# A Single-Key Attack on the Full GOST Block Cipher

Takanori Isobe

Sony Corporation
1-7-1 Konan, Minato-ku, Tokyo 108-0075, Japan
Takanori.Isobe@jp.sony.com

**Abstract.** The GOST block cipher is the Russian encryption standard published in 1989. In spite of considerable cryptanalytic efforts over the past 20 years, a key recovery attack on the full GOST block cipher without any key conditions (*e.g.*, weak keys and related keys) has not been published yet. In this paper, we show a first single-key attack, which works for all key classes, on the full GOST block cipher. To construct the attack, we develop a new attack framework called *Reflection-Meet-in-the-Middle Attack*. This approach combines techniques of the reflection attack and the meet-in-the-middle attack. We apply it to the GOST block cipher with further novel techniques which are the effective MITM techniques using equivalent keys on short rounds. As a result, a key can be recovered with $2^{225}$ computations and $2^{32}$ known plaintexts.

**Keywords:** block cipher, GOST, single-key attack, reflection attack, meet-in-the-middle attack, equivalent keys.

## 1 Introduction

The GOST block cipher [22] is known as the former Soviet encryption standard GOST 28147-89 which was standardized as the Russian encryption standard in 1989. It is based on a 32-round Feistel structure with 64-bit block and 256-bit key size. The round function consists of a key addition, eight $4 \times 4$-bit S-boxes and a rotation. Since values of S-boxes are not specified in the GOST standard [22], each industry uses a different set of S-boxes. For example, one of the S-boxes used in the Central Bank of the Russian Federation is known as in [27].

The GOST block cipher is well-suited for compact hardware implementations due to its simple structure. Poschmann *et al.* showed the most compact implementation requiring only 651 GE [24]. Therefore, the GOST block cipher is considered as one of ultra lightweight block ciphers such as PRESENT [6] and KATAN family [8], which are suitable for the constrained environments including RFID tags and sensor nodes. Note that for the remainder of this paper we refer to the GOST block cipher as GOST.

Over the past 20 years, several attacks on GOST have been published. A differential attack on 13-round GOST was proposed by Seki and Kaneko [28]. In the related-key setting, an attack is improved up to 21 rounds. Ko *et al.* showed

A. Joux (Ed.): FSE 2011, LNCS 6733, pp. 290–305, 2011.

**Table 1.** Key recovery attack on GOST

| Key setting | Type of attack | Round | Complexity | Data | Paper |
|---|---|---|---|---|---|
| Single key | Differential | 13 | Not given | $2^{51}$ CP | [28] |
| | Slide | 24 | $2^{63}$ | $2^{63}$ ACP | [2] |
| | Slide | 30 | $2^{253.7}$ | $2^{63}$ ACP | [2] |
| | Reflection | 30 | $2^{224}$ | $2^{32}$ KP | [17] |
| | Reflection-Meet-in-the-Middle | 32 | $2^{225}$ | $2^{32}$ KP | **This paper** |
| Single key (Weak key) | Slide ($2^{128}$ weak keys) | 32 | $2^{63}$ | $2^{63}$ ACP | [2] |
| | Reflection ($2^{224}$ weak keys) | 32 | $2^{192}$ | $2^{32}$ CP | [17] |
| Related key | Differential | 21 | Not given | $2^{56}$ CP | [28] |
| | Differential† | 32 | $2^{244}$ | $2^{35}$ CP | [19] |
| | Boomerang ‡ | 32 | $2^{248}$ | $2^{7.5}$ CP | [15] |

CP : Chosen plaintext, ACP : Adaptive chosen plaintext, KP : Known plaintext.

† The attack can recover 12 bits of the key with $2^{36}$ computations and $2^{35}$ CP.

‡ The attack can recover 8 bits of the key with $2^{7.5}$ computations and $2^{7.5}$ CP.

a related-key differential attack on the full GOST [19]. These results work on only the GOST that employs the S-boxes of the Central Bank of the Russian Federation [27]. Fleischmann *et al.* presented a related-key boomerang attack on the full GOST which works for any S-boxes [15]. As other types of attacks, Biham *et al.* showed slide attacks on the reduced GOST [2]. Their attack utilizes self similarities among round functions of the encryption process, and does not also depend on used values of S-boxes. Even if an attacker does not know the values of S-boxes, the 24-round GOST can be attacked by this approach. If the values are known, this attack can be improved up to 30 rounds. In addition, for a class of $2^{128}$ weak keys, the full GOST can be attacked by this approach. After that, Kara proposed a reflection attack on 30-round GOST [17]. This attack also uses self similarities among round functions, and works for any bijective S-boxes. The difference from the slide attack proposed by Biham *et al.* [2] is to use similarities of both encryption and decryption processes. The reflection attack utilizes these similarities in order to construct fixed points of some round functions. Moreover, for a class of $2^{224}$ weak keys, the full GOST can be attacked by using the reflection technique.

In spite of considerable cryptanalytic efforts, a key recovery attack on the full GOST without any key assumptions (*e.g.*, weak keys and related keys) has not been published so far. Furthermore, a weak-key attack and a related-key attack are arguable in the practical sense, because of their strong assumptions. A weak-key attack is generally applicable to very few keys, *e.g.*, in the attack of [17], the rate of weak keys is $2^{-32}(= 2^{224}/2^{256})$. Hence, almost all keys, $(2^{256} - 2^{224}) \approx 2^{256}$ keys, can not be attacked by [17]. Besides, the attacker can not

even know whether a target key is included in a weak key class or not. A related-key attack assumes that the attacker can access to the encryption/decryption under multiple unknown keys such that the relation between them is known to the attacker. Though this type of attack is meaningful during the design and certification of ciphers, it does not lead to a realistic threat in practical security protocols which use the block cipher in a standard way as stated in [13]. Therefore, the security under the single-key setting is the most important issue from the aspect of the practical security. In particular, an ultra lightweight block cipher does not need a security against related-key attacks in many cases. For example, in low-end devices such as a passive RFID tag, the key may not be changed in its life cycle as mentioned in [6, 8]. Indeed, KTANTAN supports only a fixed key [8] and the compact implementation of GOST proposed by Poschmann *et al*. also uses a hard-wired fixed key [24]. Therefore, it can be said that GOST has not been theoretically broken.

Recently, Bogdanov and Rechberger showed a new variant of the Meet-in-the-Middle (MITM) attack on block ciphers called 3-subset MITM attack [7]; it was applied to KTANTAN [8]. This attack is based on the techniques of the recent MITM preimage attacks on hash functions [1, 25]. It seems to be effective for the block cipher whose key schedule is simple, *e.g.*, a bit or a word permutation. In fact, the key schedule function of KTANTAN consists of a bit permutation. Since GOST also has a simple key schedule function, which is a word permutation, the 3-subset MITM attack seems applicable to it. However, it does not work well on the full GOST, because the key dependency of the full GOST is stronger than that of KTANTAN due to the iterative use of key words during many round functions.

**Our Contributions.** In this paper, we first introduce a new attack framework called *Reflection-Meet-in-the-Middle (R-MITM) Attack* ; it is a combination of the reflection attack and the 3-subset MITM attack. The core idea of this combination is to make use of fixed points of the reflection attack to enhance the 3-subset MITM attack. If some round functions have fixed points, we can probabilistically remove these rounds from the whole cipher. Since this skip using fixed points allows us to disregard the key bits involved in the removed rounds, the key dependency is consequently weakened. Thus, our attack is applicable to more rounds compared to the original 3-subset MITM attack if fixed points can be constructed with high probability. Then, we apply it to the full GOST block cipher with further novel techniques which make the MITM approach more efficient by using equivalent keys on short rounds. As a result, we succeed in constructing a first key recovery attack on the full GOST block cipher in the single key setting. It can recover a key with $2^{225}$ computations and $2^{32}$ known plaintext/ciphertext pairs. An important point to emphasize is that our attack does not require any assumptions for a key unlike the previous attacks. In addition, our attack can be applied to any S-boxes as long as they are bijective. These results are summarized in Table 1.

**Table 2.** Key schedule of GOST

| Round | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Key | $k_1$ | $k_2$ | $k_3$ | $k_4$ | $k_5$ | $k_6$ | $k_7$ | $k_8$ | $k_1$ | $k_2$ | $k_3$ | $k_4$ | $k_5$ | $k_6$ | $k_7$ | $k_8$ |
| Round | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| Key | $k_1$ | $k_2$ | $k_3$ | $k_4$ | $k_5$ | $k_6$ | $k_7$ | $k_8$ | $k_8$ | $k_7$ | $k_6$ | $k_5$ | $k_4$ | $k_3$ | $k_2$ | $k_1$ |

**Outline of the Paper.** This paper is organized as follows. A brief description of GOST, a 3-subset MITM attack and a reflection attack are given in Section 2. The R-MITM attack is introduced in Section 3. In Section 4, we present a R-MITM attack on the full GOST. Finally, we present conclusions in Section 5.

## 2 Preliminaries

In this section, we give a brief description of GOST, a 3-subset MITM attack and a reflection attack.

### 2.1 Description of GOST

GOST is a block cipher based on a 32-round Feistel structure with 64-bit block and 256-bit key size. The $F$-function consists of a key addition, eight $4 \times 4$-bit S-boxes $S_j$ $(1 \leq j \leq 8)$ and a 11-bit left rotation (See Fig.1).

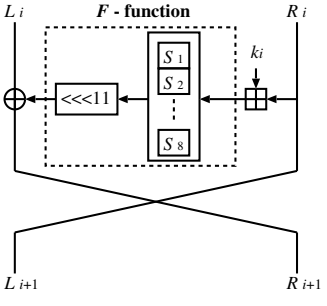


**Fig. 1.** One round of the GOST block cipher

The 256-bit master key $K$ is divided into eight 32-bit words, *i.e.*, $K = (k_1, k_2, \ldots, k_8)$, $k_i \in \{0,1\}^{32}$. Each $k_i$ is used as a round key in each round function as shown in Table 2.

In the GOST standard [22], the S-boxes are not specified. Each industry uses a different set of S-boxes. In this paper, we do not care about specific values of the S-boxes as long as they are bijective.

### 2.2 3-Subset MITM Attack

The basic concept of the MITM attack was proposed by Diffie and Helman [12]. So far, this attack has been applied to several block ciphers [9–11, 13, 14, 16]. Furthermore, over the past few years, this attack has been improved in a line of preimage attacks on hash functions, and several novel techniques are introduced, *e.g.*, a partial matching [1] and an initial structure [25]. Recently, by using these novel techniques, Bogdanov and Rechberger showed a new variant of MITM attack on block ciphers called 3-subset MITM attack [7]; it was applied to KTANTAN [8].

This attack consists of two stages: a MITM stage and a key testing stage. First, the MITM stage filters out part of wrong keys from key candidates by using MITM techniques. Then, the key testing stage finds a correct key from the surviving key candidates in a brute force manner.

Let $E_K : \{0,1\}^b \rightarrow \{0,1\}^b$ be a block cipher with an $l$-bit key $K$ and a $b$-bit block. Assume that $E_K$ is a composition of round functions as follows;

$$E_K(x) = F_{k_r} \circ F_{k_{r-1}} \circ \cdots \circ F_{k_1}(x),\ x \in \{0,1\}^b,$$

where $r$ is the number of rounds, $k_1,\ldots,k_r$ are round keys and $F_{k_i}$ is the $i$-th round function, $F_{k_i} : \{0,1\}^b \rightarrow \{0,1\}^b$. The composition of $j-i+1$ functions starting from $i$ is denoted by $F_K[i,j]$ defined as

$$F_K[i,j](x) = F_{k_j} \circ \cdots \circ F_{k_i}(x),\ 1 \leq i < j \leq r.$$

In the following, we give details of each stage of the 3-subset MITM attack.

**MITM stage :** $E_k(X)$ is divided into two functions as $E_K(X) = F_K[a+1,r] \circ F_K[1,a]$, $1 < a < r-1$ [1]. Let $K_1$ and $K_2$ be sets of key bits used in $F_K[1,a]$ and $F_K[a+1,r]$, respectively. $A_0 = K_1 \cap K_2$ is the common set of key bits used in both $F_K[1,a]$ and $F_K[a+1,r]$. $A_1 = K_1 \setminus K_1 \cap K_2$ and $A_2 = K_2 \setminus K_1 \cap K_2$ are the sets of key bits used in only $F_K[1,a]$ and only $F_K[a+1,r]$, respectively. In this stage, we use only one plaintext/ciphertext pair $(P,C)$.

The procedure of the MITM stage is as follows. Fig. 2 shows the overview of the MITM stage.

1. Guess a value of $A_0$.
2. Compute $v = F_K[1,a](P)$ for all values of $A_1$ and make a table of $(v, A_1)$ pairs. In this step, $2^{|A_1|}$ pairs are generated, where $|A_i|$ is the bit length of $A_i$ and $2^{|A_i|}$ is the number of elements of $A_i$.
3. Compute $u = F_K^{-1}[a+1,r](C)$ for all values of $A_2$. In this step, $2^{|A_2|}$ pairs are generated.

[1] As in the attack of KTANTAN [7], by using the partial matching technique, $E_K$ is divided into $F_K[1,a]$ and $F_K[a+t,r]$, $t > 1$. However, in this paper, we consider only the case of $t = 1$, because we do not use the partial matching.

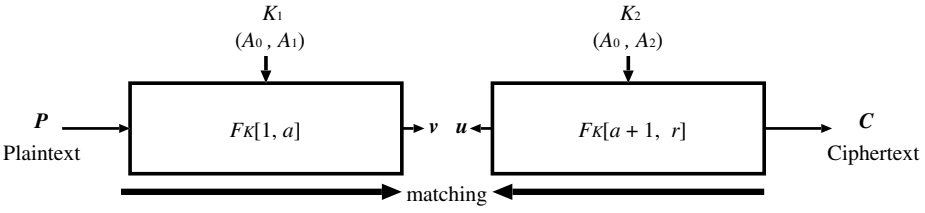


**Fig. 2.** Meet-in-the-middle stage

4. Add key candidates for which the equation $v = u$ is satisfied to the list of surviving keys.
   The number of surviving keys is $2^{|A_1|+|A_2|}/2^b$.
5. Repeat 2-4 for each different value of $A_0$. ($2^{|A_0|}$ times)

In this stage, $2^{l-b}$ key candidates survive, because $2^{|A_1|+|A_2|}/2^b \times 2^{|A_0|} = 2^l/2^b$.

**Key testing stage :** We test surviving keys in a brute force manner by using additional plaintext/ciphertext pairs.

We evaluate the cost of this attack. The whole attack complexity $C_{comp}$ is estimated as

$$C_{comp} = \underbrace{2^{|A_0|}(2^{|A_1|} + 2^{|A_2|})}_{\text{MITM stage}} + \underbrace{(2^{l-b} + 2^{l-2b} + \ldots)}_{\text{Key testing stage}}.$$

The number of required plaintext/ciphertext pair is $\lceil \frac{l}{b} \rceil$. The required memory is $\max(2^{|A_1|}, 2^{|A_2|})$, which is the cost of the table used in the MITM stage. When $\min(|A_1|, |A_2|) > 1$ the attack is more effective than an exhaustive search. Therefore, the point of the 3-subset MITM attack is to find independent sets of master key bits such as $A_1$ and $A_2$.

### 2.3 Reflection Attack

The reflection attack was first introduced by Kara and Manap [18]; it was applied to Blowfish [26]. After that, the attack was generalized by Kara [17]. In this section, we introduce a basic principle of the reflection attack used in our attack. See [17, 18] for details about the reflection attack.

The reflection attack is a kind of a self-similarity attack such as the slide attack [4, 5]. Though the reflection attack utilizes similarities of some round functions of both encryption and decryption processes, the slide attack exploits similarities among the round functions of only the encryption process. In the reflection attack, by using these similarities, fixed points of some round functions are constructed.

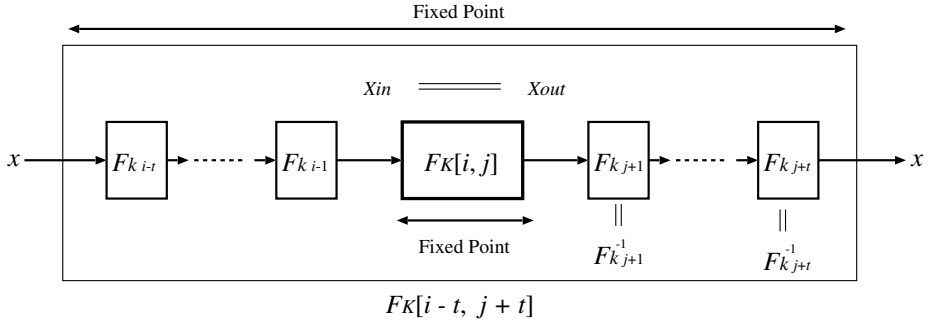


**Fig. 3.** Basic principle of the reflection attack

Let $U_K(i,j)$ be the set of fixed points of the function $F_K[i,j]$ defined as follows;

$$U_K(i,j) = \{x \in \{0,1\}^n \mid F_K[i,j](x) = x\}.$$

The basic principle of the reflection attack is given by the following Lemma.

**Lemma 1. [17]** *Let $i$ and $j$ be integers such that $0 \leq j-i < i+j < r$. Assume that $F_{k_{i-t}} = F^{-1}_{k_{j+t}}$ for all $t : 1 \leq t < i$. If $F_K[i-t, i-1](x) \in U_k(i,j)$, then $x \in U_k(i-t, j+t)$ for all $t : 1 < t < i$. In addition, if $x \in U_K(i-t, j+t)$ for certain $t : 1 < t < i$, then $F_K[i-t, i-1](x) \in U_K(i,j)$.*

From Lemma 1, if the round functions hold the conditions, a local fixed point is expanded to previous and next rounds as shown in Fig. 3. Roughly speaking, fixed points of some round functions can be constructed easily in the certain setting. These fixed points enable us to probabilistically skip the round functions from a whole cipher.

We give an example to explain this skip in detail. Let $i$ and $j$ be integers such that $0 < j-i < i+j < r$. Assume that $F_{k_{i-t}} = F^{-1}_{k_{j+t}}$ for all $t : 1 < t < i$, and $E_K(x)$ is expressed as follows;

$$\begin{aligned} E_K(x) &= F_K[j+i, r] \circ F_K[j+1, j+i-1] \circ F_K[i,j] \circ F_K[1, i-1](x), \\ &= F_K[j+i, r] \circ F_K^{-1}[1, i-1] \circ F_K[i,j] \circ F_K[1, i-1](x). \end{aligned}$$

Besides, assuming $F_K[1, i-1](x) \in U_K(i,j)$, then $F_K[1, j+i-1](x) = x$ (Lemma 1). Thus $E_K(x)$ is expressed as

$$E_K(x) = F[j+i, r](x).$$

In this case, the round functions $F_K[1, j+i-1]$ can be skipped from $E_K$. The probability $P_{ref}$ of that above skip occurs for arbitrary $x$ is $|U_K(i,j)|/2^b$. If $P_{ref} > 2^{-b}$ (*i.e.*, $|U_K[i,j]| > 1$), this skip occurs at $F_K[1, j+i-1]$ with higher probability than a random function.

## 3 Reflection-Meet-in-the-Middle Attack

We propose a new attack framework called *reflection-meet-in-the-middle (R-MITM) attack*, which is a combination of the reflection attack and the 3-subset MITM attack. As mentioned in Section 2.2, the point of the 3-subset MITM attack is to construct independent sets of master key bits. In general, if the master key bits are used iteratively in each round and the use of key bits is not biased among rounds[2], it seems to be difficult to find the independent sets of master key bits, because such cipher have the strong key dependency on even small number of rounds.

To overcome this problem, we utilize the technique of the reflection attack. In the reflection attack, some rounds satisfying certain conditions can be skipped from the whole cipher with the probability $P_{ref}$. From now on, we call this skip a *reflection skip*. Since key bits used in skipped round functions can be omitted, it becomes easier to construct independent sets of master key bits. This is the concept of the R-MITM attack. In the following, we give the detailed explanation of the attack.

### 3.1 Details of the R-MITM Attack

Suppose that $E_K$ is expressed as follows;

$$E_K(x) = F_K[a_3 + 1, r] \circ F_K[a_2 + 1, a_3] \circ F_K[a_1 + 1, a_2] \circ F_K[1, a_1](x),$$

where $2 < a_1 + 1 < a_2 < a_3 - 1 < r - 2$ and the reflection skip occurs at $F_K[a_2+1, a_3]$ with the probability $P_{ref}$. Then, $E_K$ can be redescribed as follows and denoted by $E_K^{'}(x)$,

$$E_K^{'}(x) = F_K[a_3 + 1, r] \circ F_K[a_1 + 1, a_2] \circ F_K[1, a_1](x).$$

The R-MITM attack consists of three stages; a data collection stage, a R-MITM stage and a key testing stage. In the following, we explain each stage.

**Data collection stage :** We collect plaintext/ciphertext pairs to obtain a pair in which the reflection skip occurs at $F_K[a_2+1, a_3]$. Since the probability of this event is $P_{ref}$, the number of required plaintext/ciphertext pairs is $P_{ref}^{-1}$.

After that, the R-MITM stage and the key testing stage are executed for all plaintext/ciphertext pairs obtained in the data collection stage.

**R-MITM stage :** We divide $E_K$ into two functions: $F_K[1, a_1]$ and $F_K[a_1 + 1, r]$[3]. In this stage, we ignore $F_K[a_2 + 1, a_3]$ as follows;

$$F'_K[a_1 + 1, r] = F_K[a_3 + 1, r] \circ F_K[a_1 + 1, a_2],$$

[2] In KTANTAN [8], 6 bits of master key are not used in the first 111 rounds and other 6 bits of master key are also not used in the last 131 rounds. The attack of [7] utilizes this bias of used key bits among rounds.

[3] Though there are many choices of divisions, we use it as an example.

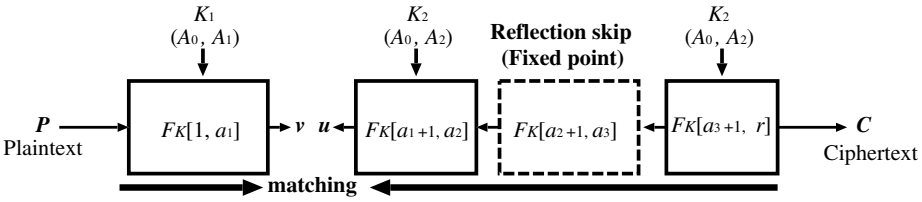


**Fig. 4.** Reflection-meet-in-the-middle stage

assuming that the reflection skip occurs. Let $K_1$ and $K_2$ be sets of key bits used in $F_K[1, a_1]$ and $F'_K[a_1 + 1, r]$, respectively. $A_0 = K_1 \cap K_2$ is the set of key bits used in both $F_K[1, a_1]$ and $F'_K[a_1 + 1, r]$. $A_1 = K_1 \setminus K_1 \cap K_2$ and $A_2 = K_2 \setminus K_1 \cap K_2$ are the sets of key bits used in only $F_K[1, a_1]$ and only $F'_K[a_1 + 1, r]$, respectively. Figure 4 illustrates the R-MITM stage.

The procedure of the R-MITM stage is almost same as the MITM stage of Section 2.2. The difference is that in the R-MITM stage, we assume that reflection skip occurs, *i.e.*, $F_K[a_2 + 1, a_3]$ is ignored. After this stage, $2^{l-b}$ key candidates survive.

**Key testing stage :** We test surviving keys in a brute force manner by using plaintext/ciphertext pairs.

### 3.2 Evaluation of the R-MITM Attack

We evaluate the cost of the R-MITM attack. The whole attack complexity $C_{comp}$ is estimated as

$$C_{comp} = \underbrace{((2^{|A_0|}(2^{|A_1|} + 2^{|A_2|}))}_{\text{R-MITM stage}} + \underbrace{(2^{l-b} + 2^{l-2b} + \ldots))}_{\text{Key testing stage}} \times R_{ref}^{-1}.$$

The number of required plaintext/ciphertext pair is $\max(\lceil l/b \rceil, R_{ref}^{-1})$. The required memory is $\max(2^{|A_1|}, 2^{|A_2|})$, which is the cost of the table in the R-MITM stage. When $\min(2^{|A_1|}, 2^{|A_2|}, 2^b) > (R_{ref}^{-1})$, the attack is more effective than an exhaustive search.

Compared with the basic 3-subset MITM attack in Section 2.2, the number of required plaintext/ciphertext pairs increases, because the R-MITM attack utilizes the probabilistic event, *i.e.*, reflection skip. In addition, more independent key bits are needed for the successful attack. However, this attack has a distinct advantage, which is to be able to skip some round functions by the reflection skip. Recall that the most important point of the 3-subset MITM attack is to find independent sets of master key bits. Since the reflection skip enables us to disregard key bits involved in some round, it obviously becomes easier to construct such independent sets. Thus, this attack seem to be applicable to more rounds than the 3-subset MITM attack when the reflection skip occurs with high probability.

## 4 R-MITM Attack on the Full GOST Block Cipher

In this section, we apply the R-MITM attack to the full GOST block cipher [22]. From Table. 2, in full 32 rounds, the master key is iteratively used four times and all master key bits are involved in every 8 rounds. The basic 3-subset MITM attack in Section 2.2 is not applicable to the full GOST, because independent sets of master key bits can not be constructed in any divisions of 32 rounds. However, by using the R-MITM attack, we can construct independent sets and mount a key recovery attack on the full GOST.

We first introduce the reflection property of GOST proposed by Kara [17] to construct the reflection skip. Next, we present effective MITM techniques to enhance the R-MITM stage. These techniques make use of the equivalent keys of short round functions. Finally, we evaluate our attack.

### 4.1 Reflection Property of GOST

The reflection attack on GOST has been proposed by Kara [17][4]. The GOST block cipher $E_K : \{0,1\}^{64} \rightarrow \{0,1\}^{64}$ is expressed as

$$\begin{aligned} E_K &= S \circ F_K[25,32] \circ F_K[17,24] \circ F_K[9,16] \circ F_K[1,8], \\ &= F_K^{-1}[1,8] \circ S \circ F_K[1,8] \circ F_K[1,8] \circ F_K[1,8], \end{aligned}$$

where $S$ is the swap of the Feistel structure.

$S$ has $2^{32}$ fixed points, because the probability of that the right halves equal to the left halves is $2^{-32}$. From Lemma 1, $F_K^{-1}[1,8] \circ S \circ F_K[1,8]$ also has $2^{32}$ fixed points, *i.e.*, $|U_K(17,32)| = 2^{32}$. Thus, with the probability $P_{ref} = 2^{-32}$ $(= (2^{32}/2^{64}))$, $F_K[17,32]$ can be ignored. $E_K$ is redescribed as follows and denoted by $E_K^{'}$

$$E_K^{'} = F_K[1,8] \circ F_K[1,8].$$

Figure 5 shows this reflection skip of GOST.

Therefore, in the data collection stage, we need to collect $P_{ref}^{-1} = 2^{32}$ plaintext/ciphertext pairs. In $2^{32}$ collected pairs, there is a pair in which the reflection skip occurs, *i.e.*, last 16 rounds can be removed as $E_K^{'}$.

### 4.2 Effective MITM Technique Using Equivalent Keys on Short Rounds

In the R-MITM stage, we mount the MITM approach on only $E_K^{'} = F_K[1,8] \circ F_K[1,8]$ for all $2^{32}$ collected pairs.

As mentioned in Section 3.2, we need to construct independent sets $A_1$ and $A_2$ which hold the condition, $\min(2^{|A_1|}, 2^{|A_2|}) > 2^{32}$. However, despite the reduction

[4] The similar technique for constructing a fixed point is also used in the attacks on the GOST hash function [20, 21].

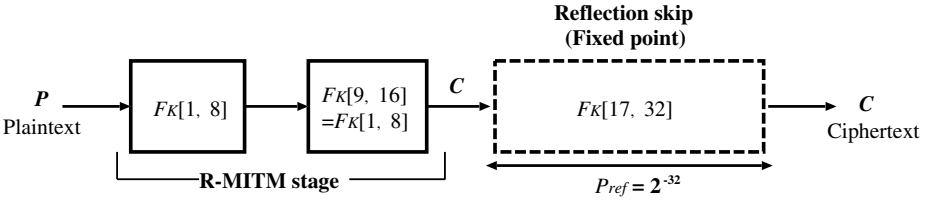


**Fig. 5.** Reflection skip of GOST

of rounds by the reflection skip, in the straightforward method, we can not find such sets in any divisions of 16 rounds, due to the strict condition of independent sets.

We introduce effective MITM techniques which make use of equivalent keys of short round functions (*i.e.*, 4 round). The aim of these techniques is to ignore the first and the last 4 rounds and to mount the MITM approach in only intermediate 8 rounds. These techniques enable us to construct independent sets enough for the successful attack.

We treat $E_K^{'}$ as following four-round units;

$$E_K^{'} = F_K[5,8] \circ F_K[1,4] \circ F_K[5,8] \circ F_K[1,4].$$

In the following, we first explain equivalent keys used in our attack. Then, we present detail of the R-MITM stage using the equivalent keys.

**Equivalent Keys on Short Rounds.** Define a set of equivalent keys on $F_K[i,j]$ as $Z(F_K[i,j],x,y)$ as follows:

$$Z(F_K[i,j],x,y) = \{ek \in \{0,1\}^{256} \mid F_{ek}[i,j](x) = y\},$$

where $(x,y) \in \{0,1\}^{64}$. Note that the class of keys defined above is the equivalent keys with respect to only one input/output pair. To put it more concretely, if equivalent keys $ek \in Z(F_K[i,j],x,y)$ are used, input $x$ is always transformed to $y$ in $F_K[i,j]$. For other input/output pairs, these relations do not hold even if the same equivalent keys are used.

GOST has an interesting property regarding the equivalent keys on short rounds as described in the following observation.

**Observation 1:** *Given any $x$ and $y$, $Z(F_K[1,4],x,y)$ and $Z(F_K^{-1}[5,8],x,y)$ can be easily obtained, and the number of each equivalent keys is $2^{64}$.*

For $F_K[1,4]$, $k_1,k_2,k_3$ and $k_4$ are added in each round. Given the values of $k_1$ and $k_2$, the other values of $k_3$ and $k_4$ are determined from $F_K[1,2](x)$ and $y$ as follows:

$$k_3 = F^{-1}(z_L + y_L) - z_R, \quad (1)$$
$$k_4 = F^{-1}(z_R + y_R) - y_R, \quad (2)$$

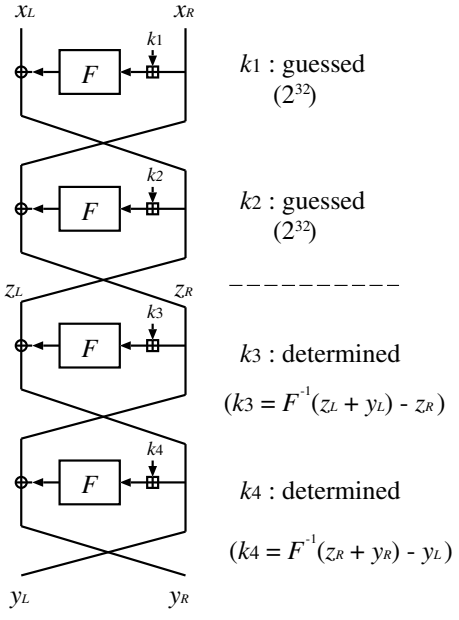


**Fig. 6.** Equivalent keys of 4 rounds

where $F^{-1}$ is the inverse of $F$ function, $y_L$ and $y_R$ are left and right halves of $y$, and $z_L$ and $z_R$ are those of $F_K[1,2](x)$. Since values of ($k_1$, $k_2$) are 64 bits, the number of $Z(F_K[1,4],x,y)$ is $2^{64}$. Figure 6 shows this procedure. A similar property holds for $F_K^{-1}[5,8]$.

From Observation 1, we can easily obtain $2^{64}$ equivalent keys of the first and the last 4 rounds for any inputs and outputs. Moreover, $F_K[1,4]$ and $F_K^{-1}[5,8]$ use different master key bits each other, $K_a = (k_1||k_2||k_3||k_4)$ and $K_b = (k_5||k_6||k_7||k_8)$, respectively. Thus, $Z(F_K[1,4],x,y)$ and $Z(F_K^{-1}[5,8],x,y)$ are expressed by sets of only $K_a$ and $K_b$ as follows;

$$Z_{Ka}(F_K[1,4],x,y) = \{ek_a \in \{0,1\}^{128} \mid F_{ek_a}[1,4](x) = y\},$$
$$Z_{Kb}(F_K^{-1}[5,8],x,y) = \{ek_b \in \{0,1\}^{128} \mid F_{ek_b}^{-1}[5,8](x) = y\}.$$

Since $K_a$ and $K_b$ are independent sets of mater key, $Z_{Ka}(F_K[1,4],x,y)$ and $Z_{Kb}(F_K^{-1}[5,8],x,y)$ are also independent sets.

**Detail of the R-MITM Stage using Equivalent Keys.** Let $S$ and $T$ be $F_K[1,4](P)$ and $F^{-1}[5,8](C)$, which are input and output values of 8 intermediate rounds, *i.e.*, $F_K[5,12] = F_K[1,4] \circ F_K[5,8]$.

From Observation 1, given values of $P$, $C$, $S$ and $T$, two sets of $2^{64}$ equivalent keys, $Z_{K_a}(F_K[1,4],P,S)$ and $Z_{K_b}(F_K^{-1}[5,8],C,T)$, can be easily obtained.

When $Z_{K_a}(F_K[1,4],P,S)$ and $Z_{K_b}(F_K^{-1}[5,8],C,T)$ are used, $S$ and $T$ are not changed. Thus by using these equivalent keys, the first and the last 4 round

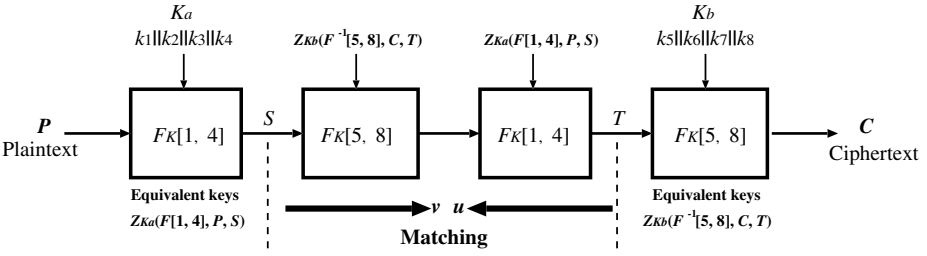


**Fig. 7.** R-MITM stage using equivalent keys

can be ignored, and we can mount the MITM attack between $F_K[5,8](S)$ and $F_K^{-1}[1,4](T)$. The number of elements in each independent set is $2^{64}$, which is enough for the successful attack.

The procedure of the R-MITM stage is as follows and illustrated in Fig. 7.

1. Guess the values $S$ and $T$.
2. Compute $v = F_K[5,8](S)$ with $2^{64}$ $K_b$ in $Z_{K_b}(F_K^{-1}[5,8], C, T)$ and make a table of $(v, K_b)$ pairs.
3. Compute $u = F_K^{-1}[1,4](T)$ with $2^{64}$ $K_a$ in $Z_{K_a}(F_K[1,4], P, S)$.
4. Add key candidates for which the equation $v = u$ is satisfied to the list of surviving keys. The number of surviving keys is $2^{64+64}/2^{64} = 2^{64}$.
5. Repeat 2-4 with the different values of $S$ and $T$. ($2^{128}$ times).

After this procedure, $2^{192}$ ($=2^{64} \times 2^{128}$) key candidates survive. These key candidates are evaluated in the key testing stage.

The R-MITM stage utilizes equivalent-key sets of $Z_{K_a}(F_K[1,4], P, S)$ and $Z_{K_b}(F_K^{-1}[5,8], C, T)$, $0 \le S,\ T < 2^{64}$, where each set includes $2^{64}$ elements. For $Z_{K_a}(F_K[1,4], P, S)$, $0 \le S < 2^{64}$, all elements of every set are different, because if the values of $S$ are different, equivalent keys of $F_K[1,4]$ are surely different from Eq. (1) and (2) as long as S-boxes are bijective. Thus, $Z_{K_a}(F_K[1,4], P, S), 0 \le S < 2^{64}$ covers all $2^{128}$ $(= 2^{64} \times 2^{64})$ values of $K_a$. A similar property holds for $K_b$. Therefore, all possible values for the master key are tested and the set of surviving key candidates surely contain the correct key if the reflection skip occurs.

### 4.3 Evaluation

The whole attack complexity $C_{comp}$ is estimated as

$$C_{comp} = (\underbrace{(2^{128}(2^{64} + 2^{64}))}_{\text{R-MITM stage}} + \underbrace{(2^{256-64} + 2^{256-128} + \ldots)}_{\text{Key testing stage}}) \times 2^{32},$$
$$= 2^{225}.$$

The number of required known plaintext/ciphertext pairs is $\max(\lceil l/b \rceil, R_{ref}^{-1}) = \max(\lceil 256/64 \rceil, 2^{32}) = 2^{32}$. The required memory is $\max(2^{64}, 2^{64}) = 2^{64}$, which

is the cost of the table used in the R-MITM stage. Therefore, this attack can recover a key with $2^{225}$ computations, $2^{32}$ known plaintext/ciphertext pairs and $2^{64}$ memory. It is more effective than an exhaustive attack.

## 5 Conclusion

This paper has presented a first single-key attack on the full GOST block cipher without relying on weak key classes. To build the attack, we introduced a new attack framework called *Reflection-Meet-in-the-Middle Attack*, which is the combination of the reflection and the 3-subset MITM attacks. The advantage of this attack over the basic 3-subset MITM attack, some rounds can be probabilistically removed from the whole cipher. Since this allows us to disregard the key bits involved in the removed rounds, it becomes easier to construct the independent sets of the key bits. Thus, our attack seems to be applicable to more rounds when the reflection skip occurs with high probability. Then we applied it to the full GOST block cipher with further novel techniques which make use of equivalent keys of short round functions (*i.e.*, 4 rounds). These techniques enable us to mount the effective MITM approach. As a result, we succeeded in constructing a first key recovery attack on the full GOST without any key conditions, which works for any bijective S-boxes. Our result shows that GOST does not have the 256-bit security for all key classes, even if a fixed key is used such as [24].

The idea of the R-MITM attack seems applicable to other block ciphers in which the fixed point can be constructed with high probability and its key schedule is simple in the sense that the key dependency is not strong. Furthermore, the basic principle of the attack does not constrain the reflection property and fixed points. Other non-random properties of round functions may also be able to be utilized as the skip techniques, *e.g.*, the strong correlations among round functions.

**Acknowledgments.** We would like to thank to Taizo Shirai, Kyoji Shibutani, Özgül Küçük, and anonymous referees for their insightful comments and suggestions.

## References

1. Aoki, K., Sasaki, Y.: Preimage Attacks on One-Block MD4, 63-Step MD5 and More. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 103–119. Springer, Heidelberg (2009)
2. Biham, E., Dunkelman, O., Keller, N.: Improved Slide Attacks. In: Biryukov, A. (ed.) [3], pp. 153–166
3. Biryukov, A. (ed.): FSE 2007. LNCS, vol. 4593. Springer, Heidelberg (2007)
4. Biryukov, A., Wagner, D.: Slide attacks. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 245–259. Springer, Heidelberg (1999)
5. Biryukov, A., Wagner, D.: Advanced Slide Attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 589–606. Springer, Heidelberg (2000)

6. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
7. Bogdanov, A., Rechberger, C.: A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 229–240. Springer, Heidelberg (2011)
8. De Cannière, C., Dunkelman, O., Knežević, M.: KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer, Heidelberg (2009)
9. Chaum, D., Evertse, J.-H.: Cryptanalysis of DES with a Reduced Number of Rounds Sequences of Linear Factors in Block Cipher. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 192–211. Springer, Heidelberg (1986)
10. Demirci, H., Selçuk, A.A.: A Meet-in-the-Middle Attack on 8-Round AES. In: Nyberg, K. (ed.) [23], pp. 116–126
11. Demirci, H., Taşkın, İ., Çoban, M., Baysal, A.: Improved Meet-in-the-Middle Attacks on AES. In: Roy, B.K., Sendrier, N. (eds.) INDOCRYPT 2009. LNCS, vol. 5922, pp. 144–156. Springer, Heidelberg (2009)
12. Diffie, W., Hellman, M.E.: Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer 10, 74–84 (1977)
13. Dunkelman, O., Keller, N., Shamir, A.: Improved Single-Key Attacks on 8-Round AES-192 and AES-256. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 158–176. Springer, Heidelberg (2010)
14. Dunkelman, O., Sekar, G., Preneel, B.: Improved Meet-in-the-Middle Attacks on Reduced-Round DES. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 86–100. Springer, Heidelberg (2007)
15. Fleischmann, E., Gorski, M., Hüehne, J., Lucks, S.: Key Recovery Attack on full GOST. Block Cipher with Negligible Time and Memory. In: Western European Workshop on Research in Cryptology (WEWoRC). LNCS, vol. 6429. Springer, Heidelberg (2009)
16. Indesteege, S., Keller, N., Dunkelman, O., Biham, E., Preneel, B.: A Practical Attack on KeeLoq. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 1–18. Springer, Heidelberg (2008)
17. 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)
18. Kara, O., Manap, C.: A New Class of Weak Keys for Blowfish. In: Biryukov, A. (ed.) [3], pp. 167–180
19. Ko, Y., Hong, S.H., Lee, W.I., Lee, S.-J., Kang, J.-S.: Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST. In: Roy, B.K., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 299–316. Springer, Heidelberg (2004)
20. Mendel, F., Pramstaller, N., Rechberger, C.: A (Second) Preimage Attack on the GOST Hash Function. In: Nyberg, K. (ed.) [23], pp. 224–234.
21. Mendel, F., Pramstaller, N., Rechberger, C., Kontak, M., Szmidt, J.: Cryptanalysis of the GOST Hash Function. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 162–178. Springer, Heidelberg (2008)
22. National Soviet Bureau of Standards. Information Processing System - Cryptographic Protection - Cryptographic Algorithm GOST 28147-89 (1989)
23. Nyberg, K. (ed.): FSE 2008. LNCS, vol. 5086. Springer, Heidelberg (2008)

24. Poschmann, A., Ling, S., Wang, H.: 256 Bit Standardized Crypto for 650 GE – GOST Revisited. In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010. LNCS, vol. 6225, pp. 219–233. Springer, Heidelberg (2010)
25. Sasaki, Y., Aoki, K.: Finding Preimages in Full MD5 Faster Than Exhaustive Search. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 134–152. Springer, Heidelberg (2009)
26. Schneier, B.: Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish). In: Anderson, R.J. (ed.) FSE 1993. LNCS, vol. 809, pp. 191–204. Springer, Heidelberg (1994)
27. Schneier, B.: Applied Cryptography, 2nd edn. Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., New York (1995)
28. Seki, H., Kaneko, T.: Differential Cryptanalysis of Reduced Rounds of GOST. In: Stinson, D.R., Tavares, S.E. (eds.) SAC 2000. LNCS, vol. 2012, pp. 315–323. Springer, Heidelberg (2001)