Abstract

Maximum distance separable (MDS) matrices are important in cryptography and particularly used in block ciphers due to their properties of diffusion. Rhotrices are represented by the coupled matrices. Therefore, maximum distance separable rhotrices are of much interest in the context of cryptography. In this paper, we define Cauchy rhotrix and then use it to construct MDS rhotrices over finite fields.

References

Construction of Maximum Distance Separable Rhotrices using Cauchy Rhotrices over Finite Fields

Thesis, Ahmadu Bello University, Zaria.


Index Terms

Computer Science

Applied Mathematics

Keywords

Cauchy rhotrix, Finite field, Maximum distance separable rhotrix, Circulant rhotrix, Vandermonde rhotrix.