UDC: 512.548:003.26

Rodiuk A. I., higher education student,
Lutsenko A. V., PhD in Mathematics, Senior Lecturer,
Acting Head of the Department of Applied Mathematics and Cybersecurity,
Vasyl' Stus Donetsk National University

APPLICATION OF TERNARY QUASIGROUPS IN CRYPTOGRAPHY

Abstract. The paper is devoted to the analysis of ternary quasigroup string transformations. The paper considers the principles of construction and properties of $e_{t,f}$-transformation, $d_{t,f}$-transformation, and demonstrates their suitability for use in cryptography as a basis for data encryption and decryption.

Keywords: ternary quasigroup, $e_{t,f}$-transformation, $d_{t,f}$-transformation, cryptography.

Introduction. An important direction in modern cryptography is the search for new algebraic methods for constructing cryptographic primitives. Quasigroups, due to their structural diversity and nonlinearity, are increasingly used as the basis for encryption schemes. In particular, since ternary quasigroups extend the concept of binary quasigroups, they can provide additional flexibility and complexity in the design of cryptographic transformations.

The purpose of this paper is to analyze ternary quasigroup string transformations and their properties in the context of constructing cryptographic primitives. Based on the structure of ternary quasigroups and their parastrophes, the paper considers the possibility of using the corresponding transformations for encryption and decryption processes.

Main text. A quasigroup (Q, f) s an algebraic structure with a single binary operation f on a nonempty set Q, in which the equations $f(x, a) = b$ and $f(a, y) = b$ have unique solutions for all $a, b \in Q$.

The quasigroup (Q, f) is called a ternary quasigroup if $f: Q^3 \to Q$ is a ternary operation on Q.

Let $x_1, x_2, x_3 \in Q$. If x_1 is a fixed element and $f_{x_1}(x_2, x_3) = f(x_1, x_2, x_3)$, then $\left(Q, f_{x_1}\right)$ is a binary quasigroup called x_1-plane quasigroup of (Q, f) [1].

Let (Q, f) be a ternary quasigroup that consists of the binary quasigroups $\left(Q, f_{n_1}\right)$, $\left(Q, f_{n_2}\right)$, …, $\left(Q, f_{n_k}\right)$ and $Q^+ = \{a_1 a_2 \dots a_k | a_i \in Q, k \geq 2\}$ is the set of all finite strings with elements of $Q = \{1,2,3,4\}$. If l_1, l_2 are fixed elements of Q, called leaders, then ternary quasigroup string transformations $e_{t_{l_1,l_2},f}, d_{t_{l_1,l_2},f} : Q^+ \to Q^+$ are defined below.

The ternary function $e_{t_{l_1,l_2},f}$ is called $e_{t,f}$-transformation of Q^+ and is defined as follows:

$$e_{t_{l_1,l_2},f}(\alpha) = b_1 b_2 \dots b_n \Leftrightarrow \begin{cases} f(l_1, l_2, a_1) = f_{l_1}(l_2, a_1) = b_1 \\ f(l_2, b_1, a_2) = f_{l_2}(b_1, a_2) = b_2 \\ f(b_1, b_2, a_3) = f_{b_1}(b_2, a_3) = b_3 \\ \dots \\ f(b_{n-2}, b_{n-1}, a_n) = f_{b_{n-2}}(b_{n-1}, a_n) = b_n, \end{cases}$$

where $a_i \in Q$, $\alpha = a_1 a_2 \dots a_n$, for each $i \in \{1,2,\dots,n\}$.

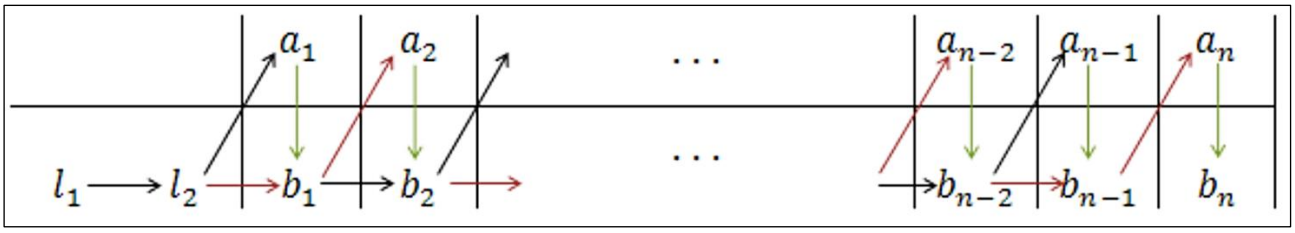

Figure 1 – Graphical representation of $e_{t,f}$-transformation

The ternary function $d_{t_{l_1,l_2},f}$ is called $d_{t,f}$-transformation of Q^+ and is defined as follows:

$$d_{t_{l_1,l_2},f}(\alpha) = c_1 c_2 \dots c_n \Leftrightarrow \begin{cases} f(l_1, l_2, a_1) = f_{l_1}(l_2, a_1) = c_1 \\ f(l_2, a_1, a_2) = f_{l_2}(a_1, a_2) = c_2 \\ f(a_1, a_2, a_3) = f_{a_1}(a_2, a_3) = c_3 \\ \dots \\ f(a_{n-2}, a_{n-1}, a_n) = f_{a_{n-2}}(a_{n-1}, a_n) = c_n, \end{cases}$$

where $a_i \in Q$, $\alpha = a_1 a_2 \dots a_n$, for each $i \in \{1,2,\dots,n\}$.

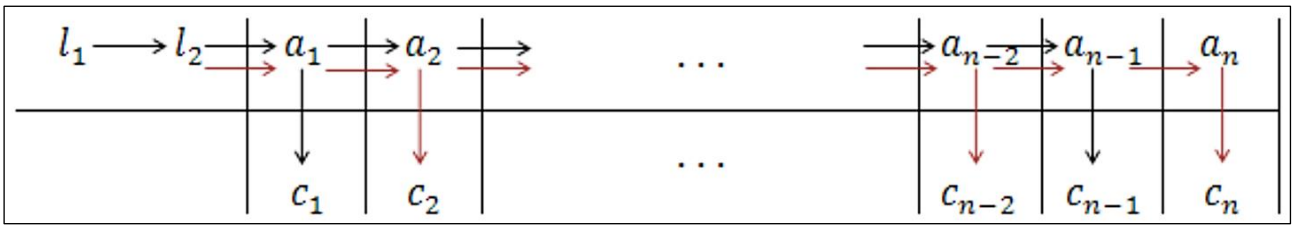

Figure 2 – Graphical representation of $d_{t,f}$-transformation

The ternary quasigroup (Q, f') is called a parastrophe of (Q, f) if it is obtained by applying parastrophic operations to each of the binary quasigroups (Q, f_i) that constitute (Q, f).

Since the transformation function $e_{t,f}$ based on operation f and $d_{t,f'}$-transformation to the operation f' are permutations on Q^+ and $\left(e_{t,f}\right)^{-1} = d_{t,f'}$ it becomes obvious that if $e_{t,f}$-transformation is applied on the starting sequence α and then $d_{t,f'}$-transformation on the obtained sequence β the starting sequence α will be returned. Then, for designing cryptographic primitives, $e_{t,f}$-transformation can be used as an encryption function and $d_{t,f'}$-transformation as a decryption function [2; 3].

Conclusion. The paper presents the definition and main properties of ternary quasigroup string transformations, which can be applied in the development of cryptographic primitives. It is shown that $e_{t,f}$-transformation and $d_{t,f'}$-transformation can be used for encryption and decryption, respectively, forming a reversible process suitable for secure data processing. The results confirm the applicability of ternary quasigroups in cryptography.

Future research may focus on a deeper analysis of the properties of ternary quasigroups, their classification, and the development of cryptographic algorithms, such as block and stream ciphers or hash functions, based on these algebraic structures.

References

1. Belousov V. D. n-ary Quasigroups. Kishinev: Stiinca Publishing House, 1972. 231 p.
2. Dimitrova V. Quasigroup Transformations and Their Application: MSc thesis. Skopje, 2005.
3. Dimitrova V., Mihajloska H. An Application of Ternary Quasigroup String Transformations. *The Second International Conference on Media, Communication and Cryptography Technologies*. 2009. 9 p.