Cryptanalysis of Symmetric Block Ciphers Based on the Feistel Network with Non-bijective S-boxes in the Round Function

Roman Oliynykov

Kharkov National University of Radioelectronics,
Ukraine
ROliynykov@gmail.com

Abstract. We consider ciphertext-only attack on symmetric block ciphers based on the Feistel network with secret S-boxes installed as an additional parameter, like in Soviet GOST 28147-89. In case when S-boxes are generated by authorized agency and cannot be verified by end-user of the cipher (e.g., in case of special equipment for encryption), application of non-bijective S-boxes allows significantly decrease deciphering complexity for authorized agency preserving high-level strength for other cryptanalysts. We show that it is necessary to have non-bijective S-boxes which outputs form non-trivial subgroup and give an example for deciphering complexity with known and secret non-bijective S-boxes for GOST.

1 Introduction

Symmetric block encryption algorithms are among of the most widely used cryptographic primitives [1]. In addition to providing confidentiality via encryption, they are often used as basic primitives in construction of hash functions, generation of pseudorandom sequences [2], etc.

One of the most common approaches in the high-level design of symmetric block ciphers is the Feistel network [3], which allows to get properties of pseudorandom permutation (block cipher) by iterative application of pseudorandom function (round transformation) [4]. This approach is used by DES [5], Camellia [6], Lucifer [7], and Soviet GOST 28147 [8]. Special feature of the Feistel network is the following: round function processing half of the block may be implemented as non-bijective transformation; encryption remains revertible, so correct decryption is possible for any type of the round function.

Non-linear transformation in modern block ciphers is usually implemented by substitution tables, or S-boxes. In some algorithms like Rijndael/AES [9], Camellia and other, developers declared the possibility of application of different S-boxes with the same properties, but in GOST 28147 S-boxes are additional secret parameters.

S-boxes properties are extremely important for cipher's strength to differential [10], linear [11], algebraic [12] and other types of cryptanalysis. Collision among output values of S-boxes may significantly decrease the strength of the cipher to differential cryptanalysis [13].

Complexity of ciphertext-only cryptanalysis for Feistel network based block ciphers with non-bijective S-boxes is not researched very well. For some ciphers, like Camellia and GOST, there are used "n-to-n" S-boxes (assumed to be bijective by design), for other ciphers, like DES and Blowfish [14], S-boxes are "m-to-n", where m is not equal to n. We propose a method for estimation of ciphertext-only cryptanalysis for block ciphers with currently installed S-boxes that have prohibited output values, and, therefore, non-bijective.

2 Model of Symmetric Block Cipher Based on the Feistel Network

Let's consider n-round ($n = 2m$) block cipher with $2l$ bit block size based on the Feistel network without initial and final permutation or whitening. Encryption transformation of such algorithm can be presented as

$$\begin{aligned} F_K &= \varphi_{n,k_n} \circ \varphi_{n-1,k_{n-1}} \circ \cdots \circ \varphi_{1,k_1} \ , \\ \varphi_{i,k_i}\left(x_i^L, x_i^R\right) &= \left(x_i^R, f\left(x_i^R, k_i\right) \oplus x_i^L\right) \ , \end{aligned} \tag{1}$$

where $K = (k_1, k_2, \cdots, k_n)$ is the sequence of round keys after the key schedule;

x_i^L and x_i^R are the values of the left and right halves of the block (each of l bits) on the input to the i-th round.

Round function $f\left(x_i, k_i\right)$ consists of initial linear transformation (for most modern ciphers it is identity), addition with the round key, S-boxes and following linear transformation:

$$f(x_i, k_i) = s(x_i \cdot E + k_i) \cdot L \ , \tag{2}$$

where E is a matrix of $l \times q$ size over $GF(2)$, for description of the initial linear transformation;

$s(x)$ is S-box layer, which performs substitution of input value of q bits to output value of l bits (application of S-boxes);

L is a matrix of $l \times l$ size over $GF(2)$, for description of the round function linear transformation.

For almost all modern block ciphers initial linear transformation is absent (the matrix E is the identity matrix of $l \times l$ size). DES is only one exception for widespread ciphers, it has E as a bit selection table, extending 32 bits to 48, so this matrix has 32×48 size.

Usually, non-linear transformation $s(x)$ is implemented as parallel application of S-boxes. Input vector is divided into several subvectors $x = (x_t, x_{t-1}, \cdots, x_1)$, each of them is substituted via S-box: $s(x) = (s_t(x_t), s_{t-1}(x_{t-1}), \cdots, s_1(x_1))$. Correspondingly, the number of S-boxes and their input and output size in bits are related by $|x_j| = q/t$ and $|s(x_j)| = l/t$.

After S-boxes output vector of l bits is processed by linear transformation. Without dependence on specific transformation (bit permutation, MDS-matrix multiplication, etc.), the general formula for its description is the matrix multiplication over $GF(2)$.

Widespread ciphers, like DES, Camellia, GOST, etc. can be described by (1) and (2).

3 Ciphertext-only Cryptanalysis with Known Non-bijective S-boxes

We consider here the main task of cryptanalyst on ciphertext-only attack is to obtain corresponding plaintexts without recovering secret encryption key.

Ciphertext $\left(c^L, c^R\right) = \left(x_{n+1}^R, x_{n+1}^L\right)$ can be presented via plaintext $\left(p^L, p^R\right) = \left(x_1^L, x_1^R\right)$ with (1) and (2):

$$\begin{cases} c^L = p^R \oplus \left(\bigoplus_{i=1}^{n/2} f_{2i}\left(x_{2i}^R, k_{2i}\right) \right) \\ c^R = p^L \oplus \left(\bigoplus_{i=1}^{n/2} f_{2i-1}\left(x_{2i-1}^R, k_{2i-1}\right) \right) \end{cases} . \tag{3}$$

Let

$$\begin{aligned} \gamma^L &= \bigoplus_{i=1}^{n/2} f_{2i}\left(x_{2i}^R, k_{2i}\right) \text{ and} \\ \gamma^R &= \bigoplus_{i=1}^{n/2} f_{2i-1}\left(x_{2i-1}^R, k_{2i-1}\right) . \end{aligned} \tag{4}$$

From (3) it can be obtained

$$\begin{cases} c_L = p^R \oplus \gamma^L \\ c_R = p^L \oplus \gamma^R \end{cases} . \tag{5}$$

Complexity of plaintext recovery from a ciphertext for a Feistel-based cipher completely defined by the complexity of XOR sum discovering of the round function outputs for odd and even rounds. It is obvious, that for a strong cipher $\left|\left\{\gamma^L\right\}\right| = \left|\left\{\gamma^R\right\}\right| = 2^l$.

Let's further consider ciphers with a permutation matrix L. This matrix describes a final linear transformation of the round function as a bit permutation (or rotation). It is possible to take an arbitrary matrix L, but in this case it is needed to combine the matrix with the output values of S-boxes, which gives much less common results.

For a permutation matrix L values (4) depend on output of S-boxes only. Application of non-bijective S-boxes allows to almost completely exclude influence of both round function inputs x_i^L, x_i^R, so as round keys k_i.

Application of non-bijective S-boxes will influence the cipher's strength to differential, linear cryptanalysis, etc. But such attacks are known or chosen plaintext attacks, while we are considering ciphertext only attack with general aim of recovering plaintext.

As an additional information on ciphertext only attack cryptanalyst should have a simple criterion for distinguishing acceptable plaintext from a random

sequence of symbols (e.g., knowledge of the plaintext natural language). In such conditions there can be applied an attack for exhaustive search of all possible values of (4) and obtaining all variants of plaintext via (5).

In general case, with bijective S-boxes and random independent round keys it is $\left|\left\{\gamma^L\right\}\right| = \left|\left\{\gamma^R\right\}\right| = 2^l$, and the solution is a full set of all possible plaintexts. Ciphertexts give no additional information to cryptanalyst in this model.

Let's consider the particular case when S-boxes are non-bijective, and the matrix L is a permutation matrix. Now it is possible $\left|\left\{\gamma^L\right\}\right| < 2^l$, $\left|\left\{\gamma^R\right\}\right| < 2^l$, and deciphering can be done with the complexity less than exhaustive search of all possible values of (4).

For non-bijective S-boxes "$\frac{q}{t}$ bits to $\frac{l}{t}$ bits" from all possible $2^{\frac{l}{t}}$ output combinations some of them are suppressed, so $\left|\left\{s(x_j)\left|x_j \in GF\left(2^{\frac{q}{t}}\right)\right.\right\}\right| < 2^{\frac{l}{t}}$

If it is supposed, that the considered property is a hidden trapdoor allowing reading of encrypted messages without knowledge of the key, then for decreasing complexity of the attack the cryptanalyst will decrease cardinality of $\left\{\gamma^L\right\}$ and $\left\{\gamma^R\right\}$.

According to (3), it is necessary for cryptanalyst to exhaust all possible combinations of (4). These values are obtained as bitwise XOR of l-bit vectors on the output of the round function. Complexity of the attack depends on the cardinal number of the XOR results set.

Let's exclude from consideration trivial variants when number of all possible output values of round function is less than the number of rounds (e.g., all input values of S-box are transformed into a single constant). Then the cardinality of this set will be not less than the cardinal number of round function outputs set:

$$\left|\left\{\gamma^L\right\}\right| \geq \left|\left\{f_{2i}\left(x_{2i}^R, k_{2i}\right)\right\}\right| \quad . \tag{6}$$

Respectively, for obtaining minimally reachable complexity of the ciphertext-only cryptanalysis it is needed a strict equation:

$$\left|\left\{\gamma^L\right\}\right| = \left|\left\{f_{2i}\left(x_{2i}^R, k_{2i}\right)\right\}\right| \quad . \tag{7}$$

From (7) it follows that addition (XORing) result of arbitrary output values of cipher's round function must give an acceptable value for a single output of the same round function. The set $\left\{f_{2i}\left(x_{2i}^R, k_{2i}\right)\right\}$ must be closed concerning operation $\oplus$ (XOR).

Operation $\oplus$ for a set of l-bits vectors is associative, has a neutral element (zero vector), and for each vector there exist an inverse. Therefore, sets $\left\{\gamma^L\right\}$ and $\left\{\gamma^R\right\}$ with operation $\oplus$ have all these properties. Bringing the additional closure property $\left(\forall\gamma_a, \gamma_b \in \left\{\gamma^L\right\}\ \exists!\gamma_c = \gamma_a \oplus \gamma_b,\ \gamma_c \in \left\{\gamma^L\right\}\right)$ leads to that algebraic systems $\left\langle\left\{\gamma^L\right\}, \oplus\right\rangle$ and $\left\langle\left\{\gamma^R\right\}, \oplus\right\rangle$ must be groups.

As long as groups $\left\langle\left\{\gamma^L\right\}, \oplus\right\rangle$ and $\left\langle\left\{\gamma^R\right\}, \oplus\right\rangle$ have the same properties and equal, each of them will be defined as $\langle\{\gamma\}, \oplus\rangle$.

Output of the round function is formed by outputs of t non-bijective S-boxes with the following bit permutation. In this case each encryption value γ is formed as concatenation and bit permutation of t bit vectors, each of them independently

calculated as a sum (XOR) of $\frac{n}{2}$ S-box output values of $\frac{l}{t}$ bit length. From this follows, that outputs of each S-box must form a group.

Let $l_S = \frac{l}{t}$ be a length of the binary vector in the S-box output. The full set of l_S-bit vectors has the cardinal number equal to 2^{l_S} and forms a group $G^S = \left\langle \left\{\gamma^S\right\}, \oplus \right\rangle$. For decreasing the complexity of cryptanalysis it is necessary to form a non-trivial subgroup G' of G^S, which will contain all outputs of non-bijective S-box. Any group or subgroup contains neutral element, so among all possible values there always be a zero vector.

From Lagrange's theorem it is known [15] that for any finite group, the order of every subgroup divides the order of the group. From this follows that cardinality of G' must be power of 2, i.e. $|G'| \in \left\{2, 4, \cdots, 2^{l_s - 1}\right\}$.

Each of t binary vectors used for generation of output encryption value γ, is independently formed. Let $\theta_1^S = |G'_1|$, $\theta_2^S = |G'_2|, \ldots, \theta_t^S = |G'_t|$ be the cardinalities of subgroups, formed by outputs of each non-bijective S-boxes of the round function with linear permutation matrix of Feistel-based block cipher. Then the complexity of obtaining each plaintext from the ciphertext without the encryption key is

$$\Theta = \left(\prod_{i=1}^{t} \theta_i^S\right)^2 \quad . \tag{8}$$

If the S-box output values set cardinality is equal ($\theta_1^S = \theta_2^S = \cdots = \theta_t^S = \theta^S$), then from (8) it can be obtained

$$\Theta^E = \left(\theta^S\right)^{2t} \quad . \tag{9}$$

From (8) and (9) it follows that when $\theta_j^S < 2^{\frac{l}{t}}$ $\left(\theta^s < 2^{\frac{l}{t}}\right)$, it is $\Theta < 2^{2l}$, so application of non-bijective S-boxes decreases the complexity of cryptanalysis.

4 Ciphertext-only Cryptanalysis With Secret Non-bijective S-boxes

Let's consider additional cryptanalysis task when S-boxes are non-bijective and kept secret as the second key element (together with the encryption key). Like in previous case, the cryptanalyst has a simple criterion for distinguishing acceptable plaintext from a random sequence of symbols. Besides it, cryptanalyst may know (or guess with high probability of success) the cardinality of S-box output values set θ^S.

This task is more complex because cryptanalyst needs to exhaustive search of possible variants of S-box outputs. One value (zero vector) is always known, and it is necessary to find the rest $\theta_j^S - 1$ outputs from $2^{\frac{l}{t}}$ variants for each S-box (all S-boxes may be different). So as order of S-box outputs is important, the general number of variants for each S-box is equal to

$$\omega_j^S = A_{2^{\frac{l}{t}}-1}^{\theta_j^S - 1} = \frac{\left(2^{\frac{l}{t}} - 1\right)!}{\left(2^{\frac{l}{t}} - \theta_j^S\right)!} \quad . \tag{10}$$

Making assumption for the cryptanalyst's favor that for distinguishing one wrong S-boxes set it is enough to analyze one half of the cipher's block only (but not only subvector corresponding to the single output for one S-box), from (8) and (10) there can be obtained complexity for cryptanalysis for the secret non-bijective S-boxes:

$$\Theta^S = \left(\prod_{j=1}^{t} \omega_j^S\right) \cdot \left(\prod_{i=1}^{t} \theta_i^S\right) = \prod_{i=1}^{t} \left(\theta_i^S \frac{\left(2^{\frac{l}{t}} - 1\right)!}{\left(2^{\frac{l}{t}} - \theta_i^S\right)!}\right) \quad . \tag{11}$$

If the S-box output values set cardinality is equal ($\theta_1^S = \theta_2^S = \cdots = \theta_t^S = \theta^S$), then from (11) it can be obtained

$$\Theta^{SE} = \left(\theta^S \frac{\left(2^{\frac{l}{t}} - 1\right)!}{\left(2^{\frac{l}{t}} - \theta^S\right)!}\right)^t \quad . \tag{12}$$

Let's note that after successful deciphering of the first block the cryptanalyst has all secret S-boxes at the same time. For all further blocks complexity of analysis is equal to values obtained according to (8) or (9).

From (11) and (12) it follows that application of secret S-boxes significantly increases the complexity of the attack, and attack becomes practically impossible even with a small cardinality of the output values group.

5 Application to GOST

GOST 28147 was adopted in 1990 [8] and now it is still to be the most widespread cipher in Russia, Ukraine and other ex-USSR countries. GOST is a Feistel-based cipher with 32 rounds and extremely simple round function [1], which consist on modulo 2^{32} addition with a round key, eight S-boxes "4-to-4 bits" and cyclic bits shifting.

Let's discuss an example when S-boxes for GOST are generated by authorized agency and delivered on special media to equipment for encryption. So, S-boxes are secret and unknown both for end-user of this equipment, so as for external cryptanalysts. Encryption key is generated by end-user and unknown both for external cryptanalysts and authorized agency.

In this example $n = 32$ is the number of rounds, $2l = 64$ is the cipher's block size ($l = 32$ is the half of the block size), $q = l = 32$, E is an identity matrix, $t = 8$ is the number of S-boxes, $|x_j| = |s(x_j)| = \frac{l}{t} = 4$ is the number of bits of S-box input and output, L is a permutation matrix.

Examples of several non-bijective S-boxes for GOST forming subgroups of different order is given in the Table 1. Let's mention, that equal probabilities of the chosen values do not have an influence to the complexity of the attack. Besides, it is possible that with application of such S-boxes some bits of ciphertexts are always be equal to corresponding bits of plaintexts (especially for subgroups

Table 1. Examples of non-bijective S-boxes for GOST

#	Subgroup order	S-box															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	15	0	0	15	15	0	15	0	0	0	15	15	0	15	0	15
2	2	0	12	12	12	0	12	12	0	0	0	0	12	0	12	12	0
3	4	9	1	9	8	8	0	0	0	1	8	1	9	9	0	1	8
4	4	6	2	0	4	6	2	0	4	0	6	4	2	0	6	2	4
5	8	13	5	0	8	4	12	1	9	0	5	13	4	1	9	8	12
6	8	10	11	3	2	1	8	0	10	0	2	1	9	3	8	11	9

of small order). Let's assume that cardinalities of output values set for each non-bijective S-box are equal. In addition, let's assume that cryptanalyst's criterion for distinguishing of acceptable plaintext from a random sequence of symbols requires 32 bits (4 symbols) of plaintext.

Deciphering complexity of ciphertext into plaintext without knowledge of encryption key is given in the Table 2, for the authorized agency with the knowledge of S-boxes (Θ^E) and for an external cryptanalysts without knowledge of S-boxes (Θ^{SE}) for different order of subgroup of S-boxes output. Therefore, if an end-user

Table 2. Ciphertext-only deciphering complexity for GOST with non-bijective S-boxes

S-box subgroup order	Complexity for authorized agency	Complexity for an external cryptanalysts	Note
1	1	1	No encryption
2	2^{16}	$2^{39,3}$	
4	2^{32}	$>2^{64}$	
8	2^{48}	$>2^{64}$	
16	2^{64}	$>2^{64}$	Normal mode with bijective S-boxes

of encryption equipment is forced to use secret non-bijective S-boxes, authorized agency can rather easily decipher ciphertexts by generation of S-boxes with output values set cardinality equal to 4 or higher. External cryptanalysts practically cannot decipher such ciphertexts.

6 Conclusions

Our results give the lower bound of ciphertext-only cryptanalysis complexity for symmetric block ciphers based on the Feistel network with the non-bijective S-boxes in the round function.

In condition that output values of each non-bijective S-box form non-trivial subgroup with the following application of a permutation matrix in the round

function, complexity of deciphering without knowledge of the encryption key is lower than the exhaustive search.

Decreasing of cryptanalysis complexity is also possible for non-permutation matrices, but in this case it is necessary to take into account internal structure of S-boxes.

Besides Feistel network, this attack may also be applied to Lai-Massey scheme as a high-level structure of block ciphers (IDEA NXT/FOX) with selection of non-bijective S-boxes.

Complexity of described attack does not depend on the number of rounds in symmetric block ciphers.

References

1. Schneier, F.: Applied Cryptography. New York: Wiley, 1996.
2. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. Boca Raton, StateFL: CRC Press, 1997.
3. Fiestel, H.: "Cryptography and Computer Privacy". Scientific American, v. 228, n. 5, May 73, pp. 15-23.
4. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput, 1988.
5. FIPS PUB 46-3. Federal Information Processing Standards Publication. U.S. Department Of Commerce/National Institute of Standards and Technology. Data Encryption Standard (DES). National Technical Information Service, Springfield StateVA, 1999. – 51p.
6. Aoki K., Ichikawa T., Kanda M., et al: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms. Nessie. September 26, 2000. http://www.cryptonessie.org.
7. Ben-Aroya, E., Biham, E.: Differential cryptanalysis of Lucifer. Advances in Cryptology — EUROCRYPT'93, Springer-Verlag, Berlin, 1993, pp. 187-199.
8. GOST 28147-89. Information processing systems. Cryptographic security. Algorithm of cryptographic transformation. Moscow, State Standard of the USSR, 1990.
9. Daemen, J., Rijmen, V.: AES Proposal: Rijndael. National Institute for Standards and Technology (NIST). "AES: A Crypto Algorithm for the Twenty-First Century". http://www.nist.gov/aes
10. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, StateNew York, 1993. – 312p.
11. Matsui, M.: Linear Cryptanalysis Method for the DES Cipher. Lecture Notes in Computer Science, Advances in Cryptology, proceedings of Eurocrypt '93, 1993. pp. 27-41.
12. Courtis, N. T.: Cryptanalysis of Block Cipher with Overdefined System of Equations / N. T. Courtois, J. Pieprzyk. // Asiacrypt 2002: http://eprint.iacr.org/2002/044.pdf
13. Vaudenay, S.: On the Weak Keys in Blowfish, *Fast Software Encryption, Third International Workshop Proceedings*, Springer-Verlag, 1996, pp. 27-32.
14. Schneier, B.: "The Blowfish Encryption Algorithm," Dr. Dobb's Journal, v. 19, n. 4, April 1994, pp. 38-40.
15. Lidl, R., Niederreiter, H.: "Finite Fields," Encyclopedia of Mathematics and its Applications 20, 2nd Ed. Cambridge University Press, 1997.