Modified AES for increasing data security and its parallel implementation

ARTAN BERISHA, FATON BERISHA

Department of Mathematics
Faculty of Mathematics and Natural Sciences
University of Prishtina, Prishtinë, Kosovo
artan.berisha@uni-pr.edu, faton.berisha@uni-pr.edu

Secure communication has been longstanding concern of mankind, starting by the Code of Caesar and until today algorithms with symmetric, asymmetric encryption and hash functions to ensure data integrity. We have built an MDS matrix (Maximal Separable Distance) that will be added during the AES algorithm encryption or decryption process. We have modified the AES algorithm to boost its security, which in fact has increased the number of calculations within the algorithm rounds. That the greater number of calculations have no impact on coding or decoding delay at the end we propose the parallel version of this algorithm.