ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 25 МАТЕМАТИКИ Выпуск 3
2018

В. О. Миронкин, **А. А. Смирнова** (Москва, НИУ ВШЭ). **О сдвиговых свойствах некоторых алгебраических операций.**

Введение

В последнее время все более активно изучаются свойства ARX-преобразований, использующих операцию XOR, сложение в конечном кольце и операцию побитового сдвига. Интерес к данной проблематике обусловлен широким применением подобных преобразований в различных криптографических приложениях.

Зачастую в рамках проводимых исследований возникают задачи, связанные с описанием отношения операции циклического сдвига и основных алгебраических операций, используемых в схемах, построенных на ARX-преобразованиях.

В настоящей работе изучается сдвиговые свойства некоторых алгебраических операций, в том числе используемых в ARX-схемах [4, 5].

Так же как и в [1, 2] через $\overrightarrow{X}_r$ обозначим результат применения к произвольной строке $X \in V^*$ операции циклического сдвига на r позиций в сторону младших разрядов, где V^* — множество всех двоичных строк конечной длины.

О п р е д е л е н и е 1. Для произвольного $X \in V_n$ сдвиг-парой с параметром r назовем пару строк $\left(X, \overrightarrow{X}_r\right)$.

О п р е д е л е н и е 2. Будем говорить, что операция $*$ сохраняет r-циклический сдвиг для t сдвиг-пар $(X_1, \overrightarrow{(X_1)}_r), \ldots, (X_t, \overrightarrow{(X_t)}_r)$, если выполняется соотношение

$$\overrightarrow{(X_1 * \ldots * X_t)}_r = \overrightarrow{(X_1)}_r * \ldots * \overrightarrow{(X_t)}_r.$$

З а м е ч а н и е 1. В настоящей работе рассматриваются случаи унарного и бинарного отношений ($t = 1, 2$).

Через $P^{(n)}_{r,t}(*)$ [5] обозначим вероятность сохранения r-циклического сдвига операцией $*$ для t произвольных сдвиг-пар.

В качестве $*$ рассмотрим некоторые алгебраические операции и изучим свойство сохранения сдвига относительно этих операций.

З а м е ч а н и е 2. Операция XOR, l-циклический сдвиг, а также булевы операции такие, как объединение, пересечение, отрицание, штрих Шеффера, стрелка Пирса, сохраняют r-циклический сдвиг для произвольного числа t сдвиг-пар с вероятностью $P^{(n)}_{r,t}(*) = 1$.

1. Сложение по модулю 2^n

Наиболее полное исследование сдвиговых свойств операции сложения по модулю 2^n ($\boxplus$) представлено в работе [3]. Авторами указанной работы вычислено точное значение вероятности

$$P^{(n)}_{r,2}(\boxplus) = \tfrac{1}{4}\left(1 + 2^{r-n} + 2^{-r} + 2^{-n}\right).$$

П р и м е р. Для значений $n = 3, 4, 5$ в табл. 1 представлены значения вероятности $P^{(n)}_{r,2}(\boxplus)$ при всевозможных значениях r.

Таблица 1. Вероятность сохранения r-циклического сдвига операцией $\boxplus$

$r \setminus n$	**3**	**4**	**5**
1	$0,46875$	$0,421875$	$0,3984375$
2	$0,46875$	$0,390625$	$0,3515625$
3		$0,421875$	$0,3515625$
4			$0,3984375$

2. Умножение на квадратную матрицу

Здесь и далее будем рассматривать унарное отношение для случая $r = 1$ (единичного циклического сдвига). При этом в качестве интересующей нас операции будет выступать умножение на квадратную матрицу $M = \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{pmatrix}$, где $m_{ij} \in \{0,1\}$, $i,j = \overline{1,n}$.

Для наглядности выполнения свойства сохранения сдвига рассмотрим произвольный 3-битный вектор $A = (a_1, a_2, a_3)$. Тогда левую и правую части решающего правила «сохранения единичного циклического сдвига» $\overrightarrow{A \times M}_1 = \overrightarrow{A}_1 \times M$ можно представить в следующем виде:

$$\begin{aligned}\overrightarrow{A \times M}_1 &= (a_1, a_2, a_3) \times \overrightarrow{\begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}}_1 \\ &= \overrightarrow{(a_1 m_{11} + a_2 m_{21} + a_3 m_{31}; a_1 m_{12} + a_2 m_{22} + a_3 m_{32}; a_1 m_{13} + a_2 m_{23} + a_3 m_{33})}_1 \\ &= (a_1 m_{13} + a_2 m_{23} + a_3 m_{33}; a_1 m_{11} + a_2 m_{21} + a_3 m_{31}; a_1 m_{12} + a_2 m_{22} + a_3 m_{32}). \quad (1)\end{aligned}$$

$$\begin{aligned}\overrightarrow{A}_1 \times M &= (a_3, a_1, a_2) \times \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} \\ &= (a_1 m_{21} + a_2 m_{31} + a_3 m_{11}; a_1 m_{22} + a_2 m_{32} + a_3 m_{12}; a_1 m_{23} + a_2 m_{33} + a_3 m_{13}). \quad (2)\end{aligned}$$

Классификация матриц, сохраняющих единичный циклический сдвиг (т. е. обеспечивающих равенство соотношений (1) и (2), будем проводить в зависимости от веса двоичных векторов. Так в табл. 2 представлено соответствие весов вектора и числа матриц, сохраняющих циклический сдвиг для 3-х, 4-х и 5-битных векторов.

Таблица 2. Зависимость количества матриц, сохраняющих сдвиг, от веса векторов

n	**Вес вектора**					
	0	**1**	**2**	**3**	**4**	**5**
3	2^9	$2^6 C_3^2$	$2^6 C_3^1$	2^7	–	–
4	2^{16}	$2^{12} C_4^3$	$2^{12} C_4^2$	$2^{12} C_4^1$	2^{13}	–
5	2^{25}	$2^{20} C_5^4$	$2^{20} C_5^3$	$2^{20} C_5^2$	$2^{20} C_5^1$	2^{21}

Проводя аналогичные рассуждения, для произвольного значения $n \in \mathbb{N}$, получаем следующий результат.

Предложение. *Для произвольного $n \in \mathbb{N}$ число матриц N_s, сохраняющих единичный циклический сдвиг для векторов веса $s \in \overline{0,n}$, равно*

- 2^{n^2} *при* $s = 0$;
- $2^{n(n-1)}C_n^{n-s}$ *при* $0 < s < n$;
- $2^{n(n-1)+1}$ *при* $s = n$.

Через ξ_n обозначим случайную величину, равную числу квадратных матриц $n \times n$ над полем $GF(2)$, сохраняющих единичный циклический сдвиг при случайном выборе вектора из V_n. Тогда согласно предложению распределение случайной величины ξ_n имеет следующий вид:

$$\xi_n \sim \begin{pmatrix} 2^{n^2} & 2^{n(n-1)} & \dots & 2^{n(n-1)} & 2^{n(n-1)+1} \\ \frac{1}{2^n} & \frac{C_n^{n-1}}{2^n} & \dots & \frac{C_n^1}{2^n} & \frac{1}{2^n} \end{pmatrix}.$$

Следствие. *Пусть на* V_n, $n \in \mathbb{N}$, *задано равномерное распределение. Тогда справедливо равенство* $\mathbf{E}\xi_n = 2^{n^2-n+1}$.

В табл. 3 представлены некоторые значения $\mathbf{E}\xi_n$ в зависимости от величины n.

Таблица 3. Зависимость $\mathbf{E}\xi_n$ от размерности векторов n

$\boldsymbol{n}$	2^2	2^3	2^4	2^5	2^6	2^7	2^8
$\mathbf{E}\xi_n$	2^{13}	2^{77}	2^{241}	2^{993}	2^{4033}	2^{16257}	2^{65280}

З а м е ч а н и е 3. Существуют матрицы, сохраняющие циклический сдвиг для произвольных сдвиг-пар независимо от величины сдвига r — инвариантные относительно сдвига матрицы. Простейшим примером таких матриц являются квадратные матрицы, содержащие в каждой строке не более одной единицы (в частности, подстановочные матрицы).

СПИСОК ЛИТЕРАТУРЫ

1. *Дали Ф. А.*, *Маршалко Г. Б.*, *Миронкин В. О.* О сдвиговых свойствах алгоритма «2-ГОСТ». — Проблемы информационной безопасности. Компьютерные системы. СПб.: СПбПУ, 2017, № 3, с. 87–90.
2. *Dali F. A.*, *Marshalko G. B.*, *Mironkin V. O.* Rotational analysis of 2-GOST. — Обозрение прикл. и промышл. матем., 2016, т. 23, в. 2, с. 163–165.
3. *Daum M.* Cryptanalysis of Hash Functions of the MD4-Family. PhD thesis, Ruhr-Universitat Bochum, 2005.
4. *Zajac P.*, *Ondros M.* Rotational Cryptanalysis of GOST with identical sboxes. Tatra Mountains Mathematical Publications 57 (2013), p. 1–19.
5. *Khovratovich D.*, *Nikolin I.* Rotational cryptanalysis of ARX. Fast Software Encryption 2010 (S. Hong, T. Iwata, eds.) LNCS Vol. 6147, Springer, Heidelberg, 2010, p. 333–346.