Mathematica Slovaca

Marcel Zanechal

An algebraic approach to fix points of GOST-algorithm

Mathematica Slovaca, Vol. 51 (2001), No. 5, 583--591

Persistent URL: `http://dml.cz/dmlcz/136854`

Mathematica Slovaca
© 2001
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **51** (2001), No. 5, 583–591

AN ALGEBRAIC APPROACH TO FIX POINTS OF GOST-ALGORITHM

MARCEL ZANECHAL

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Cryptosystem GOST belongs to DES-like cryptosystems. GOST has been published in [*Sistemy obrabotki informacii. Zashchita kryptograficheskaya, Algoritm kriptograficheskogo preobrazovaniya.* Gosudarstvennyi Standart Soyuza SSR. GOST: 28147-89, IPK Izdatelstvo standartov, Moskva, 1989], and partially analyzed in [CHARNES, C.—O'CONNOR, L.—PIEPRZYK, J.—SAFAVI-NAINI, R. ZHENG, Y.: *Comments on Soviet encryption algorithm.* Preprint, April 29, 1994].

In this paper we analyze fix points of GOST-algorithm. It is known that there exist 2^{32} fix points when a weak key is in use in this algorithm. But we have never seen any proof of this fact. So we give our brief proof of this property. Using polynomial analysis we show an exact form of these fix points when zero key is active (note that zero key is also a weak key), and all S-boxes are identity permutations. As far as we know such an approach has not been used yet.

1. Preliminaries

Cryptosystem GOST has been published in [2]. In the present time we know some other papers concerning this algorithm: [1], [3], [5], [6], [7]. Papers [3] and [6] present only a brief description of GOST-algorithm. Paper [5] treats a special kind of cryptanalysis of GOST (key-schedule cryptanalysis). In [7] one can find, besides description of GOST, also general differences of GOST and DES algorithms. Only one paper which gives first results of cryptanalysis of GOST-algorithm [1] appears in the open literature. Another paper [4] has been submitted to a computer journal.

Algorithm GOST is a block cipher which can operate in some different modes We analyse this algorithm in its basic mode, namely in *ECB* mode (Electronic Code Book). Note that in this mode GOST transforms 64-bits input block to 64-bits output block in 32 rounds. Besides secret 256-bits of a key, GOST

2000 Mathematics Subject Classification: Primary 68P25, 94A60.
Keywords: GOST, fix point, cryptanalysis.

exploits 8 secret 4 × 4 bijective substitution boxes (S-boxes). One can find details of GOST-algorithm in above mentioned papers.

2. Basic notions

Denote ciphering using GOST-algorithm under actual key $K \in \mathbb{Z}_2^{256}$ and S-boxes $S_1, \dots, S_8$ by $GOST_{K,S_1,\dots,S_8} \colon \mathbb{Z}_2^{64} \to \mathbb{Z}_2^{64}$ where $S_i \colon \mathbb{Z}_2^4 \to \mathbb{Z}_2^4$, $i = 1, \dots, 8$.

To analyse algorithm GOST we use polynomials. Arbitrary string of 32 bits can be considered as a polynomial of the degree at most 31. To be sharp a 32 bits string $(a_{31}, a_{30}, \dots, a_0)$ can be considered as a polynomial $a_0 \oplus a_1 \cdot x \oplus \cdots \oplus a_{31} \cdot x^{31}$ over $\mathbb{Z}_2$, or element of commutative ring $\mathbb{Z}_2[x]$ modulo $(x^{32} \oplus 1)$ with standard operations "XOR" and "AND". Denote this ring of polynomials by $\mathcal{K}$.

GOST-algorithm works in 32 rounds. In all rounds GOST transforms 64-bits input tuple to 64-bits output tuple using actual 32-bits subkey. Main 256-bit key is divided into eight subkeys which are used in order $K_1, \dots, K_8, K_1, \dots, K_8$, $K_1, \dots, K_8, K_8, \dots, K_1$.

In each round input tuple is divided into two halves. The right half and actual subkey act as input of round function. The output and the left half are XORed to produce new right half and the right half becomes new left half. After last round two halves are swapped. Round function consists of addition modulo 2^{32} of the right half and actual subkey. After using eight S-boxes (each S-box is a permutation of the numbers 0 through 15) a 32-bit word is rotated by 11 bits to the left.

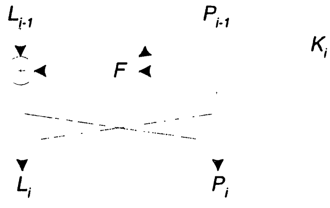

FIGURE 1. ith round of algorithm GOST.

For $i = 1, \dots, 32$, let L_i, and P_i be left and right 32 output bits of ith round. Denote by L_0, and P_0 left and right 32 input bits of the first round (i.e. of a plaintext). There is one round of GOST-algorithm in Figure 1 with round function denoted by F. Only exception is last round where swap of halves is omitted. Note that $L_1, P_1, \dots, L_{32}, P_{32} \in \mathcal{K}$. This means that transformation $GOST$ can also be considered as a function from $\mathcal{K} \times \mathcal{K}$ to $\mathcal{K} \times \mathcal{K}$.

Further, let for $i = 1, 2, 3, 4$, L^{2i-1}, and P^{2i-1} be left and right half of the output after $8 \cdot i$ rounds. Let $L^{2(i-1)}$, and $P^{2(i-1)}$ be left and right half of the input to $\left[8(i-1)+1\right]$th round (see Figure 2). Note that subkeys are used in reverse order in the last eight rounds.

A fix point of GOST-algorithm is an element $(L, P) \in \mathcal{K} \times \mathcal{K}$ which satisfies

$$GOST(L, P) = (L, P) . \tag{1}$$

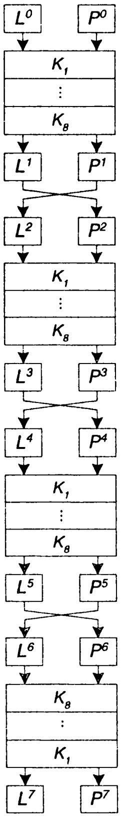

FIGURE 2. Algorithm GOST.

3. Fix points under a weak key

It is clear (from the description of GOST-algorithm) that for subkeys $K_1, \ldots$ $\ldots, K_8$ satisfying

$$K_1 = K_8 , \quad K_2 = K_7 , \quad K_3 = K_6 , \quad K_4 = K_5$$

deciphering is equal to ciphering. Moreover, for any S-box $S_1, \dots, S_8$ (denoted by S), and any plaintext $(L, P) \in \mathcal{K} \times \mathcal{K}$

$$GOST_{K_1,K_2,K_3,K_4,K_4,K_3,K_2,K_1,S}(GOST_{K_1,K_2,K_3,K_4,K_4,K_3,K_2,K_1,S}(L,P)) \\ = (L,P) \tag{2}$$

is valid.

Definition 1. Keys with derived subkeys satisfying (2) are called *weak keys* of algorithm GOST.

Theorem 1. *There exist* 2^{32} *fix points of GOST-algorithm when a weak key is in use.*

Although this fact is known we have never seen any proof of previous theorem. We give our one.

Proof. From Figure 2 it is clear that for fix points (i.e. $(L^0, P^0) = (L^7, P^7)$) of GOST-algorithm it holds that

$$(L^1, P^1) = (L^6, P^6). \tag{3}$$

But when a weak key is in use, then $K_1 = K_8$, $K_2 = K_7$, $K_3 = K_6$, $K_4 = K_5$. From Figure 2 it follows that

$$(L^3, P^3) = (L^4, P^4) \tag{4}$$

and

$$L^3 = P^4 \quad \& \quad L^4 = P^3. \tag{5}$$

From (4) and (5) we have

$$L^3 = P^3. \tag{6}$$

Thus (L^0, P^0) is a fix point of GOST-algorithm if and only if property (6) holds. Equation (6) has exactly 2^{32} solutions. Hence there exist exactly 2^{32} fix points of GOST-algorithm. □

4. Polynomial analysis

It is very difficult to handle with 32 bits during analysis. For this reason we use polynomial analysis. As far as we know such an approach has not been used yet.

Suppose now that the key is all the zeroes string, and all S-boxes are identity permutations in GOST-algorithm. It is clear (from the description of round function of algorithm GOST — see e.g. [2]) that the round function F is only 11 bits rotation to the highest significant bit now. Thus

$$F(P) = x^{11} \cdot P \qquad \text{for any} \quad P \in \mathcal{K} . \tag{7}$$

From Figure 1 and (7) it follows that

$$L_1 = L_0 \oplus x^{11} \cdot P_0 \quad \& \quad P_1 = P_0 . \tag{8}$$

We can summarize (8) in a matrix form as

$$\begin{pmatrix} L_1 \\ P_1 \end{pmatrix} = \begin{pmatrix} 1 & x^{11} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} L_0 \\ P_0 \end{pmatrix} . \tag{9}$$

From Figure 1 and (7), for $i = 1, \dots, 31$ it follows that

$$L_{i+1} = P_i \oplus x^{11} \cdot L_i \quad \& \quad P_{i+1} = L_i . \tag{10}$$

Again, in a matrix form

$$\begin{pmatrix} L_{i+1} \\ P_{i+1} \end{pmatrix} = \begin{pmatrix} x^{11} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} L_i \\ P_i \end{pmatrix} . \tag{11}$$

From (9) and (11) we have

$$\begin{pmatrix} L_{32} \\ P_{32} \end{pmatrix} = \begin{pmatrix} x^{11} & 1 \\ 1 & 0 \end{pmatrix}^{31} \begin{pmatrix} 1 & x^{11} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} L_0 \\ P_0 \end{pmatrix} . \tag{12}$$

After reduction in ring $\mathcal{K}$, from (12) we obtain

$$\begin{pmatrix} L_{32} \\ P_{32} \end{pmatrix} = \begin{pmatrix} x^{21} & x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20} \\ 1 \oplus x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20} & x^{21} \end{pmatrix} \begin{pmatrix} L_0 \\ P_0 \end{pmatrix} . \tag{13}$$

Thus a fix point (L, P) must satisfy

$$(x^{21} \oplus 1)L \oplus (x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20})P = 0 , \tag{14}$$

$$(1 \oplus x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20})L \oplus (x^{21} \oplus 1)P = 0 . \tag{15}$$

Recall that $(x^{32} \oplus 1) = (x \oplus 1)^{32}$ and $(1 \oplus x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20}) = (1 \oplus x^4 \oplus x^5 \oplus x^8 \oplus x^{10})^2$. Moreover, $(1 \oplus x^4 \oplus x^5 \oplus x^8 \oplus x^{10})$ is irreducible polynomial. Hence there exists an inverse polynomial to $(1 \oplus x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20})$, namely $(1 \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^6 \oplus x^7)^2 (1 \oplus x \oplus x^6 \oplus x^7 \oplus x^8)^2$. Thus

$$L = (1 \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^6 \oplus x^7)^2 (1 \oplus x \oplus x^6 \oplus x^7 \oplus x^8)^2 (x^{21} \oplus 1) P . \tag{16}$$

From here and (14) it follows

$$\begin{gathered} (1 \oplus x^2 \oplus x^3 \oplus x^4 \oplus x^5 \oplus x^6 \oplus x^7)^2 (1 \oplus x \oplus x^6 \oplus x^7 \oplus x^8)^2 \cdot \\ \cdot (x^{21} \oplus 1)^2 P \oplus (x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20}) P = 0 . \end{gathered} \tag{17}$$

Table 1. Relations between L and P of fix points for all rotations.

rot	**R** (L = RP)
0	0
1	$x^{31} \oplus x^{28} \oplus x^{27} \oplus x^{26} \oplus x^{25} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{9} \oplus x^{8} \oplus x^{7} \oplus x^{6} \oplus x^{5} \oplus x^{4} \oplus x^{3} \oplus x^{2} \oplus x \oplus 1$
2	$x^{28} \oplus x^{26} \oplus x^{16} \oplus x^{14} \oplus x^{12} \oplus x^{10} \oplus x^{8} \oplus x^{6} \oplus x^{4} \oplus x^{2}$
3	$x^{30} \oplus x^{29} \oplus x^{27} \oplus x^{24} \oplus x^{21} \oplus x^{20} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{9} \oplus x^{7} \oplus x^{6} \oplus x^{4} \oplus x^{3} \oplus x \oplus 1$
4	$x^{28} \oplus x^{16} \oplus x^{12} \oplus x^{8} \oplus x^{4} \oplus 1$
5	$x^{30} \oplus x^{29} \oplus x^{28} \oplus x^{27} \oplus x^{25} \oplus x^{23} \oplus x^{20} \oplus x^{18} \oplus x^{16} \oplus x^{15} \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{8} \oplus x^{7} \oplus x^{6} \oplus x^{5} \oplus x^{3} \oplus x^{2} \oplus x \oplus 1$
6	$x^{30} \oplus x^{24} \oplus x^{20} \oplus x^{18} \oplus x^{16} \oplus x^{14} \oplus x^{12} \oplus x^{10} \oplus x^{6} \oplus x^{4}$
7	$x^{31} \oplus x^{29} \oplus x^{28} \oplus x^{27} \oplus x^{25} \oplus x^{24} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{10} \oplus x^{9} \oplus x^{7} \oplus x^{6} \oplus x^{4} \oplus x^{3} \oplus x^{2} \oplus 1$
8	$x^{16} \oplus x^{8}$
9	$x^{31} \oplus x^{30} \oplus x^{28} \oplus x^{27} \oplus x^{26} \oplus x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{13} \oplus x^{12} \oplus x^{10} \oplus x^{9} \oplus x^{8} \oplus x^{7} \oplus x^{4} \oplus x^{3} \oplus x \oplus 1$
10	$x^{30} \oplus x^{28} \oplus x^{20} \oplus x^{18} \oplus x^{16} \oplus x^{12} \oplus x^{10} \oplus x^{8} \oplus x^{6} \oplus x^{2}$
11	$x^{30} \oplus x^{26} \oplus x^{25} \oplus x^{24} \oplus x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{9} \oplus x^{5} \oplus x^{4} \oplus x^{3} \oplus x^{2} \oplus x \oplus 1$
12	$x^{24} \oplus x^{20} \oplus x^{16} \oplus x^{12} \oplus x^{4} \oplus 1$
13	$x^{31} \oplus x^{28} \oplus x^{27} \oplus x^{26} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{18} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{12} \oplus x^{9} \oplus x^{8} \oplus x^{7} \oplus x^{5} \oplus x^{3} \oplus x^{2} \oplus x \oplus 1$
14	$x^{28} \oplus x^{24} \oplus x^{22} \oplus x^{20} \oplus x^{16} \oplus x^{14} \oplus x^{10} \oplus x^{6} \oplus x^{4} \oplus x^{2}$
15	$x^{30} \oplus x^{28} \oplus x^{26} \oplus x^{24} \oplus x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{13} \oplus x^{11} \oplus x^{9} \oplus x^{7} \oplus x^{6} \oplus x^{5} \oplus x^{4} \oplus x^{3} \oplus x \oplus 1$
16	$x^{16} \oplus 1$
17	$x^{31} \oplus x^{29} \oplus x^{28} \oplus x^{27} \oplus x^{26} \oplus x^{25} \oplus x^{23} \oplus x^{21} \oplus x^{19} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{9} \oplus x^{8} \oplus x^{6} \oplus x^{4} \oplus x^{2} \oplus 1$
18	$x^{30} \oplus x^{28} \oplus x^{26} \oplus x^{22} \oplus x^{18} \oplus x^{16} \oplus x^{12} \oplus x^{10} \oplus x^{8} \oplus x^{4}$
19	$x^{31} \oplus x^{30} \oplus x^{29} \oplus x^{27} \oplus x^{25} \oplus x^{24} \oplus x^{23} \oplus x^{20} \oplus x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{14} \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{6} \oplus x^{5} \oplus x^{4} \oplus x \oplus 1$
20	$x^{28} \oplus x^{20} \oplus x^{16} \oplus x^{12} \oplus x^{8} \oplus 1$
21	$x^{31} \oplus x^{30} \oplus x^{29} \oplus x^{28} \oplus x^{27} \oplus x^{23} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{9} \oplus x^{8} \oplus x^{7} \oplus x^{6} \oplus x^{2} \oplus 1$
22	$x^{30} \oplus x^{26} \oplus x^{24} \oplus x^{22} \oplus x^{20} \oplus x^{16} \oplus x^{14} \oplus x^{12} \oplus x^{4} \oplus x^{2}$
23	$x^{31} \oplus x^{29} \oplus x^{28} \oplus x^{25} \oplus x^{24} \oplus x^{23} \oplus x^{22} \oplus x^{20} \oplus x^{19} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{11} \oplus x^{10} \oplus x^{9} \oplus x^{6} \oplus x^{5} \oplus x^{4} \oplus x^{2} \oplus x \oplus 1$
24	$x^{24} \oplus x^{16}$
25	$x^{30} \oplus x^{29} \oplus x^{28} \oplus x^{26} \oplus x^{25} \oplus x^{23} \oplus x^{22} \oplus x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{12} \oplus x^{11} \oplus x^{10} \oplus x^{8} \oplus x^{7} \oplus x^{5} \oplus x^{4} \oplus x^{3} \oplus x \oplus 1$
26	$x^{28} \oplus x^{26} \oplus x^{22} \oplus x^{20} \oplus x^{18} \oplus x^{16} \oplus x^{14} \oplus x^{12} \oplus x^{8} \oplus x^{2}$
27	$x^{31} \oplus x^{30} \oplus x^{29} \oplus x^{27} \oplus x^{26} \oplus x^{25} \oplus x^{24} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{17} \oplus x^{16} \oplus x^{14} \oplus x^{12} \oplus x^{9} \oplus x^{7} \oplus x^{5} \oplus x^{4} \oplus x^{3} \oplus x^{2} \oplus 1$
28	$x^{28} \oplus x^{24} \oplus x^{20} \oplus x^{16} \oplus x^{4} \oplus 1$
29	$x^{31} \oplus x^{29} \oplus x^{28} \oplus x^{26} \oplus x^{25} \oplus x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{14} \oplus x^{12} \oplus x^{11} \oplus x^{8} \oplus x^{5} \oplus x^{3} \oplus x^{2} \oplus 1$
30	$x^{30} \oplus x^{28} \oplus x^{26} \oplus x^{24} \oplus x^{22} \oplus x^{20} \oplus x^{18} \oplus x^{16} \oplus x^{6} \oplus x^{4}$
31	$x^{31} \oplus x^{30} \oplus x^{29} \oplus x^{28} \oplus x^{27} \oplus x^{26} \oplus x^{25} \oplus x^{24} \oplus x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{16} \oplus x^{7} \oplus x^{6} \oplus x^{5} \oplus x^{4} \oplus x \oplus 1$

After reduction we can write

$$(x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20})P \oplus (x^8 \oplus x^{10} \oplus x^{16} \oplus x^{20})P = 0 . \qquad (18)$$

Relation (18) clearly holds for all $P \in \mathcal{K}$. This implies that $(L, P) \in \mathcal{K} \times \mathcal{K}$ is a fix point if and only if (16) is true. After reduction of (16) we obtain the following condition for a fix point of GOST-algorithm

$$L = (x^{30} \oplus x^{26} \oplus x^{25} \oplus x^{24} \oplus x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{19} \oplus x^{16} \oplus x^{15} \oplus x^{14} \\ \oplus x^{13} \oplus x^{12} \oplus x^{11} \oplus x^{9} \oplus x^{5} \oplus x^{4} \oplus x^{3} \oplus x^{2} \oplus x \oplus 1)P . \qquad (19)$$

Thus we proved next theorem.

THEOREM 2. *Let the key of GOST algorithm be all zeroes string, and all S-boxes are identity permutations. Then $(L, P) \in \mathcal{K} \times \mathcal{K}$ is a fix point of GOST algorithm if and only if* (19) *is satisfied.*

When zero key and identity permutations (S-boxes) are in use in GOST-algorithm, then a crucial point of this algorithm is the number of shifts in round function rotation. Recall that this is 11 bits rotation to the highest significant bit. From analysis of all possible rotations x^t, $t = 0, 1, \ldots, 31$, as a corollary we obtain:

COROLLARY 1. *For any possible rotation x^t, $t = 0, 1, \ldots, 31$, there exist 2^{32} fix points.*

In Table 1 we list similar relations to (19) for all possible rotations.

5. General case

Here we consider a situation when an arbitrary key and arbitrary S-boxes are in use in GOST-algorithm. Finding fix points of GOST-algorithm by our approach is a very complicated problem. Already a partial situation, when an arbitrary key and identity permutations (S-boxes) are in use, is also complicated. A subkey and a half of a plaintext in a round is mixed using addition modulo 2^{32} instead of standard exclusive-or addition. And this is the reason why polynomial analysis is not effective in this case.

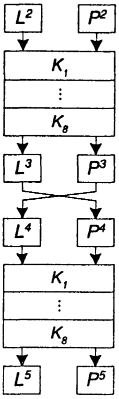

FIGURE 3. Reduction of GOST-algorithm.

From Figure 2 it is clear that for fix points (i.e. $(L^0, P^0) = (L^7, P^7)$) of algorithm GOST in the general case, relation (3) must be satisfied as well. Thus we can analyse fix points of the reduced GOST-algorithm. This reduction (see Figure 3) consists of 16 rounds of GOST-algorithm. These are rounds from 9th to 24th round. From above it is clear there is a simple bijection between fix points of the reduced algorithm GOST and fix points of full GOST-algorithm.

6. Conclusions

In this paper we present a brief proof of existence of 2^{32} fix points of GOST-algorithm when a weak key is in use. Using polynomial analysis we described exact form of fix points of algorithm GOST under the condition that zero key and identity permutations (S-boxes) are in use. Moreover we showed exact form of these fix points not only for 11 bits rotation but for any possible rotation in GOST round function. An open problem is the existence and number of fix points of GOST-algorithm in general case (i.e. case when arbitrary key and arbitrary S-boxes are in use). As a partial result in this case we show a reduction of this problem to a problem of finding fix points of 16 rounds of the algorithm.

REFERENCES

[1] CHARNES, C.—O'CONNOR, L.—PIEPRZYK, J.—SAFAVI-NAINI, R.—ZHENG, Y.: *Comments on Soviet encryption algorithm.* Preprint, April 29, 1994.

[2] *Sistemy obrabotki informacii. Zashchita kryptograficheskaya, Algoritm kriptograficheskogo preobrazovaniya.* Gosudarstvennyi Standart Soyuza SSR, GOST: 28147-89, IPK Izdatelstvo standartov, Moskva, 1989.

[3] *Cryptographic Protection for Data Processing Systems, Cryptographic Transformation Algorithm.* Government Standard of the U.S.S.R., GOST: 28147-89 (Translated from the Russian by Aleksandr Malchik) Sun Microsystems Laboratories, Mountain View, California August 20, 1994.

[4] GROŠEK, O.—NEMOGA, K.—ZANECHAL, M.: *Why to use bijective S-boxes in the GOST ciphering algorithm*, Informatica, Ljubljana (Slovenia) (Submitted).

[5] KELSEY, J.—SCHNEIER, B.—WAGNER, D.: *Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES.* Advances in Cryptology — CRYPTO '96. Lecture Notes in Comput. Sci. 1109, Springer-Verlag, Berlin, 1996.

[6] PIEPRZYK, J.—TOMBAK, L.: *Soviet encryption algorithm.* Preprint, November 24, 1993 and Jun 1, 1994.

[7] SCHNEIER, B.: *Applied Cryptography* (2nd ed.), J. Wiley & Sons, New York, 1996.

Received July 23, 1998
Revised November 15, 2000

Ministry of Interior
SK-812 72 Bratislava
SLOVAKIA
E-mail: zanechal@minv.sk