Reflections on Slide with a Twist Attacks

Itai Dinur[1], Orr Dunkelman[2], Nathan Keller[3], and Adi Shamir[4]

[1] École Normale Supérieure
Département d'Informatique,
45 rue d'Ulm, 75230 Paris, France
itai.dinur@ens.fr
[2] Computer Science Department
University of Haifa
Haifa 31905, Israel
orrd@cs.haifa.ac.il
[3] Department of Mathematics
Bar-Ilan University
Ramat Gan 52900, Israel
nkeller@math.biu.ac.il
[4] Faculty of Mathematics and Computer Science
Weizmann Institute of Science
P.O. Box 26, Rehovot 76100, Israel
adi.shamir@weizmann.ac.il

Abstract. *Slide attacks* use pairs of encryption operations which are slid against each other. *Slide with a twist* attacks are more sophisticated variants of slide attacks which slide an encryption operation against a decryption operation. Designed by Biryukov and Wagner in 2000, these attacks were used against several cryptosystems, including DESX, the Even-Mansour construction, and Feistel structures with four-round self-similarity. They were further extended in 2012 to the *mirror slidex* framework, which was used to attack the 20-round GOST block cipher and several additional variants of the Even-Mansour construction. In this paper, we revisit all the previously published applications of these techniques and show that in almost all cases, the same or better results can be achieved by a simpler attack which is based on the seemingly unrelated idea of exploiting internal *fixed points*. The observation that such fixed points can be useful in cryptanalysis of block ciphers is known for decades and is the basis of the *reflection attack* presented by Kara in 2007. However, all the examples to which reflection attacks were applied were based on particular constructions such as Feistel structures or GOST key schedules in which it was easy to explicitly list and count the fixed points. In this paper, we generalize Kara's reflection attack by using the combinatorial result that random involutions on 2^n values are expected to have a surprisingly large number of $O(2^{n/2})$ fixed points (whereas random permutations are expected to have only $O(1)$ fixed points). This makes it possible to reduce the complexity of the best known attack on additional cryptographic schemes in which it is difficult to explicitly characterize and count the internal fixed points.

Keywords: Cryptanalysis, Reflection attack, Slide with a twist, Fixed points, Random Involutions, Feistel structures, Even-Mansour scheme, DESX, GOST (block cipher)

1 Introduction

Many cryptographic schemes have some form of self similarity (in which the scheme can be compared to a modified form of itself), and many cryptanalytic techniques had been developed over the last 15 years to take advantage of this fact. The simplest technique (which was proposed by Biryukov and Wagner [2] at FSE'99) is the *slide attack*, which compares the encryption process to a slightly shifted version of itself (e.g., by a single round). A pair of encryptions is called a *slid pair* if they contain the same corresponding values after each round in their overlapping part. Such a pair makes it possible to consider only the short non-overlapping parts at the beginning and the end of the encryption, and to recover the key from their known inputs and outputs. One of the unique properties of slide attacks is that they can break an arbitrarily large number of rounds with the same complexity, since they ignore the long common part of the two encryptions.

One year later, at Eurocrypt 2000, Biryukov and Wagner developed an advanced version of this attack called a *slide with a twist attack* [3] by considering a more complicated form of self similarity, which shifts and reverses one encryption in order to get the other encryption. In their paper, they used such slid pairs of an encryption and a decryption in order to attack the Even-Mansour scheme and some variants of DES with modified key schedules.

In 2007, Kara [16] developed a different approach which he called a *reflection attack*, in which he showed how to improve the attack on the encryption scheme 2K-DES by exploiting the existence of some internal fixed points. This scheme is defined as a Feistel structure with an arbitrary number of rounds which alternately uses two keys in subsequent rounds, and the fixed point is created whenever the F function in a particular round produces a zero value. Kara showed that in this case there is a palindromic structure of values before and after this round, which can be exploited by the cryptanalyst. The same type of fixed points was already used by Coppersmith [5] at Crypto'85 to explain a mysterious cycling behavior of iterated DES which was experimentally observed by Kalisky et al. [15]. More recently, Courtois used fixed points in a series of attacks against GOST [6] and other schemes [1,7]. Also, Soleimany et al. [18] used such a fixed point based property of the lightweight block cipher PRINCE in order to construct a new type of distinguisher for that cipher.

At Eurocrypt 2012, Dunkelman, Keller and Shamir developed the *mirror slidex attack*, which avoided the need to compare encryptions with decryptions by using the existence of an involution (acting as a reflecting "mirror") in the middle of the encryption. They used this technique to obtain an attack on variants of DES, GOST, and the Even-Mansour scheme.

In this paper, we show that almost all the slide with a twist attacks mentioned above can be either matched or improved by using a unified technique (that we call *enhanced reflection*) which combines involutions and fixed points in a new way. In particular, we use a classical combinatorial result (which is not known by our entire community) that randomly chosen involutions over 2^n values are expected to have $O(2^{n/2})$ fixed points (whereas randomly chosen permutations are expected to have only $O(1)$ fixed points). By identifying a large involution deep inside a given scheme, we can use a relatively small number of encryptions in order to obtain with high probability either one or two fixed points of this involution, and then proceed to extract the key from the parts of the scheme that remain after deleting the involution. This eliminates the need in previous reflection attacks to characterize and count all the possible fixed points of such an involution. In fact, the only previously studied cases in which we could not apply this new technique were when the involutions were so simple that they behaved in a completely non-random way. For example, XORing a key to a value is an involution, but it clearly has no fixed points when the key is nonzero.

In addition to generalizing and unifying previous attacks based on such self similarity, the new approach makes it possible to improve the best known attack on several cryptographic schemes. For example, while a slide with a twist attack on 18-round GOST block cipher requires a barely-practical time complexity of 2^{64}, the enhanced reflection attack can break the same version with a practical 2^{33} time complexity using the same amount of data.[5]

Likewise, while the mirror slidex attack on a single-key Even-Mansour construction with addition operations requires either $2^{n/2}$ *adaptively chosen plaintexts* or $2^{n/2}$ memory, our enhanced reflection attack requires only $2^{n/2}$ *known plaintexts* and a constant amount of memory to achieve the same goal. Finally, we can apply our technique to a Feistel structure with four-round self-similarity surrounded by key whitenings, which was conjectured in [9] to be immune to slide-type attacks.

2 The Slide With a Twist and the Mirror Slidex Attacks

In this section, we present a brief description of the slide with a twist attack and of its enhancement – the mirror slidex attack. For sake of brevity, we present the general framework of the mirror slidex attack, and view the original slide with a twist attack as a special case. After describing the attack techniques, we list the applications presented in [3,9,10]. A detailed treatment of these applications is given in Sections 3 and 4.

[5] For sake of simpler presentation, we slightly disregard the exact success probability of the attacks. All the attacks reported in the paper have a constant non-negligible success rate (for the proposed complexities). At the same time, we alert the reader that sometimes, the success rate might be slightly lower than 50% (e.g., when we assume a collision occurs given $2^{n/2}$ n-bit strings, rather than $1.17 \cdot 2^{n/2}$). Additionally, for sake of comparison, when comparing with previous attacks, we always report the comparable data complexity that offers the same success rate.

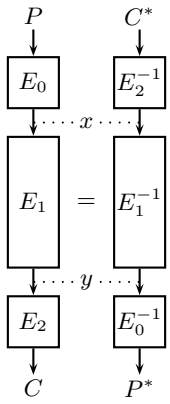

Fig. 1. A Mirror Slid Pair (P, P^*)

2.1 The General Attack Framework

The mirror slidex attack can be applied in principle to any block cipher that can be decomposed as a cascade of three sub-ciphers: $E = E_2 \circ E_1 \circ E_0$, where the middle layer E_1 is an involution, i.e., $E_1 \circ E_1$ is the identity mapping.[6]

Let E be such a cipher, and assume that for two plaintext/ciphertext pairs $(P, C), (P^*, C^*)$, we have

$$E_0(P) = E_2^{-1}(C^*). \tag{1}$$

Note that for a random choice of two pairs, this event happens with probability 2^{-n}. Since E_1 is an involution for which $E_1 = (E_1)^{-1}$, in this case we can also deduce that:

$$E_1(E_0(P)) = E_1^{-1}(E_2^{-1}(C^*)).$$

By the construction, this implies that:

$$E_2^{-1}(C) = E_1(E_0(P)) = E_1^{-1}(E_2^{-1}(C^*)) = E_0(P^*). \tag{2}$$

If Equation (1) holds (and thus, Equation (2) also holds), the pair (P, P^*) is called a *mirror slid pair* (depicted in Figure 1).

The mirror slid pairs can be used to mount a cryptanalytic attack on E. In the attack, the adversary asks for the encryption of $O(2^{n/2})$ known plaintexts $P_1, P_2, \ldots$ (where n is the block size of E) and denotes the corresponding ciphertexts by $C_1, C_2, \ldots$. For each of the $O(2^n)$ pairs (P_i, P_j), the adversary assumes that it is a mirror slid pair and tries to solve the system of equations:

$$\begin{cases} C_j = E_2(E_0(P_i)), \\ C_i = E_2(E_0(P_j)) \end{cases} \tag{3}$$

[6] Note that any cryptosystem can be represented in such a way by artificially adding an identity operation (which is an involution) in its middle, but since the omission of E_1 does not simplify the cryptosystem in this case, we will not get a better attack.

(which is equivalent to Equations (1) and (2)). If E_0 and E_2 are "simple enough", the adversary can solve the system efficiently and recover the key material used in E_0 and E_2.

If the amount of subkey material used in E_0 and E_2 is at most n bits (in total), it is expected that at most a few of the systems of equations generated by the 2^n plaintext pairs[7] are consistent (since the equation system is a $2n$-bit condition). One of them is the system generated by the mirror slid pair, which is expected to exist in the data with a non-negligible probability since the probability of a random pair to be a mirror slid pair is 2^{-n}. Hence, the adversary obtains only a few suggestions for the key, which contain the right key with a non-negligible probability. If the amount of key material used in E_0 and E_2 is larger than n bits, the adversary can still find the right key, by enlarging the data set by a small factor and using key ranking techniques (exploiting the fact that the right key is suggested by all mirror slid pairs, while the other pairs suggest "random" keys).

The data complexity of the attack is $O(2^{n/2})$ known plaintexts, and its time complexity is $O(2^n) \cdot t$, where t is the time required for solving the system (3).

The slide with a twist attack is a special case of the mirror slidex framework in which $E_2 = Identity$. In such a case, the system of equations presented above is simplified to:

$$\begin{cases} C_j = E_0(P_i), \\ C_i = E_0(P_j). \end{cases} \tag{4}$$

We note that in [3] where the slide with a twist attack was introduced, it was presented in a different way. However, the presentations are equivalent and for the purpose of the current paper, the presentation given here is sufficient.

2.2 Applications of the Slide with a Twist Attack

In [3,9,10], the authors presented numerous applications of the slide with a twist and the mirror slidex techniques.

1. **Feistel constructions with self similarity.** These constructions are based on DES, with the sequence of subkeys replaced by a periodic sequence, such as $k_0, k_1, k_0, k_1, \ldots$. In [3], the authors considered two such constructions called 2K-DES and 4K-DES (with two-round and four-round self similarity, respectively), and presented known plaintext attacks of complexity $2^{n/2}$ and chosen plaintext attacks of complexity $2^{n/4}$ on both variants. They also considered DES with a modified key schedule proposed by Brown and Seberry, which appears to be 4-round self-similar, and devised an even faster attack on it, using specific properties of DES.
2. **Feistel constructions with self similarity surrounded by key whitenings.** These constructions are based on the block cipher DESX (defined as

[7] We note that in some cases, it is possible to discard candidate plaintext pairs before applying the attack on E_0 and E_2.

DES surrounded by key whitenings), with the sequence of subkeys replaced by a periodic sequence. In [10], the authors considered 2K-DESX and 4K-DESX (with two-round and four-round self similarity, respectively). They presented a known plaintext attack of complexity $2^{n/2}$ on 2K-DESX, but stated that they could not find any attack which is faster than 2^n on 4K-DESX.

3. **Reduced variants of the GOST block cipher.** In [3], the authors considered a variant of the GOST block cipher in which the key additions are replaced by XORs. They showed that 20 rounds of this variant can be broken in 2^{33} data and 2^{70} time, and presented a set of 2^{128} weak keys for this variant, for which the encryption is reduced to a Feistel construction with 4-round self similarity. In [9], it was shown that 20 rounds of original GOST can also be broken by slide with a twist, in a slightly increased time of 2^{77}.
4. **DESX and the Even-Mansour construction.** In [3], the authors showed that the Even-Mansour construction (defined as $E(P) = K_2 \oplus F(P \oplus K_1)$, where K_1, K_2 are secret keys and F is a publicly known permutation) can be broken in $2^{n/2}$ time and memory, using $2^{n/2}$ queries to E and $2^{n/2}$ computations of F. They also presented a similar attack that breaks DESX in 2^{33} data and 2^{89} time.[8]
5. **Variants of the Even-Mansour construction.** In [9] it was shown that if the public permutation used in the Even-Mansour construction is an involution, the construction can be broken in $2^{n/2}$ time and memory, with $2^{n/2}$ queries to E and no computations of F. Numerous other variants of the Even-Mansour construction were studied in [9], most notably a variant defined as $E(P) = K + F(P + K)$ where F is a publicly known involution, that was shown to be completely breakable in $2^{n/2}$ time and memory, with $2^{n/2}$ queries to E and no computations of F.

We consider all these applications in detail in the next two sections, and show that for all of them (except for the simplest attacks of [3] on DESX and Even-Mansour, in which the involution is just a XOR with a key, which is not sufficiently random), our enhanced reflection attack performs at least as well as the slide with a twist attack, and in some cases it performs significantly better.

We consider applications (3)–(5) in Section 3, right after the presentation of the new technique. Applications (1)–(2) will be considered in Section 4, as our results for those variants require some additional observations specific to Feistel constructions, and are directly related to the original *reflection* attack [16] (that is also considered in Section 4).

[8] We alert the reader that in DES the key length is 56 bits, and thus the time complexity of the attack is essentially about $2^{56} \cdot 2^{64/2}$ (again taking into account that a small multiplicative constant in the data/time complexities increases the success rate).

Application	Technique	Reference	Data	Time	Memory
18-Round GOST	slide with a twist	[3,9]	2^{33}	2^{64}	2^{33}
	enhanced reflection	Section 3	2^{33}	$\mathbf{2^{33}}$	2^{33}
20-Round GOST	slide with a twist	[3,9]	2^{33}	2^{77}	2^{33}
	enhanced reflection	Section 3	2^{33}	2^{77}	2^{33}
DESX	slide with a twist	[3]	2^{33} KP	2^{89}	2^{33}
	enhanced reflection	Section 3	Inapplicable		
Even-Mansour	mirror slidex	[9]	$2^{n/2}$ KP	$2^{n/2}$	$2^{n/2}$
Variant (AIEM)	enhanced reflection	Section 3	$2^{n/2}$ KP	$2^{n/2}$	$2^{n/2}$
Even-Mansour	mirror slidex	[9]	$2^{n/2}$ KP	$2^{n/2}$	$2^{n/2}$
Variant (ASIEM)	enhanced reflection	Section 3	$2^{n/2}$ KP	$2^{n/2}$	$\mathbf{O(1)}$
2K-DES	slide with a twist	[3]	$2^{n/2}$ KP	$2^{n/2}$	$2^{n/2}$
and	slide with a twist	[3]	$2^{n/4}$ CP	$2^{n/4}$	$2^{n/4}$
4K-DES	enhanced reflection	Section 4	$2^{n/2}$ KP	$2^{n/2}$	$\mathbf{O(1)}$
2K-DESX	mirror slidex	[10]	$2^{n/2}$ KP	$2^{n/2}$	$2^{n/2}$
	enhanced reflection	Section 4	$2^{n/2}$ KP	$2^{n/2}$	$2^{n/2}$
4K-DESX	mirror slidex	[10]	Inapplicable		
	enhanced reflection	Section 4	$\mathbf{n \cdot 2^{n/2}}$ KP	$\mathbf{n \cdot 2^{n/2}}$	$\mathbf{2^{n/2}}$

Table 1. Summary of Applications (and Comparison with Slide-based Attacks)

3 Enhanced Reflection Attacks Using Fixed Points of Involutions

In this section we present our enhanced reflection attack which is based on the simple fact that random involutions have a surprisingly large number of fixed points. We describe scenarios in which the attack is advantageous over the slide with a twist attack. Then we consider several specific applications of the slide with a twist attack presented in [3,9,10] and show how the enhanced reflection attack applies to them.

3.1 The Basic Idea

The starting point of the enhanced reflection attack is a classical result on the number of fixed points of involutions.

Theorem 1 ([12], page 596). *Let $\mathcal{I} : S \to S$ be drawn at random from the family of involutions on a set S with N elements. Then the expected number of fixed points of $\mathcal{I}$ is $\sqrt{N} - 1/2 + o(1)$.*

Before we give a brief explanation of the claim, we note that an example for an involution with exactly $\sqrt{N}$ fixed points is mentioned in the attack of Section 3.3 and in the answer of Coppersmith [5]. On the other hand, as we discuss in

Section 3.3, XORing with a non-zero constant is an involution with no fixed points.

Denote by $f(n)$ the number of involutions on n elements. Consider a random involution σ on n elements. The explanation of the theorem starts from computing the probability that 1 is a fixed point of σ.

Observe that if we take any involution on $\{2, 3, \ldots, n\}$ and add to it 1 as a fixed point, we get an involution on $\{1, 2, \ldots, n\}$. On the other hand, all involutions that have 1 as a fixed point are of this form. Hence, the number of involutions on $\{1, 2, \ldots, n\}$ in which 1 is a fixed point is exactly $f(n-1)$. Thus, the probability that 1 is a fixed point of a random involution is $f(n-1)/f(n)$. As there is nothing special with adding 1, and by the linearity of expectation, the expected number of fixed points is $n \cdot f(n-1)/f(n)$.

Finally, to show that the expected number of fixed points is close to $\sqrt{n}$, we have to show that the number of involutions on n elements satisfies $f(n)/f(n-1) \approx \sqrt{n}$. This is a standard (but not easy) fact that follows from the exponential generating function of $f(n)$, that can be shown to be $e^{z+z^2/2}$.

The theorem allows to significantly simplify the attack of the mirror slidex framework presented in Section 2. Let E be a block cipher that can be decomposed as a cascade of three sub-ciphers: $E = E_2 \circ E_1 \circ E_0$, where the middle layer E_1 is an involution. Assume that for a plaintext/ciphertext pair (P, C), the intermediate encryption value after the application of E_0, i.e., $E_0(P)$, is a fixed point of E_1 (for a random involution on n-bit values, this happens with probability $2^{-(n/2)}$). In such a case, we have $C = E_2(E_1(E_0(P))) = E_2(E_0(P))$. If the same condition holds for two plaintext/ciphertext pairs $(P, C), (P^*, C^*)$, we obtain the following system of equations, that resembles (but is not equivalent to) the system of equations (3):

$$\begin{cases} C = E_2(E_0(P)), \\ C^* = E_2(E_0(P^*)). \end{cases} \tag{5}$$

We call plaintext/ciphertext pairs (P, C) for which the condition holds "special plaintexts".

The system of equations (5) can be constructed for a general scheme $E = E_2 \circ E_1 \circ E_0$, even if E_1 is not an involution. However, in general permutations there is only one fixed point on average, and thus, we need the entire codebook in order to exploit (5). When E_1 is an involution, we expect that it has about $2^{n/2}$ fixed points by Theorem 1, and thus, we can exploit (5) given as little as $2^{n/2}$ known plaintexts (we remind the reader that a small increase in the data complexity can increase the success rate).

The attack algorithm is very simple: The adversary asks for the encryption of $O(2^{n/2})$ known plaintexts $P_1, P_2, \ldots$ (where n is the block size of E) and denotes the corresponding ciphertexts by $C_1, C_2, \ldots$. For each of the $O(2^n)$ pairs[9]

[9] We alert the reader that in most slide attacks, the ordered pair (P_i, P_j) is different than the ordered pair (P_j, P_i), as the question of which plaintext is slid with respect to which plaintext does depend on the order.

(P_i, P_j), the adversary assumes that both P_i and P_j are special plaintexts and tries to solve the system of equations:

$$\begin{cases} C_i = E_2(E_0(P_i)), \\ C_j = E_2(E_0(P_j)). \end{cases} \tag{6}$$

If E_0 and E_2 are "simple enough", the adversary can solve the system efficiently and recover the key material used in E_0 and E_2. The data complexity of the attack is $O(2^{n/2})$ known plaintexts, and its time complexity is $O(2^n \cdot t)$, where t is the time required for solving the system (6).

In the special case in which $E_2 = Identity$, that was considered in the slide with a twist attack, the system of equations (6) is simplified to:

$$\begin{cases} C_i = E_0(P_i), \\ C_j = E_0(P_j). \end{cases} \tag{7}$$

The rest of the algorithm is the same as in the attack above.

3.2 Advantages Over the Mirror Slidex Attack

While the enhanced reflection framework looks very similar to the mirror slidex attack framework, it has several advantages over it:

1. **Attacks when $E_2 \circ E_0$ is simple.** In some cases, the function $E_2 \circ E_0$ is so simple, that a single pair $C = E_2(E_0(P))$ is sufficient for breaking $E_2 \circ E_0$. In such a case, the advantage of the enhanced reflection attack over mirror slidex can be huge, as its time complexity is only $O(2^{n/2} \cdot t)$ instead of $O(2^n \cdot t)$. Indeed, instead of iterating over all $O(2^n)$ pairs, it is sufficient to go over $O(2^{n/2})$ known plaintexts, assume for each plaintext P_i that it is special, and try to solve the equation $C_i = E_2(E_0(P_i))$. Such an optimization does not seem to be possible in the mirror slidex attack which inherently works with pairs and thus requires $O(2^n \cdot t)$ time. We demonstrate this advantage below in the concrete example of 18-round GOST, where mirror slidex requires 2^{64} time and the enhanced reflection attack requires only 2^{32} time.
2. **Exploiting differentials in E_1.** Consider the slide with a twist framework, i.e., ciphers of the form $E = E_2 \circ E_1$, and assume that there exists a differential $\alpha \to \beta$ for E_1 with probability $p \gg 2^{-n/2}$. In such a case, we can mount an improved chosen plaintext attack in which we attach to each plaintext/ciphertext pair (P, C) the pair $P^* = P \oplus \alpha$, $C^* = E(P \oplus \alpha)$. If some pair (P, C) is special, i.e., $E_1(P) = P$, then with probability p, we have $C^* = E(P^*) = E_2(P^* \oplus \beta)$, and thus, we obtain the system of equations:

$$\begin{cases} C = E_2(P), \\ C^* = E_2(P^* \oplus \beta). \end{cases} \tag{8}$$

   As the probability that a random plaintext (P, C) is special is $2^{n/2}$, this attack requires only $O(2^{n/2} \cdot (1/p) \cdot t)$ time, which may be significantly smaller

than the $O(2^n \cdot t)$ time complexity of the slide with a twist attack on the same variant. The same improvement can be obtained when the differential uses addition rather than XOR. Note that the slide with a twist attack cannot exploit differential properties of E_1 since it is *inherently independent* of the structure of E_1, apart from the fact that it is an involution.[10]

3. **Reducing the memory complexity in certain cases.** In some of the scenarios considered in [3,9], the mirror slidex attack can be optimized by reducing the system of equations (3) to a single equation of the form $P \oplus C = P^* \oplus C^*$. In such cases, the attack can be performed in time $O(2^{n/2})$ by sorting the plaintext/ciphertext pairs according to $P \oplus C$, and searching for a collision. Such an attack requires either $O(2^{n/2})$ memory or $O(2^{n/2})$ adaptively chosen plaintext queries (if we use Pollard's rho method). As we show in the examples of variants of the Even-Mansour construction below, in some of these cases, system (6) can be reduced to an extremely simple equation of the form $P \oplus C = f(K)$, for some simple function f. In such cases, the enhanced reflection attack can be performed in a memoryless manner, by iterating over $O(2^{n/2})$ known plaintexts, assuming for each plaintext that it is special, and testing the key suggestion instantly by trial encryption.
4. **Applying the two techniques in parallel.** As the enhanced reflection attack and the mirror slidex attacks exploit different properties of the data and both require only known plaintexts, they can be applied in parallel, using the same data set. While this does not reduce the overall time complexity of the attack, it reduces the data complexity by a factor of up to 2 (the exact factor depends on the desirable success probability of the attack).

3.3 Applications of the Enhanced Reflection Attack

In this section, we review several applications of the slide with a twist and mirror slidex attacks, and investigate how the enhanced reflection attack applies to them.

Reduced-Round Variants of GOST GOST [13] is the Russian government standard block cipher. It is a 64-bit block and 256-bit key cipher with a Feistel structure of 32 rounds. The round function accepts an input and a subkey of 32 bits each. As the exact structure of the round function is irrelevant to this work, we refer the interested reader to [13]. There are a few key recovery attacks on the full GOST in the single key-model (e.g., [8,14]), or in the multi-key settings (e.g., [6], which also uses fixed-point properties), and a simple 2 chosen plaintext related-key distinguisher is easy to construct for the full cipher. As we

[10] We note that in [17] the concept of probabilistic slide attacks is explored. The attack uses a differential $\alpha \rightarrow \beta$ for E_1, similarly to our framework. The data complexity of the attack is $O(2^{(n/2)} \cdot \sqrt{1/p})$ known plaintexts (and a similar memory complexity) with time complexity of $O(2^{n/2} \cdot \sqrt{1/p} \cdot t)$. Our approach uses more data (in the stricter chosen ciphertext model) but requires significantly smaller memory.

are interested in comparison of the enhanced reflection, we restrict ourselves to reduced-round variants of the GOST block cipher.

The key schedule algorithm takes the 256-bit key and treats it as eight 32-bit words, i.e., $K = K_1, \ldots, K_8$. The subkey SK_r of round r is

$$SK_r = \begin{cases} K_{(r-1) \bmod 8+1} & r \in \{1, \ldots, 24\}; \\ K_{33-r} & r \in \{25, \ldots, 32\}. \end{cases}$$

In [9], Dunkelman et al. showed that a reduced variant of GOST that consists of its last 20 rounds can be broken by a slide with a twist attack. The basic observation behind the attack is that the last 16 rounds of GOST constitute an involution, and thus, the last 20 rounds of GOST can be written as $E = E_1 \circ E_0$, where E_1 is an involution and E_0 is 4-round GOST. Thus, the slide with a twist attack can break 20-round GOST with 2^{33} known plaintexts and $2^{65} \cdot t$ time, where t is the time required to solve the system (4) for 4-round GOST. Since Dinur et al. [8] showed that 4-round GOST can be broken in 2^{12} time given two known plaintexts, the overall complexity of the attack is 2^{77} encryptions.

Using the enhanced reflection attack, we can break 20-round GOST with the same number of known plaintexts. Instead of the system of equations (4), we obtain the system (7) that can be solved with the same time complexity. Both attacks on 20-round GOST succeed once two fixed points are found, and for 2^{33} known plaintext (at least) two such fixed points exist with probability of 59.4%. With $2^{33.5}$ known plaintexts, the success rate jumps to about 90.8%.

In this case the enhanced reflection attack has the same time complexity and success rate as the previous attack. However, the advantage of the new technique over slide with a twist can be demonstrated by considering another reduced variant of GOST that consists of the last 18 rounds. This variant can again be written as $E = E_1 \circ E_0$, where E_1 is an involution, but in this case E_0 is 2-round GOST, which can be broken instantly given a *single known* plaintext/ciphertext pair. Hence, the new technique allows us to break this variant with about 2^{33} known plaintexts and 2^{33} time using key ranking techniques on the last two round keys. The slide with a twist attack on this variant requires 2^{64} time, as one cannot avoid checking all the 2^{64} candidate slid pairs.

We note that this attack on 18-round GOST can be considered as an instance of the original reflection attack [16] on GOST, which is based on exploiting fixed points of the last 16 rounds of GOST. However, the approach here is more general than in the reflection attack, and the same attack applies when the last 16 rounds of GOST are replaced by any involution, unlike in the original reflection attack that studies only certain special classes of involutions.

We further note that although our attacks on reduced GOST (as well as the previous attacks of [9]) do not recover the full 256-bit key, we still consider them as valid breaks of the scheme. The reason for this is that after we "peel off" the key material that surrounds the involution, the remaining scheme is not stronger than an involution, which is clearly a weak cipher (e.g., it has about $2^{n/2}$ fixed points, and therefore does not provide the privacy level required from a block cipher).

DESX and the Even-Mansour Construction DESX is an extension of DES proposed by Rivest in 1984, in order to defend DES against exhaustive key search attacks without changing its design significantly. It is defined as:

$$DESX_{K_0,K_1,K_2}(P) = K_2 \oplus DES_{K_1}(P \oplus K_0).$$

The Even-Mansour (EM) construction was proposed in 1991 by Even and Mansour [11], as an attempt to devise the "simplest possible" block cipher using a single unkeyed permutation. It is defined as:

$$EM_{K_0,K_1}(P) = K_1 \oplus \mathcal{F}(P \oplus K_0),$$

where $\mathcal{F}$ is modelled as a publicly known random permutation.

In [3], Biryukov and Wagner showed that the slide with a twist technique can be used to attack DESX and EM. The basic idea behind the attack is that since XOR with a key is an involution, EM can be represented as $E = E_1 \circ E_0$, where E_1 is an involution and $E_0(P) = \mathcal{F}(P \oplus K_0)$. In this case, the system of equations (4) can be written as:

$$\begin{cases} \mathcal{F}^{-1}(C_i) = P_j \oplus K_0, \\ \mathcal{F}^{-1}(C_j) = P_i \oplus K_0. \end{cases} \tag{9}$$

Summing these equations leads to cancellation of K_0, and after rearranging we obtain the single equation $P_i \oplus \mathcal{F}^{-1}(C_i) = P_j \oplus \mathcal{F}^{-1}(C_j)$. This allows to break EM in data and time of $O(2^{n/2})$, by sorting the plaintext/ciphertext pairs according to the value $P_i \oplus \mathcal{F}^{-1}(C_i)$ and looking for collisions.

DESX can be attacked in the same way, after guessing the value of K_1. For each of the 2^{56} possible DES keys, the above attack is repeated (each time taking 2^{33} known plaintexts and 2^{33} time). As the plaintexts can be reused for each DES key guess, the total data complexity of the attack on DESX is 2^{33} known plaintexts, and the time complexity is $2^{56} \cdot 2^{33} = 2^{89}$.

Somewhat surprisingly, these two attacks are the only cases we encountered so far in which the slide with a twist attack cannot be transformed to the new framework. The reason is prosaic: the XOR with a key, that is used as the involution in the attack, is so simple that it cannot be treated as a *random involution*, and thus, Theorem 1 does not apply. In fact, it is clear that unless the XORed key equals zero, this operation has no fixed points at all. This demonstrates that there exist very specific cases in which the enhanced reflection attack cannot replace the slide with a twist technique, and emphasizes the need to apply this attack carefully.

Variants of the Even-Mansour Construction In [9,10], Dunkelman et al. considered variants of EM where the random permutation $\mathcal{F}$ is an involution. Six variants were considered, and in all of them $\mathcal{I}$ is chosen at random among the set of involutions over n-bit values, and K_0, K_1 are independent n-bit keys. The first three variants are the following:

1. EM with involution (IEM): $E(P) = K_1 \oplus \mathcal{I}(P \oplus K_0)$
2. Addition EM with involution (AIEM): $E(P) = K_1 + \mathcal{I}(P + K_0)$,
3. Conjugation EM with involution (CIEM): $E(P) = -K_1 + \mathcal{I}(P + K_0)$,

The last three variants are a special case of the first three, in which $K_1 = K_0$. They are denoted SIEM, ASIEM, and CSIEM, respectively ("S" stands for single-key). Dunkelman et al. showed that in the IEM, AIEM, CIEM, and ASIEM variants the mirror slidex attack allows to recover $K_0 \oplus K_1$ or $K_0 + K_1$ using $O(2^{n/2})$ queries to E and no queries at all to $\mathcal{I}$. For the ASIEM variants , this constitutes a complete break of the construction, as the knowledge of $K_0 + K_0 = 2K_0$ reveals all the bits of K_0 except the most significant bit.

We present the enhanced reflection attack on AIEM, where similar attacks are applicable to the other variants. In the attack, AIEM is written as $E = E_2 \circ E_1 \circ E_0$, where $E_1 = \mathcal{I}$ is an involution, and E_0, E_2 are addition with a key. The system of equations (3) can be simplified in this case to

$$\begin{cases} C_i = P_j + K_0 + K_1, \\ C_j = P_i + K_0 + K_1. \end{cases} \tag{10}$$

If we subtract the two equations, the subkeys are cancelled, and after rearranging we obtain the equation $P_i + C_i = P_j + C_j$. Given $2^{n/2}$ queries to E, we expect such a pair with probability[11] 39.3%, which can be easily identified using $2^{n/2}$ time and memory without a single query to $\mathcal{I}$. The solution is then substituted into (10) to obtain $K_0 + K_1$.

The attack of [9] translates easily to the enhanced reflection framework. We consider pairs of special points $(P_i, C_i), (P_j, C_j)$. Instead of the system of equations (10), we obtain the system:

$$\begin{cases} C_i = P_i + K_0 + K_1, \\ C_j = P_j + K_0 + K_1. \end{cases} \tag{11}$$

After subtracting the two equations and rearranging we obtain the equation $P_i - C_i = P_j - C_j$. Such a pair can be found in $O(2^{n/2})$ time and memory using $2^{n/2}$ known plaintext queries to E and no queries to $\mathcal{I}$ (with probability of 39.3%).[12] The solution is then substituted into (11) to obtain $K_0 + K_1$.

In ASIEM, the situation turns out to be simpler. Each special plaintext yields the equation $C = P + K_0 + K_0$, which suggests only two values for K_0. These values can be tested immediately by a trial encryption. Hence, the enhanced

[11] To increase the probability of success to 90%, one should use $2^{n/2+1.1}$ known plaintexts.

[12] We note that both the slide with a twist attack as well as the reflection-based attack can be transformed into memoryless attacks using adaptive chosen plaintext queries and cycle finding algorithms. The resulting data complexity is about $2^{n/2}$ adaptively chosen plaintexts, and the time complexity is the same (and no additional memory is needed).

reflection attack on ASIEM is memoryless: The adversary examines $2^{n/2}$ plaintext/ciphertext pairs sequentially, and for each one of them she obtains two key suggestions that are checked immediately by a trial encryption. There is no need for more than a constant number of memory cells. It should be mentioned that in [9], memoryless variants of the mirror slidex attacks were also considered. However, these variants require $2^{n/2}$ *adaptively chosen* plaintexts, while our attack requires the same number of *known plaintexts*.

4 Improved Attacks on Feistel Constructions with Self Similarity: Reflection Attacks and Beyond

One of the first applications of the slide attack [2] is the cryptanalysis of Feistel constructions with self-similar round functions. Consider a Feistel construction E whose round function is $F(x) = f(x \oplus k)$, where k is a subkey and f is a public permutation. If the list of subkeys used in the encryption process is periodic with a period of length r, i.e., $K_1, K_2, \ldots, K_r, K_1, K_2, \ldots$, we say that E has an r-round self similarity. As this construction is obviously a generalization of the structure of DES, Biryukov and Wagner [2] called it rK-DES.

In [2], the slide attack was used to break 2K-DES using 2^{33} adaptively chosen plaintexts and 2^{33} time. In [3], Biryukov and Wagner used the slide with a twist attack to break 2K-DES and 4K-DES in 2^{33} data and time in the known plaintext model, and in 2^{17} data and time in the chosen plaintext model. Dunkelman et al. [10] used the mirror slidex framework to extend the attacks to 2K-DESX, defined as 2K-DES surrounded by key whitenings. It was mentioned in [10] that the mirror slidex attack cannot be extended to 4K-DESX.

In [16], Kara showed that 2K-DES can be broken by the original reflection attack that exploits fixed points of $(2m-1)$-round 2K-DES that turns out to be an involution. Kara's attack requires 2^{33} known plaintexts and time, but unlike the slide with a twist attack, it requires only a constant amount of memory. Kara's idea is essentially the same as the idea behind our attacks, but while we rely on a general property of random involutions to assure the existence of a large number of fixed points, Kara uses specific properties of Feistel constructions to determine the fixed points explicitly. As a result, the original reflection attack can be applied only in specific scenarios, and in particular, it cannot be applied against the ciphers considered in Section 3.3.

Since Feistel constructions with self similarity fall into the original reflection attack framework, we base our results in this section on the original reflection attack and its extensions. First, we present Kara's original reflection attack on 2K-DES, as well as two extensions that will allow extending the attack to 4K-DES. Then, we consider all known slide with a twist attacks on Feistel constructions with self similarity, and show that in all cases, the (enhanced) reflection attack can break the cipher with the same data and time complexities (in the known plaintext model). Finally, we show that the variant 4K-DESX, that cannot be attacked using mirror slidex (according to [10]), can be broken in less than 2^{40} data, memory and time, using an enhanced reflection attack.

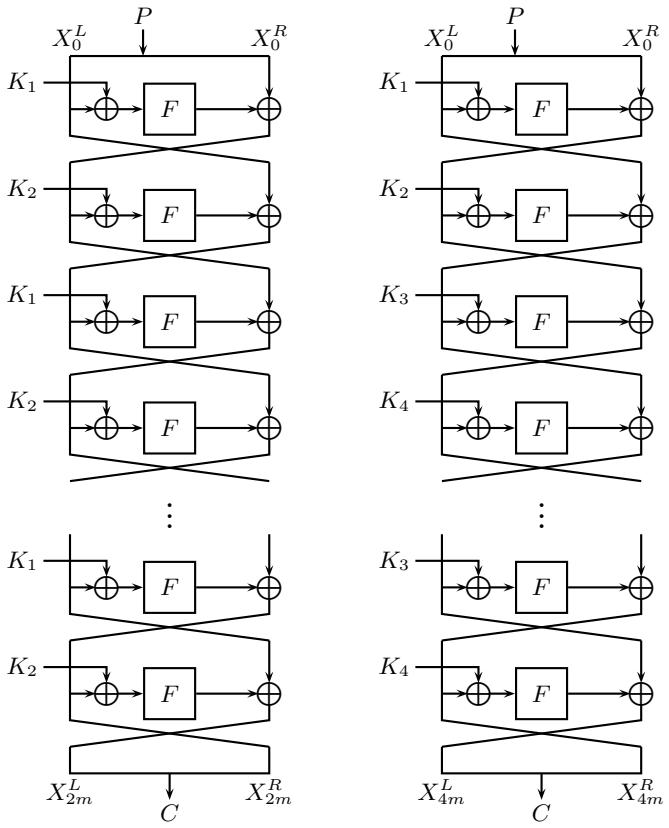

Fig. 2. The Structure of 2K-DES and 4K-DES

4.1 Reflection Properties of 2K-DES and 4K-DES

Throughout this section, E denotes a 2K-DES (or 4K-DES) construction with $2m$ (or $4m$) rounds (see Figure 2 for a figure describing 2K-DES). We denote the input to round i by (X_i^L, X_i^R). Hence, the plaintext is $P = (X_0^L, X_0^R)$ and the ciphertext is $C = (X_{2m}^L, X_{2m}^R)$ (or $C = (X_{4m}^L, X_{4m}^R)$, respectively). The output of the F-function in round r is denoted Out_r.

Kara's Reflection Attack on 2K-DES The original reflection attack on E is based on the following observation, made already in 1985 by Coppersmith [5].

Proposition 1. *Let (P, C) be a plaintext/ciphertext pair for $2m$-round 2K-DES, such that in the encryption process of P we have $Out_m = 0$. Then $P^L = C^L$ and $P^R = C^R \oplus Out_{2m}$.*

Proof. We prove by induction that for any $i \geq 1$, we have $X^L_{m+i} = X^L_{m-i}$. For $i = 1$, we have $X^L_{m+1} = X^L_{m-1} \oplus Out_m$, and thus, the assertion follows from the assumption $Out_m = 0$. Assume that the claim holds for all $i < t$. The assumption implies that $X^L_{m+t-1} = X^L_{m-t+1}$, and hence, $Out_{m+t-1} = F_{K_{m+t-1}}(X^L_{m+t-1}) = F_{K_{m-t+1}}(X^L_{m-t+1}) = Out_{m-t+1}$, as $K_{m+t-1} = K_{m-t+1}$ by the 2K-DES key schedule. Therefore,

$$X^L_{m+t} = X^L_{m+t-2} \oplus Out_{m+t-1} = X^L_{m-t+2} \oplus Out_{m-t+1} = X^L_{m-t}.$$

This completes the inductive proof. Substituting $i = m$, we obtain $P^L = X^L_0 = X^L_{2m} = C^L$. Substituting $i = m + 1$ (and treating a natural extension of the cipher in both directions), we obtain $P^R = X^L_{-1} = X^L_{2m+1} = C^R \oplus Out_{2m}$, as asserted.

We note that plaintext/ciphertext pairs that satisfy the assumption of the proposition are fixed points of the involution $\mathcal{I}$ composed of the $2m - 1$ rounds starting at 2 and ending at $2m$ of E. Hence, the proposition shows that if $\mathcal{F}$ is a permutation then the number of fixed points of $\mathcal{I}$ is at least $2^{n/2}$. In fact, as noted by Kara [16], Coppersmith [5] showed that these are the only fixed points of $\mathcal{I}$, and thus, $\mathcal{I}$ has exactly $2^{n/2}$ fixed points.

Definition 1. *If a plaintext/ciphertext pair (P, C) satisfies a reflection property (like the assumption of Proposition 1), it is called a* reflection point *of E.*

The property $P^L = C^L$ makes it possible to detect reflection points instantly. Then, given a reflection point, the equation $P^R = C^R \oplus Out_{2m}$ yields the suggestion $K_2 = f^{-1}(P^R \oplus C^R) \oplus C^L$. The suggestion can be checked instantly given another reflection point. Hence, the reflection attack requires $O(2^{n/2})$ known plaintexts and time and only a constant amount of memory.

Another Reflection Property of 2K-DES The following is an alternative reflection property of 2K-DES:

Proposition 2. *Let (P, C) be a plaintext/ciphertext pair for $2m$-round 2K-DES, such that in the encryption process of P we have $X^L_{m-1} = X^L_m \oplus \Delta$, where $\Delta = K_1 \oplus K_2$. Then $P^L = C^R \oplus \Delta$ and $P^R = C^L \oplus \Delta$.*

Proof. We prove by induction that for any $i \geq 1$, we have $X^L_{m+i-1} = X^L_{m-i} \oplus \Delta$. For $i = 1$, this is exactly the assumption. Assume that the claim holds for all $i < t$. The assumption implies that $X^L_{m+t-2} = X^L_{m-t+1} \oplus \Delta$, and hence, $Out_{m+t-2} = F_{K_{m+t-2}}(X^L_{m+t-2}) = F_{K_{m-t+1}}(X^L_{m-t+1}) = Out_{m-t+1}$ (as in 2K-DES the key schedule assures the $K_{m+t-2} \oplus K_{m-t+1} = \Delta$ for all t). Therefore,

$$X^L_{m+t-1} = X^L_{m+t-3} \oplus Out_{m+t-2} = X^L_{m-t+2} \oplus \Delta \oplus Out_{m-t+1} = X^L_{m-t} \oplus \Delta.$$

This completes the inductive proof. Substituting $i = m$, we obtain $P^L = X^L_0 = X^L_{2m-1} \oplus \Delta = C^R \oplus \Delta$. Substituting $i = m+1$ (and treating a natural extension of the cipher in both directions), we obtain $P^R = X^L_{-1} = X^L_{2m} \oplus \Delta = C^L \oplus \Delta$, as asserted.

Reflection points (according to the new property) can be detected instantly using the equation $P^L \oplus C^R = P^R \oplus C^L = \Delta$, along with a suggestion $K_1 \oplus K_2 = \Delta$. The attack can be completed, e.g., by exhaustive search over K_1 (given that $K_1 \oplus K_2$ is already known). The complexity of the attack is $2^{n/2}$ known plaintexts and time, and only a constant amount of memory. Finally, as the reflection points exploited in this attack are different from Kara's fixed points, this attack can be applied in parallel with Kara's attack, which results in reducing the data complexity by a factor of 2.

Reflection Property for 4K-DES Combining the ideas behind the two reflection properties for 2K-DES presented above, one can obtain the following reflection property of 4K-DES:

Proposition 3. *Let (P, C) be a plaintext/ciphertext pair for $4m$-round 4K-DES, such that in the encryption process of P we have $X^L_{2m-1} = X^L_{2m+1} \oplus \Delta$, where $\Delta = K_2 \oplus K_4$. Then $P^L = C^L$ and $P^R = C^R \oplus Out_{4m} \oplus \Delta$.*

Proof. We prove by induction that for any $i \geq 1$, we have

$$X^L_{2m+2i-1} = X^L_{2m-2i+1} \oplus \Delta \qquad \text{and} \qquad X^L_{2m+2i-2} = X^L_{2m-2i+2}.$$

For $i = 1$, this is exactly the assumption. Assume that the claim holds for all $i < t$. The assumption implies that $X^L_{2m+2t-3} = X^L_{2m-2t+3} \oplus \Delta$, and hence, $Out_{2m+2t-3} = F_{K_{2m+2t-3}}(X^L_{2m+2t-3}) = F_{K_{2m-2t+3}}(X^L_{2m-2t+3}) = Out_{2m-2t+3}$ by the key schedule of 4K-DES that assures that $K_{2m+2t-3} \oplus K_{2m-2t+3} = \Delta$ for all t. Therefore,

$$\begin{aligned} X^L_{2m+2t-2} &= X^L_{2m+2t-4} \oplus Out_{2m+2t-3} \\ &= X^L_{2m-2t+4} \oplus Out_{2m-2t+3} = X^L_{2m-2t+2}. \end{aligned} \tag{12}$$

By the structure of 4K-DES, the subkeys of rounds $2m + 2t - 2$ and $2m - 2t + 2$ are equal for all t. Hence, (12) implies $Out_{2m+2t-2} = Out_{2m-2t+2}$. Therefore,

$$\begin{aligned} X^L_{2m+2t-1} =& X^L_{2m+2t-3} \oplus Out_{2m+2t-2} = \\ & X^L_{2m-2t+3} \oplus \Delta \oplus Out_{2m-2t+2} = X^L_{2m-2t+1} \oplus \Delta. \end{aligned}$$

This completes the inductive proof (depicted in Figure 3). Substituting $i = 2m$, we obtain $P^L = X^L_0 = X^L_{4m} = C^L$. Substituting $i = 2m + 1$ (and treating a natural extension of the cipher in both directions), we obtain $P^R = X^L_{-1} = X^L_{4m+1} \oplus \Delta = C^R \oplus Out_{4m} \oplus \Delta$, as asserted.

The property $P^L = C^L$ allows us to detect reflection points instantly. Then, given a reflection point, the adversary guesses Δ and obtains a suggestion for K_4 from the equation $P^R = C^R \oplus Out_{4m} \oplus \Delta$. As suggestions for K_4 from different reflection points must coincide, three reflection points are sufficient to determine

both K_4 and Δ. The rest of the attack is trivial.[13], Therefore, the reflection attack requires $O(2^{n/2})$ known plaintexts (to obtain 3 reflection points) and time, and only a constant amount of memory.

4.2 Applications of the New Reflection Properties

In this section, we consider all Feistel constructions with self similar round functions studied in [3,10]. We show that all of them (including 4K-DESX for which the mirror slidex attack fails) can be broken by an enhanced reflection attack with the same data and time complexities (in the known plaintext model) as the slide with a twist attack, and sometimes with a lower memory complexity.

2K-DES and 4K-DES In [3], Biryukov and Wagner showed that 2K-DES and 4K-DES can be broken using the slide with a twist attack. The attacks require either $O(2^{n/2})$ data, time, and memory in the known plaintext model, and $O(2^{n/4})$ data, time and memory in the chosen plaintext model. The attack on 4K-DES is applied to a variant of DES proposed by Brown and Seberry [4] and to a 24-round variant of GOST under a weak key class, as both these ciphers are Feistel constructions with a 4-round self-similarity.

The attack on 2K-DES can be viewed as a typical application of the mirror slidex framework $E = E_2 \circ E_1 \circ E_0$, where E_2 is the identity function, E_1 is $(2m-1)$-round 2K-DES (which is an involution), and E_0 is a single DES round. The attack on 4K-DES is a bit more involved, as the role of E_1 is played by $(4m-3)$-round 4K-DES, which is not an involution.

As was shown in Section 4.1, both 2K-DES and 4K-DES can be broken by a reflection attack (either Kara's original attack or our enhanced reflection attacks) in data and time of $O(2^{n/2})$ and a constant amount of memory. Hence, our enhanced reflection attacks strictly improve over the attacks of [3] in the known plaintext model. It should be noted, however, that the reflection framework does not allow obtaining a speedup in the chosen plaintext model, and thus, when chosen plaintexts are available, the slide with a twist attacks of [3] are advantageous over our attacks.

Attacking 2K-DESX The construction 2K-DESX is defined as $E(P) = K_{post} \oplus (E'(K_{pre} \oplus P))$, where E' is 2K-DES with subkeys K_1, K_2. Note that K_1, K_2 are $n/2$-bit keys, while K_{pre}, K_{post} are n-bit keys.

In [10], Dunkelman et al. showed that 2K-DESX can be broken in $O(2^{n/2})$ known plaintexts and time using a variant of the mirror slidex attack. It was mentioned in [10] that the mirror slidex attack cannot break 4K-DESX. Instead, [10] considers a variant of 4K-DESX in which the last round of the middle Feistel part is removed, and shows that it can be broken in $O(2^{n/2})$ data and time, like 2K-DESX.

[13] We note that a similar reflection property exists with $P^R = C^R$ and $P^L = C^L \oplus Out_1 \oplus \Delta'$ for $\Delta' = K_1 \oplus K_3$. This property can be exploited while reusing the data used for the other attack.

Using our alternative reflection property for 2K-DES, we can break 2K-DESX in $O(2^{n/2})$ data and time (thus, achieving the same result as the mirror slidex attack of [10]). Let (P', C') be a reflection point of E' (that is an instantiation of 2K-DES, as defined above) according to our property. Then $P'^L \oplus C'^R = P'^R \oplus C'^L = K_1 \oplus K_2$. Hence, if $(P = P' \oplus K_{pre}, C = C' \oplus K_{post})$ is the corresponding plaintext/ciphertext pair for E, then (P, C) satisfies the system of equations:

$$\begin{cases} P^L \oplus C^R = K_1 \oplus K_2 \oplus K_{pre}^L \oplus K_{post}^R, \\ P^R \oplus C^L = K_1 \oplus K_2 \oplus K_{pre}^R \oplus K_{post}^L. \end{cases} \tag{13}$$

Note that the right hand side of both equations is equal for all reflection points. Hence, an adversary can ask for the encryption of $O(2^{n/2})$ known plaintexts and store them in a hash table, sorted according to $(P^L \oplus C^R, P^R \oplus C^L)$. Each pair of reflection points must yield a collision in the table (due to the system (13). On the other hand, as a collision is an n-bit condition, the table is expected to contain only $O(1)$ collisions. One of them is expected to follow from a pair of reflection points. Once the reflection points are detected, the system of equations (13) yields n bits of information on the secret keys. The rest of the keys can be recovered using auxiliary techniques.

The data and time complexities of the attack are $O(2^{n/2})$. Note that unlike the attack on 2K-DES, this attack cannot be performed in a memoryless manner (unless adaptively chosen plaintexts are used), since the reflection points are detected using a hash table. Thus, the complexity of this attack is exactly equal to the complexity of the mirror slidex attack on the same variant.

We note that Kara's reflection property cannot be used directly to attack 2K-DESX. Indeed, a fixed point (P', C') of E' with respect to Kara's property satisfies $P'^L = C'^L$, or equivalently, $P^L = C^L \oplus K_{pre}^L \oplus K_{post}^L$. Thus, any reflection point yields a suggestion for $K_{pre}^L \oplus K_{post}^L$. However, as mentioned in Section 4.1, E' has exactly $2^{n/2}$ reflection points and any non-reflection point satisfies $P'^L \neq C'^L$, and thus, necessarily suggests an incorrect value for $K_{pre}^L \oplus K_{post}^L$. Hence, the probability of the correct value of $K_{pre}^L \oplus K_{post}^L$ to be suggested is exactly $2^{-n/2}$, that is equal to the probability of a random suggestion. Therefore, the key material cannot be detected in a straightforward way.

Attacking 4K-DESX The advantage of the enhanced reflection attack over mirror slidex can be seen in the example of 4K-DESX that according to [10] cannot be attacked by mirror slidex. Our reflection property for 4K-DES allows to break 4K-DESX in $O(n2^{n/2})$ data and time.

Let (P', C') be a reflection point of E' (that is an instantiation of 4K-DES, as defined above), i.e., $P'^L = C'^L$. Hence, if $(P = P' \oplus K_{pre}, C = C' \oplus K_{post})$ is the corresponding plaintext/ciphertext pair for E, then (P, C) satisfies $P^L \oplus C^L = K_{pre}^L \oplus K_{post}^L$. In addition, a non-reflection point can be assumed to satisfy the $n/2$-bit condition $P^L \oplus C^L = K_{pre}^L \oplus K_{post}^L$ with probability $2^{-n/2}$. (Note that at this point, 4K-DESX differs from 2K-DESX where non-reflection points necessarily suggest wrong keys). Hence, the correct value of $K_{pre}^L \oplus K_{post}^L$ is

suggested with probability $2 \cdot 2^{-n/2}$, while each incorrect value is suggested with probability close to $2^{-n/2}$. This allows to detect the correct suggestion of $K^L_{pre} \oplus K^L_{post}$ using $O(n2^{n/2})$ known plaintexts and time. After the correct suggestion is detected, the adversary can detect the reflection points (as these points suggest the correct value of $K^L_{pre} \oplus K^L_{post}$), and then she can retrieve more key material by solving the second equation $P^R = C^R \oplus Out_{4m} \oplus (K_2 \oplus K_4) \oplus K^R_{pre} \oplus K^R_{post}$. (For example, she can guess $(K_2 \oplus K_4) \oplus K^R_{pre} \oplus K^R_{post}$ and check whether two reflection points yield the same suggestion for K_4 – the subkey used in F_{4m}). The rest of the key can be retrieved by auxiliary techniques.

The total data and time complexities of the attack are $O(n2^{n/2})$. As in the attack on 2K-DESX, it is not clear how to execute this attack in a memoryless manner, since the reflection points are detected using a key ranking procedure.

5 Conclusions

In this paper we devised an enhanced reflection attack which exploits the large number of fixed points we expect to find in random involutions which are located deep inside the cryptosystem. We showed that this attack is at least as good (and in many cases better) than the slide with a twist attack which was introduced in 2000, except when the involution is too simple and non-random (e.g., XORing a non-zero key is an involution which has no fixed points). In particular, we used it to improve the best known attack on GOST reduced to 18 rounds, and on DESX in which the key schedule repeats itself every four rounds.

Acknowledgements

The second author was supported in part by the Israel Science Foundation through grants No. 827/12 and No. 1910/12. The third author was supported by the Alon Fellowship.

References

1. Bard, G.V., Ault, S.V., Courtois, N.T.: Statistics of Random Permutations and the Cryptanalysis of Periodic Block Ciphers. Cryptologia 36(3), 240–262 (2012), http://dx.doi.org/10.1080/01611194.2011.632806
2. Biryukov, A., Wagner, D.: Slide Attacks. In: Knudsen, L.R. (ed.) Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1636, pp. 245–259. Springer (1999), http://dx.doi.org/10.1007/3-540-48519-8_18
3. Biryukov, A., Wagner, D.: Advanced Slide Attacks. In: Preneel, B. (ed.) Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding. Lecture Notes in Computer Science, vol. 1807, pp. 589–606. Springer (2000), http://dx.doi.org/10.1007/3-540-45539-6_41

4. Brown, L., Seberry, J.: Key Scheduling In Des Type Cryptosystems. In: Seberry, J., Pieprzyk, J. (eds.) Advances in Cryptology - AUSCRYPT '90, International Conference on Cryptology, Sydney, Australia, January 8-11, 1990, Proceedings. Lecture Notes in Computer Science, vol. 453, pp. 221–228. Springer (1990), http://dx.doi.org/10.1007/BFb0030363
5. Coppersmith, D.: The Real Reason for Rivest's Phenomenon. In: Williams [19], pp. 535–536, http://dx.doi.org/10.1007/3-540-39799-X_42
6. Courtois, N.: Algebraic Complexity Reduction and Cryptanalysis of GOST. IACR Cryptology ePrint Archive 2011, 626 (2011), http://eprint.iacr.org/2011/626
7. Courtois, N.T., Bard, G.V.: Random Permutation Statistics and an Improved Slide-Determine Attack on KeeLoq. In: Naccache, D. (ed.) Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday. Lecture Notes in Computer Science, vol. 6805, pp. 35–54. Springer (2012), http://dx.doi.org/10.1007/978-3-642-28368-0_6
8. Dinur, I., Dunkelman, O., Shamir, A.: Improved Attacks on Full GOST. In: Canteaut, A. (ed.) Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers. Lecture Notes in Computer Science, vol. 7549, pp. 9–28. Springer (2012), http://dx.doi.org/10.1007/978-3-642-34047-5_2
9. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7237, pp. 336–354. Springer (2012), http://dx.doi.org/10.1007/978-3-642-29011-4_21
10. Dunkelman, O., Keller, N., Shamir, A.: Slidex Attacks on the Even-Mansour Encryption Scheme. J. Cryptology 28(1), 1–28 (2015), http://dx.doi.org/10.1007/s00145-013-9164-7
11. Even, S., Mansour, Y.: A Construction of a Cipher from a Single Pseudorandom Permutation. J. Cryptology 10(3), 151–162 (1997), http://dx.doi.org/10.1007/s001459900025
12. Flajolet, P., Sedgewick, R.: Analytic Combinatorics. Cambridge University Press (2009), http://www.cambridge.org/uk/catalogue/catalogue.asp?isbn=9780521898065
13. Government Committee of the USSR for Standards: Gosudarstvennei Standard 28147-89: Cryptographic Protection for Data Processing Systems. Tech. rep. (1989)
14. Isobe, T.: A Single-Key Attack on the Full GOST Block Cipher. In: Joux, A. (ed.) Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers. Lecture Notes in Computer Science, vol. 6733, pp. 290–305. Springer (2011), http://dx.doi.org/10.1007/978-3-642-21702-9_17
15. Jr., B.S.K., Rivest, R.L., Sherman, A.T.: Is DES a pure cipher? (results of more cycling experiments on DES). In: Williams [19], pp. 212–226, http://dx.doi.org/10.1007/3-540-39799-X_17
16. Kara, O.: Reflection Attacks on Product Ciphers. IACR Cryptology ePrint Archive 2007, 43 (2007), http://eprint.iacr.org/2007/043
17. Soleimany, H.: Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro. In: Cid, C., Rechberger, C. (eds.) Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers. Lecture Notes in Computer Science, vol. 8540, pp. 373–389. Springer (2014), http://dx.doi.org/10.1007/978-3-662-46706-0_19

18. Soleimany, H., Blondeau, C., Yu, X., Wu, W., Nyberg, K., Zhang, H., Zhang, L., Wang, Y.: Reflection Cryptanalysis of PRINCE-Like Ciphers. In: Moriai, S. (ed.) Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers. Lecture Notes in Computer Science, vol. 8424, pp. 71–91. Springer (2013), http://dx.doi.org/10.1007/978-3-662-43933-3_5
19. Williams, H.C. (ed.): Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings, Lecture Notes in Computer Science, vol. 218. Springer (1986)

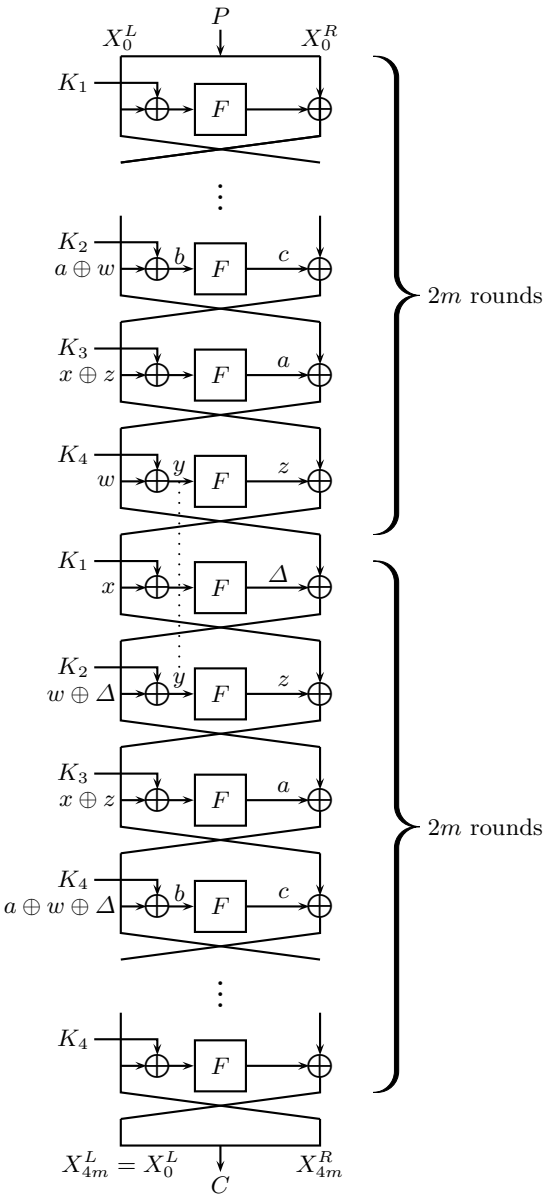

Fig. 3. The New 4K-DES Reflection Property