О ПРИМЕНЕНИИ МЕТОДОВ ТЕОРИИ ПОЛУГРУПП В КРИПТОГРАФИИ

В.А. Молчанов, В.Н. Кутин

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].

Целью данной работы является разработка и программная реализация алгоритмов вычисления конечных полугрупп с целью их дальнейших приложений в структурном анализе таких полугрупп и в криптографии. С помощью результатов [5] разработаны алгоритмы генерации конечных полугрупп преобразований и полугрупп квадратных матриц над конечным полем. На основании описанных алгоритмов реализован программный комплекс с доступным и простым интерфейсом для генерации конечных полугрупп. Программа также проводит статистический анализ процесса генерации полугрупп и на основе таких полугрупп реализует ряд криптосистем с открытым ключом. В частности, проанализированы размеры генерируемых конечных полугрупп и сложность их вычислений, получены распределения порядков элементов таких полугрупп. Помимо этого, программный комплекс на основе сгенерированных полугрупп реализует следующие криптосистемы: обобщенную криптосистему Эль-Гамаля, базирующуюся на полугруппе матриц или группе перестановок, а также криптосистему, базирующуюся на проблеме равенства слов в полугруппах. Программа зарегистрирована Федеральной службой интеллектуальной собственности, номер свидетельства 2021619325.

Литература

1. Романьков В А. Алгебраическая криптография. Омск: Изд-во Ом. гос ун-та, 2013. 136 с.

2. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM journal on computing. 1997. Vol. 26. P. 1484.

3. Lallement G. Semigroups and combinatorial applications. New York, Wiley, 1979. 376 p.

4. Maze G., Monico C., Rosenthal J. Public Key Cryptography based on Semigroup Actions / in “Advances in Mathematics of Communications”. 2007. P. 489–507.

5. Froidure V., Pin J.-E. Algorithms for computing finite semigroups / in “Foundations of Computational Mathematics”. Berlin, Springer, 1997. P. 112–126.