О вычислении некоторых характеристик конечных абелевых групп

К. Ш. Кабулов, Г. А. Серга

В данной работе представлены результаты экспериментального анализа свойств абелевых групп в связи с их криптографическими приложениями. В силу сложности вычислительной задачи рассмотрены группы малого порядка.

Ключевые слова: порядок 2-транзитивности, абелева группа, конечная группа, симметричный шифр.

1. Введение

При использовании симметричных шифров часто необходимо иметь множество преобразователей кодов, которые обладают равномерностью вероятностей возможных выходов вне зависимости от входа. Из данного множества можно случайным образом выбирать преобразователи для шифрования или перестановки входных данных. Очевидно, что большее по мощности множество удобнее в приложениях.

Данная работа является продолжением исследования, проведенного авторами Галатенко А. В., Нечаевым А. А., Панкратьевым А. Е. в работе [1]. Представлены результаты экспериментального исследования абелевых групп до порядка 16 включительно, а также их сравнительный анализ.

Авторы выражают благодарность д.ф.-м.н. В. Б. Кудрявцеву, к.ф.-м.н. А. Е. Панкратьеву и к.ф.-м.н. А. В. Галатенко за постановку задачи и ценные указания.

2. Основные определения

В продолжение результатов работы [1], в которой рассматриваются группы G_1 и G_2, порядков 8, 9, 16 и имеющие вид:

G_1 — представление циклической группы $(\mathbb{Z}_{p^n}, +)$ подстановками

$$\hat{g} = \left(\begin{smallmatrix} x \\ x+g \end{smallmatrix}\right),$$

G_2 — представление элементарной абелевой p-группы $(\mathbb{Z}_p^n, \oplus)$ подстановками

$$\hat{g} = \left(\begin{smallmatrix} x \\ x\oplus g \end{smallmatrix}\right),$$

при естественном представлении чисел из Ω ($\Omega = \overline{0, p^{n-1}}$) p-ичными векторами, соответствующими p-ичной записи, в данной работе изучены группы вида $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ и другие абелевы группы порядков 8, 9 и 16. Для удобства чтения они будут вводиться далее, причем нумерация групп $(G_i, i = \overline{1,5})$ во всех разделах своя, хотя и может совпадать (например, $G_1 \cong \mathbb{Z}_8$ для групп порядка 8 и $G_1 \cong \mathbb{Z}_9$ для групп порядка 9).

Все последующие обозначения взяты из работы [1] в целях удобства дальнейшего сравнения полученных показателей и показателй, опубликованных в данной работе. Приведем их.

В качестве усложняющих преобразований рассматриваются и сравниваются между собой случайно порожденные подстановки из множеств $(G_i h)^k$, где $h \in S(\Omega)$ — множестве перестановок на Ω. Элементы каждой из групп пронумерованы произвольным образом:

$$G_i = \{g_0^{(i)}, \cdots, g_{p^n-1}^{(i)}\},\ i = 1, 2, 3.$$

Порождение подстановок $\xi \in (G_i h)^k$ равносильно порождению управляющих комбинаций, то есть последовательности значений

$$s_1, \cdots, s_k \in \Omega$$

случайных равномерно распределенных на множестве $\overline{0, p^{n-1}}$ независимых величин, и вычислению суммарного шифра:

$$\xi = g_{s_1}^{(i)} h \cdot \cdots \cdot g_{s_k}^{(i)} h \in (G_i h)^k.$$

Множество

$$\Omega^{<2>} = \{(a, b) : a, b \in \Omega, a \neq b\}$$

называется множеством ненулевых биграмм множества Ω.

Матрицей переходных вероятностей ненулевых биграмм множества суммарных шифров $(G_i h)^k$ называют $m \times m$ матрицу $P_2((G_i h)^k)$, где $m = (q^2 - q), q = p^n$, строки и столбцы которой занумерованы в одинаковом порядке элементами из множества биграмм, и такую, что на пересечении ее строки с номером (a, b) и столбца с номером (c, d) стоит число

$$P\left(\begin{smallmatrix} ab \\ cd \end{smallmatrix}\right) = \frac{1}{q^k} \nu_k\left(\begin{smallmatrix} ab \\ cd \end{smallmatrix}\right),$$

где $\nu_k\left(\begin{smallmatrix} ab \\ cd \end{smallmatrix}\right)$ число управляющих комбинаций $s_1, \cdots, s_k \in \Omega$, которые удовлетворяют условию

$$\xi(a) = c, \xi(b) = d.$$

Множество $G_i h$ называется основанием шифра $(G_i h)^k$. Для каждого основания определяется показатель 2-транзитивности $\partial_2(G_i h)$, как наименьшее натуральное k такое, что множество $(G_i h)^k$ 2-транзитивно, или, другими словами, матрица переходных вероятностей положительна (каждый элемент больше нуля). Если подобного k не существует, то считают $\partial_2(G_i h) = \infty$.

Стоит обратить внимание, что при условии $\partial_2(G_i h) < \infty$ последовательность регулярных дважды стохастических матриц $P_2((G_i h)^k)$ сходится к равновероятной матрице [2]. Очевидно, также, что если для некоторой степени l матрица $P_2((G_i h)^l)$ становится положительной, то и все матрицы $P_2((G_i h)^{l+s})$, где $s \in \mathbb{N}$, тоже положительны.

Выделяются следующие характристики:

- $\partial_2(G_i h)$ — как основная характеристика криптографических качеств шифров вида $(G_i h)^k$;
- $N_k(G_i)$ — количество подстановок $h \in S(\Omega)$, для которых

$$\partial_2(G_i h) = k;$$

- $N_k(G_i/\mathcal{H})$ — количество подстановок h из данного подмножества $\mathcal{H} \subset S(\Omega)$, для которых

$$\partial_2(G_i h) = k.$$

Для ускорения вычислений используются вспомогательные факты из работы [3]:
1. Всегда $\partial_2(G_i h) \geqslant 3$.
2. Имеют место соотношения

$$P_2((Gh)^k) = P_2(Gh)^k = P_2(GhG)^{k-1} \cdot P_2(h),$$

из которых следует, что матрица $P_2(Gh)^k$ отличается от матрицы $P_2(GhG)^{k-1}$ лишь перестановкой столбцов, а последнюю можно вычислить, используя представление

$$P_2(GhG)^l = I \otimes Q_i(h)^l, l \in \mathbb{N},$$

где I — равновероятностная $q \times q$ матрица, а $Q_i(h)$ является $(q-1) \times (q-1)$-матрицей, у которой строки и столбцы занумерованы ненулевыми элементами из Ω и на пересечении строки с номером u и столбца с номером v стоит число

$$\frac{1}{q}\mu\binom{u}{v},$$

где $\mu\binom{u}{v}$ — число решений уравнения

$$h(x \oplus u) \oplus h(x) = v,$$

где $\oplus$ — групповая операция в G_i, $i = 1, 2, 3$.

3. Результаты вычислительного эксперимента для группы $\mathbb{Z}_2 \oplus \mathbb{Z}_4$

В таблице 1 представлены сводные данные для удобства сравнения полученных значений. Значения, полученные в данной работе, выделены **жирным**.

Таблица 1. Значения параметров $N_k(G_i)$.

k	$G_1 \cong \mathbb{Z}_8$	$\mathbf{G_3} \cong \mathbb{Z}_\mathbf{2} \oplus \mathbb{Z}_\mathbf{4}$	$G_2 \cong \mathbb{Z}_2^3$
$< \infty$	38 912	**36 480**	32 256
3	32 384	**20 480**	10 752
4	6 528	**13 568**	16 128
5	-	**1 792**	5 376
6	-	**128**	-
7	-	**0**	-
8	-	**512**	-

Для 3 840 перестановок h показатель 2-транзитивности равен бесконечности, более того :

- 536 перестановок соответствуют периодическим матрицам (периоды этих матриц различны — 2, 3 и 4). Пример получающихся матриц для перестановки 5 2 3 4 1 6 7 0 представлен ниже.

$$\begin{bmatrix} 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0 & 0 & 0 & 0.5 \end{bmatrix}$$

  Данная матрица при перемножении переставляет единицы с главной на побочную диагональ и обратно, период равен 2.

- 3 304 перестановки соответствуют идемпотентным матрицам (сюда включаются и тождественные (единичные) матрицы). Идемпотентность выбрана в качестве определяющего свойства из-за соображений неулучшаемости шифра при его многократном применении ($P^2 = P$).

Стоит обратить внимание, что $8! = 40320 = 36480 + 3304 + 536$, то есть все возможные перестановки учтены и исследованы.

Рассмотрим наши группы с точки зрения скорости сходимости матриц $P_2((Gh)^l)$ к равновероятной.

- $\overline{N_l}(G_i;\varepsilon)$ — количество подстановок $h \in S(\Omega)$, для которых все элементы $m \times m$ матрицы $P_2((Gh)^l)$ лежат в интервале $[\frac{1}{m}(1-\varepsilon), \frac{1}{m}(1+\varepsilon)]$, но не все элементы матрицы $P_2((Gh)^{l-1})$ лежат в данном интервале. Стоит отметить, что в нашем случае также рассматривались не сами матрицы $P_2((Gh)^l)$, а матрицы $Q_i(h)^{l-1}$, для чего m, согласно смыслу, заменялось на $q-1$.

Таблица 2. Значения параметров $\overline{N_l}(G_i;0.5)$.

l	$G_1 \cong \mathbb{Z}_8$	$\mathbf{G_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4}$	$G_2 \cong \mathbb{Z}_2^3$
3	6 144	**2 048**	0
4	25 216	**25 600**	10 752
5	3 584	**4 352**	16 128
6	1 536	**3 840**	5 378
7	1 536	**0**	0
8	512	**0**	0
9	128	**128**	0
10	256	**0**	0
11	0	**256**	0
12	0	**0**	0
13	0	**0**	0
14	0	**0**	0
15	0	**256**	0
всего	38 912	**36 480**	32 256

Для возможности сравнения данных с работой [1] приведем также аналогичную таблицу с $\varepsilon = 0.25$:

Таблица 3. Значения параметров $\overline{N_l}(G_i; 0.25)$.

l	$G_1 \cong \mathbb{Z}_8$	$\mathbf{G_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4}$	$G_2 \cong \mathbb{Z}_2^3$
3	1 024	**0**	0
4	17 152	**17 920**	10 752
5	13 056	**10 752**	10 752
6	2 688	**3 584**	5 376
7	1 792	**3 072**	5 376
8	2 048	**512**	0
9	256	**0**	0
10	0	**0**	0
11	512	**128**	0
12	0	**0**	0
13	128	**0**	0
14	256	**0**	0
15	0	**256**	0
16	0	**0**	0
17	0	**0**	0
18	0	**0**	0
19	0	**0**	0
20	0	**0**	0
21	0	**256**	0
всего	38 912	**36 480**	32 256

Как и в случае групп G_1 и G_2, если для какой-либо перестановки $h \in S(\Omega)$ матрица $Q_2(h)$ в какой-то конечной степени становится положительной, то и матрица $Q_3(h)$ для данной перестановки в некоторой степени станет положительной. Аналогичное утверждение имеет место в случае, когда для перестановки h матрица $Q_3(h)$ в некоторой степени становится положительной — в этом случае и матрица $Q_1(h)$ станет положительной в некоторой конечной натуральной степени. Также, можно отметить, что для некоторых перестановок h матрицы $P_2((G_3 h)^l)$ сходятся очень медленно.

4. Результаты вычислительного эксперимента для групп порядка 9

Проведен сравнительный анализ сходимости матриц переходных вероятностей для абелевых групп порядка 9. Ниже приведены результаты вычислений значений $\overline{N_l}(G_i, 0.5)$ и $\overline{N_l}(G_i, 0.25)$, где $G_1 = \mathbb{Z}_{3^2}, G_2 = \mathbb{Z}_3^2$.

Таблица 4. Значения параметров $\overline{N_l}(G_i; 0.5)$ и $\overline{N_l}(G_i; 0.25)$ (соответственно).

l	G_1	G_2
3	43740	93312
4	259038	219024
5	38394	29808
6	10206	3888
7	1944	11664
8	4860	0
9	1944	0
10	972	0
11	0	0
12	0	0
13	0	0
14	486	0
> 14	0	0
всего	361584	357696

l	G_1	G_2
3	0	0
4	159408	155520
5	143370	174960
6	36450	9072
7	10206	6480
8	1944	7776
9	2916	3888
10	3402	0
11	972	0
12	972	0
13	486	0
14	972	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	486	0
> 20	0	0
всего	361584	357696

Отметим следующие факты:

- $\overline{N_3}(G_2, 0.5)$ на 49572 больше, чем $\overline{N_3}(G_1, 0.5)$.

- Для всех перестановок их матрицы переходных вероятностей таковы, что $\overline{N_3}(G_i, 0.25) = 0$, $i = 1, 2$.
- Для G_1 некоторые матрицы сходятся достаточно медленно, к примеру, для группы G_2 показатель $\overline{N_l}(G_2, 0.25) = 0$ при $l > 9$, но для группы G_1 имеем $\overline{N_{20}}(G_1, 0.25) = 486$.

5. Результаты вычислительного эксперимента для групп порядка 16

В случае $p = 2, n = 4$ порядок симметрической группы равен 16!. Ввиду невозможности перебора 16! значений на доступных при проведении работы вычислительных машинах, для анализа данной группы использован алгоритм случайной генерации элементов из массива — алгоритм Фишера-Йетса (алгоритм Кнута). Подробнее про него можно прочитать, например, в работах [4], [5].

Для 100 000 000 (100 млн.) случайных перестановок $h \in S_{16}$, полученных с помощью указанного алгоритма (множество $\mathcal{H}$), были посчитаны данные для 5 различных групп:

$$G_1 \cong \mathbb{Z}_{16}, G_2 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4, G_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_8,$$
$$G_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4, G_5 \cong \mathbb{Z}_2^4.$$

1) Количество $h \in \mathcal{H}$, для которых $\partial_2(Gh) < \infty$
2) Количество $h \in \mathcal{H}$, для которых $\partial_2(Gh) = \infty$
3) $\max\limits_{h \in \mathcal{H}} \{\partial_2(Gh) : \partial_2(Gh) < \infty\}$
4) $N_3(G_i/\mathcal{H})$
5) $N_4(G_i/\mathcal{H})$

Таблица 5. Значения параметров для групп $G_i, i = \overline{1,5}$.

	G_1	G_2	G_3	G_4	G_5
1	99 984 167	99 953 240	99 952 898	99 891 334	99 766 042
2	15 833	46 760	47 102	108 666	233 958
3	7	6	8	7	9
4	99 559 867	96 581 642	96 493 051	75 470 644	6 036 375
5	$< 1\%$	3 365 763	3 456 269	24 370 103	93 080 529

6. Заключение

Результаты экспериментов подтверждают и уточняют данные, полученные в работе [1], а именно, помогают выдвинуть гипотезу о том, что

$$N_3(G_1) \gg \mathbf{N_3}(\mathbf{G_3}) \gg N_3(G_2).$$

Более того, количество перестановок с конечным показателем 2-транзитивности больше для групп вида G_1.
Учитывая это, использование групп $G_1 \cong \mathbb{Z}_{p^n}$ при построении криптографичесикх примитивов может оказаться более эффективным, чем использование других абелевых групп порядка p^n.

Список литературы

[1] Галатенко А. В., Нечаев А. А., Панкратьев А. Е. Сравнительный анализ конечных абелевых групп в связи с их криптографическими приложениями // Фундаментальная и прикладная математика. — В печати.

[2] Baik S., Bang K. Limit theorem of the doubly stochastic matrices // Kangweon-Kyungki Math. Jour. — 2003. 11, No. 2. — P. 155–160.

[3] Глухов М. М. О 2-транзитивных произведениях регулярных групп подстановок // Тр. по дискр. матем. — М.: Физматлит, 2000. 3. — С. 37–52.

[4] Fisher R. A., Yates F. Statistical tables for biological, agricultural and medical research. 3rd ed. — London: Oliver and Boyd, 1948 [1938]. — P. 26–27.

[5] Knuth D. E. The Art of Computer Programming. Vol. 2: Seminumerical algorithms. — MA: Addison-Wesley, 1969. — P. 125.