Des. Codes Cryptogr.
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

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

Published online: 12 November 2011

1 Introduction

Definition 1 A Vandermonde matrix $\mathbf{A} = van_d(a_0, a_1, \ldots, a_{m-1})$ is an $m \times d$ matrix built from $a_0, a_1, \ldots, a_{m-1}$ as below:

$$\mathbf{A} = van_d(a_0, a_1, \ldots, a_{m-1}) = \begin{pmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{d-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{d-1} \\ \vdots & & \ddots & & \\ 1 & a_{m-1} & a_{m-1}^2 & \cdots & a_{m-1}^{d-1} \end{pmatrix} \tag{1}$$

In this paper we focus on square Vandermonde matrices with elements in $GF(2^q)$. We represent a square Vandermonde matrix by $van(a_0, a_1, \ldots, a_{m-1})$ whose elements are all different (i.e. $i \neq j$ implies $a_i \neq a_j$). These matrices have remarkable applications in BCH and Reed Solomon codes in coding theory [10], and they can be used to generate MDS (maximum distance separable) matrices for cryptographic applications [9]. In the following, we emphasize the cryptographic application of Vandermonde matrices.

1.1 Previous works on the relation of Vandermonde and MDS matrices

We first will summarize the established theorems and results that are significant in the relation between Vandermonde and MDS matrices.

Theorem 1 ([8,14]) *A matrix $\mathbf{M}_{n\times n}$ is an MDS matrix if and only if every sub-matrix of $\mathbf{M}$ is non-singular. Also we can say $\mathbf{M}_{n\times n}$ is MDS if and only if:*

$$\mathbf{Y}_{n\times 1} = \mathbf{M}_{n\times n} \cdot \mathbf{X}_{n\times 1} \Longrightarrow \min_{\mathbf{X}\neq \mathbf{0}}(W(\mathbf{Y}) + W(\mathbf{X})) = n + 1$$

where $\mathbf{X} = [x_0, x_1, \ldots, x_{n-1}]^T$ and $\mathbf{Y} = [y_0, y_1, \ldots, y_{n-1}]^T$ are vectors in the finite field $GF(2^q)$ and $W(\mathbf{X})$ is the number of non-zero elements of $\mathbf{X}$.

Theorem 2 ([9]) *Let $\mathbf{A} = van(a_0, a_1, \ldots, a_{m-1})$ and $\mathbf{B} = van(b_0, b_1, \ldots, b_{m-1})$ be two Vandermonde matrices with different elements ($a_i \neq b_j$), then the matrix $\mathbf{AB}^{-1}$ is an MDS matrix.*

Proof Assume $\mathbf{Y}_{m\times 1} = \mathbf{AB}^{-1}\mathbf{X}_{m\times 1}$. A new vector $\mathbf{P}_{m\times 1} = [p_0, p_1, \ldots, p_{m-1}]^T$ is defined as $\mathbf{P} = \mathbf{B}^{-1}\mathbf{X}$. Then from $\mathbf{X} = \mathbf{BP}$ and $\mathbf{Y} = \mathbf{AP}$, we can represent x_i and y_i by p_i as below:

$$\begin{aligned} x_0 &= \sum_{i=0}^{m-1} b_0^i p_i, \quad & x_1 &= \sum_{i=0}^{m-1} b_1^i p_i, \quad & \ldots, \quad & x_{m-1} = \sum_{i=0}^{m-1} b_{m-1}^i p_i \\ y_0 &= \sum_{i=0}^{m-1} a_0^i p_i, \quad & y_1 &= \sum_{i=0}^{m-1} a_1^i p_i, \quad & \ldots, \quad & y_{m-1} = \sum_{i=0}^{m-1} a_{m-1}^i p_i \end{aligned} \tag{2}$$

The $2m$ values of x_i and y_i $(i = 0, 1, \ldots, m-1)$ are all of the form $\sum_{i=0}^{m-1} p_i t^i$. The equation $\sum_{i=0}^{m-1} p_i t^i = 0$ has at most $m - 1$ different roots in the finite field $GF(2^q)$. Since a_i's and b_j's are all different, at most $m - 1$ out of the $2m$ values of x_i's and y_i's might be zero. Therefore, at least $m + 1$ of x_i's and y_i's are non-zero and $\mathbf{AB}^{-1}$ is an MDS matrix. $\square$

1.2 Related work and our contribution

The main application of MDS matrices to the field of cryptography is in the design diffusion layers of block ciphers because these matrices can provide maximum diffusion. By using good non-linear parts and MDS matrices, one can design block ciphers and hash functions that have a provable security against differential cryptanalysis (DC) [2] and linear cryptanalysis (LC) [12]. Many block ciphers such as AES [5], Khazad [4], Clefia [15], and AES-MDS [13] as well as some hash functions such as Maelstrom [6] and Grøstl [7] use MDS matrices as the main part of their diffusion layers. To design MDS matrices, several methods have been proposed thus far. For small MDS matrices, an exhaustive search may be a useful method, but for large linear MDS matrices, most designers prefer one of the following two approaches:

- Construction of MDS matrices from Cauchy matrices [17].
- Construction of MDS matrices from Vandermonde matrices [9].

Definition 2 An involutory matrix $\mathbf{M}_{m\times m}$ is a matrix satisfying the property of $\mathbf{M}^2_{m\times m} = \mathbf{I}_{m\times m}$. Also a function f is an involutory function if $f(f(x)) = x$.

The design of involutory diffusion transformations is an interesting direction in the design of block ciphers. These transformations can make the decryption process the same as the encryption process. Thus the encryption and decryption can be implemented by the same module and equal speeds.

In this paper, we propose a new approach based on Vandermonde matrices to design involutory MDS matrices over the finite fields $GF(2^q)$. This approach helps us design involutory MDS matrices of arbitrary size. When the size of the involutory matrix is $2^n \times 2^n$, we add the property of a Hadamard matrix to the resulting MDS matrix. This property improves the implementation of a block cipher that uses such a matrix as its diffusion layer. Moreover, we introduce a special class of $2^n \times 2^n$ Vandermonde matrices (called Special Vandermonde matrices or SV matrices), such that their inverses can be directly calculated.

The notations used in this paper are:

$\lfloor x \rfloor$	:	floor of x,
$\mathbf{A}_{col(i)}$	:	ith column of an $m\times m$ matrix $\mathbf{A}$, $0 \le i \le m-1$,
$\mathbf{A}_{row(j)}$	:	jth row of an $m\times m$ matrix $\mathbf{A}$, $0 \le j \le m-1$,
$d_{i,j}$ in matrix $\mathbf{D}_{m\times m}$	:	the element located in row i and column j of an $m\times m$ matrix $\mathbf{D}$, where $0 \le i, j \le m-1$,
$a+b$ and $\sum_{i=0}^{m-1} a_i^k$	:	sum in $GF(2^q)$ for elements of matrix (for example $2+3=1$),
$\oplus$ in $a_{r1\oplus r2}$	:	bit-wise XOR (used for subscripts),
$HW(x)$	:	number of ones in the binary representation of x or Hamming weight of x (for example the binary representation of 13 is 1101 and $HW(13)=3$),
$a^{r_1+r_2}$	:	sum for exponents in natural number (for example $a^{2+3}=a^5$).
$0x$	:	hexadecimal representation.

Also two important arithmetic properties of the finite field $GF(2^q)$ which are applied in the proof of some theorems are:

$$(a+b)^{2^n} = a^{2^n} + b^{2^n}$$

$$a+b=c \Leftrightarrow a+c=b$$

We mention that in this paper, the notation used for elements of $GF(2^q)$ is the binary representation, and the binary vector is represented by the number whose binary representation is equal to this binary vector. In this representation, $\oplus$ and $+$ are the same, but we use them to distinguish subscripts and elements of $GF(2^q)$, respectively.

This paper proceeds as follows. In Sect. 2, we introduce a method for constructing an involutory MDS matrix from two Vandermonde matrices and discuss the requirements of these two Vandermonde matrices. Section 3 discusses the conditions on the two Vandermonde matrices, that can generate a Hadamard-type $2^n \times 2^n$ involutory MDS matrix. In addition, we show that the inverse of this class of Vandermonde matrices is directly obtained. In Sect. 4, we compare this method with the previous method of [16,17]. Finally, we conclude the paper in Sect. 5.

2 Constructing involutory MDS matrices from Vandermonde matrices

In this section, we show that for two $m \times m$ Vandermonde matrices $\mathbf{A}=van(a_0, a_1, \ldots, a_{m-1})$ and $\mathbf{B} = van(b_0, b_1, \ldots, b_{m-1}) = van(a_0 + \Delta, a_1 + \Delta, \ldots, a_{m-1} + \Delta)$, where Δ is an arbitrary non-zero number in $GF(2^q)$, the matrices $\mathbf{AB}^{-1}$ and $\mathbf{BA}^{-1}$ are involutory. Furthermore, if a_i's and b_i's are $2m$ different values, then $\mathbf{AB}^{-1}$ and $\mathbf{BA}^{-1}$ will be involutory MDS matrices.

Assume $b_i = a_i + \Delta$. The relations between powers of a_i and b_i in the finite field $GF(2^q)$ are:

$$b_i^l = (a_i + \Delta)^l = c_{l,0}a_i^l + c_{l,1}a_i^{l-1}\Delta + \cdots + c_{l,l-1}a_i\Delta^{l-1} + c_{l,l}\Delta^l \ ; \ c_{l,i} \in \{0, 1\} \quad (3)$$

where $c_{l,0} = c_{l,l} = 1$ and $c_{l,m} = 0,\ m > l$.

Theorem 3 *Assume $\mathbf{A} = van(a_0, a_1, \ldots, a_{m-1})$ and $\mathbf{B} = van(b_0, b_1, \ldots, b_{m-1})$ are two invertible Vandermonde matrices such that $b_i = a_i + \Delta$. Then $\mathbf{A}^{-1}\mathbf{B}$ is an upper triangular matrix whose non-zero elements are determined by powers of Δ.*

Proof Assume the inverse of $\mathbf{A}$ is:

$$\mathbf{A}^{-1} = \begin{pmatrix} t_{0,0} & t_{0,1} & t_{0,2} & \cdots & t_{0,m-1} \\ t_{1,0} & t_{1,1} & t_{1,2} & \cdots & t_{1,m-1} \\ \vdots & & & & \\ t_{m-1,0} & t_{m-1,1} & t_{m-1,2} & \cdots & t_{m-1,m-1} \end{pmatrix}.$$

Let us first extract some properties of $t_{i,j}$'s from the relation $\mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_{m\times m}$, and then exploit them to compute $\mathbf{A}^{-1}\mathbf{B}$. By multiplying $\mathbf{A}^{-1}_{row(0)}$ to columns of $\mathbf{A}$, we have:

$$\mathbf{A}^{-1}_{row(0)} \cdot \mathbf{A}_{col(0)} = t_{0,0} + t_{0,1} + t_{0,2} + \cdots + t_{0,m-1} = \sum_{i=0}^{m-1} t_{0,i} = 1 \quad (4)$$

$$\begin{aligned}\mathbf{A}^{-1}_{row(0)} \cdot \mathbf{A}_{col(k)} &= t_{0,0}a_0^k + t_{0,1}a_1^k + t_{0,2}a_2^k + \cdots + t_{0,m-1}a_{m-1}^k \\ &= \sum_{i=0}^{m-1} t_{0,i}a_i^k = 0 \ \ (1 \le k \le m-1) \end{aligned} \quad (5)$$

Also by multiplying $\mathbf{A}^{-1}_{row(0)}$ in column k of $\mathbf{B}$, and using the two results (4) and (5), we can compute the first row of $\mathbf{A}^{-1}\mathbf{B}$:

$$\mathbf{A}^{-1}_{row(0)} \cdot \mathbf{B}_{col(k)} = t_{0,0}b_0^k + t_{0,1}b_1^k + t_{0,2}b_2^k + \cdots + t_{0,m-1}b_{m-1}^k = \sum_{i=0}^{m-1} t_{0,i}(a_i + \Delta)^k.$$

by extending $b_i^k = (a_i + \Delta)^k$ from (3):

$$\sum_{i=0}^{m-1}(t_{0,i}a_i^k) + c_{k,1}\sum_{i=0}^{m-1}(t_{0,i}a_i^{k-1})\Delta + \cdots + c_{k,k-1}\sum_{i=0}^{m-1}(t_{0,i}a_i)\Delta^{k-1} + \sum_{i=0}^{m-1}(t_{0,i})\Delta^k = \Delta^k.$$

If we multiply $\mathbf{A}^{-1}_{row(1)}$ to columns of $\mathbf{A}$, new results are obtained:

$$\mathbf{A}^{-1}_{row(1)} \cdot \mathbf{A}_{col(0)} = t_{1,0} + t_{1,1} + t_{1,2} + \cdots + t_{1,m-1} = \sum_{i=0}^{m-1} t_{1,i} = 0,$$

$$\mathbf{A}^{-1}_{row(1)} \cdot \mathbf{A}_{col(1)} = t_{1,0}a_0 + t_{1,1}a_1 + t_{1,2}a_2 + \cdots + t_{1,m-1}a_{m-1} = \sum_{i=0}^{m-1} t_{1,i}a_i = 1 \quad \text{and}$$

$$\begin{aligned}\mathbf{A}^{-1}_{row(1)} \cdot \mathbf{A}_{col(k)} &= t_{1,0}a_0^k + t_{1,1}a_1^k + t_{1,2}a_2^k + \cdots + t_{1,m-1}a_{m-1}^k \\ &= \sum_{i=0}^{m-1} t_{1,i}a_i^k = 0 \ \ (2 \le k \le m-1).\end{aligned}$$

If this procedure proceeds by multiplying $\mathbf{A}^{-1}_{row(1)}$ to column k of $\mathbf{B}$, we obtain:

$$\begin{aligned}&\mathbf{A}^{-1}_{row(1)} \cdot \mathbf{B}_{col(k)} = \sum_{i=0}^{m-1} t_{1,i}b_i^k = \sum_{i=0}^{m-1} t_{1,i}(a_i + \Delta)^k = \\ &\sum_{i=0}^{m-1}(t_{1,i}a_i^k) + c_{k,1}\sum_{i=0}^{m-1}(t_{1,i}a_i^{k-1})\Delta + \cdots + c_{k,k-1}\sum_{i=0}^{m-1}(t_{1,i}a_i)\Delta^{k-1} \\ &\quad + \sum_{i=0}^{m-1}(t_{1,i})\Delta^k = c_{k,k-1}\Delta^{k-1}.\end{aligned}$$

By following this method to multiply the other rows of $\mathbf{A}^{-1}$ to the columns of $\mathbf{A}$ and $\mathbf{B}$, one can easily obtain:

$$\mathbf{A}^{-1}\mathbf{B} = \begin{pmatrix} 1 & \Delta & \Delta^2 & \Delta^3 & \cdots & \Delta^{m-2} & \Delta^{m-1} \\ 0 & 1 & c_{2,1}\Delta & c_{3,2}\Delta^2 & \cdots & c_{m-2,m-3}\Delta^{m-3} & c_{m-1,m-2}\Delta^{m-2} \\ 0 & 0 & 1 & c_{3,1}\Delta & \cdots & c_{m-2,m-4}\Delta^{m-4} & c_{m-1,m-3}\Delta^{m-3} \\ \vdots & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & 1 & c_{m-1,1}\Delta \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \tag{6}$$

Thus $\mathbf{A}^{-1}\mathbf{B}$ is an upper triangular matrix. □

Theorem 4 *Let* $\mathbf{A} = van(a_0, a_1, \ldots, a_{m-1})$ *and* $\mathbf{B} = van(b_0, b_1, \ldots, b_{m-1})$ *be two Vandermonde matrices where* $a_i = b_i + \Delta$, *then* $\mathbf{BA}^{-1}\mathbf{B} = \mathbf{A}$.

Proof By replacing $\mathbf{A}^{-1}\mathbf{B}$ from (6) into $\mathbf{BA}^{-1}\mathbf{B}$, we have:

$$\mathbf{BA}^{-1}\mathbf{B} = \begin{pmatrix} 1 & b_0 & b_0^2 & \cdots & b_0^{m-1} \\ 1 & b_1 & b_1^2 & \cdots & b_1^{m-1} \\ 1 & b_2 & b_2^2 & \cdots & b_2^{m-1} \\ \vdots & & \ddots & & \\ 1 & b_{m-1} & b_{m-1}^2 & \cdots & b_{m-1}^{m-1} \end{pmatrix} \times \begin{pmatrix} 1 & \Delta & \Delta^2 & \Delta^3 & \cdots & \Delta^{m-2} & \Delta^{m-1} \\ 0 & 1 & c_{2,1}\Delta & c_{3,2}\Delta^2 & \cdots & c_{m-2,m-3}\Delta^{m-3} & c_{m-1,m-2}\Delta^{m-2} \\ 0 & 0 & 1 & c_{3,1}\Delta & \cdots & c_{m-2,m-4}\Delta^{m-4} & c_{m-1,m-3}\Delta^{m-3} \\ \vdots & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \cdots & 1 & c_{m-1,1}\Delta \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

By multiplying row i to row j, we have:

$$\Delta^j + c_{j,j-1}\Delta^{j-1}b_i + \cdots + c_{j,1}\Delta b_i^{j-1} + b_i^j = (b_i + \Delta)^j = a_i^j.$$

Thus $\mathbf{BA}^{-1}\mathbf{B} = \mathbf{A}$ or $\mathbf{BA}^{-1}\mathbf{BA}^{-1} = \mathbf{I}$. □

Corollary 1 *If* $\mathbf{A}$ *and* $\mathbf{B}$ *are two invertible Vandermonde matrices in the finite field* $GF(2^q)$ *satisfying the two properties* $a_i = b_i + \Delta$ *and* $a_i \neq b_j, i, j \in \{0, 1, .., m-1\}$, *then* $\mathbf{BA}^{-1}$ *is an involutory MDS matrix.*

3 Finite Field Hadamard involutory $2^n \times 2^n$ MDS matrices

In this section, we restrict the conditions of Sect. 2 and construct some involutory MDS matrices which are also Hadamard in the finite field $GF(2^q)$. First, we obtain the required conditions for 4×4 matrices, then conditions are extended for other $2^n \times 2^n$ matrices.

Definition 3 A $2^n \times 2^n$ matrix $\mathbf{H}$ is a Finite Field Hadamard (FFHadamard) matrix in $GF(2^q)$ if it can be represented as follows:

$$\mathbf{H} = \begin{pmatrix} \mathbf{U} & \mathbf{V} \\ \mathbf{V} & \mathbf{U} \end{pmatrix}$$

and the two sub-matrices $\mathbf{U}$ and $\mathbf{V}$ are FFHadamard [3].

We can easily see that each two rows of this matrix are orthogonal in $GF(2^q)$. For example a 4×4 FFHadamard matrix is:

$$\mathbf{H} = had(a_0, a_1, a_2, a_3) = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix}$$

which implies $h_{i,j} = a_{i \oplus j}$.

3.1 Construction of 4×4 FFHadamard MDS matrices

In the following, by defining some conditions, inverse of 4×4 Vandermonde matrices are directly calculated. A 4×4 Vandermonde matrix is as below:

$$\mathbf{A} = \begin{pmatrix} 1 & a_0 & a_0^2 & a_0^3 \\ 1 & a_1 & a_1^2 & a_1^3 \\ 1 & a_2 & a_2^2 & a_2^3 \\ 1 & a_3 & a_3^2 & a_3^3 \end{pmatrix}$$

Assume $a_0 + a_1 = a_2 + a_3$ and $a_0 + a_2 = a_1 + a_3$ (these two equations are equivalent to $a_0+a_1+a_2+a_3 = 0$). Based on the finite field arithmetic in $GF(2^q)$, if $a_0+a_1+a_2+a_3 = 0$ then $a_0^2 + a_1^2 + a_2^2 + a_3^2 = 0$ and $a_0^4 + a_1^4 + a_2^4 + a_3^4 = 0$. We hypothesized the matrix $\mathbf{A1}$, defined below, is very close to $\mathbf{A}^{-1}$.

$$\mathbf{A1} = \begin{pmatrix} a_0^3 & a_1^3 & a_2^3 & a_3^3 \\ a_0^2 & a_1^2 & a_2^2 & a_3^2 \\ a_0 & a_1 & a_2 & a_3 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

At first, we calculate $\mathbf{A1} \times \mathbf{A}$ with the condition $a_0 + a_1 + a_2 + a_3 = 0$:

$$\mathbf{A1} \times \mathbf{A} = \begin{pmatrix} a_0^3 & a_1^3 & a_2^3 & a_3^3 \\ a_0^2 & a_1^2 & a_2^2 & a_3^2 \\ a_0 & a_1 & a_2 & a_3 \\ 1 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & a_0 & a_0^2 & a_0^3 \\ 1 & a_1 & a_1^2 & a_1^3 \\ 1 & a_2 & a_2^2 & a_2^3 \\ 1 & a_3 & a_3^2 & a_3^3 \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^{3} a_i^3 & 0 & \sum_{i=0}^{3} a_i^5 & \sum_{i=0}^{3} a_i^6 \\ 0 & \sum_{i=0}^{3} a_i^3 & 0 & \sum_{i=0}^{3} a_i^5 \\ 0 & 0 & \sum_{i=0}^{3} a_i^3 & 0 \\ 0 & 0 & 0 & \sum_{i=0}^{3} a_i^3 \end{pmatrix}.$$

$\mathbf{A1} \times \mathbf{A}$ is close to a diagonal matrix. To find the inverse of $\mathbf{A}$, we must modify $\mathbf{A1}$, such that $\mathbf{A1} \times \mathbf{A}$ becomes a diagonal matrix. Assume $\mathbf{A2}$ is a modified form of $\mathbf{A1}$ as below:

$$\mathbf{A2} = \begin{pmatrix} a_0^3 + s_0 a_0 + s_1 & a_1^3 + s_0 a_1 + s_1 & a_2^3 + s_0 a_2 + s_1 & a_3^3 + s_0 a_3 + s_1 \\ a_0^2 + s_0 & a_1^2 + s_0 & a_2^2 + s_0 & a_3^2 + s_0 \\ a_0 & a_1 & a_2 & a_3 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

By computing $\mathbf{A2} \times \mathbf{A}$, we have:

$$\mathbf{A2} \times \mathbf{A} = \begin{pmatrix} a_0^3 + s_0 a_0 + s_1 & a_1^3 + s_0 a_1 + s_1 & a_2^3 + s_0 a_2 + s_1 & a_3^3 + s_0 a_3 + s_1 \\ a_0^2 + s_0 & a_1^2 + s_0 & a_2^2 + s_0 & a_3^2 + s_0 \\ a_0 & a_1 & a_2 & a_3 \\ 1 & 1 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & a_0 & a_0^2 & a_0^3 \\ 1 & a_1 & a_1^2 & a_1^3 \\ 1 & a_2 & a_2^2 & a_2^3 \\ 1 & a_3 & a_3^2 & a_3^3 \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{i=0}^{3} a_i^3 & 0 & \sum_{i=0}^{3} a_i^5 + s_0 \sum_{i=0}^{3} a_i^3 & \sum_{i=0}^{3} a_i^6 + s_1 \sum_{i=0}^{3} a_i^3 \\ 0 & \sum_{i=0}^{3} a_i^3 & 0 & \sum_{i=0}^{3} a_i^5 + s_0 \sum_{i=0}^{3} a_i^3 \\ 0 & 0 & \sum_{i=0}^{3} a_i^3 & 0 \\ 0 & 0 & 0 & \sum_{i=0}^{3} a_i^3 \end{pmatrix}.$$

To make $\mathbf{A}2 \times \mathbf{A}$ a diagonal matrix, $\sum_{i=0}^{3} a_i^5 + s_0 \sum_{i=0}^{3} a_i^3$ and $\sum_{i=0}^{3} a_i^6 + s_1 \sum_{i=0}^{3} a_i^3$ must be zero. Thus:

$$s_0 = \frac{\sum_{i=0}^{3} a_i^5}{\sum_{i=0}^{3} a_i^3} \qquad \text{and} \qquad s_1 = \frac{\sum_{i=0}^{3} a_i^6}{\sum_{i=0}^{3} a_i^3} = \sum_{i=0}^{3} a_i^3 \tag{7}$$

by these s_0 and s_1, the inverse of matrix $\mathbf{A}$ is:

$$\mathbf{A}^{-1} = \left(\sum_{i=0}^{3} a_i^3\right)^{-1} \mathbf{A}2. \tag{8}$$

Now assume $\mathbf{B}$ is another 4×4 Vandermonde matrix. By multiplying $\mathbf{B}$ and $\mathbf{A}^{-1}$, we have:

$$\mathbf{D} = \mathbf{B} \times \mathbf{A}^{-1} = \begin{pmatrix} 1 & b_0 & b_0^2 & b_0^3 \\ 1 & b_1 & b_1^2 & b_1^3 \\ 1 & b_2 & b_2^2 & b_2^3 \\ 1 & b_3 & b_3^2 & b_3^3 \end{pmatrix}$$
$$\times \left(\sum_{i=0}^{3} a_i^3\right)^{-1} \begin{pmatrix} a_0^3 + s_0 a_0 + s_1 & a_1^3 + s_0 a_1 + s_1 & a_2^3 + s_0 a_2 + s_1 & a_3^3 + s_0 a_3 + s_1 \\ a_0^2 + s_0 & a_1^2 + s_0 & a_2^2 + s_0 & a_3^2 + s_0 \\ a_0 & a_1 & a_2 & a_3 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

We are interested in the conditions on $\mathbf{A}$ and $\mathbf{B}$ that make $\mathbf{D} = \mathbf{B} \times \mathbf{A}^{-1}$ an FFHadamard matrix. To obtain these conditions, we investigate only two sub-cases and by considering the conditions of these two sub-cases, other conditions are deduced.

sub-case 1: $d_{0,0} = d_{3,3}$

$$\begin{aligned} \left(\sum_{i=0}^{3} a_i^3\right) d_{0,0} &= (a_0^3 + a_0^2 b_0 + a_0 b_0^2 + b_0^3) + s_0(a_0 + b_0) + s_1 \\ &= (a_0 + b_0)^3 + s_0(a_0 + b_0) + s_1 \quad \text{and} \\ \left(\sum_{i=0}^{3} a_i^3\right) d_{3,3} &= (a_3^3 + a_3^2 b_3 + a_3 b_3^2 + b_3^3) + s_0(a_3 + b_3) + s_1 \\ &= (a_3 + b_3)^3 + s_0(a_3 + b_3) + s_1 \end{aligned}$$

when $(a_3 + b_3) = (a_0 + b_0)$, then $d_{0,0} = d_{3,3}$.

sub-case 2: $d_{1,0} = d_{2,3}$

$$\begin{aligned} \left(\sum_{i=0}^{3} a_i^3\right) d_{1,0} &= (a_0^3 + a_0^2 b_1 + a_0 b_1^2 + b_1^3) + s_0(a_0 + b_1) + s_1 \\ &= (a_0 + b_1)^3 + s_0(a_0 + b_1) + s_1 \quad \text{and} \\ \left(\sum_{i=0}^{3} a_i^3\right) d_{2,3} &= (a_3^3 + a_3^2 b_2 + a_3 b_2^2 + b_2^3) + s_0(a_3 + b_2) + s_1 \\ &= (a_3 + b_2)^3 + s_0(a_3 + b_2) + s_1 \end{aligned}$$

when $(a_3 + b_2) = (a_0 + b_1)$, then $d_{1,0} = d_{2,3}$. By checking the other sub-cases, one can easily see that the matrix $\mathbf{BA}^{-1}$ is FFHadamard if $a_i + b_j = a_l + b_{l \oplus i \oplus j}$ $(i, j, l \in \{0, 1, 2, 3\})$.

Corollary 2 *The condition $a_i + b_j = a_l + b_{l \oplus i \oplus j}$ for all $i, j, l \in \{0, 1, 2, 3\}$ implies that $a_i + b_i = a_0 + b_0 = \Delta$ where Δ is an arbitrary non-zero number in $GF(2^q)$. Thus the condition of Theorem 4 (i.e., $b_i = a_i + \Delta$) is satisfied and consequently $\mathbf{BA}^{-1}$ is involutory. Furthermore, by considering Theorem 2, if a_i and b_j in the two matrices $\mathbf{A}$ and $\mathbf{B}$ are all different, then the matrix $\mathbf{BA}^{-1}$ will be an FFHadamard involutory MDS matrix.*

To see that a 4×4 matrix generated from the two 4×4 Vandermonde matrices $\mathbf{A} = van(a_0, a_1, a_2, a_3)$ and $\mathbf{B} = van(b_0, b_1, b_2, b_3)$ is an FFHadamard involutory MDS matrix, the elements a_i and b_j must all be different and chosen such that:

$$\begin{gathered} a_0 + a_1 + a_2 + a_3 = 0 \quad (a_0 + a_1 = a_2 + a_3, a_0 + a_2 = a_1 + a_3) \text{ and} \\ a_i + b_j = a_l + b_{l \oplus i \oplus j} \quad i, j, l \in \{0, 1, 2, 3\} \end{gathered} \tag{9}$$

3.2 Extending the result for $2^n \times 2^n$ matrices

The approach is similar to the case of 4×4 matrices. A $2^n \times 2^n$ matrix $\mathbf{A}1$ is constructed from $\mathbf{A}$, and then is multiplied to $\mathbf{A}$. In $\mathbf{A}1 \times \mathbf{A}$ we should determine which elements $\sum_{i=0}^{2^n-1} a_i^k,\ k \in \{0, 1, \ldots, 2^{n+1} - 2\}$ are zero and which are not zero.

$$\mathbf{A}1_{col(j)} = \begin{pmatrix} a_j^{2^n-1} \\ \vdots \\ a_j^2 \\ a_j \\ 1 \end{pmatrix}, \quad \mathbf{A}1 \times \mathbf{A} = \begin{pmatrix} \sum_{i=0}^{2^n-1} a_i^{2^n-1} & \sum_{i=0}^{2^n-1} a_i^{2^n} & \cdots & \sum_{i=0}^{2^n-1} a_i^{2^{n+1}-2} \\ \sum_{i=0}^{2^n-1} a_i^{2^n-2} & \sum_{i=0}^{2^n-1} a_i^{2^n-1} & \cdots & \sum_{i=0}^{2^n-1} a_i^{2^{n+1}-3} \\ \vdots & & \ddots & \vdots \\ \sum_{i=0}^{2^n-1} a_i^0 & \sum_{i=0}^{2^n-1} a_i & \cdots & \sum_{i=0}^{2^n-1} a_i^{2^n-1} \end{pmatrix} \tag{10}$$

In (10), we must calculate $\sum_{i=0}^{2^n-1} a_i^j,\ j \in \{0, 1, \ldots, 2^{n+1} - 2\}$. If conditions are obtained that make a number of non-diagonal elements of $\mathbf{A1} \times \mathbf{A}$ zero, then we can use some extra variables and modify $\mathbf{A}1$ to find the inverse of $\mathbf{A}$ similar to what done in Sect. 3.1. Before getting through this procedure, we must define some definitions and lemmas.

Definition 4 Let $\mathbf{A} = van(a_0, a_1, \ldots, a_{2^n-1})$. This matrix is called a Special Vandermonde matrix (SV matrix) if a_i's satisfy the following condition:

$$a_i + a_{i \oplus 2^k} = R_k, \quad \text{for all } k \in \{0, 1, \ldots, n-1\} \tag{11}$$

where R_k's are different non-zero constants such that for $\mu_i \in \{0, 1\}$

$$\sum_{i=0}^{n-1} \mu_i R_i = 0 \Rightarrow \mu_i = 0, \quad \text{for all } i \in \{0, 1, \ldots, n-1\} \tag{12}$$

For some j, (11) causes $\sum_{i=0}^{2^n-1} a_i^j$ to become zero and (12) guarantees the invertibility of matrix $\mathbf{A}$. We easily observe that all a_i's are constructed form a_0, R_0, R_1, …and R_{n-1}.

Example 1 $\mathbf{C1} = van(0x1, 0x2, 0x3, 0x4)$ is not an SV matrix because $a_0 + a_1 = 0x3$, but $a_2 + a_3 = 0x7$ and consequently $a_0 + a_{0 \oplus 2^0} \neq a_2 + a_{2 \oplus 2^0}$, so (11) is not satisfied.

Also **C2** $= van(0x4, 0x5, 0x6, 0x7, 0x7, 0x6, 0x5, 0x4)$ is not an SV matrix. However **C2** satisfies (11) ($R_0 = 0x1$, $R_1 = 0x2$, $R_2 = 0x3$) but $R_0 + R_1 + R_2 = 0$ and (12) is not satisfied. **C3** $= van(0x4, 0x5, 0x6, 0x7, 0xd, 0xc, 0xf, 0xe)$ is an SV matrix. ($a_0 = 0x4$, $R_0 = 0x1$, $R_1 = 0x2$, $R_2 = 0x9$)

Lemma 1 *If* $\mathbf{A} = van(a_0, a_1, \ldots, a_{2^n-1})$ *is an SV matrix, then* $\sum_{j=0}^{3} a_{j\oplus i} = 0$, *and the values* $\sum_{j=0}^{3} a_{j\oplus i}^3$ *and* $\sum_{j=0}^{3} a_{j\oplus i}^5$ *depend only on* R_i *and are independent of* a_i.

Proof

$$\sum_{j=0}^{3} a_{j\oplus i} = a_i + a_{i\oplus 1} + a_{i\oplus 2} + a_{i\oplus 3} = (a_i + a_{i\oplus 2^0}) + (a_{i\oplus 2} + a_{(i\oplus 2)\oplus 2^0}) = R_0 + R_0 = 0$$

$$\begin{aligned}
\sum_{j=0}^{3} a_{j\oplus i}^3 &= a_i^3 + a_{i\oplus 1}^3 + a_{i\oplus 2}^3 + a_{i\oplus 3}^3 \\
&= (a_i + a_{i\oplus 1})^3 + a_i a_{i\oplus 1}(a_i + a_{i\oplus 1}) + (a_{i\oplus 2} + a_{i\oplus 3})^3 \\
&\quad + a_{i\oplus 2} a_{i\oplus 3}(a_{i\oplus 2} + a_{i\oplus 3}) \\
&= R_0^3 + R_0(a_i a_{i\oplus 1}) + R_0^3 + R_0(a_{i\oplus 2} a_{i\oplus 3}) \\
&= R_0(a_i a_{i\oplus 1} + (a_i + R_1)(a_{i\oplus 1} + R_1)) = R_0 R_1 (R_0 + R_1).
\end{aligned}$$

We can proceed with this procedure to prove $\sum_{j=0}^{3} a_{j\oplus i}^5$ is a constant equal to $R_1 R_0 (R_0 + R_1)(R_0^2 + R_0 R_1 + R_1^2)$.

Moreover, one can easily see that $\sum_{j=0}^{7} a_{j\oplus i}^3 = 0$ because

$$\sum_{j=0}^{7} a_{j\oplus i}^3 = \sum_{j=0}^{3} a_{j\oplus i}^3 + \sum_{j=0}^{3} a_{j\oplus(i\oplus 4)}^3 = R_0 R_1 (R_0 + R_1) + R_0 R_1 (R_0 + R_1) = 0.$$

Corollary 3 *By considering Lemma 1, we can conclude that in Eq. 7:*

$$\begin{aligned}
s_0 &= \frac{\sum_{i=0}^{3} a_i^5}{\sum_{i=0}^{3} a_i^3} = \frac{R_1 R_0 (R_0 + R_1)(R_0^2 + R_0 R_1 + R_1^2)}{R_0 R_1 (R_0 + R_1)} = (R_0^2 + R_0 R_1 + R_1^2) \text{ and} \\
s_1 &= \frac{\sum_{i=0}^{3} a_i^6}{\sum_{i=0}^{3} a_i^3} = \sum_{i=0}^{3} a_i^3 = R_0 R_1 (R_0 + R_1).
\end{aligned}$$

Definition 5 Let the $\mathbf{A} = van(a_0, a_1, \ldots, a_{2^n-1})$ be an SV matrix. For each a_i $(0 \le i \le 2^{n-1} - 1)$, we define $\tilde{a}_i$ as below:

$$\tilde{a}_i = a_i a_{i\oplus 2^{n-1}} = a_i^2 + R_{n-1} a_i, \quad i \in \{0, 1, \ldots, 2^{n-1} - 1\} \tag{13}$$

Lemma 2 *If* $\mathbf{A} = van(a_0, a_1, \ldots, a_{2^n-1})$ *is also an SV matrix, then* $\tilde{\mathbf{A}} = van(\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{2^{n-1}-1})$ *is an SV matrix too.*

Proof

$$\tilde{a}_i + \tilde{a}_{i\oplus 2^k} = a_i^2 + R_{n-1} a_i + a_{i\oplus 2^k}^2 + R_{n-1} a_{i\oplus 2^k} = R_k^2 + R_k R_{n-1} = R'_k \tag{14}$$

and $\sum_{i=0}^{n-2}\mu'_i R'_i = \sum_{i=0}^{n-2}\mu'_i R_i^2 + R_{n-1}\sum_{i=0}^{n-2}\mu'_i R_i$. It is obvious that if $\mu'_i \in \{0, 1\}$, then $\mu_i^{'2} = \mu'_i$, also $\sum_{i=0}^{n-2}\mu'_i R_i^2 = (\sum_{i=0}^{n-2}\mu'_i R_i)^2$ and $\sum_{i=0}^{n-2}\mu'_i R'_i = (\sum_{i=0}^{n-2}\mu'_i R_i)(R_{n-1} + \sum_{i=0}^{n-2}\mu'_i R_i)$. Taking Definition 4 and Eq. 12 into account, $\sum_{i=0}^{n-2}\mu'_i R_i = 0 \Rightarrow \mu'_i = 0$, but $R_{n-1} + \sum_{i=0}^{n-2}\mu'_i R_i \neq 0$ because $\mu'_{n-1} \neq 0$, thus $\tilde{\mathbf{A}}$ is an SV matrix. □

Corollary 4 *As a result of these lemmas, for $2^n \times 2^n$ SV matrices where $n \geq 3$ we can show that $\sum_{i=0}^{7}a_i^7$ is non-zero and depends on R_0, R_1 and R_2.*

We know that $\sum_{i=0}^{7}a_i^7 = \sum_{i=0}^{3}(a_i^7 + a_{i\oplus 4}^7)$ and:

$$\begin{aligned} a_i^7 + a_{i\oplus 4}^7 &= (a_i + a_{i\oplus 2^2})^7 + (a_i a_{i\oplus 4})(a_i + a_{i\oplus 2^2})^5 \\ &\quad + (a_i^3 a_{i\oplus 4}^3)(a_i + a_{i\oplus 2^2}) \\ &= R_2^7 + a_i a_{i\oplus 4} R_2^5 + a_i^3 a_{i\oplus 4}^3 R_2 \end{aligned}$$

Thus

$$\begin{aligned} \sum_{i=0}^{7} a_i^7 &= \sum_{i=0}^{3}(a_i^7 + a_{i\oplus 4}^7) = \sum_{i=0}^{3} R_2^7 + R_2^5 \sum_{i=0}^{3} a_i a_{i\oplus 4} + R_2 \sum_{i=0}^{3} a_i^3 a_{i\oplus 4}^3 \\ &= R_2^5 \sum_{i=0}^{3} \tilde{a}_i + R_2 \sum_{i=0}^{3} \tilde{a}_i^3. \end{aligned}$$

By considering Lemma 1, Definition 5 and Lemma 2,

$$\sum_{i=0}^{3} \tilde{a}_i = 0 \text{ and}$$

$$R_2 \sum_{i=0}^{3} \tilde{a}_i^3 = R_2 R'_0 R'_1 (R'_0 + R'_1) = R_0 R_1 R_2 (R_0 + R_1)(R_0 + R_2)(R_1 + R_2)(R_0 + R_1 + R_2)$$

and finally $\sum_{i=0}^{7}a_i^7$ is a function of R_0, R_1 and R_2.

Theorem 5 *Assume $\mathbf{A}$ is a $2^n \times 2^n$ SV matrix. For elements of this matrix we have:*

$$\sum_{i=0}^{2^n-1} a_i^k = \begin{cases} f_{k,n}(R_0, R_1, \ldots, R_{n-1}) \neq 0 & HW(k) = n \text{ and } k \leq 2^{n+1} - 2 \\ 0 & HW(k) < n \text{ and } k \leq 2^{n+1} - 2 \end{cases} \tag{15}$$

where $f_{k,n}(R_0, R_1, \ldots, R_{n-1})$ is a non-zero value that only depends on R_i's and does not depend on a_0. Proof of this theorem appears in Appendix A.

In the following, we investigate constructing of $2^n \times 2^n$ FFHadamard involutory MDS matrices. We first introduce the procedure for $n = 3$, and then extend it for $n > 3$. By considering all lemmas and Theorem 5 for $k \leq 14$, $\sum_{i=0}^{7}a_i^k = f_{k,3}(R_0, R_1, R_2)$ if $k \in \{7, 11, 13, 14\}$, an 8×8 matrix $\mathbf{A1}$ is generated and multiplied by $\mathbf{A}$ as below:

$$\mathbf{A1}_{col(j)}=\begin{pmatrix} a_j^7\\ a_j^6\\ a_j^5\\ a_j^4\\ a_j^3\\ a_j^2\\ a_j\\ 1\end{pmatrix},\ \ \mathbf{A1}\times\mathbf{A}=\begin{pmatrix}
\sum_{i=0}^{7}a_i^7 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^{11} & 0 & \sum_{i=0}^{7}a_i^{13} & \sum_{i=0}^{7}a_i^{14}\\
0 & \sum_{i=0}^{7}a_i^7 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^{11} & 0 & \sum_{i=0}^{7}a_i^{13}\\
0 & 0 & \sum_{i=0}^{7}a_i^7 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^{11} & 0\\
0 & 0 & 0 & \sum_{i=0}^{7}a_i^7 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^{11}\\
0 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^7 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^7 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^7 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \sum_{i=0}^{7}a_i^7
\end{pmatrix} \tag{16}$$

The procedure for the 4×4 Vandermonde matrix can be repeated here for the 8×8 Vandermonde matrix, i.e. we can define a matrix $\mathbf{A2}$ from $\mathbf{A1}$ with three additional parameters s_0, s_1 and s_2, then we compute s_0, s_1 and s_2, such that $\mathbf{A2}\times\mathbf{A}$ becomes diagonal. Column j, $j=0,1,\ldots,7$ of $\mathbf{A2}$ is

$$\mathbf{A2}_{col(j)}=\begin{pmatrix} a_j^7+s_0a_j^3+s_1a_j+s_2\\ a_j^6+s_0a_j^2+s_1\\ a_j^5+s_0a_j\\ a_j^4+s_0\\ a_j^3\\ a_j^2\\ a_j\\ 1\end{pmatrix} \tag{17}$$

In order to make $\mathbf{A2}\times\mathbf{A}$ a diagonal matrix, s_0, s_1, s_2 must be:

$$s_0=\frac{\sum_{i=0}^{7}a_i^{11}}{\sum_{i=0}^{7}a_i^{7}},\quad s_1=\frac{\sum_{i=0}^{7}a_i^{13}}{\sum_{i=0}^{7}a_i^{7}},\quad s_2=\frac{\sum_{i=0}^{7}a_i^{14}}{\sum_{i=0}^{7}a_i^{7}}=\sum_{i=0}^{7}a_i^7$$

and $\mathbf{A}^{-1}=(\sum_{i=0}^{7}a_i^7)^{-1}\times\mathbf{A2}$. s_i's can be obtained from R_i's. For example $s_0=R_0^4+R_1^4+R_2^4+R_0^2R_1^2+R_0^2R_2^2+R_1^2R_2^2+R_0R_1R_2(R_0+R_1+R_2)$.

For SV matrices $\mathbf{A}=van(a_0,a_1,\ldots,a_{2^3-1})$ and $\mathbf{B}=van(b_0,b_1,\ldots,b_{2^3-1})$, where $a_i+b_j=a_l+b_{l\oplus i\oplus j}$ and a_i's and b_j's are different, we can prove that $\mathbf{BA}^{-1}$ is an 8×8 FFHadamard involutory MDS matrix. If we consider this procedure for all $2^n\times 2^n$ SV matrices $\mathbf{A}$, we can calculate the inverse of $\mathbf{A}$ as $\mathbf{A}^{-1}=(\sum_{i=0}^{2^n-1}a_i^{2^n-1})^{-1}\mathbf{A2}$, where column j of $\mathbf{A2}$ is

$$
\mathbf{A2}_{col(j)} = \begin{pmatrix} a_j^{2^{n-1}+2^{n-2}+\cdots+1} + s_0 a_j^{2^{n-2}+2^{n-3}+\cdots+1} + \cdots + s_{n-2}a_j + s_{n-1} \\ \vdots \\ a_j^{2^{n-1}+2^{n-2}} + s_0 a_j^{2^{n-2}} + s_1 \\ \vdots \\ a_j^{2^{n-1}} + s_0 a_j \\ a_j^{2^{n-1}} + s_0 \\ \vdots \\ a_j \\ 1 \end{pmatrix} \tag{18}
$$

and parameters $s_0, s_1, \ldots, s_{n-1}$ are:

$$
s_0 = \frac{\sum_{i=0}^{2^n-1} a_i^{2^{n+1}-2^{n-1}-1}}{\sum_{i=0}^{2^n-1} a_i^{2^n-1}}, \quad s_1 = \frac{\sum_{i=0}^{2^n-1} a_i^{2^{n+1}-2^{n-2}-1}}{\sum_{i=0}^{2^n-1} a_i^{2^n-1}}, \quad \cdots; \quad s_{n-1} = \frac{\sum_{i=0}^{2^n-1} a_i^{2^{n+1}-1-1}}{\sum_{i=0}^{2^n-1} a_i^{2^n-1}} \tag{19}
$$

Similarly to what is mentioned in Corollary 2, we can calculate s_i as functions of R_k's. $\mathbf{BA}^{-1}$ is a $2^n \times 2^n$ FFHadamard involutory MDS matrix if $a_i + b_j = a_l + b_{l \oplus i \oplus j}$ and $a_i \neq b_j$ (for all $i, j, l \in \{0, 1, \ldots, 2^n - 1\}$). Moreover, the complexity for computing the inverse of $\mathbf{A}$ is $\mathcal{O}(n^2)$. Two numerical examples are given in Appendix B.

4 Comparison with previous methods

Definition 6 Assume $x_0, x_1, \ldots, x_{n-1}$ and $y_0, y_1, \ldots, y_{n-1}$ are different values in $GF(2^q)$. Matrix $\mathbf{P} = [p_{i,j}]$ is a Cauchy matrix if $p_{i,j} = \frac{1}{x_i + y_j}$ [11,17].

If x_i's and y_j's have different values, $x_i + y_j \neq 0$ holds for all i, j. This yields that any square sub-matrix of a Cauchy matrix is nonsingular over any field [11,17], i.e. $\mathbf{P}$ is an MDS matrix. If dimensions of $\mathbf{P}$ are $2^n \times 2^n$ and $y_i = x_i + \Delta$, where Δ has some properties, then $\mathbf{P}$ is an FFHadamard MDS matrix [17] and $\mathbf{P}^2 = c^2\mathbf{I}$ where $c = \sum_{i=0}^{2^n-1} p_{0,i}$. Thus $\mathbf{P}' = \frac{\mathbf{P}}{c}$ is an FFHadamard involutory MDS matrix.

The method studied in this paper has some advantages over the method of using Cauchy matrices to generate involutory MDS matrices:

- In the proposed method, we have involutory property for arbitrary dimensions.
- We can present a direct inverse for $2^n \times 2^n$ SV matrices.

Inversion of Vandermonde matrices is an interesting problem in mathematics. A method is introduced in [16] whose complexity for the calculation of the inverse of a $n \times n$ Vandermonde matrix is $\mathcal{O}(n^2)$, but the coefficient of n^2 in [16] is greater than the inversion method introduced in this paper for the SV matrices. A direct method to calculate the inverse of special class of Vandermonde matrices, where the elements are the roots of $x^n - x = 0$ in $GF(p^q)$ and n is relatively prime to p, has been investigated in [1]. Compared with the method introduced in [1], our proposed inversion method based on SV matrix covers other classes of Vandermonde matrices.

5 Conclusion

In this paper, we investigated Vandermonde matrix in the finite field $GF(2^q)$. First, we presented a method to construct an involutory MDS matrix from two Vandermonde matrices. In contrast to previous work which only supports involutory MDS matrices of size $2^n \times 2^n$, our methods constructs involutory MDS matrices with arbitrary size. In Sect. 3, we defined a class of Vandermonde matrices for $2^n \times 2^n$ matrices as Special Vandermonde matrices whose inverse matrix can be directly calculated. If $\mathbf{A}$ and $\mathbf{B}$ are two SV matrices with distinct a_i and b_j, we proved that $\mathbf{AB}^{-1}$ is an FFHadamard involutory MDS matrix. In Table 1, we compare MDS matrices constructed based on our proposal with some of the known MDS matrices.

Although in this paper, we emphasized on cryptographic applications of Vandermonde matrices, this method can be used in other applications for these matrices in the finite fields such as coding theory.

A Proof of Theorem 5

Recalling Definitions 4 and 5 for an SV matrix, we know $a_i + a_{i\oplus 2^{n-1}} = R_{n-1}$ and $a_i a_{i\oplus 2^{n-1}} = \tilde{a}_i$. To prove Theorem 5, first we try to obtain $a_i^k + a_{i\oplus 2^{n-1}}^k$ as a function of $\tilde{a}_i$ and R_{n-1}. For this propose, we introduce a new representation which will be useful for the proof of Theorem 5.

Definition A1 For each $a, b \in GF(2^q)$, $a^l + b^l$ can be represented as below:

$$\begin{aligned} a^l + b^l &= \sum_{i=0}^{\lfloor \frac{l}{2} \rfloor} \lambda_{l,i} (a+b)^{l-2i} (ab)^i \\ &= \lambda_{l,0}(a+b)^l + \lambda_{l,1}(a+b)^{l-2}ab + \lambda_{l,2}(a+b)^{l-4}a^2b^2 \\ &\quad + \cdots + \lambda_{l,\lfloor \frac{l}{2} \rfloor}(a+b)^{l-2\lfloor \frac{l}{2} \rfloor} a^{\lfloor \frac{l}{2} \rfloor} b^{\lfloor \frac{l}{2} \rfloor} \end{aligned}$$

where $\lambda_{l,i}$'s are binary coefficients ($\lambda_{l,k} \in \{0, 1\}$). For convenience, let us call this representation, Special Extended Form representation or SEF representation of $a^l + b^l$ in the $GF(2^q)$. Note that in the SEF representation $\lambda_{l,0}$ is always equal to 1. Also it is obvious that $\lambda_{l,i} = 0$ for $i > \lfloor \frac{l}{2} \rfloor$.

In $GF(2^q)$ we easily see that:

$$a^l + b^l = (a+b)(a^{l-1} + b^{l-1}) + ab(a^{l-2} + b^{l-2}). \tag{A1}$$

This relationship has an important role in the following proofs. First six lemmas are given and finally Theorem 5 is proven.

Lemma A1 *We can define SEF representation for $(ab)(a^l + b^l)$ (with coefficients $\Gamma_{l,i}$) and $(a+b)(a^l + b^l)$ (with coefficients $\Lambda_{l,i}$) in the finite field $GF(2^q)$ as below:*

$$ab(a^l + b^l) = \sum_{i=0}^{\lfloor \frac{l}{2}+1 \rfloor} \Gamma_{l,i} (a+b)^{l-2i-2} (ab)^i \quad \text{and}$$

$$(a+b)(a^l + b^l) = \sum_{i=0}^{\lfloor \frac{l}{2}+1 \rfloor} \Lambda_{l,i} (a+b)^{l-2i+1} (ab)^i$$

Table 1 Comparison between MDS matrix

Cipher	Type of MDS matrix	Dimensions	Cost	Involutory	Finite field	Reference
Anubis	Hadamard (obtained from search)	4×4	6 xtimes and 12 XORs	Yes	$GF(2^8)$	[4]
AES	Circulant	4×4	4 xtimes and 12 XORs	No	$GF(2^8)$	[5]
Khazad	Hadamard (Obtained from search)	8×8	24 xtimes and 76 XORs	Yes	$GF(2^8)$	[3]
Maelstrom	Low weight matrix	8×8	24 xtimes and 72 XORs	No	$GF(2^8)$	[6]
AES-MDS	Hadamard (Obtained from Cauchy matrix)	16×16	688 xtimes and 272 XORs	Yes	$GF(2^8)$	[13]
New	Based on Vandermonde matrices	3×3	5 xtimes and 8 XORs	Yes	$GF(2^8)$	This paper (Appendix B)
New	Hadamard (Based on Vandermonde matrices)	4×4	12 xtimes and 16 XORs	Yes	$GF(2^8)$	This paper (Appendix B)
New	Hadamard (Based on Vandermonde matrices)	$2^n \times 2^n$	–	Yes	$GF(2^q)$	This paper

where the relations between $\Gamma_{l,i}$ and $\Lambda_{l,i}$ with $\lambda_{l,i}$ are (Note that $\lambda_{l,i}$ is the coefficients of $(ab)^i$ in the SEF representation of $(a^l + b^l)$)

$$\Lambda_{l,i} = \begin{cases} \lambda_{l,i} & 0 \le i \le \lfloor \frac{l}{2} \rfloor \\ 0 & otherwise \end{cases}$$

$$\Gamma_{l,i} = \begin{cases} \lambda_{l,i-1} & 1 \le i \le \lfloor \frac{l}{2} + 1 \rfloor \\ 0 & i = 0 \end{cases}$$

The proof of this lemma is easily performed from definition of SEF representation.

Lemma A2 *In $GF(2^q)$, all $\lambda_{2k,k}$'s are 0 and all $\lambda_{2k+1,k}$'s are 1.*

Proof Induction is used for this proof. We know that $a^2 + b^2 = (a+b)^2$ and $a^3 + b^3 = (a+b)^3 + ab(a+b)$ which means $\lambda_{2,1} = 0$ and $\lambda_{3,1} = 1$. Assume this lemma holds for $k-1$ (i.e., $\lambda_{2k-2,k-1} = 0$ and $\lambda_{2k-1,k-1} = 1$). For $\lambda_{2k,k}$ in SEF representation, we have:

$$a^{2k} + b^{2k} = (a+b)(a^{2k-1} + b^{2k-1}) + ab(a^{2k-2} + b^{2k-2})$$

and from this equation, we yield :

$$\lambda_{2k,k} = \Lambda_{2k-1,k} + \Gamma_{2k-2,k}$$

Taking Definition A1($\lambda_{l,i} = 0$ if $\lfloor \frac{l}{2} \rfloor < i$) and Lemma A1 into account, $\Lambda_{2k-1,k} = \lambda_{2k-1,k} = 0$. Also based on the induction hypothesis $\lambda_{2k-2,k-1} = 0$ thus Lemma A1 yields $\Gamma_{2k-2,k} = 0$. Finally by adding these two terms, we yield $\lambda_{2k,k} = 0$.

For $\lambda_{2k+1,k}$ in SEF representation, we have:

$$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} + b^{2k}) + ab(a^{2k-1} + b^{2k-1})$$

thus from this equation, we yield:

$$\lambda_{2k+1,k} = \Lambda_{2k,k} + \Gamma_{2k-1,k} = \lambda_{2k,k} + \lambda_{2k-1,k-1} = 0 + 1 = 1.$$

□

Lemma A3 *Assume $l = (2j+1) \times 2^m$. Then for the coefficients in the SEF representation, we have:*

$$\lambda_{(2j+1)\times 2^m, i} = \begin{cases} 1 & i = 0 \\ \lambda_{2j+1,t} & i = 2^m \times t (t \le j) \\ 0 & otherwise \end{cases}.$$

Proof SEF representation of $a^{2j+1} + b^{2j+1}$ is:

$$a^{2j+1} + b^{2j+1} = (a+b)^{2j+1} + \lambda_{2j+1,1}(a+b)^{2j-1}ab + \cdots + \lambda_{2j+1,j}(a+b)a^j b^j$$

and by powering two sides of the above equation in the $GF(2^q)$ we have:

$$\begin{aligned}&(a^{2j+1} + b^{2j+1})^{2^m} = a^{(2j+1)2^m} + b^{(2j+1)2^m} = \\ &(a+b)^{(2j+1)2^m} + \lambda_{2j+1,1}(a+b)^{(2j-1)\times 2^m} a^{2^m} b^{2^m} + \cdots + \lambda_{2j+1,j}(a+b)^{2^m} a^{j\times 2^m} b^{j\times 2^m}\end{aligned}$$

□

We conclude from this lemma that coefficients of $a^l + b^l$ where l is even may be obtained from the coefficients of $a^{l'} + b^{l'}$ when l' is odd and $l = 2^t \times l'$.

Lemma A4 *In SEF representation, for $l = 2^n$, $l = 2^n + 1$ and $l = 2^n - 1$, the coefficients $\lambda_{l,i}$ are:*

$$\text{(a)} \qquad \lambda_{2^n,i} = \begin{cases} 1 & i = 0 \\ 0 & otherwise \end{cases}$$

$$\text{(b)} \qquad \lambda_{2^n+1,i} = \begin{cases} 1 & i = 0 \; or \; 2^t, \;\; 0 \le t < n-1 \\ 0 & otherwise \end{cases}$$

$$\text{(c)} \qquad \lambda_{2^n-1,i} = \begin{cases} 1 & i = 2^t - 1, \;\; 0 \le t < n-1 \\ 0 & otherwise \end{cases}$$

Proof (a) We know $a^{2^n} + b^{2^n} = (a+b)^{2^n} = (a+b)^{2^n}(ab)^0$ in $GF(2^q)$. Thus if $\lambda_{2^n,i} = 1$, then $i = 0$.

(b) To obtain coefficients of the form $\lambda_{2^n+1,i}$, we use induction. This lemma holds for $k = 1$. Assume the hypothesis is correct for $\lambda_{2^k+1,i}$. We prove this for $\lambda_{2^{k+1}+1,i}$. Considering Eq. A1, we have the following equation:

$$\begin{aligned} & a^{2^{k+1}+2} + b^{2^{k+1}+2} = (a+b)(a^{2^{k+1}+1} + b^{2^{k+1}+1}) + ab(a^{2^{k+1}} + b^{2^{k+1}}) \\ & \Rightarrow (a+b)(a^{2^{k+1}+1} + b^{2^{k+1}+1}) = a^{2^{k+1}+2} + b^{2^{k+1}+2} + ab(a^{2^{k+1}} + b^{2^{k+1}}) \\ & \Rightarrow \Lambda_{2^{k+1}+1,i} = \lambda_{2^{k+1}+2,i} + \Gamma_{2^{k+1},i}. \end{aligned}$$

In $GF(2^q)$, $(a^{2^{k+1}+2} + b^{2^{k+1}+2}) = (a^{2^k+1} + b^{2^k+1})^2$ and by considering Lemma A3 and the induction hypothesis, coefficients of $(a^{2^k+1} + b^{2^k+1})^2$ are:

$$\lambda_{2^{k+1}+2,i} = \begin{cases} 1 & i = 0 \; or \; i = 2^t, 1 \le t \le k \\ 0 & otherwise \end{cases}.$$

By considering Lemmas A1 and A4(a), $\Gamma_{2^{k+1},i}$ coefficients are:

$$\Gamma_{2^{k+1},i} = \begin{cases} 1 & i = 1 \\ 0 & otherwise \end{cases}$$

and finally:

$$\Lambda_{2^{k+1}+1,i} = \lambda_{2^{k+1}+2,i} + \Gamma_{2^{k+1},i} = \begin{cases} 1 & i = 0 \; or \; i = 2^t, 0 \le t \le k \\ 0 & otherwise \end{cases}.$$

Considering Lemma A1 ($\lambda_{2^{k+1}+1,i} = \Lambda_{2^{k+1}+1,i}, \;\; i \le 2^k$) proof is complete for coefficient $\lambda_{2^{k+1}+1,i}$.

(c) For $\lambda_{2^{k+1}-1,i}$ we use the equation below:

$$\begin{aligned} a^{2^k+1} + b^{2^k+1} &= (a+b)(a^{2^k} + b^{2^k}) + ab(a^{2^k-1} + b^{2^k-1}) \\ \Rightarrow ab(a^{2^k-1} + b^{2^k-1}) &= a^{2^k+1} + b^{2^k+1} + (a+b)(a^{2^k} + b^{2^k}). \end{aligned}$$

Based on Lemmas A4(a) and A4(b) we have:

$$\Gamma_{2^k-1,i} = \lambda_{2^k+1,i} + \Lambda_{2^k,i} =$$
$$\begin{cases} 1 & i = 0 \; or \; i = 2^t, \;\; 0 \le t \le k-1 \\ 0 & otherwise \end{cases} + \begin{cases} 1 & i = 0 \\ 0 & otherwise \end{cases} = \begin{cases} 1 & i = 2^t, 0 \le t \le k-1 \\ 0 & otherwise \end{cases}$$

by considering relation $\Gamma_{2^k-1,i} = \lambda_{2^k-1,i-1}$ for $i > 0$ in Lemma A1, the only non-zero coefficients of SEF representation of $(a^{2^k-1} + b^{2^k-1})$ are $\lambda_{2^k-1,2^t-1}$, $0 \le t \le k-1$. □

Lemma A5 *Assume $HW(X)$ is the number of ones in the binary representation of a number X.*

(a) *When X increases by 1, $HW(X)$ increases at most by 1 i.e. $HW(X+1) \leq HW(X)+1$.*
(b) $HW(X) = HW(2^t X)$.
(c) $HW(2X + 1) = HW(X) + 1$.

Example A1 $HW(7)$ increases by one in comparison with $HW(6)$, but $HW(16) = 1$ decreases by three in comparison with $HW(15) = 4$. Also $HW(3) = HW(6) = HW(12) = HW(24) = 2$. $HW(7) = HW(3) + 1 = 3$

We can deduce 2 corollaries from Lemmas A3, A4 and A5.

Corollary A1 *If the non-zeroness condition on $\lambda_{l,i}$ is $HW(i) < r$, then non-zeroness condition on $\lambda_{2^t l,i'}$ is $HW(i') < r$.*

We observe from Lemma A3, $\lambda_{l,i} = 1 \Leftrightarrow \lambda_{2^t l,2^t i} = 1$, meanwhile $HW(i) = HW(i' = 2^t i) < r$.

Corollary A2 *If the non-zeroness condition on $\lambda_{l,i}$ is $HW(i) < r$, then the non-zeroness condition on $\Gamma_{l,i}$ is $HW(i) < r + 1$ and the non-zeroness condition on $\Lambda_{l,i}$ is $HW(i) < r$.*

We observe in Lemma A1 that $\Gamma_{l,i+1} = 1 \Leftrightarrow \lambda_{l,i} = 1$ and $HW(i+1) \leq HW(i)+1 < r+1$.

Lemma A6 *In the SEF representation of $a^l + b^l$, the coefficient $\lambda_{l,i}$ may be one if $HW(i) < HW(l)$. Also we are sure that $\lambda_{l,i} = 0$ if $HW(i) \geq HW(l)$.*

Proof We only prove three sub-cases and proof of other sub-cases will be the same.

- If $HW(l) = 1$, then l must be of the form 2^k. Thus from Lemma A4(a), If $\lambda_{2^k,i} = 1$, then $i = 0$ and $HW(i) = 0$.

- If $HW(l) = 2$, then l must be of the form $2^{k_1} + 2^{k_2} (k_1 > k_2)$. We conclude from Lemma A3, coefficient of $a^l + b^l, l = 2^{k_1} + 2^{k_2}$ can be obtained from coefficient of $a^{l'} + b^{l'}, l' = 2^{k_1 - k_2} + 1$. In Lemma A4(b), if $\lambda_{2^{k'}+1,i} = 1$, then $i = 0$ or $i = 2^t$ which $HW(i) = 0, 1$. By considering to Corollary A1, if $HW(l) = 2$, then $\lambda_{l,i}$ may be one when $HW(i) = 0$ or 1.

- If $HW(l) = 3$, then l must be of the form $2^{k_1} + 2^{k_2} + 2^{k_3} (k_1 > k_2 > k_3)$. We conclude from Lemma A3, coefficients of $a^l + b^l, l = 2^{k_1} + 2^{k_2} + 2^{k_3}$ can be obtained from coefficients of $a^{l'} + b^{l'}, l' = 2^{k_1 - k_3} + 2^{k_2 - k_3} + 1$. In the following we use induction for $l' = 2^{j_1} + 2^{j_2} + 1$. Considering Lemma A4(c), this lemma holds for $l' = 7$ which is the smallest number with three ones in its binary representation ($\lambda_{7,i} = 1 \Rightarrow i = 0, 1, 3 (HW(i) < 3)$). Assume this lemma is true for all l' that $l' = 2^{j_1} + 2^{j_2} + 1$ $(0 < j_2 < j_1)$. Taking equation (A1) into account, for $l' = 2^{j_1+1} + 2^{j_3} + 1$ $(0 < j_3 < j_1 + 1)$, we have:

$$\begin{aligned}
a^{2^{j_1+1}+2^{j_3}+2} + b^{2^{j_1+1}+2^{j_3}+2} &= (a+b)(a^{2^{j_1+1}+2^{j_3}+1} + b^{2^{j_1+1}+2^{j_3}+1}) \\
&\quad + ab(a^{2^{j_1+1}+2^{j_3}} + b^{2^{j_1+1}+2^{j_3}}) \Rightarrow (a+b)(a^{2^{j_1+1}+2^{j_3}+1} + b^{2^{j_1+1}+2^{j_3}+1}) \\
&= a^{2^{j_1+1}+2^{j_3}+2} + b^{j_1+1+2^{j_3}+2} + ab(a^{2^{j_1+1}+2^{j_3}} + b^{2^{j_1+1}+2^{j_3}}) \\
&\Rightarrow \Lambda_{2^{j_1+1}+2^{j_3}+1,i} = \lambda_{2^{j_1+1}+2^{j_3}+2,i} + \Gamma_{2^{j_1+1}+2^{j_3},i}.
\end{aligned}$$

Also by considering the induction hypothesis and Corollary A1, necessary conditions for the non-zeroness of the coefficients $\lambda_{2^{j_1+1}+2^{j_3}+2,i}$ is that $HW(i) < 3$ (because $2^{j_1+1}+2^{j_3}+2 = 2(2^{j_1}+2^{j_3-1}+1)$). By considering Lemma A3 and A4, in the SEF representation of $a^{2^{j_1+1}+2^{j_3}}+b^{2^{j_1+1}+2^{j_3}}$ property of non-zero coefficient $\lambda_{2^{j_1+1}+2^{j_3},i}$ is $HW(i) < 2$. By considering Corollary A2, the coefficient $\Gamma_{2^{j_1+1}+2^{j_3},i}$ is non-zero if $HW(i) < 3$. By adding two terms, we conclude that in SEF representation, coefficients $\Lambda_{2^{j_1+1}+2^{j_3}+1,i} = \lambda_{2^{j_1+1}+2^{j_3}+1,i}$ may be non-zero when $HW(i) < 3$.

For other sub-cases $HW(l) \geq 4$, we prove this theorem step by step, by using results for coefficients $\lambda_{l',i}$ that $HW(l') < HW(l)$. We aslo use induction similar to sub-case $HW(l) = 3$; for example for $HW(l) = 4$, we use the below equations and the above inductive procedure for the sub-case $HW(l) = 3$.

$$
\begin{aligned}
&a^{2^{j_1+1}+2^{j_2}+2^{j_3}+2}+b^{2^{j_1+1}+2^{j_2}+2^{j_3}+2} = \\
&(a+b)(a^{2^{j_1+1}+2^{j_2}+2^{j_3}+1}+b^{2^{j_1+1}+2^{j_2}+2^{j_3}+1}) + ab(a^{2^{j_1+1}+2^{j_2}+2^{j_3}}+b^{2^{j_1+1}+2^{j_2}+2^{j_3}})
\end{aligned}
$$

□

After expressing these six lemmas, now we can prove Theorem 5.

Theorem 5 *Assume* $\mathbf{A} = van(a_0, a_1, \ldots, a_{2^n-1})$ *is a* $2^n \times 2^n$ *SV matrix in the finite field* $GF(2^q)$. *For elements of this matrix we have:*

$$
\sum_{i=0}^{2^n-1} a_i^k = \begin{cases} f_{k,n}(R_0, R_1, \ldots, R_{n-1})) \neq 0 & HW(k) = n \text{ and } k \leq 2^{n+1}-2 \\ 0 & HW(k) < n \text{ and } k \leq 2^{n+1}-2 \end{cases}.
$$

Proof As we observed before in Sect. 4.1, this theorem is true for $n = 2$. We assume that this theorem is true for $n > 2$ and prove it for $n+1$. In a $2^{n+1} \times 2^{n+1}$ SV Matrix, each $\sum_{i=0}^{2^{n+1}-1} a_i^k$ can be represented as below:

$$
\sum_{i=0}^{2^{n+1}-1} a_i^k = \sum_{i=0}^{2^n-1} (a_i^k + a_{i\oplus 2^n}^k)
$$

SEF representation of $(a_i^l + a_{i\oplus 2^n}^l)$ is:

$$
\begin{aligned}
&a_i^l + a_{i\oplus 2^n}^l = \\
&(a_i + a_{i\oplus 2^n})^l + \lambda_{l,1}(a_i + a_{i\oplus 2^n})^{l-2} a_i a_{i\oplus 2^n} + \lambda_{l,2}(a_i + a_{i\oplus 2^n})^{l-4}(a_i a_{i\oplus 2^n})^2 \\
&\quad + \cdots + \lambda_{l,\lfloor \frac{l}{2} \rfloor}(a_i + a_{i\oplus 2^n})^{l-2\times\lfloor \frac{l}{2} \rfloor}(a_i a_{i\oplus 2^n})^{\lfloor \frac{l}{2} \rfloor} \\
&= (R_n)^l + \lambda_{l,1}(R_n)^{l-2}\tilde{a}_i + \lambda_{l,2}(R_n)^{l-4}\tilde{a}_i^2 + \cdots + \lambda_{l,\lfloor \frac{l}{2} \rfloor}(R_n^{l-2\times\lfloor \frac{l}{2} \rfloor})\tilde{a}_i^{\lfloor \frac{l}{2} \rfloor}
\end{aligned}
$$

where $\tilde{a}_i$ belongs to the $2^n \times 2^n$ SV matrix $\tilde{\mathbf{A}} = van(\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{2^n-1})$. Therefore,

$$
\sum_{i=0}^{2^{n+1}-1} a_i^k = \sum_{i=0}^{2^n-1} \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (\lambda_{k,j} R_n^{k-2j} \tilde{a}_i^j) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (\lambda_{k,j} R_n^{k-2j} \sum_{i=0}^{2^n-1} \tilde{a}_i^j).
$$

From Lemma 2, we know that if $\sum_{i=0}^{2^n-1} a_i^j = f_{j,n}(R_0, R_1, \ldots, R_{n-1})$, then $\sum_{i=0}^{2^n-1} \tilde{a}_i^j = f_{j,n}(R'_0, R'_1, \ldots, R'_{n-1})$, where $R'_i = R_i^2 + R_i R_n$. Therefore, $f_{j,n}(R'_0, R'_1, \ldots, R'_{n-1})$ is a function of $R_0, R_1, \ldots, R_{n-1}, R_n$ and we can assume $f_{j,n}(R'_0, R'_1, \ldots, R'_{n-1}) = g_{j,n}(R_0, R_1, \ldots, R_n)$.

By considering the induction hypothesis, $\sum_{i=0}^{2^n-1}\tilde{a}_i^j \neq 0$ when $HW(j) = n$. Thus we search for $\lambda_{k,j} \neq 0$ such that $HW(j) = n$ because

$$\sum_{i=0}^{2^{n+1}-1} a_i^k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor}(\lambda_{k,j} R_n^{k-2j}\sum_{i=0}^{2^n-1}\tilde{a}_i^j) = \begin{cases} \sum\limits_{j:\lambda_{j,k}=1} g_{j,n}(R_0, R_1, \ldots, R_n) & HW(j) = n \\ 0 & otherwise \end{cases}$$

By considering Lemma A6, the non-zeroness condition for $HW(j) = n$ is that $HW(j) = n < HW(k)$. Since $k \leq 2^{n+1} - 2$ is true, we are also sure that $HW(k) \leq n+1$ is true. Thus the only acceptable value for $HW(k)$ is $n+1$. Therefore, if $HW(k) < n+1$, then $\sum_{i=0}^{2^{n+1}-1} a_i^k = 0$. In the following we prove that when $HW(k) = n+1$, $\sum_{i=0}^{2^{n+1}-1} a_i^k = \sum_{j:\lambda_{j,k}=1} g_{j,n}(R_0, R_1, \ldots, R_n) = f_{k,n+1}(R_0, R_1, \ldots, R_n)$. One can easily see that the set of all $n+2$-bit values of k with $n+1$ ones is:

$$S_k = \{2^{n+2} - 2^{n+1} - 1, 2^{n+2} - 2^n - 1, 2^{n+2} - 2^{n-1} - 1, \ldots, 2^{n+2} - 2 - 1, 2^{n+2} - 1 - 1\}$$

In this set, there exists $n+1$ odd values and only one even value. Let us prove the existence of at least one $\lambda_{k,j}$ for the odd values of $k \in S_k$. In Lemma A2, $\lambda_{2l+1,l} = 1$ and we observe $2^{n+2} - 2^k - 1 = 2(2^{n+1} - 2^{k-1} - 1) + 1, k \neq 0$ that $HW(2^{n+1} - 2^{k-1} - 1) = n$. Thus for the odd values $2^{n+2} - 2^k - 1$ exist $j = 2^{n+1} - 2^{k-1} - 1$ that $HW(j) = n$ and $\lambda_{2^{n+2}-2^k-1,j} = 1$. The only even value in S_k is $2^{n+2} - 1 - 1 = 2(2^{n+2} - 2^{n+1} - 1)$. For this value of k, we have:

$$\sum_{i=0}^{2^{n+1}-1} a_i^{2^{n+2}-1-1} = \left(\sum_{i=0}^{2^{n+1}-1} a_i^{2^{n+2}-2^{n+1}-1}\right)^2$$

and therefore the theorem is proven. □

Note that based on Definition 5, we can prove by induction:

$$\sum_{i=0}^{2^n-1} a_i^{2^n-1} = R_0R_1...R_{n-1}(R_0 + R_1)...(R_{n-2} + R_{n-1})...(R_0 + R_1 + ... + R_{n-1})$$

So based on Definition 4, $\sum\limits_{i=0}^{2^n-1} a_i^{2^n-1} = 0$ is always non-zero, and consequently $\left(\sum\limits_{i=0}^{2^n-1} a_i^{2^n-1}\right)^{-1}$ exists for each SV matrix.

B Numerical example

In this section, two numerical examples for constructing of involutory MDS matrices and $2^n \times 2^n$ FFHadamard involutory MDS matrices are presented.

Example B1 For $m = 3$, the Vandermonde matrix $\mathbf{A} = van(0x1, 0x3, 0x7e)$, the parameter $\Delta = 0xef$, and the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, we have the involutory MDS matrix $\mathbf{BA}^{-1}$ as below:

$$\mathbf{BA}^{-1} = \begin{pmatrix} 0x2 & 0x7 & 0x4 \\ 0x3 & 0x6 & 0x4 \\ 0x3 & 0x7 & 0x5 \end{pmatrix}$$

We multiply 3×3 involutory MDS matrices to an array as below

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0x2 & 0x7 & 0x4 \\ 0x3 & 0x6 & 0x4 \\ 0x3 & 0x7 & 0x5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

If three temporary variables $T1$, $T2$, and $T3$ are used to calculate y_1, y_2 and y_3, we have:

$$\begin{aligned} T_1 &= 2x_1, \quad T_2 = 7x_2, \quad T_3 = 4x_3 \\ y_1 &= T_1 + T_2 + T_3 \\ y_2 &= y_1 + x_1 + x_2 \\ y_3 &= y_1 + x_1 + x_3 \end{aligned}$$

As a result of the calculations above, we need 5 xtimes (one xtime for T_1, two xtimes for T_2 and two xtimes for T_3) and 8 XOR operations (two XORs for T_2, two XORs for y_1, two XORs for y_2 and two XORs for y_3).

Example B2 For $m = 4$, an SV matrix of parameters $a_0 = 0x3$, $R_0 = 0x1$ and $R_1 = 0xb6$ (i.e., $\mathbf{A} = van(0x3, 0x2, 0xb5, 0xb4)$), $a_i + b_i = 0x46$, and the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, we have the FFHadamard MDS matrix $\mathbf{BA}^{-1}$ as below:

$$\mathbf{BA}^{-1} = \begin{pmatrix} 0x1 & 0x5 & 0x12 & 0x17 \\ 0x5 & 0x1 & 0x17 & 0x12 \\ 0x12 & 0x17 & 0x1 & 0x5 \\ 0x17 & 0x12 & 0x5 & 0x1 \end{pmatrix}$$

and based on the method introduced in Sect. 3.1, the inverse of this SV matrix is computed as:

$$\mathbf{A}^{-1} = \begin{pmatrix} 0xc2 & 0xa3 & 0x5 & 0x65 \\ 0x41 & 0x51 & 0xef & 0xff \\ 0x30 & 0x20 & 0x9f & 0x8f \\ 0x10 & 0x10 & 0x10 & 0x10 \end{pmatrix}$$

where $s_0 = 0xd8$ ($s_0^{-1} = 0x10$) and $s_1 = 0xd9$.

We multiply this 4×4 involutory MDS matrices to an array as below

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 0x1 & 0x5 & 0x12 & 0x17 \\ 0x5 & 0x1 & 0x17 & 0x12 \\ 0x12 & 0x17 & 0x1 & 0x5 \\ 0x17 & 0x12 & 0x5 & 0x1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Like Anubis, if four temporary variables $T1$, $T2$, $T3$ and $T4$ are used to calculate y_1, y_2 and y_3, we have:

$$T_1 = 0x5(x_2 + x_4), \quad T_2 = 0x12(x_3 + x_4), \quad T_3 = 0x5(x_1 + x_3), \quad T_4 = 0x12(x_1 + x_2)$$
$$y_1 = x_1 + T_1 + T_2$$
$$y_2 = x_2 + T_3 + T_2$$
$$y_3 = x_3 + T_1 + T_4$$
$$y_3 = x_4 + T_3 + T_4$$

By the above calculation, we need 12 xtimes (four xtimes for T_1 and T_3, eight xtimes for T_2 and T_4) and 16 XOR operations (two XORs for each T_is, two XORs for calculation of y_is).

References

1. Althaus H.L., Leake R.J.: Inverse of a finite-field Vandermonde matrix. IEEE Trans. Inform. Theory **15**, 173 (1969).
2. Biham E., Shamir A.: Differential Cryptanalysis of the Data Encryption Standard. Springer, Berlin (1993).
3. Barreto P., Rijmen V.: The Anubis Block Cipher. Submission to the NESSIE Project (2000). Available at http://cryptonessie.org.
4. Barreto P., Rijmen V.: The Khazad Legacy-Level Block Cipher. Submission to the NESSIE Project (2000). Available at http://cryptonessie.org.
5. Daemen J., Rijmen V.: The Design of Rijndael: AES—The Advanced Encryption Standard. Springer, Berlin (2002).
6. Filho G.D., Barreto P., Rijmen V.: The Maelstrom-0 hash function. In: Proceedings of the 6th Brazilian Symposium on Information and Computer Systems Security (2006).
7. Gauravaram P., Knudsen L.R., Matusiewicz K., Mendel F., Rechberger C., Schlaffer M., Thomsen S.: Grøstl a SHA-3 Candidate. Submission to NIST (2008). Available at http://www.groestl.info.
8. Junod P., Vaudenay S.: Perfect Diffusion primitives for block ciphers building efficient MDS matrices. In: SAC'04, pp. 84–99. Springer, Heidelberg (2004).
9. Lacan J., Fimes J.: Systematic MDS erasure codes based on vandermonde matrices. IEEE Trans. Commun. Lett. **8**(9), 570–572 (2004).
10. Lin S., Costello D.: Error Control Coding: Fundamentals and Applications, 2nd edn. Prentice Hall, Englewood Cliffs (2004).
11. MacWilliams F.J., Sloane N.J.A.: The theory of error correcting codes. North-Holland (1977).
12. Matsui M.: Linear cryptanalysis method for DES cipher. In: EUROCRYPT'93, pp. 386–397. Springer, Heidelberg (1993).
13. Nakahara J. Jr., Abrahao E.: A new involutory MDS matrix for the AES. IJNS **9**(2), 109–116 (2009).
14. Rijmen V.: Cryptanalysis and Design of Iterated Block Ciphers. Ph.D. thesis, Dept. Elektrotechniek Katholieke Universiteit Leuven, pp. 228–238 (1998).
15. Sony Corporation: The 128-bit Block cipher CLEFIA: Algorithm Specification (2007). Available at http://www.sony.co.jp/Products/cryptography/clefia/download/data/clefia-spec-1.0.pdf.
16. Yan S., Yang A.: Explicit algorithm to the inverse of Vandermonde matrix. In: ICTM 2009, pp. 176–179 (2009).
17. Youssef A.M., Mister S., Tavares S.E.: On the design of linear transformations for substitution permutation encryption networks. In: SAC'97, pp. 1–9 (1997).