ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 2
2016

II INTERNATIONAL BALTIC SYMPOSIUM ON APPLIED AND INDUSTRIAL MATHEMATICS

F. A. Dali, G. B. Marshalko, V. O. Mironkin (Moscow, TC26, TC26, NRU HSE). **Rotational analysis of 2-GOST.**

1. Introduction. In [1] Ondros and Zajac proposed a framework for rotational analysis of GOST 28147-89 block cipher with identical s-boxes. In this paper we study rotational probabilities for 2-GOST block cipher, which is a modification of GOST 28147-89 with different key schedule and two fixed s-boxes.

Probabilistic properties of the family of *ARX*-transformations, that consist of only three types of operations: bitwise addition modulo 2, addition modulo 2^n and rotation of a string, have been extensively studied in recent years. In 2007 Khovratovich and Nicolic introduced [1] rotational analysis, which could be effectively applied to this type of transformations. Rotational analysis exploits the fact that the rotation of an input passes through round transformations of a scheme.

In this work, based on the framework proposed in [2], we study properties of the encryption algorithm 2-GOST [4]. We show that, despite the fact that this algorithm does not belong to the family of *ARX*-transformations, in some cases in is possible to evaluate its rotational properties and evaluate the applicability of rotational analysis.

2. Rotational property. We introduce the following notation:

$\ggg_r$ circular rotation by r positions in the direction of lower order components;

$\overrightarrow{X}_r$ circular rotation of X by r positions in the direction of higher order components.

Consider the pairs of the strings $(X, \overrightarrow{X}_r)$, $(Y, \overrightarrow{Y}_r)$, $X, Y \in V_n$, where the second string is a rotation of the first string by r bits (the rotation can be toward lower-order digits, and towards the senior level). Pairs of this type will be called a rotational pairs.

Definition. Let's say that rotation pairs $(X, \overrightarrow{X}_r)$, $(Y, \overrightarrow{Y}_r)$ *pass through operation* $*$, if $\overrightarrow{(X * Y)}_r = \overrightarrow{X}_r * \overrightarrow{Y}_r$.

For example, any rotational pairs $(X, \overrightarrow{X}_r)$, $(Y, \overrightarrow{Y}_r)$ pass through the operation XOR and bitwise rotation, since these operations commute:

$$\overrightarrow{(X \oplus Y)}_r = \overrightarrow{X}_r \oplus \overrightarrow{Y}_r, \overrightarrow{X_r} \ggg_s = \overrightarrow{(X \ggg_s)}_r.$$

Let $P_r(*)$ be the probability of the passage of rotational pairs through the operation $*$. Consider addition modulo 2^n. According to [3]

$$P_r(\boxplus) = \frac{1}{4}(1 + 2^{r-n} + 2^{-r} + 2^{-n}).$$

Consider an arbitrary transformation $f : V_n \to V_n$ from the family of ARX-transformation.

Let f contains q operations of addition modulo 2^n, $X, \overrightarrow{X}_r \in V_n$ — input strings of the transformation f. Then according to [1]

$$P_r(f) = P_r(\boxplus)^q. \tag{1}$$

Note that for an arbitrary random transformation $\varphi : V_n \to V_n$ random rotational pairs pass it with probability $P_r(\varphi) = 2^{-n}$. Therefore, in case $P_r(f) > 2^{-n}$ there is a possibility for constructing of a statistical distinguishing criteria. For example, when $r = 1$ any ARX, which has less than $\frac{n}{1.415}$ additions modulo 2^n, preserves rotational property.

3. Rotational property for GOST 28147-89 block cipher with identical s-boxes.

Let E_K be a Feistel cipher with N rounds, round function f, (L_0, R_0) and round keys $K_0, K_1, \ldots, K_{N-1}$.

The encryption could be represented by the following equations:

$$\begin{cases} L_{i+1} = R_i, \\ R_{i+1} = L_i \oplus f(R_i, K_i), \end{cases} \quad where \quad i = 0, 1, \ldots, n-1.$$

Then under the assumption of independence of round keys K_i for rotational pairs $((L_0, R_0), \overrightarrow{(L_0, R_0)}_r)$ when $(K, \overrightarrow{K}_r)$: $P_r(E_K) \approx P_r(f)^N$.

If f is ARX-transformation with q operations of addition modulo 2^n, in order to obtain numerical estimates for (3) one can use relation (1):

$$P_r(E_K) \approx P_r(\boxplus)^{qN}.$$

R e m a r k 1. In general, the approach of calculating the probability $P_r(E_K)$ is not applicable since the round keys may be dependent and round transformation may also use a nonlinear substitution.

Consider block cipher GOST 28147-89 (hereafter – GOST), which is a Feistel cipher with 32 rounds, a block size of 64 bits and 256-bit master key K, and a set of eight 4-bit s-boxes $\pi_0, \pi_1, \ldots \pi_7$. Master key K is represents as a concatenation of 32-bit subkeys $K^i, i = 0, 1, \ldots, 7$, $K = K^0 || K^1 || \ldots || K^7$.

Note that GOST does not belong to the family of ARX transformations and the round keys are not independent. However, if we consider GOST without s-boxes, i.e. replacing all s-boxes with identical s-box, we get an ARX-transformation.

Let L_i, R_i be two 32-bit halves of the input string at the i-th round of GOST, $i = 1, 2, \ldots, 32$.

Round keys $K_1, K_2, \ldots, K_{32}$ are derived from the master key in the following order: $K^0, K^1, \ldots, K^7, K^0, K^1, \ldots, K^7, K^0, K^1, \ldots, K^7, K^7, K^6, \ldots, K^0$.

Round function of the GOST algorithm has the form of

$$\begin{cases} L_{i+1} = R_i, \\ R_{i+1} = L_i \oplus (f(R_i \boxplus K^{i(\mathrm{mod}\ 8)}) \lll_{11}), \end{cases} \quad where \quad i = 0, 1, \ldots, 23,$$

$$\begin{cases} L_{i+1} = R_i, \\ R_{i+1} = L_i \oplus (f(R_i \boxplus K^{31-i(\mathrm{mod}\ 8)}) \lll_{11}), \end{cases} \quad where \quad i = 24, 25, \ldots, 31.$$

In [2] it is shown that if all s-boxes of GOST are identical, for random key K and random input strings P (at the fixed rotational value r) the probability of preservation of rotational pairs is $P_r(\mathrm{GOST}) > 2^{-64}$.

Let us denote the first r bit in an arbitrary string $A \in V_n$ as $r^+(A)$, and the remaining $(n - p)$ bits as $r^-(A)$.

Let $K, X_1, X_2, \ldots, X_t \in V_n$ are independent strings. Then according to [2] the probability $P_{r,t}(\boxplus)$ that a rotational pairs $(X_i, \overrightarrow{(X_i)}_r)$ and $(K, \overrightarrow{K}_r)$, $i = 1, 2, \ldots, t$ through the addition modulo 2^n is equal to

$$P_{r,t}(\boxplus) = 2^{-n(t+1)} \sum_{r^+(K)=0}^{2^r-1} (2^r - r^+(K))^t \sum_{r^-(K)=0}^{2^{n-r}-1} (2^{n-r} - r^-(K))^t.$$

Assuming that the first 8 round keys of GOST are independent, we obtain that the probability of rotational pairs after 8 rounds of transformation of GOST equals $P_{r,1}(\boxplus)^8$.

Starting from round 9 round keys in GOST key schedule repeat, so the rotation of the pair $(K_9, \overrightarrow{(K_9)}_r)$ coincides with the pair $(K_0, \overrightarrow{(K_0)}_r)$. Then the probability of rotational pairs after 9 rounds equals to $P_{r,1}(\boxplus)^7 \cdot P_{r,2}(\boxplus)$. Arguing similarly, we obtain that the probability of rotational pairs after 32 rounds is $P_{r,4}(\boxplus)^8$.

Table. Rotational probabilities after each round of GOST

N	1	2	...	8	9	10	...	16	...	25	26	...	32
$P_{r,t}$	$P_{r,1}$	$P_{r,1}^2$	...	$P_{r,1}^8$	$P_{r,1}^7 P_{r,2}$	$P_{r,1}^6 P_{r,2}^2$	...	$P_{r,2}^8$	...	$P_{r,3}^7 P_{r,4}$	$P_{r,3}^6 P_{r,4}^2$	...	$P_{r,4}^8$

For example, if $r = 1, 4, 16$ for GOST without s-boxes we get the following estimates:

r	1	4	16
${P_{r,4}}^8$	$2^{-27.8}$	$2^{-35.5}$	$2^{-37.2}$

R e m a r k 2. For GOST with identical s-boxes the results will remain the same when r is a multiple of 4 [2]. And the maximum for the discussed probability is obtained for $r = 4$.

4. Rotational property for 2-GOST. Algorithm 2-GOST [4] is a modification of algorithm GOST. For 2-GOST $\pi_0 = \cdots = \pi_3 = \alpha_0, \pi_4 = \cdots = \pi_7 = \alpha_1,$ and a key schedule has the following form:

$$K^0, K^1, K^2, K^3, K^4, K^5, K^6, K^7, K^3, K^4, K^5, K^6, K^7, K^0, K^1, K^2,$$
$$K^5, K^6, K^7, K^0, K^1, K^2, K^3, K^4, K^6, K^5, K^4, K^3, K^2, K^1, K^0, K^7.$$

Note that the sequences of round keys in 2-GOST and GOST differ starting from round 9. Therefore, the probabilities of passing fixed rotational pairs through l rounds of 2-GOST and GOST, $l \in \{9, 10, \ldots, 31\}$, will be different. However, changing the order of the round keys will not affect the rotational probability after all 32 rounds (since it depends only on the number of occurrences of subkeys $K^i, i = 9, 10, \ldots, 31,$ in the key schedule) in the case where s-boxes α_0 and α_1 are equal to identity s-box, and the rotational value r is a multiple of 4. Thus, $P_r(\text{2-GOST}) = P_{r,4}(\boxplus)^8$.

Now consider the case of two different 4-bit permutations α_0, α_1.

Proposition. *Let rotational value r is a multiple of* 4, *i. e.* $4 \mid r$. *Then for* 2-GOST *we have*: $P_r(\text{2-GOST}) = 2^{-64r} P_{r,4}(\boxplus)^8$.

5. Conclusion. Following the general framework proposed in [**?**] we have studied the rotational probabilities for 2-GOST block cipher. It turns out that the key schedule of 2-GOST does not affect the rotational probability in comparison with GOST 28147-89. At the same time two different s-boxes of the round transformation significantly reduce the rotational probability in comparison with GOST 28147-89 with identical s-boxes.

REFERENCES

1. *Khovratovich D.*, *Nikolić I.* Rotational cryptanalysis of ARX. — In: Fast Software Encryption. 17th International Workshop FSE 2010. (Seoul, Korea, February 7–10, 2010.) Revised Selected Papers. / Ed. by S. Hong, T. Iwata. Heidelberg etc.: Springer, 2010, p. 333–346. (Ser. Lect. Notes Comput. Sci. V. 6147.)
2. *Zajac P.*, *Ondroš M.* Rotational Cryptanalysis of GOST with identical s-boxes. Tatra Mt. Math. Publ., 2013, v. 57, is. 1, p. 1–19.
3. *Daum M.* Cryptanalysis of Hash Functions of the MD4-Family. PhD thesis. Bochum: Ruhr-Universität Bochum, 2005, 170 p.
4. *Dmukh A. A.*, *Dygin D. M.*, *Marshalko G. B.* A lightweight-friendly modification of GOST block cipher. — Math. Aspects Cryptogr., 2014, v. 5, No 2, p. 47–55.