УДК 004.056.5

СТАТИСТИЧЕСКИЙ АНАЛИЗ КОНЕЧНЫХ ГРУПП И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

В.Н. Кутин, В.А. Молчанов

Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, Саратов, Россия

Аннотация. В современной криптографии при построении криптографических примитивов, криптосистем и протоколов особое внимание уделяется использованию алгебраических структур, в частности, конечных групп. Группы играют ключевую роль в разработке эффективных и устойчивых к атакам криптосистем, обеспечивая математическую основу для широко применяемых криптографических схем.

Ключевые слова: конечная группа; треугольные матрицы; порядок элементов.

STATISTICAL ANALYSIS OF FINITE GROUPS AND THEIR APPLICATION IN CRYPTOGRAPHY

V.N. Kutin, V.A. Molchanov
Saratov National Research State University named after N. G. Chernyshevsky, Saratov, Russia

Abstract. In modern cryptography, when building cryptographic primitives, cryptosystems and protocols, special attention is paid to the use of algebraic structures, in particular, finite groups. The groups play a key role in the development of effective and attack-resistant cryptosystems, providing the mathematical basis for widely used cryptographic schemes.
Keywords: finite group; triangular matrices; order of elements.

Введение

Настоящая работа посвящена исследованию возможностей применения конечных групп в криптографии, включая их использование в построении криптосистем, основанных на сложных алгоритмических проблемах. Особый интерес представляют задачи, связанные с вычислительной сложностью поиска порядков элементов и проблемой дискретного логарифма в конечных группах, которые находят применение как в классической, так и в пост-квантовой криптографии.

Основная часть

Данная работа является продолжением исследований [1]. В рамках текущего исследования был проведен статистический анализ сгенерированных конечных групп верхне-треугольных матриц с элементами над полем $\mathbb{Z}_p$ (p-простое число) [2]. Также исследовалась структура этих групп, распределение порядков их элементов, а также их подгруппы. Полученные статистические характеристики позволили провести сравнительное исследование алгебраических свойств таких групп и оценить их возможное применение в криптографических и вычислительных задачах.

Выбор верхне-треугольных матриц с элементами над полем $\mathbb{Z}_p$ и ненулевым определителем, в качестве элементов множества, позволяет построить конечную группу с гарантированно обратимыми элементами. Таким образом используя свойство обратимости элементов полученной группы, был применен эффективный алгоритм Гельфонда – Шенкса для вычисления порядков элементов сгенерированной группы [3].

Были рассмотрены следующие конечные группы верхне-треугольных матриц:

1. Группа верхне-треугольных матриц размерностью 3 на 3, с элементами над полем $\mathbb{Z}_{11}$.

2. Группа верхне-треугольных матриц размерностью 3 на 3, с элементами над полем $\mathbb{Z}_{13}$.

3. Подгруппа группы верхне-треугольных матриц 3 на 3, с элементами над полем $\mathbb{Z}_{19}$, порожденная случайно выбранными элементами группы:

$$\begin{pmatrix} 2 & 1 & 6 \\ 0 & 3 & 9 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 7 & 12 \\ 0 & 3 & 9 \\ 0 & 0 & 9 \end{pmatrix}.$$

4. Подгруппа группы верхне-треугольных матриц 3 на 3, с элементами над полем $\mathbb{Z}_{19}$, порожденная случайно выбранными элементами группы:

$$\begin{pmatrix} 2 & 1 & 14 \\ 0 & 12 & 9 \\ 0 & 0 & 14 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 7 & 12 \\ 0 & 3 & 9 \\ 0 & 0 & 9 \end{pmatrix}.$$

5. Подгруппа группы верхне-треугольных матриц 3 на 3, с элементами над полем $\mathbb{Z}_{23}$, порожденная случайно выбранными элементами группы:

$$\begin{pmatrix} 2 & 1 & 6 \\ 0 & 3 & 1 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 12 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 17 \end{pmatrix}.$$

Для каждой пронумерованной выше группы и подгруппы были получены списки частот порядков элементов (в скобках указаны частоты):

1. 1(1), 2(727), 5(87124), 10(903148), 11(1330), 22(8590), 55(77920), 110(252160).

2. 1(1), 2(1015), 3(16226), 4(57800), 6(261614), 12(2630320), 13(2196), 26(14364), 39(40896), 52(65232), 78(138240), 156(568512).

3. 1(1), 2(361), 3(15884), 6(41876), 9(376884), 18(454860), 19(6858), 38(6498), 57(38988), 114(12996), 171(116964), 342(38988).

4. 1(1), 2(723), 3(15884), 6(99636), 9(376884), 18(1286604), 19(6858), 38(19854), 57(38988), 114(64980), 171(116964), 342(194940).

5. 1(1), 2(529), 11(1110900), 22(1343660), 23(12166), 253(349140), 506(116380).

В частности, были получены статистические характеристики: математическое ожидание, дисперсия, среднее квадратическое отклонение, сгенерированных групп и подгрупп, приведенные в Таблице 1, также распределения частот порядков преобразований, изображенных на Рисунке 1. Полученные распределения прошли тест Д'Агостино-Пирсона на нормальность, результаты тестов также приведены также в Таблице 1 [4]. Также согласно Рисунку 1, очевидно, что ядерные оценки плотности частот порядков элементов для групп близки нормальной кривой Гаусса.

Таблица 1. Статистические характеристики частот порядков элементов сгенерированных групп верхне-треугольных матриц, тестирование распределений полученных частот на нормальность тестом Пирсона (уровень значимости $a = 0.05$)

Table 1. Statistical characteristics of the frequencies of the orders of elements of the generated groups of upper triangular matrices, testing the distributions of the obtained frequencies for normality using the Pearson test (significance level $a = 0.05$)

№	Макс. порядок	Матем. ожидание	Дисперсия	Ср. кв. отклонение	Кол-во эл-тов	p-значние	Норм. Распр. p > 0.05
1	110	221833	99644311023	315664.87	1331000	0.0675	Да
2	156	474552	693883385533	832996.63	3796416	0.0738	Да
3	342	136458	27981412518	167276.46	1111158	0.1476	Да
4	342	259920	151540536440	389282.08	2222316	0.0677	Да
5	506	735353	1011289260182	1005628.79	2944414	0.1122	Да

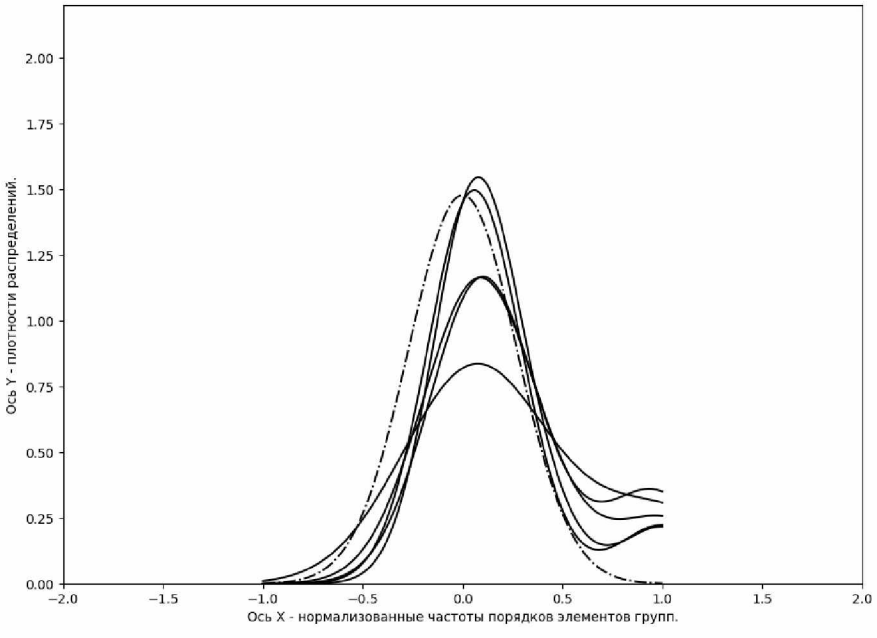

Рис. 1. Ядерные оценки плотности частот порядков элементов групп верхне-треугольных матриц (штрихпунктирный график – стандартная кривая Гаусса, черные графики – распределения частот)
Fig. 1. Nuclear estimates of the frequency density of the orders of elements of groups of upper triangular matrices (dotted line graph is the standard Gauss curve, black graphs are frequency distributions)

Заключение

В данной работе был проведен статистический анализ конечных групп верхне-треугольных матриц 3×3 с элементами над полями $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{19}$, $\mathbb{Z}_{23}$. Полученные результаты позволили изучить структуру этих групп, распределение порядков их элементов и выявить свойства их подгрупп. Анализ показал, что распределения порядков элементов таких групп обладают характеристиками, близкими к нормальному распределению Гаусса, что подтверждено тестом Д'Агостино-Пирсона.

Список использованных источников

1. Кутин В.Н., Молчанов В.А. Статистический анализ конечных полугрупп и их применение в криптографии / В.Н. Кутин, В.А. Молчанов // Технические средства защиты информации : тез. докл. XXI Белорусско-российской науч.-техн. конф. (Республика Беларусь, Минск, 6 июня 2023 года) / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2023. – 104 с.

2. Гантмахер Ф.Р. . Теория матриц. 4-е изд. – М.: Наука, 1988. – 552 с. – ISBN 5-02-013722-7.

3. Панкратова И. А. Теоретико-числовые методы в криптографии: Учебное пособие. – Томск: ТГУ, 2009. – С. 90-98. – 120 с.

4. Кобзарь А. И. Прикладная математическая статистика. – М.: Физматлит, 2006. – с. 258.

References

1. Kutin V.N., Molchanov V.A. Statistical analysis of finite semigroups and their application in cryptography / V.N. Kutin, V.A. Molchanov // Technical means of information protection : thesis of the XXI Belarusian-Russian Scientific and Technical conference (Republic of Belarus, Minsk, June 6, 2023) / editor : T. V. Borbotko [et al.]. – Minsk : BGUIR, 2023. – 104 p.

2. Gantmacher F.R. Theory of matrices. 4th ed.– Moscow: Nauka. 1988– 552 p. ISBN 5-02-013722-7.

3. Pankratova I. A. Theoretical and numerical methods in cryptography: A textbook. Tomsk: TSU. 2009. pp. 90-98. 120 p.

4. Kobzar A. I. Applied Mathematical statistics. Moscow: Fizmatlit. 2006. p. 258.

Сведения об авторах

Кутин В.Н., аспирант кафедры теоретических основ компьютерной безопасности и криптографии, Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, qooteen@mail.ru.
Молчанов В.А., доктор физ.-мат.наук, профессор, профессор кафедры теоретических основ компьютерной безопасности и криптографии, Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского, v.molchanov@inbox.ru.

Information about the authors

Kutin V.N., Postgraduate student of the Department of Theoretical Foundations of Computer Security and Cryptography, Saratov National Research State University named after N. G. Chernyshevsky, qooteen@mail.ru.
Molchanov V.A., Doctor of Physical and Mathematical Sciences, Professor, Professor of the Department of Theoretical Foundations of Computer Security and Cryptography, Saratov National Research State University named after N. G. Chernyshevsky, v.molchanov@inbox.ru.