Increasing the cryptographic strength of CETencryption by ensuring the transformation quality of the information block

Publisher: IEEE

Cite This PDF

Volodymyr Rudnytskyi ; Nataliia Lada ; Maxim Pochebut ; Olga Melnyk ; Yaroslav Tarasenko **All Authors**

Abstract:
The article is devoted to the study of the cryptographic algorithms' correctness, symmetry and quality, as well as to the analysis of ways to increase the cryptographic strength of low-resource cryptographic algorithms based on overcoming the contradiction between the quality of the information blocks transformation and the statistical characteristics of the encryption results. Basing on the formalization of the requirements for the cryptographic algorithm's correctness, the cryptographic algorithms' classification is detailed through the processes of direct and inverse transformation, as well as the keys for direct and inverse transformation of information. The causes of the contradiction appearance between the quality of the information blocks transformation and the statistical characteristics of the encryption results, as well as the ways to overcome it, are described and discussed. The conclusion is made about the expediency of additional XOR ciphering of the key sequence. The possibility of increasing the key of a low-resource cryptographic algorithm due to additional XOR ciphering in the encryption process is demonstrated and discussed. Alternative ways of increasing the cryptographic algorithms' cryptographic strength based on key management are considered.

Published in: 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)