Des. Codes Cryptogr. (2012) 64:287–308
DOI 10.1007/s10623-011-9578-x

On construction of involutory MDS matrices from Vandermonde Matrices in $GF(2^q)$

Mahdi Sajadieh · Mohammad Dakhilalian · Hamid Mala · Behnaz Omoomi

Received: 22 October 2010 / Revised: 1 October 2011 / Accepted: 4 October 2011 /
Published online: 12 November 2011

Abstract Due to their remarkable application in many branches of applied mathematics such as combinatorics, coding theory, and cryptography, Vandermonde matrices have received a great amount of attention. Maximum distance separable (MDS) codes introduce MDS matrices which not only have applications in coding theory but also are of great importance in the design of block ciphers. Lacan and Fimes introduce a method for the construction of an MDS matrix from two Vandermonde matrices in the finite field. In this paper, we first suggest a method that makes an involutory MDS matrix from the Vandermonde matrices. Then we propose another method for the construction of $2^n \times 2^n$ Hadamard MDS matrices in the finite field $GF(2^q)$. In addition to introducing this method, we present a direct method for the inversion of a special class of $2^n \times 2^n$ Vandermonde matrices.

Keywords MDS matrix · Vandermonde matrix · Hadamard matrix · Blockcipher

Mathematics Subject Classification (2000) 11T71 · 14G50 · 51E22 · 94B05 · 20H30 · 15A09

Communicated by J. Jedwab.

M. Sajadieh (✉) · M. Dakhilalian
Cryptography & System Security Research Laboratory, Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran
e-mail: sadjadieh@ec.iut.ac.ir

M. Dakhilalian
e-mail: mdalian@cc.iut.ac.ir

H. Mala
Department of Information Technology Engineering, University of Isfahan, Isfahan, Iran
e-mail: h.mala@eng.ui.ac.ir

B. Omoomi
Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, Iran
e-mail: bomoomi@cc.iut.ac.ir