УДК 512.548.7

СІР-КВАЗІГРУПИ 4-ГО ПОРЯДКУ З ОБОРОТНИМ ЕЛЕМЕНТОМ X^2 СЕРЕД ІЗОТОПІВ ГРУПИ КЛЕЙНА

Галина Крайнічук, Ігор Пилявець, Євгеній Радченко

Вінницький національний технічний університет

krainichuk@ukr.net, igormorozov920@gmail.com, jenya.radchenko@gmail.com

Найпоширенішим способом для збереження конфіденційності інформації є її шифрування, принцип якого грунтується на перетворенні даних. Одним з різновидів алгоритмів шифрування є алгоритм, побудований на квазігрупах та їх парастрофних перетвореннях [1]. Власне квазігрупи, а точніше вхідні дані, за якими будується квазігрупа, використовуються як секретний ключ, а сам алгоритм шифрування описаний на парастрофних перетвореннях квазігрупи, згідно з тотожністю, яку вона задовольняє. Результат таблички Келі квазігрупи – латинський квадрат, тобто масив $n \times n$, де кожний елемент зустрічається в кожному рядку та кожному стовпчику лише один раз.

Квазігрупою називається групоїд $(Q;\cdot)$ такий, що для довільних $a, b \in Q$ система рівнянь $a \cdot x = b$, $y \cdot a = b$ має єдиний розв'язок. Квазігрупа $(Q;\cdot)$ називається: *середньою, лівою та правою СІР-квазігрупою*, якщо відповідно існують відображення ψ, υ, γ такі, що для всіх x, y виконуються рівності $\psi(x) \cdot yx = y$; $yx \cdot y = \upsilon(x)$; $y \cdot xy = \gamma(x)$, де ψ, υ, γ називаються *лівою, правою* та *середньою функцією оборотності* [2]. Як приклад з [3], результати описані над ізотопами групи Клейна ($\overline{x} \oplus \overline{x} = \overline{0}$) для СІР-квазігруп 4-го порядку з оборотним елементом x^2, що задовольняють тотожності:

$$x \cdot yx^2 = y\,,\ xy \cdot x^2 = y\,,\ x^2 y \cdot x = y\,,\ x^2 \cdot yx = y\,. \qquad (1)$$

Твердження 1. *Квазігрупа* $(Q;\cdot)$ *задовольняє тотожності (1) над ізотопами групи Клейна* $\left(\mathbb{Z}_2^2;\oplus,\overline{0}\right)$ *тоді і тільки тоді, коли вона має канонічний розклад* $x \cdot y = \overline{x}A \oplus \overline{y}A^{-1} \oplus \overline{a}$, *де матриця* $A \in \left\{\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\right\}$, *довільний векторний елемент* $\overline{a} \in \{(0,0);(0,1);(1,0);(1,1)\}$.

Наслідок 1. *Кількість квазігруп 4-го порядку, що визначаються* (1) *над ізотопами групи Клейна є 8, латинські квадрати яких подано в таблиці* 1.

Твердження 2. *Многовид* $\mathfrak{I}$ *середніх СІР-квазігруп з оборотним елементом* x^2 *визначається однією із тотожностей* (1).

http://iapmm.lviv.ua/mpmm2023/materials/mm07_29.pdf

Таблиця 1. Таблиці Келі CIP-квазігруп над ізотопами групи Клейна

00				
·	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

01				
1)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

10				
3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

11				
5)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

•	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

2)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

4)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

6)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

Наслідок 2. *Тотожності* (1) *рівносильні і виконуються в квазігрупах, заданих табличками Келі 1) та 2).*

Твердження 3. *Многовид* ${}^{\ell}\mathfrak{I}$ *правих CIP-квазігруп з оборотним елементом* x^2 *визначається однією із тотожностей:*

$$x(yx\cdot x)=yx\cdot y\,,\ (y\cdot xy)x=y\cdot yx\,,\ y\left(\overset{\ell}{x\cdot x}\right)\cdot y=x\,,\ y\cdot\left(\overset{r}{x\cdot x}\right)y=x\,. \tag{2}$$

Наслідок 3. *Тотожності* (2) *рівносильні і виконуються в квазігрупах, заданих табличками Келі 3) та 4).*

Твердження 4. *Многовид* ${}^{r}\mathfrak{I}$ *лівих CIP-квазігруп з оборотним елементом* x^2 *визначається однією із тотожностей:*

$$x(y\cdot xy)=x\,,\ (yx\cdot y)x=x\,. \tag{3}$$

Наслідок 4. *Тотожності* (3) *рівносильні і виконуються в квазігрупі, заданою табличкою Келі 5) та 6).*

1. *Dimitrova V., Bakeva V., Popovska-Mitrovik A., Krapez A.* Cryptographic properties of parastrophic quasigroup transformation / In: Markovski S., Gusev M. (eds) ICT Innovations 2012. Advances in Intelligent Systems and Computing, vol 207. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37169-1_23
2. *Сохацький Ф.М., Луценко А.В., Фриз І.В.* Побудова квазігруп з властивістю оборотності // Мат. методи та фіз.-мех. поля. – 2021. – **64**, № 4. – С. 5–17.
3. *Сохацький Ф.М.* Invertible binary functions and quasigroups of the order four // XIII Міжн. алгебр. конф. в Україні: 6–9 лип. 2021 р. – КНУ ім. Т. Шевченка, 2021. – С. 77–78.

CIP-QUASIGROUPS OF THE 4TH ORDER WITH THE INVERTIBLE ELEMENT X^2 OVER ISOTOPES OF THE KLEIN GROPE

The description of 8 CIP-quasigroups of 4th order over isotopes of the Klein group is given. They are depicted in the form of Cayley tables. The conditions for the canonical decomposition of CIP-quasigroups are established. A list of equivalent identities that define the corresponding varieties of CIP-quasigroups is given.