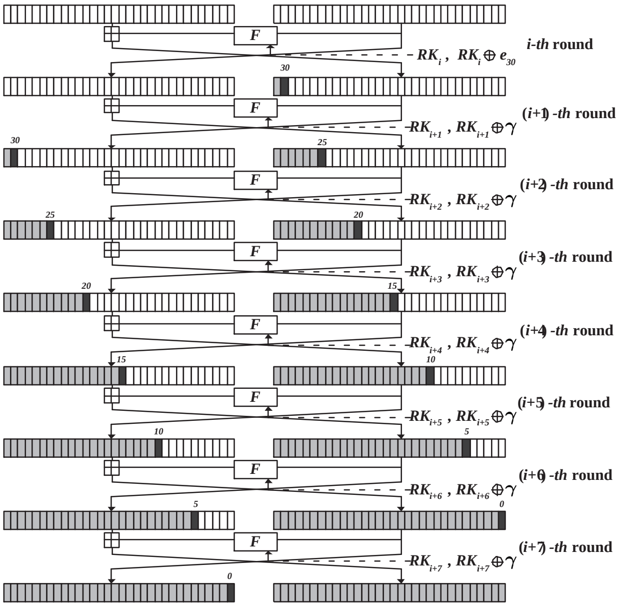

F
RK_i , $RK_i \oplus e_{30}$
i-th round
30
RK_{i+1} , $RK_{i+1} \oplus \gamma$
(i+1) -th round
30
25
RK_{i+2} , $RK_{i+2} \oplus \gamma$
(i+2) -th round
25
20
RK_{i+3} , $RK_{i+3} \oplus \gamma$
(i+3) -th round
20
15
RK_{i+4} , $RK_{i+4} \oplus \gamma$
(i+4) -th round
15
10
RK_{i+5} , $RK_{i+5} \oplus \gamma$
(i+5) -th round
10
5
RK_{i+6} , $RK_{i+6} \oplus \gamma$
(i+6) -th round
5
0
RK_{i+7} , $RK_{i+7} \oplus \gamma$
(i+7) -th round
0

Fig. 2. 8-round related key truncated differential characteristic Ψ ($\gamma = 0^{32}$ or e_{30})

3.3 Related Key Truncated Differential Attacks on XTEA

Using the above 8-round related key truncated differential characteristic, we can attack 25 (1∼25) and 27 (4∼30) rounds of XTEA. Here, we apply conventional related key differential cryptanalysis as described in [4]. We exploit the property that if there exists a related key pair (K, K') such that a non-zero input difference of two plaintexts can be changed into a zero output difference, then we can bypass several rounds for free in our attack.

Attack on 25 (1∼25) rounds of XTEA We consider the related key pair $K = (K_0, K_1, K_2, K_3)$ and $K'{=}(K_0 \oplus e_{30}, K_1, K_2, K_3)$ in order to attack 25 (1∼25) rounds of XTEA. Then, according to the key schedule of XTEA, K_0 and $K_0 \oplus e_{30}$ are used in the first round. Assume that there exist plaintext-ciphertext pairs, (P, C) and (P', C') respectively encrypted under the master keys K and K', such that the first round output value of the two plaintexts P and P' under the round keys K_0 and $K_0 \oplus e_{30}$ are the same, i.e. such that the output difference of the first round is zero. (Here, we call the first 32-bit blocks of K and K', (K_0 and $K_0 \oplus e_{30}$) 'the related round key pair'). Then, due to the key schedule of XTEA, we can bypass 6 rounds for free in our attack. This means that the input difference to the 8-th round is zero. According to the key schedule of XTEA, the related round key pair, K_0 and $K_0 \oplus e_{30}$ is reused in the 8-th round. Now, we can apply the 8-round related key truncated differential characteristic described in

Fig. 2. As a result, bit position 0 of the left input difference to round 16, which is colored in black in Fig. 3, is one with probability 1.

In order to obtain the above assumed plaintext pair P and P', which has the same output value after the first round under the key K and K' respectively, we consider the following 1-round structure of plaintexts $S(P)$.

$$S(P) = \{P, P \oplus (e_{31}, 0), P \oplus (e_{30}, 0), P \oplus (e_{31} \oplus e_{30}, 0)\}$$

We request the encryption of every plaintext in $S(P)$ under the related key pair $K = (K_0, K_1, K_2, K_3)$ and K'=$(K_0 \oplus e_{30}, K_1, K_2, K_3)$ respectively. Let $C(P)$ be the set of ciphertexts of the elements of $S(P)$ under the key $K = (K_0, K_1, K_2, K_3)$, i.e. $C(P) = \{E_K(P), E_K(P \oplus (e_{31}, 0)), E_K(P \oplus (e_{30}, 0)), E_K(P \oplus (e_{31} \oplus e_{30}, 0)), \}$. And let $C'(P)$ be the set of ciphertexts of the elements of $S(P)$ under the key K'=$(K_0 \oplus e_{30}, K_1, K_2, K_3)$, i.e. $C'(P) = \{E_{K'}(P), E_{K'}(P \oplus (e_{31}, 0)), E_{K'}(P \oplus (e_{30}, 0)), E_{K'}(P \oplus (e_{31} \oplus e_{30}, 0)), \}$. Then, it is easy to see that there are exactly four plaintext pairs that have the same output value after the first round, i.e. we can obtain the required zero output difference after the first round. We denote these four plaintext pairs as (P_u, P'_u) where $1 \leq u \leq 4$. We also denote $(C_u = E_K(P_u)$, $C'_u = E_{K'}(P'_u))$ as the ciphertexts corresponding to plaintext P_u under key K and plaintext P'_u under key K', respectively.

Now we use the above property of the black bit located in bit position 0 of the left input difference in round 16, in order to attack 25 (1∼25) rounds of XTEA and recover 111 bits of the subkey derived from master key K.

Algorithm 1 describes how to recover 111 bits of subkey material from the ciphertexts. We compute the difference of every dotted bit position and the values of the bit pair of every gray bit position in order to get the black bit of the left half of the input difference in round 16. (See Fig. 3). In detail, in order to compute the black bit of the input difference of round 16, ($L_{16}[0]$), we need to know the differences of $R_{17}[0]$, $L_{17}[0]$, and $L_{17}[5]$, respectively. Also, in order to know the differences of $R_{17}[0]$, $L_{17}[0]$, and $L_{17}[5]$ we need to know the differences of $L_{18}[10]$ and $R_{18}[5]$. (For the knowledge of these differences, we need $L_{18}[0 \sim 10]$, $R_{18}[0 \sim 5]$, and $K_0[0 \sim 4]$.). Due to the structure of the round function of XTEA, the key and output bit positions related to the black bit increase by 5 bits per round. Consequently, if we guess all the bits of K_0, K_2, K_3, and 15 bits of K_1, and we also get the output pair after the 25-th round, we can compute the black bit of the input difference in round 16.

In *Algorithm* 1, σ denotes the function which outputs the one-bit difference in $L_{16}[0]$ using a given ciphertext pair and the guessed key bits. Let $\mathbf{K}$ be the concatenation of $K_1[0 \sim 14]$, K_2, and K_3, i.e., $\mathbf{K} = K_1[0 \sim 14] || K_2 || K_3$. Note that $\mathbf{K}$ is a 79-bit string. In *Algorithm* 1, we guess K_0 and $\mathbf{K}$. Using this algorithm, we are able to find 111 bits of $K = (K_0, K_1, K_2, K_3)$.

```
Input : $m$ structures : $S(P^1), S(P^2), \cdots, S(P^m)$,
        corresponding $m$ pairs of ciphertexts :
                $(C(P^1), C'(P^1)), \cdots, (C(P^m), C'(P^m))$
Output : 111-bit partial key value of $K = (K_0, K_1, K_2, K_3)$

1. For $K_0 = 0, 1, \ldots, 2^{32} - 1$
  1.1. For $i = 1, \ldots, m$
    1.1.1 Find the four plaintext pairs $(P_u^i, P_u^{i\prime})$, $1 \le u \le 4$, such that
      for each $u$, the following two conditions hold:
      (a)$P_u^i = (LP^i \oplus v)||RP^i$ and $P_u^{i\prime} = (LP^i \oplus w)||RP^i$
        for some $v$, $w \in \{0, e_{31}, e_{30}, (e_{31} \oplus e_{30})\}$.
      (b)$[(LP^i \oplus v) \boxplus F(RP^i, K_0)] \oplus [(LP^i \oplus w) \boxplus F(RP^i, K_0 \oplus e_{30})] = 0$
      // Here, we use the notation $LP^i$ for the left half and $RP^i$ for the right
        half of the plaintext $P^i$.//
  1.2. For $\mathbf{K} = 0, 1, \ldots, 2^{79} - 1$
    1.2.1. For $i = 1, \ldots, m$
      1.2.1.1 For $u = 1, \ldots, 4$
            Compute $\sigma_u^i = \sigma(C_u^i, C_u^{i\prime}, K_0, \mathbf{K})$
            If $i = m$, $u = 4$, and $\sigma_u^i = 1$, then output $K_0$, $\mathbf{K}$ and stop.
            Else if $\sigma_u^i = 0$, goto 1.2.
```

Algorithm 1. Related key truncated differential attack on 25 rounds of XTEA

The output of the algorithm is the right value of some 111 bits of $K = (K_0, K_1, K_2, K_3)$ with high probability if m is sufficiently large. For each i $(0 \le i \le 2^{111} - 1)$, the probability that the attack algorithm outputs the i-th key-candidate is $(1 - 2^{-4m})^i$. So, the average success rate of this attack is

$$2^{-111} \sum_{i=0}^{2^{111}-1} (1 - 2^{-4m})^i = 2^{4m-111}(1 - (1 - 2^{-4m})^{2^{111}}) \approx 2^{4m-111}(1 - e^{-2^{111-4m}}).$$

Let k be a key candidate $(0 \le k \le 2^k - 1)$. For m structures of plaintexts, the expected number of trials, required until each k is determined as a wrong value, is $1 + 2^{-1} + 2^{-2} + \cdots + 2^{-4m+1} = 2 - 2^{-4m+1}$. If a key k is right, then the number of trials is exactly $4m$. Thus, the average number of trials in the attack is

$$2^{-k} \sum_{i=0}^{2^k-1} i \cdot (2 - 2^{-4m+1}) + 4m = 4m + (1 - 2^{-4m})(2^k - 1).$$

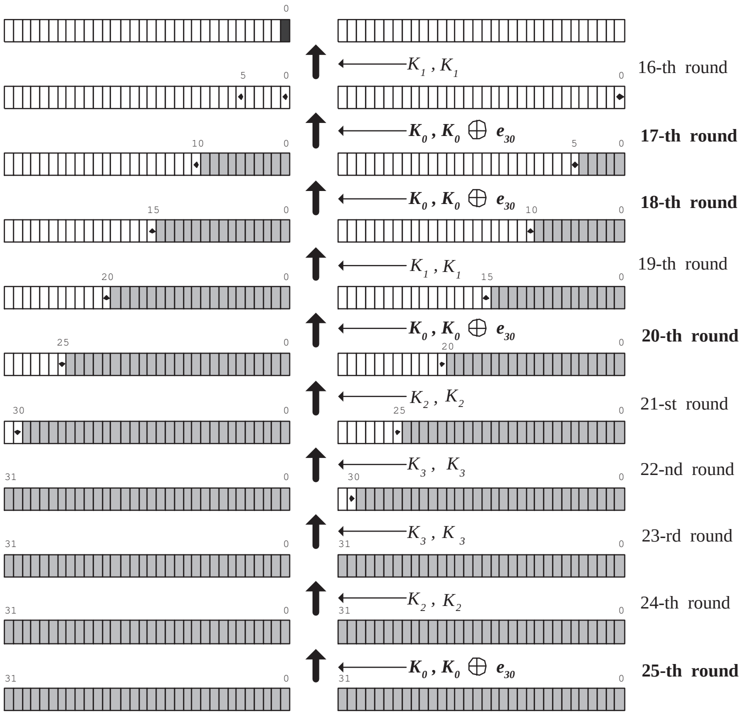


Fig. 3. Related key Truncated Differential Attack on 25 rounds of XTEA

So, if we get ≈ 29 plaintext structures, the attack on 25 rounds of XTEA will succeed on average with probability 96.9%. This success rate implies that our attack reduces almost all key spaces efficiently. It has a data complexity of $29 \cdot 4 = 116$ chosen-plaintexts and time complexity of $(116+(1-2^{-116})(2^{111}-1))\cdot\frac{6.5}{25}\cdot 2 \approx 2^{110.05}$ 25-round XTEA encryptions.

Attack on 27 (4∼30) rounds of XTEA In the key schedule of XTEA, K_3 is not used from the 24-th round until the 30-th round. This means that we may expand more rounds for free. Using this observation, we can attack 27 (4∼30) rounds of XTEA. This attack only differs from the attack on 25 (1∼25) rounds of XTEA in two aspects. One is the use of the related key pair $K = (K_0, K_1, K_2, K_3)$ and $K' = (K_0, K_1 \oplus e_{30}, K_2, K_3)$. The other is the use of 2-round plaintext structures, $S'(P)$.

First, we describe what we mean by a 2-round plaintext structure. Let P be a plaintext and A be the set of all 32-bit values whose lower 22 bits are fixed to $10\cdots 0$. We define the 2-round structure of plaintexts $S'(P)$ as follows :

$$S'(P) = \{P\} \cup \{P \oplus (w, v) | w \in A, v \in \triangle X\},$$

where $\triangle X$ is the following set :

$$\begin{aligned}\triangle X = \{&01000010\cdots 0, 01000110\cdots 0, 01001110\cdots 0,\\ &01011110\cdots 0, 01111110\cdots 0, 00111110\cdots 0,\\ &11000010\cdots 0, 11000110\cdots 0, 11001110\cdots 0,\\ &11011110\cdots 0, 11111110\cdots 0, 10111110\cdots 0\}\end{aligned}$$

Note that $S'(P)$ contains $12,289$ chosen-plaintexts and there are $12,288$ plaintext pairs of the form $(P, P\oplus(w,v))$ where $w{\in}A$ and $v{\in}\triangle X$. We consider encryptions of these plaintexts under the keys $K = (K_0, K_1, K_2, K_3)$ and $K' = (K_0, K_1{\oplus}e_{30}, K_2, K_3)$, respectively. Then, for every subkey K_2, there exist (w_1,v_1), $(w_2,\ v_2)$ and (w_3, v_3) such that the second round output differences of $(P, P\oplus(w_1, v_1))$, $(P, P\oplus(w_2, v_2))$, $(P, P\oplus(w_3, v_3))$ are respectively $(e_{30}, 0)$, $(e_{31}, 0)$ and $(e_{30}{\oplus}e_{31}, 0)$. Note that this attack is starting from the 4-th round. That is, the 4-th and 5-th round correspond to the first and second round, respectively. This means that there exist four plaintexts in $S'(P)$ which have the same property as the elements of the 1-round structure $S(P)$ described in the attack on 25 rounds of XTEA. Furthermore, in the key schedule, the related round key pair K_1 and $K_1{\oplus}e_{30}$ is first used in the 6-th round and then again in the 11-th round. So we can again get the same output values after the third round (6-th round) of encryption, i.e. the output difference after the third round is zero. Thus, we can bypass 5 rounds for free. Then, Ψ is applied from the eighth round (11-th round) through the fifteenth round (18-th round). Therefore, with similar methods as for the attack on 25 ($1{\sim}25$) rounds of XTEA, we can recover 116 bits of the master key K (K_0, K_1, K_2, and $K_3[0{\sim}19]$). Overall, we use 121 structures to attack 27 ($4{\sim}30$) rounds with an expected success rate of 96.9%. This requires $(121 * 12289 = 1486949) \approx 2^{20.5}$ chosen-plaintexts and $(121 + (1-2^{-121})(2^{116}-1)\cdot\frac{7.5}{27}\cdot 2 \approx 2^{115.15}$ 27-round XTEA encryptions.

In addition, with similar methods, various attacks on 27 rounds of XTEA are possible. Table 4. depicts these attacks. ‘Key Bits’ denotes the total number of bits in K_0, K_1, K_2, and K_3 recovered by the attack.

Table 4. Various attacks on 27 rounds of XTEA

variant rounds	Key Bits	relation of keys
13-th $\sim$ 39-th	K_1, K_2, K_3 : 32 bits, respectively, K_0 : 15 bits	$K{\oplus}K'{=}(0,0,0,e_{30})$
17-th $\sim$ 43-rd	K_0, K_1, K_3 : 32 bits, respectively, K_2 : 15 bits	$K{\oplus}K'{=}(0,e_{30},0,0)$
22-nd $\sim$ 48-th	K_1, K_2, K_3 : 32 bits, respectively, K_0 : 20 bits	$K{\oplus}K'{=}(0,0,e_{30},0)$
31-st $\sim$ 57-th	K_0, K_2, K_3 : 32 bits, respectively, K_1 : 15 bits	$K{\oplus}K'{=}(e_{30},0,0,0)$
35-th $\sim$ 61-st	K_0, K_1, K_2 : 32 bits, respectively, K_3 : 15 bits	$K{\oplus}K'{=}(0,0,e_{30},0)$

4 Related Key Differential Attacks on GOST

In this section, we describe the specification of GOST and briefly introduce H. Seki et al.'s differential cryptanalysis of a reduced-round version of it [8]. Next, we show that we can distinguish full-round GOST from a random oracle with probability $1-2^{-64}$ using a related key differential characteristic and also present a related key differential attack on 31 rounds of GOST. Finally, we propose a related key differential attack on full-round GOST.

4.1 Description of GOST and Previous work

GOST is a 32-round Feistel block cipher with 64-bit block size and 256-bit key size. It iterates a simple round function F composed of key additions, eight different 4×4 S-boxes S_i $(1 \leq i \leq 8)$ and cyclic rotations. See Fig. 4.

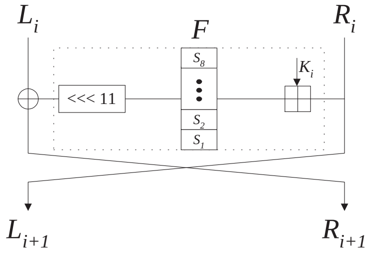


Fig. 4. i-th round of GOST

The key schedule of GOST is very simple. The 256-bit master key K is split into eight 32-bit blocks $K_1, \cdots, K_8$, i.e. $K = (K_1, \cdots, K_8)$ and each round uses one of them as shown in Table 5.

Table 5. Key schedule of GOST

Round	$1 \ldots 8$	$9 \ldots 16$	$17 \ldots 24$	$25 \ldots 32$
Key	$K_1 \ldots K_8$	$K_1 \ldots K_8$	$K_1 \ldots K_8$	$K_8 \ldots K_1$

Due to the subkey addition operation in the round function, the differential properties of GOST vary not only with the values of the input and output differences, but also with the value of the subkey itself. In order to minimize the dependence of the differential probability on the key, H. Seki et al. introduced the idea of using a set of differential characteristics [8]. They use two differential sets $\Delta = \{0abc\}$ and $\nabla = \{abc0\}$ where $a, b, c \in \{0, 1\}$, which respectively represent nonzero 4-bit input and output differences of an S-box. In addition, they computed the following average probability of differentials for each S-box represented by p_{S_i}.

$$p_{S_i} \ : \ Prob\{\varDelta \overset{S_i}{\to} \nabla\}$$

The value of $Prob\{\varDelta \overset{S_i}{\to} \nabla\}$ varies from 0.30 to 0.75 depending both on the S-box S_i and on the key value. See Table. 6 (for more details, refer to [8]). Using this set of characteristics, they attack 13 rounds of GOST and also present a combined related key attack on 21 rounds of GOST.

4.2 Related Key Differential Attacks on GOST

Now we present several attacks on GOST.

Distinguishing Attack We can distinguish full-round GOST from a truly random permutation with probability $1-2^{-64}$ using a related key differential characteristic. Here, we consider an attacker that has two oracles $\mathcal{O}$ and $\mathcal{O}'$. $\mathcal{O}$ is the oracle which, given a plaintext P, outputs a ciphertext $E_K(P)$ under key $K = (K_1, \cdots, K_8)$. $\mathcal{O}'$ is the oracle which, given a plaintext P', outputs a ciphertext $E_{K'}(P')$ under key $K' = (K_1 \oplus e_{31}, K_2 \oplus e_{31}, \cdots, K_8 \oplus e_{31})$. Note that the key $K = (K_1, \cdots, K_8)$ is unknown to the attacker. However he knows the relation $K \oplus K' = (e_{31}, \cdots, e_{31})$.

Let us first consider the function E as GOST. In this case, if we query $\mathcal{O}$ for $P = (P_L, P_R)$, and $\mathcal{O}'$ for $P' = (P_L \oplus e_{31}, P_R \oplus e_{31})$ respectively, and obtain the corresponding ciphertexts C and C', then the output difference $C \oplus C'$ of full-round GOST is always (e_{31}, e_{31}). More specifically, it is easy to see that for every round, the input difference of each S-box after key addition is zero

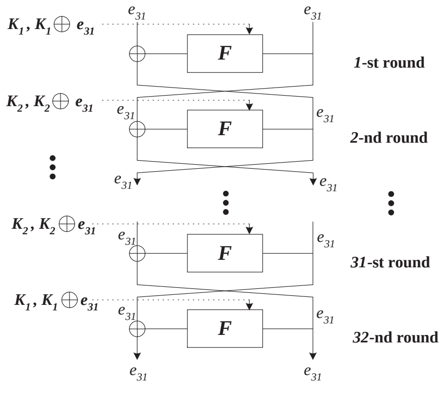


Fig. 5. 32-round related key differential characteristic of GOST.

with probability 1. Therefore the difference between the plaintexts, (e_{31}, e_{31}) is maintained after every round. In other words, this is a 32-round related key differential characteristic with probability 1 (See Fig. 5).

If we consider the function E as a truly random permutation, then the output pair of the truly random permutation is unpredictable so that we can't obtain any information from it. So we can successfully distinguish full-round GOST from a truly random permutation with high probability, namely $1-2^{-64}$. Note that this distinguishing attack is possible with only two chosen plaintexts under the given key relation.

Related Key Differential Attack on 31 Rounds of GOST We use the differential probability for each S-box presented in [8], as their differential characteristic enables us to mount a related key differential attack on 31 rounds of GOST. For this attack we consider the following two related keys K and K'.

$$\begin{aligned} K &= (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8) \\ K' &= (K_1 \oplus e_{31}, K_2, K_3 \oplus e_{31}, K_4, K_5 \oplus e_{31}, K_6, K_7 \oplus e_{31}, K_8) \end{aligned}$$

We request the encryption of $P = (P_L, P_R)$ under key K and of $P' = (P_L, P_R \oplus e_{31})$ under key K'. Then we obtain a 24-round related key differential characteristic with probability 1. See Fig. 6. With this 24-round related key differential characteristic, we can bypass 24 rounds for free in our attack. As shown in Fig. 6., the output difference of the 24-th round is $(0, e_{31})$, i.e. the input difference of the 25-th round is $(0, e_{31})$. We use the set of differential characteristics [8] mentioned in Section 4.1 in order to construct another 6-round related key differential charac-

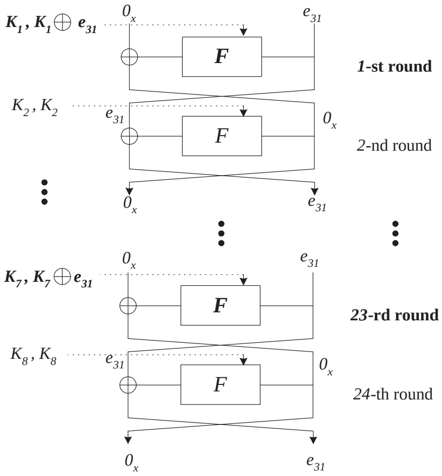


Fig. 6. 24-round related key differential characteristic (1∼24) with probability 1.

teristic from the 25-th round through the 30-th round. See Fig. 7. In this figure, # denotes an element of the differential set $\mathit{\Delta} = \{0abc\}$, where $a, b, c \in \{0, 1\}$. In the 25-th round, the input difference of round function F, 80000000_x becomes $00000\#00_x$ with probability $\frac{3}{4}$. [2] After the 25-th round, each average related key differential probability is computed using Table. 6 [8]. Thus, combining these two related key differential characteristics, we construct a 30-round related key differential characteristic from the 1-st round to the 30th-round of GOST with probability about $2^{-23.33}$.

Table 6. Average differential probability of each S-box

p_{S_1}	p_{S_2}	p_{S_3}	p_{S_4}	p_{S_5}	p_{S_6}	p_{S_7}	p_{S_8}
0.43	0.38	0.37	0.37	0.37	0.35	0.47	0.45

Now, we consider a $1R$ [1] related key differential attack on 31 rounds of GOST using the above constructed 30-round related key differential characteristic. Considering 2^{26} chosen plaintext pairs, there remain about 2^{12} ciphertext

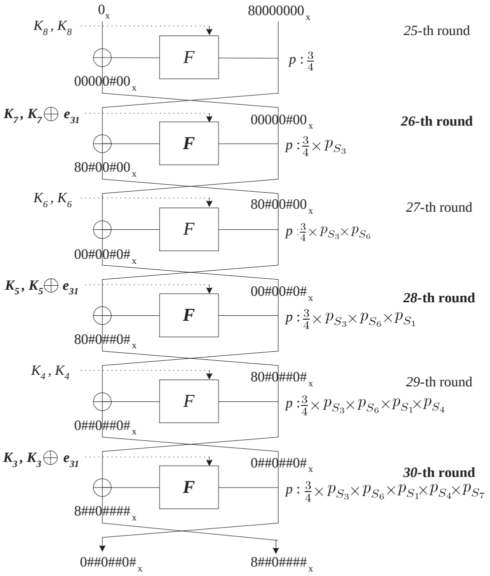


Fig. 7. 6-round related key differential characteristic (rounds 25∼30)

[2] We only need to compute the probability $Prob\{1000 \overset{S_8}{\to} \nabla = \{abc0\}\}$ because of the structure of the round function F. This probability is easily checked by simulation and also represented in [8].

pairs after the filtering step. Among them, we expect that there exist at least 5 right pairs. A wrong key is counted with probability 2^{-17} by the above 30-round related key differential characteristic. The signal-to-noise ratio S_N [1] of this related key differential characteristic is about $2^{22.67}$. Thus, according to [9], we can recover the 32 bits of the 31-st round subkey with about 2^{26} chosen plaintexts and time complexity $(2^{32} \times 2^{26} \times 2^{-14} \times \frac{1}{31}) \approx 2^{39}$ with an expected success rate of 97.9%.

Full Rounds Attack on GOST In this section, we suggest an algorithm to find 12 bits of K_1 with high probability of success.

Consider $P = (P_L, P_R)$ and $P' = (P_L \oplus e_{30}, P_R \oplus e_{30})$ encrypted under keys $K = (K_1, \cdots, K_8)$ and $K' = (K_1 \oplus e_{30}, K_2 \oplus e_{30}, \cdots, K_8 \oplus e_{30})$ respectively. Then, after key addition, in each round the input difference becomes 0 with probability 2^{-1}. Thus, we can construct a 30-round related key differential characteristic with probability 2^{-30} as shown in Fig. 8. In this figure, white bits denote a zero difference, black bits denote a nonzero difference and gray bits are unknown.

Let $C = (C_L, C_R)$, $C' = (C'_L, C'_R)$ be the ciphertexts of P and P' under keys K and K', respectively and assume that (P, P') is a right pair for a related key differential characteristic such as described in Fig. 8. (i.e. the output difference after round 30 is (e_{30}, e_{30})). Then there are four types of differential characteristics $C1, C2, C3$ and $C4$ as listed below.

C1. $C_R \oplus C'_R = e_{30}$ and $C_L \oplus C'_L = e_{30}$.
This case means that the input differences of the S-boxes in round 31 and round 32 are 0, so we can recover $K_1[30]$ by checking $C_R[30] + K_1[30] = C'_R[30] + (K_1[30] \oplus 1)$ where "+" means integer addition.

C2. $C_R \oplus C'_R = e_{30}$, $(C_L \oplus C'_L)[0 \sim 6] = 0$, $(C_L \oplus C'_L)[11 \sim 29] = 0$ and $(C_L \oplus C'_L)[31] = 0$. (Refer to Fig. 8*a*.)
This case means that the input difference of S_8 in round 31 is zero, but in round 32 it is nonzero, so we can recover $K_1[30]$ by checking $C_R[30] + K_1[30] \neq C'_R[30] + (K_1[30] \oplus 1)$. Also if such a pair is given, $K_1[28], K_1[29], K_1[31]$ can be recovered by checking

$S8(C_R[28 \sim 31] + K_1[28 \sim 31]) \oplus C_L[7 \sim 10] = S8(C'_R[28 \sim 31] + K'_1[28 \sim 31]) \oplus C'_L[7 \sim 10]$ or

$S8(C_R[28 \sim 31] + 1 + K_1[28 \sim 31]) \oplus C_L[7 \sim 10] = S8(C'_R[28 \sim 31] + 1 + K'_1[28 \sim 31]) \oplus C'_L[7 \sim 10]$.

If we add $C_R[0 \sim 27]$ to $K_1[0 \sim 27]$, a carry may occur at the 27-th bit position, so we need to check the above two equations. We denote $S8(C_R[28 \sim 31] + K_1[28 \sim 31]) \oplus C_L[7 \sim 10]$ by $F_{k_j}(C_R[28 \sim 31]) \oplus C_L[7 \sim 10]$ in *Algorithm* 2.

C3. $C_R \oplus C'_R \neq e_{30}$, $(C_R \oplus C'_R)[7] = 0$
This case means that the input difference of S_8 in round 31 is nonzero and $(C_R \oplus C'_R)[7] = 0$. In this case, if we know $K_1[0 \sim 11]$, we can compute the exact value of $(F_{K_1}(C_R))[11 \sim 22]$ and $(F_{K_1}(C'_R))[11 \sim 22]$. So $K_1[8 \sim 11]$

can be recovered by checking

$(F_{K_1[0\sim 11]}(C_R))[19 \sim 22] \oplus C_L[19 \sim 22] = (F_{K'_1[0\sim 11]}(C'_R))[19 \sim 22] \oplus C'_L[19 \sim 22]$.

Note that $(F_{K_1[0\sim 7]}(C_R))[11 \sim 18] \oplus C_L[11 \sim 18] = (F_{K'_1[0\sim 7]}(C'_R))[11 \sim 18] \oplus C'_L[11 \sim 18]$ for any arbitrary candidate key $K_1[0 \sim 7]$, so we cannot find the right value $K_1[0 \sim 7]$ with high probability. That is the reason why we only consider recovering $K_1[8 \sim 11]$.

C4. $C_R \oplus C'_R \neq e_{30}$, $(C_R \oplus C'_R)[7] \neq 0$. (Refer to Fig. 8*b*.)
This case means that the input difference of S_8 in round 31 is nonzero and $(C_R \oplus C'_R)[7] \neq 0$. By similar arguments as for case *C3* we can recover $K_1[4 \sim 11]$ by checking

$(F_{K_1[0\sim 11]}(C_R))[15 \sim 22] \oplus C_L[15 \sim 22] = (F_{K'_1[0\sim 11]}(C'_R))[15 \sim 22] \oplus C'_L[15 \sim 22]$.

Note that the key bits found in case *C1* and *C3* can also be found in case *C2* and *C4*, respectively. An attack algorithm is given in *Appendix A*.

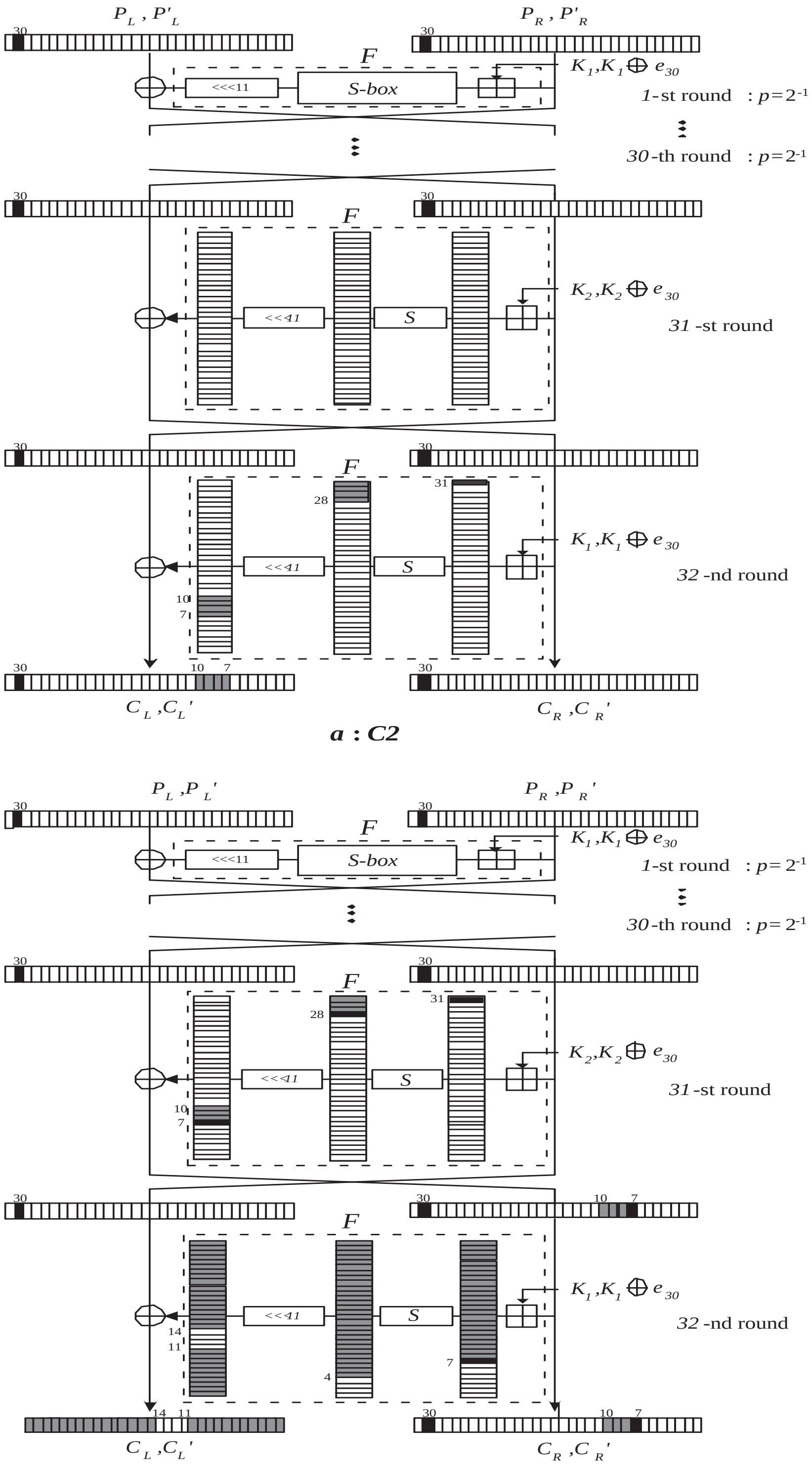
Let us consider the success probability of *Algorithm* 2. If we choose 2^{35} pairs, there exist at least 4 pairs satisfying the conditions *C2* and *C4* respectively, with probability about 0.96. Also there are at most 15 wrong pairs surviving the filtering step with probability about 0.99. Since the probability that a wrong key is counted at most 3 times in step 3 and step 4 is about 1, the success probability of *Algorithm* 2 is about 0.917 using about 2×2^{35} encryptions.

5 Conclusion

We presented related key differential attacks on XTEA and GOST. In the case of XTEA, we use 121 structures to attack 27 rounds of XTEA with an expected success rate of 96.9%; this attack requires about $2^{20.5}$ chosen-plaintexts and $2^{115.15}$ 27-round XTEA encryptions.

Furthermore, we can successfully distinguish the block cipher GOST from a random permutation with probability $1-2^{-64}$ and attack full-round GOST. As a result, we can recover 12 bits of the master key with an expected success rate of 91.7% using 2^{35} chosen plaintexts, in 2^{36} encryption operations. Therefore, we believe that our result is valuable to analyze the security of GOST.

Acknowledgements The authors are thankful to Deukjo Hong for discussing XTEA and very much appreciate Helena Handschuh's and the anonymous referees' aid in improving the presentation of this work.



a : C2

b : C4

Fig. 8. 32-round related key differential characteristic of GOST.

References

1. E. Biham and A. Shamir, “Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag, 1993.
2. GOST, Gosudarstvennyi Standard 28147-89, “Cryptographic Protection for Data Processing Systems”, Government Committee of the USSR for Standards, 1989.
3. S. Hong, D. Hong, Y. Ko, D. Chang, W. Lee, and S. Lee, “Differential Cryptanalysis of TEA and XTEA”, *Pre-Proceedings of the 6th Annual International Conference on Information Security and Cryptology (ICISC ’03)*, Lecture Notes in Computer Science. Springer-Verlag, 2003. pp. 413-428.
4. J. Kelsey, B. Schneier, and D. Wagner, “Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES”, *Advances in Cryptology - CRYPTO ’96*, volume 1109 of *Lecture Notes of Computer Science*, Springer-Verlag, 1996, pp. 237-251.
5. J. Kelsey, B. Schneier, and D. Wagner, “Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA”, *Proceedings of International Conference on Information and Communications Security (ICICS ’97)*, volume 1334 of *Lecture Notes of Computer Science*, Springer-Verlag, 1997, pp. 233-246.
6. D. Moon, K. Hwang, W. Lee, S. Lee, and J. Lim, “Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA”, *Fast Software Encryption ’02*, volume 2365 of *Lecture Notes of Computer Science*, Springer-Verlag, 2002, pp. 49-60.
7. R. Needham and D. Wheeler, “eXtended Tiny Encryption Algorithm”, October, 1997.
8. H. Seki and T. Kaneko, “Differential Cryptanalysis of Reduced Rounds of GOST”, *Seventh Annual Workshop on Selected Areas in Cryptography (SAC ’00)*, volume 2012 of *Lecture Notes of Computer Science*, Springer-Verlag, 2001, pp. 315-323.
9. A. Selçuk and A. Biçak “On Probability of Success in Linear and Differential Cryptanalysis”, *Third International Conference, SCN 2002*, volume 2365 of *Lecture Notes of Computer Science*, Springer-Verlag, 2002, pp. 174-185.
10. D. Wheeler and R. Needham, “TEA, a Tiny Encryption Algorithm”, *Fast Software Encryption, Second International Workshop Proceedings*, volume 1008 of *Lecture Notes of Computer Science*, Springer-Verlag, 1995, pp. 97-110.

Appendix A

Assumption : The attacker knows that $K \oplus K'$ is equal to $(e_{30}, e_{30}, \cdots, e_{30})$

Input : $(P_i, P_i'),\ (i = 1, \cdots, 2^{35})$ where $P_i \oplus P_i' = (e_{30}, e_{30})$ as in Fig. 8

Output: 12-bit partial key K_1; $K_1[4 \sim 11]$ and $K_1[28 \sim 31]$

```
// Setup stage //
  $\cdot\, Let\mathcal{K} = \{k_1, k_2, \cdots, k_{2^4}\}$ and $\mathcal{K}' = \{k_1', k_2', \cdots, k_{2^8}'\}$ be the set of candidate keys for
  $K_1[28 \sim 31]$ and $K_1[4 \sim 11]$, respectively
  $\cdot\, \mathcal{D}, \mathcal{D}'$ :  empty set
  $\cdot\, ctr_1 = 0, \cdots, ctr_{2^4} = 0, ctr_1' = 0, \cdots, ctr_{2^8}' = 0$
// Filtering step //
 1. For $i = 1, \ldots, 2^{35}$
   1.1. Request the ciphertexts $C_i = E_K(P_i)$ and $C_i' = E_{K'}(P_i)$
     If $C_i \oplus C_i'$ satisfies condition $C2$, $\mathcal{D} = \mathcal{D} \cup \{(C_i, C_i')\}$
     If $C_i \oplus C_i'$ satisfies condition $C4$, $\mathcal{D}' = \mathcal{D}' \cup \{(C_i, C_i')\}$
// Finding key $K_1[28 \sim 31]$ //
 2. For each $(C_i, C_i') \in \mathcal{D}$
  /* For convenience let $C_i = (C_L, C_R)$ and $C_i' = (C_L', C_R')$ */
   2.1.  For $j = 1, \ldots, 2^4$
         If $F_{k_j}(C_R[28 \sim 31]) \oplus C_L[7 \sim 10] = F_{k_j}(C_R'[28 \sim 31]) \oplus C_L'[7 \sim 10]$,
           $ctr_j+ = 1$
         If $F_{k_j}(C_R[28 \sim 31] + 1) \oplus C_L[7 \sim 10] = F_{k_j}(C_R'[28 \sim 31] + 1) \oplus C_L'[7 \sim 10]$,
           $ctr_j+ = 1$
         If $ctr_j \geq 4$, output $k_j$ as $K_1[28 \sim 31]$ and goto 3
// Finding key $K_1[4 \sim 11]$ //
 3. For each $(C_m, C_m') \in \mathcal{D}'$
  /* For convenience let $C_i = (C_L, C_R)$ and $C_i' = (C_L', C_R')$ */
   3.1.  For $j = 1, \ldots, 2^8$
     3.2.  For $i = 0, \ldots, 2^4 - 1$
           If $F_{k_j'||i}(C_R)[15 \sim 22] \oplus C_L[15 \sim 22] = F_{k_j'||i}(C_R')[15 \sim 22] \oplus C_L'[15 \sim 22]$,
             $ctr_j'+ = 1$
         /* Since $k_j'$ denotes $K_1[4 \sim 11]$ and $i$ denotes $K_1[0 \sim 3]$, $k_j'||i$ denotes
             $K_1[0 \sim 11]$ */
     3.3.  If $ctr_j' \geq 4$, output $k_j'$ as $K_1[4 \sim 11]$ and terminate this algorithm
```

Algorithm 2: 32-round related key differential attack on GOST.