УДК 003.26

Дали Ф.А.
Технический комитет по стандартизации «ТК26»

Маршалко Г.Б.
Технический комитет по стандартизации «ТК26»

Миронкин В.О.
Московский институт электроники и математики
Национальный исследовательский университет Высшая школа экономики

О СДВИГОВЫХ СВОЙСТВАХ АЛГОРИТМА «2-ГОСТ»

В настоящей работе изучаются свойства алгоритма шифрования «2-ГОСТ», представляющего собой модификацию алгоритма ГОСТ 28147-89. Авторами показано, что при проведении исследований алгоритма «2-ГОСТ», не принадлежащего семейству «ARX-преобразований», могут быть использованы сдвиговые свойства.

БЛОЧНЫЙ ШИФР, ARX-СХЕМА, СЕТЬ ФЕЙСТЕЛЯ, ЦИКЛИЧЕСКИЙ СДВИГ, 2-ГОСТ.

Dali F.A., Marshalko G.B., Mironkin V.O.

ROTATIONAL ANALYSIS OF 2-GOST

In this paper we study rotational probabilities for 2-GOST block cipher, which is a modification of GOST 28147-89. We show that despite the fact that this algorithm does not belong to the family of ARX-transformations in some cases it is possible to evaluate its rotational properties and evaluate the applicability of rotational analysis.

BLOCK CIPHER, ARX-SCHEME, FEISTEL NETWORK, ROTATION ANALYSIS, 2-GOST.

Введение

В последнее время активно изучаются вероятностные свойства ARX-преобразований, использующих операцию XOR, сложение в кольце и операцию побитового сдвига. Интерес к данной проблематике вызван распространением криптографических схем, основанных на преобразованиях такого типа. Так, например, в работе [2] предложен метод т.н. сдвигового анализа, который является вариантом хорошо известного метода дифференциального анализа и предназначен для исследований криптографических примитивов, построенных на основе ARX-преобразований. В работе [3] предложен интересный вариант применения сдвигового анализа для алгоритма ГОСТ 28147-89 (далее – ГОСТ) с одинаковыми подстановками, который, вообще говоря, не является ARX-преобразованием.

В настоящей работе изучаются сдвиговые свойства ГОСТ-подобных алгоритмов, в которых используются две различные подстановки [1]. Вариант такого алгоритма предложен, например, в работе [5].

1. Основные понятия и определения

Введем следующие обозначения:

V^*	множество всех двоичных строк конечной длины;
V_n	множество всех двоичных строк длины $n \in \mathbb{N}$ (нумерация подстрок и компонент строки осуществляется справа налево начиная с нуля);
$A \| B$	конкатенация строк $A, B \in V^*$, т.е. строка из $V_{\|A\|+\|B\|}$, в которой левая подстрока из $V_{\|A\|}$ совпадает со строкой A, а правая подстрока из $V_{\|B\|}$ совпадает со строкой B;
n	длина блока алгоритма блочного шифрования;
k	длина ключа алгоритма блочного шифрования;
$\oplus$	операция покомпонентного сложения по модулю 2 двух двоичных строк одинаковой длины;
$\boxplus$	сложение в кольце $\mathbb{Z}_{2^n}$;
π	подстановочное преобразование $V_4 \to V_4$;
$\ggg_r$	циклический сдвиг на r позиций в сторону младших разрядов;

$\overrightarrow{X}_r$	результат применения операции циклического сдвига на r позиций в сторону младших разрядов к строке X;

Не ограничивая общности, будем рассматривать циклические сдвиги векторов в сторону младших разрядов.

Определение 1. *k-блоковой сдвиг-парой с параметрами $r_1,...,r_k$ назовем пару строк* $\left(X,\overrightarrow{X}^{(k)}_{r_1,...,r_k}\right)=\left(X,\overrightarrow{\left(X_1\right)}_{r_1}\|...\|\overrightarrow{\left(X_k\right)}_{r_k}\right)$, *где* $X=X_1\|...\|X_k$, $k\,|\,n$, $X_i\in V_{\frac{n}{k}}$, $i\in\overline{1,k}$.

Определение 2. *Будем говорить, что операция * сохраняет k-кратный циклический сдвиг для t k-блоковых сдвиг-пар* $\left(X_1,\overrightarrow{\left(X_1\right)}^{(k)}_{r_1,...,r_k}\right),...,\left(X_t,\overrightarrow{\left(X_t\right)}^{(k)}_{r_1,...,r_k}\right)$, *если выполняется соотношение* $\overrightarrow{\left(X_1*...*X_t\right)}^{(k)}_{r_1,...,r_k}=\overrightarrow{\left(X_1\right)}^{(k)}_{r_1,...,r_k}*...*\overrightarrow{\left(X_t\right)}^{(k)}_{r_1,...,r_k}$.

Замечание 1. *При $k=1$ операция XOR сохраняет 1-кратный циклический сдвиг для произвольного количества сдвиг пар.*

Через $P^{(n,k)}_{r_1,...,r_k;t}(*)$ [4] обозначим вероятность сохранения k-кратного циклического сдвига операцией * для t произвольных k-блоковых сдвиг-пар. При этом справедливо соотношение:

$$P^{(n,k)}_{r_1,...,r_k;t}(\boxplus)=P^{\left(\frac{n}{k},1\right)}_{r_1;t}(\boxplus)\cdot...\cdot P^{\left(\frac{n}{k},1\right)}_{r_k;t}(\boxplus). \qquad (1)$$

В работе [3] для алгоритма ГОСТ 28147-89 с набором подстановок $\pi_0=...=\pi_7$ в условиях независимости первых восьми раундовых ключей оценена вероятность $P^{(1)}_r(G)$ того, что 32-раундовое преобразование алгоритма ГОСТ сохраняет 2-кратный циклический сдвиг для произвольной сдвиг-пары $\left(X,\overrightarrow{X}_{r,r}\right)$ при использовании связанных ключей $K,\overrightarrow{K}^{(8)}_{r,...,r}$ (рис. 1).

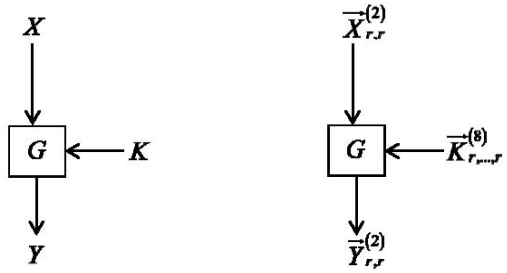

Рис. 1. Сохранение циклического сдвига преобразованием G для связанных ключей $K,\overrightarrow{K}^{(8)}_{r,...,r}$

Рассмотрим сдвиговые свойства алгоритма 2-ГОСТ, представляющего собой модификацию алгоритма ГОСТ, в которой $\pi_0 = \ldots = \pi_3 = \alpha_0$, $\pi_4 = \ldots = \pi_7 = \alpha_1$ и $\alpha_0 \neq \alpha_1$. Будем предполагать, что подстановки выбираются с помощью случайной и бесповторной выборки из множества всех подстановок подходящей размерности. Ключевая развертка алгоритма имеет вид:

$$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2,$$
$$K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_6, K_5, K_4, K_3, K_2, K_1, K_0, K_7.$$

2. Сохранение циклического сдвига в 2-ГОСТ

Через $P^{(k)}_{r,\ldots,r}(2-G)$ обозначим вероятность того, что преобразование алгоритма 2-ГОСТ сохраняет k-кратный циклический сдвиг для случайной k-блоковой сдвиг-пары $\left(X, \overrightarrow{X}^{(k)}_{r,\ldots,r}\right)$ при использовании связанных ключей $K, \overrightarrow{K}^{(4k)}_{r,\ldots,r}$. Тогда справедлив следующий результат.

Предложение 1. *Для алгоритма 2-ГОСТ с двумя различными подстановками* $\alpha_0, \alpha_1 \in S_{2^4}$ *и произвольного* $r \in \overline{1,32}$ *такого, что* $4 \mid r$, *в условиях независимости первых восьми раундовых ключей справедливо:*

$$P^{(2)}_{r,r}(2-G) = 2^{-64r} P^{(32,1)}_{r;4}(\boxplus)^8.$$

Доказательство. Пусть f - операция применения блока подстановок в одном раунде алгоритма 2-ГОСТ. Рассмотрим случай $r = 4$. Тогда для произвольной сдвиг-пары $\left(X, \overrightarrow{X}^{(1)}_r\right)$, где $X = X_0 \| \ldots \| X_7 \in V_{32}$, получаем:

$$P\left\{\overrightarrow{f(X)}^{(1)}_4 = f\left(\overrightarrow{X}^{(1)}_4\right)\right\} = P\left\{\overrightarrow{\pi_0(X_0) \| \ldots \| \pi_7(X_7)} = \pi_0(X_7) \| \ldots \| \pi_7(X_6)\right\} =$$
$$= P\left\{\pi_7(X_7) \| \pi_0(X_0) \| \ldots \| \pi_6(X_6) = \pi_0(X_7) \| \pi_1(X_0) \ldots \| \pi_7(X_6)\right\} =$$
$$= P\left\{\alpha_1(X_7) \| \alpha_0(X_0) \| \ldots \| \alpha_1(X_6) = \alpha_0(X_7) \| \alpha_0(X_0) \ldots \| \alpha_1(X_6)\right\} =$$
$$= P\left\{\alpha_1(X_7) = \alpha_0(X_7), \alpha_0(X_3) = \alpha_1(X_3)\right\} = 2^{-8}.$$

Последнее равенство справедливо в предположении о случайной и

бесповторной выборке подстановок α_0, α_1 из S_{2^4}.

Для сдвига $r = 8$ соответствующая вероятность равна 2^{-16}. В итоге для r, кратного 4, соответствующая вероятность равна 2^{-2r}.

Вероятность сохранения 1-кратного циклического сдвига операцией сложения в кольце $\mathbb{Z}_{2^{32}}$ для произвольной сдвиг-пары $\left(X, \overrightarrow{X}_r^{(1)}\right)$ при подходящих связанных ключах за 32 раунда работы 2-ГОСТ равна $P_{r;4}^{(32,1)}(\boxplus)^8$.

Следует заметить, что при дальнейшем применении циклического сдвига $\ggg_{11}$ к отдельному 32-битному полублоку в каждом раунде алгоритма 2-ГОСТ 1-кратный циклический сдвиг будет сохраняться с вероятностью 1. Таким образом, для 32 раундов алгоритма 2-ГОСТ получаем равенство

$$P_{r,r}^{(2)}(2-G) = 2^{-64r} P_{r;4}^{(32,1)}(\boxplus)^8. \ \square$$

Так как в сетях Фейстеля в каждом из раундов осуществляется перестановка преобразуемых 32-битных полублоков, то случай 2-кратного циклического сдвига принципиально отличается от остальных. Для случая $k > 2$ получен следующий результат.

Предложение 2. *Для произвольных* $\alpha_0, \alpha_1 \in S_{2^4} : \alpha_0 \neq \alpha_1$, $k \mid 32, k \geq 4$, $r : 4 \mid r$ *в условиях независимости первых восьми раундовых ключей алгоритма 2-ГОСТ*

$$P_{r,\ldots,r}^{(k)}(2-G) = 2^{-992} P_{r;4}^{\left(\frac{64}{k},1\right)}(\boxplus)^{4k}.$$

Доказательство. Пусть f - операция применения блока подстановок в одном раунде алгоритма 2-ГОСТ, тогда для 32-битного полублока при $k \mid n, k \geq 4$ и $r : 4 \mid r$ имеем:

$$P\left\{\overrightarrow{f(X)}_{r,\ldots,r}^{\left(\frac{k}{2}\right)} = f\left(\overrightarrow{X}_{r,\ldots,r}^{\left(\frac{k}{2}\right)}\right)\right\} = 1.$$

Вероятность сохранения $\frac{k}{2}$-кратного циклического сдвига (рассматривается отдельный полублок) операцией сложения в кольце $\mathbb{Z}_{2^{32}}$ для произвольной сдвиг-пары $\left(X, \overrightarrow{X}_{r,\ldots,r}^{\left(\frac{k}{2}\right)}\right)$ при подходящих связанных ключах за 32

раунда 2-ГОСТ равна $P_{r,\ldots,r;4}^{\left(32,\frac{k}{2}\right)}\left(\boxplus\right)^8$.

В условиях предложения $НОД\left(r\left(\mathrm{mod}\,32\right),11\right)=1$, поэтому $\frac{k}{2}$-кратный циклический сдвиг будет сохраняться не с вероятностью 1 (как в предыдущем предложении), а лишь для сдвиг-пар $\left(X,\overrightarrow{X}_{r,\ldots,r}^{\left(\frac{k}{2}\right)}\right)$, $X\in V_{32}$, состоящих только из всех 0 или 1 с вероятностью $P_{r,\ldots,r}^{\left(32,\frac{k}{2}\right)}\left(\ggg_{11}\right)=\frac{2}{2^{32}}=2^{-31}$.

Таким образом, для 32 раундов алгоритма 2-ГОСТ согласно (1) получаем:

$$P_{r,\ldots,r}^{(k)}\left(2-G\right)=2^{-31\cdot 32}P_{r,\ldots,r;4}^{\left(32,\frac{k}{2}\right)}\left(\boxplus\right)^8=2^{-992}P_{r;4}^{\left(\frac{64}{k},1\right)}\left(\boxplus\right)^{4k}.\ \square$$

Заключение

В настоящей работе изучены сдвиговые свойства модифицированных вариантов алгоритма ГОСТ 28147-89, в которых используется две различных подстановки и изменен порядок следования раундовых ключей.

Полученные результаты свидетельствуют, что использование нескольких подстановок в алгоритмах типа ГОСТ 28147-89 существенно уменьшает вероятность сохранения сдвиговых соотношений, по сравнению со случаем, когда используется только одна подстановка.

Список литературы

1. *Dali F.A., Marshalko G.B., Mironkin V.O.* Rotational analysis of 2-GOST. - Обозрение прикладной и промышленной математики. – М.: ОПиПМ, 2016, т. 23, в. 2, с. 163-165.
2. *Khovratovich D., Nikolic I.* Rotational cryptanalysis of ARX. Fast Software Encryption 2010 (S. Hong, T. Iwata, eds.) LNCS Vol. 6147, Springer, Heidelberg, 2010, pp. 333-346.
3. *Zajac P., Ondros M.* Rotational Cryptanalysis of GOST with identical s-boxes. Tatra Mountains Mathematical Publications 57 (2013), pp. 1-19.
4. *Daum M.* Cryptanalysis of Hash Functions of the MD4-Family. PhD thesis, Ruhr-Universitat Bochum, 2005.
5. *Dmukh A.A., Dygin D.M., Marshalko G.B.* A lightweight-friendly modification of GOST block cipher. The mathematical aspects in Cryptography, vol. 5, № 2, 2014.