Differential Cryptanalysis of Reduced Rounds of GOST

Haruki Seki[1] and Toshinobu Kaneko[2]

[1] TAO (Telecommunications Advancement Organization of Japan), 1-1-32
Shin'urashima-cho, Kanagawa-ku, Yokohama, 221-0031 Japan
hseki@yokohama.tao.go.jp
[2] Science University of Tokyo,
2641 Yamazaki, Noda-shi, Chiba, 278-8510 Japan
kaneko@ee.noda.sut.ac.jp

Abstract. The block cipher GOST was proposed in former Soviet Union in 1989. In this paper we present the first result of differential cryptanalysis of GOST with reduced number of rounds. By introducing the idea of using a set of differential characteristics, which is a partitioning type, we can reduce the influence of the key value upon the probability as well as get high differential probability. Using 2^{51} chosen plaintexts the key of 13-round GOST can be obtained. Next this differential cryptanalysis is expanded with combining related-key attack. Using 2^{56} chosen plaintexts the key of 21 rounds of GOST can be obtained.

1 Introduction

The block cipher GOST was proposed in former Soviet Union in 1989[1]. GOST is an acronym for "Gosudarstvennyi Standard", or Government Standard.

In this paper we present the first result of differential cryptanalysis of GOST with reduced number of rounds. Next the analysis is expanded with combining related-key attack.

GOST has key addition modulo 2^{32} in each round function. So orthodox differential cryptanalysis using one characteristic is not useful. The reason is that the probability of differential characteristic varies with not only the value of input-output difference but the value of the sub-key, frequently become zero. To overcome this we introduce the idea of using a set of differential characteristics. This is similar to truncated differential attack[2,3,4] in predicting only parts of all output bit value. But it is slightly different in the sense that this attack uses a set of differentials of S-boxes and applies this to round function, which is a partitioning type, and construct a new type of 2-round iterative characteristic. By this characteristic we can reduce the influence of the key value upon the probability as well as get high differential probability. On average using 2^{51} chosen plaintexts the key of 13-round GOST can be obtained. In the case of keys which make the probability the highest, 17 rounds of GOST can be attacked.

This differential cryptanalysis is expanded with combining related-key attack[5]. John Kelsey et al applied related-key attack to GOST[6]. But no concrete characteristics was revealed in [6]. In this paper we show the concrete characteristics.

D.R. Stinson and S. Tavares (Eds.): SAC 2000, LNCS 2012, pp. 315–323, 2001.

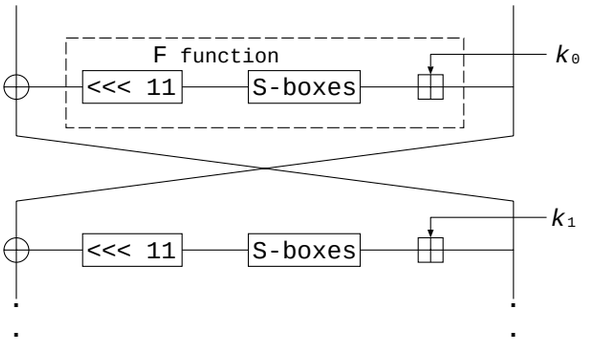

Fig. 1. GOST round function

On average using 2^{56} chosen plaintexts the key of 21-round GOST can be obtained.

These attacks are also applicable, even if the S-boxes are randomly generated.

This paper is organized as follows. Section 2 briefly reviews algorithm of GOST. In Section 3 we describe a differential cryptanalysis of GOST using one differential characteristic. In Section 4 we describe a differential cryptanalysis of GOST using a set of differential characteristics. In Section 5 we discuss the differential cryptanalysis with combining related-key attack. In Section 6 we discuss the differential cryptanalysis in the case of random S-boxes. We conclude in Section 7.

2 Description of GOST

The block cipher GOST is based on the framework of the Feistel cipher. GOST has 32 rounds, 64-bit blocksize, and 256-bit keysize. The F-function consists of operations specified as follows(see also Figure 1).

$+$: Addition modulo 2^{32}
S-boxes : 8 different 4×4-bit S-boxes $S_1, S_2, \cdot\cdot, S_8$
$<<<$ 11 : 11-bit left rotation

The S-boxes are not specified in the standard. In this paper we use a set of S-boxes used in an application for the Central Bank of the Russian Federation (tables of S-boxes are given in page 333 of [7], see also Appendix A.).

Key-schedule is simple. The 256-bit master-key is divided to eight 32-bit blocks : $k_1, k_2, \cdot\cdot, k_8$. Each round uses the subkey as shown in Table below.

Round	1	2	3	4	5	6	7	8	9	10	$\sim$	15	16	17	18	$\sim$	23	24	25	26	27	28	29	30	31	32
key	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_1	k_2	$\sim$	k_7	k_8	k_1	k_2	$\sim$	k_7	k_8	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1

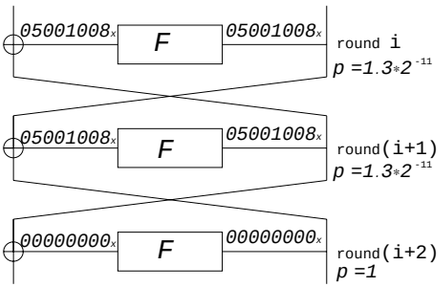

Fig. 2. One of the best 3-round iterative characteristic

3 An Attack Using One Differential Characteristic

GOST has key addition modulo 2^{32} in each round. In such a cipher the differential probability varies with not only the value of input-output difference but the value of the sub-key, and frequently become zero(see also Appendix B). Figure 2 shows one of the best 3-round iterative characteristic in case of S-boxes used in an application for the Central Bank of the Russian Federation[7][1]. This characteristic has the probability described below in one round.

$$0 \leq Prob\{05001008_x \rightarrow 05001008_x\} \leq 1.5 \times 2^{-7} \tag{1}$$

Where X $\rightarrow$ Y means that an *inputxor* X result in an *outputxor* Y. Average probability over all key values is 1.3×2^{-11} in one round. 8-round characteristic has probability 2^{-53}. So using 2-Round attack 10-round GOST is expected to be attacked using 2^{56} chosen plaintexts. But more than half of sub-key space makes the differential probability of each S-box to be zero(See also Appendix B). In 8-round characteristic the chance for the probability to be nonzero is only 2×10^{-5}. Consequently attack using one differential characteristic is not useful for GOST.

4 Cryptanalysis of GOST Using a Set of Differential Characteristics

To overcome the dependence of differential probability on the key, we introduce the idea of using a set of differential characteristics. This is slightly different from truncated differentials in the sense that this attack use a set of differentials of S-boxes and apply this to round function, which is a partitioning type, and construct a new type of 2-round iterative characteristics. By this characteristics we can considerably reduce the influence of the key value as well as get higher differential probability than described in Section 3.

[1] A 3-round iterative characteristic which has 2 active S-boxes in each round is impossible

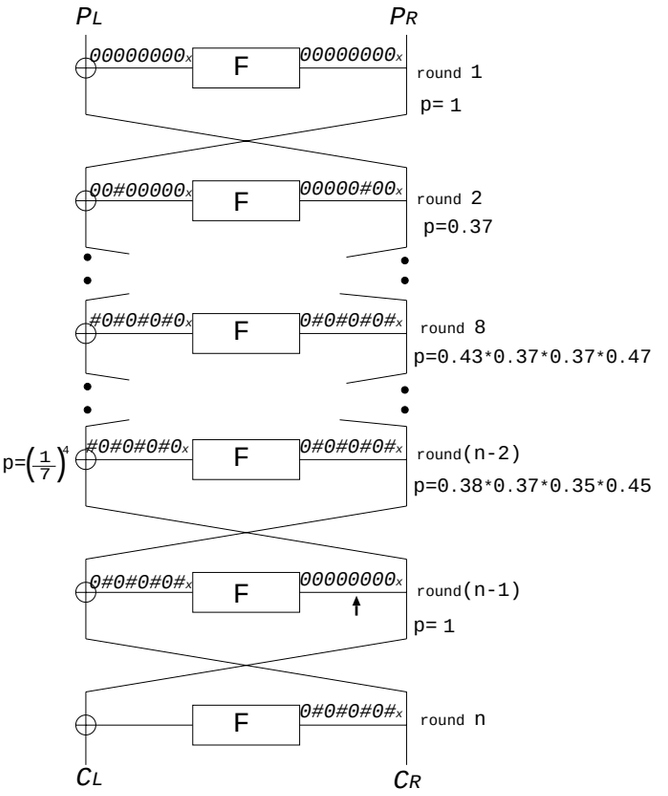

Fig. 3. A set of differential characteristics

4.1 A Set of Differential Characteristics

We use a set of differential characteristics as shown in Figure 3. The differences of plaintext pairs are $(00000\sharp00_x \parallel 00000000_x)$. $\sharp$ means nonzero 4-bit difference whose MSB(most significant bit) is zero.

This set of differential characteristics are possible when LSB(least significant bit) of output difference of each active S-box is zero. The number of active S-boxes increases one by one with the number of rounds, and saturates with 4 after round 8.

At first we estimate the probability of differentials of each S-box. That is $Prob\{$nonzero difference whose MSB is $0 \rightarrow$ nonzero difference whose LSB is $0\}$. The probability varies from 0.30 to 0.75 depending on S-box number and the key values(see Appendix C for details). Let p_{S_i} be average probability of S_i for all key values. The average probability of each round is the products of p_{S_i} of active S-boxes. For example the average probability of round 8,10, and so on is $p_{S_1} \times p_{S_3} \times p_{S_5} \times p_{S_7} = .43 \times .37 \times .37 \times .47$.

4.2 An Attack on GOST

To recover the last round sub-key, we use the characteristics as shown in Figure 3. At first we have to fix all 32 bits of input difference to $(n-1)$-th F-function to zero. To realize this a cancellation has to happen at an xor operation after the (n-2)-th F-function. If each value of $\sharp$ is randomly distributed form 1 to 7, the probability of getting zero difference is $(\frac{1}{7})^4$. We estimate the probability p_n of this characteristics for n-round GOST. The probability is shown as follows when n is even[2].

$$p_n = p_{S_3}^{\frac{n}{2}-1} \times p_{S_6}^{\frac{n}{2}-2} \times p_{S_1}^{\frac{n}{2}-2} \times p_{S_4}^{\frac{n}{2}-3} \times p_{S_7}^{\frac{n}{2}-3} \times p_{S_2}^{\frac{n}{2}-4} \times p_{S_5}^{\frac{n}{2}-4} \times p_{S_8}^{\frac{n}{2}-5} \times \left(\frac{1}{7}\right)^4. \quad (2)$$

S/N-ratio is defined as follows[8].

$$S/N = \frac{2^k \times p}{\alpha \times \beta}.$$

$k =$ number of key bits we are looking for
$p =$ probability of characteristics
$\alpha =$ average count of keys per analyzed pair
$\beta =$ ratio of analyzed pairs to all pairs

In this 2-Round attack each value is described as follows[3].

$$k = 32, \quad \alpha = 1, \quad \beta = 2^{-20}$$

Consequently we get

$$S/N = p_n \times 2^{52}. \quad (3)$$

Table 1 shows the estimated values of p, S/N, and the number of chosen plaintexts needed. If we choose a structure of 2^3 plaintexts which differ only at 3 bits of P_L($\sharp$ in Figure 3), one structure proposes 28 pairs of plaintexts. For example 2^{45} plaintexts propose about 2^{47} pairs. In the case of the keys which make the probability of differential characteristics the highest, p_{17} equals 1.6×2^{-49} and 17-round GOST can be attacked.

5 A Related-Key Attack

A related-key attack were first described in [5]. John Kelsey et al. proposed related-key attack of GOST[6]. But no concrete characteristics was revealed. In

[2] When n is odd the probability is shown in a similar way
[3] 20 bits of C_R are fixed to zero, so $\beta = 2^{-20}$. All bits of $C_L \oplus F_n(C_R)$ are fixed to zero, so $\alpha = 1$

Table 1. Estimates of pairs needed for differential attack

Rounds	Prob.	S/N	Chosen Plaintexts
12	1.2×2^{-44}	2^8	2^{45}
13	1.7×2^{-50}	7	2^{51}
14	1.5×2^{-55}	0.4	impossible

Table 2. Estimates of pairs needed for related-key attack

Rounds	Prob.	S/N	Chosen Plaintexts
20	1.8×2^{-47}	1.8×2^5	2^{49}
21	1.3×2^{-52}	1.3	2^{56}
22	1.1×2^{-57}	2^{-5}	impossible

this section the differential cryptanalysis mentioned in Section 4.2 is expanded with combining related-key attack, and the concrete characteristics are shown. Two unknown related keys K and K^* are used for attack. The relationship between two keys are described as follows.

$$K = (k_1, k_2, \cdot\cdot, k_8)$$
$$K^* = (k_1 \oplus 80000000_x, k_2, \cdot\cdot, k_8)$$

Using plaintext $P = (P_L, P_R)$ for key K and $P^* = (P_L \oplus 00000700_x, P_R)$ for key K^*, we can bypass the first 8 rounds for free with probability $\frac{1}{4}$ [4]. Figure 4 shows the differential characteristics using related-key attack.

In round 9 output difference is $00000\sharp00_x$ with probability $\frac{3}{4}$. After round 10 the differential characteristics are the same as described in Section 4.2. Consequently the probability of the differential characteristics of n-round GOST is $\frac{1}{4} \times \frac{3}{4} \times p_{n-8}$. Where p_{n-8} is calculated from equation (2).

Table 2 shows the estimated values of p, S/N, and the number of chosen plaintexts needed for attack.

6 In the Case of Random S-Boxes

The S-boxes are not specified in GOST. In this section we discuss the attack in the case of random S-boxes. We have generated 100,000 of random S-boxes, and obtained the $Prob\{$nonzero difference whose MSB is $0 \rightarrow$ nonzero difference whose LSB is $0\}$. Table 3 shows the probability, corresponding ratio of the number of S-boxes, and the number of rounds we can attack. On average 12 rounds of GOST can be attacked with a set of differential characteristics.

Next we consider the case of the analysis with combining related-key attack. The best characteristic in round 1 to bypass the first 8 rounds for free varies from

[4] $(k_1 \oplus 80000000_x) + P_R = k_1 + (P_R \oplus 80000000_x)$. So this probability is equal to $Prob\{8_x \rightarrow e_x\}$. For all values of k_1 this probability of S_8 is $\frac{1}{4}$

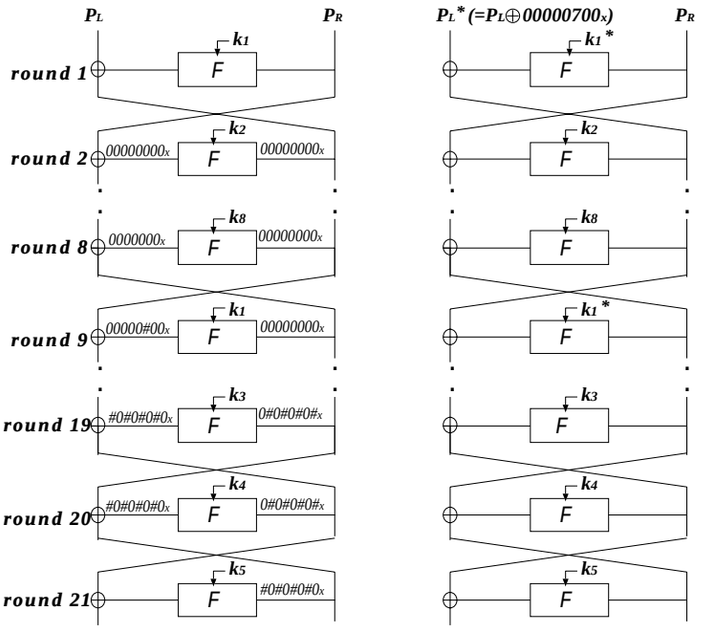

Fig. 4. The differential characteristics with related key

Table 3. Estimates in the case of random S-boxes

Prob	0.34≤	0.38≤	0.42≤	0.47≤	0.50≤	0.54≤	0.625
Ratio(%)	62	27	8	2.3	0.5	0.4	
Rounds (differential)	12	13	14	15	16	17 ∼ 20	20
Rounds (related-key)	19	20	21	22	23	24 ∼ 26	27

the S-box construction. But we can always find the characteristic which has the probability larger than $\frac{1}{8}$. So we use this probability for every S-boxes here. On average 19 rounds of GOST can be attacked with combining related-key attack.

The maximum probability of all random S-boxes[5] is 0.625. In this case 20 rounds of GOST can be attacked using a set of differential characteristics, and 27 rounds of GOST can be attacked with combining related-key attack.

Consequently this set of differential characteristics is useful even if S-boxes are randomly generated.

7 Conclusion

In this paper we described the first result of an attack on GOST with reduced number of rounds using a set of differential characteristics, which is a partitioning

[5] The S-box which has the maximum probability is {9,7,5,1,11,15,3,13,0,4,12,10,14,8,2,6}

type. In the case of S-boxes used in an application for the Central Bank of the Russian Federation, on average using 2^{51} chosen plaintexts the key of 13-round GOST can be obtained. In the case of the keys which make the probability of differential characteristics the highest, 17-round GOST can be attacked. The analysis is also expanded with combining related-key attack. Using 2^{56} chosen plaintexts the key of 21-round GOST can be obtained.

We also show this attack is applicable, even if the S-boxes are randomly generated. On average 12 rounds of GOST can be attacked with a set of differential characteristics, and 19 rounds of GOST can be attacked with combining related-key attack. In the case of the weakest S-box 20 rounds of GOST can be attacked with a set of differential characteristics, and 27 rounds of GOST can be attacked with combining related-key attack.

Appendix A: S-Boxes

A set of S-boxes used in an application for the Central Bank of the Russian Federation are given in page 333 of [7].

S_8 = {1,15,13,0,5,7,10,4,9,2,3,14,6,11,8,12}
S_7 = {13,11,4,1,3,15,5,9,0,10,14,7,6,8,2,12}
S_6 = {4,11,10,0,7,2,1,13,3,6,8,5,9,12,15,14}
S_5 = {6,12,7,1,5,15,13,8,4,10,9,14,0,3,11,2}
S_4 = {7,13,10,1,0,8,9,15,14,4,6,12,11,2,5,3}
S_3 = {5,8,1,13,10,3,4,2,14,15,12,7,6,0,9,11}
S_2 = {14,11,4,12,6,13,15,10,2,3,8,1,0,7,5,9}
S_1 = {4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3}

Appendix B: An Example of Dependence of Differential Probability on the Key

The table below shows the $Prob\{8_x \rightarrow 2_x\}$ of S_1, $Prob\{1_x \rightarrow a_x\}$ of S_4, $Prob\{5_x \rightarrow 1_x\}$ of S_7 used in an application for the Central Bank of the Russian Federation. The key values in the table are 4 bits of the round-key whose bit positions are corresponding to each S-box. We don't count the case in which differential carry bit occurs to the fourth position, because carry bit doesn't hold the input difference of upper S-box to be zero. This table shows that the probability becomes zero for more than half of the key space.

key	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S_7	0	.13	0	.25	0	.13	0	0	0	.13	0	.25	0	.13	0	0
S_4	.38	0	.38	0	.38	0	.38	0	.38	0	.38	0	.38	0	.38	0
S_1	.13	0	0	0	0	0	0	0	0	.13	.13	.13	.13	.13	.13	.13

Appendix C: Differential Distribution Table of Each S-Box

This table shows $Prob\{$nonzero difference whose MSB is $0 \rightarrow$ nonzero difference whose LSB is $0\}$ of each S-box used in an application for the Central Bank of the Russian Federation. We don't count the case in which differential carry bit to the fourth position occurs, because carry bit doesn't hold the input difference of upper S-box to be zero.

key	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	average p_{S_i}
S_8	.46	.46	.43	.43	.43	.46	.46	.46	.46	.46	.43	.43	.43	.46	.46	.46	.45
S_7	.75	.55	.43	.36	.39	.38	.43	.55	.75	.55	.43	.36	.39	.38	.43	.55	.47
S_6	.43	.39	.32	.30	.32	.32	.36	.39	.43	.39	.32	.30	.32	.32	.36	.39	.35
S_5	.46	.39	.36	.32	32	.32	.36	.43	.46	.39	.36	.32	32	.32	.36	.43	.37
S_4	.46	.38	.36	.32	.39	.32	.36	.39	.46	.38	.36	.32	.39	.32	.36	.39	.37
S_3	.43	.39	.32	.32	.32	.32	.43	.39	.43	.39	.32	.32	.32	.32	.43	.39	.37
S_2	.46	.43	.36	.36	.32	.38	.36	.38	.46	.43	.36	.36	.32	.38	.36	.38	.38
S_1	.57	.55	.43	.36	.39	.36	.36	.43	.57	.55	.43	.36	.39	.36	.36	.43	.43

References

1. GOST, Gosudarstvennyi Standard 28147-89, *"Cryptographic Protection for Data Processing Systems"*, Government Committee of the USSR for Standards, 1989.
2. L.R.Knudsen, *"Truncated and higher order differentials"*, FSE'94, Lecture Notes in Computer Science , pp.196-211, Springer-Verlag, 1994.
3. L.R.Knudsen,T.A.Berson, *"Truncated Differentials of SAFER"*, FSE'96, Lecture Notes in Computer Science , pp.15-26, Springer-Verlag, 1996.
4. J.Borst,L.R.Knudsen,V.Rijmen, *"Two Attacks on Reduced IDEA"*, Eurocrypt'97, Lecture Notes in Computer Science , pp.1-13, Springer-Verlag, 1997.
5. E.Biham, *"New Types of Cryptanalytic Attacks Using Related Keys"*, Eurocrypt'93, Lecture Notes in Computer Science , pp.398-409, Springer-Verlag, 1993.
6. J.Kelsey, B.Shneier, D.Wagner, *"Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES"*, CRYPTO'96 Proceedings, Spring-Verlag, 1996, pp.237- 251.
7. B.Shneier, *"Applied Cryptography"*, John Wiley & Sons, pp. 331-334.
8. E.Biham, A.Shamir., *"Differential Cryptanalysis of DES-like Cryptosystems,"* Journal of Cryptology 1991.