УДК: 004.056.55+512.548

Крайнічук (Шелепало) Галина
Варшавська Юлія

ВЗАЄМНО ПОПАРНО ОРТОГОНАЛЬНІ КВАЗІГРУПОВІ ОПЕРАЦІЇ ДЛЯ МАЛОРЕСУРСНОЇ КРИПТОГРАФІЇ

Вінницький національний технічний університет

Анотація. *У тезах наведено взаємно попарно ортогональні квазігрупові операції малих порядків для формування потокового шифру. Обґрунтовано використання їх для легковагової криптографії.*
Ключові слова: квазігрупова операція, латинський квадрат, потоковий шифр, LW-криптографія, кібербезпека.

Abstract. *The abstracts present mutually pairwise orthogonal quasigroup operations of small orders for forming a stream cipher. Their use for lightweight cryptography is justified.*
Keywords: quasigroup operation, Latin square, stream encryption, LW-cryptography, cybersecurity.

Вступ

Квазігрупові операцій досить широко почали використовувати у криптографії, зокрема для малоресурсної криптографії, а саме потокового шифрування. Зв'язок між квазігруповими операціями та латинськими квадратами, а також зв'язок між квазігрупами та сітками відомий давно (В. Д. Білоусов та А. С. Бектенов (1979), О. Чейн, Г. О. Плюгфельдер та Дж. Сміт (1990) та інші). Дослідженнями ортогональних квазігрупових операцій, зокрема ортогональними латинськими квадратами, займалися Ж. Дѐнес, А. Д. Кідвел, Г. Б. Білявська, В. А. Щербаков, І. В. Фриз, Ф. М. Сохацький та інші.

Пошук стійких потокових шифрів для квантової криптографії, а особливо для малоресурсної (LW) криптографії, є актуальним і залишається відкритою проблемою сьогодні. Оскільки для LW-криптографії в операційних блоках для формування шифру використовують саме квазігрупові операції, то, для кращої стійкості шифру, важливо показати такі властивості квазігрупових операцій, що мають сильнішу вимогу для застосування, а не просто набір будь-яких операцій певного порядку.

Результати дослідження

Нехай $Q_n := \{1,2,3,...,n\}$, f та g – деякі операції на Q, тоді бінарна квазігрупа – це впорядкована пара $(Q; f)$, де Q – множина, f – бінарна операція, визначена на Q така, що кожне із рівнянь $f(x; a) = b$, $f(a; y) = b$ має єдиний розв'язок для будь-якої пари елементів a, b, із Q. Бінарну операцію f з цієї впорядкованої пари називають квазігруповою [1].

Квазігрупову операцію найчастіше для шифрування подають у вигляді таблиці множення елементів, яку називають таблицею Келі. Внутрішня частина таблиці Келі квазігрупової операції є латинським квадратом. Якщо в латинському квадраті в першому рядку і в першому стовпці елементи розташовані у порядку зростання, то такий квадрат називають нормалізованим. Будь-який латинський квадрат можна звести до нормалізованого за допомогою перестановки рядків та стовпців. Два латинських квадрати є ізотопними, якщо кожен з них можна перетворити на інший шляхом перестановки рядків, стовпців та символів результату множення в таблиці Келі. Це відношення ізотопії є відношенням еквівалентності; класи еквівалентності - це класи ізотопії [2].

Для дослідження в операційному блоці для формування шифру розглядаємо лише квазігрупові операції 4-го порядку, причому необхідна кількість самих латинських квадратів, яку використовуємо, всього достатньо три. Для стійкості шифру обираємо специфічну властивість, яка поєднує всі цих три квазігрупові операції тим, що вони мають бути попарно взаємно ортогональні.

Дві квазігрупові операції f та g ортогональні ($f \perp g$) тоді і тільки тоді, коли вони визначені на одній множині та при накладанні їх елементів – результатів з таблиць Келі утворюються всі унікальні впорядковані пари цієї множини, тобто всі n^2 пар різні, що створює повний греко-латинський квадрат. Ортогональні квазігрупові операції існують всіх порядків, окрім n=2 та n=6 (відома задача про розташування 36 офіцерів із різними званнями) [3].

Набір із k квазігрупових операцій, де кожна квазігрупова операція ортогональна кожній операції в наборі, називають попарно взаємно ортогональними квазігруповими операціями. Наприклад, для квазігрупових операцій 3-го порядку така пара (табл.1), з точністю до ізотопії, єдина. Легко побачити, що вона утворює всі 9 унікальних пар при накладанні однієї операції на іншу.

Таблиця 1. *Попарно ортогональні квазігрупові операції 3-го порядку*

f	0	1	2
0	**0**	**1**	**2**
1	**1**	**2**	**0**
2	**2**	**0**	**1**

g	0	1	2
0	**0**	**1**	**2**
1	**2**	**0**	**1**
2	**1**	**2**	**0**

Для квазігрупових операцій порядку $n = 4$ (степінь простого числа 2) існує максимально 3 попарно ортогональних квазігрупових операцій. З точністю до ізотопії – це єдина трійка взаємно попарно ортогональних квазігрупових операцій 4-го порядку: $f = x + y$, $g = x + 2y$, $g = x + 3y$, де (+) – операція XOR, а операція множення визначається через підстановку $a^2 = a + 1$ в полі $GF(4)$.

Таблиця 2. *Попарно ортогональні квазігрупові операції 4-го порядку*

f	0	1	2	3
0	**0**	**1**	**2**	**3**
1	**1**	**0**	**3**	**2**
2	**2**	**3**	**0**	**1**
3	**3**	**2**	**1**	**0**

g	0	1	2	3
0	**0**	**2**	**3**	**1**
1	**1**	**3**	**2**	**0**
2	**2**	**0**	**1**	**3**
3	**3**	**1**	**0**	**2**

h	0	1	2	3
0	**0**	**3**	**1**	**2**
1	**1**	**2**	**0**	**3**
2	**2**	**1**	**3**	**0**
3	**3**	**0**	**2**	**1**

Очевидно, що при накладанні кожної з кожною операцією утворюються 16 різних пар елементів, як результатів прямого добутку операцій $f \perp g$, $f \perp h$, $h \perp g$. Легко побачити, що при накладанні всіх трьох операцій одночасно $f \perp g \perp h$, отримаємо всі 16 унікальних трійок, а саме:

{000, 123, 231, 312, 111, 032, 320, 203, 222, 301, 013, 130, 333, 210, 102, 021}.

Варто зауважити, що для шифрування можна використовувати інші ізотопні квазігрупові операції, тобто їх латинські квадрати матимуть інший вигляд, але ортогональніть при цьому незмінна, тобто множина 16-ти трійок та сама. Побудову таких ізотопних квазігрупових операцій можна знайти в [3-5]. Цікавим фактом є те, що для шифрування серед всіх ізотопних попарно ортогональних квазігрупових операцій найменшу апаратну складність матимуть саме наведені операції в табл.2.

Висновки

Запропонований підхід дозволяє реалізувати ефективне програмне або апаратне шифрування з мінімальними витратами обчислювальних ресурсів, оскільки ізотопність взаємно попарно ортогональних квазігрупових операцій гарантує стійкість утвореного шифру на їх основі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Keedwell A.D., Denes J. Latin Squares and their Applications // North Holland: Elsevier B.V. − 2015. − 455 p.
2. Шелепало Г.В. Класифікація квазігрупових функційних рівнянь і тотожностей мінімальної довжини: дис. ... канд. фіз.-мат. наук : 01.01.06 / Фриз Ірина Василівна; Хмельниц. нац. ун-т, ДВНЗ "Прикарпат. нац. ун-т ім. Василя Стефаника". - Хмельницький, 2019. - 144 арк.
3. Фриз І.В. Ортогональність багатомісних операцій та алгоритми їх побудови: дис. ... канд. фіз.-мат. наук : 01.01.06 / Фриз Ірина Василівна ; Хмельниц. нац. ун-т, ДВНЗ "Прикарпат. нац. ун-т ім. Василя Стефаника". - Хмельницький, 2019. - 144 с.
4. Belyavskaya G. B., Popovich T. V. Totally conjugate orthogonal quasigroups and complete graphs. Journal of Mathematical Sciences. 2012. Vol. 185, № 2. P. 184–191. DOI: https://doi.org/ 10.1007/s10958-012-0907-z.
5. Криворучко Ю Класифікація латинських квадратів. // Блог Сергія Негоди. Теорія чисел для школярів. 3 лютого 2017р. URL: https://teoria0432.blogspot.com/2017/02/blog-post_27.html (дата звернення: 22 березня 2026 р.)

Крайнічук (Шелепало) Галина Василівна – к.фіз.-мат.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна, email: hv.shelepalo@vntu.edu.ua
Варшавська Юлія Валентинівна – студентка групи 1БС-22б, Вінницький національний технічний університет, Вінниця, Україна, e-mail: 04-22-035.stud@vntu.edu.ua

Krainichuk (Shelepalo) Halyna Vasylivna – Candidate of Physical and Mathematical Sciences, Docent of the Department of Information Protection, Vinnytsia National Technical University, e-mail: hv.shelepalo@vntu.edu.ua
Varshavska Yulia Valentynivna – student of group 1BS-22b, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: 04-22-035.stud@vntu.edu.ua