

On the Construction of Lightweight Circulant Maximum Distance Separable Matrices

Authors : Qinyi Mei, Li-Ping Wang

Abstract : MDS matrices are of great significance in the design of block ciphers and hash functions. In the present paper, we investigate the problem of constructing MDS matrices which are both lightweight and low-latency. We propose a new method of constructing lightweight MDS matrices using circulant matrices which can be implemented efficiently in hardware. Furthermore, we provide circulant MDS matrices with as few bit XOR operations as possible for the classical dimensions 4×4 , 8×8 over the space of linear transformations over finite field F_2 . In contrast to previous constructions of MDS matrices, our constructions have achieved fewer XORs.

Keywords : linear diffusion layer, circulant matrix, lightweight, maximum distance separable (MDS) matrix

Conference Title : ICISC 2017 : International Conference on Information Security and Cryptography

Conference Location : Amsterdam, Netherlands

Conference Dates : June 18-19, 2017