УДК 004.056.55

А. В. Василина
Г.В. Крайнічук (Шелепало)

ПРО ЛАТИНСЬКІ КВАДРАТИ У КРИПТОГРАФІЇ

Вінницький національний технічний університет

Анотація
В роботі ознайомлено з латинськими квадратами та розглянуто застосування їх у криптографії.
Ключові слова: латинський квадрат, квазігрупа, шифр, метод, засіб, криптографія, кібербезпека.

Abstract
The article introduces latin squares and considers their application in cryptography.
Keywords: latin square, quasigroup, cipher, method, means, cryptography, cybersecurity.

Вступ

Перше використання латинських квадратів датується XX-XI ст. н. е. (деякі згадують I ст. н. е. [1]) для магічних ритуалів - амулети з ними, як вважалося, захищали від темних сил і допомагали вигнати духів. З XVI ст. квазігрупи та їх комбінаторні аналоги – латинські квадрати знайшли застосування в криптографії. Їхні унікальні властивості є цінним інструментом для вирішення нових і складних завдань, що з'являються в галузі кіберзахисту інформації, а також в теорії квазігруп, криптографії, теорії кодів, теорії графів, теорії функційних рівнянь, комбінаториці, логіці, статистиці, економіці тощо. На даний час латинські квадрати (їх алгебричне подання – квазігрупи) мають широке застосування в різних галузях науки і техніки, зокрема і в криптографії (різні шифри, побудова кодів, хешування, ущільнення інформації, криптопротоколи, криптосистеми захисту інформації, генерування псевдовипадкових чисел, планування експериментів, складання розкладів, ігри та інше).

Метою роботи є огляд та аналіз застосувань латинських квадратів в криптографії.

Результати дослідження

Сьогодні, перше знайомство з латинськими квадратами частіше всього відбувається з різних застосунків ігрових платформ. Наприклад, в головоломці судоку, де головне завдання полягає у заповненні клітинок таблиці латинського квадрата числами так, щоб кожне число з'являлося тільки один раз у кожному рядку та кожному стовпці. Тут латинські квадрати є основною структурою. Проте справжній поштовх до наукового вивчення та застосування латинських квадратів розпочато у XVIII ст. швейцарським математиком Л. Ейлером із задачі побудови ортогональних латинських квадратів, який використовував для побудови літери латинського алфавіту, звідси і назва – латинський квадрат.

Величезний внесок у розвиток цієї галузі зробив А. Келі [2]. Латинський квадрат n-го порядку — це таблиця $L = (L_{ij})$ розміру $n \times n$, що заповнена n елементами з множини M таким чином, що в кожному рядку i та в кожному стовпці j таблиці кожний елемент множини M зустрічається тільки один раз. Тобто рядки і стовпці є перестановками елементів множини M.

Вагомий внесок у вивчення латинських квадратів зробили роботи Л. Ейлера, який вивчав ортогональні латинські квадрати для непарного порядку n, що ділиться на 4, а саме квадратів L і K, з упорядкованими парами різних $L(l_{ij})$ і $K(k_{ij})$. Ейлеру не вдалось побудувати пари ортогональних латинських квадратів порядку для $n = 2, 6$ та 10, внаслідок чого він запропонував гіпотезу про те, що пар ортогональних латинських квадратів не існує для $n = 4t+2$. Проте гіпотеза була спростована Білоусовим, тому що він довів формулами теорії квазігруп, що є побудовані ортогональні латинські квадрати для $n=10$, а для $n=2$ і $n=6$ їх не існує. Два латинських квадрати називаються ортогональними, якщо при їх накладанні одне на одного отримується такий квадрат, де всі утворені пари різні.

Латинські квадрати, які знайшли застосування в сучасній криптографії, як метод хешування, були використані розробниками шифрів у 2002 році [3]. Вже у 2005 році алгоритм Edon80, який включає ретельно підібраний список з 80 латинських квадратів з специфічними властивостями застосовувався для шифрування. Така колекція квадратів дозволяє створювати складні конвеєри для різних цілей,

починаючи від криптографії та закінчуючи розвагами. Це підкреслює універсальність та значущість латинських квадратів у сучасному інформаційному суспільстві, де вони стають невід'ємною частиною різних технологічних і наукових досягнень. [4, 5].

У криптографії латинські квадрати використовуються у різних методах шифрування, одним із них є табличне гамування. Шифр табличного гамування в алфавіті $A = \{a_1, \dots, a_n\}$ визначається довільним латинським квадратом L на A, і способом отримання послідовності літер з A, яка отримала назву гамма шифру (рис 1). Буква a_i відкритого тексту під дією знаку гамми a_j переходить у літеру a_k тексту шифрування, яка знаходиться у $j-$ому рядку та $i-$ому стовпці квадрату L (мається на увазі, що рядки в L мають номери у відповідності з порядком послідовності літер в алфавіті A) [6].

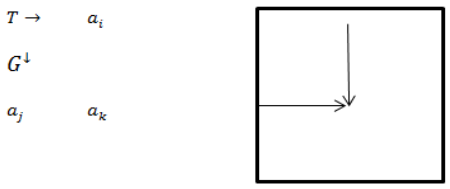

Рисунок 1 – Латинський квадрат L

У [7] Сарвате та Себеррі запропонували метод шифрування з використанням взаємних ортогональних латинських квадратів (Mutually Orthogonal Latin Squares, MOLS) (рис. 2). Основна ідея результату полягає в тому, щоб зашифрувати повідомлення *(i,j)* шляхом відправлення *m* кортежів, що з'являються в позиціях *m(i,j)* взаємно ортогональних квадратів. Через MOLS у квадраті кожен кортеж однозначно визначатиме позицію *(i, j)*. Для побудови шифру потрібен набір MOLS і спосіб вибору та впорядкування їх для шифрування або дешифрування. Ця інформація зберігатиметься в таємниці.

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

Рисунок 2 – Трійка взаємно ортогональних латинських квадратів порядку 4.

Більшість відомих структур криптографічних примітивів, а також кодів виявлення та виправлення помилок базуються на структурах асоціативної алгебри, таких як групи, кільця та поля. Проте вступ до нового етапу в розвитку криптографії був оголошений двома визначними фігурами у галузі квазігрупових досліджень - Дж. Денесом і А. Д. Кідвелом [8]. Їхнє дослідження відкрило двері для використання неасоціативних алгебричних систем, зокрема квазігруп, у криптографії. Квазігрупи та їхні комбінаторні аналоги (латинські квадрати) знайшли широке застосування в цій новій ері криптографії. Вони стали важливим інструментом для розробки і реалізації різноманітних криптографічних протоколів та алгоритмів, що вимагають більшої гнучкості та різноманітності у порівнянні з традиційними асоціативними структурами. Це відкриває нові можливості для застосування криптографії у сферах, де раніше вона не була так ефективною або навіть можливою.

Александра Мілева провела дослідження, в результаті якого було виявлено, що навіть квазігрупи малих порядків виявляються дуже придатними для застосування у криптографії [9]. Це виявлення є досить важливим, оскільки воно відкриває нові перспективи в розвитку криптографічних методів, особливо з огляду на те, що малий порядок квазігруп не завжди був розгляданий як варіант для криптографічних застосувань. Зокрема, це стосується квазігруп через їхню особливу структуру, унікальні властивості та велику кількість можливих комбінацій.

Одним із визначних досягнень у цьому напрямку є робота С. Марковського, який описав потокові шифри, побудовані на основі квазігруп та їх парастрофів [10]. Потокові шифри є одними з найпоширеніших криптографічних схем, які використовуються для захисту інформації у реальному часі. Вони працюють шляхом генерації потоку псевдовипадкових бітів, які потім комбінуються з оригінальним текстом для створення шифртексту. До того ж, використання властивості оборотності квазігруп (парастрофів) дозволяє покращити якість та надійність шифрування. Парастрофи - це спеціальні перестановки елементів

квазігрупи, які застосовуються для зміни структури криптографічного ключа. Це робить атаку на шифр ще складнішою, оскільки змінюється внутрішня структура ключа, що ускладнює проведення атак методом перебору.

У [11], використовуючи парастрофи квазігруп, Крапєж дав ідею перетворення рядка квазігрупи, яка може бути застосована в криптографії. Модифікація цього перетворення квазігрупи визначена в [12], де описано залежності між парастрофами квазігрупи.

Шифр Тритемія використовує масив з 26 × 26 квадратів, що містить 26 букв алфавіту (за умови, що мова англійська), розташованих у латинському квадраті. Різні рядки цього квадратного масиву використовуються для шифрування різних букв відкритого тексту способом, заданим ключовим словом або ключовою фразою [13]. Оскільки латинський квадрат є таблицею множення квазігрупи, це можна розглядати як найбільш раннє використання неасоціативної алгебричної структури в криптології. Існує можливість розвитку цього напряму з використанням квазігрупового підходу, зокрема, з використанням ортогональних систем бінарних або n-арних квазігруп.

Еліска Очодкова та Вацлав Снасель [14] запропонували використовувати квазігрупи для безпечного кодування файлової системи.

У [15] С. Марковський, Д. Глігороскі, Б. Стойчевська вводять потоковий шифр з майже відкритим ключем, заснований на квазігрупах для визначення відповідного шифрування і дешифрування. Вони розглядають кібербезпеку цього методу. Показано, що ключ (квазігрупи) може бути публічним і при цьому мати достатню захищеність. Також наводиться програмна реалізація.

У [16] представлена криптосистема з відкритим ключем, що використовує узагальнені потокові шифри на основі квазігруп. Показано, що така криптосистема дозволяє безпечно передавати як криптограму, так і секретну частину ключа шифрування за допомогою одного і того ж незахищеного каналу.

Великі перспективи має застосування рядково-латинських квадратів у різних галузях сучасної криптології («неокриптологія»). В [17] запропоновано використовувати рядково-латинські квадрати для генерації відкритого ключа, звичайну систему передачі повідомлення, що має форму латинського квадрата, рядково-латинського квадратного аналога системи RSA і на основі рядково-латинських квадратів процедури цифрового підпису.

У [18] автори запропонували нову схему аутентифікації на квазігрупах (латинських квадратах). Застосування квазігруп у цих потокових шифрах дає можливість створювати ефективні та безпечні криптографічні системи. Квазігрупи дозволяють забезпечити високу стійкість до атак, таких як атаки з використанням алгоритмів зворотного аналізу, колізій та інших методів криптоаналізу.

На сьогодні маємо підвищений інтерес до вивчення квазігруп та латинських квадратів, тому що розробка методів шифрування та дешифрування даних з використанням квазігруп, луп, латинських квадратів, кубів та гіперкубів дасть можливість значно підвищити надійність передачі даних незахищеними каналами.

Висновки

Таким чином, після аналізу опрацьованих джерел стає очевидним, що латинські квадрати мають широкий спектр застосування в криптографії. На жаль, незважаючи на широкі дослідження, проведені на цю тему, і гіпотези, висунуті вченими, все ще є кілька важливих запитань, що стосуються латинських квадратів, які залишаються без відповіді (межі максимальної кількості трансверсалей у латинському квадраті, характеристика латинських квадратів у таблицях множення лупи Муфанг, оцінка щільності часткового квадрату, що задовольняє властивість Блекберна тощо).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Andersen, L. D. Chapter on The history of latin squares // Department of Mathematical Sciences, Aalborg University. 2007. – Research Report Series, No. R-2007. – 32.
2. Cayley A. On Latin Square. Messenger of mathematics. 1890. V.XIX. P.135-137.
3. J. Dvorsky, E. Ochodkova, and V. Snasel. Hash functions based on large quasigroups. Velokonocni kryptologie, pages 1–8, 2002.
4. O. Sapiha. Dinytsia`s task. Режим доступу: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/6cf4bf8d-8104-4878-a1f7-60104f7bb810/content (дата звернення: 07.03.2024).
5. O. Oliinyk, V. Vyshniak, E. Kravchenko. Problems of latin squares. Режим доступу: https://archive.interconf.center/index.php/conference-proceeding/article/download/1871/1901 (дата звернення: 06.03.2024).
6. Christoffer Olsson Discreet Discrete Mathematics Secret Communication Using Latin Squares and Quasigroups // Bachelor thesis, 15 hp Spring term – 2017. Режим доступу: https://www.diva-portal.org/smash/get/diva2:1114284/FULLTEXT01.pdf (дата звернення: 07.03.2024).

7. Dinesh G. Sarvate and Jennifer Seberry. Encryption methods based on combinatorial designs. Ars Combinatoria, (21A):237–246, 1986.
8. J. Denes and A. D. Keedwell. Some applications of non-associative algebraic systems in cryptology. Pure Mathematics and Applications, 12(2):147{195, 2001.
9. A. Mileva, “Cryptographic Primitives with Quasigroup Transformations,” Ph.D. dissertation, University Ss. Cyril and Methodius, Skopje, Macedonia, 2010.
10. Markovski S, Gligoroski D, and Bakeva V. Quasigroup and hash functions Proc. of the 6th ICDMA. Bansko. 2001. P. 43-50.
11. Krapeˇz, A.: An Application Of Quasigroups in Cryptology. In: Math. Maced. Vol. 8 (2010), pp. 47-52
12. Bakeva,V., Dimitrova, V., Popovska-Mitrovikj, A.: Parastrophic Quasigrouop String Processing. In: Proc. of the 8th Conference on Informatics and Information Technology with International Participants, Macedonia (2011) pp. 19-21.
13. D. Kahn, The codebreakers: the story of secret writing, Wiedenfield and Nicolson, London, 1967.
14. E. Ochadkova, V. Snasel, Using quasigroups for secure encoding of file system, Abstract of Talk on Conference ”Security and Protection of information”, Brno, Czech Republic, 9-11.05.2001, 24 pages.
15. S. Markovski, D. Gligoroski, B. Stojcevska, Secure two-way on-line communication by using quasi group enciphering with almost public key, Novi Sad J. Math. 30, No.2, 2000,43-49.
16. C. Koscielny, G.L. Mullen A quasigroup-based public-key cryptosystem, Int. J. Appl. Math. Comput. Sci. 9, No.4, 1999, 955-963.
17. Charles F. Laywine and Gary L. Mullen, Discrete Mathematics Using Latin Squares, New York, John Wiley & Sons, Inc., 1998.
18. J. Denes, A. D. Keedwell´ , A new authentification scheme based on Latin squres, Discrete Math., 106/107, 1992, 157-161.

Василина Анастасія Василівна – студентка групи 2БС-22б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nstvsln@gmail.com.

Науковий керівник: ***Шелепало (Крайнічук) Галина Василівна*** — кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: hv.shelepalo@vntu.edu.ua.

Vasylyna Anastasia Vasylivna- is a student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Shelepalo Halyna (Krainichuk) Vasylivna*** — Candidate of Physical and Mathematical Sciences, Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia.