Секция 7

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.7 DOI 10.17223/2226308X/12/57

О СВОЙСТВАХ МАКСИМАЛЬНОГО ЭЛЕМЕНТА МАТРИЦЫ ВЕРОЯТНОСТЕЙ ПЕРЕХОДОВ РАЗНОСТЕЙ БИЕКТИВНОГО ОТОБРАЖЕНИЯ ОТНОСИТЕЛЬНО РАЗЛИЧНЫХ ГРУППОВЫХ ОПЕРАЦИЙ

В. В. Власова, М. А. Пудовкина

Рассматриваются конечные группы $(G_1, \otimes)$, $(G_2, \odot)$ с бинарными операциями $\otimes$ и $\odot$. На практике G_1, G_2 обычно равны аддитивной группе $(V_m, \oplus)$ m-мерного векторного пространства V_m над полем GF(2) или аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов $\mathbb{Z}_{2^m}$. Среди неабелевых групп порядка 2^m аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов в определённом смысле ближе всего группы, содержащие циклическую подгруппу индекса 2. Такими группами являются группа диэдра $(D_{2(m-1)}, \diamond)$ и обобщённая группа кватернионов $(Q_{2^m}, \boxtimes)$. В разностном методе и его обобщениях биективному отображению ставится в соответствие матрица вероятностей переходов разностей. В работе для всех $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$ экспериментально исследуется случайная величина $q^{(\otimes,\odot)}$, равная $|G_1|p^{(\otimes,\odot)}$, где $p^{(\otimes,\odot)}$ — наибольший элемент матрицы вероятностей переходов разностей случайного биективного отображения $s : G_1 \to G_2$.

Ключевые слова: *матрица вероятностей переходов разностей, разностно d-равномерные отображения, S-боксы, обобщённая группа кватернионов, группа диэдра.*

Пусть $(G_1, \otimes)$, $(G_2, \odot)$ — конечные группы с бинарными операциями $\otimes$, $\odot$ и нейтральными элементами e_1, e_2 соответственно, $G_i^\times = G_i \setminus \{e_i\}$ для $i = 1, 2$. В симметричных шифрсистемах группа G_1 часто интерпретируется как группа наложения ключа, а на группе G_2 задаются отображения, реализующие неформально сформулированные К. Шенноном принципы рассеивания или перемешивания. На практике группы G_1, G_2 обычно равны аддитивной группе $(V_m, \oplus)$ m-мерного векторного пространства V_m над полем GF(2) или аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов $\mathbb{Z}_{2^m}$.

Произвольному биективному отображению $s : G_1 \to G_2$ поставим в соответствие матрицу переходов разностей $\mathbf{q}^{(\otimes,\odot)}(s) = \left\| q_{\varepsilon,\delta}^{(\otimes,\odot)}(s) \right\|$, элементы которой для всех $\varepsilon \in G_1^\times$, $\delta \in G_2^\times$ заданы условием

$$q_{\varepsilon,\delta}^{(\otimes,\odot)}(s) = \left| \{\alpha \in G_1 : s(\alpha \otimes \varepsilon) = s(\alpha) \odot \delta\} \right|.$$

Посредством матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$ определяется матрица вероятностей переходов разностей $\hat{\mathbf{p}}^{(\otimes,\odot)}(s) = |G_1|^{-1}\mathbf{q}^{(\otimes,\odot)}(s)$ отображения s. Один из этапов разностного метода и его обобщений заключается в оценках элементов матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$. Все элементы матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$ удаётся вычислить только при небольшом порядке группы G_1, например 16 или 256. Если группа G_1 большого порядка, например $|G_1| \in \{2^{64}, 2^{128}\}$, то,

как правило, ищутся нетривиальные нижние или верхние оценки некоторых элементов матрицы $\mathbf{q}^{(\otimes,\odot)}(s)$. Одной из величин, характеризующей матрицу $\mathbf{q}^{(\otimes,\odot)}(s)$ в целом, является её максимальный элемент. Положим

$$q^{(\otimes,\odot)}(s) = \max\left\{q^{(\otimes,\odot)}_{\varepsilon,\delta}(s) : \varepsilon \in G_1^{\times}, \delta \in G_2^{\times}\right\}.$$

Через величину $q^{(\otimes,\odot)}(s)$ задаются классы криптографических отображений. Так, отображение $g : G_1 \to G_2$ называется *разностно d-равномерным*, если $d = q^{(\otimes,\odot)}(s)$ [1]. Если $d = 2$, то g — *APN-отображение* [2].

Для противодействия разностному методу при синтезе XSL-алгоритмов блочного шифрования в качестве S-бокса, как правило, выбирается отображение $g : G_1 \to G_2$ с наименьшим значением $q^{(\otimes,\odot)}(g)$ среди всех отображений (часто биективных) из G_1 в G_2. В работах [3, 4] приведены примеры биективных отображений, для которых достигаются равенства $q^{(\oplus,\oplus)}(s) = 2$ и $q^{(\boxplus,\boxplus)}(s) = 2$ соответственно.

Пусть $F(G_1, G_2)$ — множество всех биективных отображений из G_1 в G_2. Если подстановка s выбирается из множества $F(G_1, G_2)$ случайно и равновероятно, то $q^{(\otimes,\odot)}(s)$ является случайной величиной, которую будем обозначать через $q^{(\otimes,\odot)}$. Для криптографии представляет интерес нахождение распределения случайной величины $q^{(\otimes,\odot)}$, а также её различных моментов.

В [5] статистически исследована случайная величина $q^{(\otimes,\odot)}$ для следующих пар групповых операций: $(\otimes,\odot) \in \{(\oplus,\oplus), (\boxplus,\boxplus), (\boxdot,\boxdot)\}$, $\boxdot$ — умножение в $\mathbb{Z}^*_{2^m+1}$, где $2^m + 1$ — простое. В [5] при фиксированном $m \in \{4,\ldots,8\}$ для нескольких тысяч случайным образом сгенерированных m-битных подстановок получена выборка случайной величины $q^{(\otimes,\odot)}$ и найдено её выборочное среднее. Показано, что выборочное среднее $q^{(\oplus,\oplus)}$ больше, чем каждое из выборочных средних $q^{(\boxplus,\boxplus)}$ и $q^{(\boxdot,\boxdot)}$.

Среди неабелевых групп порядка 2^m аддитивной группе $(\mathbb{Z}_{2^m}, \boxplus)$ кольца вычетов в определённом смысле ближе всего группы, содержащие циклическую подгруппу индекса 2. Такими группами являются обобщённая группа кватернионов $(Q_{2^m}, \boxtimes)$ и группа диэдра с двумя образующими u, a и циклической подгруппой $\langle a\rangle$ индекса 2 [6].

В настоящей работе для каждого $m \in \{4,\ldots,8\}$ с использованием классического способа [7] сгенерированы 10000 псевдослучайных m-битных подстановок. Для всех $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$ получена выборка случайной величины $q^{(\otimes,\odot)}$ и найдено её выборочное среднее. Результаты приведены в табл. 1 для $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes\}$.

Таблица 1

Выборочное среднее выборки случайной величины $q^{(\otimes,\odot)}$ для псевдослучайных m-битных подстановок

m	$(\oplus,\oplus)$	$(\oplus,\boxplus)$	$(\oplus,\boxtimes)$	$(\boxplus,\oplus)$	$(\boxplus,\boxplus)$	$(\boxplus,\boxtimes)$	$(\boxtimes,\oplus)$	$(\boxtimes,\boxplus)$	$(\boxtimes,\boxtimes)$
4	6,69896	4,74291	4,72011	4,73179	4,42389	4,47999	4,72041	4,4844	4,42092
5	7,94352	5,53062	5,5322	5,53519	5,17748	5,21568	5,5268	5,21399	5,19629
6	9,10926	6,24734	6,24682	6,24594	5,89826	5,91497	6,25189	5,91757	5,911
7	10,31922	6,88711	6,88434	6,88417	6,58556	6,59382	6,88643	6,59206	6,59326
8	11,34672	7,62034	7,62162	7,62201	7,26284	7,27024	7,62459	7,26751	7,26852

В работе использовалась кодировка $\nu : \{0,\ldots,2^m-1\} \to Q_{2^m}$ элементов аддитивной группы кольца вычетов $(\mathbb{Z}_{2^m}, \boxplus)$ элементами обобщённой группы кватернионов $(Q_{2^m}, \boxtimes)$, заданная условием

$$\nu : i \mapsto \begin{cases} a^{\lfloor i/2\rfloor}, & \text{если } i \text{ чётно,} \\ a^{\lfloor i/2\rfloor}u, & \text{если } i \text{ нечётно.} \end{cases}$$

Аналогичная кодировка применена для диэдральной группы.

Для 8-битных подстановок S-боксов алгоритмов блочного шифрования Aes, Anubis, Belt, Crypton, Fantomas, iScream, Kalyna, Khazad, Kuznyechik, Picaro, Safer, Scream, Zorro и 4-битных подстановок алгоритмов Gift, Panda, Pride, Prince, Prost, Klein, Noekeon, Piccolo вычислена $q^{(\otimes,\odot)}(s)$ для всех $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes, \diamond\}$. Результаты приведены в табл. 2 для $\otimes, \odot \in \{\oplus, \boxplus, \boxtimes\}$.

Таблица 2

$q^{(\otimes,\odot)}(s)$ для некоторых S-боксов

S-боксы	$(\oplus,\oplus)$	$(\oplus,\boxplus)$	$(\oplus,\boxtimes)$	$(\boxplus,\oplus)$	$(\boxplus,\boxplus)$	$(\boxplus,\boxtimes)$	$(\boxtimes,\oplus)$	$(\boxtimes,\boxplus)$	$(\boxtimes,\boxtimes)$
Aes	4	6	7	7	7	7	6	7	8
Anubis	8	8	8	8	8	6	8	7	6
Belt	8	6	6	3	7	6	4	7	7
Crypton S0	10	7	7	8	9	7	9	9	8
Crypton S1	10	8	7	8	9	10	9	9	10
Crypton S2	10	8	7	7	9	7	6	9	8
Crypton S3	10	8	7	8	9	8	7	9	8
Fantomas	16	16	16	20	12	13	16	12	13
iScream	16	16	16	16	11	14	16	11	14
Kalyna pi0	8	6	6	6	8	6	7	8	7
Kalyna pi1	8	6	7	7	6	7	6	7	7
Kalyna pi2	8	7	8	7	7	7	6	7	6
Kalyna pi3	8	7	7	7	7	7	7	6	7
Khazad	8	8	8	8	8	8	8	8	7
Kuznyechik	8	7	6	7	7	7	8	8	6
Picaro	4	7	7	7	8	7	6	8	7
Safer	128	10	10	128	2	4	128	4	8
Scream	8	10	12	12	11	12	10	10	12
Zorro	10	8	8	7	6	7	8	8	7
Prost	4	4	4	4	4	4	4	4	5
PRINCE	4	4	4	4	5	4	4	4	4
Pride	4	4	4	4	4	4	4	4	5
Gift	6	4	4	4	3	4	4	3	4
Panda	4	4	4	4	4	3	4	4	3
Klein	4	3	4	3	5	4	3	4	4
Noekeon	4	4	4	4	4	4	4	4	3
Piccolo	4	4	4	4	6	5	4	4	5

ЛИТЕРАТУРА

1. *Canteaut A., Duval S., and Leurent G.* Construction of lightweight S-boxes using Feistel and Misty structures // SAC'2015. LNSC. 2016. V. 9566. P. 373–393.
2. *Nyberg K. and Knudsen L. R.* Provable security against differential cryptanalysis // CRYPTO'92. LNCS. 1993. V. 740. P. 566–574.
3. *Nyberg K.* Differential uniform mappings for cryptography // EUROCRYPT'93. LNCS. 1993. V. 765. P. 55–64.
4. *Massey J. L.* SAFER K-64: A byte-oriented block ciphering algorithm // FSE'93. LNCS. 1994. V. 809. P. 1–16.
5. *Hawkes P. and O'Connor L.* XOR and Non-XOR differential probabilities // EUROCRYPT'99. LNCS. 1999. V. 1592. P. 272–285.
6. *Холл М.* Теория групп. М.: ИЛ, 1962.
7. *Knuth D.* The Art of Computer Programming. V. 2. Addison-Wesley, 1981.