World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:15, No:09, 2021

The Complexity of Testing Cryptographic Devices on Input Faults

Authors : Alisher Ikramov, Gayrat Juraev

Abstract : The production of logic devices faces the occurrence of faults during manufacturing. This work analyses the complexity of testing a special type of logic device on inverse, adhesion, and constant input faults. The focus of this work is on devices that implement cryptographic functions. The complexity values for the general case faults and for some frequently occurring subsets were determined and proved in this work. For a special case, when the length of the text block is equal to the length of the key block, the complexity of testing is proven to be asymptotically half the complexity of testing all logic devices on the same types of input faults.

Keywords : complexity, cryptographic devices, input faults, testing
Conference Title : ICISC 2021 : International Conference on Information Security and Cryptography
Conference Location : Dubai, United Arab Emirates
Conference Dates : September 29-30, 2021