UDC 004.056.55:004.312.2

Lada Nataliia,
Candidate of Technical Sciences, Senior Lecturer, Cherkasy State Technological University, Cherkasy, Ukraine,
ORCID ID 0000-0002-7682-2970

Kozlovska Svitlana,
Senior Lecturer, East European University of Economics and Management, Cherkasy, Ukraine,
ORCID ID 0000-0002-1754-1220

Rudnytskyi Serhii,
Candidate of Technical Sciences, Senior Lecturer, Cherkasy State Technological University, Cherkasy, Ukraine,
ORCID ID 0000-0003-4389-1088

THE SYMMETRIC OPERATIONS' MATHEMATICAL GROUP CONSTRUCTING BASED ON MODULO-2 ADDITION

The article is devoted to improving the quality of the stream ciphering systems for confidential information encryption through increasing the variability of cryptographic transformations by using a new group of two-operand two-bit operations synthesized basing on modulo-2 addition.

For achieving the aim, a comparative analysis of two-operand operations with one-operand operations was performed, which showed that the first four operations can be obtained basing on the first four one-operand operations of the

first operand processing, by adding the modulo-2 addition operation of their base operation of transforming the second operand, and by modulo-2 adding the basic operation of processing the second operand it can be obtained the other two-operand operations from inversion operations' subgroups. The results of classifying a group of two-operand two-bit symmetric operations of information's cryptographic transformation were visualized, which made it possible to establish relationships between groups of one-and two-operand operations.

Basing on the obtained results, a method for synthesizing the operations' group of modulo-2 addition is developed for stream ciphering based on the modulo-2 addition operation. The method's crux is in the base group's two-bit two-operand operations synthesis, based on combining the same basic operations of converting the first and second operands by modulo-2 addition. Constructing a complete mathematical group of these operations is carried out by the additional use of permutation operations and operands' inversion of the base group operations.

The application of the method allows synthesizing all the twenty-four modifications of two-bit symmetric modulo-2 addition operations based on applying the three basic one-operand two-bit operations of information cryptographic conversion.

Keywords: cryptographic operation, modifications of operations, mathematical group of operations, module addition, operation models, streaming encryption.

REFERENCES

1. *Rudnitskyi V.M.* (2018). Kryptohrafichne koduvannia: obrobka ta zakhyst informatsii: kolektyvna monohrafiia. "Cryptographic encoding: processing and protection of information: a collective monograph", TOV «DISA PLIUS», Kharkiv, 139 p. [in Ukrainian].

2. *Rudnitskyi V.M., Lada N.V. and Babenko V.H.* (2018). Kryptohrafichne koduvannia: syntez operatsii potokovoho shyfruvannia z tochnistiu do perestanovki: monohrafiia. "Cryptographic encoding: Synthesis for streaming

encryption operations within the accuracy of permutation: monograph", TOV «DISA PLIUS», Kharkiv, 184 p. [in Ukrainian].

3. *Babenko V.H. and Lada N.V.* (2016). Tekhnolohiia doslidzhennia operatsii dodavannia za modulem. "Technology of research operations of addition modulo", Smart and Young: shchomisiachnyi naukovyi zhurnal, No. 11–12, (118), Vol. 1., P. 49–54 [in Ukrainian].

4. *Babenko V.H.* (2012). Doslidzhennia matrychnykh operatsii kryptohrafichnoho peretvorennia na osnovi aryfmetychnykh operatsii za modulem. "The research of matrix operations of cryptographic transformation based on arithmetic modulo". Systemy upravlinnya, navigatsiyi ta zvyazku. Zbirnyk naukovykh prats, Kyiv, No. 4(24), P. 85–88 [in Ukrainian].

5. *Holub S. V., Babenko V.H. and Rudnytskyi S.V.* (2012). Metod syntezu operatsii kryptohrafichnoho peretvorennia na osnovi dodavannia za modulem dva. "The method of synthesis of cryptographic transformation operations based on addition modulo two". Systemy obrobky informaciyi. Zbirnyk naukovykh prats KHUPS im. I. Kozheduba, Kharkiv, Vol. 1, No. 3(101), P. 119–122 [in Ukrainian].

6. *Lada N.V. and Kozlovska S.H.* (2018). Zastosuvannia operatsii kryptohrafichnoho dodavannia za modulem dva z tochnistiu do perestanovki v potokovykh shyfrakh. "Applying cryptographic addition operations by module two with accuracy of permutation in stream ciphers", Systemy upravlinnia, navihatsii ta zviazku. Zbirnyk naukovykh prats PNTU, Poltava, No. 1(47), P. 127–130 [in Ukrainian].

7. *Kozlovska S.H.* (2018). Syntez hrup dvokhoperandnykh operatsii kryptoperetvorennia na osnovi perestanovliuvanykh skhem. "Synthesis of groups two-operand operations of criptoconversion on the basis of permutation schemes", Suchasna spetsialna tekhnika, Kyiv, No. 4(55), P. 47–56 [in Ukrainian].

8. *Rudnitskyi V.M., Lada N.V. and Kozlovska S.H.* (2018). Tekhnolohiia pobudovy dvokhoperandnykh operatsii kryptohrafichnoho peretvorennia informatsii za rezultatamy modeliuvannia. "Technology of two operand operations construction of information cryptographic transformation by modeling results",

Suchasni informatsiini systemy, Kharkiv, Vol. 2, No. 4, P. 26–30 [in Ukrainian].

9. *Babenko V.H. and Lada N.V.* (2014). Syntez i analiz operatsii kryptohrafichnoho dodavannia za modulem dva. “Synthesis and analysis of operations of cryptographic addition modulo two”, Systemy obrobky informatsii: zbirnyk naukovykh prats KHUPS im. I. Kozheduba, Kharkiv, No. 2(118), P. 116–118 [in Ukrainian].