Fixed Points of Special Type and Cryptanalysis of Full GOST*

Orhun Kara[1] and Ferhat Karakoç[1,2]

[1] TÜBİTAK BİLGEM UEKAE
National Research Institute of Electronics and Cryptology
Gebze 41470 Kocaeli/Turkey
{orhun.kara,ferhat.karakoc}@tubitak.gov.tr
[2] Istanbul Technical University, Computer Engineering Department, 34469, Maslak, Istanbul/Turkey

Abstract. GOST, the Russian encryption standard, is a block cipher of 64-bit block and 256-bit key size and consists of 32 rounds. In this work, we show that the probability that the GOST permutations produced through random keys have at least one fixed point and exactly two fixed points of special type are twice and five times more than those of random permutations respectively. We utilize this property of GOST to mount a new reflection attack on full GOST.

The reflection property on GOST was defined and exploited to mount an attack on the full cipher by Kara [7] which was successful only for one out of 2^{32} keys. This property has been further studied by Courtois [1], Dinur et al. [5] and Isobe [6]. Isobe mounted an attack that works for any key with a time complexity of 2^{225} [6]. Isobe's attack was improved by Dinur et al. reducing the time complexity to 2^{192} using the whole codebook [5]. They introduce a new version of the meet-in-the-middle technique which they call "2-dimensional meet in the middle (2DMITM)" attack. Their attack is based on applying 2DMITM attack on 8-round GOST 2^{64} times. In this work, we mount an attack with time complexity of 2^{129} using 2^{32} chosen plaintexts instead of the whole codebook utilizing the 2DMITM attack. The main advantages of our attack is that we mount the 2DMITM attack on 8-round GOST only twice. On the other hand, our attack works only for the weak key set of 2^{192} keys, which indicates that the security level of full GOST is equivalent to 129 bits for these keys. In addition, we have computed the success rates of Kara attack in [7] and our attack. We have verified our calculations experimentally.

Keywords: block cipher, self similarity, reflection attack, GOST, fixed point, Feistel network.

1 Introduction

GOST, the Russian encryption standard, is a Feistel network of 64-bit block and 256-bit key size and the number of rounds is 32 [8]. It has a relatively simple key

* We would like to thank Nicolas Courtois for proposing this title to us.

J. Pieprzyk, A.-R. Sadeghi, and M. Manulis (Eds.): CANS 2012, LNCS 7712, pp. 86–97, 2012.

schedule. The key is divided into 8 parts and each part is used as a subkey, first 3 times in a direct order and then in a reversed order. This leads to a self-similarity property of the cipher which we exploit to mount a reflection attack.

Several attacks have been published recently on full GOST. The first reflection attack on full GOST exploits extending the special fixed points of the first 8 rounds that occur only for a subset of the key space, to the whole cipher [7]. The extension of these fixed points comes from the extremely simple key schedule of GOST. This attack works for 2^{224} keys with a complexity of 2^{192} encryptions by using 2^{32} chosen plaintexts. The biased distribution of fixed points through the rounds was examined in the attack which was simply called "the reflection property". The reflection property has been further exploited to mount several other attacks on GOST [1,5,6].

Recently, Isobe mounts an attack on the full cipher which works for the whole key space using the reflection property [6]. The complexity and data requirements of the attack are 2^{225} and 2^{32} respectively. Then Dinur et al. proposed an attack on the full cipher with a complexity of 2^{192} and a need of 2^{64} data [5]. In their attack, two input/output pairs for 8-round GOST are guessed using the whole codebook since each guess is correct with a probability of 2^{-64}.These two input/output pairs allow them to eliminate the possible keys to 2^{128} candidates with a cost of 2^{128} GOST encryptions with 2^{36} memory by mounting a meet in the middle type attack which they call "2-dimensional meet in the middle (2DMITM)" attack. Then, they use other pairs to check their guesses. Thus, the total time complexity of their attack is 2^{192} since the 2DMITM attack is performed 2^{64} times. The 2DMITM technique has been further improved and generalized by Zhu and Gong [9].

Courtois has proposed many different attacks on full GOST including some attacks with Misztal [4,3,2,1]. Most of his attacks are collected in [1] where he mounted several reflection and other self-similarity attacks on full GOST, some of them works on weak keys. Courtois and Misztal mounted differential attack on full GOST with a complexity of 2^{226} GOST encryptions using the whole codebook [2]. Then, Courtois himself has further improved the time complexity of a differential attack on GOST to 2^{178} [3].

In this work, we show that the probabilities of having at least one fixed point and exactly two fixed points of a special type (whose left and right parts are equal) for GOST are twice and five times more than the corresponding probabilities of random permutations respectively. Moreover, we mount an attack on full GOST with a complexity of 2^{129} encryptions using two input/output pairs for 8 rounds obtained by exploiting this non-randomness property.

In our improved attack, we make use of only 2^{32} chosen plaintext/ciphertext pairs instead of the whole codebook to construct the two pairs. If there are two fixed points having equal halves then we mount the key recovery attack. One important advantage of our attack is that two input/output pairs of 8-round GOST are known to cryptanalyst with very high probability. Therefore, we perform the 2DMITM attack typically not more than twice. However, the attack works for only 2^{192} keys. As a result, we have shown that GOST provides only 129

bit security for the weak keys. In addition, the 2DMITM attack is not performed if there isn't a pair of suitable fixed points. The complexity of the attack is only to examine the 2^{32} texts in this case. Therefore our attack gives nice results in the following realistic scenario proposed in [1]: Assume there are many distinct keys used and the attacker tries to recover some of them. Then the complexity of our attack to recover one key is $2.5 \cdot 2^{129} + (2^{64} - 2.5)2^{32} \approx 2^{130.3}$. Because, among 2^{64} keys, there is roughly one weak key and the attack is performed about 2.5 times. On the other hand, if a random number generator providing keys to GOST, produces weak keys deliberately then the security margin of GOST declines dramatically.

We have calculated the success rate of the Kara attack on full GOST which is left out in [7] and the success rate of our attack. We prove that the probability of having two fixed points with equal halves is around $5 \cdot 2^{-65}$ and we can recover the key with a probability of 40% if such two fixed points occur. We have validated these calculations by computer simulations.

The paper is organized as follows. We give a short description of GOST and the first reflection attack on it given in [7] in Section 2. The improved attack is stated in Section 3. Then, the success rates of both the first reflection attack and the improved attack are computed in Section 4 and the experimental results are depicted in Section 5. We conclude the paper in the last section with an open question.

2 A Brief Description of GOST and the First Reflection Attack

GOST, the Russian encryption standard [8], is a 32-round Feistel network with 64-bit block and 256-bit key length. It has a simple key schedule: 256 bit key is divided into eight 32 bit words $k_0, ..., k_7$ and the sequence of round keys is given as $k_0, ..., k_7, k_0, ..., k_7, k_0, ..., k_7, k_7, k_6, ..., k_1, k_0$. We do not consider details of the round function. We only assume that it is bijective. Denote the first eight rounds of GOST as $F_K[1, 8]$. Note that $F_K[1, 8]$ ends with a swap operation. Then, the GOST encryption function is given as $E_K(x) = F_K[8, 1] \circ S \circ F_K^3[1, 8](x)$ where S is the swap operation of the Feistel network and $F_K[8, 1]$ is the inverse of $F_K[1, 8]$.

The first attempt to propose a key recovery attack on full GOST was the reflection attack [7]. We briefly describe this attack in this section. Assume there exists (x, x) for $x \in GF(2)^{32}$ such that (x, x) is a fixed point $F_K[1, 8]$. Note that (x, x) is also a fixed point of the swap operation S. Then, (x, x) will be a fixed point of the encryption function E_K. This observation leads to the following attack. Encrypt all 2^{32} plaintexts whose left and right halves are equal and collect the fixed points in a set, say U_E. If U_E is empty, then the attack is not applicable. Otherwise, for any (x, x) in U_E solve the equation $F_K[1, 8](x, x) = (x, x)$ for K. Guessing $k_0, k_1, ..., k_5$, one can construct a two-round Feistel network with unknown keys k_6 and k_7 and an input/output pair given as $(F_K[1, 6](x, x), (x, x))$. Then, solving the system for k_6 and k_7 is straightforward since the round functions

F_{k_6} and F_{k_7} are bijective and their outputs are known. By taking the inverses of F_{k_6} and F_{k_7}, obtain the inputs and then k_6 and k_7. Consequently, obtain 2^{192} candidates for the key by solving $F_K[1,8](x,x) = (x,x)$. Then one can recover the correct key by searching over all the candidates by roughly 2^{192} encryptions. However, it is most likely that U_E is empty if there exists no fixed point of $F_K[1,8]$ with the equal halves. On the other hand, the expected number of fixed points is one and the probability that any arbitrary value is a fixed point of S is 2^{-32}. Hence, the number of keys satisfying that $\exists\ x$ such that $F_K[1,8](x,x) = (x,x)$ is roughly 2^{224}.

3 Improved Attack on Full GOST

We improve the Kara attack on full GOST given in [7] by exploiting the additional fixed points and using the attack idea given by Dinur et al. in [5]. Dinur et al. showed that for a given two input/output pairs for 8 rounds, the key space is diminished to 2^{128} with 2^{128} GOST encryptions using 2^{36} memory and the right key can be recovered by searching these 2^{128} by using some other plaintext/ciphertext pairs for full GOST. The total complexity is 2^{192} since the probability of finding two correct input/output pairs for the 8-round GOST is 2^{-64}. One input/output pair produces just one guess for two pairs of 8-round GOST and hence they use the whole codebook to produce a right pair overall. We give our observation finding the two pairs in Theorem 1 with much less data complexity.

Theorem 1. *Assume that* $\exists(x,x)$ *and* (y,y) *such that* $F_K[1,8](x,x) = (y,y)$ *and* $F_K[1,8](y,y) = (x,x)$ *where* x *and* y *are 32-bit values. Then* $E_K(x,x) = (x,x)$ *and* $E_K(y,y) = (y,y)$.

Proof. Remember that $E_K(x,x) = F_K[8,1] \circ S \circ F_K^3[1,8](x,x)$. Then $E_K(x,x) = F_K[8,1] \circ S \circ F_K^2[1,8](y,y) = F_K[8,1] \circ S \circ F_K[1,8](x,x) = F_K[8,1] \circ S(y,y) = F_K[8,1](y,y) = (x,x)$. The proof for the equality $E_K(y,y) = (y,y)$ is similar.

Let us note that a more generalized property than the property given in Theorem 1 has been studied in [1] to obtain four input/output pairs for 8-round GOST. The idea is based on forming two points of order two where one is the output of the other for 8-round GOST. The probability that a given pair satisfies this property is 2^{-127}. Hence, it is expected to have one such pair among all the pairs produced from the whole codebook. The nice property that these points provide is that the required pair gives two more input/output pairs for 8-round GOST. These pairs are formed by the completion of two points with their corresponding ciphertexts. The main difference which gives us an advantage in reducing the complexity of our attack is that four input/output pairs are not known to the attacker in [1]. She has to try each pair as a candidate. However, in the case given in Theorem 1, the attacker most probably knows which plaintext/ciphertext pairs give two input/output pairs for 8-round GOST. We give these pairs a special name since we use it through the paper.

Definition 1. *Let us call that a given pair* $((x,x),(y,y))$ *satisfies Event-1 if* $F_K[1,8](x,x) = (y,y)$ *and* $F_K[1,8](y,y) = (x,x)$*; and similarly* $((x,x),(y,y))$ *satisfies Event-2 if the points* (x,x) *and* (y,y) *are fixed points of* $F_K[1,8]$.

Let us recall that similar to Theorem 1, we can state that a fixed point (x,x) of F_K is also a fixed point for E_K. This is because (x,x) is also a fixed point of both F_K^{-1} and the swap operation.

The probability of Event-1 for a pair $((x,x),(y,y))$ where $x \neq y$ is $\frac{1}{2^{64}(2^{64}-1)}$. For a fixed key, the probability that there exists one pair satisfying Event-1 is roughly 2^{-65} since there are approximately 2^{63} such pairs. Thus, only about $2^{256-65} = 2^{191}$ keys will produce pairs satisfying Event-1 that means we can find two pairs for 8 rounds for 2^{191} keys. We expect roughly 2^{191} more keys that satisfy Event-2 (none of them do not satisfy Event-1 most probably). So, there are approximately 2^{192} weak keys in total.

The attack works as follows. Get the encryptions of 2^{32} possible (x,x)'s checking fix points. If there are two fixed points then these are most probably caused due to either Event-1 or Event-2. Each event provides two input/output pairs for 8-round GOST. The attacker checks if full GOST has two fixed points of form (x,x) and (y,y), and if so, he applies the 2DMITM attack by Dinur et al. for the resulting input/output pairs for 8 rounds which are $((x,x),(y,y))$ and $((y,y),(x,x))$ with time 2^{128} and 2^{36} of memory. This produces 2^{128} candidates for the key which are then filtered by checking with 2-3 additional plaintext/ciphertext pairs for full GOST. If this is not successful then one needs to run the 2DMITM attack once more this time with the input/output pairs $((x,x),(x,x))$ and $((y,y),(y,y))$ for 8-round GOST. Thus the number of keys which subject to this attack and the time complexity of the attack will be 2^{192} and 2^{129} respectively.

The probability that full GOST has two fixed points of the form (x,x) is approximately $5 \cdot 2^{-65}$ whereas the probability that a random permutation of 64-bit block length has two fixed points of the form (x,x) is approximately 2^{-65}. The detailed calculations are given in Section 4.

4 Success Rates of the Attacks

In this section we give the success rates of both the Kara attack in [7] and our improved attack. By the success rate we mean the ratio of the number of the successful key recoveries among all the key recovery attempts. Hence, it is the probability that F_K has a fixed point of the form (x,x) when full GOST has a fixed point of the form (x,x) for the Kara attack and the probability of having a pair $((x,x),(y,y))$, where $x \neq y$, satisfying Event-1 or Event-2 when (x,x) and (y,y) are fixed points of full GOST for the improved attack.

4.1 Success Rate of the First Reflection Attack on Full GOST

The success rate of the attack on full GOST is left out in [7]. Indeed, if the function $F_K[1,8]$ has a fixed point of the form (x,x) where the former half of

the input is equal to its latter half, it is definitely a fixed point of the encryption function E_K. Nevertheless, the attack makes use of the opposite direction of the statement. That is, the attack is mounted if there is a fixed point of E_K, assuming that it is (probably) a fixed point for also $F_K[1,8]$. In this section, we examine this direction and find the probability that any fixed point of E_K is also a fixed point of $F_K[1,8]$. Let us remark that the attack is not successful for those fixed points of E_K which are not fixed points of $F_K[1,8]$.

Let the set of the fixed points of the form (x,x) of $F_K[1,8]$ be U_F. Recall that U_E is the set of the fixed points of E_K of the form (x,x). Then, the success rate, $\Pr(S)$, of the attack is given as the conditional probability that U_F is nonempty given that U_E is nonempty. That is, $\Pr(S) = \Pr(U_F \neq \emptyset | U_E \neq \emptyset)$. The following statement gives the success rate explicitly.

Theorem 2. *Assume the encryption function E_K behaves randomly when the function F_K has no fixed point of the form (x,x). Then, the probability that U_F is nonempty given that U_E is nonempty is*

$$\Pr(S) = \Pr(U_F \neq \emptyset | U_E \neq \emptyset) = \frac{1}{1+(1-2^{-64})^{2^{32}}} \approx \frac{1}{2-2^{-32}}.$$

Proof. We have $\Pr(S) = \Pr(U_F \neq \emptyset | U_E \neq \emptyset)$ which leads to $\Pr(S) = \frac{\Pr(U_F \neq \emptyset)}{\Pr(U_E \neq \emptyset)}$ since U_F is a subset of U_E. On the other hand $\Pr(U_F \neq \emptyset) = 1-(1-2^{-64})^{2^{32}}$ and $\Pr(U_E \neq \emptyset)$ is given as $\Pr(U_F \neq \emptyset) + \Pr(U_F = \emptyset)\Pr(U_E \neq \emptyset)|U_F = \emptyset)$. Assuming that E_K is a random function when F_K has no fixed point of the form (x,x), we have $\Pr(U_E \neq \emptyset)|U_F = \emptyset) = 1-(1-2^{-64})^{2^{32}}$. Hence, we calculate $\Pr(U_E \neq \emptyset)$ as $1-(1-2^{-64})^{2^{32}} + (1-2^{-64})^{2^{32}}(1-(1-2^{-64})^{2^{32}})$ which yields to the probability

$$\Pr(S) = \Pr(U_F \neq \emptyset | U_E \neq \emptyset) = \frac{1-(1-2^{-64})^{2^{32}}}{(1-(1-2^{-64})^{2^{32}})(1+(1-2^{-64})^{2^{32}})}.$$

For the Kara attack, the key recovery attempt is successful if U_F is nonempty and hence the probability given in Theorem 2 gives the success rate of the key recovery part of the attack. Let us remark that the success rate is very close to one half since the value $(1-2^{-64})^{2^{32}}$ is roughly $1-2^{-32}$. One interesting result is that assuming that the encryption permutation E_K behaves randomly when the function F_K has no fixed point of the form (x,x), then E_K does not behave as a random permutation because the probability that U_E is not empty is twice as large as the probability for a random permutation. Note that the probability that a random permutation has at least one fixed point of the form (x,x) is $1-(1-2^{-64})^{2^{32}}$. The following corollary states this phenomena formally.

Corollary 1.

$$\Pr(U_E \neq \emptyset) = (1-(1-2^{-64})^{2^{32}})(1+(1-2^{-64})^{2^{32}}) \approx 2(1-(1-2^{-64})^{2^{32}}).$$

which is roughly 2^{-31}.

4.2 Success Rate of Improved Attack

Similarly, we compute the success rate of the improved attack given in Section 3. The key recovery part of the attack is performed if there exists (at least) two symmetric fixed points for the encryption function. The attack is mounted by assuming that the fixed points are due to the existence of (x, x) and (y, y) such that $F_K[1, 8](x, x) = (y, y)$ and $F_K[1, 8](y, y) = (x, x)$ (Event-1) or the existence of two fixed points of $F_K[1, 8]$ (Event-2). However, there is a probability that two fixed points may occur by chance also. That is, E_K may have two fixed points of the symmetric form whereas neither Event-1 nor Event-2 happened. In this case the key recovery attack will not be successful.

Recall that we simple call the success rate of the attack as the ratio of the attempts where the keys are recovered over all the attempts. Hence, it is the ratio of the probability of having a pair $((x, x), (y, y))$ which satisfies Event-1 or Event-2 over the probability of having two fixed points of the form (x, x) for the encryption function E_K. Because we attempt to recover the key when there are two symmetric fixed points for full GOST and we get exactly two input/output pairs for 8-round GOST when these fixed points satisfy Event-1 or Event-2. We derive this ratio in the following statements. We also show that the probability of having two symmetric fixed points for E_K is five times more then the probability of having two symmetric fixed points for a random permutation of the same size.

Lemma 1. *The probability that a given pair $((x, x), (y, y))$, where $x \neq y$, satisfies Event-1 or Event-2 is*

$$\frac{1}{2^{63}(2^{64} - 1)}.$$

Proof. Let us recall that Event-1 is the event that $F_K[1, 8](x, x) = (y, y)$ and $F_K[1, 8](y, y) = (x, x)$. The probability that a given pair $(x, x), (y, y)$ satisfies Event-1 where $x \neq y$ is

$$\frac{1}{2^{64}(2^{64} - 1)}$$

since the probability that $F_K[1, 8](x, x) = (y, y)$ is 2^{-64} and the probability that $F_K[1, 8](y, y) = (x, x)$ provided that $F_K[1, 8](x, x) = (y, y)$ is $(2^{64} - 1)^{-1}$. Similarly, the probability that the pair $(x, x), (y, y)$ satisfies Event-2 is

$$\frac{1}{2^{64}(2^{64} - 1)}.$$

On the other hand the pair $((x, x), (y, y))$ cannot satisfy both Event-1 and Event-2 simultaneously since $x \neq y$. Hence, the probability that $((x, x), (y, y))$ satisfies Event-1 or Event-2 is

$$2 \cdot \frac{1}{2^{64}(2^{64} - 1)} = \frac{1}{2^{63}(2^{64} - 1)}.$$

The following lemma gives the probability that any given two symmetric points are the fixed points for full GOST. This probability is about five times more than the probability for the random case.

Lemma 2. *For a given pair* $((x,x),(y,y))$ *where* $x \neq y$*, the probability that* $E_K(x,x) = (x,x)$ *and* $E_K(y,y) = (y,y)$ *is given as*

$$\frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} - \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2}.$$

Proof. The probability that $E_K(x,x) = (x,x)$ and $E_K(y,y) = (y,y)$ can be evaluated when $((x,x),(y,y))$ satisfies Event-1 or Event-2 and when $((x,x),(y,y))$ satisfies neither Event-1 nor Event-2. Hence the probability is given as

$$1 \cdot \frac{1}{2^{63}(2^{64}-1)} + \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} \cdot \left(1 - \frac{1}{2^{63}(2^{64}-1)}\right)$$

since both (x,x) and (y,y) are the fixed points of E_K when $((x,x),(y,y))$ satisfies Event-1 or Event-2 and the probability that both (x,x) and (y,y) are the fixed points of E_K is

$$\frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)}$$

otherwise. Let us recall that if neither Event-1 nor Event-2 happened then we have either (x,x) is a fixed point of F_K and (y,y) is not a fixed point of F_K or vice versa ((x,x) is not a fixed point of F_K and (y,y) is a fixed point of F_K) or none of them are fixed points of F_K. The probability that they both are fixed points of E_K in all three cases is

$$\frac{1-2^{-64}}{2^{64}(2^{64}-1)} + \frac{1-2^{-64}}{2^{64}(2^{64}-1)} + \frac{(1-2^{-64})^2}{2^{64}(2^{64}-1)} = \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)}.$$

The probability of satisfying Event-1 or Event-2 is taken from Lemma 1. Then, if we add all the probabilities we obtain the probability that both the points are the fixed points of E_K as

$$\frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} - \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2}.$$

The following theorem is the main statement of this section. It shows the nonrandom selection process of GOST permutations in terms of having two symmetric fixed points and gives the success rate of the improved attack.

Theorem 3. *For a randomly chosen key* K*, the encryption function* E_K *of GOST has the following properties:*

- *The probability that* E_K *has two fixed points of the form* (x,x) *is given as*

$$2^{31}(2^{32}-1) \cdot \left(\frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} - \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2}\right) \cdot \left(1 - \frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} + \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2}\right)^{2^{31}(2^{32}-1)-1}$$

  which is approximately $5 \cdot 2^{-65}$.

– *Assume there are two fixed points of E_K of the form (x, x) for some K. Then the probability that these fixed points satisfy either Event-1 or Event-2 is*

$$\left(1 + \frac{2^{64}-1}{2^{64}} + \frac{(1-2^{-64})^2}{2} - \frac{1}{2^{127}} - \frac{(1-2^{-64})^2}{2^{128}}\right)^{-1} \approx 0.40.$$

Proof. We prove the statements as we have itemized them.

– The probability that a given pair $((x, x), (y, y))$ forms two fixed points of E_K where $x \neq y$ is given by Lemma 2 as

$$\frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} - \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2}.$$

On the other hand, for a fixed key, there are $\binom{2^{32}}{2}_1 = 2^{31}(2^{32}-1)$ pairs $((x, x), (y, y))$ that can be produced from the symmetric points. We expect just one pair to satisfy the fixed point condition. Hence the probability is derived.

For the approximation, we have $2^{31}(2^{32}-1) \approx 2^{63}$,

$$\frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} - \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2} \approx \frac{5}{2^{128}}$$

and

$$\begin{aligned}(1 - \frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} + \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2})^{2^{31}(2^{32}-1)-1}\\ \approx (1 - \frac{5}{2^{128}})^{2^{63}} \approx \exp(-5/2^{65}) \approx 1 - \frac{5}{2^{65}} \approx 1\end{aligned}$$

and hence if we combine all these approximations we have the probability approximately $5 \cdot 2^{-65}$.

– The probability that a given pair $((x, x), (y, y))$ satisfies Event-1 or Event-2 given that the pair $((x, x), (y, y))$ forms two fixed points for E_K is given as the ratio of the probability that a given pair $((x, x), (y, y))$ satisfies Event-1 or Event-2 over the probability that the pair forms two fixed points of E_K since if the pair $((x, x), (y, y))$ satisfies Event-1 or Event-2 then both (x, x) and (y, y) are the fixed points of E_K. On the other hand, the ratio is given as the inverse of the ratio

$$2^{63}(2^{64}-1)\left(\frac{2 + 2(1-2^{-64}) + (1-2^{-64})^2}{2^{64}(2^{64}-1)} - \frac{2(1-2^{-64}) + (1-2^{-64})^2}{2^{127}(2^{64}-1)^2}\right)$$

which is equal to

$$1 + \frac{2^{64}-1}{2^{64}} + \frac{(1-2^{-64})^2}{2} - \frac{1}{2^{127}} - \frac{(1-2^{-64})^2}{2^{128}}.$$

Let us remark that this ratio is close to 2.5 since $\frac{2^{64}-1}{2^{64}} \approx 1$, $\frac{(1-2^{-64})^2}{2} \approx 0.5$ and $\frac{1}{2^{127}} + \frac{(1-2^{-64})^2}{2^{128}} \approx 0$. Hence the probability is approximately 0.40.

Let us remark that the probability that two symmetric fixed points of E_K satisfy Event-1 or Event-2 is equivalent to success rate of the key recovery part of the improved attack. Hence the success rate of the improved attack is approximately 40%. Also remark that the probability that E_K has two fixed points of the form (x, x) is roughly $5 \cdot 2^{-65}$ which is 5 times more then that of random permutations. Note that the probability that a random permutation has two fixed points among 2^{32} points of the form (x, x) is approximately 2^{-65} (see Appendix). Hence we derive a distinguisher for the selection process of random permutations through the GOST encryption by random keys.

5 Experimental Results

In this section we show the experimental results for both the Kara attack and the improved attack.

We have computed the success rates and the probabilities of having symmetric fixed points for minimized versions of GOST with block sizes of 16, 20, 24 and 28-bit lengths for the Kara attack and 12, 16, and 20-bit lengths for the improved attack. The number of rounds is fixed to 32 for any block length and we use $n \times 8$-bit key for the n-bit block length. The key is divided into 8 equal parts $k_0, ..., k_7$ and incorporated into the round function as for the original GOST function. The experimental results verify our statements in Theorem 2 and Theorem 3.

Table 1. The expected # of fixed points and weak keys are 3200 and 1600 respectively

Block length	# of keys	# of keys with symmetric fixed points of GOST	# of weak keys	Success rate
16 bits	100×2^{12}	3153	1556	0.493
20 bits	100×2^{14}	3255	1618	0.497
24 bits	100×2^{16}	3193	1598	0.501
28 bits	100×2^{18}	3229	1588	0.492

The expected number of fixed points of the form (x, x) for the encryption is fixed to 3200 and the expected number of weak keys is fixed to 1600 for the first experiment. The experimental results verify our statements for the Kara attack as depicted in Table 1. We have seen that the probability of having at least one symmetric fixed point for full GOST is roughly $2^{1-n/2}$ (the third column divided by the second column) and the probability that it is caused by having fixed point in 8-round GOST is around 50% where n is the block length.

We perform another set of experiments for the improved attack. The results are depicted in Table 2 which go along with the theoretical statements. We scan $2^{21}, 2^{25}$ and 2^{28} keys randomly for 12, 16 and 20-bit block lengths respectively. We count the number of keys which produce two fixed points of the form (x, x) for the encryption function E_K and keys which produce pairs $((x, x), (y, y))$ satisfying Event-1 or Event-2 which give weak keys. We have seen that the

Table 2. The expected number of keys which have two fixed points

Block length	# of keys	# of keys with two symmetric fixed points of GOST	# of weak keys	Success rate
12-bit	2^{21}	1228	526	0.428 %
16-bit	2^{25}	1312	533	0.406 %
20-bit	2^{28}	675	267	0.395 %

probability that GOST has two symmetric fixed points is around $5 \cdot 2^{1-n}$ (the third column divided by the second column) and the success rate is roughly 40%.

6 Conclusion

We show that the probabilities that a randomly chosen GOST permutation has a fixed point and two fixed points of special type are twice and five times more than those of a random permutation respectively. This allowed us to propose a new attack in which the reflection property introduced by Kara occurs twice. Our attack has a time complexity of 2^{129} encryptions and requires only 2^{32} chosen plaintexts in order to break GOST for a subset of the key space of size approximately 2^{192}. Let us remark that 2^{32} data is used to identify if the key is weak. One can note that given 2^{32} of data we can see if the key is weak very efficiently.

The open question is how to efficiently enumerate the set of weak keys. If it is possible to produce weak keys by a polynomial time algorithm then an intentionally weak protocol having a random number generator which provides weak keys to GOST can decrease the security margin of GOST to 129 bits even though the key length is 256 bits. In addition, we have calculated the success probabilities of the attacks given in [7] and our attack. We have validated these calculations by computer simulations.

Acknowledgments. We would like to thank the anonymous reviewers for their invaluable comments. In particular, we greatly appreciate the interest shown by Nicolas Courtois in our work. The quality of the presentation of the work has been improved by his detailed comments.

This work is supported by the project COGSA.

References

1. Courtois, N.T.: Algebraic Complexity Reduction and Cryptanalysis of GOST. IACR Cryptology ePrint Archive, 2011:626 (2011)
2. Courtois, N.T., Misztal, M.: Differential Cryptanalysis of GOST. IACR Cryptology ePrint Archive, 2011:312 (2011)
3. Courtois, N.T.: A Differential Attack on Full GOST. IACR Cryptology ePrint Archive, 2012:138 (2012)

4. Courtois, N.T.: Security Evaluation of GOST 28147-89 in View of International Standardisation. Cryptologia 36(1), 2–13 (2012)
5. Dinur, I., Dunkelman, O., Shamir, A.: Improved Attacks on Full GOST. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 9–28. Springer, Heidelberg (2012)
6. Isobe, T.: A Single-Key Attack on the Full GOST Block Cipher. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 290–305. Springer, Heidelberg (2011)
7. Kara, O.: Reflection Cryptanalysis of Some Ciphers. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 294–307. Springer, Heidelberg (2008)
8. Zabotin, I.A., Glazkov, G.P., Isaeva, V.B.: Cryptographic Protection for Information Processing Systems. Cryptographic Transformation Algorithm. Government Standard of the USSR, GOST 28147-89 (1989)
9. Zhu, B., Gong, G.: Multidimensional Meet-in-the-Middle Attack and Its Applications to GOST, KTANTAN and Hummingbird-2. Cryptology ePrint Archive, Report 2011/619 (2011), http://eprint.iacr.org/

A The Probability of Having Two Symmetric Fixed Points of Random Permutations

In this section we show the probability that a random permutation of 64-bit block length has two fixed points.

Theorem 4. *The probability that a random permutation of 64-bit block length has two fixed points of the form* (x, x) *is given as*

$$2^{31}(2^{32}-1)\cdot\left(\frac{1}{2^{64}(2^{64}-1)}\right)\left(1-\frac{1}{2^{64}(2^{64}-1)}\right)^{2^{31}(2^{32}-1)-1}$$

which is approximately 2^{-65}.

Proof. For a random permutation of 64-bit block length, the probability that given two distinct symmetric points are fixed points is given as

$$\frac{1}{2^{64}(2^{64}-1)}$$

and hence among $2^{31}(2^{32}-1)$ pairs, the probability that just one pair forms fixed points is

$$2^{31}(2^{32}-1)\cdot\left(\frac{1}{2^{64}(2^{64}-1)}\right)\left(1-\frac{1}{2^{64}(2^{64}-1)}\right)^{2^{31}(2^{32}-1)-1}.$$

For the approximation we can deduce similarly that $\frac{1}{2^{64}(2^{64}-1)} \approx 2^{-128}$ and

$$(1-\frac{1}{2^{64}(2^{64}-1)})^{2^{31}(2^{32}-1)-1} \approx \exp(-2^{-65}) \approx 1-\frac{1}{2^{65}} \approx 1$$

and hence the probability will be approximately 2^{-65}.