СТАТИСТИЧЕСКИЙ АНАЛИЗ КОНЕЧНЫХ ПОЛУГРУПП И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

В.А. Молчанов, В.Н. Кутин

ФГБОУ ВО «Саратовский научный исследовательский государственный университет имени Н.Г. Чернышевского», Саратов, Россия

В современной криптографии при построении криптографических примитивов, криптосистем и протоколов особое внимание уделяется применению методов универсальной алгебры [1]. Важность этих исследований обосновывается, в частности, тем, что алгебраическая криптография является одной из альтернатив решения проблемы постквантовой криптографии [2].

Настоящая работа посвящена применению в криптографии методов теории полугрупп [3], которые не только позволяют естественно обобщать известные криптосистемы, но и разрабатывать принципиально новые криптосистемы на основе неразрешимых и трудноразрешимых алгоритмических проблем теории полугрупп [4]. Например, одной из таких проблем теории полугрупп является известная проблема равенства слов [3].

Данная работа является продолжением исследований [5]. В рамках настоящей работы был проведен статистический анализ генерируемых симметрических полугрупп преобразований множеств небольшой мощности, а также эмпирических множеств преобразований мощности 100, 500, 1000, 5000, 10000, 50000, 100000, 500000, 800000, полученных путем случайной выборки элементов из симметрической полугруппы для дальнейшего проецирования результатов анализа на симметрические полугруппы преобразований множеств большой мощности. В частности, были получены: математическое ожидание, дисперсия, среднее квадратическое отклонение и распределения порядков элементов (преобразований) таких полугрупп. На основе вычисленных статистических характеристик были построены графики ядерных оценок плотности, полученные кривые, оказались близки по построению к нормальной кривой Гаусса. Полученные распределения прошли тест Д'Агостино-Пирсона на нормальность. Также было замечено, что с увеличением мощности генерируемой симметрической полугруппы, растет и значение математического ожидания количеств порядков

элементов, при этом значение математического ожидания количеств порядков элементов случайно выбранных множеств преобразований практически не меняется с ростом мощности множества.

Список литературы

1. Романьков В.А. Алгебраическая криптография. Омск: изд-во Ом. гос ун-та, 2013.
2. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM journal on computing. 1997. Vol. 26. 1484.
3. Lallement G. Semigroups and combinatorial applications. Pure and Applied Mathematics Series, Wiley, New York, 1979.
4. Maze G., Monico C., Rosenthal J. Public Key Cryptography based on Semigroup Actions. Advances in Mathematics of Communications 1.4. 2007. P. 489–507.
5. Молчанов В.А., Кутин В.Н. О применении методов теории полугрупп в криптографии // Технические средства защиты информации: тез. докл. XX Белорусско-российской науч.-техн. конф., Минск, 7 июня 2022 г. С. 73–74.