On computation of some properties of finite abelian groups

Kabulov K.S., Serga G.A.

2015

Аннотация

This work contains results of experimental analysis of some properties of abelian groups regarding their applications to cryptography. Due to computational heaviness of the problem, groups of small orders are studied.

Keywords: abelian group, finite group, symmetric cypher, 2-transitiveness index.

1 Introduction

When using symmetric cryptosystems, the researcher often has to use lots of code converters which have the property of uniformness of output for any input. One can pick at random any code converter from a set of converters with the property described above to use it for encryption or permutation of input data. Obviously, the more elements such set of converters has, the more desired it is for a researcher.

This work is a continuation of the study conducted by Galatenko A.V., Nechaev A.A., Pankratyev A.E. in [1]. This work contains results of experimental research of abelian groups of orders up 16^{th} inclusively, and their comparative analysis.

The authors express their gratitude to the doctor of physical and mathematical sciences Kudryavcev V.B., Pankratyev A.E. and to the candidate of physical and mathematical sciences Galatenko A.V. for the statement of the problem, their support and valuable instructions.

2 Basic definitions

In continuation of the results of [1], in which the authors study groups G_1 and G_2, whith orders 8, 9, 16 and having the following form:

G_1 is a representation of a cyclic group $(\mathbb{Z}_{p^n}, +)$ using substitutions of the following form

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

G_2 is a representation of an abelian $p-$group $(\mathbb{Z}_p^n, \oplus)$ using substitutions of the following form

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

under the natural representation of the numbers in Ω ($\Omega = \overline{0, p^{n-1}}$) using p-ary vectors, corresponding to p-ary notation, in this work we study groups of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ and other abelian groups of orders 8, 9 и 16. For ease of reading, these groups will be introduced later, and moreover, enumeration of groups $(G_i, i = \overline{1, 5})$ in each chapter is different from enumeration in other chapters, although inadvertent coincidences might exist (e.g., $G_1 \cong \mathbb{Z}_8$ for groups of order 8 and $G_1 \cong \mathbb{Z}_9$ for groups of order 9 do coincide).

All of the following notation is taken from [1] to make it easy to compare the results of this paper with results of [1]. Notation is the following.

As complicating transformations, we consider and compare between each other randomly generated permutations from the set $(G_i h)^k$, where $h \in S(\Omega)$ – is a set of permutations over Ω. Elements of each group are numbered arbitrarily:

$$G_i = \{g_0^{(i)}, \cdots, g_{p^n-1}^{(i)}\}, i = \overline{1, 5}.$$

Generation of substitutions $\xi \in (G_i h)^k$ is the same as generation of control combinations, that is the following sequence

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

of uniformly and randomly distributed independent variables over the set $\overline{0, p^{n-1}}$, and computation of the total cipher:

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

The set

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

is referred to as the set of nonzero bigrams over the set Ω.

The matrix of transition probabilities of nonzero bigrams over the set of nonzero bigrams over the set of cumulatove ciphers $(G_i h)^k$ stands for the matrix of the form $P_2((G_i h)^k)$ and size $m \times m$, where $m = (q^2 - q), q = p^n$, with rows and columns enumerated in the same order by elements of the set of bigrams, and which satisfies the condition that at a cell with row number (a, b) and a column number (c, d) there is a number of the following form

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

where $\nu_k \left(\begin{smallmatrix} ab \\ cd \end{smallmatrix}\right)$ is the amount of control combinations of the form $s_1, \cdots, s_k \in \Omega$ which satisfy

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

The set $G_i h$ is called the base of the cypher $(G_i h)^k$. For each base of the cypher we define 2-transitiveness index $\partial_2(G_i h)$, as the least natural number k such that the set $(G_i h)^k$ is 2-transitive, which means that the matrix of transition probabilities is positive (each element of the matrix is greater than zero). In the case when such k does not exist by definition $\partial_2(G_i h) = \infty$.

It is important to mention that in the case when $\partial_2(G_i h) < \infty$ the sequence of regular doubly stochastic matrices $P_2((G_i h)^k)$ converges to an equiprobable matrix [2]. It is also obvious that if the matrix $P_2((G_i h)^l)$ is positive for some degree l, then all the following matrices $P_2((G_i h)^{l+s})$, where $s \in \mathbb{N}$, are positive too.

The following properties are distinguished:

- $\partial_2(G_i h)$ is the basic property representing cryptographical quality of the cypher of the form $(G_i h)^k$;

- $N_k(G_i)$ is the amount of substitutions $h \in S(\Omega)$, for which the following holds
$$\partial_2(G_i h) = k;$$
- $N_k(G_i/\mathcal{H})$ is the amount of substitutions h from subset $\mathcal{H} \subset S(\Omega)$ for which the following holds
$$\partial_2(G_i h) = k.$$

To speed up calculations following auxiliary facts from [3] are applied:

1. $\partial_2(G_i h) \geq 3$ always.
2. The following relations hold

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

which lead to the fact that the matrix $P_2(Gh)^k$ might be derived from matrix $P_2(GhG)^{k-1}$ using just permutation of columns, where the latter matrix can be calculated, using the following representation

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

where I is equiprobable $q \times q$ matrix, and $Q_i(h)$ is $(q-1)\times(q-1)$-matrix, rows and columns of which are enumberated using elements the elements of the set Ω and the intersection of the row u and the column v contains the number of the form

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

where $\mu\binom{u}{v}$ is the amount of the solutions of the equation

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

where $\oplus$ is the group operation in G_i, $i = \overline{1,5}$.

3 The results of the computational experiment for the group $\mathbb{Z}_2 \oplus \mathbb{Z}_4$

Table 1 summarizes the data for easy comparison of the values obtained. Values obtained in this work are **bold**.

Table 1: Values of $N_k(G_i)$.

k	$G_1 \cong \mathbb{Z}_8$	$\mathbf{G_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4}$	$G_2 \cong \mathbb{Z}_2^3$
$< \infty$	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**	-

For 3 840 permutations h 2-transitiveness index is infinity, moreover:

- 536 permutations correspond to periodic matrices (with different periods – 2, 3 и 4). For example, for permutation 5 2 3 4 1 6 7 0 we get the following matrices.

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

  When multiplied by, this matrix rearranges units from the main diagonal to the auxiliary diagonal and vice versa, thus having period equal to 2.

- 3 304 permutations correspond to idempotent matrices (this includes the identity (unit) matrices). Idempotency is chosen as the defining property due to the reasons for the unimprovability of the cipher in its repeated application ($P^2 = P$).

It is worth paying attention to that $8! = 40320 = 36480 + 3304 + 536$, that is, all possible permutations are taken into account and investigated.

We consider our groups from the point of view of the rate of convergence of matrices $P_2((Gh)^l)$ to equiprobable ones.

- $\overline{N_l}(G_i;\varepsilon)$ is the amount of substitutions $h \in S(\Omega)$, with property that for all elements of $m \times m$ matrix $P_2((Gh)^l)$ lie in the interval $[\frac{1}{m}(1-\varepsilon), \frac{1}{m}(1+\varepsilon)]$, but not all the elements of matrix $P_2((Gh)^{l-1})$ lie in this interval. It is worth noting that in our case, we considered matrices of the form $Q_i(h)^{l-1}$ rather than the ones of the form $P_2((Gh)^l)$, for which m, according to the meaning, was replaced by $q-1$.

Table 2: Values of the parameters $\overline{N_l}(G_i; 0.5)$.

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
Total	38 912	**36 480**	32 256

In order to be able to compare the data with [1], we also give a similar table with $\varepsilon = 0.25$:

Table 3: Values of the parameters $\overline{N_l}(G_i; 0.25)$.

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
Total	38 912	**36 480**	32 256

As with groups G_1 and G_2, if for any permutation $h \in S(\Omega)$, the matrix $Q_2(h)$ at some finite degree becomes positive, then matrix $Q_3(h)$ too at some finite degree becomes positive for the same permutation. The same statement holds in the case when for permutation h matrix $Q_3(h)$ at some degree becomes positive and this in turn results in $Q_1(h)$ being positive at some finite degree. Also, it can be noted that for some permutations h matrices $P_2((G_3h)^l)$ converge very slowly.

4 The results of a computational experiment for groups of order 9

A comparative analysis of the convergence of matrices of transition probabilities for abelian groups of order 9 was performed. Below are the results of calculating the values $\overline{N_l}(G_i, 0.5)$ and $\overline{N_l}(G_i, 0.25)$, where $G_1 = \mathbb{Z}_{3^2}, G_2 = \mathbb{Z}_3^2$.

Таблица 4: Values of the parameters $\overline{N_l}(G_i; 0.5)$ и $\overline{N_l}(G_i; 0.25)$ correspondingly).

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
Total	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
Total	361584	357696

We note the following facts:

- $\overline{N_3}(G_2, 0.5)$ is 49572 times greater than $\overline{N_3}(G_1, 0.5)$.
- For all permutations, their matrix of transition probabilities is such that $\overline{N_3}(G_i, 0.25) = 0$, $i = 1, 2$.
- For G_1 some matrices converge quite slowly, for example, for group G_2 parameter $\overline{N_l}(G_2, 0.25) = 0$ when $l > 9$, but for group G_1 we have $\overline{N_{20}}(G_1, 0.25) = 486$.

5 The results of a computational experiment for groups of order 16

In the case when $p = 2, n = 4$ the order of symmetric group is 16!. Due to computational heaviness of using brute force to study all 16! possible elements, for the analysis of this group we used the algorithm based upon generating random elements of the array – Fischer-Yates algorithm (also known as Knuth's algorithm). For a deeper discussion of this algorithm, we refer the reader to [4], [5].

Based upon 100 000 000 (hundred million) random permutations $h \in S_{16}$, derived using the algorithm mentioned above (the set $\mathcal{H}$), we calculated parameters of 5 different groups:

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

1. Amount of $h \in \mathcal{H}$, with $\partial_2(Gh) < \infty$
2. Amount of $h \in \mathcal{H}$, with $\partial_2(Gh) = \infty$
3. $max_{h \in \mathcal{H}}\{\partial_2(Gh) : \partial_2(Gh) < \infty\}$
4. $N_3(G_i/\mathcal{H})$
5. $N_4(G_i/\mathcal{H})$

Table 5: Parameter values for groups $G_i, i = \overline{1,5}$.

	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 Conclusion

The results of the experiments confirm and refine the data obtained in [1], namely, they help to put forward the hypothesis that

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

Moreover, the number of permutations with a finite 2-transitiveness index is greater for groups of the form G_1.

Considering this, we conclude that using groups $G_1 \cong \mathbb{Z}_{p^n}$ for building cryptographic primitives may be more effective, than using other abelian groups of order p^n.

Список литературы

[1] Galatenko A.V., Nechaev A.A., Pankratyev A.E., "Comparing finite Abelian groups from the standpoint of their cryptographic applications". "Fundamental and applied mathematics", to be printed.

[2] Seung-il Baik and Keumseong Bang, Limit theorem of the doubly stochastic matrices, Kangweon-Kyungki Math. Jour. 11 (2003), No. 2, pp. 155-160

[3] M.M. Glukhov, "On 2-transitive products of regular permutation groups", treatise on discrete mathematics, 3, Физматлит, M., 2000, 37—52.

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

[5] Donald E. Knuth, The Art of Computer Programming, volume 2: Seminumerical algorithms, Reading, MA: Addison-Wesley, 1969, pp. 125-125.