УДК 004.056.55

О. В. Семенюк
Г.В. Крайнічук (Шелепало)

УМОВИ ВІДНОВЛЕННЯ СЕКРЕТНОГО КЛЮЧА НА ВІДКРИТИХ КОМІРКАХ ЛАТИНСЬКОГО КВАДРАТА

Вінницький національний технічний університет

Анотація. *В цій роботі встановлено умови всеможливих відкритих комірок всіх латинськиих квадратів 3-го порядку з однозначним латинським заповненням та розглянуто застосування їх для криптоаналізу.*
Ключові слова: латинський квадрат, квазігрупа, шифр, метод, криптоаналіз, кібербезпека.

Abstract. *In this article, the conditions for all possible open cells of all Latin squares of order 3 with single-valued Latin filling are established and their application for cryptanalysis are considered.*
Keywords: latin square, quasigroup, cipher, method, cryptography, cryptanalysis, cybersecurity.

Вступ

На сьогодні квазігрупи та їх комбінаторні аналоги – латинські квадрати широко застосовуються 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). А. Мілєва виявила, що навіть квазігрупи малих порядків є достатньо придатними для застосування у криптографії [1]. Це виявлення є досить важливим, оскільки відкриває нові перспективи в розвитку криптографічних методів, особливо з огляду на те, що малий порядок квазігруп не завжди розглядався як варіант для криптаоаналізу. Зокрема, це стосується квазігруп через їхню особливу структуру, унікальні властивості та велику кількість можливих комбінацій. Одним з найпоширеніших криптографічних схем, що використовуються для захисту інформації у реальному часі є робота С. Марковського для потокових шифрів, побудованих на основі квазігруп та їх парастрофів [2]. Шляхом генерації потоку псевдовипадкових бітів, які потім комбінуються з оригінальним текстом, створюється структура секретного ключа. Оскільки парастрофами є спеціальні перестановки елементів квазігрупи, що застосовуються для зміни структури криптографічного ключа, то атака на шифр стає складнішою, бо змінюється внутрішня структура ключа, що ускладнює проведення атак методом повного перебору. В низці наукових праць та, зокрема, в книгах Д.Кідвела [3], Щербакова В.І. [4] згадується застосування кількості латинських квадратів для криптоаналізу. Це стає цінним інструментом для розв'язування нових і складних завдань, що з'являються в галузі кіберзахисту інформації.

Метою роботи є розробка для відновлення секретного ключа, побудованого на основі квазігруп, а точніше на відкритих комірках таблиць Келі латинських квадратів 3-го порядків.

Результати дослідження

Латинський квадрат – це квадратна матриця розміру n, в якій кожен рядок і стовпець є перестановкою елементів скінченної множини S, що має n елементів. При цьому кожен елемент з'являється лише один раз у кожному рядку та кожному стовпці.

Для встановлення умов існування кількості можливих варіацій мінімальної кількості відкритих комірок для відновлення секретного ключа з однозначним доповненням до латинського квадрата досить розглянути лише нормалізовані латинські квадрати. Нормалізованим називають латинський квадрат, в якого елементи першого рядка і першого стовпця розташовані в лексикографічному порядку.

Нормалізованих латинських квадратів 2-го та 3-го порядку існує тільки по одному. Для 2-го порядку необхідно і достатньо відкрити хоча б один елемент, щоб однозначно його заповнити. А от вже починаючи для 3-го порядку і вище таких умов досить багато і щоб їх розпізнавати, нагадаємо деякі основні означення понять та термінів, що використано для доведень результатів. Діагоналлю квадрата n-го порядку є сукупність n-комірок, взятих з різних рядків і різних стовпців. Всього в квадраті n-го порядку є $n!$ діагоналей. Кількість діагоналей квадрату порядку існує $3! = 6$. Діагональ латинського квадрата називають трансверсаллю, якщо в її комірках всі елементи різні. [3]

Нехай маємо таблицю Келі латинського квадрата $\mathcal{L}$ 3-го порядку (див. пункт А в таблиці 1), де елементи k_{ij} мають індекси відповідного рядка i та відповідного стовпця j, на перетині яких є елемент k.

Лема 1. *Нормалізований латинський квадрат 3-го порядку має 3 трансверсалі, а саме* $(0_{00}; 2_{11}; 1_{22})$, $(1_{01}; 0_{12}; 2_{20})$, $(0_{00}; 2_{11}; 1_{22})$. (Приклад трансверсалі див. пункт Б в таблиці 1).

Твердження 1. *Якщо в нормалізованому латинському квадраті 3-го порядку заповнені 3 комірки, що утворюють трансверсаль, то такий латинський квадрат має однозначне латинське заповнення.*

Наслідок 1. *Кількість заповнень 3-ьох комірок латинського квадрата 3-го порядку, які утворюють трансверсаль, всього є 3.* (Приклад нормалізованого квадрата див. пункт В у таблиці 1)

$\mathcal{L}$	0	1	2
0	k_{00}	k_{01}	k_{02}
1	k_{10}	k_{11}	k_{12}
2	k_{20}	k_{21}	k_{22}

А

L_x	0	1	2
0	x	1	x
1	x	x	0
2	2	x	x

Б

L	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

В

Таблиця 1 прикладів латинських квадратів 3-го порядку

Твердження 2. *Якщо в нормалізованому латинському квадраті 3-го порядку заповнені 4 комірки, три з яких утворюють діагональ одного елемента, то такий латинський квадрат має однозначне латинське заповнення.* (Приклад діагоналей див. таблиця 2).

Наслідок 2. *Кількість заповнень 4-ьох довільних комірок латинського квадрата 3-го порядку 3 з яких утворюють діагональ одного елемента, становить 18.*

	0	1	2
0	0		
1			0
2		0	

	0	1	2
0		1	
1	1		
2			1

	0	1	2
0			2
1		2	
2	2		

Таблиця 2. Приклад діагоналей одного елемента для латинського квадрата 3-го порядку

Твердження 3. *Якщо в нормалізованому латинському квадраті заповнені 4 комірки, три з яких це будь-який рядок чи стовпець, то такий латинський квадрат має однозначне латинське заповнення.* (приклад див. таблиця 3)

Наслідок 3. *Кількість заповнень 4-ьох довільних комірок латинського квадрата 3-го порядку, три з яких утворюють заповнений рядок або стовпець, становить 36.*

	0	1	2
0	0	1	2
1			
2			

	0	1	2
0			
1	1	2	0
2			

	0	1	2
0			
1			
2	2	0	1

	0	1	2
0	0		
1	1		
2	2		

L_x	0	1	2
0		1	
1		2	
2		0	

L	0	1	2
0			2
1			0
2			1

Таблиця 3. Приклад рядкового (стовпцевого) заповнення для нормалізованого часткового латинського квадрата 3-го порядку

Твердження 4. *Якщо в нормалізованому латинському квадраті 3-го порядку заповнені 3 комірки, дві з яких один і той самий елемент, а третій довільний інший елемент, що не повторюється, то такий латинський квадрат має однозначне латинське заповнення.* (Приклад див. таблиця 4)

Наслідок 4. *Кількість заповнень 3-ьох довільних комірок латинського квадрата 3-го порядку, дві з яких один елемент, а третя комірка довільний інший елемент, що не повторюється, становить 54.*

Лема 2. *Для нормалізованого латинського квадрата 3-го порядку мінімальна кількість відновлень секретного ключа за відомими відкритими комірками становить 111 латинських заповнень.*

	0	1	2
0	0	1	
1	1		
2			

L_x	0	1	2
0	0	1	
1			
2			1

L	0	1	2
0	0		
1	1		
2			1

	0	1	2
0		1	
1	1		0
2			

L_x	0	1	2
0		1	
1			0
2			1

L	0	1	2
0			
1	1		0
2			1

	0	1	2
0		1	
1	1		
2		0	

L_x	0	1	2
0		1	
1			
2		0	1

L	0	1	2
0			
1	1		
2		0	1

Таблиця 4. Приклад варіацій заповнення відомих 3-ох комірок 2-ма різними елементами для нормалізованого латинського квадрата 3-го порядку

Теорема 1. *Оскільки всього існує 12 латинських квадратів 3-го порядку, то мінімальна кількість відновлень секретного ключа за відомими будь-якими 3-ма чи 4-ма відкритими комірками латинських квадратів 3-го порядку становить 1332 однозначних латинських заповнень.*

Таким чином, для криптоаналізу шифрів, де використовуються в якості секретного ключа латинські квадрати навіть такого малого порядку за різними атаками, що відновлюють комірки, в яких зашифровані повідомлення, можна застосувати таке використання однозначного заповнення секретного ключа за повним перебором та комбінаторним обчисленням.

Висновки

Отже, після аналізу опрацьованих матеріалів та доведених тверджень стає доцільним метод повного опису однозначних заповнень латинських квадратів за мінімальною кількістю відомих комірок для криптоаналізу. А звідси випливає дослідження для виявлення умов відновлення секретного ключа, використаного в якості латинських квадратів більших порядків, що і, власне, є подальшою перспективою майбутніх досліджень даного напрямку.

Подяка

Автори висловлюють подяку професору, д.т.н. Лужецькому В.А. за ідею використання квазігруп в криптоаналізі та рецензенту д.фіз-мат.н. Сохацькому Ф.М. за актуальні обговорення та дискусії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A. Mileva, “Cryptographic Primitives with Quasigroup Transformations,” Ph.D. dissertation, University Ss. Cyril and Methodius, Skopje, Macedonia, 2010.
2. Markovski S, Gligoroski D, and Bakeva V. Quasigroup and hash functions Proc. of the 6th ICDMA. Bansko. 2021. P. 43-50.
3. Keedwell A. D., Dénes J. Latin Squares and Their Applications. Elsevier Science & Technology Books, 2015.
4. Shcherbacov V. Elements of Quasigroup Theory and Applications. Taylor & Francis Group, 2017.

Семенюк Олег Андрійович – студент групи 1БС-23м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет,

м. Вінниця, e-mail: olegmarkelov72@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.

Semeniuk Oleh Andriyovych - is a student of group 1BS-23m, 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.