УДК 546.07

Ребренюк А.Л., студент 1 курсу спеціальності 029 «Інформаційна, бібліотечна та архівна справа»
Луценко А.В., асистент кафедри прикладної математики та кібербезпеки

ПРО ЗАСТОСУВАННЯ КВАЗІГРУП У КРИПТОГРАФІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

У сучасній Інтернет-цивілізації ми як ніколи стикаємося з потребою у швидкому та безпечному спілкуванні.

Безпека зв'язку реалізується в основному за допомогою двох типів алгоритмів: 1) Алгоритми, які використовують відкриті ключі; 2) Алгоритми, які використовують секретний ключ.

Більшість відомих конструкцій криптографічних примітивів, кодів виявлення та виправлення помилок використовують структури з асоціативної алгебри як групи, кільця та поля. Два видатних спеціалісти з квазігруп, Дж. Денес і А. Д. Кідвел [1], проголосили настання нової ери в криптології, яка полягає у застосуванні неасоціативних алгебраїчних систем як квазігрупи.

Квазігрупи та їхні комбінаторні еквіваленти латинські квадрати дуже підходять для цієї мети через їхню структуру, особливості, велику кількість. Тим не менш, на даний момент дуже мало дослідників використовують ці інструменти, а криптографічна спільнота все ще вагається щодо них.

Перше застосування квазігрупи-латинського квадрата в криптографії датується 16 століттям.

Більшість результатів застосування квазігруп у криптології описано в праці [2]. За останні роки з'явилися різні криптосистеми, засновані на квазігрупах.

Квазігрупою називається групоїд $(Q;\cdot)$ такий, що для довільних a,b кожне з рівнянь $a\cdot x=b$, $y\cdot a=b$ має єдиний розв'язок.

Ізотопія квазігруп вперше була розглянута при розробці блокового шифру IDEA, де були використані три неізотопні групи. Квазігрупи мають дуже корисні властивості, які дозволяють використовувати їх для побудови функцій шифрування та розшифрування. Особливо це стосується квазігруп з властивостями оборотності.

Застосування квазігруп у криптографії наведені у багатьох працях, зокрема потокові шифри на основі квазігруп та їх парастрофів були описані С.Марковським [3].

Для ефективного використання квазігруп потрібно дати відповіді на такі питання:

1) Які властивості повинна мати квазігрупа, щоб її можна було використовувати як будівельний блок для криптографічних схем і вона могла забезпечити надійний захист?

2) Як згенерувати та як обчислити велику кількість квазігруп?

3) Які особливості мають квазігрупи, отримані новим методом побудови?

4) Які є способи використання квазігруп як будівельні блоки криптографічних схем?

А. Мілева показала, що навіть квазігрупи малих порядків дуже придатні для застосування в криптографії [4]. Особливо це стосується квазігруп через їх структуру, особливості та велику кількість.

Сьогодні існує кілька класифікацій, які допомагають нам у виборі квазігруп, які мають властивості для ефективногоо застосування. Три основні класифікації отримані шляхом використання алгебраїчних властивостей квазігруп до класів ізотопних квазігруп, класів ізоморфних квазігруп і класів парастрофних квазігруп. Квазігрупи класифікуються на многовиди відповідно до тотожностей, яким вони задовольняють. Одна із таких класифікацій наведена в праці [5].

Список літератури.

1. *J. Denes and A. D. Keedwell. Some applications of non-associative algebraic systems in cryptology. Pure Mathematics and Applications, 12(2):147{195, 2001.*
2. *Shcherbacov V.A. Quasigroups in cryptology. Computer Science Journal of Moldova. 2009. Vol.17, No 2. P. 193-228.*
3. *Markovski S, Gligoroski D, and Bakeva V. Quasigroup and hash functions Proc. of the 6th ICDMA. Bansko. 2001. P. 43-50.*
4. *A. Mileva, "Cryptographic Primitives with Quasigroup Transformations," Ph.D. dissertation, University Ss. Cyril and Methodius, Skopje, Macedonia, 2010.*
5. *Sokhatsky F.M., Lutsenko A.V. Classification of quasigroups according to directions of translations II. Commentationes Mathematicae Universitatis Carolinae. 2021. Vol. 62, No 3. P. 309-323.*

УДК 004.5

Рудь О. С., студентка 2 курсу
спеціальності 122 «Комп'ютерні науки»,
Науковий керівник:
Потапова Н. А., к.е.н., доцент
кафедри інформаційних технологій

АНАЛІЗ ПОВЕДІНКИ ПРОЦЕСІВ НА ЗАСАДАХ ОБЧИСЛЮВАЛЬНИХ АЛГОРИТМІВ

Донецький національний університет імені Василя Стуса, м. Вінниця

Аналіз поведінки процесів на засадах обчислювальних алгоритмів - це використання математичних методів та алгоритмів для аналізу даних та