电子与信息学报 2010 32 (2): 500-503 ISSN: 1009-5896 CN: 11-4494/TN

研究简报

对合Cauchy-Hadamard型MDS矩阵的构造

崔 霆, 金晨辉

信息工程大学电子技术学院 郑州 450004

收稿日期 2009-1-16 修回日期 2009-6-29 网络版发布日期 2010-2-4 接受日期

摘要
MDS矩阵和对合MDS矩阵在分组密码中有广泛应用。该文将考察同时是Hadamard矩阵和Cauchy矩阵的那些MDS矩阵，给出了这类矩阵的结构、构造方法和个数，从而得到了MDS矩阵一种新的构造方法。该文还证明了Cauchy-Hadamard型MDS矩阵都等效于对合的Cauchy-Hadamard型MDS矩阵，并给出了由Cauchy-Hadamard型MDS矩阵构造对合的Cauchy-Hadamard型MDS矩阵的方法。

关键词 分组密码 扩散结构 分支数 MDS矩阵 Cauchy-Hadamard矩阵

分类号 TN918.1

Construction of Involution Cauchy-Hadamard Type MDS Matrices

Cui Ting, Jin Chen-hui

Institution of Electronic Technology, Information Engineering University, Zhengzhou, 450004 China

Abstract
MDS matrices and involution MDS matrices are widely used in block ciphers. This paper deals with those MDS matrices which are Hadamard matrices and Cauchy matrices simultaneously. Then the structure, the method of constructing and the count value of this kind of matrices are presented. By this, a new method for constructing MDS matrices is obtained. Additionally, this paper proves that a Cauchy-Hadamard type MDS matrix can be transformed into an involution Cauchy-Hadamard type MDS, and then proposes a new method to construct an involution Cauchy-Hadamard type MDS matrix from a Cauchy-Hadamard type MDS matrix.

Key words Block cipher Diffusion structure Branch number MDS(Maximum Distance Separable) matrices Cauchy-Hadamard matrices

DOI: 10.3724/SP.J.1146.2009.00070

通讯作者 崔 霆 cuiting_1209@yahoo.com.cn

作者个人主页 崔 霆; 金晨辉