We consider the property in the variety of loops for all kinds of translations: left, right and middle. There are 9 defining relations:

$$L_x^{-1} = L_{\alpha x}, \quad L_x^{-1} = R_{\alpha x}, \quad L_x^{-1} = M_{\alpha x}, \quad R_x^{-1} = R_{\alpha x}, \quad R_x^{-1} = L_{\alpha x},$$

$$R_x^{-1} = M_{\alpha x}, \quad M_x^{-1} = M_{\alpha x}, \quad M_x^{-1} = L_{\alpha x}, \quad M_x^{-1} = R_{\alpha x}.$$

Theorem 1. *If inverses of some kind of translations of a loop $(Q;\cdot,e)$ are also translations of some fixed kind, then the loop belongs to one of the following classes of loops:*

$L_x^{-1} = L_{\alpha x}$	$x^{-1} \cdot xy = y$	*left IP-loop*
$R_x^{-1} = R_{\alpha x}$	$yx \cdot x^{-1} = y$	*right IP-loop*
$R_x^{-1} = L_{\alpha x}$	${}^{-1}x \cdot yx = y$	*left CIP-loop*
$L_x^{-1} = R_{\alpha x}$	$xy \cdot x^{-1} = y$	*right CIP-loop*
$L_x^{-1} = M_{\alpha x}$ $M_x^{-1} = L_{\alpha x}$	$xy \cdot y = x$	*right symmetric loop*
$R_x^{-1} = M_{\alpha x}$ $M_x^{-1} = R_{\alpha x}$	$xy \cdot x = y$	*semi-symmetric loop*
$M_x^{-1} = M_{\alpha x}$	$yx = xy$	*commutative loop*

where ${}^{-1}x \cdot x = e$ *and* $x \cdot x^{-1} = e$.

References

1. V.D. Belousov, *Foundations of the theory of quasigroups and loops*, M.: Nauka (1967), 222 (Russian).
2. N.N. Didurik and V.A. Shcherbacov, *On definition of CI-quasigroup*, ROMAI Journal (2017), Vol. 13 Issue 2, p. 55 –58.

Contact information

Alla Lutsenko
Department of mathematical analysis and differential equations, Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine
Email address: lucenko.alla32@gmail.com

Key words and phrases. Quasigroup, *IP*-loop, invertible function, invertibility property

Models of Cryptography Transformations Based on Quasigroups

Volodymyr Luzhetskyi, Yurii Baryshev

It is intuitively obvious, that usage of unknown cryptographic transformations should be more secure against breaking, than usage of known ones. Modern cryptography approaches alters that statements reasoning, that the transformation infeasibility of breaking should be visible for customers for the verification sake. Consequently, the task of this transformation modeling to find the way out of the contradictive conditions arose.

According to the automatons definition given in [**1**] they were used to describe cryptographic transformations. An open cryptographic algorithm from the cryptanalysis point of view could be described as one performed by a deterministic automaton *ADC* [**2**]:

$$ADC = (PT, CT, k, IS, f(*)), \quad (1)$$

where PT – a set of all possible plaintexts; CT – a set of all possible ciphertext; k – used key; $f(*)$ – a function, which formilize known to an intruder cryptographic transformations.

Therefore unknown cryptographic algorithms are more infeasible and could be considered by the intruders as ones performed by the following nondeterministic automaton [**2**]:

$$ANDC = (PT, CT, k, IS, F), \quad (2)$$

where F – an unknown to an intruder set of all possible cryptographic transformations.

The uncertainty of the performed action forces intruder to perform additional picking out while cryptanalitical attack designing, which obviously increases infeasibility of analyzed cryptographic algorithms. However the need of cryptographic transformations to be open causes the need of the following modification of 1 to perform action like 2, consequently named pseudonondeterministic ones [**2, 3**]:

$$APNDC = (PT, CT, k, IS, F_v, V), \quad (3)$$

where $v \in V$ – a control vector used to determine the instance of F, which was used for the transformation during its performance.

The main difficulty of APNDC implementation covers programmed generation of set F. To solve the task authors propose to use quasigroups as cryptographic primitives for the transformation designing [**3**]. The performed expiriments results confirms correctness the proposition.

References

1. J. A. Anderson , *Discrete Mathematics with Combinatorics*, Prentice Hall, Upper Saddle River, New Jersey, 2004, 960.
2. V. Luzhetskyi, Y. Baryshev and V. Derech *Pseudonondeterministic Approach of Control Systems Cryptographic Protection*, Information Technology in Selected Areas of Management 2017, AGH University of Science and Technology Press, Krakow, 2018, 25-39.
3. V. Luzhetskyi and Y. Baryshev *Data-driven Pseudonondeterministic Hashing Constructions*, Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, 114z-116..

Contact information

Volodymyr Luzhetskyi
Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine

Yurii Baryshev
Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine
Email address: yuriy.baryshev@gmail.com

Key words and phrases. Algebra, automaton, cryptography, pseudonondeterministic, semigroups